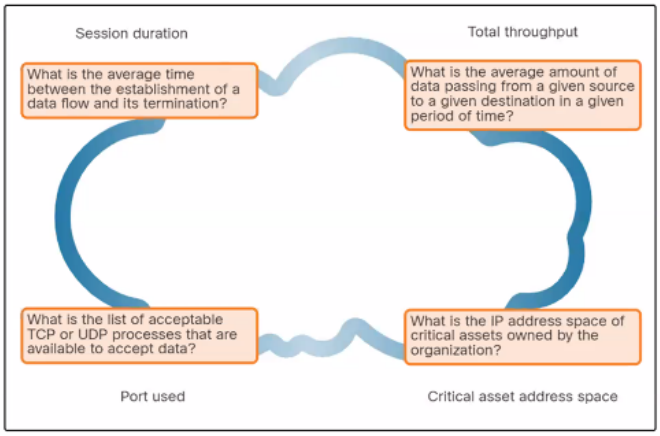
Module 23: Endpoint Vulnerability Assessment

CyberOps Associate v1.0

23.1 Network and Server Profiling

Network Profiling

- Network and device profiling provides statistical baseline information that can serve as a reference point for normal network and device performance.
- Elements of network profile:
  - Session duration
  - Total throughput
  - Critical asset address space
  - Typical traffic type



Elements of a Network Profile

Network and Server Profiling

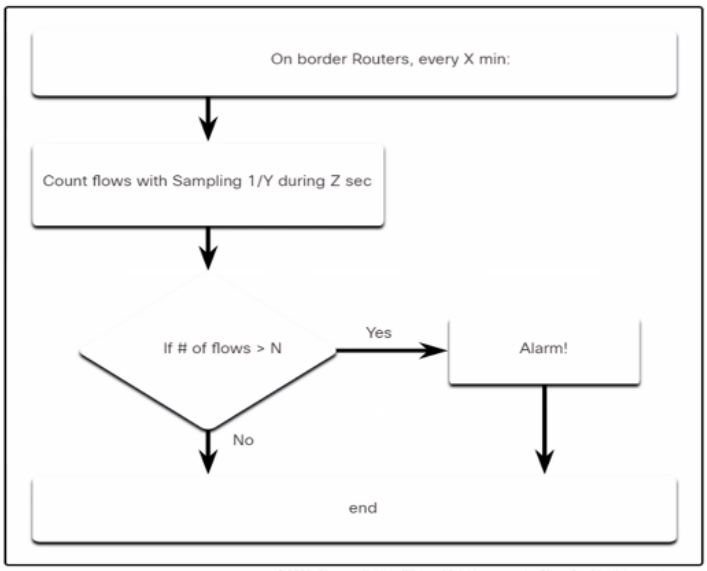
Server Profiling

- A server profile is a security baseline for a given server.
- Server profiling is used to establish the accepted operating state of servers.
- The server profile elements are as follows:
  - Listening ports
  - Logged in users and accounts
  - Service accounts
  - Software environment

Network and Server Profiling

Network Anomaly Detection

- Network behavior is described by a large amount of diverse data such as the features of packet flow, features of the packets themselves, and telemetry from multiple sources.
- Big Data analytics techniques can be used to analyze this data and detect variations from the baseline.
- Anomaly detection can identify infected hosts on the network that are scanning for other vulnerable hosts.
- The figure illustrates a simplified version of an algorithm designed to detect an unusual condition at the border routers of an enterprise.



Network and Server Profiling

Network Vulnerability Testing

- Network Vulnerability Testing includes Risk Analysis, Vulnerability Assessment and Penetration Testing.
- The table lists examples of activities and tools that are used in vulnerability testing:

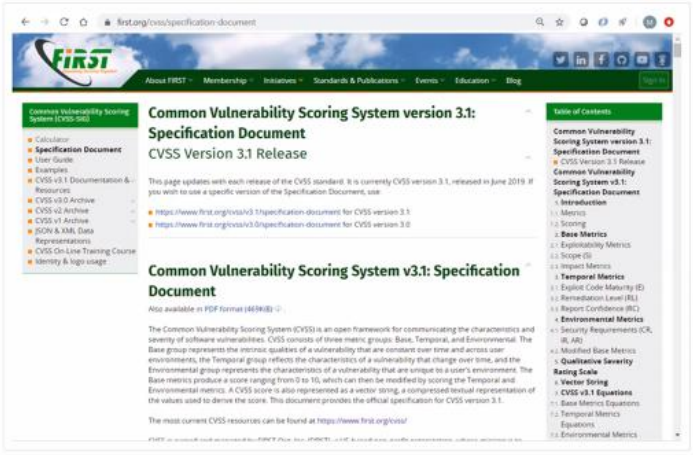
Activity	Description	Tools
Risk analysis	Individuals conduct comprehensive analysis of impacts of attacks on core company assets and functioning	Internal or external consultants, risk management frameworks
Vulnerability Assessment	Patch management, host scans, port scanning, other vulnerability scans and services	OpenVas, Microsoft Baseline Analyzer, Nessus, Qualys, Nmap
Penetration Testing	Use of hacking techniques and tools to penetrate network defenses and identify depth of potential penetration	Metasploit, CORE Impact, ethical hackers

23.2 Common Vulnerability Scoring System (CVSS)

CVSS Overview

CVSS VALORE 0-10

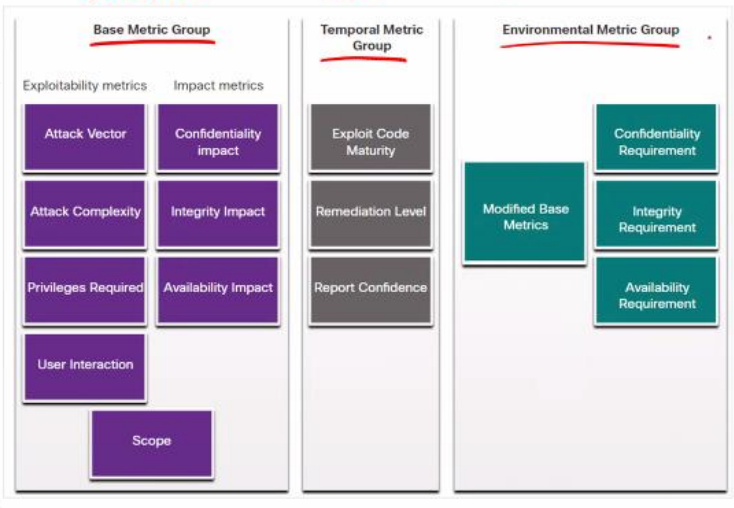
- The Common Vulnerability Scoring System (CVSS) is a risk assessment tool designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems.
- CVSS provides standardized vulnerability scores.
- It provides an open provides an open framework with metrics to all users.
- CVSS helps prioritize risk.
- The Forum of Incident Response and Security Teams (FIRST) has been designated as the custodian of the CVSS to promote its adoption globally.



CVSS Metric Groups

- The CVSS uses three groups of metrics to assess vulnerability.
  - **Base Metric Group**: Represents the characteristics of a vulnerability that are constant over time and across contexts.
  - **Temporal Metric Group**: Measures the characteristics of a vulnerability that may change over time, but not across user environments.
  - **Environmental Metric Group**: Measures the aspects of a vulnerability that are rooted in a specific organization's environment.

GLOBALE GLOBALE INDIVIDUALE



Common Vulnerability Scoring System (CVSS)

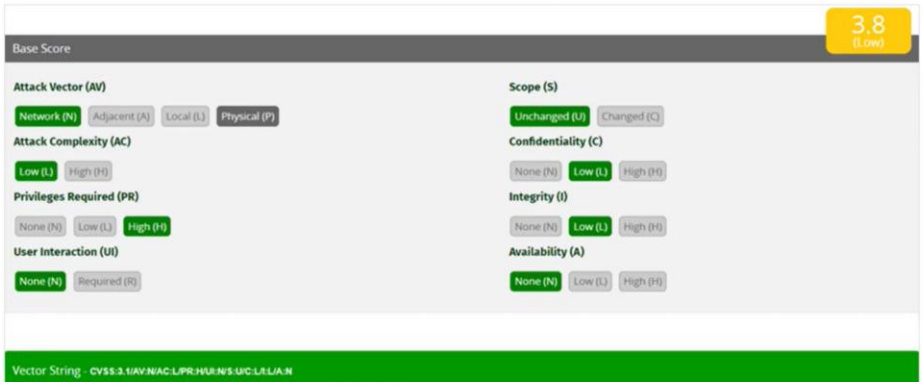
CVSS Base Metric Group

- Base Metric Group Exploitability metrics include the following criteria:
  - Attack vector
  - Attack complexity
  - Privileges required
  - User interaction
  - Scope
- Base Metric Group Impact metrics components include the following criteria:
  - Confidentiality Impact
  - Integrity Impact
  - Availability Impact

Common Vulnerability Scoring System (CVSS)

The CVSS Process

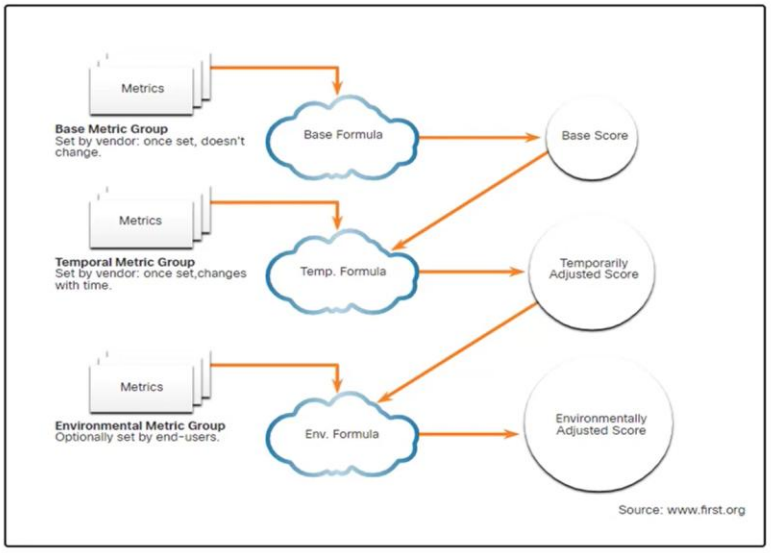
- The CVSS process uses a tool called the CVSS v3.1 Calculator.
- The calculator is like a questionnaire in which the choices are made that describe the vulnerability for each metric group.
- Later, a score is generated and numeric severity rating is displayed.



Common Vulnerability Scoring System (CVSS)

The CVSS Process (Contd.)

- After the Base Metric group is completed, the Temporal and Environmental metric values modify the Base Metric results to provide an overall score.



CVSS Reports

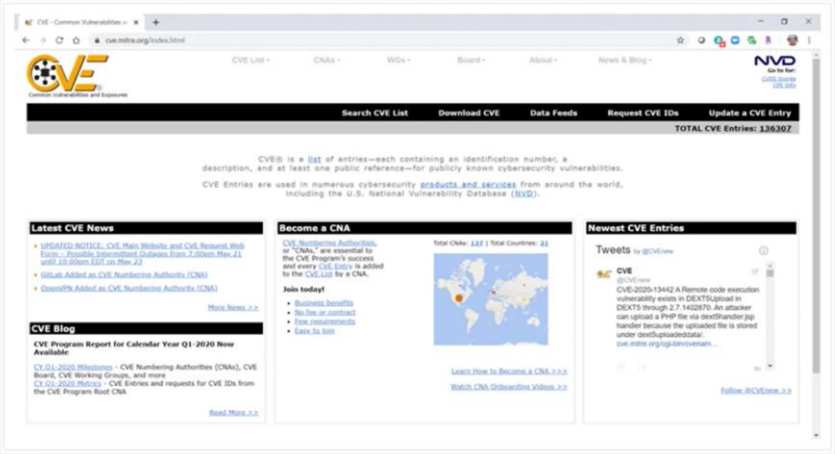
- The higher the severity rating, the greater the potential impact of an exploit and the greater the urgency in addressing the vulnerability.
- Any vulnerability that exceeds 3.9 should be addressed.
- The ranges of scores and the corresponding qualitative meaning is shown in the table:

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Other Vulnerability Information Sources

Common Vulnerabilities and Exposures (CVE):

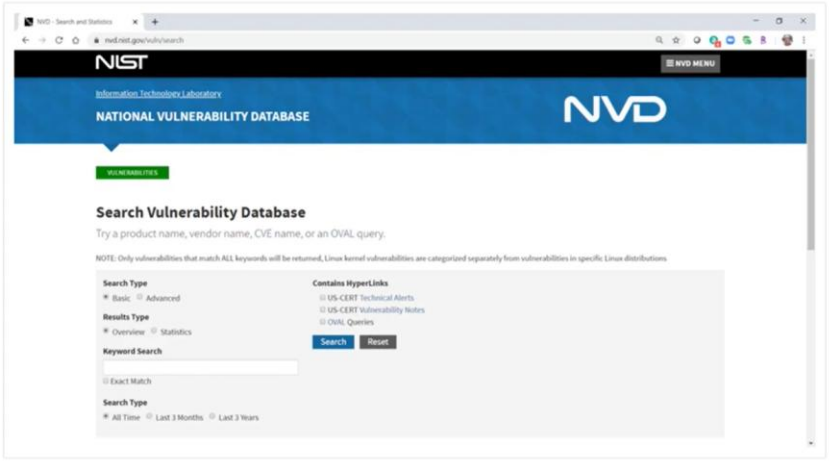
- CVE identifier provides a standard way to research a reference to vulnerabilities.
- Threat intelligence services use CVE identifiers, and they appear in various security system logs.
- The CVE Details website provides a linkage between CVSS scores and CVE information.



Other Vulnerability Information Sources (Contd.)

National Vulnerability Database (NVD):

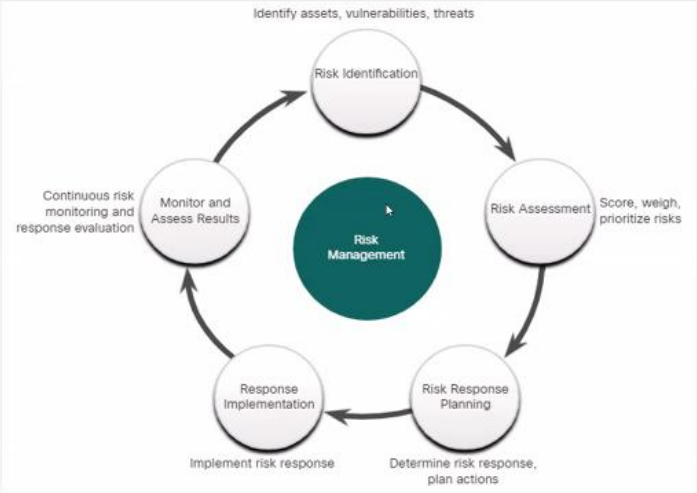
- This utilizes CVE identifiers and supplies additional information on vulnerabilities such as CVSS threat scores, technical details, affected entities, and resources for further investigation.
- The database was created and is maintained by the U.S. government National Institute of Standards and Technology (NIST) agency.



23.3 Secure Device Management

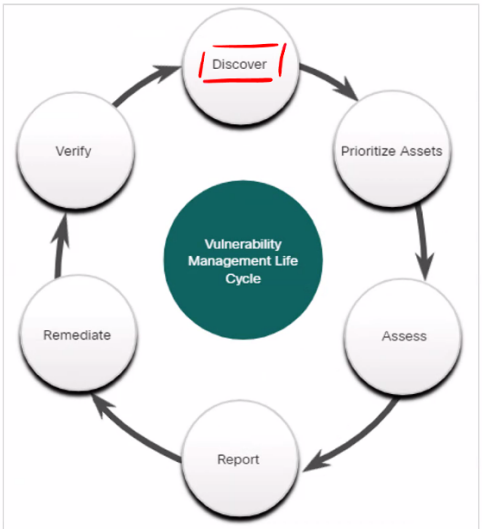
Secure Device Management
Risk Management

- Risk management involves the selection and specification of security controls for an organization.
- A mandatory activity in risk assessment is to identify threats and vulnerabilities.
- Ways to respond to identified risks:
  - **Risk avoidance** - Stop performing the activities that create risk.
  - **Risk reduction** - Take measures to reduce vulnerability.
  - **Risk sharing** - Shift some risk to other parties.
  - **Risk retention** - Accept the risk and its consequences.



Secure Device Management
Vulnerability Management

- Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities.
- The steps in the Vulnerability Management Life Cycle:
  - **Discover** - Develop a network baseline. Identify security vulnerabilities on a regular automated schedule.
  - **Prioritize Assets** - Categorize assets into groups or business units, and assign a business value based on their criticality to business operations.
  - **Assess** - Determine a baseline risk profile to eliminate risks based on asset criticality, vulnerability, threats, and asset classification.



Secure Device Management

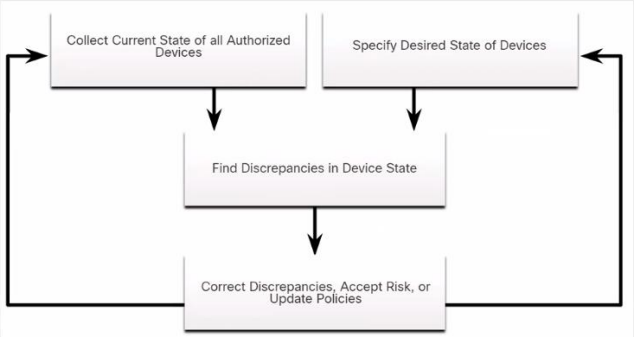
Vulnerability Management (Contd.)

- **Report** - Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
- **Remediate** - Prioritize according to business risk and address vulnerabilities in order of risk.
- **Verify** - Verify that threats have been eliminated through follow-up audits.

Secure Device Management

Asset Management

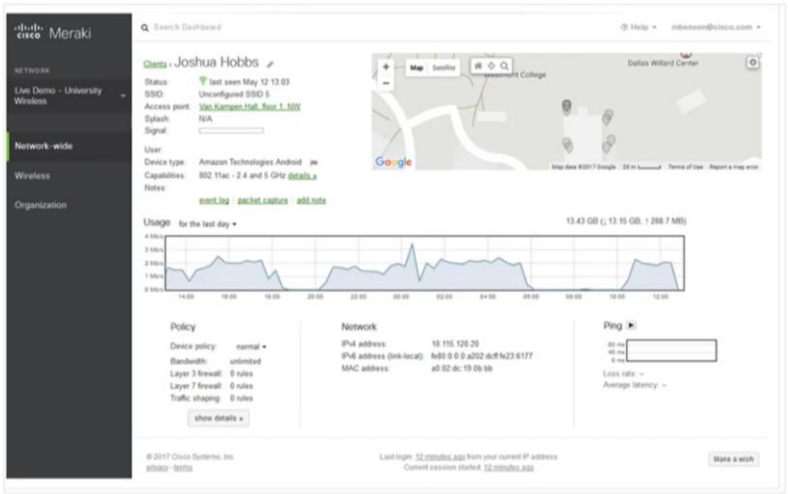
- Asset management involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise.
- **Tools and Techniques for Asset management:**
  - Automated discovery and inventory of the actual state of devices
  - Articulation of the desired state for those devices using policies, plans, and procedures in the organization's information security plan
  - Identification of non-compliant authorized assets
  - Remediation or acceptance of device state, possible iteration of desired state definition
  - Repeat the process at regular or ongoing intervals



Secure Device Management

Mobile Device Management

- Mobile devices cannot be physically controlled on the premises of an organization.
- MDM systems, such as Cisco Meraki Systems Manager, allows the security personnel to configure, monitor and update a very diverse set of mobile clients from the cloud.



Secure Device Management

Configuration Management

- **Configuration Management**: As defined by NIST, configuration management:

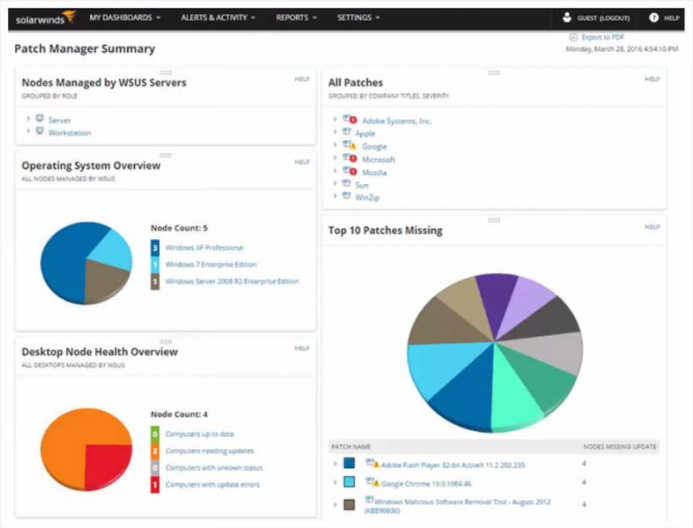
  Comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

- **Configuration tools** : Puppet, Chef, Ansible, and SaltStack

Secure Device Management

Enterprise Patch Management

- Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, installing, and verifying.
- Patch management is required by some compliance regulations such as Sarbanes Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA).

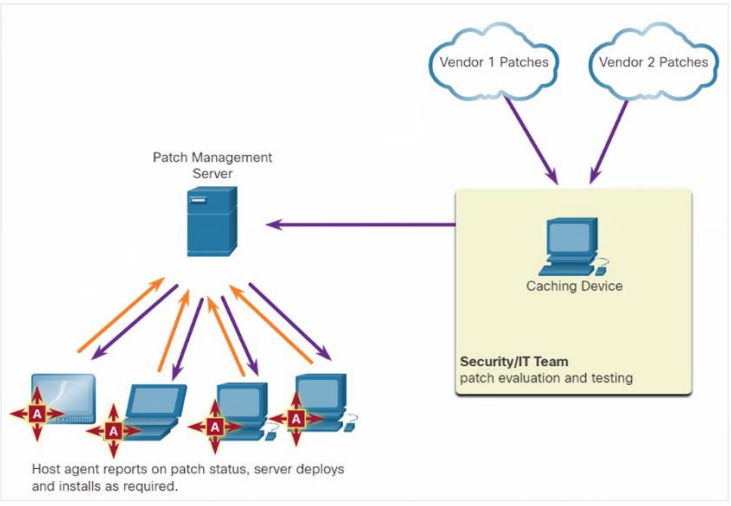


Secure Device Management

Patch Management Techniques

Agent-based:

- This requires a software agent to be running on each host to be patched.
- The agent reports whether vulnerable software is installed on the host.
- The agent communicates with the patch management server and determines if patches exist that require installation, and installs the patches.
- Agent-based approaches are the preferred means of patching mobile devices.

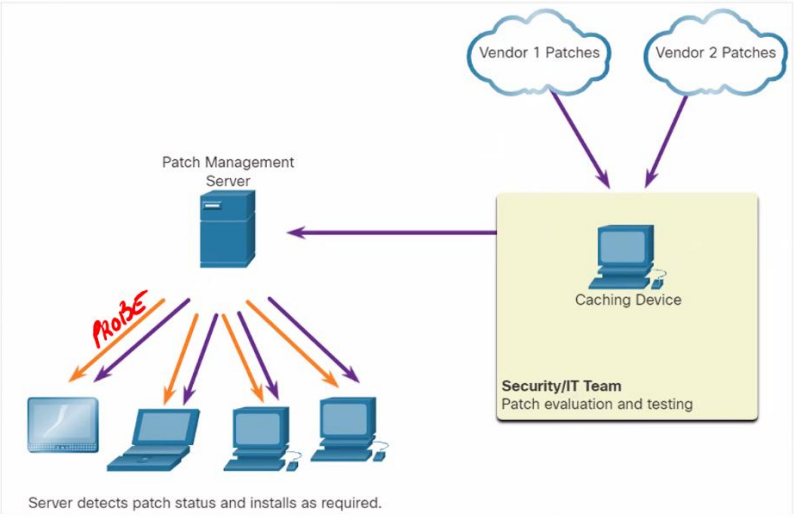


Secure Device Management

Patch Management Techniques

Agentless Scanning:

- Patch management servers scan the network for devices that require patching.
- The server determines which patches are required and installs those patches on the clients.
- Only devices that are on scanned network segments can be patched, which can be a problem for mobile devices.

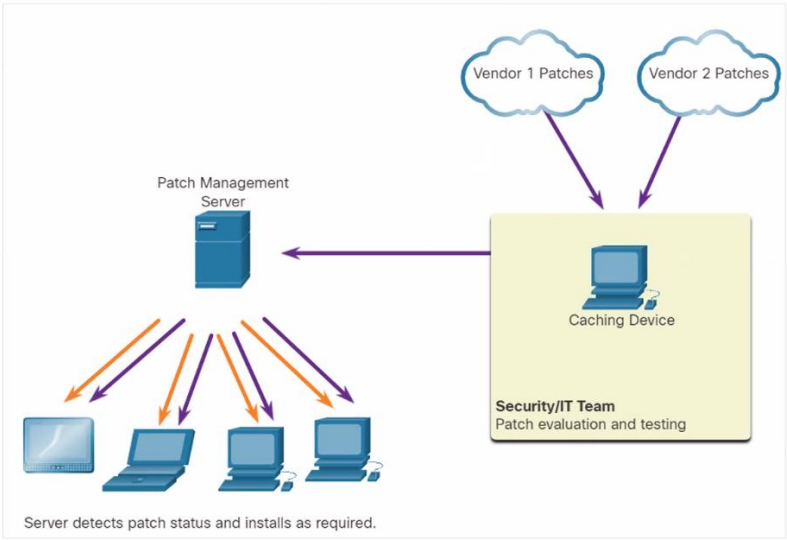


Secure Device Management

Patch Management Techniques

Passive Network Monitoring:

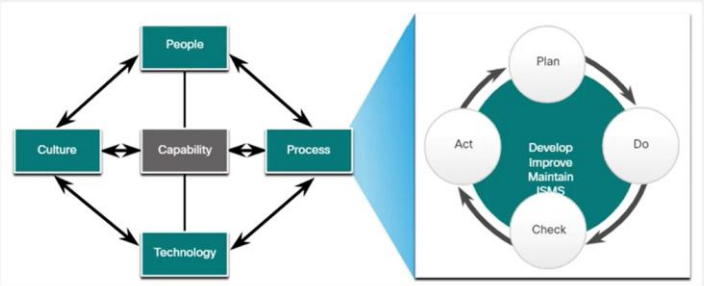
- Devices requiring patching are identified through the monitoring of traffic on the network.
- This approach is only effective for software that includes version information in its network traffic.



23.4 Information Security Management Systems

Security Management Systems

- An Information Security Management System (ISMS) consists of a management framework to identify, analyze, and address information security risks.
- ISMSs provide conceptual models that guide organizations in planning, implementing, governing, and evaluating information security programs.
- It incorporates the "plan-do-check-act" framework, known as the Deming cycle.
- ISM is seen as an elaboration on People-Process-Technology-Culture model of organizational capability

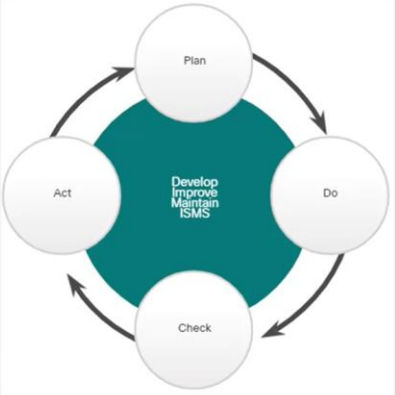


A General Model for Organizational Capability

ISO-27001

- ISO/IEC 27000 family of standards – internationally accepted standards that facilitate business conducted between countries. The ISO 27001 - global, industry-wide specification for an ISMS.

Plan	Do	Check	Act
• Understand business objectives • Define activities scope • Access and manage support • Assess and define risk • Perform asset management and vulnerability assessment	• Create and implement risk management plan • Establish and enforce risk management policies and procedures • Train personnel, allocate resources	• Monitor exécution • Compile reports • Support external certification audit	• Continually audit processes • Continually improve processes • Take corrective action • Take preventive action



NIST Cybersecurity Framework

- **NIST Cybersecurity Framework** – is a set of standards designed to integrate existing standards, guidelines, and practices to help better manage and reduce cybersecurity risk.
- The below table describes the core functions in NIST Cybersecurity Framework:

Core Function	Description
IDENTIFY	Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
RESPOND	Develop and implement the appropriate activities to act on a detected cybersecurity event.
RECOVER	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

23.5 Endpoint Vulnerability Assessment Summary

Endpoint Vulnerability Assessment Summary

- Network and device profiling provides statistical baseline information that can serve as a reference point for normal network and device performance.
- Network security can be evaluated using a variety of tools and services.
- Vulnerability assessment uses software to scan Internet-facing servers and internal networks for various types of vulnerabilities.
- The Common Vulnerability Scoring System (CVSS) is a vendor-neutral, industry standard, open framework for rating the risks of a given vulnerability by using a variety of metrics to calculate a composite score.
- Vulnerabilities are rated according to the attack vector, attack complexity, privileges required, user interaction, and scope.
- Risk management involves the selection and specification of security controls for an organization.
- Vulnerability management is a security practice that is designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization.
- Organizations can use an Information Security Management System (ISMS) to identify, analyze, and address information security risks.
- Standards for managing cybersecurity risk are available from ISO and NIST.
- NIST has also developed the Cybersecurity Framework, which is similar to the ISO/IEC 27000 standards.