CIS Control 12: Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices in order to prevent attackers from exploiting vulnerable network services and access points.

Why is this CIS Control Critical?

Secure network infrastructure is an essential defense against attacks. This includes an appropriate security architecture, addressing vulnerabilities that are, often times, introduced with default settings, monitoring for changes, and reassessment of current configurations. Network infrastructure includes devices such as physical and virtualized gateways, firewalls, wireless access points, routers, and switches.

Default configurations for network devices are geared for ease of deployment and ease-of-use -- not security. Potential default vulnerabilities include open services and ports, default accounts and passwords (including service accounts), support for older vulnerable protocols, and pre-installation of unneeded software. 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 data while in transmission.

Network security is a constantly changing environment that necessitates regular re-evaluation of architecture diagrams, configurations, access controls, and allowed traffic flows. Attackers take advantage of network device configurations becoming less secure over time as users demand exceptions for specific business needs. Sometimes, the exceptions are deployed but not removed when they are no longer applicable to the business's needs. In some cases, the security risk of an exception is neither properly analyzed nor measured against the associated business need and can change over time.

12.1: Ensure Network Infrastructure is Up-to-Date

Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of the software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

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

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. `GV1`: Enterprise asset inventory
2. Authoritative source of latest version information

3. Date of last review of network infrastructure

Operations

1. Use `GV1` to identify and enumerate assets that are part of the network infrastructure `GV35` (M1)

2. Compare the network infrastructure asset version to the version in Input 2

    1. Identify and enumerate assets that match the most recent version (M2)
    2. Identify and enumerate assets that don't match the most recent version (M3)

3. Compare Input 3 to the current date and capture the timeframe in days (M4)

Measures

- M1 = Count of network infrastructure assets
- M2 = Count of network infrastructure assets up to date
- M3 = Count of network infrastructure assets not up to date
- M4 = Timeframe since the last review of network infrastructure

Metrics

- If M4 is greater than thirty days, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

Metric	**The percentage of network infrastructure assets that are up to date**
Calculation	`M2 / M1`

12.2: Establish and Maintain a Secure Network Architecture

Design and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Example implementations will not solely include documentation, but also policy and design components.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

Dependencies

- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)
- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV4`: Enterprise network architecture documentation
2. `GV5`: Authorized software inventory

Operations

1. Use the network architecture `GV4` to identify and enumerate the segments within the enterprise network `GV36` (M1)

2. For each network segment identified in Operation 1, attempt to connect an unauthorized device

    1. Identify and enumerate segments that allow you to connect unauthorized devices (M2)
    2. Identify and enumerate segments that do not allow you to connect unauthorized devices (M3)

3. Use `GV5` to identify authorized availability monitoring software

4. For each network segment identified in Operation 1, determine whether an authorized availability monitoring software from Operation 3 covers the segment

    1. Identify and enumerate segments that are covered by availability monitoring software (M4)
    2. Identify and enumerate segments that are not covered by availability monitoring software (M5)

Measures

- M1 = Count of network segments within the enterprise
- M2 = Count of segments not compliant with least privilege
- M3 = Count of segments compliant with least privilege
- M4 = Count of segments monitored for availability
- M5 = Count of segments not monitored for availability

Metrics

Segmentation

Metric	**If M1 is equal to 1, this metric is measured at a 0. Subsequent metrics can still be assessed.**
Calculation	`If M1 <= 1, Fail or If M1 >= 1, Pass`

Least Privilege

Metric	The percentage of network segments implementing least privilege
Calculation	`M3 / M1`

Availability

Metric	The percentage of network segments monitored for network availability
Calculation	`M4 / M1`

12.3: Securely Manage Network Infrastructure

Securely manage network infrastructure. Example implementations include version-controlled infrastructure-as-code (IaC), and the use of a secure network protocols, such as SSH and HTTPS.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

Inputs

1. `GV36`: Segments within the enterprise network
2. `GV35`: Assets that are part of the network infrastructure
3. `GV37`: Network architecture configuration standards

Operations

1. For each asset in Input 2 `GV35`, use Input 3 `GV37` to check for the use of encrypted sessions

    1. Identify and enumerate assets using encrypted sessions (M2)
    2. Identify and enumerate assets not using encrypted sessions (M3)

2. For each network segment in Input 1 `GV36`, check for the use of infrastructure-as-code

    1. Identify and enumerate network segments that use infrastructure-as-code for the whole segment or partial (M5)
    2. Identify and enumerate network segments that do not use infrastructure-as-code for any portion of the segment (M6)

3. For each network segment identified in Operation 1, use Input 3 `GV37` to determine whether the infrastructure-as-code is managed using version control
    1. Identify and enumerate network segments covered by version-controlled infrastructure-as-code (M7)
    2. Identify and enumerate network segments covered by infrastructure-as-code is not managed through version control (M8)

Measures

- M1 = Count of `GV35` assets that are part of the network infrastructure
- M2 = Count of network infrastructure assets using encrypted sessions
- M3 = Count of network infrastructure assets not using encrypted sessions
- M4 = Count of `GV36` segments within the enterprise network
- M5 = Count of network segments using infrastructure-as-code
- M6 = Count of network segments not using infrastructure-as-code
- M7 = Count of network segments covered by version-controlled infrastructure-as-code
- M8 = Count of network segments covered by unmanaged infrastructure-as-code

Metrics

Encrypted Session Coverage

Metric	The percentage of network infrastructure assets using encrypted sessions
Calculation	`M2 / M1`

Infrastructure-As-Code Coverage

Metric	The percentage of network segments covered by version-controlled infrastructure-as-code
Calculation	`M7 / M4`

12.4: Establish and Maintain Architecture Diagram(s)

Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Documentation	Govern	2, 3

Dependencies

- None

Inputs

1. GV4: Enterprise network architecture documentation
2. Date of last review or update to documentation

Operations

1. Determine if Input 1 GV4 exists within the enterprise
    1. If the network architecture documentation exists, M1 = 1
    2. If the network architecture documentation does not exist, M1 = 0
2. Compare Input 2 to the current date. Capture the timeframe in months.

Measures

- M1 = Output of Operation 1.
- M2 = Timeframe in months of the last review or update to the documentation

Metrics

- If M1 is not provided or available, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.
- If M2 is greater than twelve months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

12.5: Centralize Network Authentication, Authorization, and AuCentralize network AAA

Centralize network AAA.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. GV5: Authorized Software Inventory
2. GV35: Assets that are part of the network infrastructure

Operations

1. Use Input 1 `GV5` to identify and enumerate all AAA services within the enterprise `GV38` (M1)
2. For each centralized AAA point identified in Operation 1, determine whether it is necessary or can be consolidated
    1. Identify and enumerate authentication points that are unnecessary or can be consolidated (M2)
    2. Identify and enumerate authentication points that are necessary and cannot be consolidated (M3)
3. Use the output of Operation 1 to check if each asset in Input 2 `GV35` is covered by at least one AAA system
    1. Identify and enumerate network infrastructure assets that are covered by at least one AAA system (M4)
    2. Identify and enumerate network infrastructure assets that are not covered by an AAA system (M5)

Measures

- M1 = Count of AAA services within the enterprise
- M2 = Count of unnecessary AAA services
- M3 = Count of necessary AAA services
- M4 = Count of network infrastructure covered by AAA services
- M5 = Count of network infrastructure not covered by AAA services
- M6 = Count of `GV35`

Metrics

Centralized AAA

Metric	**Percentage of properly centralized AAA services**
Calculation	`M3 / M1`

Network Coverage

Metric	**Percentage of network infrastructure assets managed through AAA**
Calculation	`M4 / M6`

12.6: Use of Secure Network Management and Communication Protocols

Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

Dependencies

- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Safeguard 12.2: Establish and Maintain a Secure Network Architecture

Inputs

1. `GV36`: Segments within the enterprise network
2. `GV37`: Network infrastructure configuration standards
3. Authorized list of secure network management and communication protocols

Operations

1. For each network segment in Input 1 `GV36`, use Input 3 to identify communication protocols

    1. Identify and enumerate segments using only communication protocols on the authorized list (M2)
    2. Identify and enumerate segments using communication protocols not on the authorized list (M3)

2. For each communication protocol identified in Operation 1.1, check configuration standards `GV37`

    1. Identify and enumerate segments using properly configured communication protocols (M4)
    2. Identify and enumerate segments using improperly configured communication protocols (M5)

3. For each network segment in Input 1 `GV36`, use Input 3 to identify network management protocols

    1. Identify and enumerate segments using only network management protocols on the authorized list (M6)
    2. Identify and enumerate segments using network management protocols not on the authorized list (M7)

4. For each communication protocol identified in Operation 1.1, check configuration standards `GV37`

5. Identify and enumerate segments using properly configured network management protocols (M8)
6. Identify and enumerate segments using improperly configured network management protocols (M9)

Measures

- M1 = Count of `GV36`
- M2 = Count of segments using authorized communication protocols
- M3 = Count of segments using unauthorized communication protocols
- M4 = Count of segments using properly configured authorized communication protocols
- M5 = Count of segments using improperly configured authorized communication protocols
- M6 = Count of segments using unauthorized network management protocols
- M7 = Count of segments using unauthorized network management protocols
- M8 = Count of segments using properly configured authorized network management protocols
- M9 = Count of segments using improperly configured authorized network management protocols

Metrics

Communication Protocol Coverage

Metric	**The percentage of network segments using properly configured and authorized communication protocols**
Calculation	`M4 / M1`

Network Management Protocol Coverage

Metric	**The percentage of network segments using properly configured and authorized network management protocols**
Calculation	`M8 / M1`

12.7: Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure

Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 12.5: Centralize Network Authentication, Authorization, and Auditing (AAA)

Inputs

1. `GV1`: Enterprise Asset Inventory
2. `GV5`: Authorized Software Inventory
3. `GV38`: AAA services within the enterprise
4. `GV37`: Network infrastructure configuration standards

Operations

1. Use Input 1 `GV1` to identify and enumerate remote enterprise assets `GV39` (M1)

2. Use Input 1 `GV1` and Input 2 `GV5` to identify and enumerate all VPN devices and software (M2)

3. Use the output of Operation 2 and Input 4 `GV37` to check the configuration of the VPN

    1. Identify and enumerate VPN devices and software properly configured to require authentication prior to granting access (M3)
    2. Identify and enumerate VPN devices and software not properly configured to require authentication prior to granting access (M4)

4. For each asset identified in Operation 1, check if is covered by a VPN device or software identified in Operation 3.1

    1. Identify and enumerate assets that are covered by a VPN (M5)
    2. Identify and enumerate assets that are not covered by a VPN (M6)

5. Use Input 3 `GV38` and Input 4 `GV37` to check configuration of AAA services

    1. Identify and enumerate AAA services properly configured to require authentication prior to granting access (M7)
    2. Identify and enumerate AAA services not properly configured to require authentication prior to granting access (M8)

6. For each asset identified in Operation 1, check if it is covered by an AAA service identified in Operation 5.1

    1. Identify and enumerate assets that are covered by an AAA service (M9)
    2. Identify and enumerate assets that are not covered by an AAA service (M10)

7. Compare the output of Operation 4.1 and 6.1

    1. Identify and enumerate assets covered by both VPN and AAA (M1)

Measures

- M1 = Count of remote enterprise assets
- M2 = Count of VPN devices and software
- M3 = Count of properly configured VPN devices and software
- M4 = Count of improperly configured VPN devices and software
- M5 = Count of remote assets covered by a properly configured VPN
- M6 = Count of remote assets not covered by a properly configured VPN
- M7 = Count of properly configured AAA services
- M8 = Count of improperly configured AAA services
- M9 = Count of remote assets covered by a properly configured AAA service

- M10 = Count of remote assets not covered by a properly configured AAA service
- M11 = Count of remote assets covered by both VPN and AAA
- M12 = Count of AAA services within the enterprise

Metrics

VPN Compliance

Metric	The percentage of properly configured VPN devices and software
Calculation	`M3 / M2`

AAA Compliance

Metric	The percentage of properly configured AAA services
Calculation	`M7 / M12`

Coverage

Metric	The percentage of remote assets using VPN and AAA
Calculation	`M11 / M1`

12.8: Establish and Maintain Dedicated Computing Resources for All Administrative Work

Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

Inputs

1. `GV1`: Enterprise Asset Inventory
2. `GV37`: Network infrastructure configuration standards

Operations

1. Use Input 1 `GV1` to identify and enumerate assets used for administrative purposes (M1)

2. For each asset identified in Operation 1, use Input 2 `GV37` to check configurations

    1. Identify and enumerate assets that do not have internet access (M2)
    2. Identify and enumerate assets that have internet access (M3)
    3. Identify and enumerate assets that are physically or logically separated from the primary network (M4)
    4. Identify and enumerate assets that are not physically or logically separated from the primary network (M5)

3. Compare the output of Operation 2.1 and 2.3

    1. Identify and enumerate assets that do not have internet access and are physically or logically separated (M6)

Measures

- M1 = Count of assets used for administrative purposes
- M2 = Count of assets configured to not allow internet access
- M3 = Count of assets configured to allow internet access
- M4 = Count of assets physically or logically separated from the primary network
- M5 = Count of assets not physically or logically separated from the primary network
- M6 = Count of assets configured to not allow internet access and are physically or logically separated

Metrics

Compliance

Metric	**The percentage of properly configured administrative assets**
Calculation	`M6 / M1`