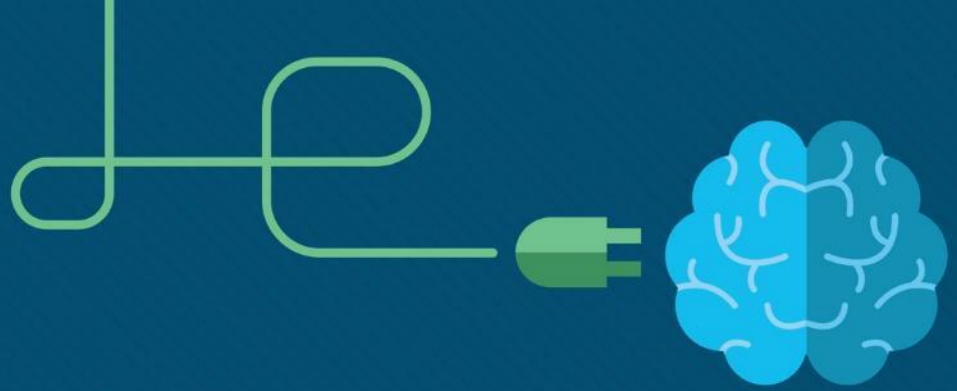


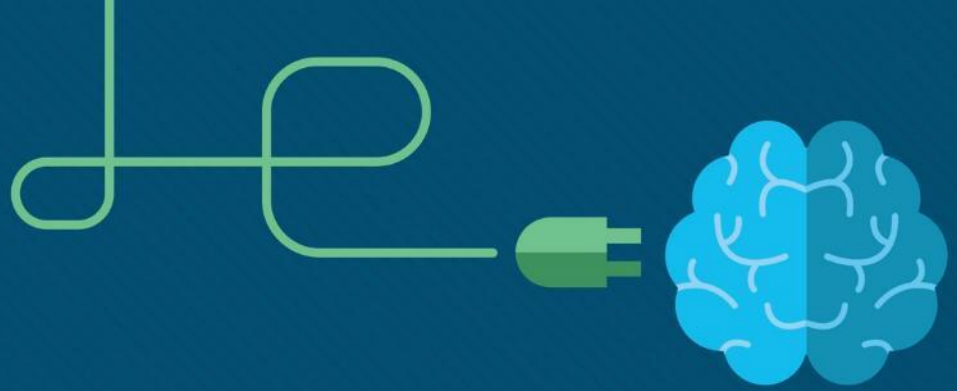
Chapter 10: Endpoint Security and Analysis

Instructor Materials

CCNA Cybersecurity Operations v1.1

Chapter 10: Endpoint Security and Analysis

CCNA Cybersecurity Operations v1.1 Planning Guide



Chapter 10: Endpoint Security and Analysis

CCNA Cybersecurity Operations v1.1

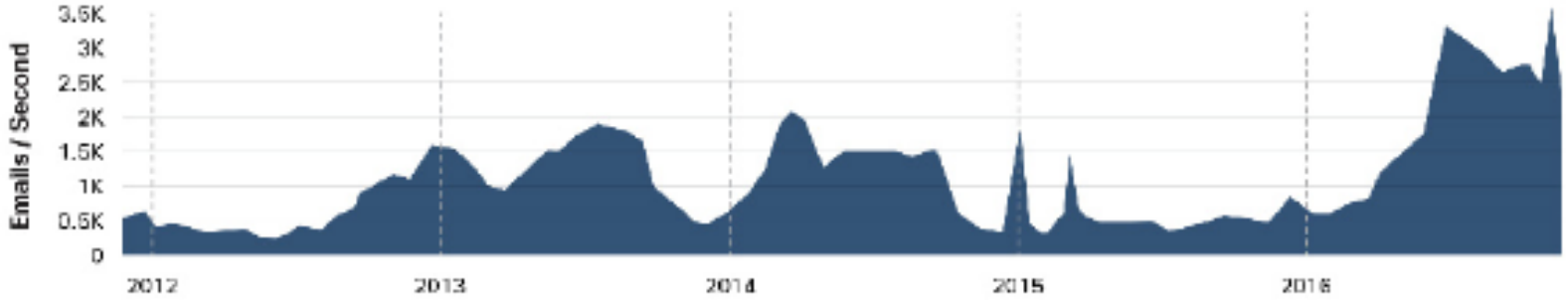
Chapter 10 - Sections & Objectives

- 10.1 Endpoint Protection
  - Use a malware analysis website to generate a malware analysis report.
    - Explain methods of mitigating malware.
    - Explain host-based IPS/IDS log entries.
    - Use virustotal.com to generate a malware analysis report.
- 10.2 Endpoint Vulnerability Assessment
  - Classify endpoint vulnerability assessment information.
    - Explain the value of network and server profiling.
    - Classify CVSS reports.
    - Explain compliance frameworks and reporting.
    - Explain how secure device management techniques are used to protect data and assets.
    - Explain how information security management systems are used to protect assets.

10.1 Endpoint Protection

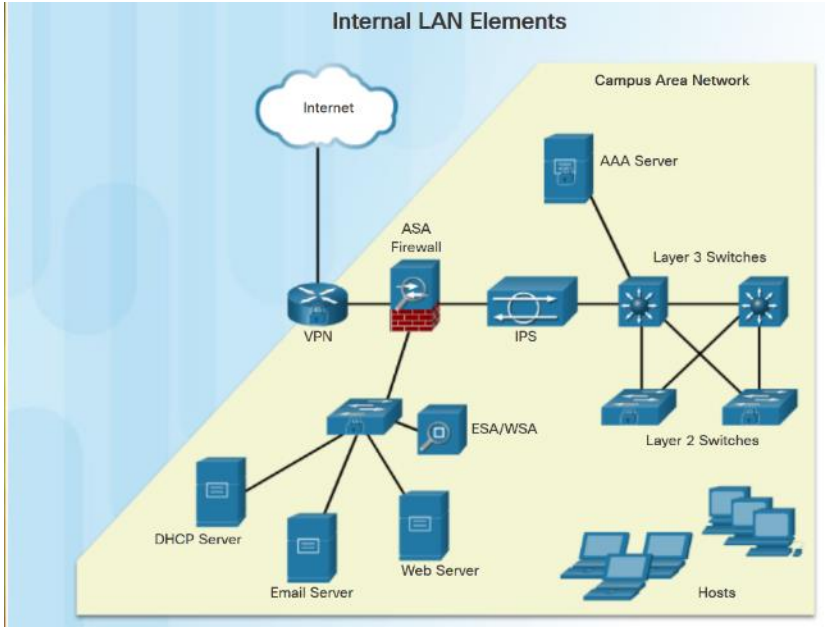
Endpoint Threats

- Endpoint Threats
  - Increased number of devices due to mobility and IoT
  - Over 75% of organizations experienced adware infections from 2015-2016
  - From 2016 to early 2017, global spam volume increased dramatically
  - Malware that targets the Android mobile operating system was in the top ten most common type found in 2016
  - Several common types of malware can significantly change features in less than 24 hours in order to evade detection.



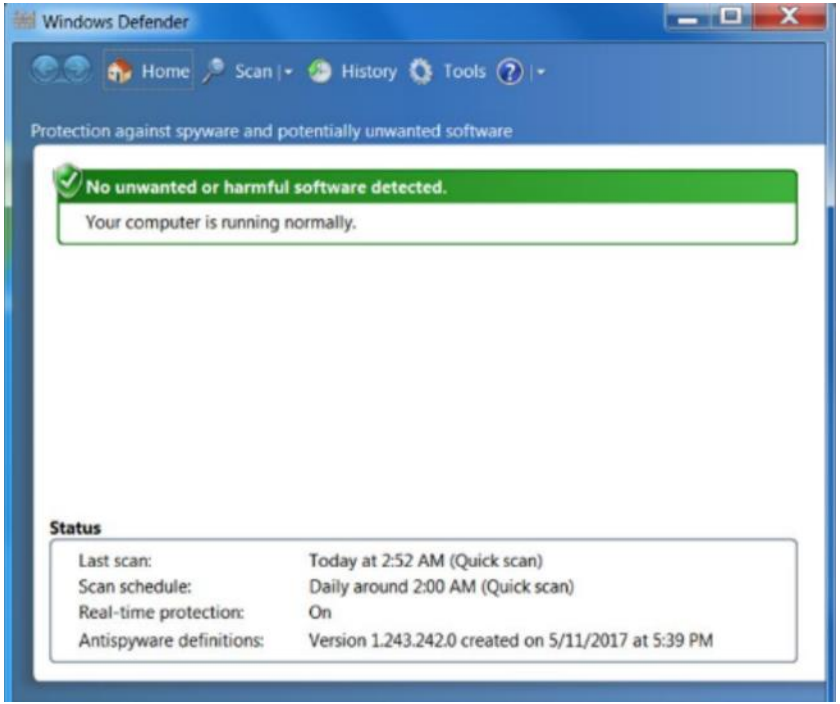
Endpoint Security

- Two internal LAN elements to secure:
  - Endpoints - Hosts commonly consist of laptops, desktops, printers, servers, and IP phones.
  - Network infrastructure - LAN infrastructure devices interconnect endpoints and typically include switches, wireless devices, and IP telephony devices.



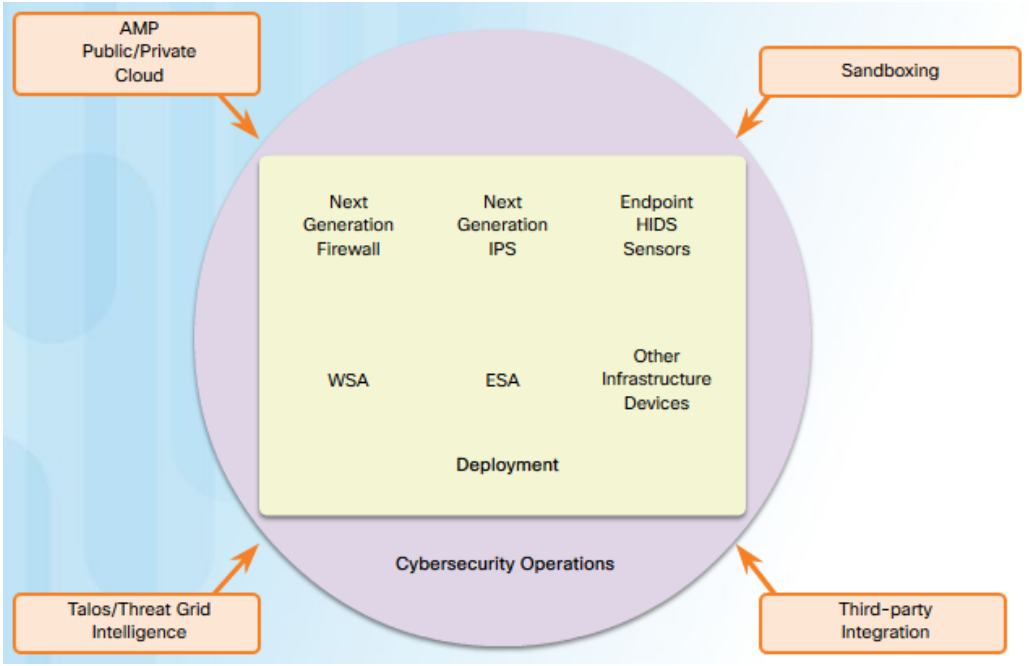
Host-Based Malware Protection

- Antimalware/antivirus software.
  - Signature-based – Recognizes various characteristics of known malware files.
  - Heuristics-based – Recognizes general features shared by various types of malware.
  - Behavior-based – Employs analysis of suspicious behavior.
- Host-based Firewall - restricts incoming and outgoing connections.
- Host-based Security Suites - include antivirus, anti-phishing, safe browsing, Host-based intrusion prevention system, firewall capabilities and robust logging functionality.

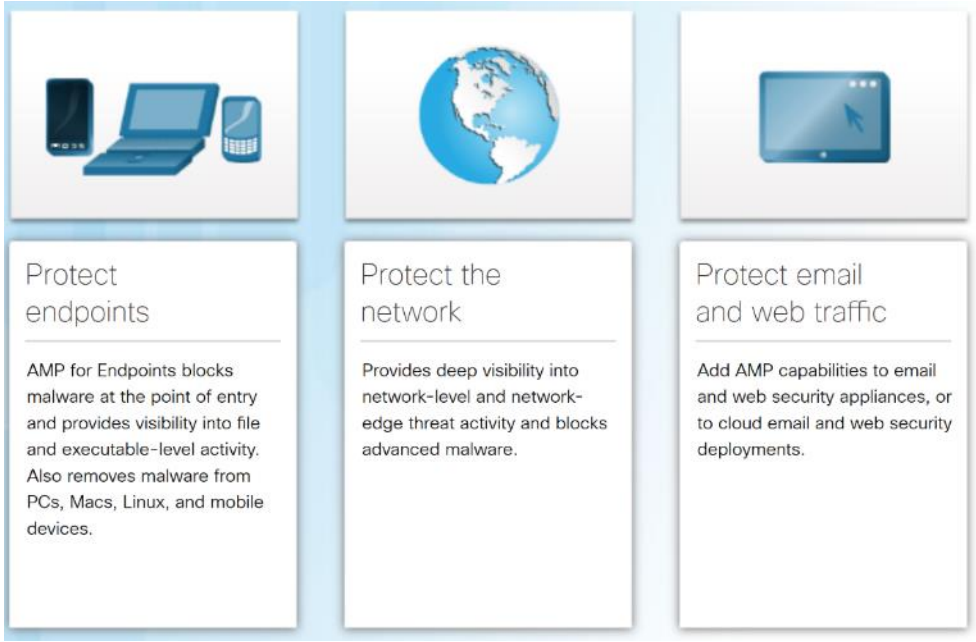


Network-Based Malware Protection

- Network-based malware protection
  - Advanced Malware Protection (AMP)
  - Email Security Appliance (ESA)
  - Web Security Appliance (WSA)
  - Network Admission Control (NAC)



Cisco Advanced Malware Protection (AMP)

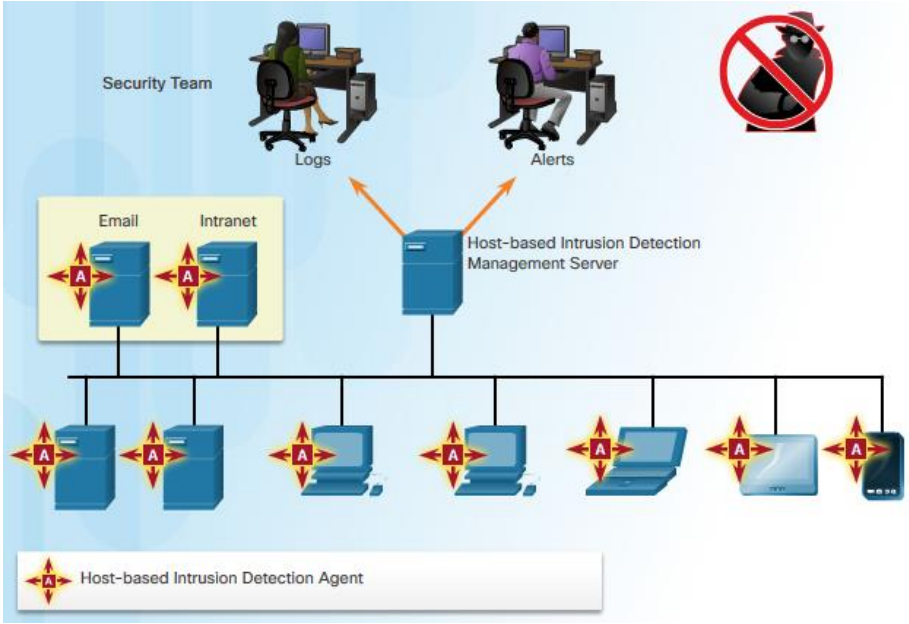


- Cisco Advanced Malware Protection (AMP) addresses all phases of a malware attack:
  - **Before an attack** - AMP uses global threat intelligence from Cisco's Talos Security Intelligence and Research Group, and Threat Grid's threat intelligence feeds.
  - **During an attack** - AMP uses that intelligence coupled with known file signatures and Cisco Threat Grid's dynamic malware analysis technology.
  - **After an attack** - The solution goes beyond point-in-time detection capabilities and continuously monitors and analyzes all file activity and traffic.

Host-Based Firewalls

- Host-based personal firewalls are standalone software programs that control traffic entering or leaving a computer.
- Host-based firewalls include;
  - **Windows Firewall** - uses a profile-based approach to configuring firewall functionality.
  - **Iptables** - allows Linux system administrators to configure network access rules.
  - **Nftables** - successor to iptables, nftables is a Linux firewall application that uses a simple virtual machine in the Linux kernel.
  - **TCP Wrapper for Linux-based devices** - rule-based access control and logging system.

Host-Based Intrusion Detection



- Host-Based Intrusion Detection System (HIDS) protects hosts against malware and can perform the following:
  - monitoring and reporting
  - log analysis
  - event correlation
  - integrity checking
  - policy enforcement
  - rootkit detection
- HIDS software must run directly on the host, so it is considered an agent-based system.

HIDS Operation

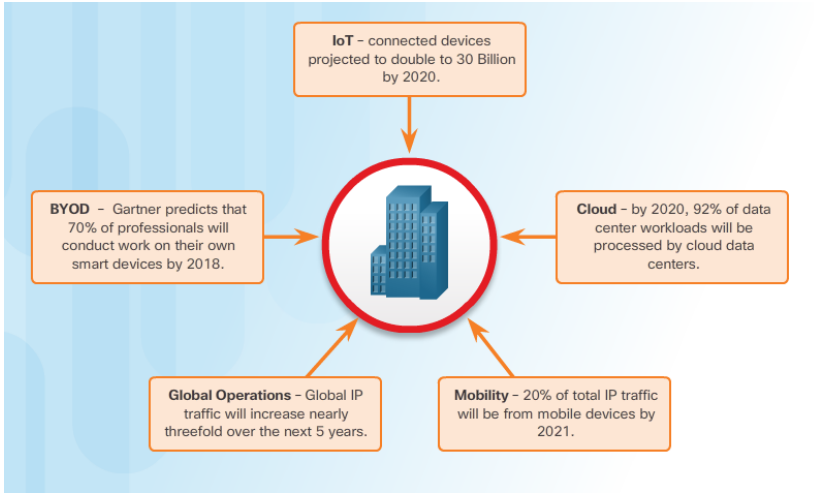
- A HIDS can prevent intrusion because it uses signatures to detect known malware and prevent it from infecting a system.
- An additional set of strategies are used to detect malware that evades signature detection:
  - **Anomaly-based** - host behavior is compared to a learned baseline model.
  - **Policy-based** – normal behavior is described by rules or by the violation of predefined rules.

HIDS Products

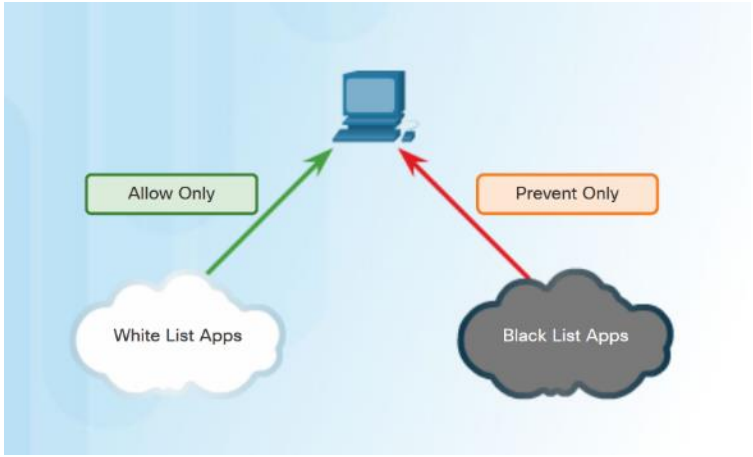
- Most HIDS utilize software on the host and some sort of centralized security management functionality that allows integration with network security monitoring services and threat intelligence.
  - Examples: Cisco AMP, AlienVault USM, Tripwire, and Open Source HIDS SECurity (OSSEC).
  - OSSEC uses a central manager server and agents that are installed on individual hosts.

Attack Surface

- An attack surface is the total sum of the vulnerabilities.
  - Include open ports, applications, wireless connections, and users.
- Expanding due to cloud-based systems, mobile devices, BYOD and the IoT.
- The SANS Institute describes three components of the attack surface:
  - Network Attack Surface
  - Software Attack Surface
  - Human Attack Surface



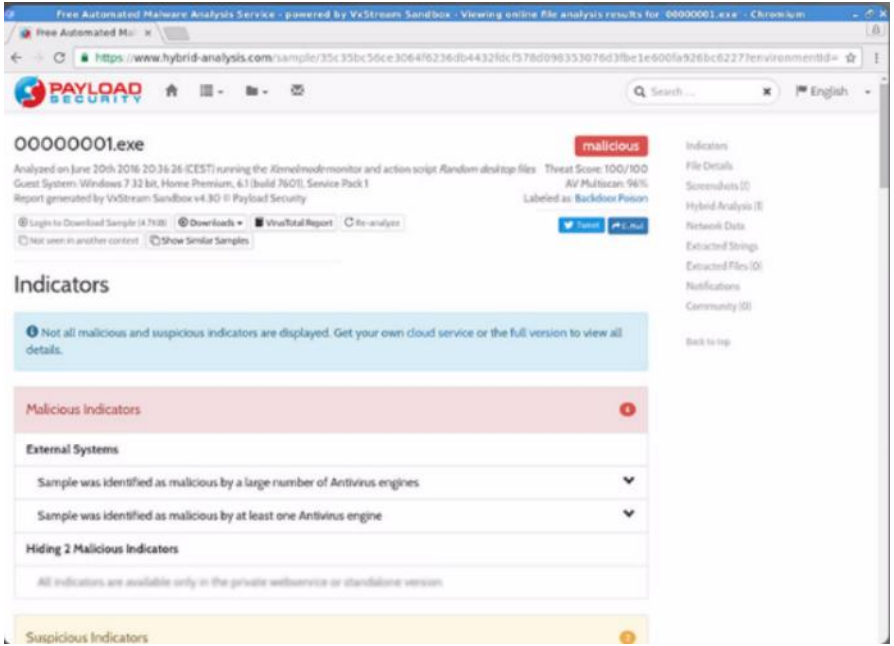
Application Blacklisting and Whitelisting



- Application blacklist – which apps are not permitted.
- Application whitelist – which apps are allowed to run.
- Whitelists are created in accordance with a security baseline that has been established by an organization.
- Websites can also be whitelisted and blacklisted.
  - Cisco's FireSIGHT security management system is an example of a device that can access the Cisco Talos security intelligence service to obtain blacklists.

System-Based Sandboxing

- Sandboxing is a technique that allows suspicious files to be analyzed and run in a safe environment.
- Cuckoo Sandbox for example, is a free malware analysis system sandbox. It can be run locally and have malware samples submitted to it for analysis.

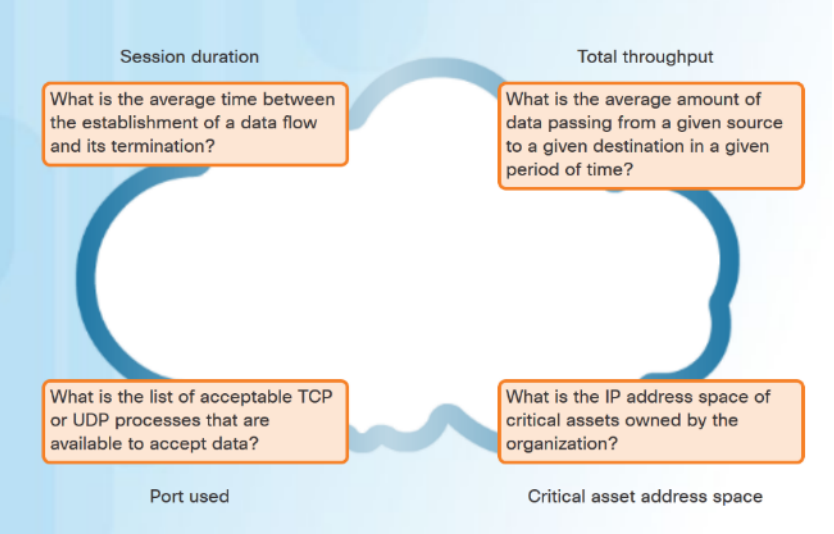


Video Demonstration - Using a Sandbox to Launch Malware

10.2 Endpoint Vulnerability Assessment

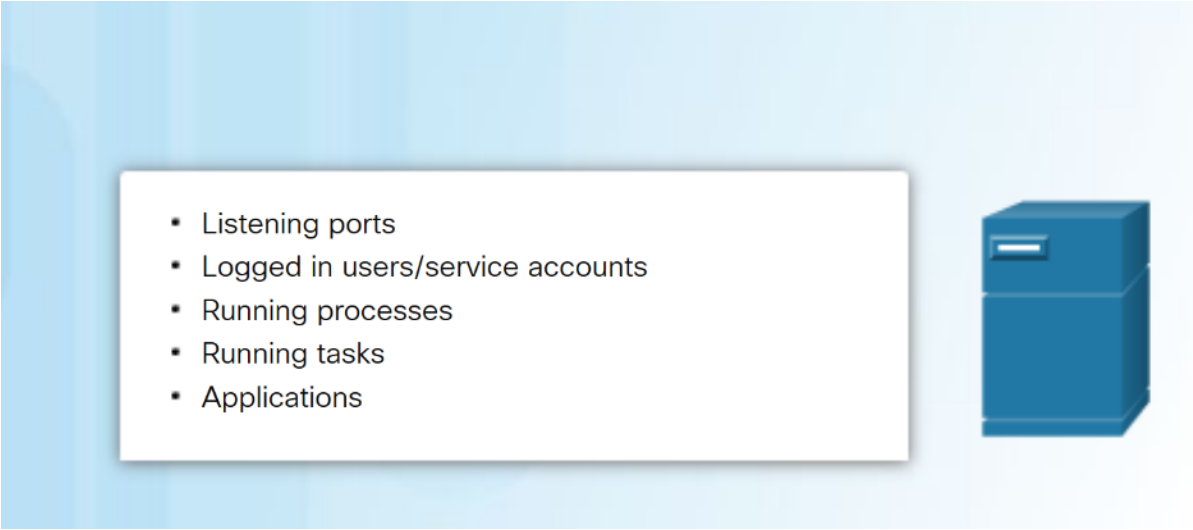
Network Profiling

- Network profiling – create a baseline to compare against when an attack occurs.
- Elements of a network baseline should include:
  - **Session duration**
  - **Total throughput**
  - **Critical asset address space**
  - **Typical traffic type**



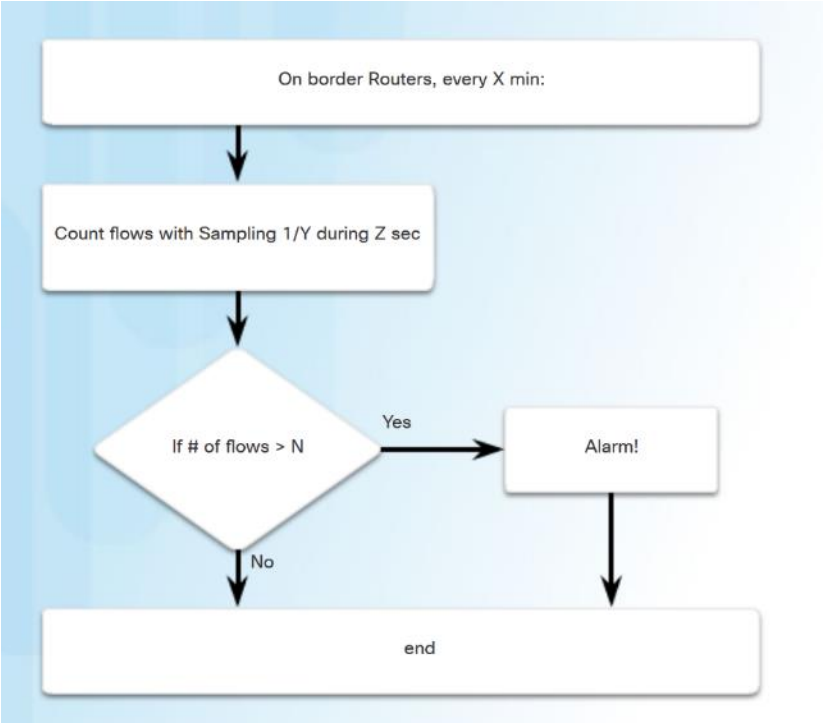
Server Profiling

- 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 recognize network congestion caused by worm traffic and also identify infected hosts on the network.



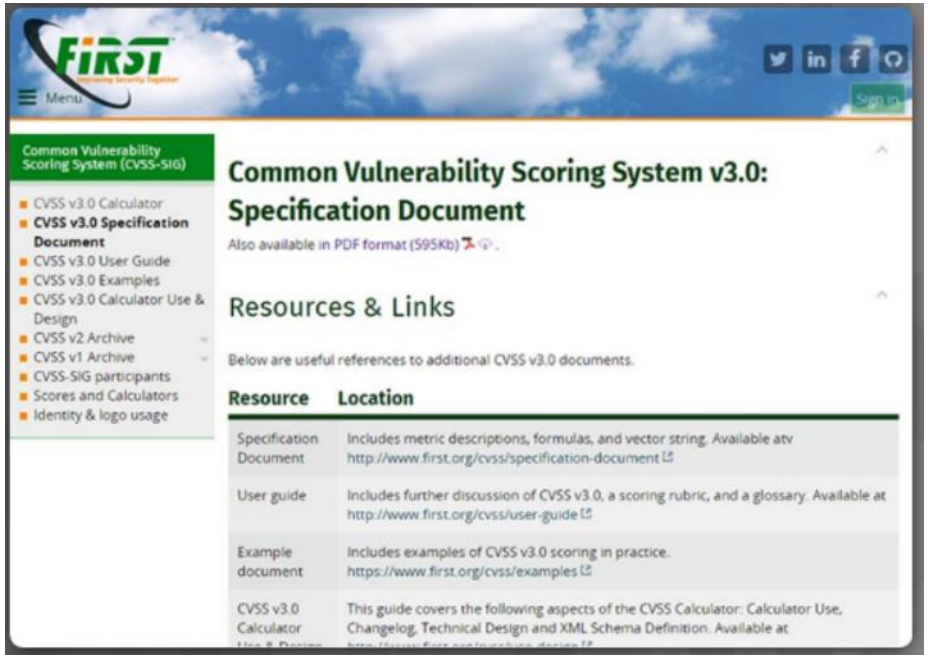
Network Vulnerability Testing

- 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

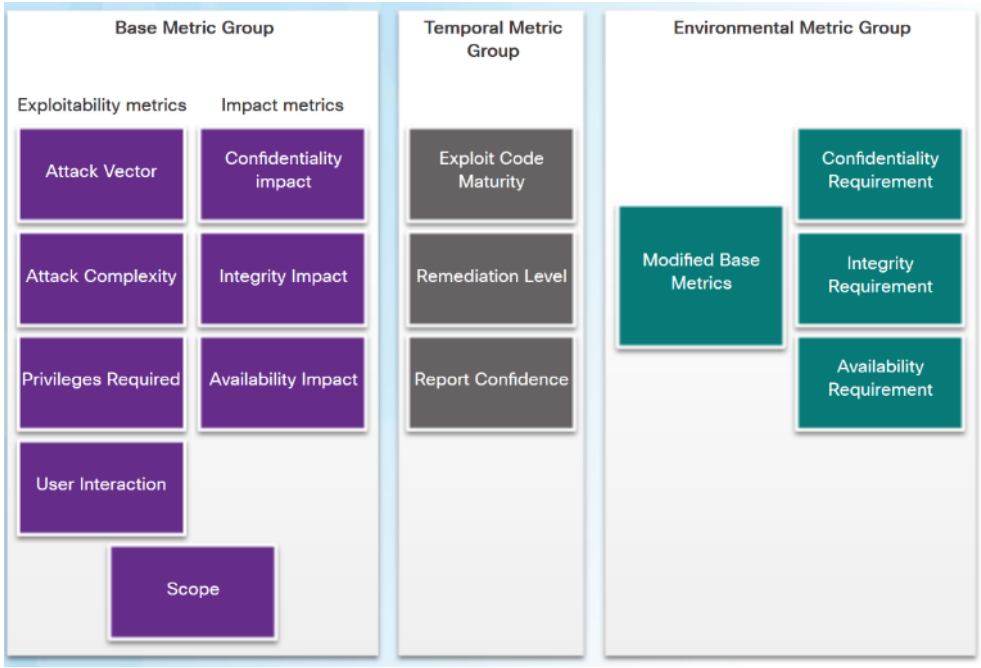
CVSS Overview

- 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

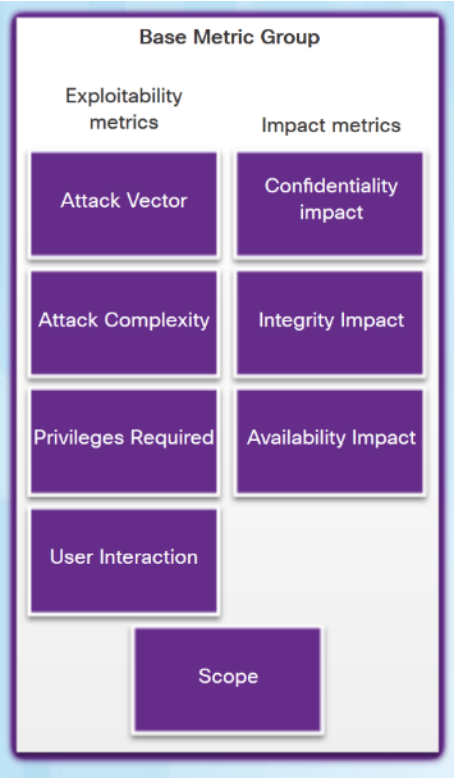


CVSS Metric Groups

- 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.



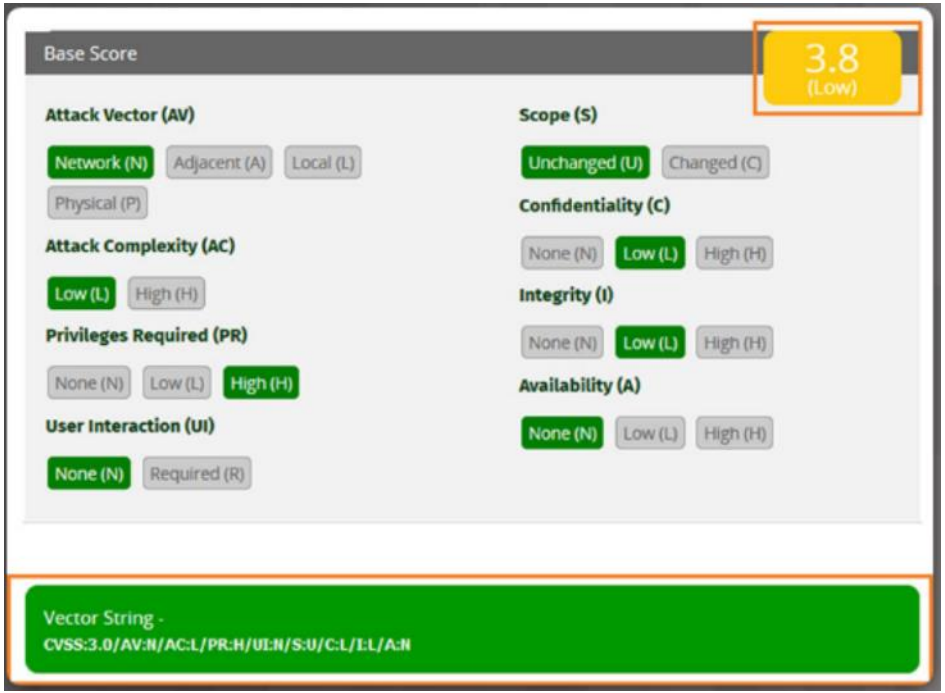
CVSS Base Metric Group



- 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

- CVSS process uses a tool called the CVSS v3.0 Calculator.
- The calculator is similar to a questionnaire in which choices are made that describe the vulnerability for each metric group. Then a score is generated.
- The Base Metric group is first completed.
- Then the Temporal and Environmental metric values modify the Base Metric results to provide an overall score.

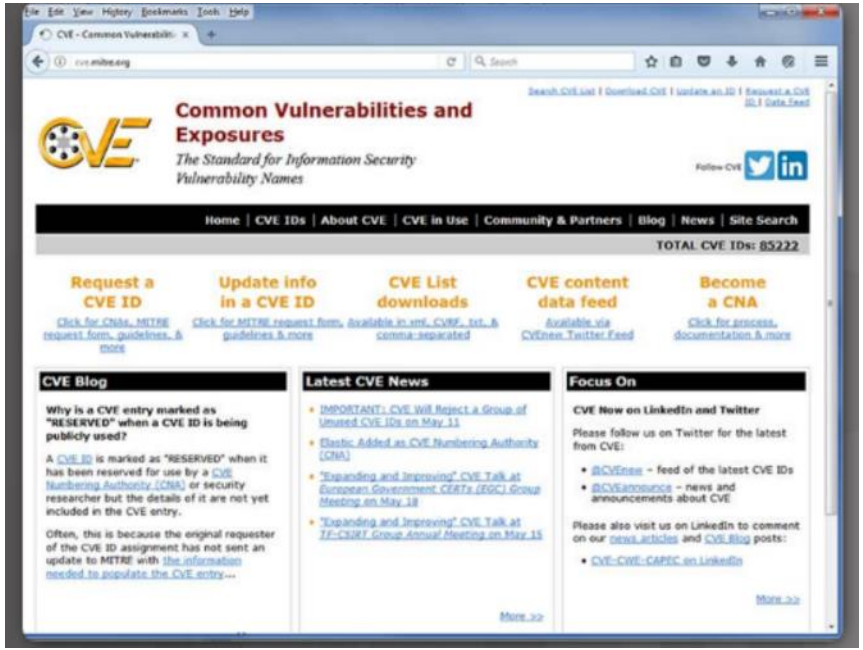


CVSS Reports

- The higher the severity rating, the greater the potential impact of an exploit and the greater the urgency in addressing the vulnerability.
- A vulnerability that exceeds 3.9 should be addressed.

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

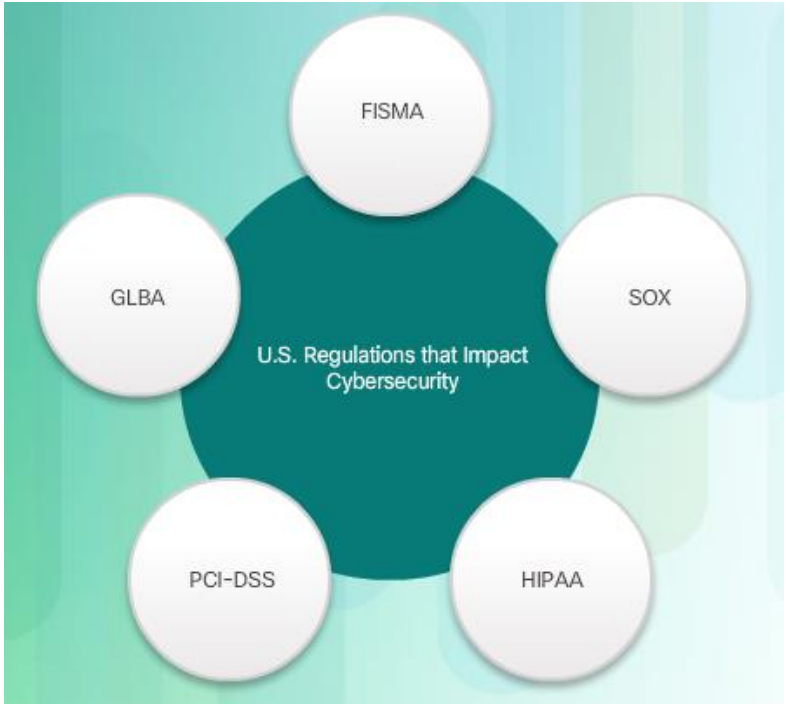
Other Vulnerability Information Sources



- **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.

Compliance Regulations

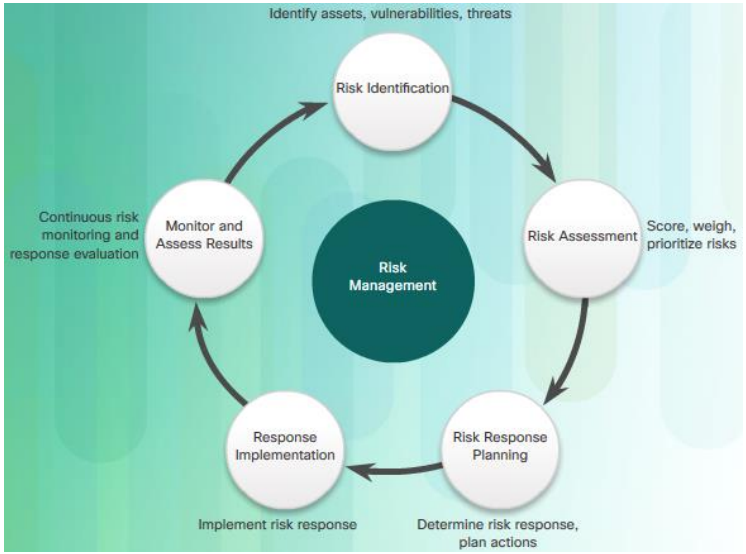
- To prevent security breaches, a number of security compliance regulations have emerged.
- The regulations offer a framework for practices that enhance information security while also stipulating incidence response actions and penalties for failure to comply.



Overview of Regulatory Standards

- Cybersecurity regulations that impact cybersecurity
  - **FISMA (Federal Information Security Management Act of 2002)** – security standards for U.S. government systems and contractors.
  - **SOX (Sarbanes-Oxley Act of 2002)** – requirements for U.S. public company boards, management, and public accounting firms regarding control and disclosure of financial information.
  - **HIPAA (Health Insurance Portability and Accountability Act)** – protection of patient healthcare information.
  - **PCI-DSS (Payment Card Industry Data Security Standard)** – proprietary, non-governmental standard created by five major credit card companies that defines requirements for secure handling of customer credit card data.
  - **GLBA (Gramm-Leach-Bliley Act)** – requirements for security of customer information by financial institutions.

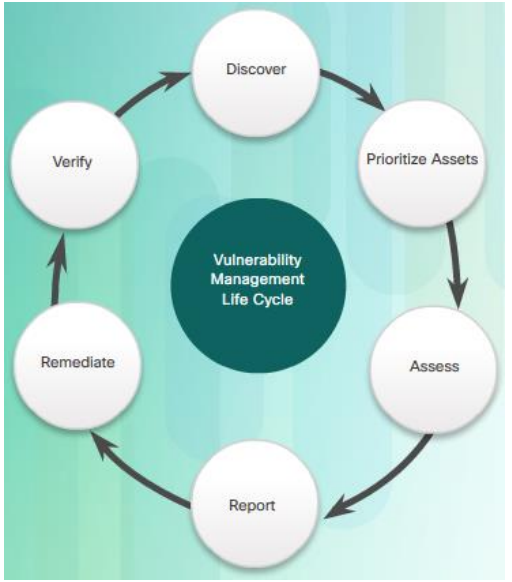
Risk Management



- 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.

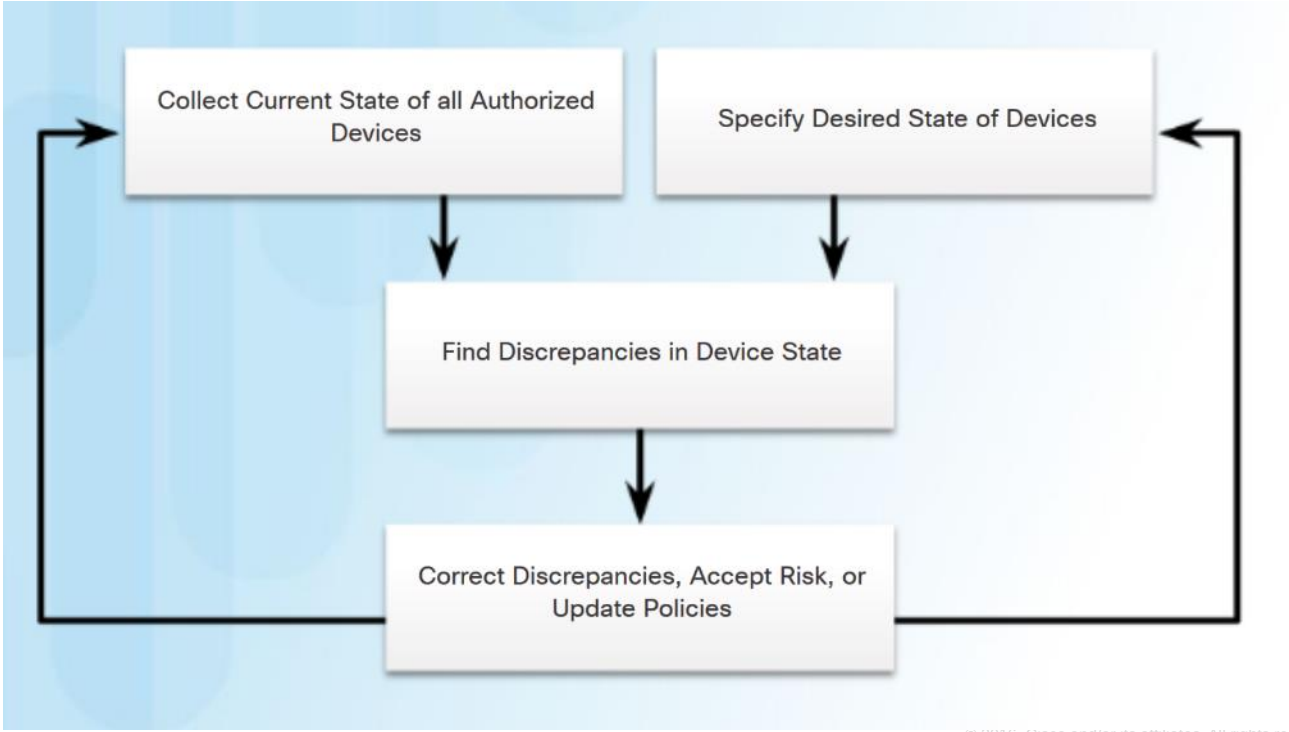
Vulnerability Management

- 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.



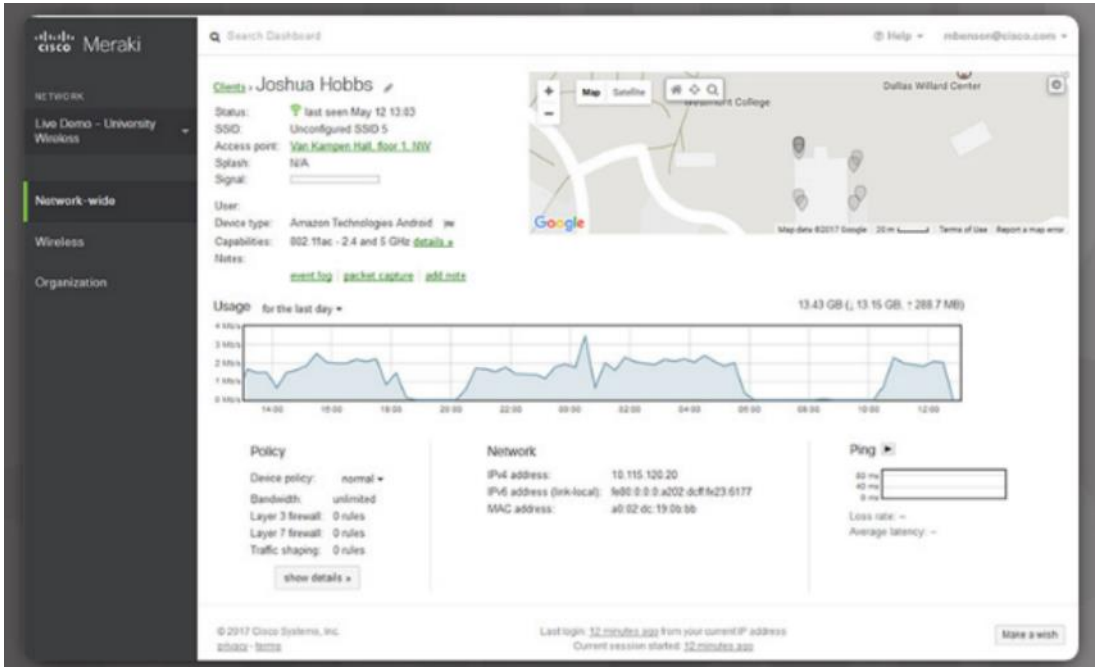
Asset Management

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



Mobile Device Management

- Mobile device management (MDM) – configure, monitor, and update mobile clients

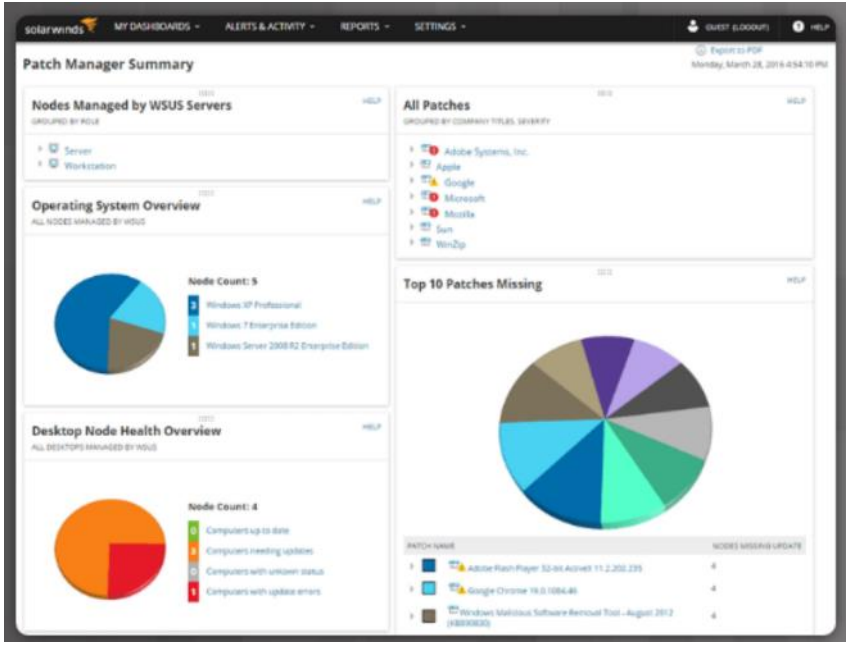


Configuration Management

- **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.

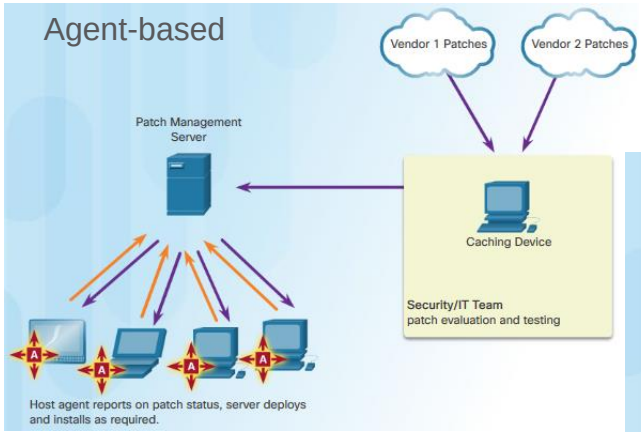
Enterprise Patch Management

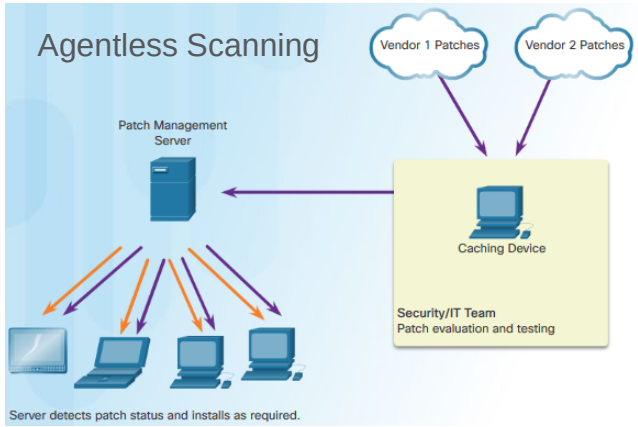
- Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, installing, and verifying that the patch is installed on all required systems.

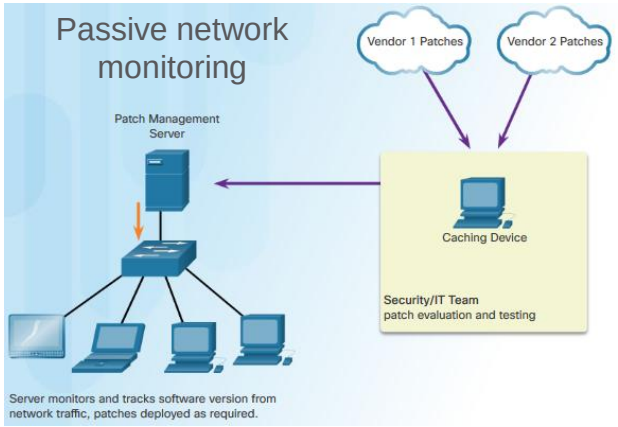


Patch Management Techniques

- 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.

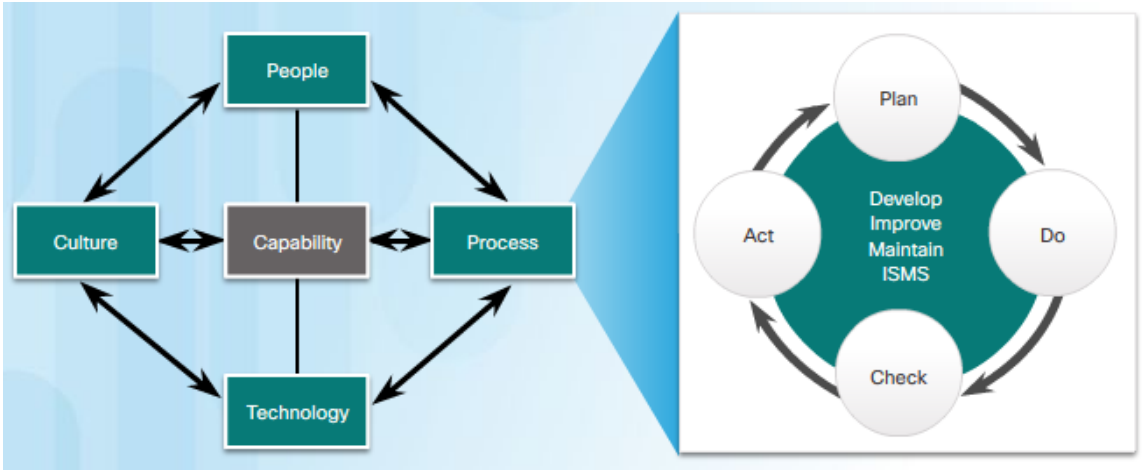






Security Management Systems

- 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.



ISO-27001

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

Plan

- Understand relevant business objectives
- Define scope of activities
- Access and manage support
- Assess and define risk
- Perform asset management and vulnerability assessment

Do

- Create and implement risk management plan
- Establish and enforce risk management policies and procedures
- Train personnel, allocate resources

Check

- Monitor implementation
- Compile reports
- Support external certification audit

Act

- Continually audit processes
- Continual process improvement
- 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.

10.3 Chapter Summary

Summary

- Investigate endpoint vulnerabilities and attacks using antimalware, host-based firewall, and host-based intrusion detection systems (HIDS).
- Attack surface is all of the vulnerabilities accessible to an attacker and can include open ports, applications, wireless connections, and users.
- Three components of the attack surface: network, software, and human.
- Baselining is performed by network profiling and server profiling.
- A network profile could contain session duration, total throughput, port(s) used, and critical asset address space.
- A server profile commonly contains listening ports, logged in users/service accounts, running processes, running tasks, and applications.
- Network vulnerability testing is performed using risk analysis, vulnerability assessment, and penetration testing.
- CVSS is a vendor-neutral risk assessment that contains three main metric groups (base, temporal, and environmental). Each group has specific metrics that can be measured.

Summary (Cont.)

- Compliance regulations include FISMA, SOX, HIPAA, PCI-DSS, and GLBA.
- Risk management is used to identify assets, vulnerabilities and threats.
- 4 methods of risk reduction include risk avoidance, risk reduction, risk sharing, and risk retention
- Vulnerability management proactively prevents the exploitation of IT vulnerabilities. The 6 steps of the vulnerability management lifecycle include discover, prioritize assets, assess, report, remediate, and verify.
- Other device managements that must be considered include asset management, mobile device management, configuration management, and patch management.
- An ISMS consists of a management framework used to identify, analyze, and address information security risks. Examples include the ISO/IEC 27000 family of standards and the NIST Cybersecurity Framework Core and Functions.

New Terms and Commands

- Antivirus/Antimalware
- endpoint
- Federal Information Security Management Act of 2002 (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Host-based firewall
- host-based intrusion detection system (HIDS)
- Information Security Management System (ISMS)
- Payment Card Industry Data Security Standard (PCI-DSS)
- profiling
- Sandboxing
- Sarbanes-Oxley Act of 2002 (SOX)

Cybersecurity Operations Certification

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 2: Security Concepts**
  - 2.6 Compare and contrast the following terms:
    - Network and Host Antivirus
    - Agent-less and Agent Based protections
  - 2.7 Describe the following concepts:
    - Asset management
    - Configuration management
    - Mobile device management
    - Patch management
    - Vulnerability management

Cybersecurity Operations Certification

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-255 SECOPS - Implementing Cisco Cybersecurity Operations

- **Domain 3: Incident Response**
  - 3.5 Identify the following elements used for Network Profiling:
    - Total throughput
    - Session duration
    - Ports used
    - Critical asset address space
  - 3.6 Identify the following elements used for Server Profiling:
    - Listening ports
    - Logged in users/service accounts
    - Running processes
    - Running tasks
    - Applications


CISCO