CIS Controls Assessment Specification for Controls v7.1

Release 2025 Q1

Center for Internet Security

Mar 19, 2025

GENERAL

The table of contents below and in the sidebar should let you easily access the documentation for your topic of interest. You can also use the search function in the top left corner.

The main documentation for the site is organized into sections for each individual CIS Control.

The “About the CIS Controls” section provides background information about the CIS Controls.

The “About the CIS Controls Assessment Specification” provides information about the Controls Assessment Specification including its purpose, methodology, and structure.

The “Terms of Use” section provides the terms of use policy.

The “Contributing” section provides details on how you can contribute to the Controls Assessment Specification.

CHAPTER

ONE

ABOUT THE CIS CRITICAL SECURITY CONTROLS® (CIS CONTROLS®)

The CIS Controls® are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

We are at a fascinating point in the evolution of what we now call cyber defense. Massive data losses, theft of intellectual property, credit card breaches, identity theft, threats to our privacy, denial of service – these have become a way of life for all of us in cyberspace.

As defenders we have access to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogs of security controls, and countless security checklists, benchmarks, and recommendations. To help us understand the threat, we have seen the emergence of threat information feeds, reports, tools, alert services, standards, and threat sharing frameworks. To top it all off, we are surrounded by security requirements, risk management frameworks, compliance regimes, regulatory mandates, and so forth. There is no shortage of information available to security practitioners on what they should do to secure their infrastructure.

But all of this technology, information, and oversight has become a veritable "Fog of More" – competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings us great benefits, but it also means that our data and applications are now distributed across multiple locations, many of which are not within our organization's infrastructure. In this complex, interconnected world, no enterprise can think of its security as a standalone problem.

So how can we as a community – the community-at-large, as well as within industries, sectors, partnerships, and coalitions – band together to establish priority of action, support each other, and keep our knowledge and technology current in the face of a rapidly evolving problem and an apparently infinite number of possible solutions? What are the most critical areas we need to address and how should an enterprise take the first step to mature their risk management program? Rather than chase every new exceptional threat and neglect the fundamentals, how can we get on track with a roadmap of fundamentals, and guidance to measure and improve? Which defensive steps have the greatest value?

These are the kinds of issues that led to and now drive the CIS Controls. They started as a grassroots activity to cut through the "Fog of More" and focus on the most fundamental and valuable actions that every enterprise should take. And **value** here is determined by knowledge and data – the ability to prevent, alert, and respond to the attacks that are plaguing enterprises today.

Led by CIS®, the CIS Controls have been matured by an international community of individuals and institutions that:

- Share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action;
- Document stories of adoption and share tools to solve problems;
- Track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions;

- Map the CIS Controls to regulatory and compliance frameworks and bring collective priority and focus to them;
- Share tools, working aids, and translations; and
- Identify common problems (like initial assessment and implementation roadmaps) and solve them as a community.

These activities ensure that the CIS Controls are not just another list of good things to do, but a prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements.

1.1 Why the CIS Controls Work: Methodology and Contributors

The CIS Controls are informed by actual attacks and effective defenses and reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals); with every role (threat responders and analysts, technologists, vulnerability-finders, tool makers, solution providers, defenders, users, policy-makers, auditors, etc.); and within many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT) who have banded together to create, adopt, and support the Controls. Top experts from organizations pooled their extensive first-hand knowledge from defending against actual cyber-attacks to evolve the consensus list of Controls, representing the best defensive techniques to prevent or track them. This ensures that the CIS Controls are the most effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks.

The CIS Controls are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions. The defenses identified through these Controls deal with reducing the initial attack surface by hardening device configurations, identifying compromised machines to address long-term threats inside an organization's network, disrupting attackers' command-and-control of implanted malicious code, and establishing an adaptive, continuous defense, and response capability that can be maintained and improved.

The five critical tenets of an effective cyber defense system as reflected in the CIS Controls are:

Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.

Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment. The CIS Implementation Groups discussed below are a great place for organizations to start identifying relevant Sub-Controls.

Measurements and Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.

Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

1.2 Getting Started

The CIS Controls are a relatively small number of prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. They also change the discussion from "What should my enterprise do?" to "What should we ALL be doing?" to improve security across a broad scale.

But this is not a one-size-fits-all solution, in either content or priority. You must still understand what is critical to your business, data, systems, networks, and infrastructures, and you must consider the adversarial actions that could

impact your ability to be successful in the business or operation. Even a relatively small number of Controls cannot be executed all at once, so you will need to develop a plan for assessment, implementation, and process management.

CHAPTER

TWO

ABOUT THE CIS CONTROLS ASSESSMENT SPECIFICATION

2.1 Purpose

The CIS Controls provide essential best practices that organizations can implement to improve their cybersecurity posture. In addition to implementing the CIS Controls, it is also important that organizations measure their implementations to ensure that Sub-Controls are in place and working properly. The purpose of the CIS Controls Assessent Specification (CAS) is to provide a common understanding of what should be measured in order to verify that CIS Sub-Controls are properly implemented. The hope is that those developing related tools will then build these measures into their tools so that the CIS Controls are measured in a uniform way.

Note that the focus of CAS is on "what to measure" rather than "how to measure". With the goal of being platform agnostic, a conscious effort was made to avoid addressing the "how to measure" in writing CAS, leaving those platform specific details to specific implementations of these measures. Tool developers will determine the "hows" that are appropriate for their tools and use cases.

2.2 Methodology

The CIS Controls provide cybersecurity best practices designed to help organizations of all types secure a wide variety of systems. Because the CIS Controls cover so many security topics, and apply to such a wide variety of hardware and software that can be used in many different ways, measuring the CIS Controls is a complex challenge. Different approaches to measuring the Controls can result in multiple ways of measuring the same Sub-Control.

One useful distinction is measuring whether a Sub-Control has been implemented vs. measuring how well the Sub-Control was implemented. Measuring whether a Sub-Control is implemented need not be a binary yes or no; for instance, it could be a numerical score indicating how many endpoints in an environment have implemented that Sub-Control. Measuring how well a Sub-Control is implemented looks more to the intended effect of the Sub-Control examining whether the desired security gains are being realized. Measuring whether a Sub-Control is implemented often involves checking whether something is configured in a certain way, while measuring how well often requires more involved checks including more active testing.

While both of these measurement approaches are useful and have their place, for this first version of CAS, we have focused on measuring whether a Sub-Control has been implemented (which we have termed Level 1 checks). It is our hope that future versions of CAS will expand to include measurements of how well a Sub-Control is implemented as well (which we have termed Level 2 checks).

Specific configuration details are not specified in CAS, as these would vary from platform to platform, and would encroach on "how to measure". When there are multiple ways to implement a Sub-Control, CAS attempts to be generic enough to cover these varying methods in its measures. Where assumptions are made, CAS attempts to explicitly state them.

2.3 Structure of a Sub-Control Measurement

This section describes the standard structure of a Sub-Control Measurement in CAS.

2.3.1 Basic CIS Sub-Control Information

This section includes the Sub-Control number, title, description, asset type, security function, and implementation group. This information matches the information in the CIS Controls v7.1 document.

2.3.2 Assumptions

Assumptions are provided inside of the section to which they are most applicable, or not in any specific section if they are general to the entire Sub-Control measurement.

2.3.3 Sub-Control Dependencies

This is an optional section that may not appear for all Sub-Control measurements. When present, this section lists any other Sub-Controls that are prerequisites for measuring this Sub-Control. Completion of the Sub-Controls specified in this section will typically generate data necessary as an Input for measuring this Sub-Control.

2.3.4 Inputs

This section includes the data that is expected as an input in order to measure this Sub-Control.

2.3.5 Operations

This section specifies actions to be performed on the inputs in order to generate the measures. The operations provide a linkage between the inputs and measures.

2.3.6 Measures

This section describes the information that should be measured, generally as a result of performing operations on the inputs. Measures are combined to form metrics.

2.3.7 Metrics

This section describes standard metrics that can be calculated from the measures, providing a description of the metricalong with the formula for calculating the metric. In general, CAS attempts to frame metrics in a positive light - i.e., the ratio of items that are compliant with the Sub-Control (as opposed to the ratio of items that are not compliant). The provided metrics are not meant to be an exhausive list of metrics, rather it is just meant to list some examples of common metrics that are likely to be useful. The hope is that if appropriate measures have been defined, other metrics can be built from those measures to suit different use cases.

2.3.8 Procedure Review

This is an optional section that may not appear for all Sub-Control measurements. When present, this section describes a manual review of a procedure that helps fulfill the Sub-Control.

2.4 Versioning

CAS follows a semantic versioning approach based on semver.org and having the following format: *major.minor.point*.

- Major: Significant and material changes to * The organization of the document * Structure of sub-control measures * Inputs, measures, metrics on the whole

- Minor: Material changes to parts of sub-control measures or metrics
- Point: Immaterial changes, such as prose typos, document look and feel

CHAPTER

THREE

TERMS OF USE

CHAPTER

FOUR

CONTRIBUTING TO THE CIS CONTROLS ASSESSMENT SPECIFICATION

CIS welcomes contributions to the CIS Controls Assessment Specification. There are no special requirements to contribute beyond recognizing our Terms of Use. If you have a suggestion for improvement to any one of the defined measures, to the content as a whole, or have other suggestions for enhancement, email us at controlsinfo@cisecurity.org.

CHAPTER

FIVE

CIS CONTROL 1: INVENTORY AND CONTROL OF HARDWARE ASSETS

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Why is this CIS Control Critical?

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise's network such as laptops or Bring-Your-Own-Device (BYOD) which might be out of synchronization with security updates or might already be compromised. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims. Additional systems that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. But attackers have shown the ability, patience, and willingness to "inventory and control" our assets at very large scale in order to support their opportunities.

Managed control of all devices also plays a critical role in planning and executing system backup, incident response, and recovery.

5.1 1.1: Utilize an Active Discovery Tool

Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.

Asset Type	Security Function	Implementation Groups
Devices	Identify	2, 3

5.1.1 Dependencies

- Sub-control 5.1: Establish Secure Configurations

5.1.2 Inputs

1. The hardware asset inventory
2. The asset discovery tool(s) used by the organization
3. The most recent scan results from the asset discovery tool(s)

4. Configuration information for the asset discovery tool(s)
5. Approved configuration(s) to all tools to interface with the hardware asset inventory

Assumptions

1. The asset discovery tools on the provided list are active asset discovery tools, as opposed to passive asset discovery tools (verification of this is not performed during the following operations).
2. The asset discovery tools are used regularly (this is not verified during the following operations).

5.1.3 Operations

1. Create a list of the assets discovered by the tools by enumerating the assets from the scans provided in I3, and creating a union of those enumerations (this list of discovered assets will be M1).
2. Use M1 and I1 to generate the list of assets that are on the Hardware Asset Inventory but were not discovered by any of the tools (this list will be M2).
3. Using the information in I4, check the configuration information of each tool against the appropriate approved configuration from I5 to verify that the tool is capable of interfacing with the hardware asset inventory to make automatic updates. Create a list of those tools that are compliant (M3), and a list of those that are not (M4).

5.1.4 Measures

- M1 = List of discovered assets
- M2 = List of undiscovered assets
- M3 = List of compliant tools
- M4 = List of non-compliant tools
- M5 = Count of discovered assets (count of M1)
- M6 = Count of compliant tools (count of M3)
- M7 = Total count of hardware assets (count of Input 1)
- M8 = Total count of asset discovery tools (count of Input 2)

5.1.5 Metrics

- If M8 is 0, then this Sub-Control receives a failing score and the other metrics don't apply.

Asset Discovery Coverage

Metric	Asset Discovery Coverage
Calculation	`M5 / M7`

Tool Compliance Ratio

Metric	Tool Compliance Ratio
Calculation	`M6 / M8`

5.2 1.2: Use a Passive Asset Discovery Tool

Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.

Asset Type	Security Function	Implementation Groups
Devices	Identify	3

5.2.1 Dependencies

- Sub-control 12.1: Maintain an Inventory of Network Boundaries

5.2.2 Inputs

1. The list of the organization's networks
2. The list of passive asset discovery tools in use by the organization. For each, include the location of the tool's configuration information and which networks it covers.
3. Approved configuration(s) for each passive asset discovery tool. Configurations should include the settings necessary for the tool to be able to update the organization's hardware asset inventory.

5.2.3 Operations

1. **For each passive asset discovery tool provided in Input 2, check the tool's configuration against the appropriate approved configuration from Input 3.**
    1. Create a list of those tools that are properly configured (M1)
    2. Create a list of those tools that are improperly configured (M2) noting the deviations from proper configuration
2. **For each of the organization's networks provided in Input 1, check Input 2 and M1 to ensure that at least one properly configured passive asset discovery tool covers that network.**
    1. Create a list of the organization's networks that have coverage from at least one properly configured passive asset discovery tool (M3)
    2. Create a list of the organization's networks that do not have coverage from any properly configured passive asset discovery tools (M4)

5.2.4 Measures

- M1 = List of properly configured passive asset discovery tools (compliant tool list)
- M2 = List of improperly configured passive asset discovery tools (non-compliant tool list)
- M3 = List of organization's networks with coverage from at least one properly configured passive asset discovery tool (compliant network list)

- M4 = List of organization's networks that do not have coverage from any properly configured passive asset discovery tool (non-compliant network list)
- M5 = Count of networks with coverage from at least one properly configured passive asset discovery tool (count of M3)
- M6 = Total count of the organization's networks (count of Input 1)

5.2.5 Metrics

Coverage

Metric	
	The ratio of the organization's networks with coverage from at least one properly configured passive asset discovery tool to the total number of networks
Calculation	`M5 / M6`

5.3 1.3: Use DHCP Logging to Update Asset Inventory

Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.

Asset Type	Security Function	Implementation Groups
Devices	Identify	2, 3

5.3.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory

5.3.2 Inputs

1. The list of DHCP servers
2. The list of CMDB servers (i.e. asset inventory systems)

5.3.3 Operations

1. For each DHCP server, check whether DHCP logging is enabled
2. For each CMDB server, check whether DHCP logs are used to update IP addresses

Assumptions

- CMDB servers are configured to pull from DHCP logs

5.3.4 Measures

- M1 = Count of DHCP servers (using Input 1)
- M2 = List of DHCP servers with logging enabled
- M3 = Count of M2
- M4 = Count of CMDB servers (using Input 2)
- M5 = List of CMDB servers configured to use DHCP logs to update IP addresses
- M6 = Count of M5
- M7 = List of devices in the DHCP server logs that are not included in the CMDB servers
- M8 = Count of M7
- M9 = List of devices in the DHCP server logs that are included in the CMDB servers
- M10 = Count of M9

5.3.5 Metrics

- M5 > 0 indicates a non up-to-date asset inventory

DHCP Logging Quality

Metric	Ratio of appropriately configured DHCP logging enabled to known DHCP servers
Calculation	`M3 / M1`

CMDB Configuration Quality

Metric	Ratio of appropriately configured CMDB servers using DHCP logging to update IP addresses
Calculation	`M6 / M4`

5.4 1.4: Maintain Detailed Asset Inventory

Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.

Asset Type	Security Function	Implementation Groups
Devices	Identify	1, 2, 3

5.4.1 Dependencies

- None

5.4.2 Inputs

1. Endpoint Inventory: The organization's current inventory list (the "to be checked" list).
2. A "ground truth" inventory list to compare with input 1. This list would be enhanced by manual verification, but a tool-generated or aggregated list could be substituted here. This should be an aggregation of the devices detected over a period of time, preferably not from a single scan.
3. A write-up of the procedure for adding or removing assets to or from the inventory - only for manual review.

Assumptions

- Devices belonging to the organization, but not connected to the organization's network, require manual discovery in order to be included in the "ground truth" inventory.

5.4.3 Operations

- If Input 1 is not provided, this sub-control is measured at a 0 (complete fail).
- If Input 2 is not provided, no true accuracy measurement can be made for this sub-control.
- Calculate the intersection of Input 1 and Input 2, noting items in the inventory and not in "ground truth" and items in "ground truth" not in the inventory.

5.4.4 Measures

- M1 = List of items in the intersection of Input 1 and Input 2
- M2 = Count of items in M1
- M3 = List of items in Input 2
- M4 = Count of items in M3
- M5 = List of items in the inventory and not in "ground truth"
- M6 = Count of items in M5
- M7 = List of items not in the inventory and in "ground truth"
- M8 = Count of items in M7

5.4.5 Metrics

Accuracy Score

Metric	
	What percentage of the "ground truth" inventory is accounted for in the organization's current asset inventory?
Calculation	`M2 / M4`

Procedure Review

Second, manual review/rating of the inventory procedures, to include adding and removing assets, and the time allowable or expected, after acquisition or disposal of assets.

5.5 1.5: Maintain Asset Inventory Information

Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.

Asset Type	Security Function	Implementation Groups
Devices	Identify	2, 3

5.5.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory

5.5.2 Inputs

1. Detailed endpoint inventory

5.5.3 Operations

1. **For each endpoint, identify detailed information, such as:**
    - Network Address
    - Hardware Address (applies to virtual endpoints)
    - Machine name
    - Data asset owner
    - Assigned department
2. Identify endpoints with all detailed information identified
3. For each endpoint, identify network connection approval

5.5.4 Measures

- M1 = List of endpoints in inventory
- M2 = Count of M1
- M3 = List of endpoints with network connection approval
- M4 = Count of M3
- M5 = List of endpoints with all detailed information
- M6 = Count of M5

5.5.5 Metrics

Endpoint Inventory Quality

Metric	
	The ratio of endpoints with all detailed information to the total number of inventoried endpoints
Calculation	`M6 / M2`

Endpoint Inventory Authorization Quality

Metric	
	The ratio of endpoints with approval to connect to the network
Calculation	`M4 / M2`

5.6 1.6: Address Unauthorized Assets

Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.

Asset Type	Security Function	Implementation Groups
Devices	Respond	1, 2, 3

5.6.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory

5.6.2 Inputs

1. A list of discovered assets not currently present in the asset inventory ("unauthorized" assets).
2. Endpoint Inventory: Current hardware inventory (sub-control 1.4)
3. An organizationally defined time frame for "timely" (recommend 24 hours or better)
4. (Optional) Measurement results would be more useful if the disposition of the items (removed, added to inventory, quarantined, etc.) was provided to be verified, but this is not absolutely necessary.

5.6.3 Operations

If the optional disposition list is provided, the checks would be tailored to those dispositions. For the following, assume no disposition list is available:

1. At the time frame specified by Input 3, for each unauthorized asset (Input 1), check to see if the asset is present in the updated asset inventory (Input 2), keeping track of unauthorized items
2. For those Input 1 items that are not in Input 2, scan the network to determine if the item is still reachable on the network.

Assumptions

If the item is not reachable, it may be reasonable to assume it has been removed from the network and therefore dealt with.

5.6.4 Measures

- M1 = List of items not in the inventory
- M2 = Count of items in M1
- M3 = List of items not reachable
- M4 = Count of items in M3
- M5 = List of items not in the inventory or that are unreachable
- M6 = Count of items in M5
- M7 = List of items in the inventory
- M8 = Count of items in M7
- M1 = The number of items from Input 1 **NOT** passing either Operation 1 or Operation 2
- M2 = The total number of items in Input 1

5.6.5 Metrics

Unauthorized Asset Remediation

Metric	
	The ratio of unaccounted for, unauthorized assets, to the total assets in the asset inventory
Calculation	
	If the value of M6 is 0, there are no unauthorized assets that remain unaccounted for. In this case, the value of the metric is 1. Otherwise, the value is `(M8 - M6) / M8`

5.7 1.7: Deploy Port Level Access Control

Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

5.7.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

Assumptions

1. Use of an 802.1x network design to control network access
2. The 802.1x system can query the endpoint inventory system
3. The CMDB is a separate entity from the authentication server.

5.7.2 Inputs

1. List of 802.1x authenticators
2. List of 802.1x authentication servers (i.e. RADIUS/Diameter servers)
3. List of CMDB servers

5.7.3 Operations

1. For each 802.1x authenticator, ensure proper configuration
2. For each 802.1x authentication server, ensure proper configuration, including connection to at least one CMDB server

5.7.4 Measures

- M1 = Boolean: 802.1x authenticators are in use
- M2 = Boolean: 802.1x authentication servers are in use
- M3 = List of inappropriately configured 802.1x authenticators
- M4 = Count of M3
- M5 = List of appropriately configured 802.1x authenticators
- M6 = Count of M5
- M7 = List of inappropriately configured 802.1x authentication servers
- M8 = Count of M7
- M9 = List of appropriately configured 802.1x authentication servers
- M10 = Count of M9
- M11 = Count of 802.1x authentication servers (from Input 2)
- M12 = Count of 802.1x authenticators (from Input 1)

5.7.5 Metrics

802.1x Deployment

Metric	Is 802.1x deployed?
Calculation	`M1 AND M2`

Authenticator Coverage

Metric	
	Ratio of improperly configured 802.1x authenticators to total number of 802.1x authenticators
Calculation	`M4 / M12`

Authentication Server Coverage

Metric	
	Ratio of improperly configured 802.1x authentication servers to total number of 802.1x authentication servers
Calculation	`M8 / M11`

5.8 1.8: Utilize Client Certificates to Authenticate Hardware Assets

Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

5.8.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

5.8.2 Inputs

1. The list of endpoints

5.8.3 Operations

1. Enumerate hardware devices (physical and virtual) from the endpoint inventory
2. For each hardware device, examine device client authentication certificate configuration noting appropriate and inappropriate configurations

5.8.4 Measures

- M1 = List of hardware devices (operation 1)
- M2 = List of appropriately configured hardware devices (operation 2)
- M3 = List of inappropriately configured hardware devices (operation 2)
- M4 = Count of hardware devices (count of M1)

- M5 = Count of appropriately configured hardware devices (count of M2)
- M6 = Count of inappropriately configured hardware devices (count of M3)

5.8.5 Metrics

Coverage

Metric	
	The ratio of appropriately configured hardware devices to the number of hardware devices
Calculation	`M5 / M4`

CHAPTER

SIX

CIS CONTROL 2: INVENTORY AND CONTROL OF SOFTWARE ASSETS

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.

Why is this CIS Control Critical?

Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

Poorly controlled machines are more likely to be either running software that is unneeded for business purposes (introducing potential security flaws), or running malware introduced by an attacker after a system is compromised. Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.

Managed control of all software also plays a critical role in planning and executing system backup, incident response, and recovery.

6.1 2.1: Maintain Inventory of Authorized Software

Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.

Asset Type	Security Function	Implementation Groups
Applications	Identify	1, 2, 3

6.1.1 Dependencies

- None

6.1.2 Inputs

1. Authorized Software List: The authorized software list (containing a timestamp indicating both last updated and last verified values).
2. An organizationally defined acceptable timeframe for "up-to-date" (recommend at least monthly)

6.1.3 Operations

1. Test for the presence of the list; A TRUE/FALSE value (M1)
2. (Optional) If specific attributes of the software are deemed required, test for those (vendor, product name, version, business case, etc.)
3. Compare the timestamp of Input 1 against the current date to determine if the most recent update/verification is within the timeframe specified by Input 2; A TRUE/FALSE value (M2).

6.1.4 Measures

- M1 = TRUE if authorized software list is present and in the proper format, FALSE otherwise
- M2 = TRUE if the most recent update/verification is within the "up-to-date" threshold; FALSE otherwise

6.1.5 Metrics

Update Quality

Metric	Is the authorized software list present and up-to-date?
Calculation	`M1 AND M2`

6.2 2.2: Ensure Software is Supported by Vendor

Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

Asset Type	Security Function	Implementation Groups
Applications	Identify	1, 2, 3

6.2.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

6.2.2 Inputs

1. Authorized Software List: The authorized software list with a notation of "supported" or "unsupported" for each entry (sub-control 2.1)
2. Access to an authoritative source of information indicating supported/unsupported details by product.

6.2.3 Operations

1. For each entry in Input 1, perform a lookup in Input 2 to verify.
2. For each entry in Input 1 labeled "supported", perform a lookup in Input 2. From these lookups, note the list of authorized software labeled "supported" but are actually not supported based on the authoritative source lookup.
3. For each entry in Input 1 labeled "unsupported", perform a lookup in Input 2. From these lookups, note the list of authorized software labeled "unsupported" but are actually supported based on the authoritative source lookup.

6.2.4 Measures

- M1 = List of items in the authorized software list that are unsupported (combination of Operation 1 and those initially marked as unsupported in Input 1)
- M2 = Count of M1
- M3 = List of authorized software
- M4 = Count of M3
- M5 = List of items in the authorized software list that are mislabeled as supported
- M6 = Count of M5
- M7 = List of items in the authorized software list that are mislabeled as unsupported
- M8 = Count of M7
- M1 = # of items in Input 1 that are unsupported (combination of Operation 1 results and those initially marked as unsupported in Input 1)
- M2 = Total # of authorized software (from Input 1)
- M3 = The number of items from Input 1 labeled "supported" but are actually not supported (from Operation 2)
- M4 = The number of items from Input 1 labeled "unsupported" but are actually supported (from Operation 3)

6.2.5 Metrics

Percentage of Unsupported Software in Use

Metric	What percentage of authorized software in use is unsupported?
Calculation	`(M4 - M2) / M4`

Rate of False Positives

Metric	What percentage of software listed as supported is actually not supported?
Calculation	`(M4 - M5) / M4`

Rate of False Negatives

Metric	
	What percentage of software listed as unsupported is actually supported?
Calculation	`(M4 - M8) / M4`

6.3 2.3: Utilize Software Inventory Tools

Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.

Asset Type	Security Function	Implementation Groups
Applications	Identify	2, 3

6.3.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory

Assumptions

- The documentation referenced by this sub-control intends to mean an enumeration of software load on endpoints capable of running installed software
- A business system is any endpoint owned or operated by the enterprise/organization
- The CMDB does not contain and up-to-date software load for each endpoint in its inventory

6.3.2 Inputs

1. Endpoint inventory
2. List of software inventory tools

6.3.3 Operations

1. For each software inventory, count covered endpoints and calculate the aggregate (becomes M2)
2. Count number of endpoints loadable with software (becomes M3)

6.3.4 Measures

- M1 = Count of software inventory tools (from Input 2)
- M2 = List of endpoints covered by software inventory tools
- M3 = Count of M2
- M4 = List of endpoints not covered by software inventory tools
- M5 = Count of M4
- M6 = List of endpoints loadable with software
- M7 = Count of M6

- M8 = List of endpoints not loadable with software
- M9 = Count of M8

6.3.5 Metrics

Software Inventory Tool Usage

Metric	
	Are software inventory tools used?
Calculation	`(M1 == 0) OR (M1 == 1)`

Inventory Tool Coverage

Metric	
	The ratio of endpoints covered by automated software inventory tools to the total number of applicable endpoints
Calculation	`M3 / M7`

6.4 2.4: Track Software Inventory Information

The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.

Asset Type	Security Function	Implementation Groups
Applications	Identify	2, 3

6.4.1 Dependencies

- Sub-control 2.3: Utilize Software Inventory Tools

6.4.2 Inputs

1. Detailed software inventory

6.4.3 Operations

1. **For each entry in the software inventory, including operating systems, identify detailed information such as:**
    - Software name (market name)
    - Software version (market version)
    - Software publisher
    - Installation date (timestamp)
2. For each entry in the software inventory, including operating systems, identify authorization state

3. Identify software with all detailed information identified

6.4.4 Measures

- M1 = Count of entries in software inventory (from Input 1)
- M2 = List of entries authorized for installation
- M3 = Count of M2
- M4 = List of entries not authorized for installation
- M5 = Count of M4
- M6 = List of entries with all detailed information
- M7 = Count of M6
- M8 = List of entries without all detailed information
- M9 = Count of M8

6.4.5 Metrics

Inventory Quality

Metric	
	The ratio of entries with all detailed information to the total number of entries
Calculation	`M7 / M1`

Inventory Authorization Quality

Metric	
	The ratio of entries authorized to be installed to the total number of entries
Calculation	`M3 / M1`

6.5 2.5: Integrate Software and Hardware Asset Inventories

The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

Asset Type	Security Function	Implementation Groups
Applications	Identify	3

6.5.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

6.5.2 Inputs

1. The list of endpoints

6.5.3 Operations

1. Enumerate software inventory systems from the endpoint inventory
2. Enumerate hardware inventory systems from the endpoint inventory
3. For each software inventory system, examine its configuration to ensure that it is tied to at least one hardware inventory system, noting appropriately and inappropriately configured software inventory systems

6.5.4 Measures

- M1 = List of software inventory systems
- M2 = List of hardware inventory systems
- M3 = List of appropriately configured software inventory systems
- M4 = List of inappropriately configured software inventory systems
- M5 = Count of software inventory systems (count of M1)
- M6 = Count of hardware inventory systems (count of M2)
- M7 = Count of appropriately configured software inventory systems (count of M3)
- M8 = Count of inappropriately configured software inventory systems (count of M4)

6.5.5 Metrics

Coverage

Metric	The ratio of appropriately configured software inventory systems to the number of software inventory systems
Calculation	`M7 / M5`

6.6 2.6: Address Unapproved Software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.

Asset Type	Security Function	Implementation Groups
Applications	Respond	1, 2, 3

6.6.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 2.1: Maintain Inventory of Authorzied Software

6.6.2 Inputs

1. Authorized Software List$_i$: The previous list of authorized software
2. An organizationally defined allowable time frame for resolution of discovered unauthorized software (recommend at least monthly)
3. Software-capable Endpoints: The list of endpoints to be checked (derived from hardware inventory; see sub-control 1.4)
4. Authorized Software List$_{i+1}$: The updated authorized software list, following the time frame defined by Input 2
5. The "scanning threshold"; the time period between scan 1 and scan 2

Assumptions

- For Input 4, that the authorized software list may have been updated after a manual review of unauthorized software based on user requests, etc.
- For Input 5, that the scanning threshold time period is greater than Input 2 (resolution time frame).

6.6.3 Operations

1. For each endpoint in Input 3, scan the installed software present on that endpoint.
2. Compare the installed software list for each endpoint (M1) to the authorized software list (Input 1) to generate the unauthorized software list for that endpoint (M2).
3. Wait the "scanning threshold" time period (Input 5) and re-scan the endpoints specified by Input 3.
4. For each software on the M2 list, determine if that software is still present in the Operation 3 scan.
5. For those that are still present, check Input 4 to determine if the software is now present on the updated authorized software list (Input 4). Software that remains installed on the machine, but does not appear on the updated authorized software list is added to the unaddressed software list for that endpoint (M3).

6.6.4 Measures

- M1 = The list of software installed on a given endpoint, per Operation 1.
- M2 = The list of unauthorized software installed on a given endpoint, identified by comparing M1 to Input 1.
- M3 = The list of unaddressed software installed on a given endpoint, identified by follow-up scan.
- M4 = The number of items in M2 (# of unauthorized software per endpoint).
- M5 = The number of items in M3 (# of unaddressed software per endpoint).

6.6.5 Metrics

Unauthorized Software (Per Endpoint)

Metric	
	Ensure unauthorized software installations are addressed
Calculation	`(M4 - M5) / M4`

Unauthorized Software (Organizational)

The organizational metric is calculated by averaging the results of the "per endpoint" metric above.

6.7 2.7: Utilize Application Whitelisting

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.

Asset Type	Security Function	Implementation Groups
Applications	Protect	3

6.7.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

6.7.2 Inputs

1. The list of endpoints
2. The list of authorized software

6.7.3 Operations

1. Enumerate endpoints capable of leveraging whitelisting technology (e.g. some network and other devices may not enable third-party software installation or otherwise have constrained environments precluding the use of whitelisting software)
2. For each eligible endpoint (operation 1), examine the software inventory for whitelisting applications related to that endpoint, noting endpoints with and without whitelisting capabilities
3. For each endpoint with whitelisting capabilities, examine the whitelisting software's configuration to ensure only authorized software is considered executable and that attempts to execute unauthorized software is blocked, noting appropriately and inappropriately configured software

6.7.4 Measures

- M1 = List of endpoints capable of leveraging whitelisting technology
- M2 = List of endpoints with whitelisting capabilities installed
- M3 = List of endpoints without whitelisting capabilities installed
- M4 = List of endpoints with appropriately configured whitelisting capabilities
- M5 = List of endpoints with inappropriately configured whitelisting capabilities
- M6 = Count of endpoints capable of leveraging whitelisting technology (count of M1)
- M7 = Count of endpoints with whitelisting capabilities installed (count of M2)
- M8 = The number of endpoints without whitelisting capabilities installed (count of M3)
- M9 = Count of endpoints with appropriately configured whitelisting capabilities (count of M4)
- M10 = Count of endpoints with inappropriately configured whitelisting capabilities (count of M5)

6.7.5 Metrics

Whitelisting Installation Coverage

Metric	The ratio of endpoints with whitelisting capabilities installed to the number of whitelisting-eligible endpoints
Calculation	`M7 / M6`

Whitelisting Configuration Coverage

Metric	The ratio of endpoints with appropriately configured whitelisting capabilities to the number of endpoints with whitelisting capabilities
Calculation	`M9 / M7`

6.8 2.8: Implement Application Whitelisting of Libraries

The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.

Asset Type	Security Function	Implementation Groups
Applications	Protect	3

6.8.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.7: Utilize Application Whitelisting

6.8.2 Inputs

1. The list of authorized software
2. The list of authorized software libraries

6.8.3 Operations

1. Enumerate all instances of whitelisting software from the software inventory
2. For each instance of whitelisting software, examine its configuration to ensure that it is configured to allow process loading of authorized libraries found in the authorized software library list, noting appropriately and inappropriately configured whitelisting software

6.8.4 Measures

- M1 = List of all instances of whitelisting software found in the software inventory
- M2 = List of appropriately configured whitelisting software instances
- M3 = List of inappropriately configured whitelisting software instances
- M4 = Count of all instances of whitelisting software found in the software inventory (count of M1)
- M5 = Count of appropriately configured whitelisting software instances (count of M2)
- M6 = Count of inappropriately configured whitelisting software instances (count of M3)

6.8.5 Metrics

Coverage

Metric	
	The ratio of appropriately configured whitelisting software instances to the total number of whitelisting software instances in the enterprise
Calculation	`M5 / M4`

6.9 2.9: Implement Application Whitelisting of Scripts

The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1,*.py, macros, etc.) are allowed to run on a system.

Asset Type	Security Function	Implementation Groups
Applications	Protect	3

6.9.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.7: Utilize Application Whitelisting

6.9.2 Inputs

1. The list of authorized software
2. The list of authorized scripts

6.9.3 Operations

1. Enumerate all instances of whitelisting software from the software inventory
2. For each instance of whitelisting software, examine its configuration to ensure that it is configured to allow execution of authorized and signed scripts, noting appropriately and inappropriately configured whitelisting software

6.9.4 Measures

- M1 = List of all instances of whitelisting software found in the software inventory
- M2 = List of appropriately configured whitelisting software instances
- M3 = List of inappropriately configured whitelisting software instances
- M4 = Count of all instances of whitelisting software found in the software inventory (count of M1)
- M5 = Count of appropriately configured whitelisting software instances (count of M2)
- M6 = Count of inappropriately configured whitelisting software instances (count of M3)

6.9.5 Metrics

Coverage

Metric	
	The ratio of appropriately configured whitelisting software instances to the total number of whitelisting software instances in the enterprise
Calculation	`M5 / M4`

6.10 2.10: Physically or Logically Segregate High Risk Applications

Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.

Asset Type	Security Function	Implementation Groups
Applications	Protect	3

6.10.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

6.10.2 Inputs

1. List of approved high-risk applications (subset of Approved Software List). For each, include the mechanisms used to provide separation.
2. Approved configuration(s) for each separation mechanism listed in Input 1

6.10.3 Operations

1. **For each application in Input 1, compare the configurations of the associated separation mechanisms to the appropriate approved configuration(s) from Input 2.**
    1. Create a list of applications that are adequately separated noting which configuration(s) were checked (M1)
    2. Create a list of applications that are not adequately separated noting which configurations were checked and any deviations

6.10.4 Measures

- M1 = List of high-risk applications that are properly segregated (compliant list)
- M2 = List of high-risk applications that are not properly segregated (non-compliant list)
- M3 = Count of high-risk applications that are properly segregated (count of M1)
- M4 = The total number of approved high-risk applications (count of Input 1)

6.10.5 Metrics

Metric	
	The ratio of properly separated high-risk applications to the total number of high-risk applications
Calculation	`M3 / M4`

CHAPTER

SEVEN

CIS CONTROL 3: CONTINUOUS VULNERABILITY MANAGEMENT

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Why is this CIS Control Critical?

Cyber defenders must operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention, and resources.

Attackers have access to the same information and can take advantage of gaps between the appearance of new knowledge and remediation. For example, when researchers report new vulnerabilities, a race starts among all parties, including: attackers (to "weaponize," deploy an attack, exploit), vendors (to develop, deploy patches or signatures and updates), and defenders (to assess risk, regression-test patches, install).

Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, and sometimes uncertain side effects.

7.1 3.1: Run Automated Vulnerability Scanning Tools

Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

Asset Type	Security Function	Implementation Groups
Applications	Detect	2, 3

7.1.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 2.3: Utilize Software Inventory Tools

7.1.2 Inputs

1. List of endpoints
2. List of vulnerability scanning tools
3. List of SCAP-validated vulnerability scanning tools
4. Most recent scan results for each vulnerability scanning tool

7.1.3 Operations

1. For each vulnerability scanning tool, enumerate the set of covered endpoints
2. Union the set of covered endpoints
3. For each vulnerability scanning tool, inspect tool configuration for at least weekly scans
4. For each vulnerability scanning tool, inspect tool results/logs for at least weekly scans

7.1.4 Measures

- M1 = List of endpoints covered by vulnerability scanning tools
- M2 = Count of M1
- M3 = Count of endpoints (from Input 1)
- M4 = List of vulnerability scanning tools configured to scan at least weekly
- M5 = Count of M4
- M6 = List of vulnerability scanning tools not configured to scan at least weekly
- M7 = Count of M6
- M8 = List of vulnerability scanning results having occurred in at least the past week
- M9 = Count of M8
- M10 = List of vulnerability scanning results having not occurred in at least the past week
- M11 = Count of M10
- M12 = Count of SCAP-validated vulnerability scanning tools (from Input 2)
- M13 = Count of vulnerability scanning tools (from Input 3)

7.1.5 Metrics

Vulnerability Scanning Coverage

Metric	The ratio of endpoints covered by at least one vulnerability scanning tool to the total number of endpoints
Calculation	`M2 / M3`

Vulnerability Scanner Configuration Quality

Metric	The ratio of correctly configured vulnerability scanners to the total number of vulnerability scanners
Calculation	`M5 / M13`

Vulnerability Scan Timeliness

Metric	
	The ratio of scanners having actually scanned in at least the past week to the total number of vulnerability scanners
Calculation	`M9 / M13`

SCAP-Validated Vulnerability Scanner Coverage

Metric	
	The ratio of SCAP-validated scanners to the total number of vulnerability scanners
Calculation	`M12 / M13`

7.2 3.2: Perform Authenticated Vulnerability Scanning

Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.

Asset Type	Security Function	Implementation Groups
Applications	Detect	2, 3

7.2.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

7.2.2 Inputs

1. List of deployed vulnerability scanning tools
2. List of authenticated vulnerability scanners
3. Time threshold for last use of vulnerability scanner

7.2.3 Operations

1. For each deployed vulnerability scanner, check whether it is in the list of authenticated vulnerability scanners, noting those that are and those that are not
2. For each deployed vulnerability scanner, verify that it has been used within time threshold
3. **For each authorized vulnerability scanner**
    1. Enumerate endpoints covered
    2. Check configuration for authenticated scanning on each endpoint
4. Aggregate number of endpoints covered (becomes M5)
5. Aggregate correct configuration (becomes M6)

7.2.4 Measures

- M1 = Count of deployed vulnerability scanning tools (from Input 1)
- M2 = List of unauthenticated vulnerability scanning tools
- M3 = Count of M2
- M4 = List of authenticated vulnerability scanning tools
- M5 = Count of M4
- M6 = List of vulnerability scanning tools recently used
- M7 = Count of M6
- M8 = List of vulnerability scanning tools not recently used
- M9 = Count of M8
- M10 = List of endpoints covered by at least one authenticated vulnerability scanner
- M11 = Count of M10
- M12 = List of endpoints scanned in an authenticated manner
- M13 = Count of M12
- M14 = List of endpoints not scanned in an authenticated manner
- M15 = Count of M14

7.2.5 Metrics

Authenticated Vulnerability Scanning Tool Coverage

Metric	Percentage of authenticated vulnerability scanning tools (100% is desired)
Calculation	`(M1 - M5) / M1`

Recently Used Vulnerability Scanning Tools

Metric	Percentage of vulnerability scanning tools recently used
Calculation	`(M1 - M7) / M1`

Coverage

Metric	Authenticated scanning coverage
Calculation	`M13 / M11`

7.3 3.3: Protect Dedicated Assessment Accounts

Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

7.3.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory

7.3.2 Inputs

1. List of vulnerability scanning accounts
2. List of vulnerability scanning machines

7.3.3 Operations

1. For each vulnerability scanning account, ensure account configuration to log in only to one or more of the vulnerability scanning machines

7.3.4 Measures

- M1 = Total number of vulnerability scanning accounts (from Input 1)
- M2 = List of vulnerability scanning accounts configured to log in only to one or more of the vulnerability scanning machines
- M3 = Count of M2
- M4 = List of vulnerability scanning account configured to log in to any machine other than one of the vulnerability scanning machines
- M5 = Count of M4

7.3.5 Metrics

Misconfigured Account Ratio

Metric	Ratio of misconfigured vulnerability scanning accounts to the total number of vulnerability scanning accounts
Calculation	`(M1 - M3) / M1`

7.4 3.4: Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

Asset Type	Security Function	Implementation Groups
Applications	Protect	1, 2, 3

7.4.1 Dependencies

- Sub-control 5.1: Establish Secure Configurations

7.4.2 Inputs

1. The required OS auto-update configuration (this could vary by organization, by product, by security tool, etc.). It could be 1 setting or multiple settings. It would need to be determined if partial settings are creditable, potential weighting of settings, any dependencies, etc. Such logic should all be part of Input 1.
2. The list of required updates (this could be pulled from the vendor's website, or could be an organization's selected subset of updates). *Optional Field*: If time metrics are desired, this list would also need a date when each update on the list was released by the vendor.
3. The list of endpoints to be checked.
4. *Optional*: If time metrics are desired, the allowable time frame for installation of an update after its release (recommend at least 30 days)

7.4.3 Operations

1. For each endpoint in Input 3, compare that endpoint's auto-update configuration to that provided in Input 1 and generate a score based on the logic provided by Input 1 (M1).
2. For each endpoint in Input 3, retrieve a list of installed OS updates (M2) and compare that endpoint's installed updates to the required updates provided by Input 2. The list of matching updates is M3.
3. (Optional) If timing metrics are desired, for each endpoint, also determine the elapsed time between the update release date provided in Input 2 and the install date for each of the corresponding updates on the endpoint; this information could be added as another field attached to each update entry in M3.

7.4.4 Measures

- M1 = Endpoint-specific auto-update configuration score as determined in Operation 1.
- M2 = Endpoint-specific list of installed updates as determined in Operation 2.
- M3 = Endpoint-specific list of required updates that are installed, as determined in Operation 2.
- M4 = The number of required OS updates per Input 2.
- M5 = The number of required OS updates that are installed on the endpoint, per M3.

7.4.5 Metrics

Update Effectiveness (Per Endpoint)

Metric	For a given endpoint, calculate the ratio of installed OS updates to the total number of OS updates required.
Calculation	If M4 = 0, this indicates the endpoint requires no OS updates. Otherwise, this metric is calculated as `M5 / M4`

Update Effectiveness (Organizational)

The organizational metric is calculated by averaging the results of the "per endpoint" metric above.

7.5 3.5: Deploy Automated Software Patch Management Tools

Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

Asset Type	Security Function	Implementation Groups
Applications	Protect	1, 2, 3

7.5.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

7.5.2 Inputs

1. From the authorized software list (ASL; sub-control 2.1), information on the current authorized version.
2. Access to an authoritative source of information indicating version details by product.
3. A list of approved exceptions, noting any reasons that an authorized software package does not match the latest version.

7.5.3 Operations

1. For each software in Input 1, list the software products which do not match the latest version as described by Input 2.
2. For each endpoint, obtain the current software load (the list of installed software).
3. For each endpoint, list the installed software that does not match the current authorized version from Input 1.
4. For each software product listed in Operation 3, list any that exist in the approved exceptions list (Input 3).

7.5.4 Measures

- M1 = List of authorized software products installed on the endpoint which are not at the latest version.
- M2 = Count of M1
- M3 = List of authorized software products installed on the endpoint.
- M4 = Count of M3
- M5 = List of authorized software products installed on the endpoint which are not at the latest version, but have approved exceptions.
- M6 = Count of M5

7.5.5 Metrics

Update Effectiveness (Per Endpoint)

Metric	For a given endpoint, calculate the ratio of installed software updates to the total number of required software updates.
Calculation	If `M2 == 0`, this indicates the endpoint requires no software updates. If `(M2 - M5) == 0`, this indicates the endpoint requires software updates, but the out-of-date software has an approved exception. Otherwise, this metric is calculated as `(M2 - M5) / M4`

Update Effectiveness (Organizational)

The organizational metric is calculated by averaging the results of the "per endpoint" metric above.

7.6 3.6: Compare Back-to-Back Vulnerability Scans

Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

Asset Type	Security Function	Implementation Groups
Applications	Respond	2, 3

7.6.1 Dependencies

- Sub-control 1.5: Maintain Asset Inventory Information

7.6.2 Inputs

1. The list of endpoints
2. Previous vulnerability scan results for all covered endpoints
3. Current vulnerability scan results for all covered endpoints

7.6.3 Operations

1. **For each covered endpoint:**
    1. Intersection of previous scan results with current scan results (Assumption: this should result in the complete set of results from the previous scan and set aside the new vulnerability checks introduced in the current scan)
    2. Identify set of detected vulnerabilities from previous scan, based on intersection
    3. Identify set of detected vulnerabilities from current scan, based on intersection
2. Count endpoints in the set of covered endpoints eligible for back-to-back comparisons

Assumption

- The first operation carries the assumption that the intersection of previous scan results with current scan results yields the complete set of results from the previous scan and sets aside any new vulnerability checks introduced in the current scan. Doing so should also accommodate the dynamic enterprise that is adding and removing assets as a matter of course.

7.6.4 Measures

- M1 = Set of previously detected vulnerabilities
- M2 = Set of currently detected vulnerabilities
- M3 = Count of previously detected vulnerabilities
- M4 = Count of currently detected vulnerabilities
- M5 = List of covered endpoints with back-to-back comparisons
- M6 = Count of M5
- M7 = List of endpoints in inventory eligible for back-to-back comparisons
- M8 = Count of M7

7.6.5 Metrics

Unmitigated Vulnerabilities

Metric	
	Count of vulnerabilities previously discovered that are still discovered.
Calculation	`M3 - M4`

Coverage

Metric	
	Coverage of back-to-back comparisons against eligible endpoints
Calculation	`M6 / M8`

7.7 3.7: Utilize a Risk-Rating Process

Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

Asset Type	Security Function	Implementation Groups
Applications	Respond	2, 3

7.7.1 Dependencies

- None

7.7.2 Inputs

1. Security program vulnerability management policy

7.7.3 Operations

1. Review vulnerability management policy for risk-rating process description
2. Review risk-rating process description to ensure risk-rating is used for prioritization

7.7.4 Measures

- M1 (Boolean) = Risk-rating process exists or does not exist
- M2 (Boolean) = Risk-rating process is used for prioritization

7.7.5 Metrics

Risk-Rating Process

Metric	
	Manual review: Does a risk-rating process exist and is it utilized for prioritization?
Calculation	`M1 AND M2`

CHAPTER

EIGHT

CIS CONTROL 4: CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Why is this CIS Control Critical?

The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content. If the victim user's account has administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrative passwords and other sensitive data. Similar attacks occur with email. An administrator inadvertently opens an email that contains an infected attachment and this is used to obtain a pivot point within the network that is used to attack other systems.

The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

8.1 4.1: Maintain Inventory of Administrative Accounts

Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

Asset Type	Security Function	Implementation Groups
Users	Detect	2, 3

8.1.1 Dependencies

- None

8.1.2 Inputs

1. Inventory of authorized administrative accounts including which system the account is authorized for and which individual the account is associated with
2. Output from the automated tool(s) identifying the discovered administrative accounts accompanied by which system that account is on

8.1.3 Operations

1. Generate a count of the administrative accounts in Inventory 1 (this count becomes M1). If this count is 0, skip the remaining Operation(s).
2. Check Input 2 - if there is at least 1 administrative account provided in Input 2, set M2 equal to 1 and continue on to the next Operation. If there are no administrative accounts provided in Input 2, set M2 equal to 0 and skip the remaining Operation(s).
3. Compare Input 1 and Input 2, creating a list accounts that are in Input 2 which are also found in Input 1 (this is the list of discovered authorized administrative accounts that becomes M3) and a list of accounts that are in Input 2 that are not found in Input 1 (this is the list of discovered unauthorized administrative accounts that becomes M4).

8.1.4 Measures

- M1 = Count of authorized administrative accounts in Input 1
- M2 = A binary value, 1 if the automated tool(s) provided at least 1 administrative account (Input 2); 0 if the automated tool(s) did not provide any administrative accounts (Input 2)
- M3 = List of discovered authorized administrative accounts
- M4 = List of discovered unauthorized administrative accounts
- M5 = Count of discovered authorized administrative accounts
- M6 = Count of discovered unauthorized administrative accounts

8.1.5 Metrics

Administrative Account Inventory

Metric	
	Ensure the administrative account inventory exists. If `M1 == 0`, this metric fails and the remaining metrics are not applicable.
Calculation	`M1`

Automated Tool Functioning

Metric	
	Ensure any automated tools are properly functioning. If `M2 == 0`, this metric fails and the remaining metrics are not applicable.
Calculation	`M2`

Tool Coverage

Metric	
	The ratio discovered administrative accounts to the inventoried administrative accounts.
Calculation	`M5 / M1`

Unauthorized Accounts

Metric	
	The ratio of discovered unauthorized administrative accounts to total discovered administrative accounts
Calculation	`M6 / (M5 + M6)`

8.2 4.2: Change Default Passwords

Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

Asset Type	Security Function	Implementation Groups
Users	Protect	1, 2, 3

8.2.1 Dependencies

- Sub-control 2.4: Track Software Inventory Information

8.2.2 Inputs

1. The organization's inventory of endpoints which utilize credentials, either at the OS level or at the application software level (ideally software inventory from sub-control 2.4)
2. An authoritative source of known default passwords
3. The organization's defined password policy configuration

8.2.3 Operations

1. For each endpoint in Input 1, enumerate the available logins, including hashed credentials (becomes M1)
2. For each endpoint in Input 1, generate password hashes for all relevant default passwords provided in Input 2 in accordance with the corresponding hashing procedures for the appropriate OS, application, etc. including any applicable salting
3. For each login, compare the password hash for that login to the default password hashes generated in the previous operation. Create a list containing any logins that have hashes that match default password hashes, including the endpoint to which the login corresponds and the default password and hash that was matched (becomes M3)
4. For each endpoint, collect the applied password policy configuration (becomes M5)

5. For each endpoint, compare the password policy configuration to the organizationally defined password policy recommendations (including password length, complexity requirements, etc.), creating a list of endpoint password policies that adhere to organizational policy (becomes M7) and a list of endpoint password policies that deviate from the organizational policy (becomes M9) noting where the deviations occur.

8.2.4 Measures

- M1 = The list of available logins for endpoints which utilized credentialed accounts
- M2 = The count of logins from all endpoints that use credentiale accouts (count of M1)
- M3 = The list of enumerated logins with a password hash that matches a known default password hash
- M4 = The count of logins with a password hash that matches a known default password hash (count of M3)
- M5 = The list of the collected endpoint password policy configurations
- M6 = The count of collected password policy configurations (count of M5)
- M7 = The list of collected password policy configurations that do match organizationally defined recommendations
- M8 = The count of compliant collected password policies (count of M7)
- M9 = The list of collected password policy configurations that do not match organizationally defined recommendations

8.2.5 Metrics

Default Password Usage

Metric	What percentage of credentials have been changed from the default value?
Calculation	`(M2 - M4) / M2`

Password Policy Compliance

Metric	What percentage of collected password policies comply with the organization's password policies?
Calculation	If M6 = 0, then no endpoint password policy configurations were collected. Otherwise, the value of this metric is `M8 / M6`

8.3 4.3: Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities.

Asset Type	Security Function	Implementation Groups
Users	Protect	1, 2, 3

8.3.1 Dependencies

- None

8.3.2 Inputs

1. The list of users defined as Administrators
2. The list of user accounts for the users defined in Input 1
3. The list of users NOT defined as Administrators
4. The list of user accounts for the users defined in Input 3
5. The list of all user accounts.
6. The list of all Administrative user accounts
7. The list of non-Administrative user accounts

8.3.3 Operations

1. For each user defined in Input 1, collect the Administrative user account for that user from Input 6 and the non-Administrative user account from Input 7
2. For each user defined in Input 3, collect any Administrative user account for that user from Input 6 and the non-Administrative user account from Input 7

8.3.4 Measures

- M1 = The list of defined Administrative users
- M2 = The count of M1
- M3 = The list of users collected in Operation 1
- M4 = The count of M3
- M5 = The list of users collected in Operation 2
- M6 = The count of M5
- M1 = The number of users defined as Administrators
- M2 = For each user, this measure describes the number of user accounts identified by Operation 1
- M3 = For each user, this measure describes the number of user accounts identified by Operation 2

8.3.5 Metrics

Administrative User Accounts

Metric	This metric is intended to determine whether those users identified as Administrative-level have at least one Administrative-level and one non-Administrative level user account.
Calculation	The mapping performed by Operation 1 must show that, for each Administrative-level user, at least 1 Administrative-level user account and at least 1 non-Administrative-level user account are available. Otherwise, this metric is a `FAIL`

Unauthorized User Accounts

Metric	This metric is intended to illustrate any non-Administrative-level users that have been assigned an Administrative-level user account.
Calculation	If `M6 > 0`, then `FAIL`; otherwise `PASS`

8.4 4.4: Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

8.4.1 Dependencies

- None

8.4.2 Inputs

1. Password policy that includes requirement for unique passwords

8.4.3 Operations

1. Verify that a password policy was provided and set M1 accordingly.
2. (Optional) Manually review the provided password policy. Determine if it includes a valid requirement for unique passwords and set M2 accordingly.

8.4.4 Measures

- M1 = Boolean value indicating whether a password policy was provided; 1 if policy provided, 0 if not
- M2 = (From optional manual review) Binary value indicating whether the provided password policy includes a valid requirement for unique passwords; 1 if unique passwords required, 0 if not

8.4.5 Metrics

Password Policy Existence

Metric	
	This metric indicates the existence of a password policy for the organization
Calculation	`M1 == 1`

Policy Review

(Optional Manual Review) Pass if the organization's password policy includes a unique password requirement.

8.5 4.5: Use Multi-Factor Authentication for All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

8.5.1 Dependencies

- Sub-control 2.4: Track Software Inventory Information
- Sub-control 4.1: Maintain Inventory of Administrative Accounts

8.5.2 Inputs

1. List of Administrative accounts in the organization along with corresponding authentication system for each
2. Approved Multi-Factor Authentication Configuration(s) - there may be multiple configurations based on the types of accounts and authentication systems involved
3. Approved Encrypted Channel Configuration(s) - there may be multiple configurations based on the types of accounts and authentication systems involved

8.5.3 Operations

1. For each account in Input 1, check its configuration against the appropriate Multi-Factor Authentication configuration in Input 2. Create a list of compliant accounts (M1) and non-compliant accounts (M2)
2. For each account in Input 1, check its configuration against the appropriate Encrypted Channel configuration in Input 3. Create a list of compliant accounts (M3) and non-compliant accounts (M4)

8.5.4 Measures

- M1 = List of Administrative Accounts that are configured properly for Multi-Factor Authentication (Multi-Factor compliant list)
- M2 = List of Administrative Accounts that are not configured properly for Multi-Factor Authentication (Multi-Factor non-compliant list)
- M3 = List of Administrative Accounts that are configured properly to be accessed through encrypted channels (Encrypted Channel compliant list)
- M4 = List of Administrative Accounts that are not configured properly to be accessed through encrypted channels (Encrypted Channel non-compliant list)
- M5 = Count of Multi-Factor compliant Administrative Accounts (count of M1)
- M6 = Count of Encrypted Channel compliant Administrative Accounts (count of M3)
- M7 = Total count of Administrative Accounts (count of Input 1)

8.5.5 Metrics

Multi-Factor Compliance

Metric	
	Calculate the ratio of administrative accounts configured to use multi-factor authentication to the total number of administrative accounts
Calculation	`M5 / M7`

Encrypted Channel Compliance

Metric	
	Calculate the ratio of administrative accounts configured to use encrypted channels to the total number of administrative accounts
Calculation	`M6 / M7`

8.6 4.6: Use Dedicated Workstations For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading email, composing documents, or browsing the Internet.

Asset Type	Security Function	Implementation Groups
Users	Protect	3

8.6.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

8.6.2 Inputs

1. The list of endpoints
2. The list of authorized software

8.6.3 Operations

1. Enumerate the devices used for administrative purposes based on the endpoint inventory
2. Enumerate all software identified as administrative from the software inventory
3. **For each identified device:**
    1. Enumerate the devices configured/managed by this device
    2. **Examine its configuration noting whether it is appropriately or inappropriately configured:**
        1. The device has internet access
        2. The device can run unauthorized software
        3. The device can be reached by any device not in the enumeration identified above

8.6.4 Measures

- M1 = List of devices used for administrative purposes
- M2 = List of administrative software
- M3 = List of appropriately configured devices
- M4 = List of inappropriately configured devices
- M5 = Count of devices used for administrative purposes (count of M1)
- M6 = Count of administrative software (count of M2)
- M7 = Count of appropriately configured devices (count of M3)
- M8 = Count of inappropriately configured devices (count of M4)

8.6.5 Metrics

Coverage

Metric	
	The ratio of appropriately configured administrative devices to the total number of administrative devices
Calculation	`M7 / M5`

8.7 4.7: Limit Access to Scripting Tools

Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

8.7.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 5.1: Establish Secure Configurations
- Sub-control 16.6: Maintain an Inventory of Accounts

8.7.2 Inputs

1. Inventory of Accounts including how/where access to scripting tools is restricted
2. List of accounts (administrative or developer accounts) with the need to access scripting tools, including which scripting tools are required for each account
3. Approved configuration(s) to restrict scripting tool access to only approved accounts
4. List of scripting tools to be checked
5. (Optional) List of scripting tools allowed in organization (subset of the Authorized Software List)

8.7.3 Operations

1. For each account in Input 1, determine if the account has access to any of the scripting tools provided in Input 4 by comparing the appropriate approved configuration(s) from Input 3 to the configuration location(s) specified for that account in Input 1. Create a list of accounts that conform to the appropriate configuration(s) and policy for scripting tool access (M1) noting which configuration(s) they were checked against, and a list of accounts that do not conform to the appropriate configuration(s) and policy for scripting tool access (M2) noting the configuration(s) they were checked against and the deviations from those configurations. For each account on both lists, note which, if any, scripting tools that account has access to.
2. (Optional) Compare the scripting tools authorized for particular accounts identified in Input 2 to the authorized scripting tools provided in Input 5. Create a list of scripting tools that are authorized for particular accounts but are not authorized for use in the organization (M5).
3. (Optional) For each account authorized to access scripting tools in M2, verify that the account is an administrative or developer account. Create a list of accounts that are authorized for scripting tools but that are not administrative or developer accounts (M6).

8.7.4 Measures

- M1 = List of accounts that conform to the appropriate configuration(s) and policy for scripting tool access (compliant list)
- M2 = List of accounts that do not conform to the appropriate configuration(s) and policy for scripting tool access (non-compliant list)
- M3 = Count of accounts that are compliant with the scripting tool access policy (count of M1)
- M4 = Total count of accounts (count of Input 1)
- M5 (Optional) = List of scripting tools authorized for particular accounts but not authorized for use in the organization
- M6 (Optional) = List of accounts that are authorized for scripting tools but that are not administrative or developer accounts

8.7.5 Metrics

Coverage

Metric	
	Ratio of accounts that comply with the scripting tool access policy
Calculation	`M3 / M4`

8.8 4.8: Log and Alert on Changes to Administrative Group Membership

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

Asset Type	Security Function	Implementation Groups
Users	Detect	2, 3

8.8.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 5.1: Establish Secure Configurations

8.8.2 Inputs

1. Endpoint inventory
2. Approved configuration(s) for logging of accounts being added to groups with administrative privileges
3. Approved configuration(s) for logging of accounts being removed from groups with administrative privileges
4. Approved configuration(s) for alerting when accounts are added to groups with administrative privileges
5. Approved configuration(s) for alerting when accounts are removed from groups with administrative privileges

Note: there may be multiple configurations for Inputs 2 - 5 to account for various groups/types of endpoints.

8.8.3 Operations

1. For each endpoint in Input 1, select the appropriate approved configuration from Inputs 2 - 5 in turn for that endpoint and check to see if that endpoint's actual configuration complies with the approved configuration for each Input. Record this information as M1 - a list of endpoints annotated with whether that endpoint is compliant or non-compliant with the appropriate approved configuration from each of the four inputs (Input 2 - Input 5).
2. For each of the Inputs 2 - 5, generate a count of compliant endpoints from M1 and record these as M2, M3, M4, and M5 respectively
3. Count the number of endpoints that are compliant with all 4 inputs and record this as M6

8.8.4 Measures

- M1 = List of endpoints with each endpoint entry labeled with compliance or non-compliance for each of the 4 logging/alerting configurations from Inputs 2 - 5
- M2 = Count of compliant endpoints based on Input 2 configurations
- M3 = Count of compliant endpoints based on Input 3 configurations
- M4 = Count of compliant endpoints based on Input 4 configurations
- M5 = Count of compliant endpoints based on Input 5 configurations
- M6 = Count of endpoints that are compliant with configurations from all 4 inputs
- M7 = Count of endpoints from Input 1
- M8 = List of compliant endpoints based on Input 2 configurations
- M9 = List of non-compliant endpoints based on Input 2 configurations
- M10 = List of compliant endpoints based on Input 3 configurations
- M11 = List of non-compliant endpoints based on Input 3 configurations
- M12 = List of compliant endpoints based on Input 4 configurations
- M13 = List of non-compliant endpoints based on Input 4 configurations
- M14 = List of compliant endpoints based on Input 5 configurations
- M15 = List of non-compliant endpoints based on Input 5 configurations
- M16 = Count of non-compliant endpoints based on Input 2 configurations
- M16 = Count of non-compliant endpoints based on Input 3 configurations
- M16 = Count of non-compliant endpoints based on Input 4 configurations
- M16 = Count of non-compliant endpoints based on Input 5 configurations

8.8.5 Metrics

Logging of Accounts Added to Groups

Metric	The ratio of endpoints logging when accounts are added to groups to the total number of endpoints
Calculation	`M2 / M7`

Logging of Accounts Removed from Groups

Metric	The ratio of endpoints logging when accounts are removed from groups to the total number of endpoints
Calculation	`M3 / M7`

Alerting of Accounts Added to Groups

Metric	The ratio of endpoints alerting when accounts are added to groups to the total number of endpoints
Calculation	`M4 / M7`

Alerting of Accounts Removed from Groups

Metric	The ratio of endpoints alerting when accounts are removed from groups to the total number of endpoints
Calculation	`M5 / M7`

Combined Compliance

Metric	The ratio of endpoints both alerting and logging when accounts are both added and removed to the total number of endpoints
Calculation	`M6 / M7`

8.9 4.9: Log and Alert on Unsuccessful Administrative Account Login

Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

Asset Type	Security Function	Implementation Groups
Users	Detect	2, 3

8.9.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 5.1: Establish Secure Configurations

8.9.2 Inputs

1. Endpoint inventory
2. Approved configuration(s) for logging on unsuccessful login attempts to administrative accounts
3. Approved configuration(s) for alerting on unsuccessful login attempts to administrative accounts

Note: there may be multiple configurations for Inputs 2 and 3 to account for various groups/types of endpoints.

8.9.3 Operations

1. For each endpoint in Input 1, select the appropriate approved configuration from Inputs 2 and 3 in turn for that endpoint and check to see if that endpoint's actual configuration complies with the approved configuration for each Input. Record this information as M1 - a list of endpoints annotated with whether that endpoint is compliant or non-compliant with the appropriate approved configuration from each of the two inputs (Input 2 and Input 3).
2. For Input 2, and for Input 3, generate a count of compliant endpoints from M1 and record these as M2 and M3 respectively.
3. Count the number of endpoints that are compliant with both inputs and record this as M4

8.9.4 Measures

- M1 = List of endpoints with each endpoint entry labeled with compliance or non-compliance for both Input 2 and Input 3
- M2 = Count of compliant endpoints based on Input 2 configurations
- M3 = Count of compliant endpoints based on Input 3 configurations
- M4 = Count of endpoints that are compliant with configurations from both inputs
- M5 = Total number of endpoints from Input 1
- M6 = List of compliant endpoints based on Input 2 configurations
- M7 = List of non-compliant endpoints based on Input 2 configurations
- M8 = List of compliant endpoints based on Input 3 configurations
- M9 = List of non-compliant endpoints based on Input 3 configurations
- M10 = Count of non-compliant endpoints based on Input 2 configurations
- M11 = Count of non-compliant endpoints based on Input 3 configurations

8.9.5 Metrics

Logging Unsuccessful Login Attempts

Metric	The ratio of endpoints logging when unsuccessful login attempts are made, to the total number of endpoints
Calculation	`M2 / M5`

Alerting Unsuccessful Login Attempts

Metric	The ratio of endpoints alerting when unsuccessful login attempts are made, to the total number of endpoints
Calculation	`M3 / M5`

Combined Compliance

Metric	The ratio of endpoints both alerting and logging unsuccessful login attempts are made, to the total number of endpoints
Calculation	`M4 / M5`

CHAPTER

NINE

CIS CONTROL 5: SECURE CONFIGURATION FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS AND SERVERS

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why is this CIS Control Critical?

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared towards ease-of-deployment and ease-of-use – not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, and pre-installation of unneeded software can be exploitable in their default state.

Developing configuration settings with good security properties is a complex task beyond the ability of individual users, requiring analysis of potentially hundreds or thousands of options in order to make good choices (the Procedures and Tools section below provides resources for secure configurations). Even if a strong initial configuration is developed and installed, it must be continually managed to avoid security "decay" as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked" to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network accessible services and client software.

9.1 5.1: Establish Secure Configurations

Maintain documented security configuration standards for all authorized operating systems and software.

Asset Type	Security Function	Implementation Groups
Applications	Protect	1, 2, 3

9.1.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

9.1.2 Inputs

1. Authorized Software List: The list of authorized software (sub-control 2.1).
2. Security Configuration Standards: The list of enterprise security configuration standards.

Assumptions

- Documentation of secure configuration standards should include any approved deviations/exceptions from industry-standard security baselines such as CIS benchmarks, DISA Security Technical Implementation Guides (STIGs), or U.S. government configuration baselines (USGCB).

9.1.3 Operations

1. Perform a set calculation, computing the Intersection (M1) of Input 1 and Input 2

9.1.4 Measures

- M1 = The list of authorized software with associated enterprise security configuration standards
- M2 = Count of M1
- M3 = The list of authorized software without enterprise security configuration standards (the "left" side of the set calculation)
- M4 = Count of M3
- M5 = The list of enterprise security configuration standards without associated authorized software (the "right" side of the set calculation)
- M6 = Count of M5
- M7 = The list of authorized software
- M8 = Count of M7

9.1.5 Metrics

Security Configuration Standards Coverage

Metric	For what percentage of the total OS/Software in an enterprise, are security configuration standards documented and maintained?
Calculation	`(M8 - M4) / M8`

9.2 5.2: Maintain Secure Images

Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

9.2.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 5.1: Establish Secure Configurations

9.2.2 Inputs

1. The list of the organization's approved configuration standards, per implementation of sub-control 5.1
2. The inventory of systems
3. The mapping of systems in the inventory to any secure configurations that should be applied. This input assumes that multiple configurations could apply to a single system in the inventory.
4. The inventory of images

9.2.3 Operations

1. For each system in the inventory, determine the list of systems which have had an image taken and the list of systems without a corresponding image.
2. For each system with a corresponding image, compare the image's configuration with the configuration standard(s) mapped to that system.

9.2.4 Measures

- M1 = Count of systems in the inventory (from Input 2)
- M2 = Count of systems with a corresponding image taken
- M3 = 1 if an image is configured according to the standards mapped to that system; 0 otherwise.
- M4 = List of systems with a corresponding image taken
- M5 = List of systems without a corresponding image taken

9.2.5 Metrics

Image Coverage

Metric	The ratio of systems with a corresponding image taken to the total number of inventoried systems
Calculation	`M2 / M1`

Configuration Coverage

Metric	
	The ratio of all systems with a corresponding image taken to those configured according to the standards mapped to that system
Calculation	`(SUM from 1..M2 (M3)) / M2`

9.3 5.3: Securely Store Master Images

Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

9.3.1 Dependencies

- None

9.3.2 Inputs

1. The list of master images/templates
2. An available integrity monitoring tool
3. The inventory of master images mapped to the output of the integrity monitoring tool's identifying information (such as a hash).
4. A documented procedure detailing authorizations required for updates to the master images/templates

9.3.3 Operations

1. Collect the list of master images/templates' integrity monitoring identifying information (i.e. for each master image, collect the hash).
2. Determine whether the update procedure documentation exists (M3)

9.3.4 Measures

- M1 = Count of master images/templates (from Input 3)
- M2 = Count of master images/templates identified by integrity monitoring tools
- M3 = 1 if the documented master image update procedure exists; 0 otherwise.
- M4 = List of master images/templates identified by integrity monitoring tools
- M5 = List of master images/templates unidentified by integrity monitoring tools
- M6 = Count of master images/templates unidentified by integrity monitoring tools (M5)

9.3.5 Metrics

Integrity Monitoring Coverage

Metric	
	The ratio of master images/templates identified by integrity monitoring tools, to the total number of images/templates.
Calculation	`M2 / M1`

Update Procedures

Metric	
	Determine if the documented master image update procedure exists
Calculation	`M3 == 1`

9.4 5.4: Deploy System Configuration Management Tools

Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

9.4.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 2.4: Track Software Inventory Information
- Sub-control 5.1: Establish Secure Configurations

9.4.2 Inputs

1. The organization's configuration monitoring system
2. The list of endpoints
3. The inventory and mappings of secure configuration policy(ies) to the list of endpoints
4. The organization's approved configuration scanning interval (at least weekly)

Assumptions

1. A timestamp "t" is defined as the time of a given configuration assessment
2. A subsequent assessment, following the approved scanning interval (Input 4), is noted as "t+1"

9.4.3 Operations

1. For each endpoint, obtain the configuration assessment results using Input 1. Note this as M1(t).
2. Following the time period specified by Input 4, re-assess to obtain a comparative assessment result. Note this as M1(t+1)

Assumptions

- The assumption is that remediation/redeployment of configuration settings is occurring based on the improvement of scores over time and subsequent assessments.

9.4.4 Measures

- M1(t) = (For each endpoint) Count of non-compliant recommendations resulting from Operation 1
- M1(t+1) = (For each endpoint) Count of non-compliant recommendations resulting from Operation 2
- M2 = (For each endpoint) Count of recommendations assessed
- M3 = The number of endpoints
- M4 = List of non-compliant endpoints resulting from Operation 1
- M5 = List of non-compliant endpoints resulting from Operation 2

9.4.5 Metrics

Initial Non-Compliance

Metric	The ratio of non-compliant recommendations at time "t", to the total recommendations assessed.
Calculation	`M1(t) / M2`

Subsequent Non-Compliance

Metric	The ratio of non-compliant recommendations at time "t+1" ()
Calculation	`M1(t+1) / M2`

Overall Compliance

Metric	What is the average overall compliance for all assessed endpoints at time "t"
Calculation	`(SUM from 1..M3 (M1(t) / M2)) / M3`

9.5 5.5: Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

Asset Type	Security Function	Implementation Groups
Applications	Detect	2, 3

9.5.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 2.4: Track Software Inventory Information
- Sub-control 5.1: Establish Secure Configurations

9.5.2 Inputs

1. The organization's configuration monitoring system
2. The list (maintained by NIST) of SCAP-validated tools
3. The list of endpoints
4. The inventory and mappings of secure configuration policy(ies) to the list of endpoints
5. The list of approved exceptions, mapped to the endpoints on which they are approved (i.e. some endpoints may be excepting certain configurations, but others under the same configuration policy may not).
6. The organization's approved configuration scanning interval (at least weekly)

9.5.3 Operations

1. (Manual) Ensure the configuration scanning tool (Input 1) is present in the list of SCAP-validated tools (Input 2).
2. For each endpoint, obtain the configuration assessment results using Input 1
3. For each assessment result in Operation 2, obtain the list of recommendations which map to the catalog of approved exceptions for that endpoint.
4. Following the time period specified by Input 6, re-assess to obtain a comparative assessment result

9.5.4 Measures

- M1 = 1 if Operation 1 indicates the organization's scanning tool is present in the list of SCAP-validated tools; 0 otherwise
- M2 = (For each endpoint) The number of non-compliant recommendations resulting from Operation 2
- M3 = (For each endpoint) The number of non-compliant recommendations that do not map to the catalog of approved exceptions for the endpoint
- M4 = (For each endpoint) The number of non-compliant recommendations resulting from Operation 4
- M5 = (For each endpoint) The number of non-compliant recommendations that do not map to the catalog of approved exceptions for the endpoint
- M6 = (For each endpoint) The number of recommendations assessed
- M7 = (For each endpoint) The number of approved configuration policy exceptions

- M8 = The number of the organization's SCAP-validated tools
- M9 = The number of the organization's configuration management tools

9.5.5 Metrics

Tooling Compliance

Metric	Are SCAP-validated configuration scanning tool(s) being used?
Calculation	`M1 == 1`

Tooling Compliance Coverage

Metric	The ratio of SCAP-validated tools to the total number of configuration management tools
Calculation	`M8 / M9`

Initial Non-Compliance (Per Endpoint)

Metric	Per endpoint, the ratio of non-compliant recommendations to the total recommendations assessed.
Calculation	`M2 / M6`

Initial Exception Coverage (Per Endpoint)

Metric	Per endpoint, the ratio of non-compliant recommendations with approved exceptions, to the total recommendations assessed.
Calculation	`(M7 - M3) / M7`

Subsequent Non-Compliance (Per Endpoint)

Metric	
	Per endpoint, the ratio of non-compliant recommendations to the total recommendations assessed.
Calculation	`M4 / M6`

Subsequent Exception Coverage (Per Endpoint)

Metric	
	Per endpoint, the ratio of non-compliant recommendations with approved exceptions, to the total recommendations assessed.
Calculation	`(M7 - M5) / M7`

CHAPTER

TEN

CIS CONTROL 6: MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Why is this CIS Control Critical?

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

10.1 6.1: Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

10.1.1 Dependencies

- Sub-control 1.5: Maintain Asset Inventory Information

10.1.2 Inputs

1. The list of endpoints
2. The list of network time sources/NTP servers

10.1.3 Operations

1. From the list of endpoints, filter to collect the list of those servers and network devices that should be configured.
2. From the list of servers/network devices, collect each endpoint's network time configuration
3. Collect the list of servers/network devices whose network time configuration does not include a network time source.

10.1.4 Measures

- M1 = Count of endpoints
- M2 = Count of endpoints configured to synchronize with NTP servers
- M3 = Count of endpoints whose network time configuration does not include an approved network time source
- M4(i) = (For each endpoint "i" collected in Operation 1) 1 when the number of configured NTP servers >= 3; 0 otherwise.
- M5 = List of endpoints configured to synchronize with NTP servers
- M6 = List of endpoints whose network time configuration does not include an approved network time source

10.1.5 Metrics

NTP Compliance Coverage

Metric	
	The ratio of endpoints using at least 3 synchronized time sources to the total set of endpoints
Calculation	`(SUM from i=1..M2 (M4(i)) / M2)`

10.2 6.2: Activate Audit Logging

Ensure that local logging has been enabled on all systems and networking devices.

Asset Type	Security Function	Implementation Groups
Network	Detect	1, 2, 3

10.2.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 5.1: Establish Secure Configurations

10.2.2 Inputs

1. Endpoint Inventory: The list of endpoints from the endpoint inventory
2. The list of events that should be logged (an event logging policy).

Assumptions

The assumption is that there could potentially be numerous events which should be logged, and that a checklist verifying the logging policy can be examined per endpoint.

10.2.3 Operations

1. For each endpoint, determine if the configured event logging policy matches the policy defined by Input 2, noting appropriately and inappropriately configured endpoints.

10.2.4 Measures

- M1 = The list of endpoints
- M2 = Count of M1
- M3 = The list of appropriately configured endpoints
- M4 = Count of M3
- M5 = The list of inappropriately configured endpoints
- M6 = Count of M5

10.2.5 Metrics

Logging Policy Coverage

Metric	
	Determine the ratio of endpoints implementing the prescribed event logging policy to the total number of endpoints.
Calculation	`M4 / M6)`

10.3 6.3: Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

10.3.1 Dependencies

- Sub-control 1.5: Maintain Asset Inventory Information

10.3.2 Inputs

1. The list of endpoints (subject to system logging configuration)
2. The organization's logging configuration policy, outlining the detailed information to be written to system logs

10.3.3 Operations

1. For each endpoint, collect the system logging configuration

10.3.4 Measures

- M1(i) = (For each endpoint "i") 1 if the endpoint's logging configuration complies with the organizations logging policy; 0 otherwise.
- M2 = Count of endpoints from Input 1
- M3 = List of compliant endpoints
- M4 = List of non-compliant endpoints

10.3.5 Metrics

Logging Coverage

Metric	
	The ratio of endpoints configured to enable detailed system logging to the total number of endpoints.
Calculation	`(SUM from i=1..M2 (M1(i))) / M2`

10.4 6.4: Ensure Adequate Storage for Logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

10.4.1 Dependencies

- Sub-control 1.5: Maintain Asset Inventory Information

10.4.2 Inputs

1. The list of endpoints (subject to system logging configuration)
2. The organization's logging configuration policy, outlining log rotation policy, maximum log storage size, etc.

10.4.3 Operations

1. For each endpoint, collect the system logging configuration

10.4.4 Measures

- M1(i) = (For each endpoint "i") 1 if an endpoint's logging configuration complies with the organizations logging policy; 0 otherwise.
- M2 = The number of endpoints from Input 1
- M3 = List of compliant endpoints
- M4 = List of non-compliant endpoints

10.4.5 Metrics

Logging Storage Coverage

Metric	
	The ratio of endpoints compliant with the organization's logging policy to the total number of endpoints.
Calculation	`(SUM from i=1..M2 (M1(i))) / M2`

10.5 6.5: Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

10.5.1 Dependencies

- Sub-control 2.4: Track Software Inventory Information

10.5.2 Inputs

1. The total number of log producers (M1)
2. The number of sensors correlated in a central service (M2)

10.5.3 Operations

N/A

10.5.4 Measures

- M1 = Count log producers
- M2 = Count of sensors correlated in a central service

10.5.5 Metrics

Quality of Log correlation/aggregation

Metric	
	The ratio of log producers correlated in a central service to the total number of log producers.
Calculation	`M2 / M1`

10.6 6.6: Deploy SIEM or Log Analytic Tools

Deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

10.6.1 Dependencies

- Sub-control 2.4: Track Software Inventory Information

10.6.2 Inputs

1. Install location of SIEM or log analytic tool
2. The number of log producers correlated by a SIEM
3. The total number of log producers

10.6.3 Operations

N/A

10.6.4 Measures

- M1 = 1 if a SIEM or other log analytics tool is installed/present; 0 otherwise
- M2 = Count of log producers correlated by a SIEM
- M3 = Count of log producers
- M4 = List of log producers correlated by a SIEM
- M5 = List of log producers not correlated by a SIEM

10.6.5 Metrics

Quality of SIEM Correlation

Metric	
	The ratio of log producers correlated by a SIEM to the total number of log producers
Calculation	`IF M1 == 1 THEN M2 / M3; OTHERWISE 0`

10.7 6.7: Regularly Review Logs

On a regular basis, review logs to identify anomalies or abnormal events.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

10.7.1 Dependencies

- None

10.7.2 Inputs

1. The timestamp at which a log review i has been made, represented as t(i)
2. The number of reviews (timestamps) taken so far, represented as N
3. The maximum possible irregularity (can be fixed as 30 day), represented as R
4. (Optional) Target/desirable review interval threshold, represented as T
5. The number of log reviews in which at least one anomaly was detected, represented as D
6. The total number of Log Reviews, represented as L

10.7.3 Operations

1. Calculate the average of log review, M1 = `(SUM from i=1..N (t(i+1) - t(i))) / N`
2. Calculate the threshold-based regularity measure of log review, M2 = `(SUM from i=1..N ( (t(i+1) - t(i)) - T)^2 / N ) / R`
3. Calculate the probability of detecting an anomaly in log review, M3 = `D / L`

10.7.4 Measures

- M1 = The average of log review from Operation 1
- M2 = The threshold-based regularity measure of log review from Operation 2
- M3 = The probability of detecting an anomaly in log review from Operation 3

10.7.5 Metrics

Regularity Measure of Log Review

Metric	
	Measure the irregularity or variance of log review. The higher the value the more irregularity.
Calculation	`(SUM from i=1..N ( (t(i+1) - t(i)) - M1)^2 / N ) / R`

Quality of Log Review

Metric	
	The quality of review is high if-and-only-if the review is highly regular and the potential for detecting anomalies (at least one per review) is also high.
Calculation	`(1-M2) * M3`

10.8 6.8: Regularly Tune SIEM

On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

Asset Type	Security Function	Implementation Groups
Network	Detect	3

10.8.1 Dependencies

- Sub-control 6.6: Deploy SIEM or Log Analytic Tools

10.8.2 Inputs

1. Enterprise-defined SIEM operation procedures
2. Current time

10.8.3 Operations

1. Examine enterprise SIEM operation procedures to identify maximum allowed delay in tuning frequency (default: 1 week)
2. Ask SIEM operators when they last tuned the SIEM

10.8.4 Measures

- M1 = Boolean value, 1, if a set of enterprise-defined SIEM operational procedures exists, 0 otherwise
- M2 = Maximum allowed delay in tuning
- M3 = Current time
- M4 = Last SIEM tuning time

10.8.5 Metrics

Procedure Existence

Metric	Does an enterprise-defined set of SIEM operational procedures exist?
Calculation	`M1 = 1?`

SIEM Tuning Freshness

Metric	How recently was the SIEM last tuned?
Calculation	`(M3 - M4) / M2`

CHAPTER

ELEVEN

CIS CONTROL 7: EMAIL AND WEB BROWSER PROTECTIONS

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Why is this CIS Control Critical?

Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means that users interact with untrusted environments, these are potential targets for both code exploitation and social engineering.

11.1 7.1: Ensure Use of Only Fully Supported Browsers and Email Clients

Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.

Asset Type	Security Function	Implementation Groups
Applications	Protect	1, 2, 3

11.1.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

11.1.2 Inputs

1. From the authorized software list (ASL: sub-control 2.1), the inventory of web browser and email client software with a notation of "supported" or "unsupported" for each entry.
2. Access to an authoritative source of information indicating supported/unsupported details by product.

11.1.3 Operations

1. For each entry in Input 1, perform a lookup in Input 2 to verify.
2. For each entry in Input 1 labeled "supported", perform a lookup in Input 2. From these lookups, note the list of authorized software labeled "supported" but are actually not supported based on the authoritative source lookup.
3. For each entry in Input 1 labeled "unsupported", perform a lookup in Input 2. From these lookups, note the list of authorized software labeled "unsupported" but are actually supported based on the authoritative source lookup.

11.1.4 Measures

- M1 = List of unsupported items in Input 1 (combination of Operation 1 results and those initially marked as unsupported in input 1)
- M2 = Count of M1
- M3 = List of authorized web browser/email client software
- M4 = Count of M3
- M5 = List of items from Input 1 labeled as "supported" that are not actually supported
- M6 = Count of M5
- M7 = List of items from Input 1 labeled as "unsupported" but are actually supported
- M8 = Count of M7

11.1.5 Metrics

Percentage of Unsupported Web Browser/Email Client Software in Use

Metric	
	The calculation of this metric is determined by the ratio of unsupported web browser/email client software to the total authorized web browser/email client software in use.
Calculation	`(M4 - M2) / M4`

Rate of False Positives

Metric	
	The calculation of this metric is determined by the ratio of web browser/email client software labeled "supported" but found to be unsupported, to the total authorized web browser/email client software in use.
Calculation	`(M4 - M6) / M4`

Rate of False Negatives

Metric	
	The calculation of this metric is determined by the ratio of web browser/email client software labeled "unsupported" but found to be supported, to the total authorized web browser/email client software in use.
Calculation	`(M4 - M8) / M4`

11.2 7.2: Disable Unnecessary or Unauthorized Browser or Email Client Plugins

Uninstall or disable any unauthorized browser or email client plugins or add-on applications.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

11.2.1 Dependencies

- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software

11.2.2 Inputs

1. The list of authorized browser plugins
2. The list of authorized email client plugins
3. The list of endpoints

11.2.3 Operations

1. From the list of all endpoints, collect the list of endpoints subject to browser/email plugin restrictions
2. For each endpoint listed by Operation 1, collect the list of installed browser plugins
3. For each endpoint listed by Operation 1, collect the list of installed email client plugins
4. For each endpoint, calculate the complement of the installed browser plugins with the list of approved browser plugins from Input 1. The complement will yield any installed browser plugins not on the approved list.
5. For each endpoint, calculate the complement of the installed email client plugins with the list of approved email client plugins from Input 2. The complement will yield any installed email client plugins not on the approved list.

11.2.4 Measures

- M1 = Count of endpoints subject to browser/email plugin restrictions
- M2(i) = (For each endpoint "i") Count of installed browser plugins not in the approved list (The count resulting from Operation 4)

- M3(i) = 0 if, for each endpoint "i", the value of M2 > 0; 1 if the value of M2 == 0
- M4(i) = (For each endpoint "i") Count of installed email client plugins not in the approved list (The count resulting from Operation 5)
- M5(i) = 0 if, for each endpoint "i", the value of M4 > 0; 1 if the value of M4 == 0

11.2.5 Metrics

Browser Plugin Enforcement Quality

Metric	
	The ratio of endpoints utilizing browser plugins on the approved list to the total number of endpoints.
Calculation	`(SUM from i=1..M1 (M3(i))) / M1`

Email Client Plugin Enforcement Quality

Metric	
	The ratio of endpoints utilizing email client plugins on the approved list to the total number of endpoints.
Calculation	`(SUM from i=1..M1 (M5(i))) / M1`

11.3 7.3: Limit Use of Scripting Languages in Web Browsers and Email Clients

Ensure that only authorized scripting languages are able to run in all web browsers and email clients.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

11.3.1 Dependencies

- Sub-control 2.5: Integration Software and Hardware Asset Inventories
- Sub-control 5.1: Establish Secure Configurations

11.3.2 Inputs

1. List of web browsers and email clients installed in the organization by endpoint
2. Approved configuration(s) covering each web browser and email client in Input 1 to restrict the scripting languages that can run to only the authorized scripting languages

11.3.3 Operations

1. For each application instance (web browser or email client) in Input 1, check the application's configuration against the appropriate approved configuration(s) from Input 2.
2. Create a list of the application instances that meet the approved configuration (M1)
3. Create a list of the application instances that that do not meet the approved configuration (M2) noting each deviation.

11.3.4 Measures

- M1 = List of application instances (web browser or email client) that meet the approved configuration (compliant list)
- M2 = List of application instances (web browser or email client) that do not meet the approved configuration (non-compliant list)
- M3 = Count of compliant application instances (count of M1)
- M4 = Count of non-compliant application instances (count of M2)
- M5 = Total count of installed web browser and email client instances (count of Input 1)

11.3.5 Metrics

Coverage

Metric	Ratio of compliant web browser and email client instances
Calculation	`M3 / M5`

11.4 7.4: Maintain and Enforce Network-Based URL Filters

Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

11.4.1 Dependencies

- Sub-control 2.5: Integration Software and Hardware Asset Inventories
- Sub-control 5.1: Establish Secure Configurations

11.4.2 Inputs

1. List of web clients/browsers installed in the organization by endpoint
2. Approved configuration(s) covering each web browser/client in Input 1 indicating whether or not the browser must utilize URL filtering

11.4.3 Operations

1. For each application instance (web browser/client) in Input 1, check the application's configuration against the appropriate approved configuration(s) from Input 2.
2. Create a list of the application instances that meet the approved configuration (M1)
3. Create a list of the application instances that that do not meet the approved configuration (M2) noting each deviation.

11.4.4 Measures

- M1 = List of application instances (web browser/client) that meet the approved configuration (compliant list)
- M2 = List of application instances (web browser or email client) that do not meet the approved configuration (non-compliant list)
- M3 = Count of compliant application instances (count of M1)
- M4 = Count of non-compliant application instances (count of M2)
- M5 = Total count of installed web browser and email client instances (count of Input 1)

11.4.5 Metrics

Coverage

Metric	Calculate the quality of URL-filter enforcement.
Calculation	`M3 / M5`

11.5 7.5: Subscribe to URLCategorization Service

Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

11.5.1 Dependencies

- None

11.5.2 Inputs

1. The organization's URL categorization service subscription.

Assumptions

- Subscription to a URL categorization service provides an organization the ability to intercept a user's intended URL, determine if it has been categorized, and allow/prevent access to that URL based on the (lack of) categorization. Potentially a browser plugin? Potentially some filtering method on a network device or the organization's network perimeter?

11.5.3 Operations

1. A user attempts to access an uncategorized URL

11.5.4 Measures

- M1 = 1 if the organization subscribes to URL categorization services; 0 otherwise
- M2 = 1 if access to the uncategorized URL is blocked; 1 otherwise.

11.5.5 Metrics

Enforcement

Metric	
	Calculate whether URL categorization is successfully blocking uncategorized URL access.
Calculation	`M1 AND M2`

11.6 7.6: Log All URL Requests

Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

11.6.1 Dependencies

- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

11.6.2 Inputs

1. The list of endpoints
2. The organization's logging configuration policy, detailing URL logging configuration

11.6.3 Operations

1. For each endpoint, collect the system logging configuration

11.6.4 Measures

- M1(i) = (For each endpoint "i") 1 if the endpoint's logging configuration complies with the organizations logging policy; 0 otherwise.
- M2 = Count of endpoints from Input 1

11.6.5 Metrics

Configuration Coverage

Metric	
	The ratio of devices which enable URL request logging to the total number of devices.
Calculation	`(SUM from i=1..M2 (M1(i))) / M2`

11.7 7.7: Use of DNS Filtering Services

Use Domain Name System (DNS) filtering services to help block access to known malicious domains.

Asset Type	Security Function	Implementation Groups
Network	Protect	1, 2, 3

11.7.1 Dependencies

- Sub-control 1.5: Maintain Asset Inventory Information

11.7.2 Inputs

1. Endpoint Inventory: The list of endpoints to be audited (sub-control 1.5).
2. The list of accepted DNS filtering services, such as Quad-9.

11.7.3 Operations

1. For each endpoint in Input 1, collect it's DNS configuration setting noting appropriately and inappropriately configured endpoints.

11.7.4 Measures

- M1 = List of audited endpoints
- M2 = Count of M1
- M3 = List of appropriately configured endpoints
- M4 = Count of M3
- M5 = List of inappropriately configured endpoints
- M6 = Count of M5

11.7.5 Metrics

DNS Filtering Coverage

Metric	
	Determine the ratio of endpoints configured to use accepted DNS filtering services to the total number of endpoints which utilize DNS.
Calculation	`M4 / M2`

Traffic Analysis

NOTE A second measurement could utilize traffic analysis to determine if any traffic is *not* being sent through the prescribed DNS services.

11.8 7.8: Implement DMARC and Enable Receiver-Side Verification

To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

11.8.1 Dependencies

- Sub-control 2.4: Track Software Inventory Information

11.8.2 Inputs

1. DMARC policy
2. TXT record published in DNS
3. The Mail Transfer Agent used by the organization (this could indicate DKIM is used to sign outgoing messages)
4. The Mail User Agent used by the organization (this could indicate DKIM is used to verify incoming messages)

Assumptions

- The DMARC configuration policy includes instructions to produce either Aggregate (rua) or Forensic (ruf) reports.
- The organization has access to these reports either daily (for Aggregate) or in real-time (for Forensic).

11.8.3 Operations

1. Examine the TXT records in DNS for a `v` value indicating DMARC
2. Examine the TXT records in DNS for a `v` value indicating SPF
3. Examine the TXT records in DNS for a `v` value indicating DKIM

11.8.4 Measures

- M1 = 1 if Input 1 exists and Operation 1 indicates the use of DMARC
- M2 = 1 if Operation 2 indicates the use of SPF
- M3 = 1 if Operation 3 indicates the use of DKIM

11.8.5 Metrics

DMARC Usage

Metric	
	Ensure usage and proper configuration of DMARC/SPF/DKIM
Calculation	`M1 AND M2 AND M3`

11.9 7.9: Block Unnecessary File Types

Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

11.9.1 Dependencies

- Sub-control 2.5: Integration Software and Hardware Asset Inventories
- Sub-control 5.1: Establish Secure Configurations

11.9.2 Inputs

1. The list of endpoints
2. The organization's approved email gateway configuration, including file types to be blocked.

11.9.3 Operations

1. From Input 1, collect endpoints configured as email gateway(s) (M2)
2. For each endpoint collected in Operation 1, collect the system's attachment blocking configuration

11.9.4 Measures

- M1(i) = (For each email gateway "i") 1 if the email gateway's configuration complies with the organizations attachment blocking policy; 0 otherwise.
- M2 = Count of email gateways

11.9.5 Metrics

Coverage

Metric	
	The ratio of endpoints configured as email gateways that are properly configured to the total number of email gateway endpoints
Calculation	`(SUM from i=1..M2 (M1(i))) / M2`

11.10 7.10: Sandbox All Email Attachments

Use sandboxing to analyze and block inbound email attachments with malicious behavior.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

11.10.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

11.10.2 Inputs

1. The list of authorized software

11.10.3 Operations

1. Enumerate all e-mail servers in the enterprise
2. For each identified e-mail server, examine its configuration to ensure that either native attachment sandboxing is configured or that an external system is configured to be used for that purpose, noting appropriately and inappropriately configured servers

Assumptions

- The majority of e-mail servers have appropriate configuration attributes to examine.

11.10.4 Measures

- M1 = List of all e-mail servers in the enterprise
- M2 = List of appropriately configured e-mail servers
- M3 = List of inappropriately configured e-mail servers
- M4 = Count of all e-mail servers in the enterprise (count of M1)
- M5 = Count of appropriately configured e-mail servers (count of M2)
- M6 = Count of inappropriately configured e-mail servers (count of M3)

11.10.5 Metrics

Coverage

Metric	
	The ratio of appropriately configured e-mail servers to the total number of e-mail servers
Calculation	`M5 / M4`

CHAPTER

TWELVE

CIS CONTROL 8: MALWARE DEFENSES

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Why is this CIS Control Critical?

Malicious software is an integral and dangerous aspect of Internet threats, as it is designed to attack your systems, devices, and your data. It is fast-moving, fast-changing, and enters through any number of points like end-user devices, email attachments, web pages, cloud services, user actions, and removable media. Modern malware is designed to avoid defenses, and attack or disable them.

Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating, and integration with processes like incident response. They must also be deployed at multiple possible points of attack to detect, stop the movement of, or control the execution of malicious software. Enterprise endpoint security suites provide administrative features to verify that all defenses are active and current on every managed system.

12.1 8.1: Utilize Centrally Managed Anti-Malware Software

Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

12.1.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software

Assumption(s)

- It is assumed that this sub-control is specific to host-based anti-malware solutions.

12.1.2 Inputs

1. List of deployed anti-malware software
2. The list of endpoints

12.1.3 Operations

1. For each deployed anti-malware solution, verify that it is centrally managed
2. For each deployed anti-malware solution, enumerate the set of endpoints covered
3. Union the set of covered endpoints
4. Identify set of endpoints eligible for anti-malware coverage (i.e. network devices likely do not run anti-malware agents)

12.1.4 Measures

- M1 = Count of anti-malware solutions in use
- M2 = Count of anti-malware solutions that are centrally managed
- M3 = Total number of endpoints covered by anti-malware solutions
- M4 = Total number of endpoints eligible for anti-malware coverage
- M5 = List of anti-malware solutions that are centrally managed
- M6 = List of anti-malware solutions that are not centrally managed
- M7 = List of endpoints covered by anti-malware solutions
- M8 = List of endpoints not covered by anti-malware solutions

12.1.5 Metrics

Anti-Malware Management Coverage

Metric	Percentage of anti-malware solutions that are centrally managed
Calculation	`M2 / M1`

Endpoint Anti-Malware Coverage

Metric	Percentage of endpoints covered by anti-malware solutions
Calculation	`M3 / M4`

12.2 8.2: Ensure Anti-Malware Software and Signatures Are Updated

Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

Asset Type	Security Function	Implementation Groups
Devices	Protect	1, 2, 3

12.2.1 Dependencies

- Sub-control 1.4: Integrate Software and Hardware Asset Inventories
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.4: Track Software Inventory Information

12.2.2 Inputs

1. Endpoint Inventory: Endpoint inventory (with entry for each endpoint indicating whether that endpoint can support anti-malware software or not; sub-control 1.4)
2. Anti-malware software version information (this is a list of acceptable versions for the scanning engines and the signature databases for any anti-malware products in use on endpoints in Input 1; this version information needs to be updated frequently to reflect current version information and age off outdated versions; reference the ASL per sub-control 2.1 and ideally leverage the software inventory in sub-control 2.4)
3. Maximum time allowed for anti-malware software updates to be applied to endpoints

Assumptions

- Some endpoints, such as network devices, may not support anti-malware software. Whether an endpoint supports anti-malware software is provided as part of Input 1. Devices that cannot support anti-malware software are removed from the list of endpoints to be checked during Operation 1, and these devices are not counted in the metric below.

12.2.3 Operations

1. Refine the endpoint inventory (Input 1) to only contain endpoints that can support anti-malware software endpoint inventory - this reduced list of endpoints becomes M1
2. For each endpoint in M1, generate a list of those endpoints that have an acceptable version of anti-malware software installed and enabled (both scanning engine and signature database) according to the information provided in Input 2 (M2) and a list of those endpoints that do not have an acceptable version of anti-malware software installed and enabled (M3).
3. For each endpoint in M1, generate a list of those endpoints that have been updated within the time frame specified by Input 3 (M4), and a list of those endpoints that have not been updated within that time-frame (M5)

12.2.4 Measures

- M1 = List of endpoints capable of supporting anti-malware software
- M2 = List of endpoints with an acceptable version of anti-malware software installed and enabled (version compliant list)
- M3 = List of endpoints that do not have an acceptable version of anti-malware software installed and enabled (version non-compliant list)
- M4 = List of endpoints that have had their anti-malware software updated within the specified time-frame (time compliant list)
- M5 = List of endpoints that have not had their anti-malware software updated within the specified time-frame (time non-compliant list)
- M6 = Count of endpoints in M1 (number of endpoints capable of supporting anti-malware software)
- M7 = Count of endpoints in M2 (number of version compliant endpoints)
- M8 = Count of endpoints in M3 (number of version non-compliant endpoints)

- M9 = Count of endpoints in M4 (number of time compliant endpoints)
- M10 = Count of endpoints in M5 (number of endpoints that have not had updates within acceptable time frame)

12.2.5 Metrics

Coverage

Metric	
	The ratio of anti-malware software version compliant endpoints to the total number of endpoints capable of supporting anti-malware software?
Calculation	`M7 / M9`

Freshness

Metric	
	The ratio of endpoints whose anti-malware software has been updated within the specified timeframe?
Calculation	`M9 / M6`

NOTE: Comparing the coverage metric to the freshness metric can serve as a useful check - for instance, if the coverage metric tends to be high, while the freshness metric is low, that would suggest that Input 2 might not have been updated recently enough (that is, outdated versions are being considered acceptable)?

12.3 8.3: Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

12.3.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

12.3.2 Inputs

1. List of endpoints
2. Approved configuration(s) to enable anti-exploitation features (Operating System feature, toolkit, etc.) for each type of endpoint in Input 1

12.3.3 Operations

1. For each endpoint in Input 1, examine the endpoint to see if it is configured according to the approved configuration(s).
2. Create a list of the endpoints that meet the the approved configurations (M1)
3. Create a list of the endpoints that do not meet the approved configurations (M2), noting each deviation.

12.3.4 Measures

- M1 = Count of endpoints that meet the approved anti-exploitation configurations, such as DEP, ASLR or similar technologies (compliant list)
- M2 = Count of endpoints
- M3 (Optional) = List of endpoints that meet the approved anti-exploitation configurations, such as DEP, ASLR or similar technologies (compliant list)
- M4 (Optional) = List of endpoints that do not meet the approved anti-exploitation configurations, such as DEP, ASLR or similar technologies (non-compliant list)
- M5 (Optional) = Count of non-compliant endpoints (M2 - M1)
- M6 = List of non-compliant endpoints

12.3.5 Metrics

Metric	
	Ratio of endpoints compliant with anti-exploitation configurations to the total number of endpoints
Calculation	`M1 / M2`

12.4 8.4: Configure Anti-Malware Scanning of Removable Media

Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

Asset Type	Security Function	Implementation Groups
Devices	Detect	1, 2, 3

12.4.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 5.1: Establish Secure Configurations

12.4.2 Inputs

1. Endpoint Inventory: Endpoint inventory (with entry for each endpoint indicating whether that endpoint can support anti-malware software or not)
2. Desired anti-malware configuration (to automatically scan removable media when inserted/connected)

12.4.3 Assumptions

Some endpoints, such as network devices, may not support anti-malware software. Whether an endpoint supports anti-malware software is provided as part of Input 1. Devices that cannot support anti-malware software are removed from the list of endpoints to be checked during Operation 1, and these devices are not counted in the metric below.

12.4.4 Operations

1. Refine the endpoint inventory (Input 1) to only contain endpoints that can support anti-malware software endpoint inventory - this reduced list of endpoints becomes M1
2. Of the set of endpoints that can support anti-malware software (M1), generate a list of those endpoints that actually have anti-malware software installed, enabled, and adhere to the configuration specified in Input 2 (M2) and a list of the endpoints that do not adhere to the specified configuration (M3). Note: Endpoints in M1 that do not have anti-malware installed and enabled, are considered non-compliant and added to M3.

12.4.5 Measures

- M1 = List of endpoints capable of supporting anti-malware software
- M2 = List of endpoints with anti-malware software installed, enabled, and properly configured to scan removable media (compliant list)
- M3 = List of endpoints not adhering to the specified configuration (non-compliant list)
- M4 = Count of endpoints in M1 (number of endpoints capable of supporting anti-malware software)
- M5 = Count of endpoints in M2 (number of compliant endpoints)
- M6 = Count of endpoints in M3 (number of non-compliant endpoints)

12.4.6 Metrics

Coverage

Metric	What is the ratio of endpoints compliant with the desired anti-malware configuration to the total number of endpoints capable of supporting anti-malware software?
Calculation	`M5 / M4`

12.5 8.5: Configure Devices to Not Auto-Run Content

Configure devices to not auto-run content from removable media.

Asset Type	Security Function	Implementation Groups
Devices	Protect	1, 2, 3

12.5.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 5.1: Establish Secure Configurations

12.5.2 Inputs

1. Endpoint Inventory: Endpoint inventory
2. Desired configuration(s) to disable auto-run. There may be multiple configurations targeted at different types of endpoints (for instance, a different configuration might be provided for each type of operating system used on the endpoints in the provided inventory). If the endpoints are capable of performing multiple types of auto-run behavior (i.e., auto-run vs. auto-play), appropriate configurations should be provided for each type.

12.5.3 Operations

1. For each endpoint in Input 1, compare the endpoint's configuration to the appropriate configuration from Input 2. Generate a list of endpoints that adhere to the specified configuration (M1) and a list of the endpoints that do not adhere to the specified configuration (M2).

Assumption

Endpoints that are not capable of performing any type of auto-run behavior would be included in the compliant list (M1).

12.5.4 Measures

- M1 = List of endpoints adhering to the specified configuration (compliant list)
- M2 = List of endpoints not adhering to the specified configuration (non-compliant list)
- M3 = Count of endpoints in M1 (number of compliant endpoints)
- M4 = Count of endpoints in M2 (number of non-compliant endpoints)
- M5 = Count of endpoints in the endpoint inventory (Input 1)

12.5.5 Metrics

Metric	The ratio of endpoints properly disabling auto-run to the total number of endpoints?
Calculation	`M3 / M5`

12.6 8.6: Centralize Anti-Malware Logging

Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

12.6.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 5.1: Establish Secure Configurations

12.6.2 Inputs

1. List of software instances (anti-malware software, anti-malware administration tools, and event log servers) that need to be configured to properly send, receive, and log these malware detection events.
2. Approved configuration(s) for anti-malware software, anti-malware administration tools, and event log servers to ensure that malware detection events are properly sent, received, and logged.
3. The total number of malware detection events (M5)
4. The number of alerts being correlated in a central service (M6)

12.6.3 Operations

1. For each software instance in Input 1, check to see if it is configured according to the appropriate approved configuration(s) in Input 2.
2. Create a list of the software instances that are properly configured (M1)
3. Create a list of the software instances that are not properly configured (M2) noting where the deviations occur.

12.6.4 Measures

- M1 = List of software instances that are properly configured for the sending/receiving of malware detection events (compliant list)
- M2 = List of software instances that are not properly configured for the sending/receiving of malware detection events (non-compliant list)
- M3 = Count of properly configured software instances (count of M1)
- M4 = Total count of software instances that need to be configured to properly send/receive malware detection events (count of Input 1)
- M5 = Count of malware detection events
- M6 = Count of alerts being correlated in a central service

12.6.5 Metrics

Coverage

Metric	
	Ratio of properly configured software instances for sending/receiving malware detection events.
Calculation	`M3 / M4`

Quality

Metric	
	Quality of Log correlation/aggregation for Anti-Malware
Calculation	`M6 / M5`

12.7 8.7: Enable DNS Query Logging

Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

12.7.1 Dependencies

- Sub-control 2.5: Integrate Software and Hardware Asset Inventories
- Sub-control 5.1: Establish Secure Configurations

12.7.2 Inputs

1. The list of internal DNS servers
2. The organization's DNS configuration policy

Assumption

- The organization maintains its own internal DNS server

12.7.3 Operations

1. For each internal DNS server (Input 1), compare the server's DNS configuration with the organization's DNS configuration policy

12.7.4 Measures

- M1 = Count of internal DNS servers
- M2 = Count of internal DNS servers matching the organization's configuration policy

- M3 = List of compliant DNS servers
- M4 = List of non-compliant DNS servers

12.7.5 Metrics

DNS Configuration Coverage

Metric	
	The ratio of internal DNS servers matching the approved configuration to the total number of internal DNS servers.
Calculation	`M2 / M1`

12.8 8.8: Enable Command-Line Audit Logging

Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

12.8.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 5.1: Establish Secure Configurations

12.8.2 Inputs

1. The list of endpoints
2. Approved configuration(s) for command line auditing of command shells (note: there may be multiple configurations based on the various types of endpoints, including various operating systems, etc.)

12.8.3 Operations

1. For each endpoint in Input 1, examine the endpoint to see if it is configured according to the appropriate approved configuration(s) from Input 2.
2. Create a list of endpoints that meet the approved configuration (M1)
3. Create a list of endpoints that do not meet the approved configuration (M3), noting the deviations.

12.8.4 Measures

- M1 = List of endpoints that meet the approved command shell logging configurations (compliant list)
- M2 = Count of endpoints (count of Input 1)
- M3 (Optional) = List of endpoints that do not meet the approved command shell logging configurations (non-compliant list)
- M4 (Optional) = Count of non-compliant endpoints (count of M3)

12.8.5 Metrics

Coverage

Metric	
	The ratio of endpoints compliant with command shell logging configurations to the total number of endpoints
Calculation	`M1 / M2`

CHAPTER

THIRTEEN

CIS CONTROL 9: LIMITATION AND CONTROL OF NETWORK PORTS, PROTOCOLS AND SERVICES

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers

Why is this CIS Control Critical?

Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and DNS servers installed by default on a variety of different device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such services and attempt to exploit these services, often attempting to exploit default user IDs and passwords or widely available exploitation code.

13.1 9.1: Associate Active Ports, Services, and Protocols to Asset Inventory

Associate active ports, services, and protocols to the hardware assets in the asset inventory.

Asset Type	Security Function	Implementation Groups
Devices	Identify	2, 3

13.1.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

13.1.2 Inputs

1. The list of endpoints

13.1.3 Operations

1. **For each endpoint, identify necessary detailed information**
    1. **Active ports**
        1. Protocol Served
    2. Installed services (running or not)
2. Identify endpoints with all detailed information identified

13.1.4 Measures

- M1 = Count of endpoints in inventory
- M2 = Count of endpoints with all detailed information
- M3 = List of endpoints with all detailed information
- M4 = List of endpoints missing at least one piece of detailed information
- M5 = Count of endpoints missing at least one piece of detailed information

13.1.5 Metrics

Quality

Metric	
	The ratio of endpoints with all detailed information to the total number of endpoints under management.
Calculation	`M2 / M1`

13.2 9.2: Ensure Only Approved Ports, Protocols, and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

13.2.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

13.2.2 Inputs

1. List of authorized ports with validated business need
2. List of authorized protocols with validated business need
3. List of authorized services with validated business need
4. List of endpoints

13.2.3 Operations

1. **For each endpoint perform the following to build sets of information:**
    1. Scan for open ports
    2. **For each open port**

        1. Test protocol running on that port
    3. Enumerate installed services
2. Enumerate discovered ports
3. Enumerate discovered services
4. Determine set of unauthorized ports
5. Determine set of unauthorized services

13.2.4 Measures

- M1 = Set of open ports
- M2 = Set of unauthorized ports
- M3 = Set of discovered services
- M4 = Set of unauthorized services
- M5 = Set of unexpected protocols discovered on open ports

13.2.5 Metrics

Ports

Metric	Ratio of unauthorized ports to open ports
Calculation	`M2 / M1`

Services

Metric	Ratio of unauthorized services to discovered services
Calculation	`M4 / M3`

Unexpected Protocols

Metric	Ratio of unexpected protocols discovered on open ports to total number of open ports
Calculation	`M5 / M1`

13.3 9.3: Perform Regular Automated Port Scans

Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

13.3.1 Dependencies

- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

13.3.2 Inputs

1. t(i): the timestamp at which a port scan i has been performed
2. N: the number of port scans (timestamps) taken so far
3. M: the maximum possible irregularity (can be fixed as 30 day)
4. T: (optional) target/desirable review interval threshold
5. D: the number of port scan in which at least one anomaly was detected
6. L: The total number of port scans
7. UP: The number of alerts received due to unauthorized ports (M5)
8. NP: The number of unauthorized ports (M6)

13.3.3 Operations

- Enumerate endpoints and identify port scanning software
- Calculate measures M1 - M6 for each port scanning software, tracking endpoints covered
- Enumerate set of endpoints covered by port scanning software
- Compare enumeration of covered endpoints against the list of all endpoints to identify those endpoints that are not covered

13.3.4 Measures

- M1 (the average of port scans) = `SUM from i=1..N ( t(i+1) - t(i) ) / N`
- M2 (Regularity Measure of Port Scan) = `(SUM from i=1..N ( (t(i+1) - t(i) - M1)^2 / N ) / M`
- M3 (Threshold-based Regularity Measure of Port Scan) = `(SUM from i=1..N ( ( t(i+1) - t(i) - T )^2 / N ) / M`
- M4 (The Probability of detecting an anomaly in port scans) = `D / L`
- M5 = Count of alerts received due to unauthorized ports
- M6 = Count of unauthorized ports
- M7 = List of endpoints covered by port scanning tools
- M8 = List of endpoints not covered by port scanning tools
- M9 = Count of endpoints covered by port scanning tools
- M10 = Count of endpoints

13.3.5 Metrics

Quality of Port Scan

Metric	
	Quality of review is high if and only if the review is highly regular and the potential for detecting anomalies (at least one per review) is also high.
Calculation	`(1 - M2) * M4` or (if M3) `(1 - M3) * M4`

Quality

Metric	
	Ratio of unauthorized ports reported
Calculation	`M5 / M6`

Coverage

Metric	
	Ratio of covered endpoints to the total number of endpoints
Calculation	`M9 / M10`

13.4 9.4: Apply Host-Based Firewalls or Port-Filtering

Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Asset Type	Security Function	Implementation Groups
Devices	Protect	1, 2, 3

13.4.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

13.4.2 Inputs

1. Endpoint Inventory: Derive from the endpoint inventory those endpoints able to scan (assumed capable of hosting firewall/port-filtering software)
2. A policy (or set of policies, potentially individually per endpoint) indicating the ports that are allowed to be open

13.4.3 Operations

1. For each endpoint, retrieve the firewall policy
2. For each firewall policy, enumerate both the ports which allow communication, and any configuration of a default deny rule (could that be a default?), noting along the way appropriately configured policies and inappropriately configured policies

13.4.4 Measures

- M1 = List of endpoints
- M2 = Count of M1
- M3 = List of endpoints with appropriately configured firewall ports policy
- M4 = Count of M3
- M5 = List of endpoints with inappropriately configured firewall ports policy
- M6 = Count of M5
- M7 = List of endpoints with appropriately configured default deny rule
- M8 = Count of M7
- M9 = List of endpoints with inappropriately configured default deny rule
- M10 = Count of M9
- M11 = List of endpoints with both appropriately configured firewall policy
- M12 = Count of M11
- M13 = List of endpoints with at least one inappropriate firewall configuration
- M14 = Count of M13

13.4.5 Metrics

Coverage

Metric	
	The ratio of correctly configured endpoints to the total number of endpoint?
Calculation	`M14 / M2`

13.5 9.5: Implement Application Firewalls

Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

13.5.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

13.5.2 Inputs

1. The list of endpoints
2. The list of authorized software

13.5.3 Operations

1. Enumerate endpoints identified as critical in the endpoint inventory
2. Enumerate all application firewalls from the software inventory
3. **For each identified application firewall, enumerate the endpoints it covers**
    1. Enumerate the set of identified endpoints - covered endpoints
4. Complement the set of covered endpoints with the set of critical endpoints

13.5.4 Measures

- M1 = List of critical endpoints
- M2 = List of application firewalls
- M3 = List of endpoints covered by at least one application firewall
- M4 = List of endpoints not covered by at least one application firewall
- M5 = Count of critical endpoints (count of M1)
- M6 = Count of application firewalls (count of M2)
- M7 = Count of endpoints covered by at least one application firewall (count of M3)
- M8 = Count of endpoints not covered by at least one application firewall (count of M4)

13.5.5 Metrics

Coverage

Metric	The ratio of endpoints covered by at least one application firewall to the total number of critical endpoints
Calculation	`M7 / M5`

CHAPTER

FOURTEEN

CIS CONTROL 10: DATA RECOVERY CAPABILITIES

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Why is this CIS Control Critical?

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

14.1 10.1: Ensure Regular Automated Backups

Ensure that all system data is automatically backed up on a regular basis.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

14.1.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

14.1.2 Inputs

1. Endpoint Inventory: Endpoint Inventory
2. Backup configuration policy is available
3. Backup software (either OS or 3d party) configuration is available and able to be queried
4. Backup software logs are available and can be queried
5. Successful backup staleness threshold is defined (a maximum time period allowed between backups; recommended value of at least weekly)

14.1.3 Operations

#. For each endpoint, examine its backup configuration with the available configuration policy (noting appropriately configured and inappropriately configured endpoints along the way), and examine its logs to determine the most recent

successful backup completion time (noting whether it was run within the enterprise-defined staleness threshold). # Enumerate the endpoints that are both appropriately configured and do not have stale backups

1. Compare an endpoints backup configuration with available configuration policy
2. Interrogate logs to determine most recent successful backup completion time

14.1.4 Measures

- M1 = List of endpoints
- M2 = Count of M1
- M3 = List of appropriately configured endpoints
- M4 = Count of M3
- M5 = List of inappropriately configured endpoints
- M6 = Count of M5
- M7 = List of endpoints both appropriately configured and without stale backups
- M8 = Count of M7
- M9 = List of endpoints either inappropriately configured or without stale backups
- M10 = Count of M9

14.1.5 Metrics

Coverage

Metric	What percentage of endpoints are successfully backing up system data on a regular basis?
Calculation	`M8 / M2`

14.2 10.2: Perform Complete System Backups

Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

14.2.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

14.2.2 Inputs

1. Key Systems: The list of "key systems" identified by the organization, as derived from the endpoint inventory (see sub-control 1.4)
2. The organization's backup/imaging configuration policy

Assumptions

- Backup software (either OS or 3d party) is installed and appropriately configured on "key systems" identified in Input 1

14.2.3 Operations

1. For each endpoint in the list of "key systems", examine its backup configuration against the available backup configuration policy, noting appropriately and inappropriately configured endpoints along the way.

14.2.4 Measures

- M1 = List of "key system" endpoints
- M2 = Count of M1
- M3 = List of appropriately configured "key systems"
- M4 = Count of M3
- M5 = List of inappropriately configured "key systems"
- M6 = Count of M5

14.2.5 Metrics

Coverage

Metric	What percentage of key systems are successfully backed up as a complete system?
Calculation	`M4 / M2`

14.3 10.3: Test Data on Backup Media

Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

14.3.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

14.3.2 Inputs

1. The current set of backup media for the organization
2. t(i): the timestamp at which a backup restoration i has been performed
3. N: the number of backup restorations (timestamps) performed so far
4. M: the maximum possible irregularity (can be fixed as 30 day)
5. T: (optional) target/desirable review interval threshold

6. D: the number of backup restorations in which at least one anomaly was detected
7. L: The total number of backup restorations

14.3.3 Operations

1. Given a sampling of backup media from Input 1, restore the backup to a temporary location

Assumption

- The assumption is made that the organization will know what a "properly working" restored backup entails.

14.3.4 Measures

- M1 = Count of backups under test
- M2 = Count of restored backups deemed "properly working" following restoration
- M3 = The average of backup restorations = `SUM from i=1..N ( t(i+1) - t(i) ) / N`
- M4 (Regularity Measure of Backup Restoration) = `(SUM from i=1..N ((t(i+1) - t(i)) - M3)^2 / N ) / M`
- M5 (Threshold-based Regularity Measure of Backup Restoration) = `(SUM from i=1..N ((t(i+1) - t(i) - T)^2 / N ) / M`
- M6 (The Probability of detecting an anomaly in Backup Restoration) = `D / L`

14.3.5 Metrics

Backup Integrity Quality

Metric	The ratio of "properly working" backups to the total number of backups under test
Calculation	`M2 / M1`

Quality of Backup Restoration

Metric	Quality of backup restoration is high if and only if the backup restoration is highly regular and the potential for detecting anomalies (at least one per review) is also high.
Calculation	`(1-M4) * M6` or (if M5) :code:`(1 - M5) / M6

14.4 10.4: Protect Backups

Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

14.4.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

14.4.2 Inputs

1. The list of endpoints configured for periodic backup, derived from the endpoint inventory (see sub-control 1.4)
2. The organization's backup configuration policy

Assumptions

- Backup software (either OS or 3d party) is installed and appropriately configured on endpoints identified in Input 1

14.4.3 Operations

1. Interrogate the organization's backup configuration policy to determine if backups are configured to be encrypted
2. For each endpoint, examine its backup configuration policy to ensure that encrypted backups are configured, noting appropriately and inappropriately configured endpoints along the way.

14.4.4 Measures

- M1 = List of endpoints
- M2 = Count of M1
- M3 = List of appropriately configured endpoints
- M4 = Count of M3
- M5 = List of inappropriately configured endpoints
- M6 = Count of M5

14.4.5 Metrics

Coverage

Metric	What percentage backups are protected via physical security/encryption?
Calculation	`M6 / M2`

14.5 10.5: Ensure All Backups Have at Least One Offline Backup Destination

Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

14.5.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

14.5.2 Inputs

1. Endpoint Inventory: List of endpoints
2. Backup configuration policy assuming inclusion of "offline" backup destination

14.5.3 Operations

1. Collect list of endpoints matching/not-matching policy specified by Input 2

14.5.4 Measures

- M1 = List of endpoints
- M2 = Count of M1
- M3 = List of endpoints matching policy
- M4 = Count of M3
- M5 = List of endpoints not matching policy
- M6 = Count of M5

14.5.5 Metrics

Coverage

Metric	What is the ratio of endpoints matching the backup configuration policy to the total number of endpoints?
Calculation	`M4 / M2`

Lack of Coverage

Metric	What is the ratio of endpoints *not* matching the backup configuration policy to the total number of endpoints?
Calculation	`M5 / M2`

CHAPTER

FIFTEEN

CIS CONTROL 11: SECURE CONFIGURATION FOR NETWORK DEVICES, SUCH AS FIREWALLS, ROUTERS, AND SWITCHES

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why is this CIS Control Critical?

As delivered from manufacturers and resellers, the default configurations for network infrastructure devices are geared for ease-of-deployment and ease-of-use – not security. Open services and ports, default accounts (including service accounts) or passwords, support for older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state. The management of the secure configurations for networking devices is not a onetime event, but a process that involves regularly re-evaluating not only the configuration items but also the allowed traffic flows. Attackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed and then left undone when they are no longer applicable to the business needs. In some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need and can change over time.

Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses a compromised machine to pose as another trusted system on the network.

15.1 11.1: Maintain Standard Security Configurations for Network Devices

Maintain documented security configuration standards for all authorized network devices.

Asset Type	Security Function	Implementation Groups
Network	Identify	2, 3

15.1.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

15.1.2 Inputs

1. The list of authorized network devices, per Control 1.
2. The list of enterprise security configuration standards.

Assumption

- Documentation of secure configuration standards should include any approved deviations/exceptions from industry-standard security baselines such as CIS benchmarks, DISA Security Technical Implementation Guides (STIGs), or U.S. government configuration baselines (USGCB).

15.1.3 Operations

1. Perform a set calculation, computing the Intersection (M1) of Input 1 and Input 2

15.1.4 Measures

- M1 = The intersection of Input 1 and Input 2. This intersection measures those authorized network devices with security configuration standards.
- M2 = The "left" side of the set calculation measures the number of authorized network devices without security configuration standards.
- M3 = The "right" side of the set calculation measures the number of security configuration standards without any authorized network devices to which they are associated.
- M4 = Count of authorized network devices.

15.1.5 Metrics

Coverage

Metric	
	The ratio of network devices to which standard, documented security configuration standards exist to the total number of network devices
Calculation	`(M4 - M2) / M4`

15.2 11.2: Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need

Asset Type	Security Function	Implementation Groups
Network	Identify	2, 3

15.2.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

15.2.2 Inputs

1. The list of traffic flow configurations for network devices. (M5)
2. The inventory of configuration rules pertaining to traffic flow through network devices. (M4)

15.2.3 Operations

1. Perform a set calculation, computing the Intersection (M1) of Input 1 and Input 2
2. Examine the inventory of configuration rules to manually determine those traffic flow rules which do not contain complete information (such as names, business needs, etc) (M6)

15.2.4 Measures

- M1 = The intersection of Input 1 and Input 2. This intersection measures which of the inventoried configuration rules are contained in the enterprise's security configuration standards.
- M2 = The "left" side of the set calculation measures the traffic flow configuration which are not documented in the inventory.
- M3 = The "right" side of the set calculation measures any configuration rules in the inventory which are not currently configured on the network device.
- M4 = Count of traffic flow configuration rules in the inventory.
- M5 = The current traffic flow configuration for the network device
- M6 = Count of traffic flow rules in the inventory that are incomplete

15.2.5 Metrics

- If M2 > 0 then there are traffic flows configured on the device which are not documented in the inventory.
- If M3 > 0, there are configuration items in the inventory no longer configured in the device's configuration.

Coverage

Metric	The ratio of undocumented traffic flow configurations to the current total traffic flow configurations
Calculation	`M2 / M5`

Completeness

Metric	
	The ratio of inventoried but incomplete traffic flow rules to the total set of traffic flow rules.
Calculation	`M6 / M4`

15.3 11.3: Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configurations against approved security configurations defined for each network device in use, and alert when any deviations are discovered.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

15.3.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software

15.3.2 Inputs

1. The organization's configuration monitoring system
2. The list of network devices
3. The inventory and mappings of secure configuration policy(ies) to the list of network devices

15.3.3 Operations

1. For each network devices, obtain the configuration assessment results using Input 1

15.3.4 Measures

- M1(i) = (For each network device "i") Count of non-compliant recommendations resulting from Operation 1
- M2(i) = (For each network device "i") Count of recommendations assessed

15.3.5 Metrics

Non-Compliance Ratio

Metric	
	The ratio of network devices not in compliance with secure configuration policies to the total number of network devices.
Calculation	`(SUM from i=1..M2 (M1(i))) / M2`

15.4 11.4: Install the Latest Stable Version of Any Security-Related Updates on All Network Devices

Install the latest stable version of any security-related updates on all network devices.

Asset Type	Security Function	Implementation Groups
Network	Protect	1, 2, 3

15.4.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

15.4.2 Inputs

1. Network device inventory, derived from the endpoint inventory (see sub-control 1.4)
2. Network device version information (this is a list of acceptable versions for each model of network device in Input 1; this version information needs to be updated frequently to reflect current version information and age off outdated versions)

15.4.3 Operations

1. For each network device in Input 1, compare the network device's version to the allowable versions from Input 2.
2. Generate a list of those network devices that match an allowable version (M1)
3. Generate a list of those network devices that do not match an allowable version (M2).

15.4.4 Measures

- M1 = List of network devices
- M2 = Count of M1
- M3 = List of network devices that match an allowable version (compliant list)
- M4 = Count of M3
- M5 = List of network devices that do not match an allowable version (non-compliant list)
- M6 = Count of M5

15.4.5 Metrics

Coverage

Metric	
	What percentage of inventoried network devices match the allowable version for that device/OS?
Calculation	If M2 > 0, then `M4 / M2`; otherwise `0`

15.5 11.5: Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions

Manage all network devices using multi-factor authentication and encrypted sessions.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

15.5.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

15.5.2 Inputs

1. Network device inventory
2. Network device configuration policy

Assumption

- The network device configuration policy (Input 2) details the use of multi-factor authentication and use of encrypted sessions

15.5.3 Operations

1. For each network device, compare its running configuration to the device's configuration policy for use of multi-factor authentication
2. For each network device, compare its running configuration to the device's configuration policy for use of encrypted sessions

15.5.4 Measures

- M1 = Count of network devices
- M2(i) = (For each network device "i") 1 if the network device's running configuration matches the configuration policy for use of multi-factor authentication (Operation 1); 0 otherwise
- M3(i) = (For each network device "i") 1 if the network device's running configuration matches the configuration policy for use of encrypted sessions (Operation 1); 0 otherwise

15.5.5 Metrics

Multi-Factor Coverage

Metric	
	The ratio of network devices properly configured for multi-factor authentication to the total number of network devices.
Calculation	`(SUM from i=1..M1 (M2(i))) / M1`

Encrypted Session Coverage

Metric	
	The ratio of network devices properly configured for use of encrypted sessions to the total number of network devices.
Calculation	`(SUM from i=1..M1 (M3(i))) / M1`

15.6 11.6: Use Dedicated Workstations for All Network Administrative Tasks

Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

15.6.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

15.6.2 Inputs

1. The set of devices used for administrative purposes
2. The access control configuration

15.6.3 Operations

N/A

15.6.4 Measures

- M1(i) = (For each machine "i") 1 if an administrative device has internet access; 0 otherwise.
- M2(i) = (For each machine "i") 1 if administrative device can run any application that is not administrative; 0 otherwise.
- M3 = Count of administrative devices

15.6.5 Metrics

Administrative Device Configuration

Metric	
	The ratio of improperly configured administrative devices to the total number of administrative devices.
Calculation	`(SUM from i=1..M3 (M1(i) AND M2(i))) / M3`

15.7 11.7: Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

15.7.1 Dependencies

- None

15.7.2 Inputs

1. List of management/administration paths for network infrastructure

15.7.3 Operations

1. For each management path in Input 1, use a tool or process (which might be manual review) to determine if that management network connection is separate from all business (non-network management) network connections.
2. Create a list (M1) of the management paths that are separate from all non-network management network connections (noting the type of network separation - VLAN, physical, etc.)
3. Create a list of the management paths that do not have adequate separation from non-network management connections (M2) noting the deviations.

15.7.4 Measures

- M1 = List of network management paths that are adequately separated (compliant list)
- M2 = List of network management paths that are not adequately separated (non-compliant list)
- M3 = Count of adequately separated network management paths (count of M1)
- M4 = Total count of network management paths (count of Input 1)

15.7.5 Metrics

Coverage

Metric	
	The ratio of adequately separated management paths to the total number of management paths.
Calculation	`M3 / M4`

CHAPTER

SIXTEEN

CIS CONTROL 12: BOUNDARY DEFENSE

Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

Why is this CIS Control Critical?

Attackers focus on exploiting systems that they can reach across the Internet, including not only DMZ systems but also workstations and laptop computers that pull content from the Internet through network boundaries. Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters.

To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic.

It should be noted that boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies. These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems. However, even with this blurring of boundaries, effective security deployments still rely on carefully configured boundary defenses that separate networks with different threat levels, sets of users, data and levels of control. And despite the blurring of internal and external networks, effective multi-layered defenses of perimeter networks help lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

16.1 12.1: Maintain an Inventory of Network Boundaries

Maintain an up-to-date inventory of all of the organization's network boundaries.

Asset Type	Security Function	Implementation Groups
Network	Identify	1, 2, 3

16.1.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

16.1.2 Inputs

1. An inventory of expected boundary devices (M1) as derived from the endpoint inventory (see sub-control 1.4)

16.1.3 Operations

1. Utilize a discovery tool or process to examine the network topology to collect the list of devices considered boundary devices (M2).
2. Evaluate the complement of Input 1 and Operation 1 to get the list of non-inventoried boundary devices (M3).

16.1.4 Measures

- M1 = List of expected network boundary devices
- M2 = Count of M1
- M3 = List of discovered network boundary devices
- M4 = Count of M3
- M5 = List of non-inventoried boundary devices
- M6 = Count of M5

16.1.5 Metrics

Coverage

Metric	
	What is the ratio of non-inventoried boundary devices to expected boundary devices? If the calculated value is greater than zero, the inventory is not current.
Calculation	`M6 / M2`

16.2 12.2: Scan for Unauthorized Connections Across Trusted Network Boundaries

Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

16.2.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 12.1: Maintain an Inventory of Network Boundaries

16.2.2 Inputs

1. Inventory of Network Boundaries
2. List of most recent scan times for each network boundary
3. Maximum allowable time frame between scans

16.2.3 Operations

1. For each network boundary in Input 1, compare the corresponding time of most recent scan from Input 2 to the maximum allowable time provided in Input 3.
2. Create a list of network boundaries whose most recent scan time was within the allowable time frame (M1).
3. Create a list of network boundaries whose most recent scan time was outside the allowable time frame (M2).

16.2.4 Measures

- M1 = List of network boundaries whose most recent scan time was within the allowable time frame (compliant list)
- M2 = List of network boundaries whose most recent scan time was outside the allowable time frame (non-compliant list)
- M3 = Count of network boundaries that were scanned recently enough (count of M1)
- M4 = Total count of network boundaries (count of Input 1)

16.2.5 Metrics

Coverage

Metric	
	The ratio of network boundary devices scanned within the allowable timeframe to the total number of network boundary devices
Calculation	`M3 / M4`

16.3 12.3: Deny Communications With Known Malicious IP Addresses

Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

16.3.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 12.1: Maintain an Inventory of Network Boundaries

16.3.2 Inputs

1. The list of endpoints
2. The list of trusted and necessary IP address ranges
3. The list of known malicious IP addresses
4. The list of unused Internet IP addresses

16.3.3 Operations

1. Enumerate all network devices identified as guarding a network boundary
2. **For each network boundary device, examine its configuration to ensure rules as follows, noting appropriately and inappropriately configured devices:**
    1. Allow communications only with IP addresses in the list of trusted and necessary IP address ranges
    2. Explicitly deny communications with IP addresses in the list of known malicious IP addresses
    3. Explicitly deny communications with IP addresses in the list of unused IP addresses

16.3.4 Measures

- M1 = List of all network boundary devices
- M2 = List of appropriately configured network boundary devices
- M3 = List of inappropriately configured network boundary devices
- M4 = Count of network boundary devices (the count of M1)
- M5 = Count of appropriately configured network boundary devices (the count of M2)
- M6 = Count of inappropriately configured network boundary devices (the count of M3)

16.3.5 Metrics

Coverage

Metric	The ratio of appropriately configured network boundary devices to the total number of network boundary devices
Calculation	`M5 / M4`

16.4 12.4: Deny Communication Over Unauthorized Ports

Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

Asset Type	Security Function	Implementation Groups
Network	Protect	1, 2, 3

16.4.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.4: Track Software Inventory Information

16.4.2 Inputs

1. List of endpoints to scan (assumed capable of hosting firewall/port-filtering software) as derived from the endpoint inventory (see sub-control 1.4), and potentially as additionally informed the software inventory (see sub-control 2.4)
2. A policy (or set of policies, potentially individually per endpoint) indicating the ports that are allowed to be open

16.4.3 Operations

1. For each endpoint, retrieve its firewall policy
2. For each endpoint/firewall policy pair, examine the endpoint's configuration to enumerate the ports that allow communication and any configuration of a default deny rule, noting appropriately configured and inappropriately configured endpoints along the way.

16.4.4 Measures

- M1 = List of scanned endpoints
- M2 = Count of M1
- M3 = List of endpoints with appropriate port configuration
- M4 = Count of M3
- M5 = List of endpoints with inappropriate port configuration
- M6 = Count of M5
- M7 = List of endpoints with appropriately configured default deny rule
- M8 = Count of M7
- M9 = List of endpoints with inappropriately configured default deny rule
- M10 = Count of M9
- M11 = List of endpoints with both appropriately configured ports and default deny rules
- M12 = Count of M11
- M13 = List of endpoints with at least one inappropriate configuration relative to ports or default deny rule
- M14 = Count of M14

16.4.5 Metrics

Metric	What is the ratio of correctly configured endpoints to the total number of endpoints?
Calculation	`M12 / M2`

16.5 12.5: Configure Monitoring Systems to Record Network Packets

Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

16.5.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 12.1: Maintain an Inventory of Network Boundaries

16.5.2 Inputs

1. List of network monitoring systems
2. List of network boundaries

16.5.3 Operations

1. **For each network monitoring system:**
    1. Retrieve configuration
    2. Check configuration for recording
    3. Enumerate network boundaries covered

16.5.4 Measures

- M1 = Count of network monitoring systems (from Input 1)
- M2 = List of misconfigured network monitoring systems
- M3 = Count of misconfigured network monitoring systems
- M4 = Count of network boundaries (from Input 2)
- M5 = List of network boundaries covered by network monitoring systems
- M6 = Count of network boundaries covered by network monitoring systems
- M7 = List of network boundaries not covered by network monitoring systems
- M8 = Count of network boundaries not covered by network monitoring systems

16.5.5 Metrics

Monitoring System Configuration

Metric	
	Percentage of appropriately configured monitoring systems
Calculation	`(M1 - M3) / M1`

Network Boundary Coverage

Metric	
	Percentage of network boundaries not covered by a monitoring system
Calculation	`(M4 - M6) / M4`

16.6 12.6: Deploy Network-Based IDS Sensors

Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

16.6.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 12.1: Maintain an Inventory of Network Boundaries

16.6.2 Inputs

1. List of network boundaries
2. List of IDS sensors

16.6.3 Operations

1. For each IDS sensor, enumerate network boundaries covered

16.6.4 Measures

- M1 = Count of network boundaries (from Input 1)
- M2 = Count of IDS sensors (from Input 2)
- M4 = List of network boundaries covered by IDS sensors

- M5 = Count of network boundaries covered by IDS sensors
- M6 = List of network boundaries not covered by IDS sensors
- M7 = Count of network boundaries not covered by IDS sensors

16.6.5 Metrics

Coverage

Metric	Ratio of network boundaries covered by IDS sensors to total number of network boundaries
Calculation	`M5 / M1`

16.7 12.7: Deploy Network-Based Intrusion Prevention Systems

Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

16.7.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 12.1: Maintain an Inventory of Network Boundaries

16.7.2 Inputs

1. The list of authorized software
2. The list of network boundaries

16.7.3 Operations

1. Enumerate all IPS systems in the software inventory
2. **For each IPS system:**
    1. Enumerate the network boundaries covered by the system
    2. Examine its configuration to ensure that the system is configured to block malicious network traffic through that boundary
3. Enumerate network boundaries covered by all IPS systems (i.e. create a set of covered network boundaries)
4. Complement the set of covered network boundaries with the list of network boundaries to identify all uncovered network boundaries

16.7.4 Measures

- M1 = List of all IPS systems
- M2 = List of network boundaries
- M3 = List of appropriately configured IPS systems
- M4 = List of inappropriately configured IPS systems
- M5 = List of network boundaries covered by at least one IPS system
- M6 = List of network boundaries not covered by at least one IPS system
- M7 = Count of IPS systems (count of M1)
- M8 = Count of network boundaries (count of M2)
- M9 = Count of appropriately configured IPS systems (count of M3)
- M10 = Count of inappropriately configured IPS systems (count of M4)
- M11 = Count of network boundaries covered by at least one IPS system (count of M5)
- M12 = Count of network boundaries not covered by at least one IPS system (count of M6)

16.7.5 Metrics

IPS Coverage

Metric	The ratio of appropriately configured IPS systems to the total number of IPS systems
Calculation	`M9 / M7`

Boundary Coverage

Metric	The ratio of covered network boundaries to the total number of network boundaries
Calculation	`M11 / M8`

16.8 12.8: Deploy NetFlow Collection on Networking Boundary Devices

Enable the collection of NetFlow and logging data on all network boundary devices.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

16.8.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 12.1: Maintain an Inventory of Network Boundaries

16.8.2 Inputs

1. List of network boundary devices (from inventory)

Assumption

- Assumes organization has positive control over inventory - explicitly ignores the case where there may be a network boundary device present and not accounted for (if other controls are working, this should not be the case).

16.8.3 Operations

1. **For each network boundary device,**
    1. Check configuration for NetFlow data (i.e. NetFlow is enabled)
    2. Check configuration for logging data (i.e. logging is enabled)

16.8.4 Measures

- M1 = Count of network boundary devices (from Input 1)
- M2 = List of network boundary devices with NetFlow enabled
- M3 = Count of M2
- M4 = List of network boundary devices without NetFlow enabled
- M5 = Count of M4
- M6 = List of network boundary devices with logging enabled
- M7 = Count of M6
- M8 = List of network boundary devices without logging enabled
- M9 = Count of M8
- M10 = List of network boundary devices with both NetFlow and logging enabled
- M11 = Count of M10
- M12 = List of network boundary devices with either NetFlow or logging disabled
- M13 = Count of M12

16.8.5 Metrics

NetFlow Coverage

Metric	Ratio of network boundary devices with appropriately configured NetFlow to the total number of network boundary devices
Calculation	`M3 / M1`

Logging Coverage

Metric	Ratio of network boundary devices with appropriately configured logging to the total number of network boundary devices
Calculation	`M7 / M1`

Total Coverage

Metric	Ratio of appropriately configured network boundary devices to the total number of network boundary devices
Calculation	`M11 / M1`

16.9 12.9: Deploy Application Layer Filtering Proxy Server

Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.

Asset Type	Security Function	Implementation Groups
Network	Detect	3

16.9.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

16.9.2 Inputs

1. The list of endpoints
2. The list of authorized software
3. The list of unauthorized connections

16.9.3 Operations

1. Enumerate network devices guarding Internet network boundaries
2. Enumerate application-layer proxies
3. **For each application-layer proxy**
    1. Enumerate the network boundary devices it covers
    2. **For each Internet network boundary device it covers**
        1. Ensure it is appropriately configured to filter against the list of unauthorized connections
4. Enumerate the set of covered Internet network boundary devices

16.9.4 Measures

- M1 = List of Internet network boundary devices
- M2 = List of application-layer proxies
- M3 = List of appropriately configured application-layer proxies
- M4 = List of inappropriately configured application-layer proxies
- M5 = List of covered Internet network boundary devices
- M6 = Count of Internet network boundary devices (count of M1)
- M7 = Count of application-layer proxies (count of M2)
- M8 = Count of appropriately configured application-layer proxies (count of M3)
- M9 = Count of inappropriately configured application-layer proxies (count of M4)
- M10 = Count of covered Internet network boundary devices (count of M5)

16.9.5 Metrics

Proxy Coverage

Metric	The ratio of appropriately configured application-layer proxies to the total number of application-layer proxies.
Calculation	`M8 / M7`

Internet Network Boundary Coverage

Metric	
	The ratio of covered Internet network boundary devices to the total number of Internet network boundary devices
Calculation	`M10 / M6`

16.10 12.10: Decrypt Network Traffic at Proxy

Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.

Asset Type	Security Function	Implementation Groups
Network	Detect	3

16.10.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

16.10.2 Inputs

1. The list of authorized software
2. The list of authorized sites not requiring decryption before analysis

16.10.3 Operations

1. Enumerate each boundary proxy system
2. **For each identified proxy system, examine its configuration as follows, noting appropriately and inappropriately configured systems:**
    1. Encrypted network traffic is decrypted prior to analysis, when traffic is not related to an authorized site
3. Enumerate the set of appropriately configured proxy systems
4. Enumerate the set of inappropriately configured proxy systems

16.10.4 Measures

- M1 = List of boundary proxy systems
- M2 = List of appropriately configured boundary proxy systems
- M3 = List of inappropriately configured boundary proxy systems
- M4 = Count of boundary proxy systems (count of M1)
- M5 = Count of appropriately configured boundary proxy systems (count of M2)
- M6 = Count of inappropriately configured boundary proxy systems (count of M3)

16.10.5 Metrics

Coverage

Metric	
	The ratio of appropriately configured boundary proxy systems to the total number of boundary proxy systems
Calculation	`M5 / M4`

16.11 12.11: Require All Remote Logins to Use Multi-Factor Authentication

Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

16.11.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

16.11.2 Inputs

1. List of authorized remote hosts

16.11.3 Operations

1. **For each host in the list of authorized remote hosts, check the remote access software configuration:**
    1. Encrypted connections are required
    2. Multi-factor authentication is required

16.11.4 Measures

- M1 = Count of authorized remote hosts (from Input 1)
- M2 = List of authorized remote hosts with encryption required
- M3 = Count of M2
- M4 = List of authorized remote hosts without encryption required
- M5 = Count of M4
- M6 = List of authorized remote hosts with multi-factor authentication required
- M7 = Count of M6
- M8 = List of authorized remote hosts without multi-factor authentication required

- M9 = Count of M8
- M10 = List of authorized remote hosts with both encryption and multi-factor authentication required
- M11 = Count of M10
- M12 = List of authorized remote hosts without either encryption or multi-factor authentication required
- M13 = Count of M12

16.11.5 Metrics

Encryption Coverage

Metric	
	Ratio of authorized remote hosts with encryption required to the total number of authorized remote hosts
Calculation	`M3 / M1`

Multi-Factor Authentication Coverage

Metric	
	Ratio of authorized remote hosts with multi-factor authentication required to the total number of authorized remote hosts
Calculation	`M7 / M1`

Total Coverage

Metric	
	Ratio of authorized remote hosts with both encryption and multi-factor authentication required to the total number of authorized remote hosts required
Calculation	`M11 / M1`

16.12 12.12: Manage All Devices Remotely Logging Into Internal Network

Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

16.12.1 Dependencies

- Sub-control 16.1: Maintain an Inventory of Authentication Systems

16.12.2 Inputs

1. List of the organization's authentication systems that allow remote logins (subset of Inventory of Authentication Systems). For each, provide the configuration location(s) for the mechanisms used to ensure remote device security policy enforcement.
2. Approved configuration(s) for each type of remote device security policy enforcement mechanism provided in Input 1

16.12.3 Operations

1. **For each authentication system in Input 1, check each of the enforcement mechanisms provided for that authentication system against the appropriate approved configuration(s) provided in Input 2.**
    1. Create a list of those authentication systems for which all of the associated enforcement mechanisms comply with the approved configuration(s) noting which configurations were checked (M1).
    2. Create a list of those authentication systems for which at least one of the associated enforcement mechanisms does not comply with the appropriate configurations, noting the configurations checked and any deviations (M2).

16.12.4 Measures

- M1 = List of authentication systems that have properly configured mechanisms in place to ensure that organizational security policies are enforced in remote devices (compliant list)
- M2 = List of authentication systems that do not have properly configured mechanisms in place to ensure that organizational security policies are enforced in remote devices (non-compliant list)
- M3 = Count of authentication systems with properly configured mechanisms in place (count of M1)
- M4 = The total number of authentication systems that allow remote connections (count of Input 1)

16.12.5 Metrics

Coverage

Metric	The ratio of authentication systems with properly configured mechanisms to ensure that organizational security policies are enforced in remote devices to the total number of authentication systems
Calculation	`M3 / M4`

CHAPTER

SEVENTEEN

CIS CONTROL 13: DATA PROTECTION

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Why is this CIS Control Critical?

Data resides in many places. Protection of that data is best achieved through the application of a combination of encryption, integrity protection, and data loss prevention techniques. As organizations continue their move towards cloud computing and mobile access, it is important that proper care be taken to limit and report on data exfiltration while also mitigating the effects of data compromise.

Some organizations do not carefully identify and separate their most sensitive and critical assets from less sensitive, publicly accessible information on their internal networks. In many environments, internal users have access to all or most of the critical assets. Sensitive assets may also include systems that provide management and control of physical systems, such as Supervisory Control and Data Acquisition (SCADA). Once attackers have penetrated such a network, they can easily find and exfiltrate important information, cause physical damage, or disrupt operations with little resistance. For example, in several high-profile breaches over the past few years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data. There are also examples of using access to the corporate network to gain access to, then control over, physical assets and cause damage.

17.1 13.1: Maintain an Inventory of Sensitive Information

Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.

Asset Type	Security Function	Implementation Groups
Data	Identify	1, 2, 3

17.1.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory

17.1.2 Inputs

1. Classification Scheme: The organizationally-defined classification scheme
2. The data set of sensitive information for which the organization is responsible, mapped to the classification scheme defined by Input 1
3. A mapping of an organization's endpoints/systems containing sensitive information classified by Input 2 (ideally using the endpoint inventory; see sub-control 1.4)

17.1.3 Operations

1. Create the mappings of information deemed "sensitive" to the organization to the organization's classification scheme.
2. Create the mappings of classified, sensitive information to the endpoints/systems on which that information is stored

17.1.4 Measures

- M1 = 1 if the mappings of "sensitive" information to the organization's classification scheme is provided; 0 otherwise
- M2 = 1 if the mappings of classified, sensitive information to the endpoints/systems on which it resides is provided; 0 otherwise

17.1.5 Metrics

Existence

Metric	
	Ensure the inventory of all sensitive information, cross-referenced with the systems on which that information is kept, exists.
Calculation	`M1 AND M2`

17.2 13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization

Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

17.2.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 13.1: Maintain an Inventory of Sensitive Information

17.2.2 Inputs

1. List of sensitive systems (ideally using the endpoint inventory; see sub-control 1.4)
2. The access frequency for any sensitive systems
3. An organizationally-defined access frequency threshold

Assumptions

- Access to sensitive data takes place through some system, therefore the system, when processing, storing, or transmitting sensitive data, is a sensitive system.
- Isolation/exposure score of zero is assumed ideal

17.2.3 Operations

1. Determine subset of sensitive systems that are infrequently used (using all Inputs)
2. For each infrequently used sensitive system, calculate isolation/exposure

17.2.4 Measures

- M1 = List of all systems used to process sensitive information
- M2 = Count of M1
- M3 = Set of infrequently used sensitive systems
- M4 = Count of infrequently used sensitive systems
- M5 = List of infrequently used sensitive systems with isolation/exposure scores greater than 0
- M6 = Count of M4

17.2.5 Metrics

Coverage

Metric	What percentage of infrequently used sensitive systems are not properly isolated?
Calculation	`M6 / M4`

17.3 13.3: Monitor and Block Unauthorized Network Traffic

Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

Asset Type	Security Function	Implementation Groups
Data	Detect	3

17.3.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 12.1: Maintain an Inventory of Network Boundaries

17.3.2 Inputs

1. The list of authorized software
2. The list of network perimeters

17.3.3 Operations

1. Enumerate all network perimeter monitoring systems
2. **For each network perimeter monitoring system:**
    1. Enumerate the network perimeters covered by the system
    2. **Examine its configuration to ensure that the system is configured to:**
        1. Monitor for sensitive information
        2. Block transfer of detected sensitive information
        3. Alert appropriately
3. Enumerate network perimeters covered by all network perimeter monitoring systems
4. Complement the set of covered network perimeters with the list of network perimeters to identify all uncovered network perimeters

Assumptions

- Network perimeter monitoring systems are primarily software-based

17.3.4 Measures

- M1 = List of network perimeter monitoring systems
- M2 = List of network perimeters
- M3 = List of appropriately configured perimeter monitoring systems
- M4 = List of inappropriately configured perimeter monitoring systems
- M5 = List of network perimeters covered by at least one network perimeter monitoring system
- M6 = List of network perimeters not covered by at least one network perimeter monitoring system
- M7 = Count of network perimeter monitoring systems (count of M1)
- M8 = Count of network perimeters (count of M2)
- M9 = Count of appropriately configured perimeter monitoring systems (count of M3)
- M10 = Count of inappropriately configured perimeter monitoring systems (count of M4)
- M11 = Count of network perimeters covered by at least one network perimeter monitoring system (count of M5)
- M12 = Count of network perimeters not covered by at least one network perimeter monitoring system (count of M6)

17.3.5 Metrics

Coverage

Metric	The ratio of covered network perimeters to the total number of network perimeters
Calculation	`M11 / M8`

Perimeter Monitoring Configuration Coverage

Metric	
	The ratio of appropriately configured network perimeter monitoring systems to the total number of network perimeter monitoring systems
Calculation	`M9 / M7`

17.4 13.4: Only Allow Access to Authorized Cloud Storage or Email Providers

Only allow access to authorized cloud storage or email providers.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

17.4.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

17.4.2 Inputs

1. List of endpoints. For each, include the configuration locations that restrict which cloud providers the endpoint can access (this could be a firewall, etc.)
2. List of cloud storage providers (this list should be as complete as possible and should indicate whether each provider is allowed or prohibited)
3. List of cloud email providers (this list should be as complete as possible and should indicate whether each provider is allowed or prohibited)
4. Organization's security policy regarding access to cloud storage and cloud email providers, including a list of which ones are allowed

17.4.3 Operations

1. For each of the endpoint configuration locations identified in Input 1, identify which of the cloud storage providers from Input 2 are reachable based on the configuration at that location, creating a list of reachable cloud storage providers by configuration location (M1). Mark each of the configuration locations in the list as either compliant (if it does not allow access to prohibited cloud storage providers), or non-compliant (if it allows access to at least one of the prohibited cloud storage providers).
2. For each of the endpoint configuration locations identified in Input 1, identify which of the cloud email providers from Input 3 are reachable based on the configuration at that location, creating a list of reachable cloud email providers by configuration location (M2). Mark each of the configuration locations in the list as either compliant (if it does not allow access to prohibited cloud storage providers), or non-compliant (if it allows access to at least one of the prohibited cloud storage providers).
3. For each endpoint in Input 1, check the status of each of that endpoint's configuration locations in M1 and M2, and create a count of the endpoints that have configuration locations that are all compliant (M3).

4. Manually review the organization's security policy provided in Input 4 to ensure that it properly outlines the organization's rules for accessing cloud storage and cloud email providers, including identifying which providers are allowed and which are prohibited. Score this review as M5 (could be a binary 1 for adequate, 0 for inadequate; or a more nuanced score could be generated).

17.4.4 Measures

- M1 = List of reachable cloud storage providers by configuration location
- M2 = List of reachable cloud email providers by configuration location
- M3 = Count of endpoints for which all their configuration locations are compliant
- M4 = Count of endpoints (count of Input 1)
- M5 = Score resulting from the manual review of the cloud provider access policy

17.4.5 Metrics

Coverage

Metric	
	Ratio of endpoints with cloud provider access properly limited to the total number of endpoints
Calculation	`M3 / M4`

Manual Review

Metric	
	Manual policy review included for this Sub-Control because it is not feasible to identify (and therefore check for) all cloud storage and email providers.
Calculation	`M5`

17.5 13.5: Monitor and Detect Any Unauthorized Use of Encryption

Monitor all traffic leaving the organization and detect any unauthorized use of encryption.

Asset Type	Security Function	Implementation Groups
Data	Detect	3

17.5.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 12.1: Maintain an Inventory of Network Boundaries

17.5.2 Inputs

1. The list of authorized software
2. The list of network boundaries at the organization's perimeter
3. Unauthorized encrypted connections

17.5.3 Operations

1. Enumerate all network monitoring systems in the software inventory
2. **For each network monitoring system**
    1. Enumerate the network boundaries covered by the system
    2. Examine its configuration to ensure that the system is configured to monitor for unauthorized encrypted connections
3. Enumerate network boundaries covered by all network monitoring systems (i.e. create a set of covered network boundaries)
4. Complement the set of covered network boundaries with the list of network boundaries to identify all uncovered network boundaries

17.5.4 Measures

- M1 = List of all network monitoring systems
- M2 = List of network boundaries at the perimeter
- M3 = List of appropriately configured network monitoring systems
- M4 = List of inappropriately configured network monitoring systems
- M5 = List of network boundaries covered by at least one network monitoring system
- M6 = List of network boundaries not covered by at least one network monitoring system
- M7 = Count of network monitoring systems (count of M1)
- M8 = Count of network boundaries at the perimeter (count of M2)
- M9 = Count of appropriately configured network monitoring systems (count of M3)
- M10 = Count of inappropriately configured network monitoring systems (count of M4)
- M11 = Count of network boundaries covered by at least one network monitoring system (count of M5)
- M12 = Count of network boundaries not covered by at least one network monitoring system (count of M6)

17.5.5 Metrics

Network Monitoring Coverage

Metric	The ratio of appropriately configured network monitoring systems to the total number of network monitoring systems
Calculation	`M9 / M7`

Network Boundary Coverage

Metric	
	The ratio of covered network boundaries to the total number of network boundaries
Calculation	`M11 / M8`

17.6 13.6: Encrypt Mobile Device Data

Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

17.6.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain an Inventory of Authorized Software
- Sub-control 5.1: Establish Secure Configurations

17.6.2 Inputs

1. The list of approved mobile devices (derived from endpoint inventory; sub-control 1.4)
2. The list of approved mobile device encryption software (ideally derived from authorized software list; sub-control 2.1)
3. For each software in Input 2, the approved software configuration policy.

17.6.3 Operations

1. For each mobile device in Input 1, determine if any of the approved encryption software from Input 2 is installed.
2. For each mobile device with installed approved encryption software, collect the software configuration information and compare it to the approved configuration policy (Input 3).

17.6.4 Measures

- M1 = List of approved mobile devices
- M2 = Count of M1
- M3 = List of approved mobile devices with approved encryption software installed
- M4 = Count of M3
- M5 = List of approved mobile devices without approved encryption software installed
- M6 = Count of M5
- M7 = List of appropriately configured mobile devices

- M8 = Count of M7
- M9 = List of inappropriately configured mobile devices
- M10 = Count of M9

17.6.5 Metrics

Installed Software Coverage

Metric	
	What percentage of approved mobile devices are equipped with approved encryption software?
Calculation	`M4 / M2`

Appropriately Configured Devices

Metric	
	What percentage of approved mobile devices equipped with approved encryption software meet or exceed the approved configuration policy?
Calculation	`M8 / M2`

17.7 13.7: Manage USB Devices

If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

17.7.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

17.7.2 Inputs

1. The list of endpoints
2. The list of authorized USB storage devices
3. Enterprise software which can configure systems to allow the use of specific devices

17.7.3 Operations

1. For each endpoint "i", determine if the software specified by Input 3 is installed (M2(i))
2. For each endpoint "i", collect the whitelist of USB devices allowed for use (M3(i))
3. For each endpoint's whitelist, calculate the intersection with the authorized USB device inventory from Input 2. The "right-side" of the calculation indicates USB devices on the endpoint's whitelist which are not contained in the authorized USB device inventory.

17.7.4 Measures

- M1 = Count of endpoints
- M2(i) = (For each endpoint "i") 1 if Operation 1 indicates the appropriate software is installed on device "i"; 0 otherwise
- M3 = (For each endpoint) The number of USB devices allowed
- M4 = (For each endpoint) The number of USB devices contained in the whitelist which are not in the authorized USB device inventory
- M5(i) = (For each endpoint "i") 1 if M4 > 0 for device "i"; 0 otherwise

17.7.5 Metrics

Whitelisting Software Coverage

Metric	The ratio of endpoints with whitelisting software installed to the total number of endpoints.
Calculation	`(SUM from i=1..M1 (M2(i))) / M1`

Non-Inventoried but Whitelisted

Metric	The ratio of endpoints with non-inventories but whitelisted USB device allowance to the total number of endpoints.
Calculation	`(SUM from i=1..M1 (M5(i))) / M1`

Full Coverage

Metric	The ratio of endpoints with inventoried USB storage device capability and USB whitelisting software installed to the total number of endpoints.
Calculation	`(SUM from i=1..M1 (M2(i) * M5(i))) / M1`

17.8 13.8: Manage System's External Removable Media's Read/Write Configurations

Configure systems not to write data to external removable media, if there is no business need for supporting such devices.

Asset Type	Security Function	Implementation Groups
Data	Protect	3

17.8.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

17.8.2 Inputs

1. The list of endpoints

17.8.3 Operations

1. Enumerate all endpoints supporting external removable media
2. Enumerate all endpoints with a business need to support external removable media
3. Enumerate all endpoints without a business need to support external removable media
4. For each endpoint without a business need to support external removable media, examine its external media configuration, noting whether it is appropriately or inappropriately configured
5. Enumerate the inappropriately configured endpoints
6. Enumerate the appropriately configured endpoints

17.8.4 Measures

- M1 = List of all endpoints supporting external removable media
- M2 = List of all endpoints with a business need to support external removable media
- M3 = List of all endpoints without a business need to support external removable media
- M4 = List of appropriately configured endpoints without a need to support external removable media
- M5 = List of inappropriately configured endpoints without a need to support external removable media
- M6 = Count of endpoints supporting external removable media (count of M1)
- M7 = Count of endpoints with a business need to support external removable media (count of M2)
- M8 = Count of endpoints without a business need to support external removable media (count of M3)
- M9 = Count of appropriately configured endpoints without a need to support external removable media (count of M4)
- M10 = Count of inappropriately configured endpoints without a need to support external removable media (count of M5)

17.8.5 Metrics

Coverage

Metric	
	The ratio of appropriately configured endpoints to the total number of endpoints without a business need to support external removable media
Calculation	`M9 / M8`

17.9 13.9: Encrypt Data on USB Storage Devices

If USB storage devices are required, all data stored on such devices must be encrypted while at rest.

Asset Type	Security Function	Implementation Groups
Data	Protect	3

17.9.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

17.9.2 Inputs

1. The list of endpoints

Assumptions

- Asset inventory includes USB storage devices.

17.9.3 Operations

1. Enumerate all endpoints capable of supporting USB storage devices
2. **For each identified endpoint**
    1. Examine the endpoint's configuration to determine its USB storage device encryption configuration, noting along the way those that are appropriately and inappropriately configured

17.9.4 Measures

- M1 = List of endpoints capable of supporting USB storage devices
- M2 = List of endpoints appropriately configured
- M3 = List of endpoints inappropriately configured
- M4 = Count of endpoints capable of supporting USB storage devices (count of M1)
- M5 = Count of endpoints appropriately configured (count of M2)
- M6 = Count of endpoints inappropriately configured (count of M3)

17.9.5 Metrics

Coverage

Metric	
	The ratio of appropriately configured endpoints to the total number of endpoints supporting USB storage devices
Calculation	`M5 / M4`

CHAPTER

EIGHTEEN

CIS CONTROL 14: CONTROLLED ACCESS BASED ON THE NEED TO KNOW

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Why is this CIS Control Critical?

Encrypting data provides a level of assurance that even if data is compromised, it is impractical to access the plaintext without significant resources; however, controls should also be put in place to mitigate the threat of data exfiltration in the first place. Many attacks occurred across the network, while others involved physical theft of laptops and other equipment holding sensitive information. Yet, in many cases, the victims were not aware that the sensitive data were leaving their systems because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

The loss of control over protected or sensitive data by organizations is a serious threat to business operations and a potential threat to national security. While some data are leaked or lost as a result of theft or espionage, the vast majority of these problems result from poorly understood data practices, a lack of effective policy architectures, and user error. Data loss can even occur as a result of legitimate activities such as e-Discovery during litigation, particularly when records retention practices are ineffective or nonexistent.

The adoption of data encryption, both in transit and at rest, provides mitigation against data compromise. This is true if proper care has been taken in the processes and technologies associated with the encryption operations. An example of this is the management of cryptographic keys used by the various algorithms that protect data. The process for generation, use, and destruction of keys should be based on proven processes as defined in standards such as NIST SP 800-57.

Care should also be taken to ensure that products used within an enterprise implement well known and vetted cryptographic algorithms, as identified by NIST. Re-evaluation of the algorithms and key sizes used within the enterprise on an annual basis is also recommended to ensure that organizations are not falling behind in the strength of protection applied to their data.

For organizations that are moving data to the cloud, it is important to understand the security controls applied to data in the cloud multi-tenant environment, and determine the best course of action for application of encryption controls and security of keys. When possible, keys should be stored within secure containers such as Hardware Security Modules (HSMs).

Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance.

18.1 14.1: Segment the Network Based on Sensitivity

Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

18.1.1 Dependencies

- Sub-control 13.1: Maintain an Inventory of Sensitive Information

18.1.2 Inputs

1. Sensitive Information Inventory including which systems store, process, or transmit that sensitive information.
2. Network Architecture information outlining network separation including VLANs

Assumption

- A system's overall sensitivity level shall be the highest sensitivity level of the data it stores/processes/transmits. If a system contains any sensitive information, that system should be treated accordingly, and should be properly separated from networks or network segments that don't have a need to access that type of sensitive information.

18.1.3 Operations

1. For each system that stores, processes, or transmits sensitive information identified in Input 1, use the information in Input 2 to identify any networks/VLANs the system is connected to and ensure that each of those networks/VLANs are adequately separated from less sensitive networks (note: this might be a manual review).
2. Use these results to create a list of systems that are adequately separated from less sensitive networks (M1)
3. Use these results to create a list of systems that are not adequately separated (M2) noting the less sensitive networks that they are connected to.

18.1.4 Measures

- M1 = List of sensitive systems that are adequately separated from less sensitive networks (compliant list)
- M2 = List of sensitive systems that are not adequately separated from less sensitive networks (non-compliant list)
- M3 = Count of sensitive systems that are adequately separated from less sensitive networks (count of M1)
- M4 = Total count of sensitive systems (count of Input 1)

18.1.5 Metrics

Coverage

Metric	
	The ratio of adequately separated sensitive systems to the total number of sensitive systems.
Calculation	`M3 / M4`

18.2 14.2: Enable Firewall Filtering Between VLANs

Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

18.2.1 Dependencies

- None

18.2.2 Inputs

1. List of the organization's VLANs, along with the systems (network devices, etc.) associated with administering, configuring, and filtering between them
2. Approved configuration(s) for these VLANs and related systems to enable firewall filtering between VLANs

18.2.3 Operations

1. For each VLAN in Input 1, check each of its related systems to see if they are configured in accordance with the appropriate approved configurations from Input 2 to enable firewall filtering between VLANs.
2. Create a list of VLANs that are correctly configured (M1)
3. Create a list of VLANs that are not correctly configured (M2) noting which related systems are misconfigured and the details of the misconfiguration.

18.2.4 Measures

- M1 = List of correctly configured VLANs (compliant list)
- M2 = List of incorrectly configured VLANs along with deviations (non-compliant list)
- M3 = Count of correctly configured VLANs (count of M1)
- M4 = Total count of VLANs (count of Input 1)

18.2.5 Metrics

Coverage

Metric	
	The ratio of VLANs properly configured for firewall filtering to the total number of VLANs.
Calculation	`M3 / M4`

18.3 14.3: Disable Workstation-to-Workstation Communication

Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as private VLANs or micro segmentation.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

18.3.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

18.3.2 Inputs

1. The list of endpoints. For each endpoint, include the corresponding policy configuration locations that are used to restrict workstation to workstation communication (network device configurations, workstation configurations, virtual network configurations, etc.)
2. Approved configuration(s) for each type of configuration in Input 1

18.3.3 Operations

1. For each endpoint, check each corresponding policy configuration location specified in Input 1, comparing the configuration at that location against the appropriate configurations provided in Input 2.
2. Create a list of endpoints for which all of the endpoint's corresponding policy configuration points are configured in accordance with the approved configurations (M1), noting the approved configurations that were used for each.
3. Create a list of the endpoints that have at least one policy configuration points that is not configured appropriately (M2) noting the deviations from the approved configurations.

18.3.4 Measures

- M1 = List of endpoints with all workstation to workstation policy configuration points configured appropriately (compliant list)
- M2 = List of endpoints with at least one misconfigured workstation to workstation policy configuration point (non-compliant list)
- M3 = Count of endpoints with all policy configuration points configured appropriately (count of M1)
- M4 = Total count of endpoints (count of Input 1)

18.3.5 Metrics

Coverage

Metric	
	The ratio of endpoints correctly configured to restrict workstation to workstation communication to the total number of endpoints.
Calculation	`M3 / M4`

18.4 14.4: Encrypt All Sensitive Information in Transit

Encrypt all sensitive information in transit.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

18.4.1 Dependencies

- Sub-control 13.1: Maintain an Inventory of Sensitive Information

18.4.2 Inputs

1. Inventory of Sensitive Information (for each type of information listed in the inventory, include a description of how the encryption of this information in transit is accomplished, along with a list of the components used to achieve that encryption)
2. Approved configuration(s) for each of the components identified in Input 1

18.4.3 Operations

1. For each type of sensitive information listed in the inventory provided in Input 1, check each of the components used to encrypt that information in transit against the appropriate approved configuration(s) in Input 2.
2. Create a list of the sensitive information types for which all of the associated components are properly configured (M1) noting which configurations they were checked against.
3. Create a list of sensitive information types for which at least one of the associated components was not properly configured (M2) noting which configurations they were checked against and any deviations from the approved configurations.

18.4.4 Measures

- M1 = List of sensitive information types for which all associated components were properly configured (compliant list)
- M2 = List of sensitive information types for which at least one associated component was not properly configured (non-compliant list)
- M3 = Count of compliant sensitive information types (count of M1)
- M4 = Total count of sensitive information types (count of Input 1)

18.4.5 Metrics

Coverage

Metric	
	The ratio of sensitive information types properly configured to be encrypted in transit to the total set of sensitive information types.
Calculation	`M3 / M4`

18.5 14.5: Utilize an Active Discovery Tool to Identify Sensitive Data

Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.

Asset Type	Security Function	Implementation Groups
Data	Detect	3

18.5.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

18.5.2 Inputs

1. The list of endpoints
2. The list of authorized software
3. The inventory of sensitive data

18.5.3 Operations

1. Using the sensitive data inventory, enumerate all endpoints storing, processing, or transmitting sensitive information.
2. Enumerate all sensitive information active monitoring tools from the software inventory
3. **For each identified active monitoring tool:**
    1. Enumerate the endpoints covered by the system
    2. **Examine its configuration to ensure that the system is configured to:**
        1. Monitor for sensitive information (noting appropriately and inappropriately configured systems along the way)
4. Enumerate endpoints covered by all sensitive information active monitoring systems
5. Complement the set of covered endpoints with the list of identified endpoints to identify all uncovered endpoints

Assumptions

- Sensitive information monitoring systems are primarily software-based

18.5.4 Measures

- M1 = List of endpoints storing, processing, or transmitting sensitive information
- M2 = List of sensitive information monitoring tools
- M3 = List of monitoring tools appropriately configured
- M4 = List of monitoring tools inappropriately configured
- M5 = List of endpoints covered by at least one monitoring tool
- M6 = List of endpoints not covered by at least one monitoring tool
- M7 = Count of endpoints storing, processing, or transmitting sensitive information (count of M1)
- M8 = Count of sensitive information monitoring tools (count of M2)
- M9 = Count of monitoring tools appropriately configured (count of M3)
- M10 = Count of monitoring tools inappropriately configured (count of M4)
- M11 = Count of endpoints covered by at least one monitoring tool (count of M5)
- M12 = Count of endpoints not covered by at least one monitoring tool (count of M6)

18.5.5 Metrics

Endpoint Coverage

Metric	The ratio of covered endpoints to the total number of endpoints storing, processing, or transmitting sensitive information
Calculation	`M11 / M7`

Monitoring Coverage

Metric	The ratio of appropriately configured active sensitive information monitoring tools to the total number of active sensitive information monitoring tools
Calculation	`M9 / M8`

18.6 14.6: Protect Information Through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

18.6.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

18.6.2 Inputs

1. Endpoint Inventory
2. Access control configuration policy

18.6.3 Operations

1. For each endpoint in Input 1, collect the "ground truth" access policy for that endpoint and compare it to the access control configuration policy in Input 2. Generate a list of endpoints which comply with the specified access control configuration policy (M1) and a list of endpoints that do not comply with the specified policy (M2)

18.6.4 Measures

- M1 = List of endpoints that comply with access control configuration policy (compliant list)
- M2 = List of endpoints that do not comply with access control configuration policy (non-compliant list)
- M3 = Count of endpoints in M1 (number of compliant endpoints)
- M4 = Count of endpoints in M2 (number of non-compliant endpoints)
- M5 = Count of endpoints in Input 1 (total number of endpoints to check)

18.6.5 Metrics

Coverage

Metric	What is the percentage of endpoints which are compliant with the organization's access control policy?
Calculation	`M3 / M5`

18.7 14.7: Enforce Access Control to Data Through Automated Tools

Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when the data is copied off a system.

Asset Type	Security Function	Implementation Groups
Data	Protect	3

18.7.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

18.7.2 Inputs

1. The list of endpoints
2. The list of authorized software

18.7.3 Operations

1. Enumerate endpoints capable of storing data
2. Enumerate all DLP software
3. **For each instance of DLP software:**
    1. Enumerate the endpoints covered by the DLP software
4. Enumerate all endpoints covered by the set of DLP software
5. Complement the list of covered endpoints with the list of endpoints enumerated in the first operation to get the enumeration of endpoints not covered

18.7.4 Measures

- M1 = List of endpoints capable of storing data
- M2 = List of DLP software instances
- M3 = List of all endpoints covered by the set of DLP software
- M4 = List of all endpoints not covered by the set of DLP software
- M5 = Count of endpoints capable of storing data (count of M1)
- M6 = Count of DLP software instances (count of M2)
- M7 = Count of endpoints covered by the set of DLP software (count of M3)
- M8 = Count of endpoints not covered by the set of DLP software (count of M4)

18.7.5 Metrics

Coverage

Metric	
	The ratio of endpoints covered by at least one DLP software instance to the total number of endpoints capable of storing data
Calculation	`M7 / M5`

18.8 14.8: Encrypt Sensitive Information at Rest

Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.

Asset Type	Security Function	Implementation Groups
Data	Protect	3

18.8.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

18.8.2 Inputs

1. The list of endpoints
2. The list of authorized software
3. The list of sensitive information

18.8.3 Operations

1. Enumerate all encryption tools requiring secondary authentication systems from the software inventory
2. Enumerate all endpoints storing sensitive information using the sensitive information inventory
3. **For each identified encryption tool**
    1. Enumerate endpoints covered by the encryption tool
4. Enumerate all endpoints covered by at least one encryption tool
5. Complement all covered endpoints with the enumeration of all endpoints storing sensitive information to find those endpoints not covered by at least one encryption tool

18.8.4 Measures

- M1 = List of all encryption tools that require secondary authentication
- M2 = List of all endpoints storing sensitive information
- M3 = List of all endpoints covered by at least one encryption tool

- M4 = List of all endpoints not covered by at least one encryption tool
- M5 = Count of encryption tools that require secondary authentication (count of M1)
- M6 = Count of endpoints storing sensitive information (count of M2)
- M7 = Count of endpoints covered by at least one encryption tool (count of M3)
- M8 = Count of endpoints not covered by at least one encryption tool (count of M4)

18.8.5 Metrics

Coverage

Metric	
	The ratio of endpoints covered by an encryption tool to the total number of endpoints storing sensitive information
Calculation	`M7 / M6`

18.9 14.9: Enforce Detail Logging for Access or Changes to Sensitive Data

Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

Asset Type	Security Function	Implementation Groups
Data	Detect	3

18.9.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

18.9.2 Inputs

1. The list of endpoints
2. The list of authorized software
3. The list of sensitive information

18.9.3 Operations

1. Enumerate all endpoints storing sensitive information using the endpoint inventory and the sensitive information inventory
2. **For each identified endpoint, examine its configuration as follows noting appropriately and inappropriately configured endpoints along the way:**

    1. Detailed audit logging is enabled for access to sensitive data
    2. Detailed audit logging is enabled for changes to sensitive data
3. Enumerate appropriately configured endpoints
4. Enumerate inappropriately configured endpoints
5. Enumerate endpoints inappropriately configured to log access to sensitive data
6. Enumerate endpoints inappropriately configured to log changes to sensitive data

18.9.4 Measures

- M1 = List of all endpoints storing sensitive information
- M2 = List of appropriately configured endpoints (those that have detailed audit logging enabled for access and changes to sensitive data)
- M3 = List of inappropriately configured endpoints (those that do not have detailed audit logging enabled for access or changes to sensitive data)
- M4 = List of endpoints inappropriately configured to log access to sensitive data
- M5 = List of endpoints inappropriately configured to log changes to sensitive data
- M6 = Count of endpoints storing sensitive information (count of M1)
- M7 = Count of appropriately configured endpoints (count of M2)
- M8 = Count of inappropriately configured endpoints (count of M3)
- M9 = Count of endpoints inappropriately configured to log access to sensitive data (count of M4)
- M10 = Count of endpoints inappropriately configured to log changes to sensitive data (count of M5)

18.9.5 Metrics

Coverage

Metric	The ratio of appropriately configured endpoints to the total number of endpoints storing sensitive information
Calculation	`M7 / M6`

CHAPTER

NINETEEN

CIS CONTROL 15: WIRELESS ACCESS CONTROL

The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

Why is this CIS Control Critical?

Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying travelers are infected on a regular basis through remote exploitation while on public wireless networks found in airports and cafes. Such exploited systems are then used as backdoors when they are reconnected to the network of a target organization. Other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target environment.

19.1 15.1: Maintain an Inventory of Authorized Wireless Access Points

Maintain an inventory of authorized wireless access points connected to the wired network.

Asset Type	Security Function	Implementation Groups
Network	Identify	2, 3

19.1.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

19.1.2 Inputs

1. The list of wireless access points

19.1.3 Operations

1. Utilize a discovery tool or process to examine the network topology to collect the "ground truth" list of wireless access points connected to the wired network.
2. Evaluate the complement of Input 1 and Operation 1 to obtain the list of non-inventoried wireless access points.
3. Evaluate the intersection of Input 1 and Operation 1 to obtain the list of inventoried wireless access points.

4. Compare the results of Operation 3 to the inventory to determine which access points in the inventory are noted as *not* authorized.

19.1.4 Measures

- M1 = Count of wireless access points in the inventory (from Input 1)
- M2 = List of discovered wireless access points, from Operation 1
- M3 = Count of M2
- M4 = List of non-inventoried wireless access points, as discovered by Operation 2
- M5 = Count of M4
- M6 = List of inventoried wireless access points, as discovered by Operation 3
- M7 = Count of M6
- M8 = List of discovered, but unauthorized, wireless access points, as discovered by Operation 4
- M9 = Count of M8

19.1.5 Metrics

Coverage

Metric	The ratio of discovered wireless access points to the total inventoried list of wireless access points.
Calculation	`(M3 - M1) / M1`

Inventory Gap

Metric	Are there any discovered wireless access points that are *not* contained in the inventory?
Calculation	`M5 > 0`

Unauthorized Usage

Metric	Are there any discovered wireless access points which are contained in the inventory but are noted as *not* authorized?
Calculation	`M9 > 0`

19.2 15.2: Detect Wireless Access Points Connected to the Wired Network

Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

19.2.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

19.2.2 Inputs

1. The list of network vulnerability scanning tools
2. Approved configuration(s) for detecting unauthorized wireless access points (WAPs)
3. Approved configuration(s) for alerting on unauthorized wireless access points (WAPs)

19.2.3 Operations

1. For each network vulnerability scanning tool in Input 1, check its configuration against the appropriate approved detection configuration in Input 2.
2. Make a list of those network vulnerability scanning tools that are configured correctly for detecting unauthorized WAPs (M1)
3. Make a list of those that are not configured correctly (M2) noting the deviations.
4. For each network vulnerability scanning tool in Input 1, check its configuration against the appropriate approved alerting configuration in Input 3.
5. Make a list of those network vulnerability scanning tools that are configured correctly for alerting on unauthorized WAPs (M3)
6. Make a list of those that are not configured correctly (M4) noting the deviations.

19.2.4 Measures

- M1 = List of network vulnerability scanning tools correctly configured for detecting unauthorized WAPs
- M2 = List of network vulnerability scanning tools not correctly configured for detecting unauthorized WAPs
- M3 = List of network vulnerability scanning tools correctly configured for alerting on unauthorized WAPs
- M4 = List of network vulnerability scanning tools not correctly configured for alerting on unauthorized WAPs
- M5 = Count of network vulnerability scanning tools correctly configured for detecting unauthorized WAPs (count of M1)
- M6 = Count of network vulnerability scanning tools correctly configured for alerting on unauthorized WAPs (count of M3)
- M7 = Total count of network vulnerability scanning tools (count of Input 1)
- M8 = List of network vulnerability scanning tools correctly configured for both detecting and alerting on unauthorized WAPs (intersection of M1 and M3)

- M9 = Count of network vulnerability scanning tools correctly configured for both detecting and alerting on unauthorized WAPs (count of M8)

19.2.5 Metrics

Detection Coverage

Metric	
	The ratio of network vulnerability scanning tools correctly configured for detecting unauthorized WAPs
Calculation	`M5 / M7`

Alerting Coverage

Metric	
	The ratio of network vulnerability scanning tools correctly configured for alerting on unauthorized WAPs
Calculation	`M6 / M7`

Full Coverage

Metric	
	The ratio of network vulnerability scanning tools correctly configured for both detecting and alerting on unauthorized WAPs
Calculation	`M9 / M7`

19.3 15.3: Use a Wireless Intrusion Detection System

Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

19.3.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

19.3.2 Inputs

1. The list of approved wireless access points connected to the network
2. The list of WIDS sensors

19.3.3 Operations

1. For each WIDS sensor, enumerate the approved wireless access points covered

19.3.4 Measures

- M1 - Count of approved wireless access points (from Input 1)
- M2 - Count of WIDS sensors (from Input 2)
- M3 = List of approved wireless access points covered by WIDS sensors
- M4 = Count of M3
- M5 = List of approved wireless access points not covered by WIDS sensors
- M6 = Count of M5

19.3.5 Metrics

Coverage

Metric	Ratio of wireless access points covered by WIDS sensors to the total number of wireless access points
Calculation	`M4 / M1`

19.4 15.4: Disable Wireless Access on Devices if Not Required

Disable wireless access on devices that do not have a business purpose for wireless access.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

19.4.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

19.4.2 Inputs

1. The list of endpoints

19.4.3 Operations

1. Enumerate all wireless-access-capable endpoints
2. **For each identified endpoint:**
    1. Determine whether the device has an identified business purpose for wireless access
    2. Examine the endpoint's configuration to determine whether wireless access is enabled
3. Enumerate all endpoints with wireless access enabled and without an identified business purpose for wireless access
4. Enumerate all endpoints without wireless access enabled and without an identified business purpose for wireless access
5. Enumerate all endpoints with wireless access enabled and with an identified business purpose for wireless access

19.4.4 Measures

- M1 = List of all wireless-access-capable endpoints
- M2 = List of endpoints with wireless access enabled and without an identified business purpose for wireless access
- M3 = List of endpoints without wireless access enabled and without an identified business purpose
- M4 = List of endpoints with wireless access enabled and with an identified business purpose for wireless access
- M5 = Count of wireless-access-capable endpoints (count of M1)
- M6 = Count of endpoints with wireless access enabled and without an identified business purpose for wireless access (count of M2)
- M7 = Count of endpoints without wireless access enabled and without an identified business purpose (count of M3)
- M8 = Count of endpoints with wireless access enabled and with an identified business purpose for wireless access (count of M4)
- M9 = M7 + M8

19.4.5 Metrics

Coverage

Metric	The ratio of appropriately configured wireless-access-capable endpoints to the total number of wireless-access-capable endpoints
Calculation	`M9 / M5`

19.5 15.5: Limit Wireless Access on Client Devices

Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

19.5.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

19.5.2 Inputs

1. The list of endpoints
2. The list of authorized wireless networks

19.5.3 Operations

1. Enumerate wireless-client-capable endpoints
2. Enumerate authorized wireless networks
3. **For each identified endpoint:**
    1. Determine whether the endpoint is identified as having a business purpose for wireless access
    2. **Examine the endpoint's configuration as follows:**
        1. Access is only allowed to authorized wireless networks
        2. Access to any other wireless network is restricted
4. Enumerate all endpoints having a business purpose for wireless access
5. Enumerate all appropriately configured endpoints
6. Enumerate all inappropriately configured endpoints

19.5.4 Measures

- M1 = List of wireless-client-capable endpoints
- M2 = List of authorized wireless networks
- M3 = List of endpoints authorized for wireless access
- M4 = List of appropriately configured endpoints
- M5 = List of inappropriately configured endpoints
- M6 = Count of wireless-client-capable endpoints (count of M1)
- M7 = Count of authorized wireless networks (count of M2)
- M8 = Count of endpoints authorized for wireless access (count of M3)
- M9 = Count of appropriately configured endpoints (count of M4)
- M10 = Count of inappropriately configured endpoints (count of M5)

19.5.5 Metrics

Configuration Coverage

Metric	
	The ratio of appropriately configured endpoints to the total number of authorized wireless-client-capable endpoints
Calculation	`M9 / M8`

Authorization Coverage

Metric	
	The ratio of authorized wireless-client-capable endpoints to the total number of wireless-client-capable endpoints
Calculation	`M8 / M6`

19.6 15.6: Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients

Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

19.6.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

19.6.2 Inputs

1. The list of wireless clients (subset of hardware inventory)
2. Approved configurations to disable peer-to-peer (adhoc) wireless network capabilities

19.6.3 Operations

1. For each wireless client in Input 1, compare its configuration against the appropriate approved configuration(s) from Input 2.
2. Make a list of wireless clients that adhere to the approved configurations (M1)
3. Make a list of wireless clients that do not (M2), noting the deviations from the approved configurations.

19.6.4 Measures

- M1 = List of wireless clients properly configured to disable peer-to-peer (adhoc) wireless network capabilities (compliant list)
- M2 = List of wireless clients not properly configured to disable peer-to-peer (adhoc) wireless network capabilities (non-compliant list)
- M3 = Count of wireless clients with peer-to peer (adhoc) wireless network capabilities disabled (count of M1)
- M4 = Total count of wireless clients (count of Input 1)

19.6.5 Metrics

Coverage

Metric	
	The ratio of wireless clients with peer-to-peer (adhoc) wireless network capabilities disabled
Calculation	`M3 / M4`

19.7 15.7: Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.

Asset Type	Security Function	Implementation Groups
Network	Protect	1, 2, 3

19.7.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

19.7.2 Inputs

1. List of wireless devices (derived from Endpoint Inventory; sub-control 1.4)
2. List of AES-capable wireless devices (sub-control 1.5)

19.7.3 Operations

1. For each AES-capable wireless device, collect cipher suite configuration

19.7.4 Measures

- M1 = List of wireless devices
- M2 = Count of wireless devices
- M3 = List of AES-capable wireless devices

- M4 = Count of AES-capable wireless devices
- M5 = List of non-AES-capable wireless devices
- M6 = Count of non-AES-capable wireless devices
- M7 = List of appropriately configured AES-capable wireless devices
- M8 = Count of appropriately configured AES-capable wireless devices
- M9 = List of inappropriately configured AES-capable wireless devices
- M10 = Count of inappropriately configured AES-capable wireless devices

19.7.5 Metrics

Coverage

Metric	What percentage of AES-capable devices are configured to use cipher suites leveraging AES?
Calculation	`M8 / M4`

19.8 15.8: Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication

Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

19.8.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

19.8.2 Inputs

1. The list of endpoints
2. The list of authorized authentication protocols

19.8.3 Operations

1. Enumerate all wireless access points
2. **For each identified wireless access point, examine its configuration for the following noting appropriately and inappropriately configured endpoints along the way:**
    1. Configured authentication protocol (compare to list of authorized authentication protocols)
3. Enumerate all appropriately configured endpoints
4. Enumerate all inappropriately configured endpoints

19.8.4 Measures

- M1 = List of all wireless access points
- M2 = List of appropriately configured wireless access points
- M3 = List of inappropriately configured wireless access points
- M4 = Count of wireless access points (count of M1)
- M5 = Count of appropriately configured wireless access points (count of M2)
- M6 = Count of inappropriately configured wireless access points (count of M3)

19.8.5 Metrics

Coverage

Metric	
	The ratio of appropriately configured wireless access points to the total number of wireless access points
Calculation	`M5 / M4`

19.9 15.9: Disable Wireless Peripheral Access to Devices

Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

19.9.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

19.9.2 Inputs

1. The list of devices capable of wireless peripheral access including Bluetooth and NFC (subset of hardware inventory)
2. Approved configuration(s) to disable wireless peripheral access
3. The list of devices with an approved business purpose to have wireless peripheral access enabled, along with which form(s) of wireless peripheral access are approved (Bluetooth, NFC, etc.)

19.9.3 Operations

1. For each device in Input 1, check to see if that device adheres to the appropriate configuration(s) from Input 2 to disable wireless peripheral access, excluding any form(s) of wireless peripheral access that the device is approved to have enabled according to Input 3.

2. Create a list of devices that are properly configured (M1)
3. Create a list of devices that are not properly configured (M2) noting the deviations from approved configuration.

19.9.4 Measures

- M1 = List of devices that are properly configured to disable wireless peripheral access (compliant list)
- M2 = List of devices that are not properly configured to disable wireless peripheral access (non-compliant list)
- M3 = Count of devices that are properly configured to disable wireless peripheral access (count of M1)
- M4 = Total count of devices capable of wireless peripheral access including Bluetooth and NFC (count of Input 1)

19.9.5 Metrics

Coverage

Metric	
	The ratio of devices properly configured to disable wireless peripheral access
Calculation	`M3 / M4`

19.10 15.10: Create Separate Wireless Network for Personal and Untrusted Devices

Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.

Asset Type	Security Function	Implementation Groups
Network	Protect	1, 2, 3

19.10.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

19.10.2 Inputs

1. Isolated wireless network SSID(s)
2. List of corporate wireless network SSID(s)

19.10.3 Operations

1. For each corporate wireless network SSID, attempt to connect non-corporate device (M2)
2. Determine access policy for other wireless network

19.10.4 Measures

- M1 = 1 if the separate wireless network exists for personal/non-corporate devices; 0 otherwise.
- M2 = List of corporate wireless network SSID(s) accepting non-corporate devices
- M3 = Count of M2
- M4 = List of corporate wireless network SSID(s)
- M5 = Count of M4

19.10.5 Metrics

Logical Isolation

The overall measure fails if there is no separate network for personal/non-corporate devices (M1 = 0)

Coverage

Metric	What percentage of the total number of wireless networks exist but are misconfigured?
Calculation	`M3 / M5`

CHAPTER

TWENTY

CIS CONTROL 16: ACCOUNT MONITORING AND CONTROL

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Why is this CIS Control Critical?

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for security personnel watchers. Accounts of contractors and employees who have been terminated and accounts formerly set up for Red Team testing (but not deleted afterwards) have often been misused in this way. Additionally, some malicious insiders or former employees have gained access to accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system, and sensitive data for unauthorized and sometimes malicious purposes.

20.1 16.1: Maintain an Inventory of Authentication Systems

Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.

Asset Type	Security Function	Implementation Groups
Users	Identify	2, 3

20.1.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software

20.1.2 Inputs

1. Inventory of the organization's authentication systems (including onsite and remote)

20.1.3 Operations

1. Verify that the inventory of authentication systems (Input 1) was provided. The presence or absence of this list will be indicated with M1.
2. (Optional) Manually review Input 1 to ensure that it includes all of the authentication systems utilized by the organization, including those located onsite and by remote service providers (for instance, be sure authentication systems for any cloud services used by the organization are included). An optional manual score can be generated from this review and provided as M2.

20.1.4 Measures

- M1 = 1 if the inventory was provided, 0 if it was not provided
- M2 = (Optional) Indicates manual review of the authentication systems inventory was performed; 0 otherwise

20.1.5 Metrics

Existence

Metric	Does the organization's authentication systems inventory exist?
Calculation	`M1`

Manual Review

Metric	Was a manual review of the organization's systems inventory performed?
Calculation	`M2`

20.2 16.2: Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

20.2.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

20.2.2 Inputs

1. The list of endpoints

20.2.3 Operations

1. Enumerate centralized authentication points in inventory
2. For each identified centralized authentication point to determine necessity (i.e. can a given authentication system be consolidated with another?)
3. Enumerate the list of unnecessary centralized authentication points

20.2.4 Measures

- M1 = List of centralized authentication points in inventory
- M2 = List of unnecessary centralized authentication points
- M3 = Count of centralized authentication points in the inventory (The count of M1)
- M4 = Count of unnecessary centralized authentication points (The count of M2)
- M5 = M3 - M4 (the target number of centralized authentication points)

20.2.5 Metrics

Coverage

Metric	
	The ratio of desired centralized authentication points to actual authentication points, where the goal is for M5 / M3 = 1.
Calculation	`M5 / M3`

20.3 16.3: Require Multi-Factor Authentication

Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

20.3.1 Dependencies

- Sub-control 16.6: Maintain an Inventory of Accounts

20.3.2 Inputs

1. Account inventory organized by authentication system (from Sub-Control 16.6)
2. Approved configuration(s) to require multi-factor authentication (MFA). This will likely be a configuration for each type of authentication system in use

20.3.3 Operations

1. For each account in the account inventory (Input 1), check to see if that account is configured to require MFA in accordance with the appropriate approved configuration(s) from Input 2.
2. Create a list of accounts that are properly configured to require MFA (M1)
3. Create a list of accounts that are not properly configured to require MFA (M2) noting the deviations from the approved configuration.

20.3.4 Measures

- M1 = List of accounts that are properly configured to require MFA (compliant list)
- M2 = List of accounts that are not properly configured to require MFA (non-compliant list)
- M3 = Count of accounts properly configured to require MFA (count of M1)
- M4 = Total number of accounts (count of Input 1)

20.3.5 Metrics

Metric	
	The ratio of accounts that are properly configured to require MFA to the total number of accounts.
Calculation	`M3 / M4`

20.4 16.4: Encrypt or Hash All Authentication Credentials

Encrypt or hash with a salt all authentication credentials when stored.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

20.4.1 Dependencies

- Sub-control 16.1: Inventory of Authentication Systems

20.4.2 Inputs

1. Inventory of Authentication Systems (for each, include any related components used for credential storage for that authentication system such as any databases that require configuration independent of the authentication system)
2. Approved configuration(s) to ensure that all credentials are encrypted and/or hashed with a salt when stored. There may be multiple configurations to handle the different types of authentication systems used in the organization, and configurations may also be required for related components involved in storing this data (i.e. database configurations).

20.4.3 Operations

1. For each authentication system provided in Input 1 (along with any listed related components), check to see if it is configured properly according to the appropriate configuration(s) provided in Input 2.
2. Create a list of the authentication systems that are properly configured (M1)
3. Create a list of the authentication systems that are not properly configured (M2) including the deviations from proper configuration (if any related component identified in Input 1 is not configured according to the appropriate configuration, then its associated authentication system should be considered improperly configured, and the specific component should be noted as part of the deviation from proper configuration).

20.4.4 Measures

- M1 = List of properly configured authentication systems (compliant list)
- M2 = List of improperly configured authentication systems (non-compliant list)
- M3 = Count of properly configured authentication systems (count of M1)
- M4 = Total count of authentication systems (count of Input 1)

20.4.5 Metrics

Coverage

Metric	
	The ratio of properly configured authentication systems to the total number of authentication systems.
Calculation	`M3 / M4`

20.5 16.5: Encrypt Transmittal of Username and Authentication Credentials

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

20.5.1 Dependencies

- Sub-control 16.1: Inventory of Authentication Systems

20.5.2 Inputs

1. Inventory of Authentication Systems (for each, include any related components used by that authentication system to transmit credential information over the network)
2. Approved configuration(s) to ensure that all credentials are transmitted over encrypted channels. There may be multiple configurations to handle the different types of authentication systems used in the organization, and configurations may also be required for related components involved in transmitting this data (i.e. VPNs).

20.5.3 Operations

1. For each authentication system provided in Input 1 (along with any listed related components), check to see if it is configured properly according to the appropriate configuration(s) provided in Input 2.
2. Create a list of the authentication systems that are properly configured (M1)
3. Create a list of the authentication systems that are not properly configured (M2) including the deviations from proper configuration (if any related component identified in Input 1 is not configured according to the appropriate configuration, then its associated authentication system should be considered improperly configured, and the specific component should be noted as part of the deviation from proper configuration).

20.5.4 Measures

- M1 = List of properly configured authentication systems (compliant list)
- M2 = List of improperly configured authentication systems (non-compliant list)
- M3 = Count of properly configured authentication systems (count of M1)
- M4 = Total count of authentication systems (count of Input 1)

20.5.5 Metrics

Coverage

Metric	
	The ratio of properly configured authentication systems to the total number of authentication systems
Calculation	`M3 / M4`

20.6 16.6: Maintain an Inventory of Accounts

Maintain an inventory of all accounts organized by authentication system.

Asset Type	Security Function	Implementation Groups
Users	Identify	2, 3

20.6.1 Dependencies

- Sub-control 16.1: Inventory of Authentication Systems

20.6.2 Inputs

1. Authentication System Inventory
2. The organization's current account inventory (the "to be checked" inventory)

20.6.3 Operations

1. For each authentication system in Input 1, enumerate the accounts under that authentication system. This ground truth list of accounts organized by authentication system becomes M1.
2. Compare the accounts listed in M1 to the accounts listed in the current account inventory (Input 2).
3. Create a list of the correct accounts in Input 2 (which will be M2)
4. Create a list of the incorrect accounts in Input 2 (which will be M3).

20.6.4 Measures

- M1 = Ground truth account inventory
- M2 = List of correct accounts from the current (to be checked) inventory
- M3 = List of incorrect accounts from the current (to be checked) inventory

- M4 = Count of accounts in the ground truth account inventory (count of M1)
- M5 = Count of correct accounts in the current (to be checked) account inventory (count of M2)

20.6.5 Metrics

Metric	
	Calculate the accuracy of current (to be checked) account inventory
Calculation	`M5 / M4`

20.7 16.7: Establish Process for Revoking Access

Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

20.7.1 Dependencies

- Sub-control 16.6: Maintain an Inventory of Accounts

20.7.2 Inputs

1. The inventory of employee accounts
2. A given time period for analysis

20.7.3 Operations

1. For each employee terminated or changed responsibilities within the Input 2 time period, enumerate the employee's accounts (a given employee may have a number of accounts)

20.7.4 Measures

- M1 = List of employee accounts collected by Operation 1
- M2 = Count of M1
- M3 = List of employee accounts disabled within the Input 2 time period
- M4 = Count of M3

20.7.5 Metrics

Enforcement Quality

Metric	
	The ratio of employee accounts that have been terminated/revoked within the acceptable timeframe.
Calculation	`M2 / M4`

20.8 16.8: Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

Asset Type	Security Function	Implementation Groups
Users	Respond	1, 2, 3

20.8.1 Dependencies

- None

20.8.2 Inputs

1. Inventory of accounts
2. Inventory of business processes and/or business owners

20.8.3 Operations

1. For each account, enumerate any associated business processes or ownership

20.8.4 Measures

- M1 = List of accounts
- M2 = Count of M1
- M3 = List of accounts not associated with any business process or ownership
- M4 = Count of M3
- M5 = List of accounts associated with at least one business process or ownership
- M6 = Count of M5

20.8.5 Metrics

Coverage

Metric	What percentage of accounts are associated with at least one business process or ownership?
Calculation	`M6 / M2`

20.9 16.9: Disable Dormant Accounts

Automatically disable dormant accounts after a set period of inactivity.

Asset Type	Security Function	Implementation Groups
Users	Respond	1, 2, 3

20.9.1 Dependencies

- None

20.9.2 Inputs

1. The list of all accounts created in the enterprise
2. An organizationally defined policy indicating a "dormant threshold"; the period of inactivity after which the account is considered dormant (recommended value 1 month)

Assumptions

- The list of accounts for the enterprise includes OS-level, database, internal and external application accounts.
- Based on the account location, a query interface is assumed enabling collection of a "last activity" timestamp, such as last logon, as well as a status indicating if the account is enabled or disabled.

20.9.3 Operations

1. For each account, query the respective interface to collect the account's last activity.
2. For each account, query the respective interface to collect the account's enabled/disabled status.
3. Based on Operations 1 and 2, collect those accounts still marked as enabled but whose last activity is beyond the "dormant threshold" defined in Input 2

20.9.4 Measures

- M1 = List of Accounts
- M2 = Count of M1
- M3 = List of accounts marked as enabled
- M4 = Count of M3
- M5 = List of accounts enabled and not used for a time period outside the dormant threshold
- M6 = Count of M5

20.9.5 Metrics

Dormant Accounts

Metric	What percentage of all accounts are currently dormant but still enabled?
Calculation	`M6 / M2`

Enabled Dormant Accounts

Metric	What percentage of accounts marked enabled are currently dormant and still enabled?
Calculation	`M3 / M2`

20.10 16.10: Ensure All Accounts Have An Expiration Date

Ensure that all accounts have an expiration date that is monitored and enforced.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

20.10.1 Dependencies

- Sub-control 16.1: Inventory of Authentication Systems

20.10.2 Inputs

1. Account Inventory
2. Authentication System Inventory
3. Approved Configuration(s) for ensuring that account expiration dates are automatically enforced (there may be multiple configurations that vary by type of authentication system, etc.)
4. Optional: Maximum amount of time in the future allowed for an expiration date (example: the organization may require all accounts to have an expiration date no more than 1 year in the future so that all accounts must be re-justified every year). This time frame could be specific to certain account types (Administrator for example), or specific to certain authentication systems.

20.10.3 Operations

1. For each account in the account inventory (Input 1), check to see if that account has a valid expiration date that is in the future. If the optional Input 4 was provided, also verify if that expiration date complies with any applicable additional time frame restrictions. Based on these checks, create a list (M1) of accounts with valid expiration dates, and a list (M2) of accounts with invalid expiration dates (noting why the expiration date is invalid).
2. For each authentication system in Input 2, check to see if it is configured according to the appropriate configuration(s) from Input 3.
3. Create a list (M3) of authentication systems that are configured correctly
4. Create a list (M4) of authentication systems that are not configured correctly (noting the deviations).

20.10.4 Measures

- M1 = List of accounts with valid expiration dates
- M2 = List of accounts with invalid expiration dates
- M3 = List of authentication systems that are configured correctly
- M4 = List of authentication systems that are not configured correctly
- M5 = Count of accounts with valid expiration dates (count of M1)
- M6 = Total count of accounts (count of Input 1)

- M7 = Count of authentication systems that are configured correctly (count of M3)
- M8 = Total count of authentication systems (count of Input 2)

20.10.5 Metrics

Metric	
	The ratio of accounts with valid expiration dates to the total number of accounts
Calculation	`M5 / M6`

Metric	
	The ratio of correctly configured authentication systems to the total number of authentication systems
Calculation	`M7 / M8`

20.11 16.11: Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

Asset Type	Security Function	Implementation Groups
Users	Protect	1, 2, 3

20.11.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

20.11.2 Inputs

1. List of workstations which have enabled automatic workstation locking
2. List of workstations
3. The workstation configuration policy establishing the organization's workstation locking time threshold

20.11.3 Operations

1. For each workstation with locking enabled, collect the locking time threshold
2. Collect the list of workstations whose locking time threshold exceeds the value specified by Input 3

20.11.4 Measures

- M1 = List of workstations
- M2 = Count of M1
- M3 = List of workstations having enabled automatic workstation locking
- M4 = Count of M3
- M5 = List of appropriately configured workstations
- M6 = Count of M5
- M7 = List of inappropriately configured workstations
- M8 = Count of M7

20.11.5 Metrics

Misconfigured Workstations

Metric	What percentage of automatic locking enabled workstations are configured within the locking time threshold?
Calculation	`M6 / M2`

Unconfigured Workstations

Metric	How many workstations do *not* have automatic locking enabled?
Calculation	`M2 - M4`

20.12 16.12: Monitor Attempts to Access Deactivated Accounts

Monitor attempts to access deactivated accounts through audit logging.

Asset Type	Security Function	Implementation Groups
Users	Detect	2, 3

20.12.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 16.1: Inventory of Authentication Systems

20.12.2 Inputs

1. Authentication System Inventory
2. Approved configuration(s) for logging attempts to access deactivated accounts
3. Approved configuration(s) for alerting on attempts to access deactivated accounts

Note: There may be multiple configurations for Inputs 2 and 3 to account for various groups/types of authentication systems.

20.12.3 Operations

1. For each authentication system in Input 1, select the appropriate approved configuration from Inputs 2 and 3 in turn for that endpoint and check to see if that authentication system's actual configuration complies with the approved configuration for each Input. Record this information as M1 - a list of authentication systems annotated with whether that authentication system is compliant or non-compliant with the appropriate approved configuration from each of the two inputs (Input 2 and Input 3).
2. For Input 2, and for Input 3, generate a count of compliant authentication systems from M1 and record these as M2 and M3 respectively.
3. Count the number of authentication systems that are compliant with both inputs and record this as M4

20.12.4 Measures

- M1 = List of authentication systems with each endpoint entry labeled with compliance or non-compliance for both Input 2 and Input 3
- M2 = Count of compliant authentication systems based on Input 2 configurations
- M3 = Count of compliant authentication systems based on Input 3 configurations
- M4 = Count of authentication systems that are compliant with configurations from both inputs
- M5 = Total count of authentication systems from Input 1

20.12.5 Metrics

Logging Coverage

Metric	
	The ratio of authentication systems configured to log attempts to access deactivated accounts to the total number of authentication systems.
Calculation	`M2 / M5`

Alerting Coverage

Metric	
	The ratio of authentication systems configured to log attempts to access deactivated accounts to the total number of authentication systems.
Calculation	`M3 / M5`

Full Coverage

Metric	
	The ratio of authentication systems configured to both log and alert on attempts to access deactivated accounts to the total number of authentication systems.
Calculation	`M4 / M5`

20.13 16.13: Alert on Account Login Behavior Deviation

Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.

Asset Type	Security Function	Implementation Groups
Users	Detect	3

20.13.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

20.13.2 Inputs

1. The list of endpoints
2. The list of authorized software

20.13.3 Operations

1. Enumerate user behavioral monitoring software systems
2. Enumerate endpoints
3. **For each identified behavioral monitoring system**
    1. Enumerate endpoints covered by this behavioral monitoring system
    2. **Examine the system's configuration, noting appropriate and inappropriate configurations along the way, to ensure that it is configured to alert for at least the following deviation points:**
        1. Time of day
        2. Workstation location
        3. Duration
4. Enumerate all endpoints covered by at least one behavioral monitoring system
5. Complement covered endpoints with the list of all endpoints to enumerate the list of endpoints not covered by at least one behavioral monitoring system
6. Enumerate all appropriately configured behavioral monitoring systems

7. Enumerate all inappropriately configured behavioral monitoring systems

20.13.4 Measures

- M1 = List of user behavioral monitoring software systems
- M2 = List of endpoints
- M3 = List of endpoints covered by at least one behavioral monitoring system
- M4 = List of endpoints not covered by at least one behavioral monitoring system
- M5 = List of appropriately configured behavioral monitoring systems
- M6 = List of inappropriately configured behavioral monitoring systems
- M7 = Count of user behavioral monitoring software systems (count of M1)
- M8 = Count of endpoints (count of M2)
- M9 = Count of endpoints covered by at least one behavioral monitoring system (count of M3)
- M10 = Count of endpoints not covered by at least one behavioral monitoring system (count of M4)
- M11 = Count of appropriately configured behavioral monitoring systems (count of M5)
- M12 = Count of inappropriately configured behavioral monitoring systems (count of M6)

20.13.5 Metrics

Endpoint Coverage

Metric	
	The ratio of endpoints covered by at least one behavioral monitoring system to the total number of endpoints
Calculation	`M9 / M8`

Behavioral Monitoring System Coverage

Metric	
	The ratio of appropriately configured behavioral monitoring systems to the total number of behavioral monitoring systems
Calculation	`M11 / M7`

CHAPTER

TWENTYONE

CIS CONTROL 17: IMPLEMENT A SECURITY AWARENESS AND TRAINING PROGRAM

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Why is this CIS Control Critical?

It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. People fulfill important functions at every stage of system design, implementation, operation, use, and oversight. Examples include: system developers and programmers (who may not understand the opportunity to resolve root cause vulnerabilities early in the system life cycle); IT operations professionals (who may not recognize the security implications of IT artifacts and logs); end users (who may be susceptible to social engineering schemes such as phishing); security analysts (who struggle to keep up with an explosion of new information); and executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational/mission risk, and have no reasonable way to make relevant investment decisions).

Attackers are very conscious of these issues and use them to plan their exploitations by, for example: carefully crafting phishing messages that look like routine and expected traffic to an unwary user; exploiting the gaps or seams between policy and technology (e.g., policies that have no technical enforcement); working within the time window of patching or log review; using nominally non-security-critical systems as jump points or bots.

No cyber defense approach can effectively address cyber risk without a means to address this fundamental vulnerability. Conversely, empowering people with good cyber defense habits can significantly increase readiness.

21.1 17.1: Perform a Skills Gap Analysis

Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

21.1.1 Dependencies

- None

21.1.2 Inputs

1. Security awareness skill topic areas to be assessed
2. Set of exams/exercises mapped to the topics in Input 1
3. Minimum acceptable score

21.1.3 Operations

1. For each workforce member, administer the exams/exercises from Input 2
2. Score each of the exams/exercises
3. **For each security awareness skill topic area in Input 1, average the results of the exams/exercises mapped to that topic area to generate an organizational average for that topic area.**
    1. Generate a list of topic areas and the organizational averages that are greater than or equal to the minimum acceptable score provided as Input 3 (M1).
    2. Generate a list of topic areas and organizational averages that are below the minimum acceptable score (M2).

21.1.4 Measures

- M1 = List of security awareness topic areas with averages in the acceptable range (compliant list)
- M2 = List of security awareness topic areas with averages below the acceptable range (non-compliant list)
- M3 = Count of security awareness topic areas with averages in the acceptable range (count of M1)
- M4 = Total count of security awareness topic areas assessed (count of Input 1)

21.1.5 Metrics

Scoring

Metric	The ratio of security awareness topic areas with organizational averages in the acceptable range
Calculation	`M3 / M4`

21.2 17.2: Deliver Training to Fill the Skills Gap

Deliver training to address the skills gap identified to positively impact workforce members' security behavior.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

21.2.1 Dependencies

- Sub-control 17.1: Perform a Skills Gap Analysis

21.2.2 Inputs

1. Skills gap topics (areas of weakness as determined by the skills gap analysis in Sub-Control 17.1)
2. Modules/topics covered in the organization's security awareness training

21.2.3 Operations

1. **For each skills gap in Input 1, determine if that topic is adequately covered in the organization's security awareness training program (Input 2).**
    1. Create a list of the topics that are adequately covered (M1)
    2. Create a list of the topics that are not adequately covered (M2) including notes on what needs to be added to achieve adequate coverage of the topic.

21.2.4 Measures

- M1 = List of skills gap topics that are adequately covered in the organization's security awareness training
- M2 = List of skills gap topics that are not adequately covered in the organization's security awareness training
- M3 = Count of skills gap topics that are adequately covered in the organization's security awareness program (count of M1)
- M4 = Total count of skills gap topics (count of Input 1)

21.2.5 Metrics

Coverage

Metric	The ratio of skills gap topics that are adequately covered in the organization's security awareness training
Calculation	`M3 / M4`

21.3 17.3: Implement a Security Awareness Program

Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

21.3.1 Dependencies

- None

21.3.2 Inputs

1. List of workforce members
2. List of most recent security awareness training completion dates for each workforce member
3. Required frequency of training (at least annually)

21.3.3 Operations

1. For each workforce member in Input 1, check Input 2 to see if that workforce member's most recent security awareness training completion date was within the time frame specified by Input 3 (if the workforce member is not listed in Input 2, assume the workforce member is not compliant). Generate a list of compliant workforce members (M1) and a list of non-compliant workforce members (M2).

21.3.4 Measures

- M1 = List of workforce members who have completed the security awareness training within the specified time frame (compliant list)
- M2 = List of workforce members who have not completed the security awareness training within the specified time frame (non-compliant list)
- M3 = Number of workforce members in the compliant list (M1)
- M4 = Number of workforce members in the non-compliant list (M2)
- M5 = Total number of workforce members in Input 1

21.3.5 Metrics

Coverage

Metric	
	What percentage of workforce members have completed the security awareness training module within the specified timeframe?
Calculation	`M3 / M5`

21.4 17.4: Update Awareness Content Frequently

Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards, and business requirements.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

21.4.1 Dependencies

- Sub-control 17.3: Implement a Security Awareness Program

21.4.2 Inputs

1. Date the organization's security awareness program was last updated
2. Maximum time allowed between updates to the organization's security awareness program

21.4.3 Operations

1. Verify that the maximum time allowed between updates to the security awareness program (Input 2) is one year or less and set M1 accordingly.
2. Check the date that the security awareness program was last updated (Input 1) to make sure that it occurred within the required time frame (Input 2) and set M2 accordingly.

21.4.4 Measures

- M1 = 1 if maximum time allowed between security awareness program updates is one year or less, 0 if greater than one year
- M2 = 1 if the last update to the security awareness program was within the required time frame, 0 otherwise

21.4.5 Metrics

Update Timeliness

Metric	Is the organization's security awareness program updated within acceptable time frame?
Calculation	`M1 AND M2`

21.5 17.5: Train Workforce on Secure Authentication

Train workforce members on the importance of enabling and utilizing secure authentication.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

21.5.1 Dependencies

- None

21.5.2 Inputs

1. List of workforce members
2. List of most recent security awareness training completion dates for each workforce member
3. Required frequency of training (at least annually)

21.5.3 Operations

1. For each workforce member in Input 1, check Input 2 to see if that workforce member's most recent security awareness training completion date was within the time frame specified by Input 3 (if the workforce member is not listed in Input 2, assume the workforce member is not compliant). Generate a list of compliant workforce members (M1) and a list of non-compliant workforce members (M2).

21.5.4 Measures

- M1 = List of workforce members who have completed the security awareness training within the specified time frame (compliant list)
- M2 = List of workforce members who have not completed the security awareness training within the specified time frame (non-compliant list)
- M3 = Number of workforce members in the compliant list (M1)
- M4 = Number of workforce members in the non-compliant list (M2)
- M5 = Total number of workforce members in Input 1

21.5.5 Metrics

Coverage

Metric	
	What percentage of workforce members have completed the security awareness training module within the specified timeframe?
Calculation	`M3 / M5`

21.6 17.6: Train Workforce on Identifying Social Engineering Attacks

Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

21.6.1 Dependencies

- None

21.6.2 Inputs

1. List of workforce members
2. List of most recent security awareness training completion dates for each workforce member
3. Required frequency of training (at least annually)

21.6.3 Operations

1. For each workforce member in Input 1, check Input 2 to see if that workforce member's most recent security awareness training completion date was within the time frame specified by Input 3 (if the workforce member is not listed in Input 2, assume the workforce member is not compliant). Generate a list of compliant workforce members (M1) and a list of non-compliant workforce members (M2).

21.6.4 Measures

- M1 = List of workforce members who have completed the security awareness training within the specified time frame (compliant list)
- M2 = List of workforce members who have not completed the security awareness training within the specified time frame (non-compliant list)
- M3 = Number of workforce members in the compliant list (M1)
- M4 = Number of workforce members in the non-compliant list (M2)
- M5 = Total number of workforce members in Input 1

21.6.5 Metrics

Coverage

Metric	
	What percentage of workforce members have completed the security awareness training module within the specified timeframe?
Calculation	`M3 / M5`

21.7 17.7: Train Workforce on Sensitive Data Handling

Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

21.7.1 Dependencies

- None

21.7.2 Inputs

1. List of workforce members
2. List of most recent security awareness training completion dates for each workforce member
3. Required frequency of training (at least annually)

21.7.3 Operations

1. For each workforce member in Input 1, check Input 2 to see if that workforce member's most recent security awareness training completion date was within the time frame specified by Input 3 (if the workforce member is not listed in Input 2, assume the workforce member is not compliant). Generate a list of compliant workforce members (M1) and a list of non-compliant workforce members (M2).

21.7.4 Measures

- M1 = List of workforce members who have completed the security awareness training within the specified time frame (compliant list)
- M2 = List of workforce members who have not completed the security awareness training within the specified time frame (non-compliant list)
- M3 = Number of workforce members in the compliant list (M1)
- M4 = Number of workforce members in the non-compliant list (M2)
- M5 = Total number of workforce members in Input 1

21.7.5 Metrics

Coverage

Metric	
	What percentage of workforce members have completed the security awareness training module within the specified timeframe?
Calculation	`M3 / M5`

21.8 17.8: Train Workforce on Causes of Unintentional Data Exposure

Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to *autocomplete* in email.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

21.8.1 Dependencies

- None

21.8.2 Inputs

1. List of workforce members
2. List of most recent security awareness training completion dates for each workforce member
3. Required frequency of training (at least annually)

21.8.3 Operations

1. For each workforce member in Input 1, check Input 2 to see if that workforce member's most recent security awareness training completion date was within the time frame specified by Input 3 (if the workforce member is not listed in Input 2, assume the workforce member is not compliant). Generate a list of compliant workforce members (M1) and a list of non-compliant workforce members (M2).

21.8.4 Measures

- M1 = List of workforce members who have completed the security awareness training within the specified time frame (compliant list)
- M2 = List of workforce members who have not completed the security awareness training within the specified time frame (non-compliant list)
- M3 = Number of workforce members in the compliant list (M1)
- M4 = Number of workforce members in the non-compliant list (M2)
- M5 = Total number of workforce members in Input 1

21.8.5 Metrics

Coverage

Metric	What percentage of workforce members have completed the security awareness training module within the specified timeframe?
Calculation	`M3 / M5`

21.9 17.9: Train Workforce Members on Identifying and Reporting Incidents

Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

21.9.1 Dependencies

- None

21.9.2 Inputs

1. List of workforce members
2. List of most recent security awareness training completion dates for each workforce member
3. Required frequency of training (at least annually)

21.9.3 Operations

1. For each workforce member in Input 1, check Input 2 to see if that workforce member's most recent security awareness training completion date was within the time frame specified by Input 3 (if the workforce member is not listed in Input 2, assume the workforce member is not compliant). Generate a list of compliant workforce members (M1) and a list of non-compliant workforce members (M2).

21.9.4 Measures

- M1 = List of workforce members who have completed the security awareness training within the specified time frame (compliant list)
- M2 = List of workforce members who have not completed the security awareness training within the specified time frame (non-compliant list)
- M3 = Number of workforce members in the compliant list (M1)
- M4 = Number of workforce members in the non-compliant list (M2)
- M5 = Total number of workforce members in Input 1

21.9.5 Metrics

Coverage

Metric	What percentage of workforce members have completed the security awareness training module within the specified timeframe?
Calculation	`M3 / M5`

CHAPTER

TWENTYTWO

CIS CONTROL 18: APPLICATION SOFTWARE SECURITY

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Why is this CIS Control Critical?

Attacks often take advantage of vulnerabilities found in web-based and other application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Examples of specific errors include: the failure to check the size of user input; failure to filter out unneeded but potentially malicious character sequences from input streams; failure to initialize and clear variables; and poor memory management allowing flaws in one part of the software to affect unrelated (and more security critical) portions.

There is a flood of public and private information about such vulnerabilities available to attackers and defenders alike, as well as a robust marketplace for tools and techniques to allow "weaponization" of vulnerabilities into exploits. In one attack, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites using SQL injection. During that attack, trusted websites from state governments and other organizations compromised by attackers were used to infect hundreds of thousands of browsers that accessed those websites. Many more web and non-web application vulnerabilities are discovered on a regular basis.

22.1 18.1: Establish Secure Coding Practices

Establish secure coding practices appropriate to the programming language and development environment being used.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.1.1 Dependencies

- None

22.1.2 Inputs

1. List of programming languages and development environments that the organization uses for software development
2. The organization's secure coding guides, with each guide tagged with the programming languages and development environments that it covers

22.1.3 Operations

1. **For each programming language and development environment in Input 1, check to see if it is covered by at least one secure coding guide in Input 2.**
    1. Create a list of the programming languages and development environments that are covered by secure coding guide (M1)
    2. Create a list of programming languages and development environments that are not covered by at least one secure coding guide (M2)
2. (Optional) Manually review the secure coding guides to ensure that they cover all the needed aspects of secure coding for the programming languages and development environments in question, noting any topics or sections that need improvement (M3).

22.1.4 Measures

- M1 = List of programming languages and development environments covered by at least one secure coding guide (compliant list)
- M2 = List of programming languages and development environments not covered by at least one secure coding guide (non-compliant list)
- M3 = (Optional) From optional manual review, list/description of topics or sections that need to be improved
- M4 = Count of programming languages and development environments covered by at least one secure coding guide (count of M1)
- M5 = Total count of programming languages and development environments that the organization uses for software development (count of Input 1)

22.1.5 Metrics

Coverage

Metric	The ratio of programming languages and development environments covered by a secure coding guide
Calculation	`M4 / M5`

22.2 18.2: Ensure That Explicit Error Checking Is Performed for All In-House Developed Software

For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.2.1 Dependencies

- Sub-control 18.1: Establish Secure Coding Practices

22.2.2 Inputs

1. List of in-house developed software
2. Documentation for in-house developed software
3. Code for in-house developed software (the software itself)

22.2.3 Operations

1. For each piece of in-house developed software in Input 1, identify all of the inputs for that software and associated properties of those inputs including size, data type, and acceptable ranges or formats (M1).
2. **For each piece of in-house developed software, review the associated documentation provided in Input 2 to ensure that each of the inputs and associated properties identified in M1 are properly documented.**
    1. Create a list of the software for which all inputs and associated properties are properly documented (M2)
    2. Create a list of software for which at least one input and/or associated properties is not properly documented noting which inputs/properties are insufficiently documented (M3).
3. **For each piece of in-house developed software, review the associated code provided in Input 3 to ensure that explicit error checking is performed for each of the inputs identified in M1 to ensure that those inputs are of acceptable sizes, data types, formats, and within the proper ranges.**
    1. Create a list of the software for which all inputs have explicit error checking for the identified properties (M4)
    2. Create a list of software for which at least one of the inputs/properties is not properly checked (M5) noting the improperly checked inputs/properties and why they are deficient.
4. Compare M2 and M4 to generate the count of which pieces of in-house developed software are in both lists (M6).

22.2.4 Measures

- M1 = List of all inputs for each piece of in-house developed software and associated properties of those inputs including size, data type, and acceptable ranges or formats
- M2 = List of the software for which all inputs and associated properties are properly documented (compliant documentation list)
- M3 = List of software for which at least one input and/or associated properties is not properly documented (non-compliant documentation list)
- M4 = List of the software for which all inputs have explicit error checking for the identified properties (compliant code list)
- M5 = List of software for which at least one of the inputs/properties is not properly checked (non-compliant code list)
- M6 = Count of compliant software (count of intersection of M2 and M4)
- M7 = Total count of in-house developed software (count of Input 1)

22.2.5 Metrics

Coverage

Metric	
	The ratio of software that contains proper error checking of inputs and is properly documented
Calculation	`M6 / M7`

22.3 18.3: Verify That Acquired Software Is Still Supported

Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.3.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.2: Ensure Software is Supported by Vendor
- Sub-control 5.1: Establish Secure Configurations

22.3.2 Inputs

1. List of software acquired from outside the organization, including version information for each (subset of Authorized Software List from Sub-Control 2.1). As described in Sub-Control 2.2, this list should also include the supported or unsupported status for each.
2. The list of organizational security configuration standards from Sub-Control 5.1

22.3.3 Operations

1. **For each software version listed in Input 1, check the list of organizational security configuration standards provided in Input 2.**
    1. Create a list of software versions that have at least one associated organizational security configuration standard (M1) including identifiers for the associated standard(s)
    2. Create a list of software versions that do not have any associated organizational security configuration standards (M2)
2. **For each software version listed in M2, check the supported/unsupported status field for that software version in Input 1 to see if that product version is still supported by the developer.**
    1. Create a list of software versions that appear in M2 and are not supported (M3).

22.3.4 Measures

- M1 = List of externally acquired software that has an associated organizational security configuration standard
- M2 = List of externally acquired software that does not have an associated organizational security configuration standard
- M3 = List of externally acquired software that does not have an associated organizational security configuration standard and is also not supported by the developer (non-compliant list)
- M4 = Count of externally acquired software that does not have an associated organizational security configuration standard and is also not supported by the developer (count of M3)
- M5 = Total count of externally acquired software (count of Input 1)

22.3.5 Metrics

Coverage

Metric	
	The ratio of externally acquired software that is either supported or has an associated organizational security configuration standard
Calculation	`(M5 - M4) / M5`

22.4 18.4: Only Use Up-to-Date and Trusted Third-Party Components

Only use up-to-date and trusted third-party components for the software developed by the organization.

Asset Type	Security Function	Implementation Groups
N/A	N/A	3

22.4.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

22.4.2 Inputs

1. The list of authorized software
2. Third-party component inventory (possibly from your automated build systems)

22.4.3 Operations

1. Enumerate all third-party components in the inventory
2. **For each component, verify:**
    1. Latest component is being used
    2. The component is explicitly trusted by the organization
3. Enumerate compliant components
4. Enumerate non-compliant components

22.4.4 Measures

- M1 = List of all third-party components being used
- M2 = List of all third-party components that are up-to-date and explicitly trusted
- M3 = List of all third-party components that are not up-to-date or not explicitly trusted
- M4 = Count of third-party components being used (count of M1)
- M5 = Count of third-party components that are up-to-date and explicitly trusted (count of M2)
- M6 = Count of third-party components that are not up-to-date or not explicitly trusted (count of M3)

22.4.5 Metrics

Coverage

Metric	
	The ratio of compliant third-party components to the total number of third-party components in use
Calculation	`M5 / M4`

22.5 18.5: Use only Standardized and Extensively Reviewed Encryption Algorithms

Use only standardized, currently accepted, and extensively reviewed encryption algorithms.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.5.1 Dependencies

- None

22.5.2 Inputs

1. List of encryption algorithms used by the organization
2. Authoritative source that identifies which encryption algorithms are standardized, currently accepted, and extensively reviewed.

22.5.3 Operations

1. **For each encryption algorithm in Input 1, check Input 2 to see if that encryption algorithm is standardized, currently accepted, and extensively reviewed.**
    1. Create a list of the encryption algorithms that meet all of these criteria (M1)
    2. Create a list of the encryption algorithms that do not meet all of these criteria (M2).

22.5.4 Measures

- M1 = List of encryption algorithms used by the organization that are standardized, currently accepted, and extensively reviewed (compliant list)
- M2 = List of encryption algorithms used by the organization that do not meet these criteria (non-compliant list)
- M3 = Count of encryption algorithms used by the organization that are standardized, currently accepted, and extensively reviewed (count of M1)
- M4 = Total count of encryption algorithms used by the organization (count of Input 1)

22.5.5 Metrics

Coverage

Metric	The ratio of encryption algorithms used by the organization that are standardized, currently accepted, and extensively reviewed
Calculation	`M3 / M4`

22.6 18.6: Ensure Software Development Personnel Are Trained in Secure Coding

Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.6.1 Dependencies

- None

22.6.2 Inputs

1. List of software development personnel including assigned development environments and roles
2. List of secure coding training courses required for each development environment and role
3. List of secure coding training courses that each person has completed

22.6.3 Operations

1. For each person in Input 1, use the development environments and roles assigned to that person to determine which secure coding training courses the person is required to take; note these individual lists of required courses in M1.
2. **For each person in Input 1, compare the courses that person is required to take from M1 to the courses that person has completed from Input 3.**
    1. Create a list of the required courses the person has completed (M2)

2. Create a list of the required courses the person has not completed (M3).

22.6.4 Measures

- M1 = List of courses that software development personnel are required to take, by individual
- M2 = List of required courses that software development personnel have completed, by individual (compliant list)
- M3 = List of required courses that software development personnel have not completed, by individual (non-compliant list)
- M4 = Count of required courses by individual (count of M1)
- M5 = Count of completed required courses by individual (count of M2)

22.6.5 Metrics

Coverage

Metric	THe ratio of completed required courses to total required courses by individual
Calculation	`Individual's M5 / Individual's M4`

NOTE: An organizational average completion rate can be calculated by averaging the individual completion ratios from the above "Coverage" metric.

22.7 18.7: Apply Static and Dynamic Code Analysis Tools

Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.7.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

22.7.2 Inputs

1. The inventory of internally-developed software (from the organization's software inventory)
2. The inventory of static analysis tools (from the organization's software inventory)
3. The inventory of dynamic analysis tools (from the organization's software inventory)

22.7.3 Operations

1. Map the inventory of internally-developed software to the applicable static/dynamic analysis tools which are used for verification.

22.7.4 Measures

- M1(i) = (For each software "i" from Input 1) 1 if the software is verified by static analysis tool(s); 0 otherwise
- M2(i) = (For each software "i" from Input 1) 1 if the software is verified by dynamic analysis tool(s); 0 otherwise
- M3 = Count of internally developed software (the count of Input 1)

22.7.5 Metrics

Static Analysis Tool Coverage

Metric	The ratio of internally developed software verified by static analysis tools to the total number of internally developed software applications
Calculation	`(SUM from i=1..M3 (M1(i))) / M3`

Dynamic Analysis Tool Coverage

Metric	The ratio of internally developed software verified by dynamic analysis tools to the total number of internally developed software applications
Calculation	`(SUM from i=1..M3 (M2(i))) / M3`

22.8 18.8: Establish a Process to Accept and Address Reports of Software Vulnerabilities

Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.8.1 Dependencies

- None

22.8.2 Inputs

1. Written process for accepting and addressing software vulnerabilities

22.8.3 Operations

1. Determine whether a written process for accepting and addressing software vulnerabilities exists (M1).
2. **Manually review the written process for accepting and addressing software vulnerabilities (Input 1).**
    1. Identify whether the document provides a means for external entities to contact your security group (M2)
    2. Identify whether the document adequately describes the process for accepting reports of software vulnerabilities (M3)
    3. Identify whether the document adequately describes the process for addressing those reports (M4)

22.8.4 Measures

- M1 = Boolean value indicating whether a written process for accepting and addressing software vulnerabilities exists; 1 if it exists, 0 if it does not
- M2 = Boolean value indicating whether the document provides a means for external entities to contact your security group; 1 if the document provides this info, 0 if it does not
- M3 = Boolean value indicating whether the document adequately describes the process for accepting reports of software vulnerabilities; 1 if the document adequately describes this process, 0 if it does not
- M4 = Boolean value indicating whether the document adequately describes the process for addressing reports of software vulnerabilities; 1 if the document adequately describes this process, 0 if it does not

22.8.5 Metrics

Process Completeness

Metric	Does the written process for accepting and addressing reports of software vulnerabilities exist and is it complete?
Calculation	`M1 AND M2 AND M3 AND M4`

22.9 18.9: Separate Production and Non-Production Systems

Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.9.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories

22.9.2 Inputs

1. The inventory of systems used for production and non-production deployments
2. The inventory of user accounts
3. The mechanism for monitoring user account access to systems

22.9.3 Operations

1. From Input 1, categorize the deployments of systems into those with production deployments and those with non-production deployments. Note that systems *should* have both production and 1..n non-production deployments (including development, staging, integration testing, etc).
2. From Input 2, determine the list of user accounts with access to production environments

22.9.4 Measures

- M1(i) = (For each system with a production deployment "i") 1 if at least one non-production deployment environment exists for that system, 0 otherwise.
- M2 = Count of systems with a production deployment
- M3 = Count of user accounts whose access to production environments is monitored by the mechanism defined by Input 3.
- M4 = Count of user accounts with access to production environments (the count from Operation 2).

22.9.5 Metrics

Environment Coverage

Metric	
	The ratio of production systems where at least one non-production deployment exists to the total number of production systems
Calculation	`(SUM from i=1..M2 (M1(i))) / M2`

Monitored Account Coverage

Metric	
	The ratio of accounts with production system access that are monitored to the total accounts with production system access
Calculation	`M3 / M4`

22.10 18.10: Deploy Web Application Firewalls

Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.10.1 Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

22.10.2 Inputs

1. The inventory of authorized software

22.10.3 Operations

1. Enumerate all in-house owned and operated software (i.e. applications in the software inventory that are developed in-house and/or acquired) for which there is an application-level firewall technology exists
2. Enumerate all application-level firewalls (including WAF and host-based firewalls)
3. For each application-level firewall, enumerate covered software applications
4. Complement the set of software applications identified in the first operation with the covered software applications

22.10.4 Measures

- M1 = Enumerated list of all software in the inventory for which an application-level firewall technology exists
- M2 = Enumerated list of all application-level firewalls
- M3 = Enumerated list of applications covered by application-level firewalls
- M4 = Enumerated list of applications not covered by software applications (fourth operation)
- M5 = Count of software for which an application-level firewall technology exists (count of M1)
- M6 = Count of application-level firewalls (count of M2)
- M7 = Count of applications covered by application-level firewalls (count of M3)

- M8 = Count of applications not covered by software applications (count of M4)

22.10.5 Metrics

Coverage

Metric	
	The ratio of the number of applications covered by an application-level firewall to the number of eligible applications in the enterprise.
Calculation	`M7 / M5`

22.11 18.11: Use Standard Hardening Configuration Templates for Databases

For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

22.11.1 Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.5: Integrate Software and Hardware Asset Inventories
- Sub-control 5.1: Establish Secure Configurations

22.11.2 Inputs

1. The list of database management software being used in the organization
2. The list of systems on which database instances reside
3. The list of enterprise security configuration standards

22.11.3 Operations

1. Determine, from the list of enterprise security configuration standards, which are applicable to database management software (M1)
2. From the list of enterprise security configuration standards, calculate the number of database management software that are covered by the standards (perform the intersection of the results of Operation 1 with Input 1; the result is M2)

22.11.4 Measures

- M1 = List of enterprise security configuration standards specific to database management systems
- M2 = Count of M1
- M3 = List of database management software covered by applicable enterprise security configuration standards
- M4 = Count of M3
- M5 = List of database management software not covered by applicable enterprise security configuration standards
- M6 = Count of M5
- M7 = Count of database management software being used in the organization (from Input 1)

22.11.5 Metrics

Coverage

Metric	
	The ratio of database management software covered by applicable enterprise security configuration standards to the total number of database management software
Calculation	`M4 / M7`

NOTE: The second ask of this sub-control speaks to assessment of Input 2 against security configuration standards determined by Operation 1.

CHAPTER

TWENTYTHREE

CIS CONTROL 19: INCIDENT RESPONSE AND MANAGEMENT

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Why is this CIS Control Critical?

Cyber incidents are now just part of our way of life. Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. The question of a successful cyber-attack against an enterprise is not "if" but "when."

When an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and potentially exfiltrating more sensitive data than would otherwise be possible were an effective incident response plan in place.

23.1 19.1: Document Incident Response Procedures

Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

23.1.1 Dependencies

- None

23.1.2 Inputs

1. Incident response plan

23.1.3 Operations

1. Determine whether incident response plan exists (becomes M1)
2. If it exists, then manual review of incident response plan (determine M2 and M3)

23.1.4 Measures

- M1 = A plan exists
- M2 = The plan defines incident response roles
- M3 = The plan defines incident handling/management phases

23.1.5 Metrics

Existence

Metric	
	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.
Calculation	`M1 AND M2 AND M3`

23.2 19.2: Assign Job Titles and Duties for Incident Response

Assign job titles and duties for handling computer and network incidents to specific individuals, and ensure tracking and documentation throughout the incident through resolution.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

23.2.1 Dependencies

- Sub-control 19.1: Document Incident Response Procedures

23.2.2 Inputs

1. Incident Response Plan including Incident Response Job Titles/Duties
2. Mapping of individuals to Incident Response Job Titles/Duties

23.2.3 Operations

1. Manually review the Incident Response Plan to verify that it exists and that it contains Incident Response job titles and duties. If the document exists and contains job titles and duties, set M1 equal to 1. If it does not exist, set M1 equal to 0 and skip the remaining operations.
2. Manually review the Incident Response Plan to verify that it ensures tracking and documentation throughout the incident through resolution. If this is adequately addressed in the document, set M2 equal to 1. If it is not, set M2 equal to 0.
3. For each job title specified in the Incident Response Plan, check Input 2 to ensure that at least one individual is mapped to that job. Create a list of jobs that have been assigned at least one individual (M3) and a list of jobs that have not been assigned at least one individual (M4).

23.2.4 Measures

- M1 = Boolean value indicating if the Incident Response Plan exists and contains Incident Response job titles and duties; 1 if so, 0 if not
- M2 = Boolean value indicating if the Incident Response Plan adequately addresses tracking and documentation throughout the incident; 1 if so, 0 if not
- M3 = List of Incident Response jobs with individuals assigned
- M4 = List of Incident Response jobs without individuals assigned
- M5 = Count of Incident Response jobs with individuals assigned (count of M3)
- M6 = Total number of Incident Response jobs defined

23.2.5 Metrics

Incident Response Plan Completeness

Metric	Does the incident response plan exist, contain job titles/duties, and adequately address tracking and documentation throughout the incident?
Calculation	`M1 AND M2`

Assignment Coverage

Metric	The ratio of incident response jobs/duties with assignees to the total number of incident response jobs/duties
Calculation	`M4 / M6`

23.3 19.3: Designate Management Personnel to Support Incident Handling

Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

23.3.1 Dependencies

- Sub-control 19.1: Document Incident Response Procedures

23.3.2 Inputs

1. Incident response plan

23.3.3 Operations

1. Determine whether incident response plan exists (becomes M1)
2. If it exists, then manual review of incident response plan (determine M2 and M3)

23.3.4 Measures

- M1 = A plan exists
- M2 = The plan identifies management personnel filling incident response handling decision-making roles
- M3 = The plan identifies backup personnel to the management personnel identified by M2

23.3.5 Metrics

Metric	Are personnel, including backups, designated to support the incident handling process?
Calculation	`M1 AND M2 AND M3`

23.4 19.4: Devise Organization-wide Standards For Reporting Incidents

Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

23.4.1 Dependencies

- Sub-control 19.1: Document Incident Response Procedures

23.4.2 Inputs

1. Incident Reporting Standards document

23.4.3 Operations

1. Determine whether the Incident Reporting Standards document exists. If the document exists, set M1 equal to 1. If it does not exist, set M1 equal to 0 and skip the remaining operations.
2. **Manually review the Incident Reporting Standards document to determine if it addresses:**
    1. The time required for system administrators and other workforce members to report anomalous events to the incident handling team (M2)

2. The mechanisms for such reporting (M3)
3. The kind of information that should be included in the incident notification (M4)

3. For each, set the measure to 1 if the document adequately addresses the topic, or 0 if the document fails to adequately address the topic.

23.4.4 Measures

- M1 = Boolean value indicating if the Incident Reporting Standards document exists; 1 if it exists, 0 if not
- M2 = Boolean value indicating if the Incident Reporting Standards document adequately addresses the time required for system administrators and other workforce members to report anomalous events to the incident handling team; 1 if it does, 0 if it does not
- M3 = Boolean value indicating if the Incident Reporting Standards document adequately addresses the mechanisms for reporting anomalous events to the incident handling team; 1 if it does, 0 if it does not
- M4 = Boolean value indicating if the Incident Reporting Standards document adequately addresses the kind of information that should be included in an incident notification to the incident handling team; 1 if it does, 0 if it does not

23.4.5 Metrics

Incident Reporting Standards Completeness

Metric	
	Does the Incident Reporting Standards document exist and adequately addresses the specified topics?
Calculation	`M1 AND M2 AND M3 AND M4`

23.5 19.5: Maintain Contact Information For Reporting Security Incidents

Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

23.5.1 Dependencies

- Subcontrol 19.1: Document Incident Response Procedures

23.5.2 Inputs

1. Incident response plan
2. List of relevant third-party incident reporting entities

23.5.3 Operations

1. Determine whether incident response plan exists (becomes M1)
2. If it exists, then manual review of incident response plan (determine M2)

23.5.4 Measures

- M1 = Boolean value indicating whether an incident response plan exists; 1 if an incident response plan exists, 0 otherwise.
- M2 = The plan includes information on third-party contacts for incident reporting (M1 includes Input 2)

23.5.5 Metrics

Metric	Is information on third-party contact information maintained, for use in incident handling?
Calculation	`M1 AND M2`

23.6 19.6: Publish Information Regarding Reporting Computer Anomalies and Incidents

Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

23.6.1 Dependencies

- Subcontrol 19.1: Document Incident Response Procedures

23.6.2 Inputs

1. Incident response plan
2. Security awareness program documentation

23.6.3 Operations

1. Determine whether incident response plan exists (becomes M1)
2. Determine whether the security awareness documentation exists (becomes M2)
3. If both exist, then review the security awareness plan (determine M3 and M4)

23.6.4 Measures

- M1 = Boolean value indicating whether an incident response plan exists; 1 if an incident response plan exists, 0 otherwise.
- M2 = Boolean value indicating whether a security awareness program exists; 1 if an incident response plan exists, 0 otherwise.
- M3 = The incident response plan requires publishing incident reporting information for all workforce members as part of the organization's security awareness program

- M4 = The security awareness program publishes incident reporting information for all workforce members

23.6.5 Metrics

Metric	
	Is information regarding reporting of computer anomalies and incidents published for all workforce members?
Calculation	`M1 AND M2 AND M3 AND M4`

23.7 19.7: Conduct Periodic Incident Scenario Sessions for Personnel

Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responder's technical capabilities using tools and data available to them.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

23.7.1 Dependencies

- Sub-control 19.1: Document Incident Response Procedures

23.7.2 Inputs

1. After Action Report from most recent incident response exercise
2. Incident Response Plan

23.7.3 Operations

1. Examine the After Action Report (Input 1) and determine the date of the exercise. Examine the Incident Response Plan (Input 2) to determine the required time frame for incident response exercises and determine if the most recent exercise was within that time frame (M1).
2. Manually review the After Action Report to determine if it details that the incident response exercise tested the following: communication channels (M2), decision making (M3), incident responder's technical capabilities using the tools and data available to them (M4).

23.7.4 Measures

- M1 = Boolean value indicating if the most recent incident response exercise was within the required time frame; 1 if so, 0 if not
- M2 = Boolean value indicating if the most recent incident response exercise After Action Report contains information about the exercise's testing of communication channels; 1 if so, 0 if not
- M3 = Boolean value indicating if the most recent incident response exercise After Action Report contains information about the exercise's testing of decision making; 1 if so, 0 if not

- M4 = Boolean value indicating if the most recent incident response exercise After Action Report contains information about the exercise's testing of incident responder's technical capabilities using the tools and data available to them; 1 if so, 0 if not

23.7.5 Metrics

Timeliness

Metric	Timeliness of most recent incident response exercise
Calculation	`M1`

Completeness

Metric	Were incident response After Action Reports complete, containing information regarding testing of communication channels, decision making, and technical competence?
Calculation	`(M2 + M3 + M4) / 3`

23.8 19.8: Create Incident Scoring and Prioritization Schema

Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.

Asset Type	Security Function	Implementation Groups
N/A	N/A	3

23.8.1 Dependencies

- Sub-control 19.1: Document Incident Response Procedures

23.8.2 Inputs

1. Enterprise incident management policy

23.8.3 Operations

1. **Examine the enterprise incident management policy for the following properties:**
    1. Incident scoring and prioritization schema based on known or potential impact
    2. Procedure relying on this schema is used to determine status update frequency during incident handling
    3. Procedure relying on this schema is used to determine escalation paths during incident handling

23.8.4 Measures

- M1 = (Boolean) 1 if an incident scoring and prioritization schema is present in the policy; 0 otherwise
- M2 = (Boolean) 1 if status update procedure relies on aforementioned schema; 0 otherwise
- M3 = (Boolean) 1 if escalation procedure relies on aforementioned schema; 0 otherwise

23.8.5 Metrics

Scoring/Prioritization

Metric	
	Does the incident management policy include a scoring/prioritization schema, and are status update frequency and escalation paths reliant upon that schema?
Calculation	`M1 AND M2 AND M3`

CHAPTER

TWENTYFOUR

CIS CONTROL 20: PENETRATION TESTS AND RED TEAM EXERCISES

Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Why is this CIS Control Critical?

Attackers often exploit the gap between good defensive designs and intentions and implementation or maintenance. Examples include: the time window between announcement of a vulnerability, the availability of a vendor patch, and actual installation on every machine. Other examples include: well-intentioned policies that have no enforcement mechanism (especially those intended to restrict risky human actions); failure to apply good configurations to machines that come on and off of the network; and failure to understand the interaction among multiple defensive tools, or with normal system operations that have security implications.

A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defenses, and appropriate action by people. In a complex environment where technology is constantly evolving, and new attacker tradecraft appears regularly, organizations should periodically test their defenses to identify gaps and to assess their readiness by conducting penetration testing.

Penetration testing starts with the identification and assessment of vulnerabilities that can be identified in the enterprise. Next, tests are designed and executed to demonstrate specifically how an adversary can either subvert the organization's security goals (e.g., the protection of specific Intellectual Property) or achieve specific adversarial objectives (e.g., establishment of a covert Command and Control infrastructure). The results provide deeper insight, through demonstration, into the business risks of various vulnerabilities.

Red Team exercises take a comprehensive approach at the full spectrum of organization policies, processes, and defenses in order to improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels. Independent Red Teams can provide valuable and objective insights about the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even of those planned for future implementation.

24.1 20.1: Establish a Penetration Testing Program

Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

24.1.1 Dependencies

- None

24.1.2 Inputs

1. A Penetration Testing Program document

24.1.3 Operations

1. Determine whether the Penetration Testing Program document exists. If the document exists, set M1 equal to 1. If it does not exist, set M1 equal to 0 and skip the remaining operations.
2. Manually review the Penetration Testing Program document to determine if it addresses a full scope of blended attacks (including wireless, client-based, and web application). If the document adequately addresses a full scope of attacks, set M2 equal to 1. If it does not, set M2 equal to 0.

24.1.4 Measures

- M1 = Boolean value indicating if the Penetration Testing Program document exists; 1 if it exists, 0 otherwise
- M2 = Boolean value indicating if the Penetration Testing Program document adequately addresses a full scope of attacks; 1 if it does, 0 otherwise

24.1.5 Metrics

Metric	
	Does a penetration testing program document exist and adequately address a full scope of attacks?
Calculation	:code:` M1 AND M2`

24.2 20.2: Conduct Regular External and Internal Penetration Tests

Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

24.2.1 Dependencies

- Sub-control 20.1: Establish a Penetration Testing Program

24.2.2 Inputs

1. Penetration Testing Report for most recent external penetration test
2. Penetration Testing Report for most recent internal penetration test
3. Penetration Testing Program document

24.2.3 Operations

1. **Examine the Penetration Testing Reports (Inputs 1 and 2) to determine the dates that the most recent penetration tests of each type (external and internal) occurred. Examine the Penetration Testing Program document (Input 3) to determine how frequently the organization is required to conduct external and internal penetration tests, and use those required time frames to determine:**
    1. if the most recent external penetration test was within the required time frame (M1)
    2. if the most recent internal penetration test was within the required time frame (M2)
2. Manually review the Penetration Testing Reports to confirm that they contain any discovered vulnerabilities and attack vectors that can be used to successfully exploit the organization's systems (M3); or, if none were successful, verify that the documentation describes those that were attempted but were unsuccessful.

24.2.4 Measures

- M1 = Boolean value indicating if the most recent external penetration test was within the required time frame; 1 if so, 0 otherwise
- M2 = Boolean value indicating if the most recent internal penetration test was within the required time frame; 1 if so, 0 otherwise
- M3 = Boolean value indicating if the Penetration Testing Reports contain discovered vulnerabilities and attack vectors that were successful against the organization's systems; 1 if so, 0 otherwise

24.2.5 Metrics

Penetration Testing Reports

Metric	Are both internal and external penetration tests conducted regularly?
Calculation	`M1 AND M2`

Vulnerability Discovery

Metric	Do penetration testing reports document discovered vulnerabilities?
Calculation	`M3`

24.3 20.3: Perform Periodic Red Team Exercises

Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

Asset Type	Security Function	Implementation Groups
N/A	N/A	3

24.3.1 Dependencies

- Sub-control 20.1: Establish a Penetration Testing Program

24.3.2 Inputs

1. Enterprise penetration test policy

24.3.3 Operations

1. **Examine the enterprise penetration test policy for the following properties:**
    1. Red team exercises are specified to occur periodically
2. Note the periodicity of expected red team exercises
3. Interview security operations personnel to determine the last time a red team exercise was performed

24.3.4 Measures

- M1 = (Boolean) 1 if the enterprise penetration testing policy contains periodicity for red team exercises; 0 otherwise
- M2 = Time of last red team exercise
- M3 = Current time
- M3 = Current time - maximum period between red team exercises
- M4 = (Boolean) 1 if the time of last red team exercise is greater than or equal to M3; 0 otherwise

24.3.5 Metrics

Red Team Exercises

Metric	Are periodic Red Team exercises required by the enterprise's penetration testing policy?
Calculation	`M1`

Frequency

Metric	Was the last Red Team exercise performed within the appropriate time period?
Calculation	`M4`

24.4 20.4: Include Tests for Presence of Unprotected System Information and Artifacts

Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other

information critical to system operation.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

24.4.1 Dependencies

- Sub-control 20.1: Establish a Penetration Testing Program

24.4.2 Inputs

1. Penetration Testing Program document

24.4.3 Operations

1. **Manually review the Penetration Testing Program document (Input 1) to determine if it requires tests to discover the following unprotected system information:**
    1. Network diagrams (M1)
    2. Configuration files (M2)
    3. Penetration test reports (M3)
    4. Emails or documents containing passwords or other information critical to system operation (M4)

24.4.4 Measures

- M1 = Boolean value indicating if the Penetration Testing Program document requires tests to discover unprotected network diagrams; 1 if so, 0 otherwise
- M2 = Boolean value indicating if the Penetration Testing Program document requires tests to discover unprotected configuration files; 1 if so, 0 otherwise
- M3 = Boolean value indicating if the Penetration Testing Program document requires tests to discover unprotected penetration test reports; 1 if so, 0 otherwise
- M4 = Boolean value indicating if the Penetration Testing Program document requires tests to discover unprotected emails or documents containing passwords or other critical system information; 1 if so, 0 otherwise

24.4.5 Metrics

Coverage

Metric	Does the Penetration Testing Program Includes Tests for the Presence of Unprotected System Information and Artifacts?
Calculation	`(M1 + M2 + M3 + M4) / 4`

24.5 20.5: Create a Test Bed for Elements Not Typically Tested in Production

Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

24.5.1 Dependencies

- Sub-control 20.1: Establish a Penetration Testing Program

24.5.2 Inputs

1. List of penetration tests and Red Team attacks and associated elements that are not typically tested in production (i.e. SCADA systems)
2. Description of test bed(s) that have been setup to mimic these production environments

24.5.3 Operations

1. **For each penetration test and Red Team attack in Input 1, manually review the Inputs to see that there is at least one appropriate test bed in Input 2 to cover that test or attack.**
    1. Those tests/attacks that have at least one matching test bed will be included in list M1
    2. Those tests/attacks that do not have at least one matching test bed will be included in list M2

24.5.4 Measures

- M1 = List of penetration tests and Red Team attacks that have at least one matching test bed
- M2 = List of penetration tests and Red Team attacks that do not have at least one matching test bed
- M3 = Count of tests/attacks that do have a matching test bed (count of M1)
- M4 = Total count of tests/attacks in Input 1

24.5.5 Metrics

Coverage

Metric	
	The ratio of tests/attacks not typically tested in production that have a matching test bed
Calculation	`M3 / M4`

24.6 20.6: Use Vulnerability Scanning and Penetration Testing Tools in Concert

Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

24.6.1 Dependencies

- Sub-control 20.1: Establish a Penetration Testing Program

24.6.2 Inputs

1. Penetration Testing Program document

24.6.3 Operations

1. Manually review the Penetration Testing Program document (Input 1) to verify that it instructs the organization to use vulnerability scan results to inform penetration testing efforts. The presence or absence of this instruction becomes M1.

24.6.4 Measures

- M1 = Boolean value indicating if the Penetration Testing Program document includes instructions for using vulnerability scan results to inform penetration testing efforts; 1 if instructions are included, 0 otherwise.

24.6.5 Metrics

Presence

Metric	Presence or absence of instructions to use vulnerability scan results to inform penetration testing efforts
Calculation	`M1`

24.7 20.7: Ensure Results From Penetration Test Are Documented Using Open, Machine-Readable Standards

Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.

Asset Type	Security Function	Implementation Groups
N/A	N/A	3

24.7.1 Dependencies

- Sub-control 20.1: Establish a Penetration Testing Program

24.7.2 Inputs

1. Enterprise red team policy
2. Latest red team result documentation

24.7.3 Operations

1. **Examine the enterprise red team policy for the following properties:**
    1. Red team documentation is machine-readable
    2. Red team documentation is based on open specification
    3. Red team results must be scored to support ongoing comparison
2. **Examine the latest red team results documentation to verify**
    1. Documentation is machine-readable
    2. Documentation is based on open specification
    3. Current score was compared to previous score

24.7.4 Measures

- M1 = (Boolean) 1 if the Policy demands machine-readable red team results documentation; 0 otherwise
- M2 = (Boolean) 1 if the Policy demands open specification for machine-readable results; 0 otherwise
- M3 = (Boolean) 1 if the Policy demands results to be scored to support ongoing comparison; 0 otherwise
- M4 = (Boolean) 1 if the Last red team results are machine-readable; 0 otherwise
- M5 = (Boolean) 1 if the Last red team results are based on an open specification; 0 otherwise
- M6 = (Boolean) 1 if the Last red team results includes current and previous score for comparison. In the event the current score is the result of the enterprise's first red team exercise, this can be set to 1; 0 otherwise

24.7.5 Metrics

Policy Conformance

Metric	
	Is the enterprise's Red Team policy specified to produce results using open, machine readable standards, and is scoring designed to facilitate ongoing comparison?
Calculation	`M1 AND M2 AND M3`

Operational Conformance

Metric	
	Is the enterprise's Red Team policy being practiced operationally?
Calculation	`M4 AND M5 AND M6`

24.8 20.8: Control and Monitor Accounts Associated With Penetration Testing

Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

24.8.1 Dependencies

- Sub-control 16.6: Maintain an Inventory of Accounts
- Sub-control 20.1: Establish a Penetration Testing Program

24.8.2 Inputs

1. The historical inventory of user and system accounts (prior to input 3)
2. The current inventory of user and system accounts (after input 4)
3. The timestamp for the beginning of the most recent penetration testing period
4. The timestamp for the ending of the most recent penetration testing period

24.8.3 Operations

1. Enumerate historical user and system accounts (Input 1) and note any privileges specifically assigned for penetration testing (M1)
2. Enumerate the current user and system accounts and privileges for those accounts determined in Operation 1

24.8.4 Measures

- M1 = The list of historical user and system accounts authorized for use in penetration testing
- M2 = Count of historical user and system accounts authorized for use in penetration testing (count of M1)
- M3 = The list of current user and system accounts that were authorized for use in penetration testing
- M4 = Count of current user and system accounts that were authorized for use in penetration testing (count of M3)
- M5 = The list of current user and system accounts with penetration testing privileges still assigned
- M6 = Count of current user and system accounts with penetration testing privileges still assigned (count of M5)

24.8.5 Metrics

Privileged Accounts Remain

Metric	
	If `M5 > 0`, then privileged user accounts remain following the penetration testing period.
Calculation	`M5 > 0`