CIS Control 13: Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Why is this CIS Control Critical?

We cannot rely on network defenses to be perfect. Adversaries continue to evolve and mature as they share or sell information among their community on exploits and bypasses security controls. Even if security tools work "as advertised," it takes an understanding of the enterprise risk posture to configure, tune, and log them to be effective. Often, misconfigurations due to human error or lack of knowledge of tool capabilities give enterprises a false sense of security.

Security tools can only be effective if they support a process of continuous monitoring that allows staff the ability to be alerted and respond to security incidents quickly. Enterprises that adopt a purely technology-driven approach will also experience more false positives due to their over-reliance on alerts from tools. Identifying and responding to these threats requires visibility into all threat vectors of the infrastructure and leveraging humans in the process of detection, analysis, and response. It is critical for large or heavily targeted enterprises to have a security operations capability to prevent, detect, and quickly respond to cyber threats before they can impact the enterprise. This process will generate activity reports and metrics that will help enhance security policies and support regulatory compliance for many enterprises.

As we have seen many times in the press, enterprises have been compromised for weeks, months, or years before discovery. The primary benefit of having comprehensive situational awareness is to increase the speed of detection and response. This is critical to respond quickly when malware is discovered, credentials are stolen, or when sensitive data is compromised to reduce impact on the enterprise.

Through good situational awareness (i.e., security operations), enterprises will identify and catalog Tactics, Techniques, and Procedures (TTPs) of attackers, including their IOCs, that will help the enterprise become more proactive in identifying future threats or incidents. Recovery can be achieved faster when the response has access to complete information about the environment and enterprise structure to develop efficient response strategies.

13.1: Centralize Security Event Alerting

Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of an SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. Location of `GV42`: log correlation or log analytic tool
2. `GV1`: Enterprise asset inventory

Operations

1. Check if Input 1 exists within the enterprise

    1. If Input 1 exists, M1 = 1

    2. 1. If Input 1 does not exist, M1 = 0

2. Use `GV1` to identify and enumerate enterprise assets that produce security event logs (M2)

3. For every asset identified in Operation 2, check if logs are centralized at the location of the log correlation or log analytic tool Input 1

    1. Identify and enumerate assets whose logs are centralized (M3)
    2. Identify and enumerate assets whose logs are not centralized (M4)

Measures

- M1 = Output of Operation 1
- M2 = Count of assets that produce security event logs
- M3 = Count of assets with security event logs being centralized
- M4 = Count of assets with security event logs not being centralized

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.

Coverage

Metric	The percentage of assets whose security logs are centralized
Calculation	`M3 / M2`

13.2: Deploy a Host-Based Intrusion Detection Solution

Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory

Operations

1. Use `GV1` to identify and enumerate assets capable of supporting host based intrusion detection systems (M1)

2. Use: `GV5` to identify authorized host-based intrusion detection software

3. For each asset identified in Operation 1, check if it is covered by at least one authorized host-based intrusion detection software

    1. Identify and enumerate assets with host-based intrusion detection software installed (M2)
    2. Identify and enumerate assets without host-based intrusion detection software installed (M3)

Measures

- M1 = Count of enterprise assets capable of supporting host-based intrusion detection systems
- M2 = Count of assets with host-based intrusion detection systems
- M3 = Count of assets without host-based intrusion detection systems

Metrics

Coverage

Metric	**The percentage of assets capable of supporting host-based intrusion detection systems with host-based intrusion detection software installed**
Calculation	`M2 / M1`

13.3: Deploy a Network Intrusion Detection Solution

Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

Inputs

1. `GV35`: Assets that are part of the network infrastructure
2. `GV4`: Enterprise Network Architecture Documentation

Operations

1. Use Input 1 `GV35` to identify the network intrusion detection solutions for the enterprise

2. Use Input 2 `GV4` to identify and enumerate network boundaries (M1)

3. For each network boundary identified in Operation 2, determine whether it is covered by at least one network intrusion detection solution

    1. Identify and enumerate boundaries covered by at least one network intrusion detection solution (M2)
    2. Identify and enumerate boundaries not covered by at least one network intrusion detection solution (M3)

Measures

- M1 = Count of network boundaries
- M2 = Count of network boundaries covered by a network intrusion detection solution
- M3 = Count of network boundaries not covered by a network intrusion detection solution

Metrics

Coverage

Metric	**The percentage of network boundaries covered by network intrusion detection solutions**
Calculation	`M2 / M1`

13.4: Perform Traffic Filtering Between Network Segments

Perform traffic filtering between network segments, where appropriate.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

Dependencies

- None

Inputs

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

Operations

1. Use Input 1 `GV36` to identify and enumerate network segments that require communication with other network segments (M1)

2. For each network segment identified in Operation 1, use Input 2 `GV35` to identify network infrastructure assets responsible for traffic filtering

3. For each network infrastructure asset identified in Operation 1, check configurations using Input 3 `GV37` to determine whether each segment is properly configured to filter traffic

    1. Identify and enumerate network segments with properly configured filtering assets (M2)
    2. Identify and enumerate network segments with improperly configured filtering assets (M3)

Measures

- M1 = Count of network segments that communicate with other networks segments
- M2 = Count of network segments with properly configured filtering assets
- M3 = Count of network segments with improperly configured filtering assets

Metrics

Coverage

Metric	The percentage of network segments properly configured to filter traffic between segments
Calculation	`M2 / M1`

13.5: Manage Access Control for Remote Assets

Manage access control for assets remotely connecting to enterprise resources. Determine the amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process and ensure the operating system and applications are up-to-date.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

Inputs

1. `GV23`: Authentication and Authorization System Inventory
2. `GV3`: Configuration Standard
3. `GV39`: Remote enterprise assets

Operations

1. Use Input 1 `GV23` to identify and enumerate authorization systems that allow remote logins (M1)

2. For each authorization system identified in Operation 1, use Input 2 `GV3` to check if the configuration for each type of policy

    1. Identify and enumerate authorization systems properly configured for all the policies (M2)
    2. Identify and enumerate authorization systems for which at least one configuration does not comply with the policies (M3)

3. For each remote enterprise asset from Input 3 `GV39`, compared to the output of Operation 2.1

1. Identify and enumerate assets that are covered by at least one compliant authorization system (M4)
2. Identify and enumerate assets that are not covered by a compliant authorization system (M5)

Measures

- M1 = Count of authorization systems that allow remote logins
- M2 = Count of authorization systems properly configured to comply with policies
- M3 = Count of authorization systems not properly configured to comply with policies
- M4 = Count of remote enterprise assets covered by a compliant authorization system
- M5 = Count of remote enterprise assets not covered by a compliant authorization system
- M6 = Count of remote enterprise assets `GV39`

Metrics

Authorization System Compliance

Metric	**The percentage of properly configured authorization systems that allow remote login**
Calculation	`M2 / M1`

Coverage

Metric	**The percentage of remote enterprise assets covered by compliant authorization systems**
Calculation	`M4 / M6`

13.6: Collect Network Traffic Flow Logs

Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

Asset Type	Security Function	Implementation Groups
Network	Detect	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. `GV35`: Assets that are part of the network infrastructure
2. `GV37`: Network infrastructure configuration standards

Operations

1. Use Input 1 `GV35` to identify and enumerate network boundary assets (M1)

2. For each network boundary asset identified in Operation 1, check configuration `GV37` to determine if network traffic or network traffic flow logging is enabled

    1. Identify and enumerate assets with either network traffic flow or network traffic logging enabled (M2)
    2. Identify and enumerate assets that have neither network traffic flow nor network traffic logging enabled (M3)

Measures

- M1 = Count of network boundary assets
- M2 = Count of properly configured network boundary assets
- M3 = Count of improperly configured network boundary assets

Metrics

Coverage

Metric	**The percentage of network boundary assets properly configured to log network traffic flow or network traffic**
Calculation	`M2 / M1`

13.7: Deploy a Host-Based Intrusion Prevention Solution

Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include the use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory

Operations

1. Use `GV1` to identify and enumerate assets capable of supporting host-based intrusion prevention systems (M1)

2. Use: `GV5` to identify authorized host-based intrusion prevention software

3. For each asset identified in Operation 1, check if it is covered by at least one authorized host-based intrusion prevention software

    1. Identify and enumerate assets with host-based intrusion prevention software installed (M2)
    2. Identify and enumerate assets without host-based intrusion prevention software installed (M3)

Measures

- M1 = Count of enterprise assets capable of supporting host-based intrusion prevention systems
- M2 = Count of assets with host-based intrusion prevention systems
- M3 = Count of assets without host-based intrusion prevention systems

Metrics

Coverage

Metric	**The percentage of assets capable of supporting host-based intrusion prevention systems with software installed**
Calculation	`M2 / M1`

13.8: Deploy a Network Intrusion Prevention Solutions

Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

Inputs

1. `GV35`: Assets that are part of the network infrastructure
2. `GV40`: Network Boundaries

Operations

1. Use Input 1 `GV35` to identify the network intrusion prevention solutions for the enterprise

2. For each network boundary identified in Input 2, determine whether it is covered by at least one network intrusion prevention solution

    1. Identify and enumerate boundaries covered by at least one network intrusion prevention solution (M2)
    2. Identify and enumerate boundaries not covered by at least one network intrusion prevention solution (M3)

Measures

- M1 = Count of network boundaries `GV40`
- M2 = Count of network boundaries covered by a network intrusion prevention solution
- M3 = Count of network boundaries not covered by a network intrusion prevention solution

Metrics

Coverage

Metric	The percentage of network boundaries covered by network intrusion prevention solutions
Calculation	`M2 / M1`

13.9: Deploy Port-Level Access Control

Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. `GV5`: Authorized Software Inventory
2. `GV38`: AAA services within the enterprise
3. `GV41`: List of CMDB servers
4. `GV35`: Assets that are part of the network infrastructure
5. `GV37`: Network infrastructure configuration standards

Operations

1. If the enterprise uses an 802.1x network design to control network access:

    1. Use Input 1 `GV5` to identify and enumerate 802.1x authenticators

2. For each authenticator identified in Operation 1, use Input 5 `GV37` to check configurations

    1. Identify and enumerate properly configured authenticators (M2)
    2. Identify and enumerate improperly configured authenticators (M3)

3. Use Input 2 `GV38` to identify 802.1x authentication servers (M4)

4. For each authentication server identified in Operation 3, use Input 5 ``GV37`to check configurations to ensure a connection to at least one CMDB server from Input 3:code:`GV41``

    1. Identify and enumerate properly configured authentication servers (M5)
    2. Identify and enumerate improperly configured authentication servers (M6)

5. If the enterprise does not use 802.1x network design to control network access:

    1. For each asset in Input 4 `GV35`, use Input 5 `GV37` to check client authentication certificate configuration

        1. Identify and enumerate properly configured assets (M8)
        2. Identify and enumerate improperly configured assets (M9)

Measures

- M1 = Count of 802.1x authenticators
- M2 = Count of 802.1x properly configured authenticators
- M3 = Count of 802.1x improperly configured authenticators
- M4 = Count of 802.1x authentication servers
- M5 = Count of 802.1x properly configured authentication servers
- M6 = Count of 802.1x improperly configured authentication servers
- M7 = Count of Input 4 `GV35`
- M8 = Count of assets properly configured for client authentication certificates
- M9 = Count of assets improperly configured for client authentication certificates

Metrics

- If the enterprise uses an 802.1x network design to control network access:

Authenticator Coverage

Metric	The percentage of properly configured authenticators
Calculation	`M2 / M1`

Authentication Server Coverage

Metric	The percentage of properly configured authentication servers
Calculation	`M5 / M4`

- If the enterprise does not use 802.1x network design to control network access:

Client Authentication Certificate Coverage

Metric	The percentage of assets properly configured for authentication certificate coverage
Calculation	`M8 / M7`

13.10: Perform Application Layer Filtering

Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

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

Operations

1. Use Input 2 `GV5` to identify software used for application layer filtering

2. For each asset in Input 1 `GV35, determine whether it is covered by at least one software identified in Operation 1

    1. Identify and enumerate assets covered by application layer filtering software (M2)
    2. Identify and enumerate assets not covered by application layer filtering software (M3)

Measures

- M1 = Count of network infrastructure assets
- M2 = Count of network infrastructure assets covered by the application layer filtering software
- M3 = Count of network infrastructure assets not covered by application layer filtering software

Metrics

Coverage

Metric	The percentage of network infrastructure assets covered by application layering software
Calculation	`M2 / M1`

13.11: Tune Security Event Alerting Thresholds

Tune security event alerting thresholds monthly, or more frequently.

Asset Type	Security Function	Implementation Groups
Network	Detect	3

Dependencies

- Safeguard 13.1: Centralize Security Event Alerting

Inputs

1. Date of last tuning of security event alert thresholds of `GV42` Log correlation or log analytic tool

Operations

1. Compare Input 1 to the current date and capture the timeframe in days

Measures

- M1 = Timeframe in days since the last tuning of security event alert thresholds for log correlation or log analytic tool

Metrics

- If M1 is greater than thirty days, then this Safeguard is measured at a 0 and receives a failing score.