CIS Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities in all enterprise assets within the enterprise's infrastructure in order to remediate, and minimize the window of opportunity for attackers. Monitor public and private industry sources for new threats and vulnerability information.

Why is this CIS Control Critical?

Cyber defenders are constantly being challenged by attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Attackers have access to the same information and can often take advantage of vulnerabilities more quickly than an enterprise can remediate. While there is a gap in time from a vulnerability being known to when it is patched, defenders can prioritize which vulnerabilities are most impactful to the enterprise or likely to be exploited first due to ease of use. For example, when researchers or the community report new vulnerabilities, vendors have to develop and deploy patches, indicators of compromise (IOCs), and updates. Defenders need to assess the risk of the new vulnerability to the enterprise, regression-test patches, and install the patch.

There is never perfection in this process. Attackers might be using an exploit to a vulnerability that is not known within the security community. They might have developed an exploit to this vulnerability, referred to as a "zero-day" exploit. Once the vulnerability is known in the community, the process mentioned above starts. Therefore, defenders must keep in mind that an exploit might already exist when the vulnerability is widely socialized. Sometimes vulnerabilities might be known within a closed community (e.g., vendor still developing a fix) for weeks, months, or years before it is disclosed publicly. Defenders have to be aware that there might always be vulnerabilities they cannot remediate and, therefore, need to use other controls to mitigate.

Enterprises that do not assess their infrastructure for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their enterprise assets compromised. Defenders face particular challenges in scaling remediation across an entire enterprise and prioritizing actions with conflicting priorities while not impacting the enterprise's business or mission.

7.1: Establish and Maintain a Vulnerability Management Process

Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Documentation	Govern	1, 2, 3

Dependencies

- None

Inputs

1. Enterprise vulnerability management process.
2. Date of the last update to the vulnerability management process.

Operations

1. Determine whether the enterprise maintains a vulnerability management process:
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0
2. Compare the date from Input 1 to the current date and enumerate the timeframe in months (M2)

Measures

- M1 = Output of Operation 1.
- M2 = Timeframe since the last update to the vulnerability management process.

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M2 is greater than twelve, this Safeguard receives a failing score. The other metrics don't apply.

7.2: Establish and Maintain a Remediation Process

Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

Asset Type	Security Function	Implementation Groups
Documentation	Govern	1, 2, 3

Dependencies

- None

Inputs

1. Enterprise remediation strategy process.
2. Date of the last review of the process.

3. `GV18`: Enterprise assets storing, processing, and transmitting sensitive data.

Operations

1. Determine whether the enterprise maintains a documented remediation process:
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0
2. Check the documented remediation process to identify whether it includes a risk-based process based on the following elements: Sensitive assets `GV18` and criticality of vulnerability:
    1. Each element, if included, gets a value of 1. Sum all elements (M2)
3. Compare the date from Input 2 and the current date. Enumerate the timeframe in terms of days (M3)

Measures

- M1 = Output of Operation 1.
- M2 = Sum of elements included in the remediation process.
- M3 = Timeframe since the last review of the process in days.

Metrics

- If M1 is 0, the Safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than thirty, the Safeguard receives a failing score. The other metrics don't apply.

Completeness

Metric	**The percentage of elements included in the process**
Calculation	`M2 / 2`

7.3: Perform Automated Operating System Patch Management

Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

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

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. GV5: Authorized software inventory.
2. GV1: Enterprise asset inventory.
3. Authoritative source of information indicating version details by product.
4. GV3: Configuration standards.

Operations

1. Use GV5 to identify authorized operating systems within the enterprise.

2. Use GV1 and the output of Operation 1 to identify the operating system currently running on each asset (M1).

3. For each asset, compare the version of the operating system to that listed in Input 4:

    1. Identify and enumerate operating systems that are up to date (M2).
    2. Identify and enumerate operating systems that are not up to date (M3).

4. For each operating system identified in Operation 2.2, determine whether there is a documented exception:

    1. Identify and enumerate operating systems with a documented exception (M4).
    2. Identify and enumerate operating systems without a documented exception (M5).

5. Use GV5 to identify authorized automated patch management software (M6).

6. Compare the output of Operation 5 and Operation 1:

    1. Identify and enumerate operating systems covered by at least one automated patch management software (M7).
    2. Identify and enumerate operating systems not covered by at least one automated patch management software (M8).

7. Check configurations of automated patch management software identified in Operation 5 using GV3:

    1. Identify and enumerate those configured to run every 30 days or less (M9).
    2. Identify and enumerate those not configured to run every 30 days or less (M10).

Measures

- M1 = Count of the authorized operating systems installed on an asset.
- M2 = Count of up-to-date operating systems installed on an asset.
- M3 = Count of operating systems installed on an asset that is not up-to-date.
- M4 = Count of not up-to-date operating systems with a documented exception.
- M5 = Count of not up-to-date operating systems without a documented exception.
- M6 = Count of authorized automated patch management software.

- M7 = Count of operating systems covered by at least one automated patch management software.
- M8 = Count of operating systems not covered by at least one automated patch management software.
- M9 = Count of automated patch management software properly configured to run every 30 days or less.
- M10 = Count of automated patch management software not properly configured to run every 30 days.

Metrics

Update Effectiveness (Per Asset)

Metric	**The percent of operating systems on an asset that is up-to-date**
Calculation	(M2 + M4) / M1

Update Effectiveness (Organizational)

Calculate the organizational metric by averaging the asset scores.

Coverage of Automation

Metric	**The percent of operating systems covered by at least one automated patch management software**
Calculation	M7 / M1

Scan Compliance

Metric	**The percent of automated patch management software configured to run every 30 days or less**
Calculation	M9 / M6

7.4: Perform Automated Application Patch Management

Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

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

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. GV5: Authorized software inventory.
2. GV1: Enterprise asset inventory.
3. Authoritative source of information indicating version details by product.
4. GV3: Configuration standards.
5. GV24: Authorized automated patch management software.

Operations

1. Use GV5 to identify authorized applications within the enterprise.

2. Use GV1 and the output of Operation 1 to identify the applications currently running on each asset (M1).

3. For each asset, compare the version of the application to that listed in Input 4:

    1. Identify and enumerate applications that are up to date (M2).
    2. Identify and enumerate applications that are not up to date (M3).

4. For each application identified in Operation 2.2, determine whether there is a documented exception:

    1. Identify and enumerate applications with a documented exception (M4).
    2. Identify and enumerate applications without a documented exception (M5).

5. Compare GV24 and Operation 1:

    1. Identify and enumerate applications covered by at least one automated patch management software (M7).
    2. Identify and enumerate applications not covered by at least one automated patch management software (M8).

6. Check configurations of automated patch management software GV24 using GV3:

    1. Identify and enumerate those configured to run every 30 days or less (M9).
    2. Identify and enumerate those not configured to run every 30 days or less (M10).

Measures

- M1 = Count of authorized applications installed on an asset.
- M2 = Count of up-to-date applications installed on an asset.
- M3 = Count of applications installed on an asset that is not up to date.
- M4 = Count of not up to date applications with a documented exception.
- M5 = Count of not up to date applications without a documented exception.
- M6 = Count of GV24 authorized automated patch management software.

- M7 = Count of applications covered by at least one automated patch management software.
- M8 = Count of applications not covered by at least one automated patch management software.
- M9 = Count of automated patch management software properly configured to run every 30 days or less.
- M10 = Count of automated patch management software not properly configured to run every 30 days.

Metrics

Update Effectiveness (Per Asset)

Metric	**The percent of applications on an asset that are up to date**
Calculation	`(M2 + M4) / M1`

Update Effectiveness (Organizational)

Calculate the organizational metric by averaging the asset scores.

Coverage of Automation

Metric	**The percent of operating systems covered by at least one automated patch management software.**
Calculation	`M7 / M1`

1

Scan Compliance

Metric	**The percent of automated patch management software configured to run every 30 days or less.**
Calculation	`M9 / M6`

7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets

Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.

Asset Type	Security Function	Implementation Groups
Software	Identify	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. GV1: Enterprise asset inventory.
2. GV5: Authorized software inventory.
3. GV3: Configuration standard.

Operations

1. Use the GV5authorized software inventory to:
    1. Identify and enumerate GV25 vulnerability scanning software (M1)
    2. Identify and enumerate authenticated vulnerability scanning software (M2)
2. Use the GV1 enterprise asset inventory to identify and enumerate all internal assets (M3)
3. Use the output of Operation 2 and Operation 1.1:
    1. Identify and enumerate internal assets covered by at least one vulnerability scanning software (M4)
    2. Identify and enumerate internal assets not covered by at least one vulnerability scanning software (M5)
4. Use the output of Operation 2 and Operation 1.2:
    1. Identify and enumerate internal assets covered by at least one authenticated vulnerability scanner (M6)
    2. Identify and enumerate internal assets not covered by at least one authenticated vulnerability scanner (M7)
5. Use the output of Operation 1.1 and GV3:
    1. Identify and enumerate vulnerability scanners properly configured to scan every 3 months or less (M8)
    2. Identify and enumerate vulnerability scanners not properly configured to scan every 3 months or less (M9)
6. Use the output of Operation 1.2 and GV3:
    1. Identify and enumerate authenticated vulnerability scanners properly configured to scan every 3 months or less (M10)
    2. Identify and enumerate authenticated vulnerability scanners not properly configured to scan every 3 months or less (M11)

Measures

- M1 = Count of authorized vulnerability scanning software.
- M2 = Count of authorized authenticated vulnerability scanning software.
- M3 = Count of internal enterprise assets.
- M4 = Count of internal assets covered by a vulnerability scanner.
- M5 = Count of internal assets not covered by a vulnerability scanner.
- M6 = Count of internal assets covered by an authenticated vulnerability scanner.
- M7 = Count of internal assets not covered by an authenticated vulnerability scanner.
- M8 = Count of vulnerability scanners properly configured to run every 3 months or less.
- M9 = Count of vulnerability scanners not properly configured to run every 3 months or less.
- M10 = Count of authenticated vulnerability scanners properly configured to run every 3 months or less.
- M11 = Count of authenticated vulnerability scanners not properly configured to run every 3 months or less.

Metrics

Coverage of Vulnerability Scans

Metric	**The percentage of internal assets covered by a vulnerability scanner**
Calculation	`M4 / M3`

Coverage of Authenticated Scans

Metric	**The percentage of internal assets covered by an authenticated vulnerability scanner**
Calculation	`M6 / M3`

Compliance with Vulnerability Scans

Metric	**The percentage of vulnerability scanners properly configured to scan every 3 months or less**
Calculation	`M8 / M1`

Compliance with Authenticated Scans

Metric	**The percentage of authenticated vulnerability scanners properly configured to scan every 3 months or less**
Calculation	`M10 / M2`

7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets

Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.

Asset Type	Security Function	Implementation Groups
Software	Identify	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory.
2. `GV25`: Vulnerability scanning software.
3. `GV3`: Configuration standard.

Operations

1. Use the `GV1` enterprise asset inventory to identify and enumerate all external assets (M2)

2. Use the output of Operation 1 and `GV25` to:

    1. Identify and enumerate external assets covered by at least one vulnerability scanning software (M3)
    2. Identify and enumerate external assets not covered by at least one vulnerability scanning software (M4)

3. Use the `GV25` and `GV3` to:

    1. Identify and enumerate vulnerability scanners properly configured to scan every 30 days or less (M5)
    2. Identify and enumerate vulnerability scanners not properly configured to scan every 30 days or less (M6)

Measures

- M1 = Count of authorized `GV25` vulnerability scanning software.
- M2 = Count of external enterprise assets.
- M3 = Count of external assets covered by a vulnerability scanner.
- M4 = Count of external assets not covered by a vulnerability scanner.
- M5 = Count of vulnerability scanners properly configured to run every 30 days or less.
- M6 = Count of vulnerability scanners not properly configured to run every 30 days or less.

Metrics

Coverage of Vulnerability Scans

Metric	**The percentage of external assets covered by a vulnerability scanner**
Calculation	`M3 / M2`

Compliance with Vulnerability Scans

Metric	**The percentage of vulnerability scanners properly configured to scan every 30 days or less**
Calculation	`M5 / M1`

7.7: Remediate Detected Vulnerabilities

Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

Asset Type	Security Function	Implementation Groups
Software	Respond	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. `GV1`: Enterprise asset inventory.
2. Current vulnerability scan.
3. Previous vulnerability scan.
4. Date of current vulnerability scan.
5. Date of the previous vulnerability scan.

Assumptions

- Asset-vulnerability combinations not found in the most recent scan are indicative of remediation of that vulnerability on that asset.

Operations

1. For each asset in `GV1`, compare Inputs 2 and 3:

1. Identify and enumerate assets listed with the same vulnerability on both scans (M2)
2. Identify and enumerate assets previously found in Input 3 that are no longer listed in Input 2 with the same vulnerability (M3)

2. Compare Inputs 4 and 5 and capture the timeframe between scans in days (M4)

Measures

- M1 = Count of vulnerabilities identified in Input 3
- M2 = Count of unremediated vulnerabilities
- M3 = Count of remediated vulnerabilities
- M4 = Timeframe in between scans

Metrics

Remediation

Metric	**The percentage of remediated vulnerabilities**
Calculation	`M3 / M1`