Chapter 11: Endpoint Security and Analysis

Information Security

Dr. Ayman Aljarbouh

11.2 Endpoint Vulnerability Assessment

Module Objectives

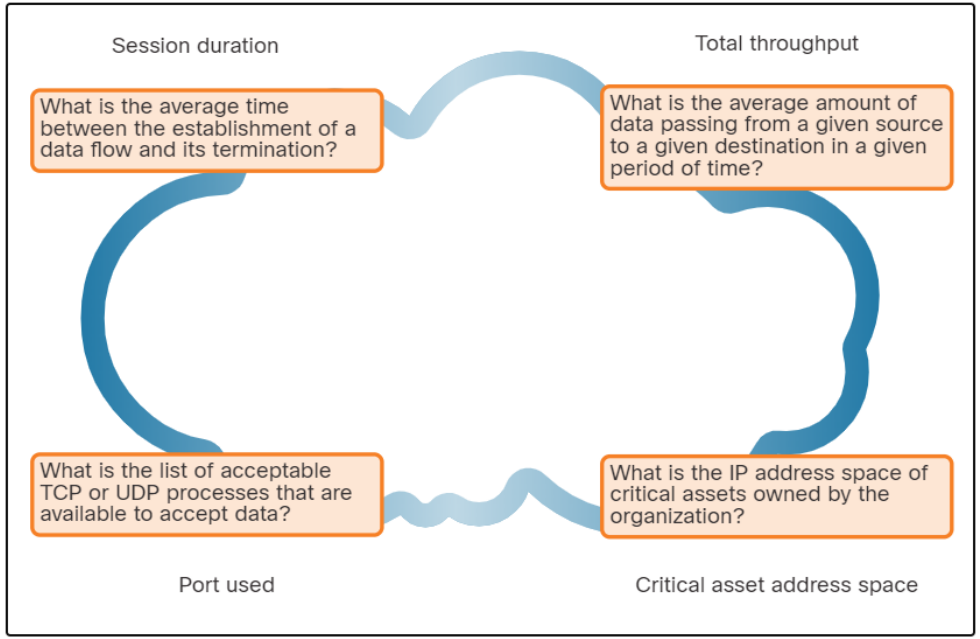
Module Title: Endpoint Vulnerability Assessment

Module Objective: Explain how endpoint vulnerabilities are assessed and managed.

Topic Title	Topic Objective
Network and Server Profiling	Explain the value of network and server profiling.
Common Vulnerability Scoring System (CVSS)	Explain how CVSS reports are used to describe security vulnerabilities.
Secure Device Management	Explain how secure device management techniques are used to protect data and assets.
Information Security Management Systems	Explain how information security management systems are used to protect assets.

Network Profiling

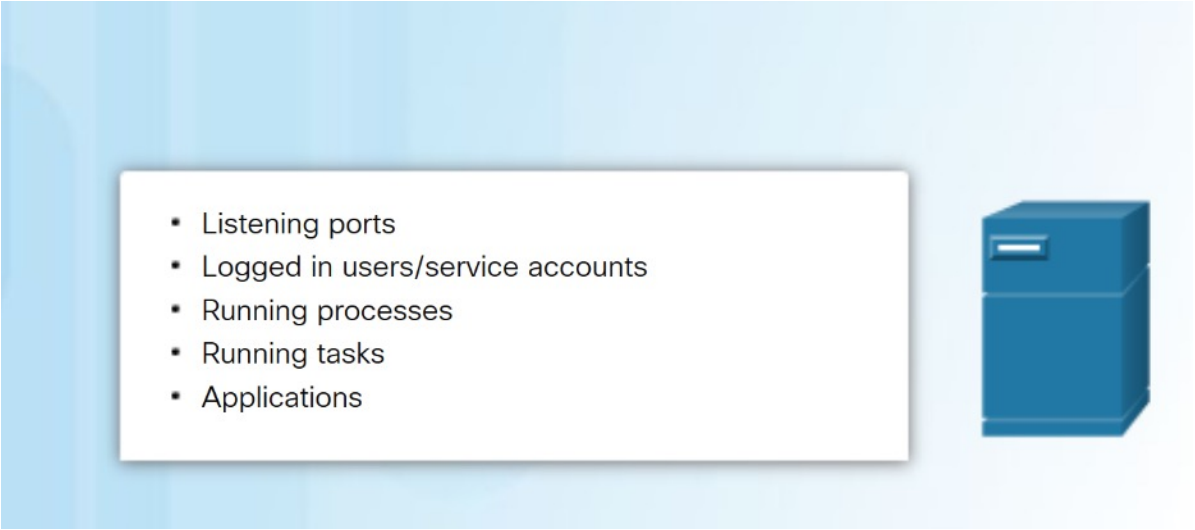
- Network and device profiling provides statistical baseline information that can serve as a reference point for normal network and device performance.
- Elements of network profile:
  - Session duration
  - Total throughput
  - Critical asset address space
  - Typical traffic type



Elements of a Network Profile

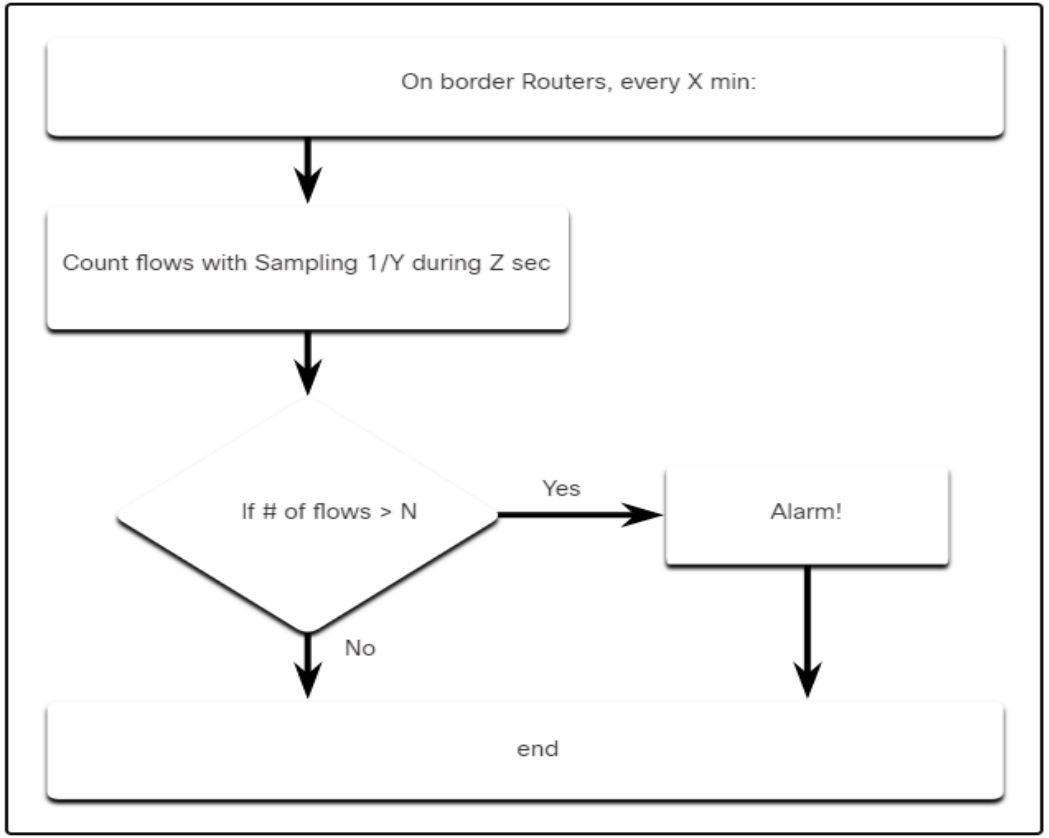
Server Profiling

- Server profiling – includes listening ports, logged in users/service accounts, running processes, running tasks, and applications



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.



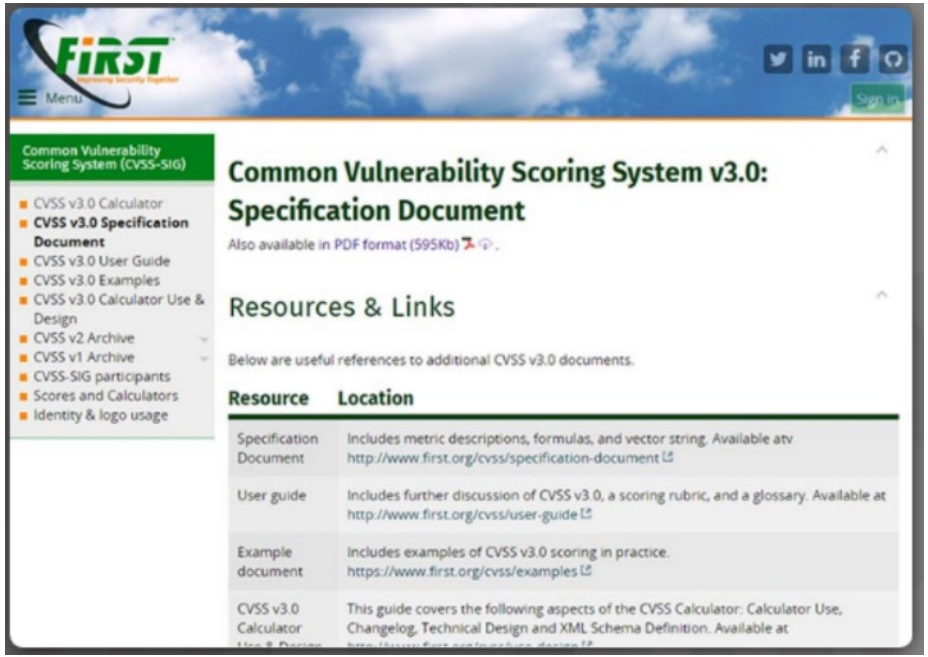
Network Vulnerability Testing

- Network vulnerability testing can include risk analysis, vulnerability assessment, and penetration testing.

Activity	Examples	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

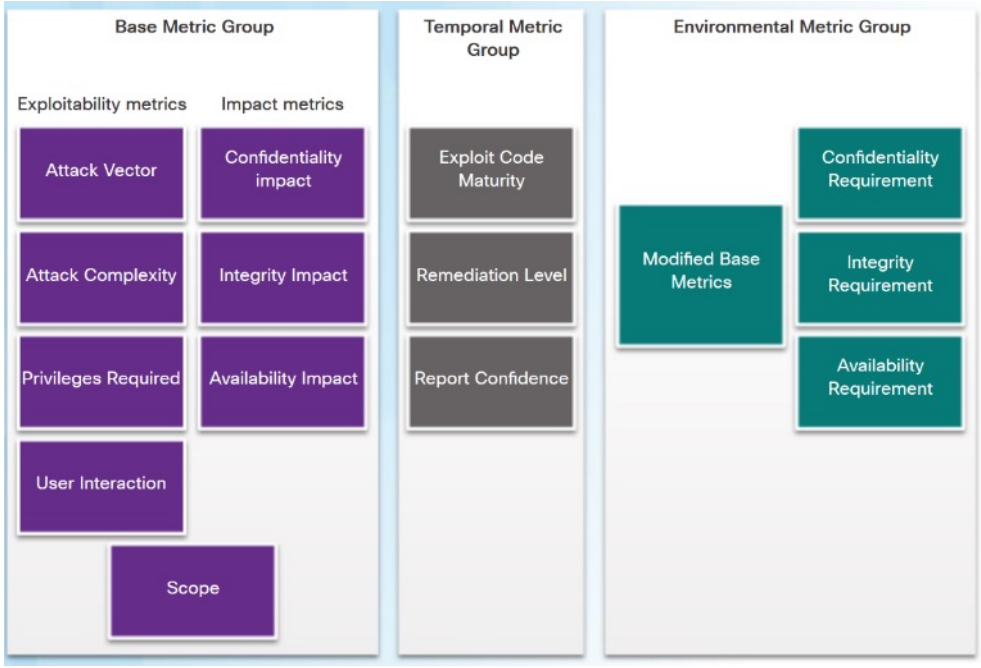
CVSS Overview

- Common Vulnerability Scoring System (CVSS) is a risk assessment designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems.
- Standardized vulnerability scores
- Open framework with metrics
- Helps prioritize risk in a meaningful way



CVSS Metric Groups

- 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.



CVSS Base Metric Group

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

The CVSS Process

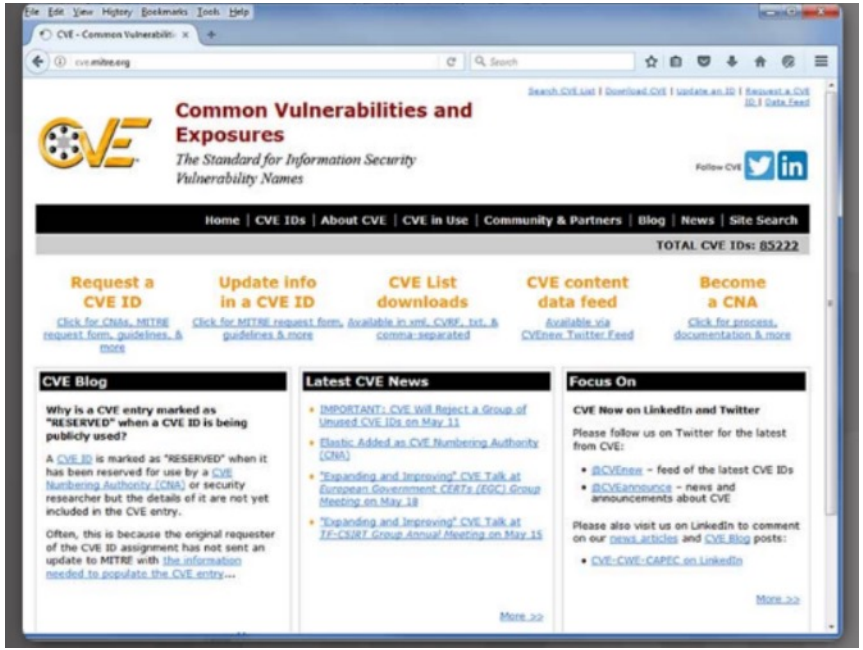
- The CVSS process uses a tool called the CVSS v3.1 Calculator.
- The calculator is like a questionnaire in which the choices are made that describe the vulnerability for each metric group.
- Later, a score is generated and numeric severity rating is displayed.

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:

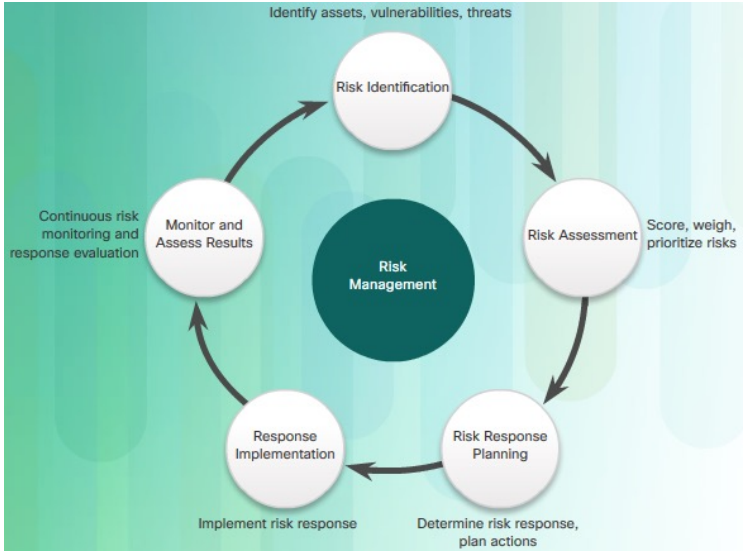
Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Other Vulnerability Information Sources



- **Common Vulnerabilities and Exposures (CVE)** - dictionary of common names, in the form of CVE identifiers, for known cybersecurity vulnerabilities.
- **National Vulnerability Database (NVD)** - utilizes CVE identifiers and supplies additional information such as CVSS threat scores, technical details, affected entities, and resources for further investigation.

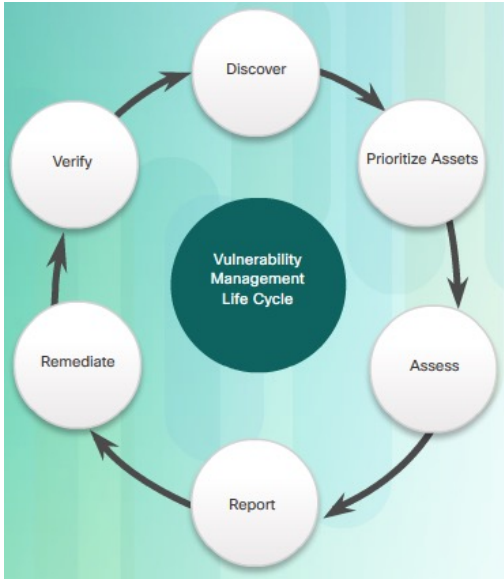
Risk Management



- Risk management involves the selection and specification of security controls for an organization.
  - **Risk avoidance** - Stop performing the activities that create risk.
  - **Risk reduction** - Take measures to reduce vulnerability.
  - **Risk sharing** - Shift some of the risk to other parties.
  - **Risk retention** - Accept the risk and its consequences.

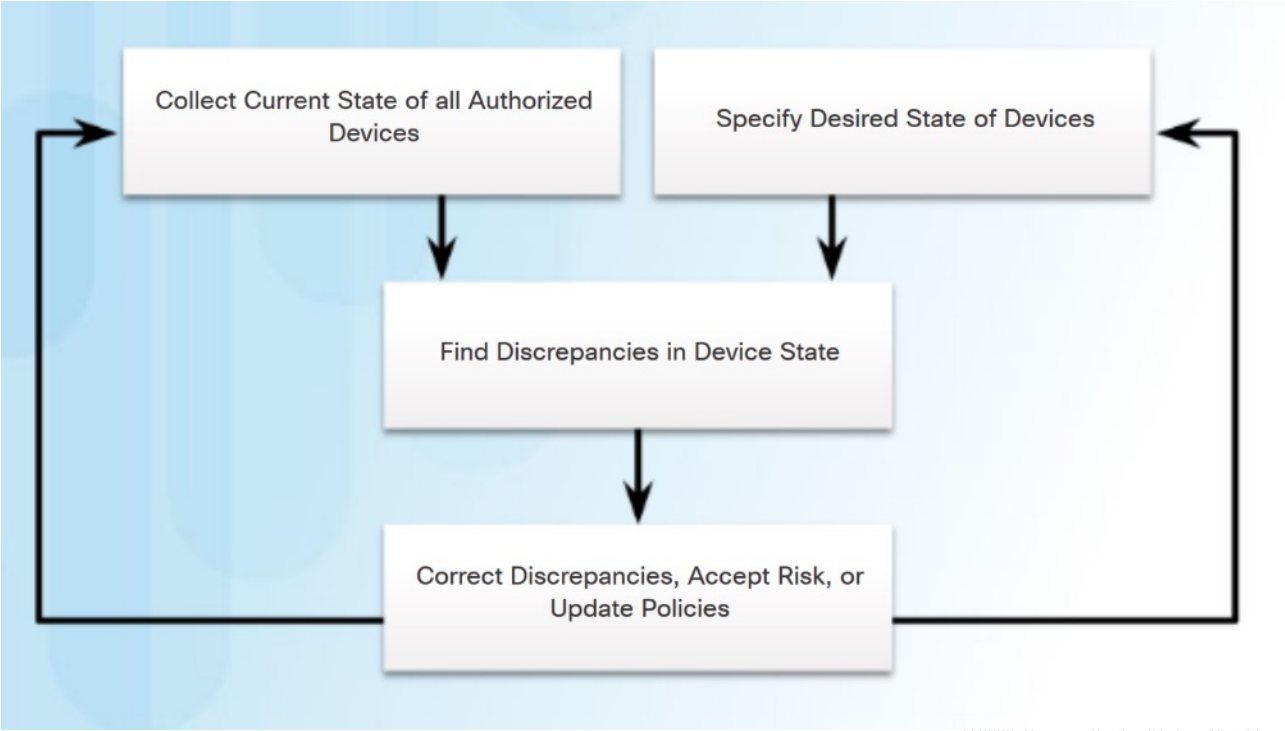
Vulnerability Management

- Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities.
- The steps in the Vulnerability Management Life Cycle:
  - **Discover** - Inventory all assets across the network and identify host details. 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 to asset groups based on their criticality to business operations.
  - **Assess** - Determine a baseline risk profile to eliminate.
  - **Report** - Measure the level of business risk associated with your assets. 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.



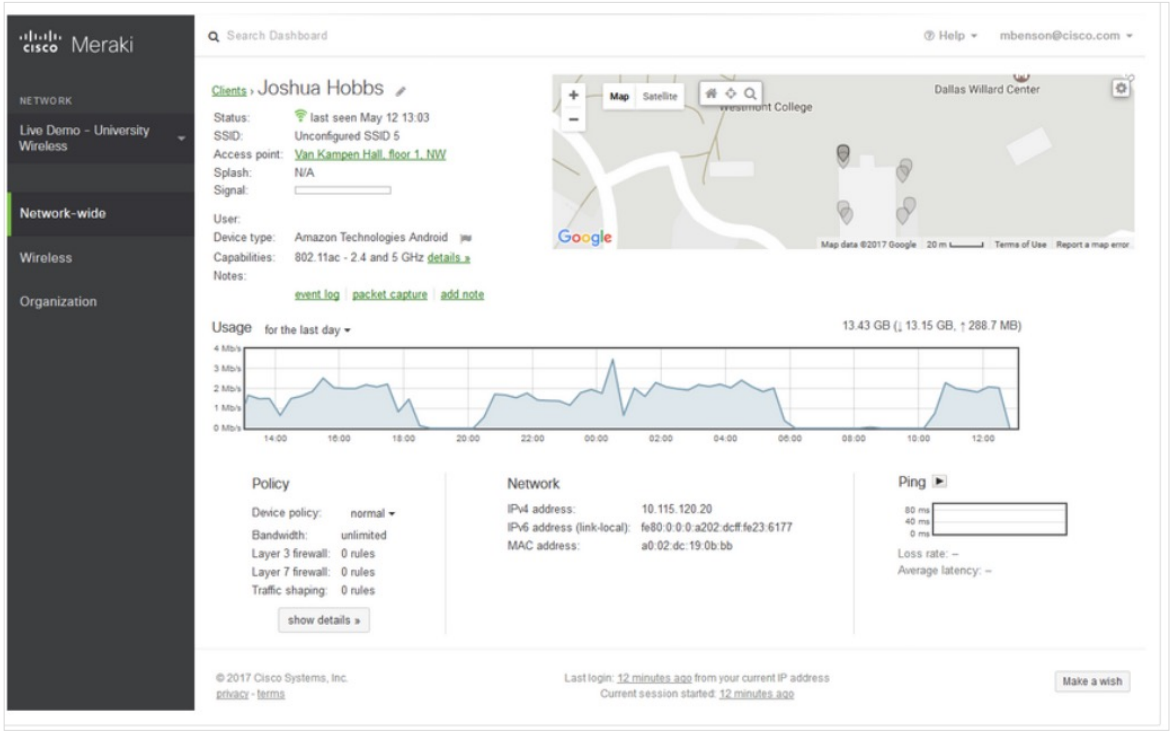
Asset Management

- Asset management – track location and configuration of devices and software



Mobile Device Management

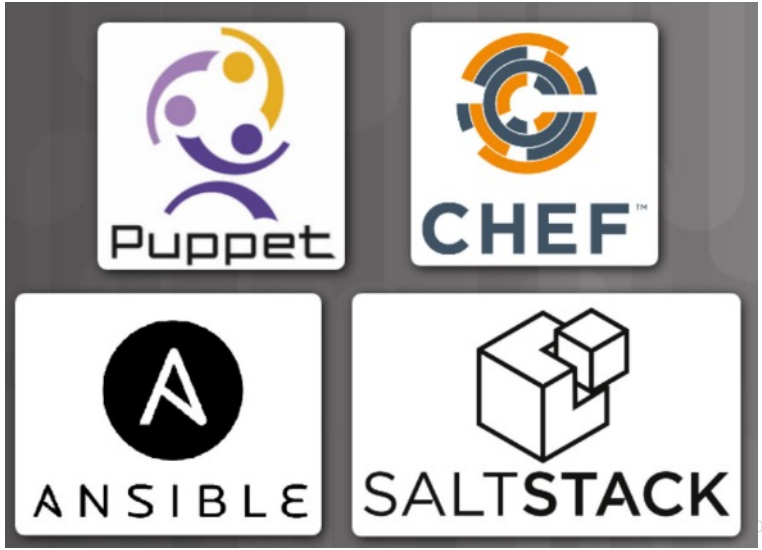
- Mobile devices cannot be physically controlled on the premises of an organization.
- MDM systems, such as Cisco Meraki Systems Manager, allows the security personnel to configure, monitor and update a very diverse set of mobile clients from the cloud.



Configuration Management

- **Configuration Management** – NIST Definition - *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 management tools examples – Puppet, Ansible, Saltsack, Chef.

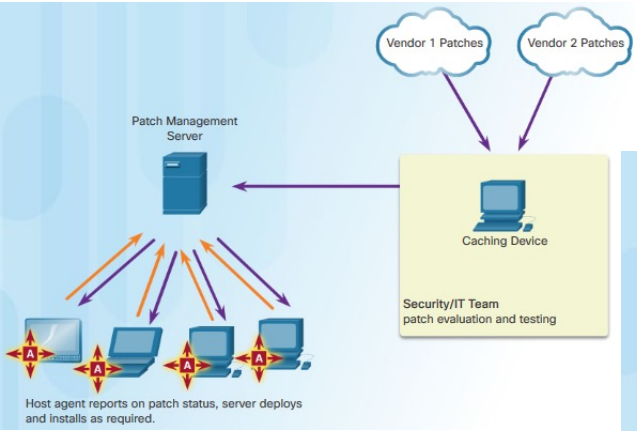


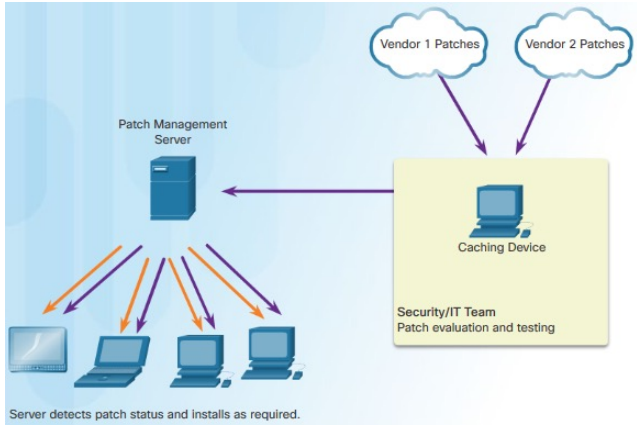
Enterprise Patch Management

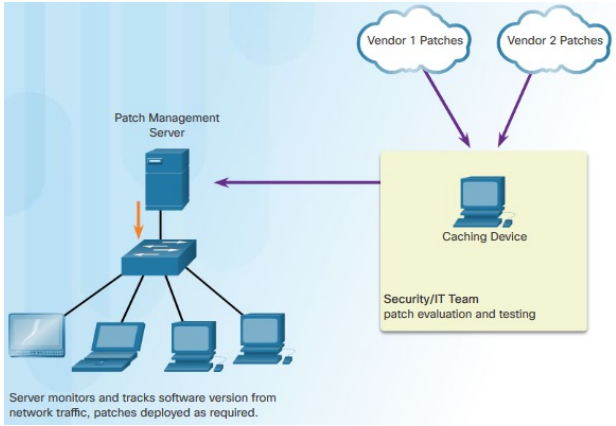
- Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, installing, and verifying that the patch is installed on all required systems.

Patch Management Techniques

- Three patch management techniques:
  - **Agent-based** – software on each host.
  - **Agentless scanning** – patch management servers scan for devices that need patching.
  - **Passive network monitoring** – monitor network traffic to identify which devices need patching.



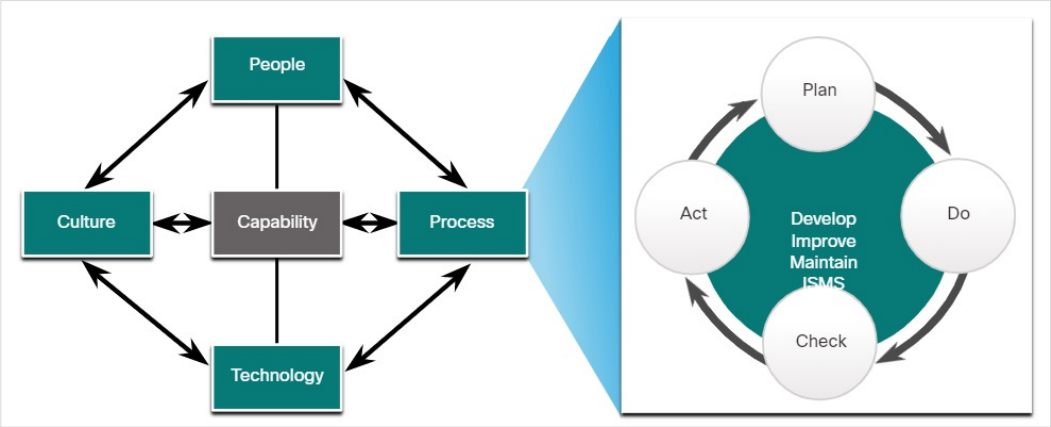




Security Management Systems

- 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



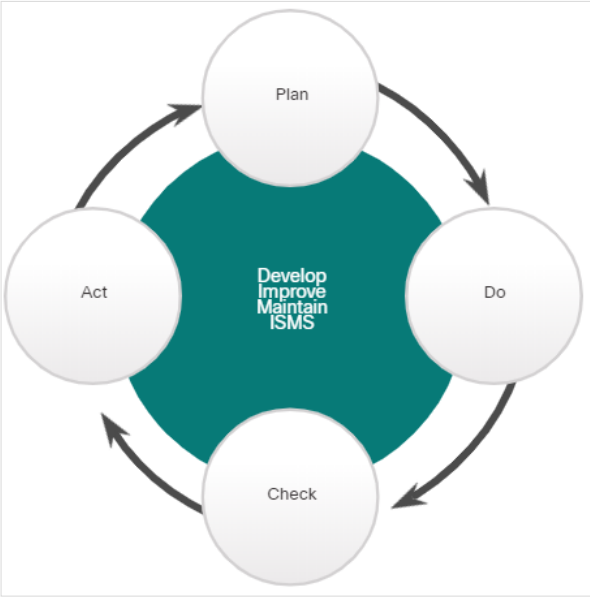
A General Model for Organizational Capability

Information Security Management Systems

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** - a set of standards designed to integrate existing standards, guidelines, and practices to help better manage and reduce cybersecurity risk.

Core Function	Description
IDENTIFY	Develop the 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 take action regarding 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.

New Terms and Commands

• Network Profiling • Server Profiling • Information Security Management System (ISMS) • Network Anomaly Detection • Network Vulnerability Testing • Common Vulnerability Scoring System (CVSS) • Base Metric Group • Temporal Metric Group	• Environmental Metric Group • Common Vulnerabilities and Exposures (CVE) • National Vulnerability Database (NVD) • Mobile Device Management (MDM) • Patch Management • Agent-based Patch Management • Agentless Scanning • Passive Network Monitoring

Lab 39 - Isolate Compromised Host Using 5-Tuple

In this lab, you will complete the following objective:

- Use Security Onion tools to investigate an exploit.

Lab 40 - Investigate a Malware Exploit

In this lab, you will complete the following objective:

- Use Security Onion to investigate a more complex malware exploit the uses an exploit kit to infect hosts.