


# CCNA Cyber Ops (Version 1.1) – Chapter 10: Endpoint Security and Analysis

 [itexamanswers.net/ccna-cyber-ops-version-1-1-chapter-10-endpoint-security-and-analysis.html](https://itexamanswers.net/ccna-cyber-ops-version-1-1-chapter-10-endpoint-security-and-analysis.html)

June 16, 2019

## Contents

---

## Objectives

---

Upon completion of this chapter, you will be able to answer the following questions:

- What are some methods of mitigating malware?
- What are the contents of host-based IPS/IDS log entries?
- How do you use a public service to generate a malware analysis report?
- How do you classify endpoint vulnerability assessment information?
- What is the value of network and server profiling?
- How do you classify CVSS reports?
- What are the compliance frameworks and reporting methods?
- How are secure device management techniques used to protect data and assets?
- How are information security management systems used to protect assets?

## Key Terms

---

This chapter uses the following key terms. You can find the definitions in the Glossary.

*endpoint*

*antivirus/antimalware*

*host-based firewalls*

*host-based intrusion detection system (HIDS)*

*sandboxing*

*profiling*

*Payment Card Industry Data Security Standard (PCI DSS)*

*Federal Information Security Management Act of 2002 (FISMA)*

*Sarbanes-Oxley Act of 2002 (SOX)*

*Gramm-Leach-Bliley Act (GLBA)*

*Health Insurance Portability and Accountability Act (HIPAA)*

*Information Security Management System (ISMS)*

## Introduction (10.0)

---

Endpoints are the most numerous devices on a network; therefore, they are the targets of the majority of network attacks. A cybersecurity analyst must be familiar with the threats to endpoints, the methods for protecting endpoints from attacks, and the methods for detecting compromised endpoints.

This chapter discusses how to investigate endpoint vulnerabilities and attacks.

## **Endpoint Protection (10.1)**

---

In this section, you will learn how to use a malware analysis website to generate a malware analysis report.

### **Antimalware Protection (10.1.1)**

---

In this topic, you will learn how to explain methods of mitigating malware.

#### **Endpoint Threats (10.1.1.1)**

---

The term endpoint is defined in various ways. For the purpose of this course, we can define endpoints as hosts on the network that can access or be accessed by other hosts on the network. This obviously includes computers and servers, but many other devices can also access the network. With the rapid growth of the Internet of Things (IoT), other types of devices are now endpoints on the network. This includes networked security cameras, controllers, and even light bulbs and appliances. Each endpoint is potentially a way for malicious software to gain access to a network. In addition, new technologies, such as cloud, expand the boundaries of enterprise networks to include locations on the Internet for which the enterprises are not responsible.

Devices that remotely access networks through VPNs are also endpoints that need to be considered. These endpoints could inject malware into the VPN network from the public network.

The following points summarize some of the reasons why malware remains a major challenge:

- More than 75% of organizations experienced adware infections from 2015 to 2016.
- From 2016 to early 2017, global spam volume increased dramatically (Figure 10-1); 8 to 10% of this spam can be considered to be malicious (Figure 10-2).

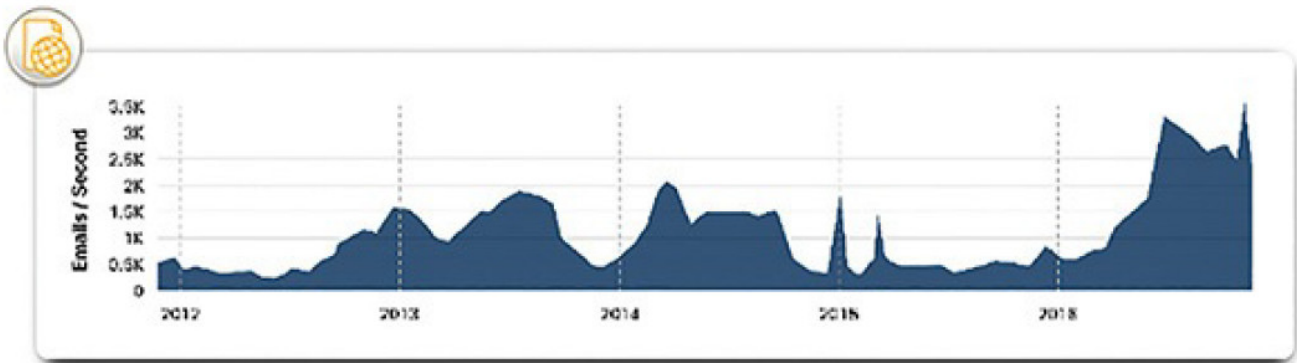


Figure 10-1 Total Spam Volume

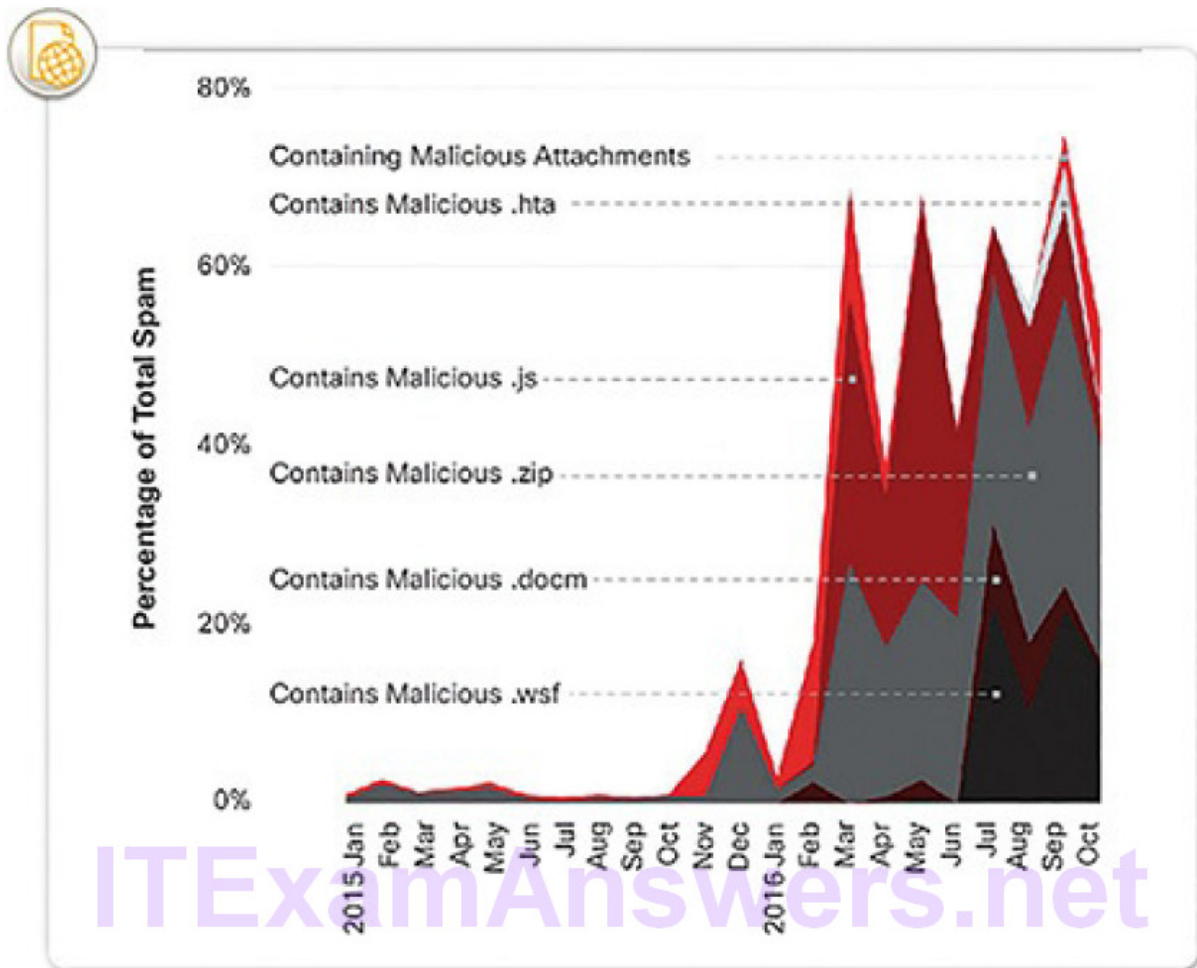


Figure 10-2 Malicious Spam Percentage

- Malware that targets the Android mobile operating system was in the top ten most common types of malware found in 2016.
- Several common types of malware have been found to significantly change features in less than 24 hours in order to evade detection.

### Endpoint Security (10.1.1.2)

News media commonly cover external network attacks on enterprise networks. These are some examples of such attacks:

- DoS attacks on an organization's network to degrade or even halt public access to it
- Breach of an organization's web server to deface their web presence
- Breach of an organization's data servers and hosts to steal confidential information

Various network security devices are required to protect the network perimeter from outside access. As shown in Figure 10-3, these devices could include a hardened router that is providing VPN services, a next-generation firewall (ASA in Figure 10-3), an IPS appliance, and an authentication, authorization, and accounting service (AAA server in Figure 10-3).

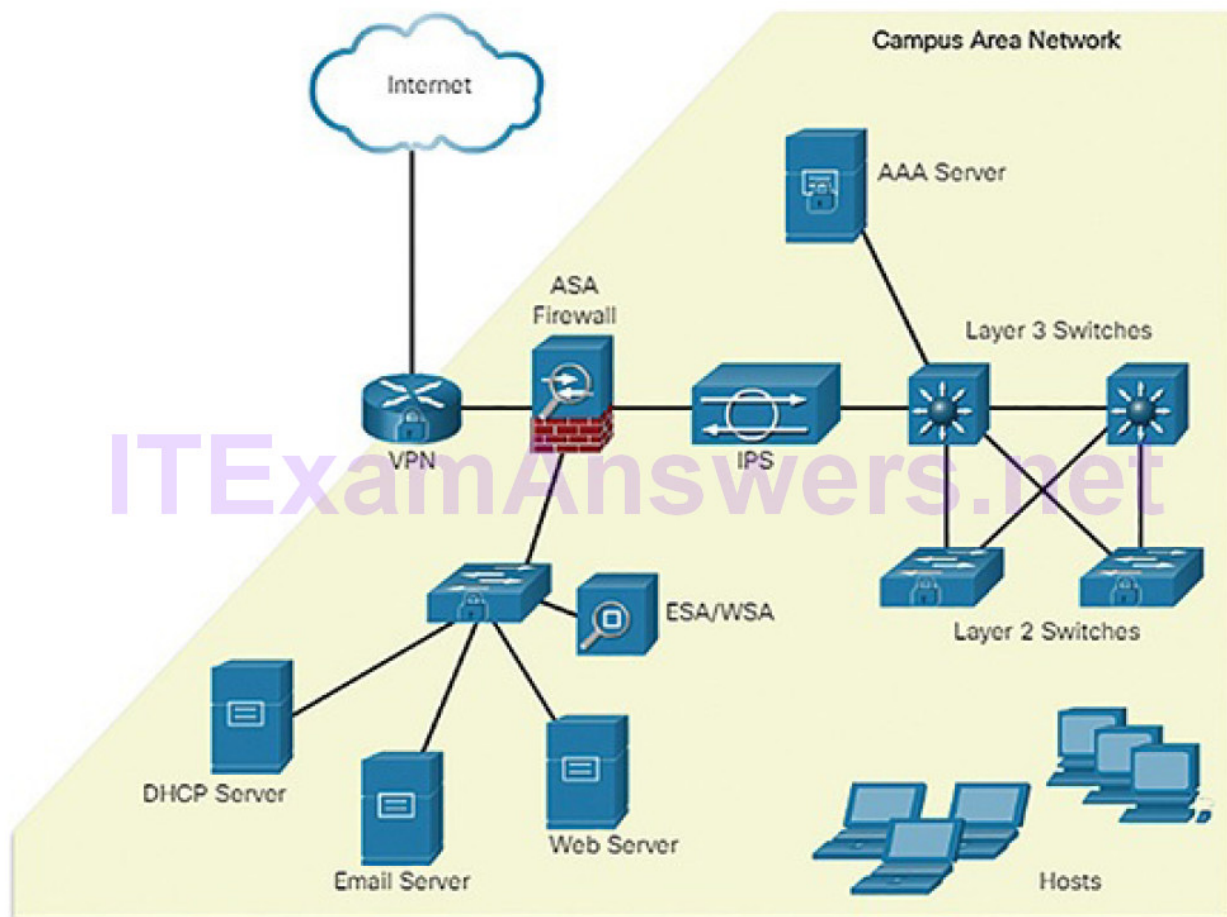


Figure 10-3 Internal LAN Elements

However, many attacks originate from inside the network. Therefore, securing an internal LAN is nearly as important as securing the outside network perimeter. Without a secure LAN, users within an organization are still susceptible to network threats and outages that can directly affect an organization's productivity and profit margin. After an internal host is infiltrated, it can become a starting point for an attacker to gain access to critical system devices, such as servers and sensitive information.

Specifically, there are two internal LAN elements to secure:

**Endpoints:** Hosts commonly consist of laptops, desktops, printers, servers, and IP phones, all of which are susceptible to malware-related attacks.

**Network infrastructure:** LAN infrastructure devices interconnect endpoints and typically include switches, wireless devices, and IP telephony devices. Most of these devices are susceptible to LAN-related attacks including MAC address table overflow attacks, spoofing attacks, DHCP-related attacks, LAN storm attacks, STP manipulation attacks, and VLAN attacks.

This chapter focuses on securing endpoints.

### Host-Based Malware Protection (10.1.1.3)

---

The network perimeter is always expanding. People access corporate network resources with mobile devices that use remote access technologies such as VPN. These same devices are also used on unsecured, or minimally secured, public and home networks. Host-based antimalware/antivirus software and host-based firewalls are used to protect these devices.

#### Antivirus/Antimalware Software

Antivirus/antimalware is software that is installed on a host to detect and mitigate viruses and malware. Examples are Windows Defender (Figure 10-4), Norton Security, McAfee, Trend Micro, and others.

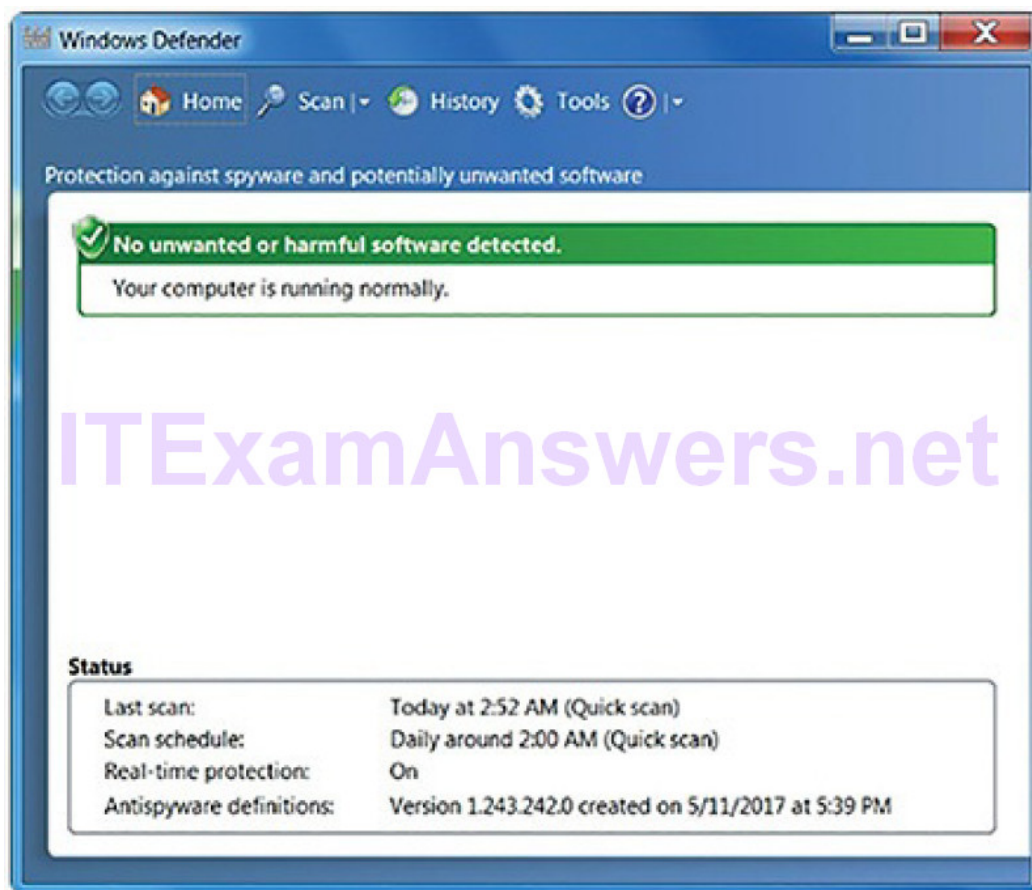


Figure 10-4 Windows Defender

Antimalware programs may detect viruses using three different approaches:

**Signature-based:** This approach recognizes various characteristics of known malware files.

**Heuristics-based:** This approach recognizes general features shared by various types of malware.

**Behavior-based:** This approach employs analysis of suspicious behavior.

Many antivirus programs are able to provide real-time protection by analyzing data as it is used by the endpoint. These programs also scan for existing malware that may have entered the system prior to it being recognizable in real time.

Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system. Agentless systems have become popular for virtualized environments in which multiple OS instances are running on a host simultaneously. Agent-based antivirus running in each virtualized system can be a serious drain on system resources. Agentless antivirus for virtual hosts involves the use of a special security virtual appliance that performs optimized scanning tasks on the virtual hosts. An example of this is VMware's vShield.

#### Host-Based Firewall

This software is installed on a host. It restricts incoming and outgoing connections to connections initiated by that host only. Some firewall software can also prevent a host from becoming infected and stop infected hosts from spreading malware to other hosts. This function is included in some operating systems. For example, Windows includes Windows Defender (Figure 10-4) and Windows Firewall (Figure 10-5). Other solutions are produced by other companies or organizations. The Linux iptables and TCP Wrapper tools are examples. Host-based firewalls are discussed in more detail later in the chapter.



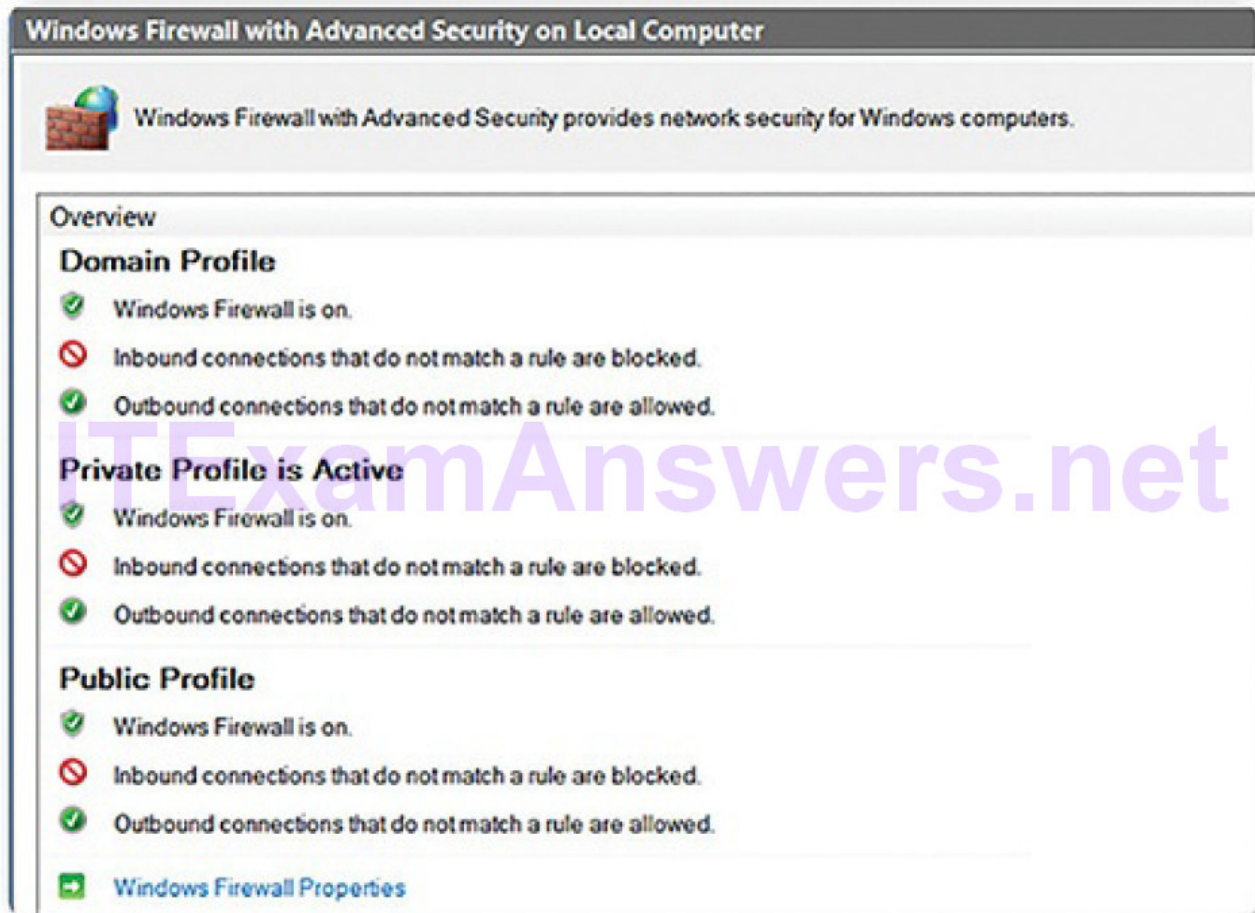


Figure 10-5 Windows Firewall

#### Host-Based Security Suites

It is recommended to install a host-based suite of security products on home networks as well as business networks. These host-based security suites include antivirus, anti-phishing, safe browsing, host-based intrusion prevention system, and firewall capabilities. These various security measures provide a layered defense that will protect against most common threats.

In addition to the protection functionality provided by host-based security products is the telemetry function. Most host-based security software includes robust logging functionality that is essential to cybersecurity operations. Some host-based security programs will submit logs to a central location for analysis.

There are many host-based security programs and suites available to users and enterprises. The independent testing laboratory AV-TEST, whose website is shown in Figure 10-6, provides high-quality reviews of host-based protections, as well as information about many other security products.

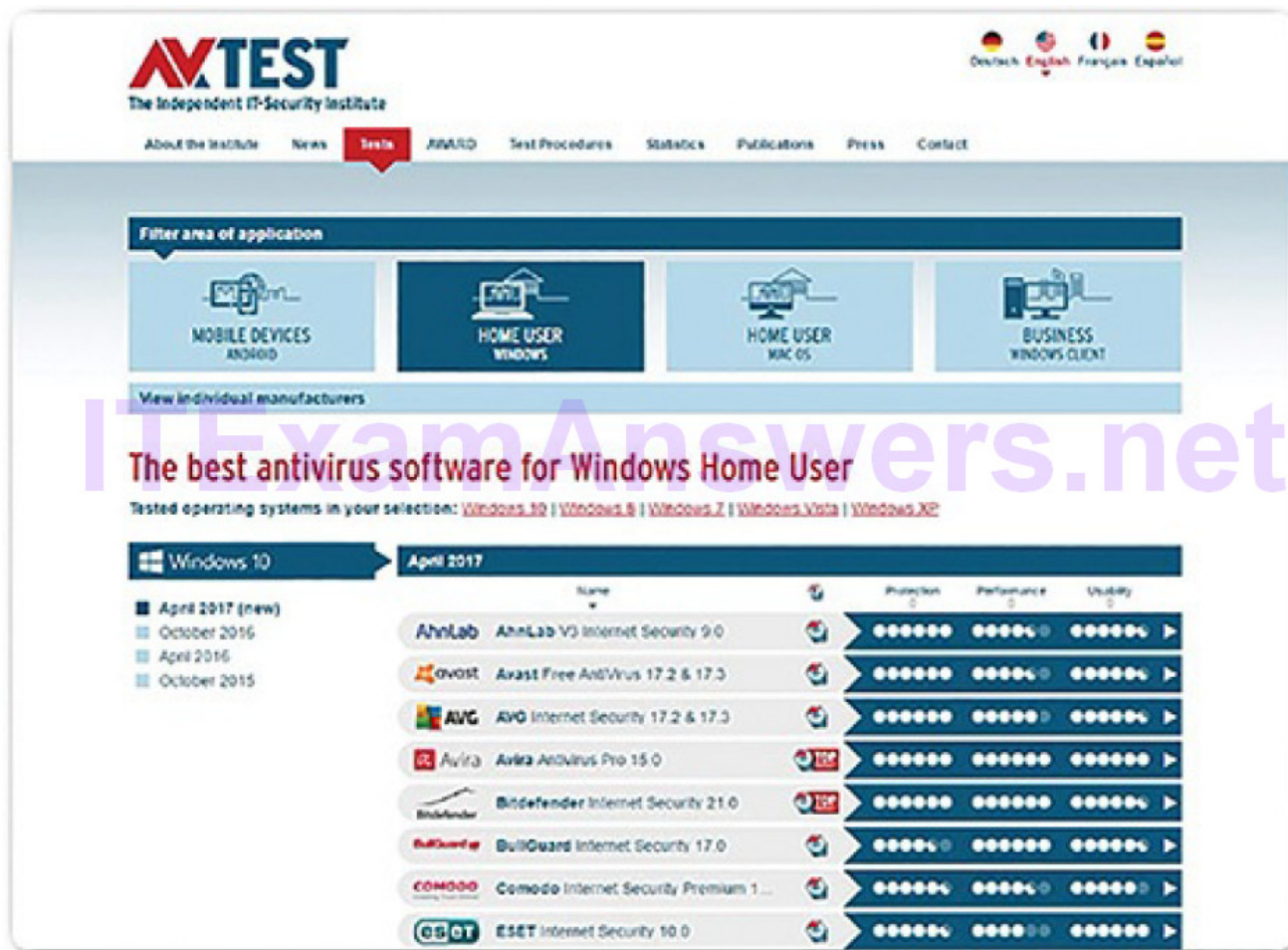


Figure 10-6 AV-TEST Website

#### Network-Based Malware Protection (10.1.1.4)

New security architectures for the borderless network address security challenges by having endpoints use network scanning elements. These devices provide many more layers of scanning than a single endpoint possibly could. Network-based malware prevention devices are also capable of sharing information among themselves to make better-informed decisions.

Protecting endpoints in a borderless network can be accomplished using both network-based and host-based techniques. The following are examples of devices and techniques that implement host protections and the network level:

**Advanced Malware Protection (AMP):** This provides endpoint protection from viruses and malware.

**Email Security Appliance (ESA):** This provides filtering of spam and potentially malicious emails before they reach the endpoint. An example is the Cisco ESA.

**Web Security Appliance (WSA):** This provides filtering of websites and blacklisting to prevent hosts from reaching dangerous locations on the web. The Cisco WSA provides control over how users access the Internet and can enforce acceptable use policies, control access to



specific sites and services, and scan for malware.

**Network Admission Control (NAC):** This permits only authorized and compliant systems to connect to the network.

These technologies work in concert with each other to give more protection than host-based suites can provide, as shown in Figure 10-7.

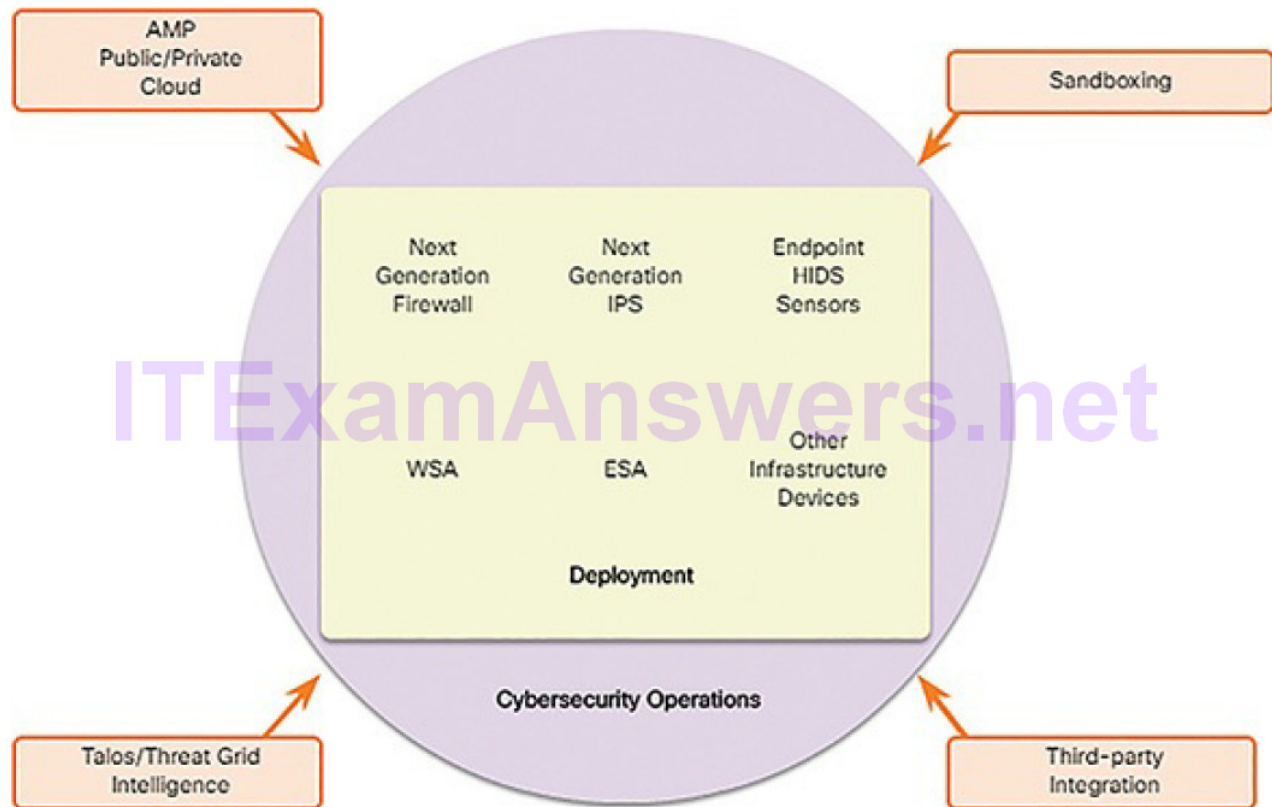


Figure 10-7 Network-Based Malware Protection Structure

### Cisco Advanced Malware Protection (AMP) (10.1.1.5)

Cisco Advanced Malware Protection (AMP) addresses all phases of a malware attack, from breach prevention to detection, response, and remediation. AMP is an integrated, enterprise-class malware analysis and protection solution. It provides comprehensive protection for organizations across the attack continuum:

**Before an attack:** AMP uses global threat intelligence from Cisco's Talos Security Intelligence and Research Group, and Threat Grid's threatintelligence feeds to strengthen defenses and protect against known and emerging threats.

**During an attack:** AMP uses that intelligence coupled with known file signatures and Cisco Threat Grid's dynamic malware analysis technology. It identifies and blocks policy-violating file types and exploit attempts, as well as malicious files trying to infiltrate the network.

**After an attack:** The solution goes beyond point-in-time detection capabilities and continuously monitors and analyzes all file activity and traffic, regardless of disposition, searching for any indications of malicious behavior. This happens not only after an attack, but also after a file is initially inspected. If a file with an unknown or previously deemed “good” disposition starts behaving badly, AMP will detect it and instantly alert security teams with an indication of compromise. It then provides visibility into where the malware originated, what systems were affected, and what the malware is doing. It also provides the controls to rapidly respond to the intrusion and remediate it with a few clicks. This gives security teams the level of deep visibility and control they need to quickly detect attacks, determine the impact, and contain malware before it causes damage.

Cisco AMP is very flexible and can be deployed on endpoints, on Cisco ASA and FirePOWER firewalls, and on various other appliances, such as ESA, WSA, and Meraki MX.

### **Activity 10.1.1.6: Identify Antimalware Terms and Concepts**

Refer to the online course to complete this Activity.

## **Host-Based Intrusion Protection (10.1.2)**

---

In this topic, you will learn how to explain host-based IPS/IDS log entries.

### **Host-Based Firewalls (10.1.2.1)**

---

Host-based firewalls are stand-alone software programs that control traffic entering or leaving a computer. Firewall apps are also available for Android phones and tablets.

Host-based firewalls may use a set of predefined policies, or profiles, to control packets entering and leaving a computer. They also may have rules that can be directly modified or created to control access based on addresses, protocols, and ports. Host-based firewall applications can also be configured to issue alerts to users if suspicious behavior is detected. They can then offer the user the ability to allow an offending application to run or to be prevented from running in the future.

Logging data varies depending on the firewall application. It typically includes date and time of the event, whether the connection was allowed or denied, information about the source or destination IP addresses of packets, and the source and destination ports of the encapsulated segments. In addition, common activities such as DNS lookups and other routine events can show up in host-based firewall logs, so filtering and other parsing techniques are useful for inspecting large amounts of log data.

One approach to intrusion prevention is the use of distributed firewalls. Distributed firewalls combine features of host-based firewalls with centralized management. The management function pushes rules to the hosts and may also accept log files from the hosts.

Whether installed completely on the host or distributed, host-based firewalls are an important layer of network security along with network-based firewalls. Here are some examples of host-based firewalls:

**Windows Firewall:** First included with Windows XP, Windows Firewall uses a profile-based approach to configuring firewall functionality. Access to public networks is assigned the restrictive Public firewall profile. The Private profile is for computers that are isolated from the Internet by other security devices, such as a home router with firewall functionality. The Domain profile is the third available profile. It is chosen for connections to a trusted network, such as a business network that is assumed to have an adequate security infrastructure. Windows Firewall has logging functionality and can be centrally managed with customized group security policies from a management server such as System Center 2012 Configuration Manager.

**iptables:** This is an application that allows Linux system administrators to configure network access rules that are part of the Linux kernel Netfilter modules.

**nftables:** The successor to iptables, nftables is a Linux firewall application that uses a simple virtual machine in the Linux kernel. Code is executed within the virtual machine that inspects network packets and implements decision rules regarding packet acceptance and forwarding.

**TCP Wrapper:** This is a rule-based access control and logging system for Linux. Packet filtering is based on IP addresses and network services.

### Host-Based Intrusion Detection (10.1.2.2)

---

The distinction between host-based intrusion detection and intrusion prevention is blurred. In fact, some sources refer to host-based intrusion detection and prevention systems (HIPDS). Because the industry seems to favor the use of the acronym HIDS, we will use it in our discussion here.

A host-based intrusion detection system (HIDS) is designed to protect hosts against known and unknown malware. An HIDS can perform detailed monitoring and reporting on the system configuration and application activity. It can provide log analysis, event correlation, integrity checking, policy enforcement, rootkit detection, and alerting. An HIDS will frequently include a management server endpoint, as shown in Figure 10-8.

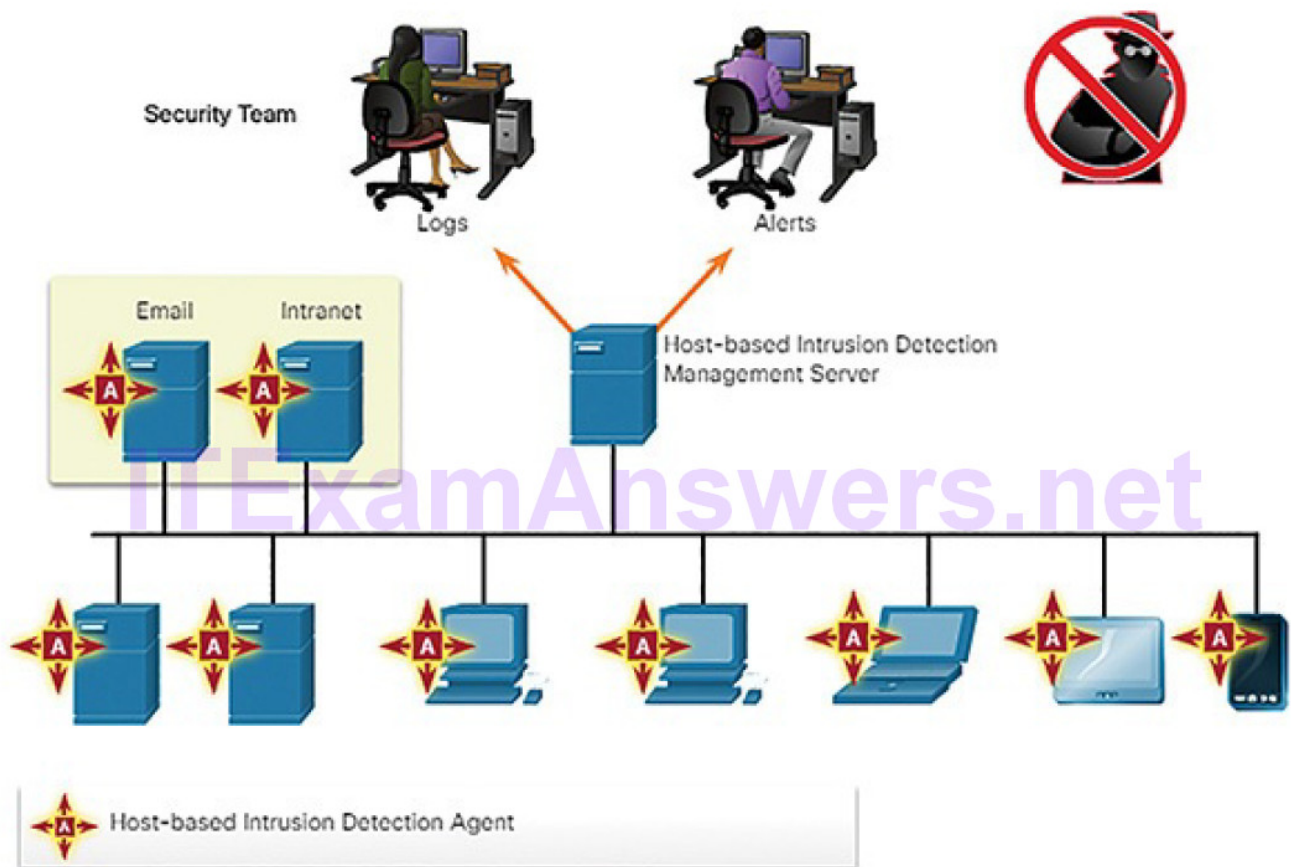


Figure 10-8 Host-Based Intrusion Detection Architecture

An HIDS is a comprehensive security application that combines the functionalities of antimalware applications with firewall functionality. An HIDS not only detects malware but also can prevent it from executing if it should reach a host. Because the HIDS software must run directly on the host, it is considered an agent-based system.

### HIDS Operation (10.1.2.3)

It can be said that host-based security systems function as both detection and prevention systems because they prevent known attacks and detect unknown potential attacks. An HIDS uses both proactive and reactive strategies. An HIDS can prevent intrusion because it uses signatures to detect known malware and prevent it from infecting a system. However, this strategy is only good against known threats. Signatures are not effective against new, or zero day, threats. In addition, some malware families exhibit polymorphism. This means that variations of a type, or family, of malware may be created by attackers that will evade signature-based detections by changing aspects of the malware signature just enough so that it will not be detected. An additional set of strategies are used to detect the possibility of successful intrusions by malware that evades signature detection:

**Anomaly-based:** Host system behavior is compared to a learned baseline model. Significant deviations from the baseline are interpreted as the result of some sort of intrusion. If an intrusion is detected, the HIDS can log details of the intrusion, send alerts to

security management systems, and take action to prevent the attack. The measured baseline is derived from both user and system behavior. Because many things other than malware can cause system behavior to change, anomaly detection can create many erroneous results, which can increase the workload for security personnel and also lower the credibility of the system.

**Policy-based:** Normal system behavior is described by rules, or the violation of rules, that are predefined. Violation of these policies will result in action by the HIDS. The HIDS may attempt to shut down software processes that have violated the rules and can log these events and alert personnel to violations. Most HIDS software comes with a set of predefined rules. With some systems, administrators can create custom policies that can be distributed to hosts from a central policy management system.

#### **HIDS Products (10.1.2.4)**

---

There are a number of HIDS products on the market today. Most of them 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 are Cisco AMP, AlienVault Unified Security Management (USM), Tripwire, and Open Source HIDS SECurity (OSSEC).

OSSEC uses a central manager server and agents that are installed on individual hosts. Currently, agents only exist for Microsoft Windows platforms. For other platforms, OSSEC can also operate as an agentless system, and can be deployed in virtual environments. The OSSEC server can also receive and analyze alerts from a variety of network devices and firewalls over syslog. OSSEC monitors system logs on hosts and also conducts file integrity checking. OSSEC can detect rootkits, and can also be configured to run scripts or applications on hosts in response to event triggers.

#### **Activity 10.1.2.5: Identify the Host-Based Intrusion Protection Terminology**

Refer to the online course to complete this Activity.

#### **Application Security (10.1.3)**

---

In this topic, you will learn about attack surfaces, application blacklisting and whitelisting, and sandboxing.

##### **Attack Surface (10.1.3.1)**

---

Recall that a vulnerability is a weakness in a system or its design that could be exploited by a threat. An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker. The attack surface can consist of open ports on servers or hosts, software that runs on Internet-facing servers, wireless network protocols, and even users.

The attack surface is continuing to expand, as shown Figure 10-9.



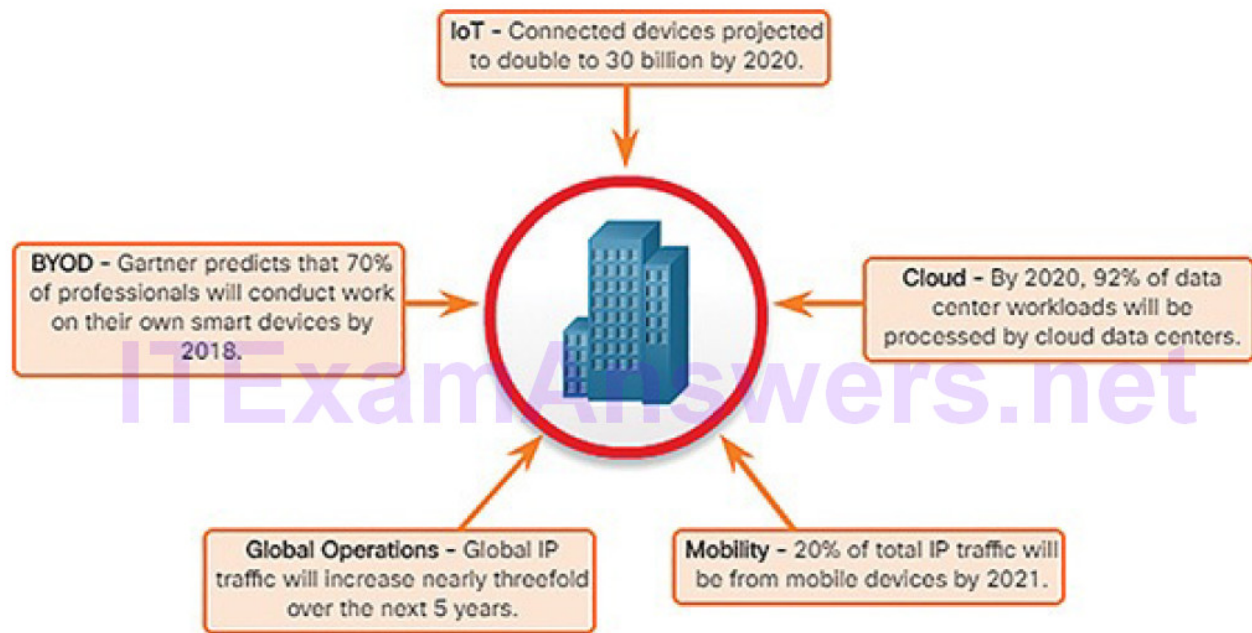


Figure 10-9 An Expanding Attack Surface

More devices are connecting to networks through the Internet of Things (IoT) and Bring Your Own Device (BYOD). Much of network traffic now flows between devices and some location in the cloud. Mobile device use continues to increase. All of these trends contribute to a prediction that global IP traffic will increase threefold in the next five years.

The SANS Institute describes three components of the attack surface:

**Network Attack Surface:** The attack exploits vulnerabilities in networks. This can include conventional wired and wireless network protocols, as well as other wireless protocols used by smartphones or IoT devices. Network attacks also exploit vulnerabilities at the network and transport layers.

**Software Attack Surface:** The attack is delivered through exploitation of vulnerabilities in web, cloud, or host-based software applications.

**Human Attack Surface:** The attack exploits weaknesses in user behavior. Such attacks include social engineering, malicious behavior by trusted insiders, and user error.

### Application Blacklisting and Whitelisting (10.1.3.2)

One way of decreasing the attack surface is to limit access to potential threats by creating lists of prohibited applications. This is known as blacklisting.

Application blacklists can dictate which user applications are not permitted to run on a computer, as shown in Figure 10-10. Similarly, whitelists can specify which programs are allowed to run, also shown in Figure 10-10. In this way, known vulnerable applications can be prevented from creating vulnerabilities on network hosts.

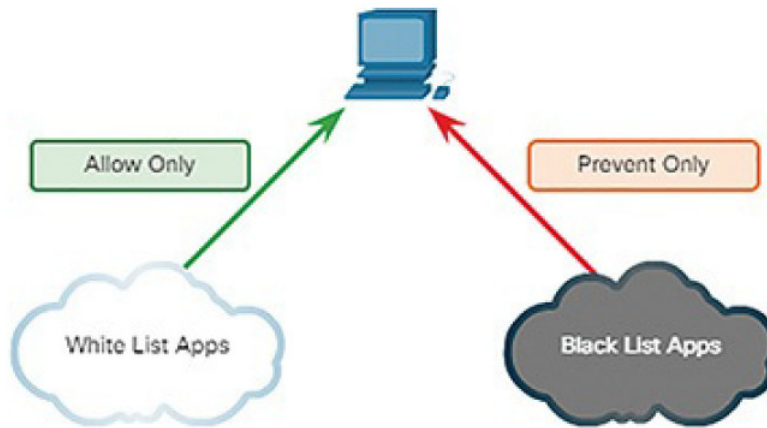


Figure 10-10 Application Blacklisting and Whitelisting

Whitelists are created in accordance with a security baseline that has been established by an organization. The baseline establishes an accepted amount of risk, and the environmental components that contribute to that level of risk. Non-whitelisted software can violate the established security baseline by increasing risk.

Figure 10-11 shows the Windows Local Group Policy Editor blacklisting and whitelisting settings.

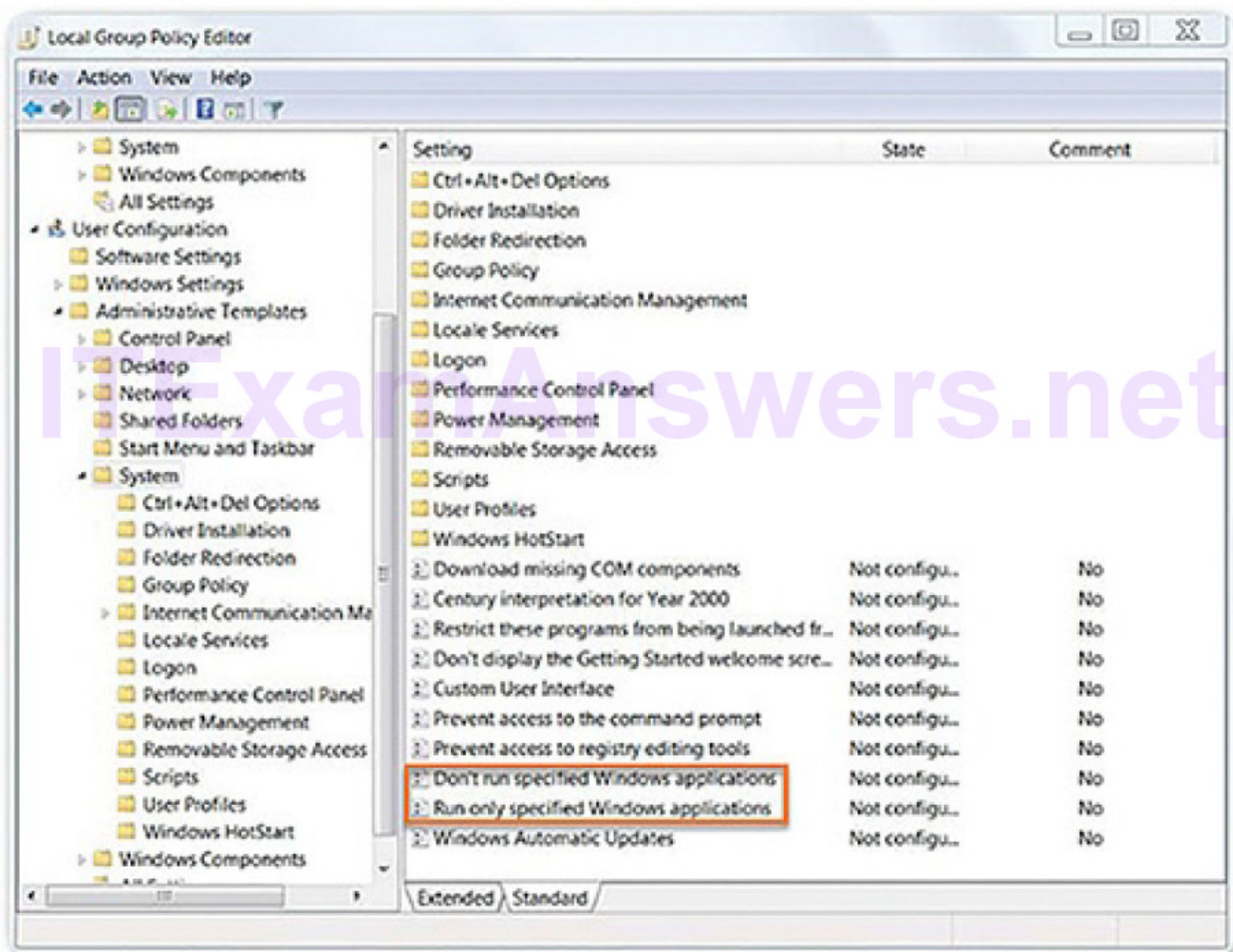


Figure 10-11 Editing Windows Local Group Policy

Figure 10-12 shows how entries can be added, in this case to the list of blacklisted applications.

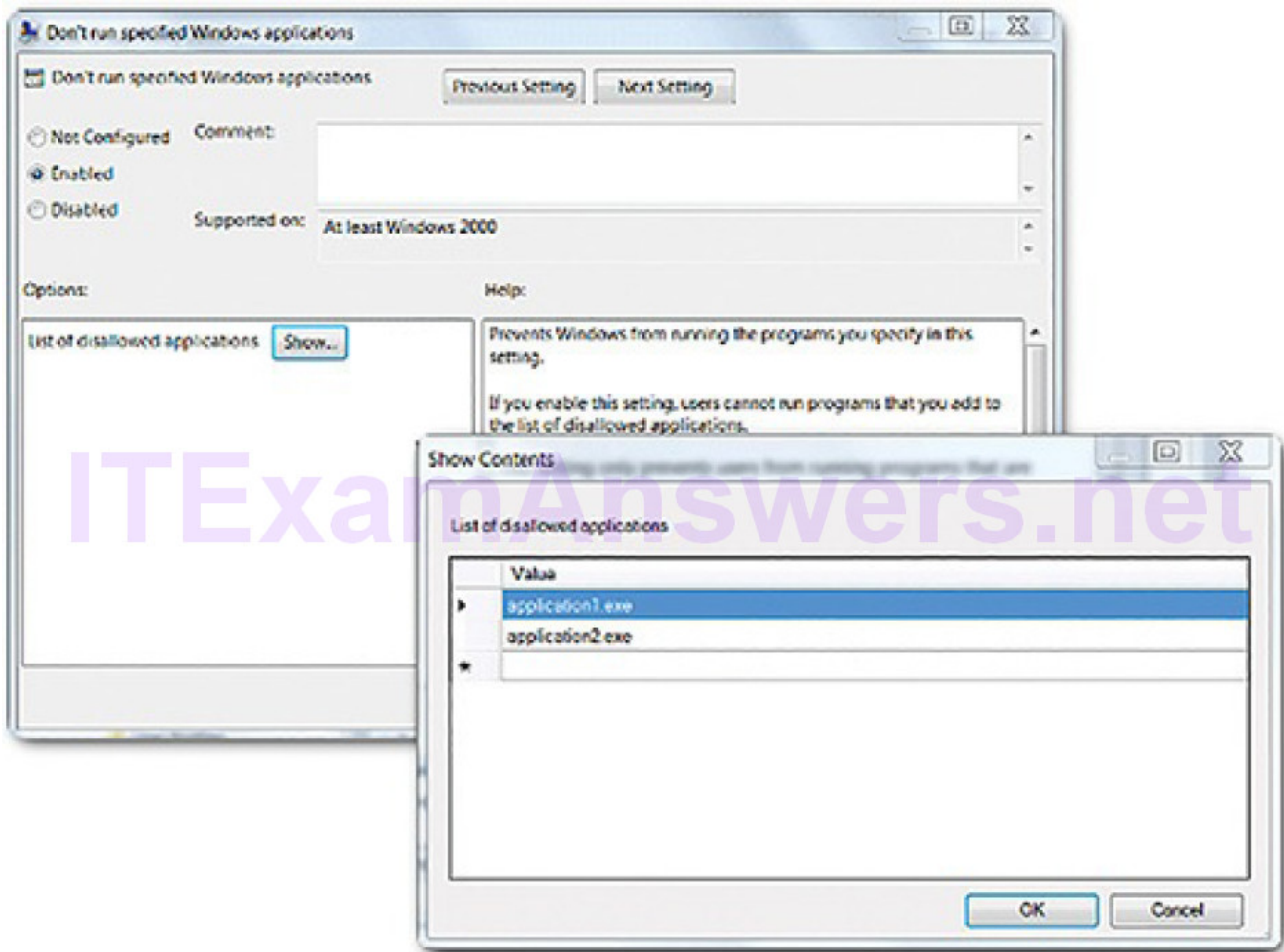


Figure 10-12 Verifying Windows Blacklisted Applications

Websites can also be whitelisted and blacklisted. These blacklists can be manually created, or they can be obtained from various security services. Blacklists can be continuously updated by security services and distributed to firewalls and other security systems that use them. Cisco's FireSIGHT security management system is an example of a device that can access the Cisco Talos security intelligence service to obtain blacklists. These blacklists can then be distributed to security devices within an enterprise network.

### System-Based Sandboxing (10.1.3.3)

Sandboxing is a technique that allows suspicious files to be executed and analyzed in a safe environment. Automated malware analysis sandboxes offer tools that analyze malware behavior. These tools observe the effects of running unknown malware so that features of malware behavior can be determined and then used to create defenses against it.

As mentioned previously, polymorphic malware changes frequently and new malware appears regularly. Malware will enter the network despite the most robust perimeter and host-based security systems. HIDS and other detection systems can create alerts on suspected malware that may have entered the network and executed on a host. Systems such as Cisco AMP can track the trajectory of a file through the network, and can “roll back” network events to obtain a copy of the downloaded file. This file can then be executed in a sandbox, such as Cisco Threat Grid Glovebox, and the activities of the file documented by the system. This information can then be used to create signatures to prevent the file from entering the network again. The information can also be used to create detection rules and automated plays that will identify other systems that have been infected.

Cuckoo Sandbox is a free malware analysis system sandbox. It can be run locally and have malware samples submitted to it for analysis.

A number of online public sandboxes also exist. These services allow malware samples to be uploaded for analysis. Some of these services are VirusTotal, Payload Security VxStream Sandbox, and Malwr.

#### **Video Demonstration 10.1.3.4: Using a Sandbox to Launch Malware**

Refer to the online course to view this video.

## **Endpoint Vulnerability Assessment (10.2)**

---

In this section, you will learn how to classify endpoint vulnerability assessment information.

### **Network and Server Profiling (10.2.1)**

---

In this topic, you will learn how to explain the value of network and server profiling.

#### **Network Profiling (10.2.1.1)**

---

In order to detect serious security incidents, it is important to understand, characterize, and analyze information about normal network functioning. Networks, servers, and hosts all exhibit typical behavior for a given point in time. Network and device profiling can provide a baseline that serves as a reference point. Unexplained deviations from the baseline may indicate a compromise.

Increased utilization of WAN links at unusual times can indicate a network breach and exfiltration of data. Hosts that begin to access obscure Internet servers, resolve domains that are obtained through dynamic DNS, or use protocols or services that are not needed by the system user can also indicate compromise. Deviations in network behavior are difficult to detect if normal behavior is not known.



Tools like NetFlow and Wireshark can be used to characterize normal network traffic characteristics. Because organizations can make different demands on their networks depending on the time of day or day of the year, network baselining should be carried out over an extended period of time. Some questions to ask when establishing a network baseline, as shown Figure 10-13, address important elements of the network profile:

**Session duration:** This is the time between the establishment of a data flow and its termination.

**Total throughput:** This is the amount of data passing from a given source to a given destination in a given period of time.

**Ports used:** This is a list of TCP or UDP processes that are available to accept data.

**Critical asset address space:** These are the IP addresses or the logical location of essential systems or data.

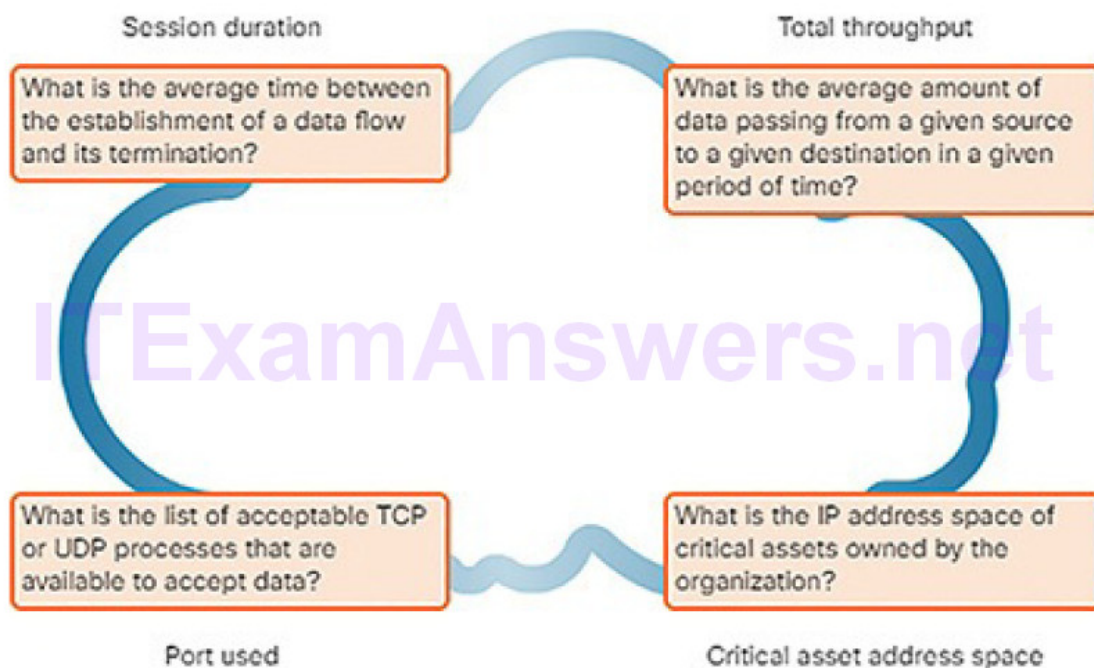


Figure 10-13 Elements of a Network Profile

In addition, a profile of the types of traffic that typically enter and leave the network is an important tool in understanding network behavior. Malware can use unusual ports that may not be typically seen during normal network operation. Host-to-host traffic is another important metric. Most network clients communicate directly with servers, so an increase of traffic between clients can indicate that malware is spreading laterally through the network. Finally, changes in user behavior, as revealed by AAA, server logs, or a user profiling system like Cisco Identity Services Engine (ISE), is another valuable indicator.

Knowing how individual users typically use the network leads to detection of potential



compromise of user accounts. A user who suddenly begins logging in to the network at strange times from a remote location should raise alarms if this behavior is a deviation from a known norm.

### Server Profiling (10.2.1.2)

---

Server profiling is used to establish the accepted operating state of servers. A server profile is a security baseline for a given server. It establishes the network, user, and application parameters that are accepted for a specific server.

In order to establish a server profile, it is important to understand the function that a server is intended to perform in a network. From there, various operating and usage parameters can be defined and documented. A server profile may establish the following:

**Listening ports:** These are the TCP and UDP daemons and ports that are allowed to be open on the server.

**User accounts:** These are the parameters defining user access and behavior.

**Service accounts:** These are the definitions of the type of service that an application is allowed to run on a given host.

**Software environment:** This contains the tasks, processes, and applications that are permitted to run on the server.

### Network Anomaly Detection (10.2.1.3)

---

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. One approach to detection of network attacks is the analysis of this diverse, unstructured data using Big Data analytics techniques.

This entails the use of sophisticated statistical and machine learning techniques to compare normal performance baselines with network performance at a given time. Significant deviations can be indicators of compromise.

Anomaly detection can recognize network congestion caused by worm traffic that exhibits scanning behavior. Anomaly detection also can identify infected hosts on the network that are scanning for other vulnerable hosts.

Figure 10-14 illustrates a simplified version of an algorithm designed to detect an unusual condition at the border routers of an enterprise.

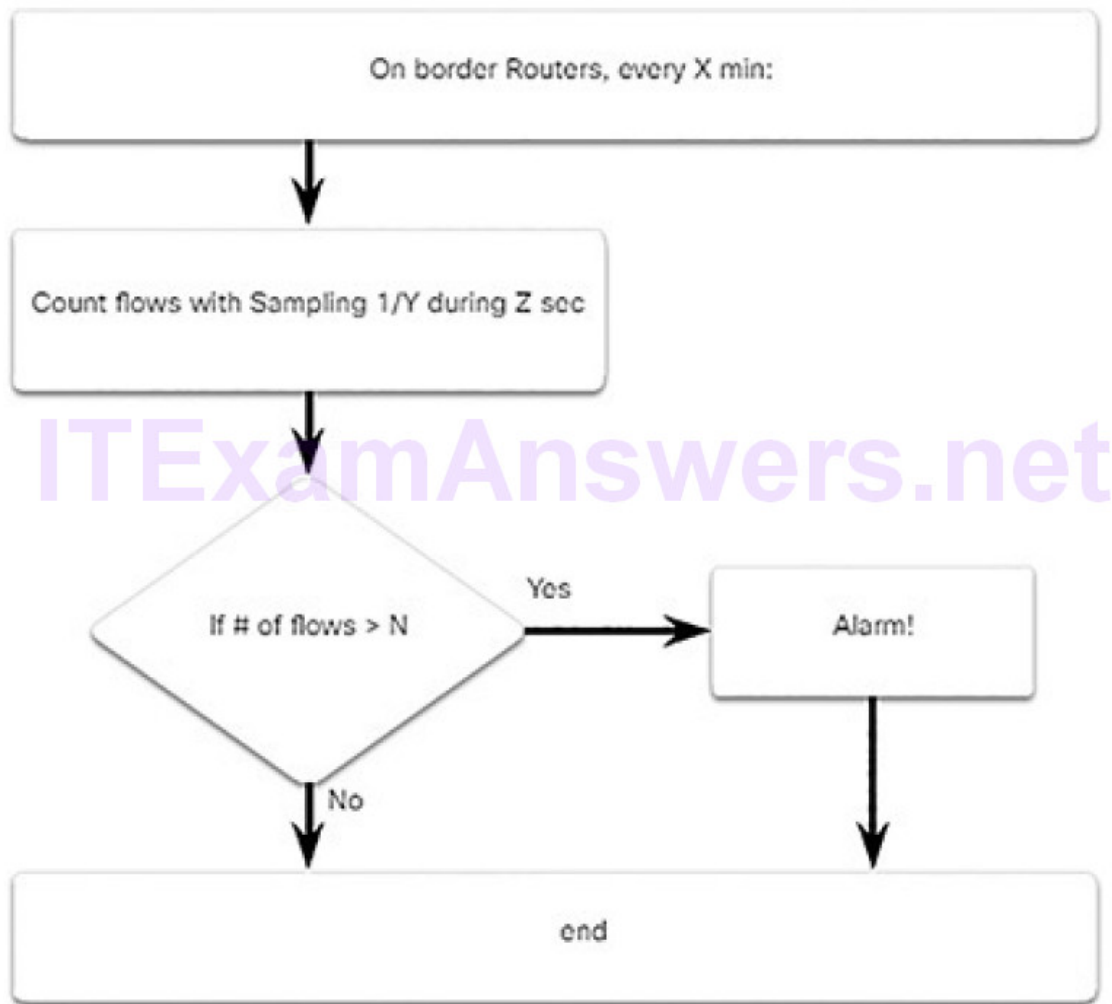


Figure 10-14 Example of a Simple Anomaly Detection Algorithm

For example, the cybersecurity analyst could provide the following values:

$X = 5$

$Y = 100$

$Z = 30$

$N = 500$

Now, the algorithm can be interpreted as “Every 5th minute, get a sampling of 1/100th of the flows during second 30. If the number of flows is greater than 500, generate an alarm. If the number of flows is less than 500, do nothing.” This is a simple example of using a traffic profile to identify the potential for data loss.

#### Network Vulnerability Testing (10.2.1.4)

---

Most organizations connect to public networks in some way due to the need to access the Internet. These organizations must also provide Internet-facing services of various types to the public. Because of the vast number of potential vulnerabilities, and the fact that new

vulnerabilities can be created within an organization network and its Internet-facing services, periodic security testing is essential. Network security can be tested using a variety of tools and services. Various types of tests can be performed:

**Risk analysis:** This is a discipline in which analysts evaluate the risk posed by vulnerabilities to a specific organization. A risk analysis includes assessment of the likelihood of attacks, identifies types of likely threat actors, and evaluates the impact of successful exploits on the organization.

**Vulnerability assessment:** This test employs software to scan Internet-facing servers and internal networks for various types of vulnerabilities. These vulnerabilities include unknown infections, weaknesses in web-facing database services, missing software patches, unnecessary listening ports, etc. Tools for vulnerability assessment include the open source OpenVAS platform, Microsoft Baseline Security Analyzer, Nessus, Qualys, and FireEye Mandiant services. Vulnerability assessment includes, but goes beyond, port scanning.

**Penetration testing:** This type of test uses authorized simulated attacks to test the strength of network security. Internal personnel with hacker experience, or professional ethical hackers, identify assets that could be targeted by threat actors. A series of exploits is used to test security of those assets. Simulated exploit software tools are frequently used. Penetration testing does not only verify that vulnerabilities exist, it actually exploits those vulnerabilities to determine the potential impact of a successful exploit. An individual penetration test is often known as a pen test. Metasploit is a tool used in penetration testing. Core Impact offers penetration testing software and services.

### **Activity 10.2.1.5: Identify the Elements of Network Profiling**

Refer to the online course to complete this Activity.

## **Common Vulnerability Scoring System (CVSS) (10.2.2)**

---

In this topic, you will learn how to classify CVSS reports.

### **CVSS Overview (10.2.2.1)**

---

The 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. The third revision, CVSS 3.0, is a vendor-neutral, industry-standard, open framework for weighting the risks of a vulnerability using a variety of metrics. These weights combine to provide a score of the risk inherent in a vulnerability. The numeric score can be used to determine the urgency of the vulnerability, and the priority of addressing it. The benefits of the CVSS can be summarized as follows:

- It provides standardized vulnerability scores that should be meaningful across organizations.

- It provides an open framework with the meaning of each metric openly available to all users.
- It helps prioritize risk in a way that is meaningful to individual organizations.

The Forum of Incident Response and Security Teams (FIRST) has been designated as the custodian of the CVSS to promote its adoption globally. Version 3.0 was under development for 3 years, and Cisco and other industry partners contributed to the standard.

### CVSS Metric Groups (10.2.2.2)

Before performing a CVSS assessment, it is important to know key terms that are used in the assessment instrument.

Many of the metrics address the role of what the CVSS calls an authority. An authority is a computer entity, such as a database, operating system, or virtual sandbox, which grants and manages access and privileges to users.

As shown Figure 10-15, the CVSS uses three groups of metrics to assess vulnerability: Base, Temporal, and Environmental.

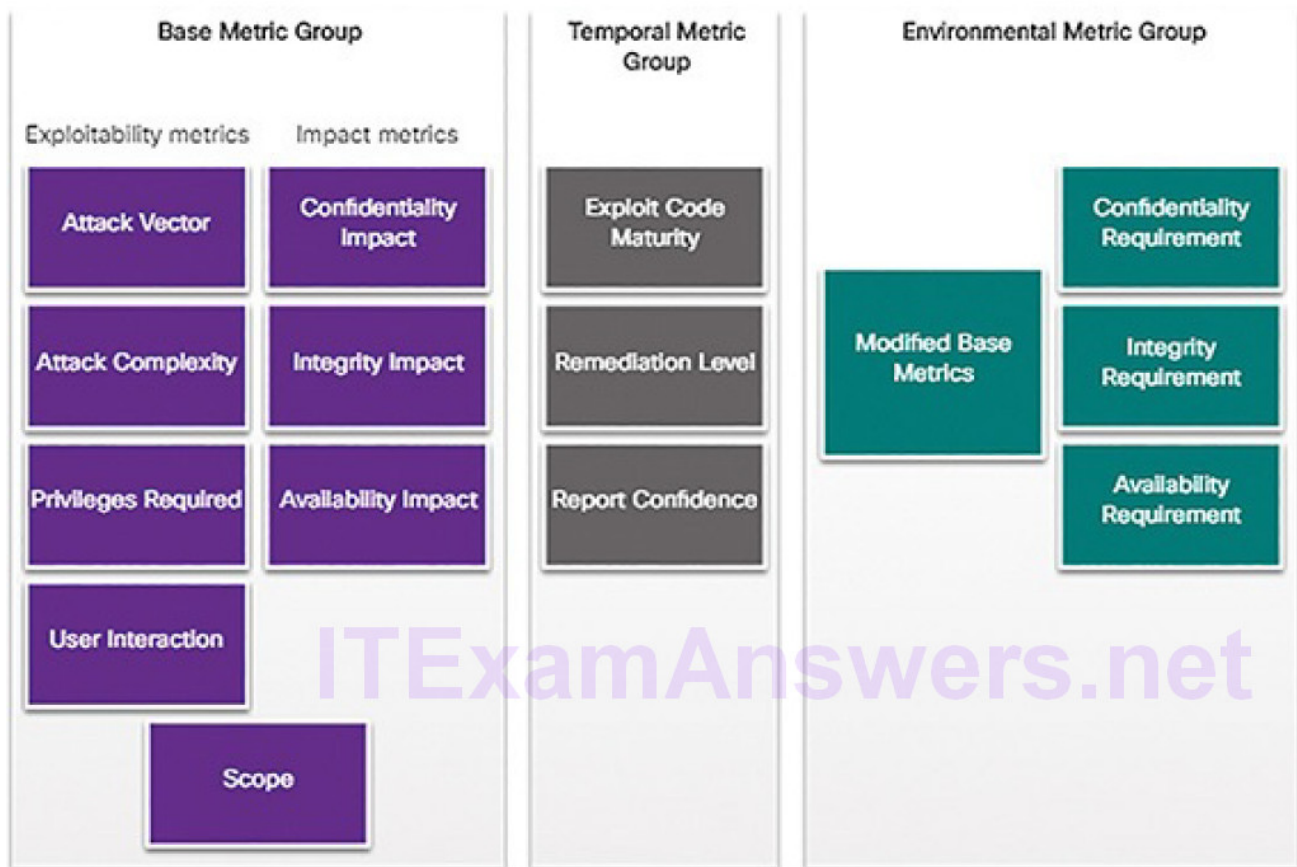


Figure 10-15 CVSS Metric Groups

Base Metric Group

This represents the characteristics of a vulnerability that are constant over time and across contexts. It has two classes of metrics:

**Exploitability:** These are features of the exploit such as the vector, complexity, and user interaction required by the exploit.

**Impact:** The impacts of the exploit are rooted in the CIA triad of confidentiality, integrity, and availability.

#### Temporal Metric Group

This measures the characteristics of a vulnerability that may change over time, but not across user environments. Over time, the severity of a vulnerability will change as it is detected and measures to counter it are developed. The severity of a new vulnerability may be high, but will decrease as patches, signatures, and other countermeasures are developed.

#### Environmental Metric Group

This measures the aspects of a vulnerability that are rooted in a specific organization's environment. These metrics help to guide consequences within an organization and also allow adjustment of metrics that are less relevant to what an organization does.

### CVSS Base Metric Group (10.2.2.3)

---

The Base metric group Exploitability metrics include the following:

**Attack Vector (AV):** This is a metric that reflects the proximity of the threat actor to the vulnerable component. The more remote the threat actor is to the component, the higher the severity. Threat actors close to your network or inside your network are easier to detect and mitigate.

**Attack Complexity (AC):** This is a metric that expresses the number of components, software, hardware, or networks that are beyond the attacker's control and that must be present in order for a vulnerability to be successfully exploited.

**Privileges Required (PR):** This is a metric that captures the level of access that is required for a successful exploit of the vulnerability.

**User Interaction (UI):** This metric expresses the presence or absence of the requirement for user interaction in order for an exploit to be successful.

**Scope (S):** This metric expresses whether multiple authorities must be involved in an exploit. This is expressed as whether the initial authority changes to a second authority during the exploit.

The Base metric group Impact metrics increase with the degree or consequence of loss due to the impacted component. Impact metrics include:



**Confidentiality Impact (C):** This is a metric that measures the impact to confidentiality due to a successfully exploited vulnerability. Confidentiality refers to the limiting of access to only authorized users.

**Integrity Impact (I):** This is a metric that measures the impact to integrity due to a successfully exploited vulnerability. Integrity refers to the trustworthiness and authenticity of information.

**Availability Impact (A):** This is a metric that measures the impact to availability due to a successfully exploited vulnerability. Availability refers to the accessibility of information and network resources. Attacks that consume network bandwidth, processor cycles, or disk space all impact the availability.

### The CVSS Process (10.2.2.4)

The CVSS Base metric group is designed as a way to assess security vulnerabilities found in software and hardware systems. It describes the severity of a vulnerability based on the characteristics of a successful exploit of the vulnerability. The other metric groups modify the base severity score by accounting for how the base severity rating is affected by time and environmental factors.

The CVSS process uses a tool called the CVSS v3.0 Calculator, shown in Figure 10-16.

The screenshot shows the CVSS v3.0 Calculator web application. The browser address bar displays the URL <https://www.first.org/cvss/calculator/3.0>. The page features the FIRST logo and a navigation menu with links to 'About FIRST', 'FIRST Members', 'Global Initiatives', 'Events', 'Security Library', and 'Newsroom'. A sidebar on the left lists various resources including the CVSS v3.0 Calculator, Specification Document, User Guide, Examples, and Archives. The main content area is titled 'Common Vulnerability Scoring System Version 3.0 Calculator' and includes a 'Base Score' section with dropdown menus for Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), and User Interaction (UI). To the right, there are sections for Scope (S), Confidentiality (C), Integrity (I), and Availability (A), each with a dropdown menu. A callout box on the right side of the form instructs the user to 'Select values for all base metrics to generate score'.

Figure 10-16 CVSS Calculator

The calculator is similar to a questionnaire in which choices are made that describe the vulnerability for each metric group. After all choices are made, a score is generated. Pop-up text that offers an explanation for each metric and metric value are displayed by hovering a mouse over each. Choices are made by choosing one of the values for the metric. Only one choice can be made per metric.

A detailed user guide that defines metric criteria, examples of assessments of common vulnerabilities, and the relationship of metric values to the final score is available to support the process.

After the Base metric group is completed, the numeric severity rating is displayed, as shown in Figure 10-17.

The screenshot displays a 'Base Score' calculation interface. At the top right, a yellow box shows the final score: **3.8 (Low)**. Below this, various metric groups are listed with their selected values highlighted in green:

- Attack Vector (AV):** Network (N), Adjacent (A), Local (L), Physical (P)
- Attack Complexity (AC):** Low (L), High (H)
- Privileges Required (PR):** None (N), Low (L), High (H)
- User Interaction (UI):** None (N), Required (R)
- Scope (S):** Unchanged (U), Changed (C)
- Confidentiality (C):** None (N), Low (L), High (H)
- Integrity (I):** None (N), Low (L), High (H)
- Availability (A):** None (N), Low (L), High (H)

At the bottom, a green box displays the **Vector String -** CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N.

Figure 10-17 Example of a Base Score Calculation

A vector string is also created that summarizes the choices made. If other metric groups are completed, those values are appended to the vector string. The string consists of the initial(s) for the metric, and an abbreviated value for the selected metric value separated by a colon. The metric-value pairs are separated by slashes. An example vector for the Base metric group is shown in the Figure 10-18. The vector strings allow the results of the assessment to be easily shared and compared.

Metric Name	Initials	Possible Values	Values
Attack Vector	AV	[N,A,L,P]	N = network A = adjacent L = local P = physical
Attack Complexity	AC	[L,H]	L = low H = high
Privileges Required	PR	[N,L,H]	N = none L = low H = high
User Interaction	UI	[N,R]	N = none R = required
Scope	S	[U,C]	U = unchanged C = changed
Confidentiality Impact	C	[H,L,N]	H = high L = low N = none
Integrity Impact	I	[H,L,N]	H = high L = low N = none
Availability Impact	A	[H,L,N]	H = high L = low

Metric Name	Values
Attack Vector, AV	Network
Attack Complexity, AC	Low
Privileges Required, PR	High
User Interaction, UI	None
Scope, S	Unchanged
Confidentiality Impact, C	Low
Integrity Impact, I	Low
Availability Impact, A	None

Figure 10-18 Example of a Vector for the Base Group Metric

In order for a score to be calculated for the Temporal or Environmental metric groups, the Base metric group must first be completed. The Temporal and Environmental metric values then modify the Base metric results to provide an overall score. The interaction of the scores for the metric groups is shown in Figure 10-19.

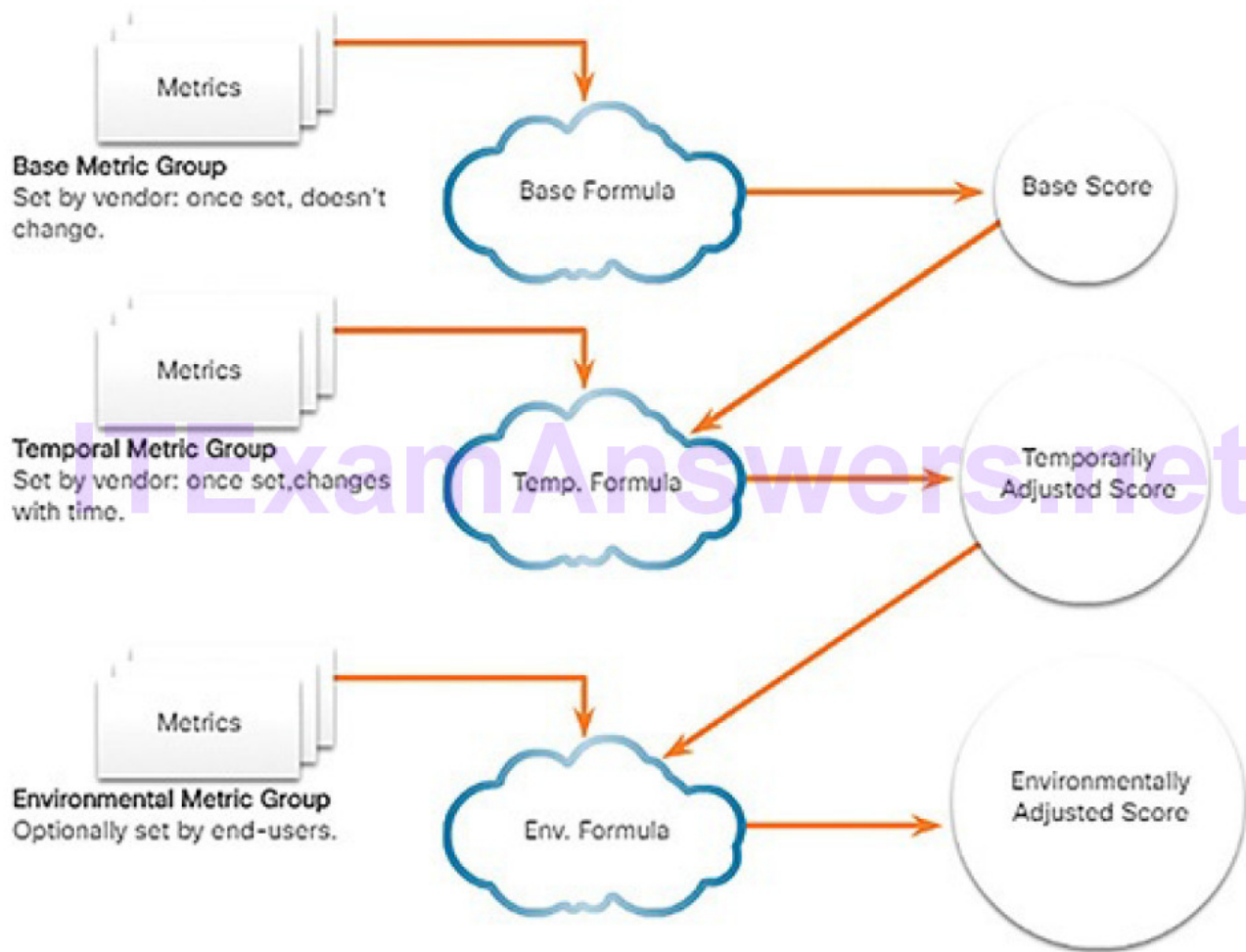


Figure 10-19 Interaction of CVSS Scores for Metric Groups

### CVSS Reports (10.2.2.5)

The ranges of scores and the corresponding qualitative meaning are shown in Table 10-1.

Table 10-1 CVSS Qualitative Scores for Ranges

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

Frequently, the Base and Temporal metric group scores will be supplied to customers by the application or security vendor in whose product the vulnerability has been discovered. The affected organization completes the Environmental metric group to tailor the vendor-supplied scoring to the local context.

The resulting score serves to guide the affected organization in the allocation of resources to address the vulnerability. The higher the severity rating, the greater the potential impact of an exploit and the greater the urgency in addressing the vulnerability. While not as precise as the numeric CVSS scores, the qualitative labels are very useful for communicating with stakeholders who are unable to relate to the numeric scores.

In general, any vulnerability that exceeds 3.9 should be addressed. The higher the rating level, the greater the urgency for remediation.

### **Other Vulnerability Information Sources (10.2.2.6)**

---

There are other important vulnerability information sources. These work together with the CVSS to provide a comprehensive assessment of vulnerability severity. There are two systems that operate in the United States: CVE and NVD.

#### **Common Vulnerabilities and Exposures (CVE)**

This is a dictionary of common names, in the form of CVE Identifiers, for known cybersecurity vulnerabilities. The CVE Identifier provides a standard way to research a reference to vulnerabilities. When a vulnerability has been identified, CVE Identifiers can be used to access fixes. In addition, threat intelligence services use CVE Identifiers, and they appear in various security system logs. The CVE Details website (<https://www.cvedetails.com/>) provides a linkage between CVSS scores and CVE information. It allows browsing of CVE vulnerability records by CVSS severity rating.

#### **National Vulnerability Database (NVD)**

This database 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. National Institute of Standards and Technology (NIST) agency.

### **Activity 10.2.2.7: Identify CVSS Metrics**

Refer to the online course to complete this Activity.

### **Compliance Frameworks (10.2.3)**

---

In this topic, you will learn how to explain compliance frameworks and reporting.

#### **Compliance Regulations (10.2.3.1)**

---



Recent history is full of instances in which sensitive information has been lost to threat actors. Recent security breaches at large retailers have resulted in the loss of personally identifiable information (PII) for millions of people. Corporations have lost valuable intellectual property which has resulted in the loss of millions of dollars in revenue. In addition, security breaches have resulted in the loss of sensitive information related to national security.

To prevent similar losses, 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. Organizations can verify compliance through the process of compliance assessment and audit. Assessments verify compliance or noncompliance for informational purposes. Audits also verify compliance but can result in consequences, such as financial penalties or loss of business opportunity.

This topic will discuss and differentiate the important and far reaching compliance regulations.

### **Overview of Regulatory Standards (10.2.3.2)**

---

There are five major regulatory compliance regulations.

#### **Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is a proprietary, non-governmental standard maintained by the Payment Card Industry Security Standards Council, which was formed by the five major credit card companies. The standard specifies requirements for the secure handling of customer credit card data by merchants and service providers. It dictates standards for how credit card information is to be stored and transmitted, and when customer information must be removed from storage systems.

PCI DSS applies to any entity that stores, processes, and/or transmits data about credit cardholders. As shown in Figure 10-20, cardholder data includes



Figure 10-20 Bank Cardholder Data

- Cardholder name
- Primary account number (PAN)
- Expiration date
- Service Code (part of the magnetic strip)
- Card Verification Code (CVC), Card Verification Value (CVV), Card Security Code (CSC)
- Card Identification Code (CID)
- Sensitive data stored on magnetic strip or chip

Many network management platforms include compliance reporting in their security management–related functionalities.

### **Federal Information Security Management Act of 2002 (FISMA)**

FISMA was established by NIST by an act of the U.S. Congress. FISMA regulations specify security standards for U.S. government systems and contractors to the U.S. government. FISMA also provides standards for the categorization of information and information systems according to a range of risk levels, and requirements for the security of information in each risk category.

### **Sarbanes-Oxley Act of 2002 (SOX)**

SOX set new or expanded requirements for all U.S. public company boards, management, and public accounting firms regarding the way in which corporations control and disclose financial information. The act is designed to ensure the integrity of financial practices and reporting. It also dictates controls for access to financial information and information systems.

### **Gramm-Leach-Bliley Act (GLBA)**

GLBA established that financial institutions must ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Financial institutions are considered to be banks, brokerages, insurance companies, etc.

### **Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA requires that all patient personally identifiable healthcare information be stored, maintained, and transmitted in ways that ensure patient privacy and confidentiality. HIPAA stipulates controlled access policies and data encryption of patient information. HIPAA specifies detailed administrative safeguards and implementation specifications in the areas of security management, workforce security, and information access management, among others.

### **Activity 10.2.3.3: Identify Regulatory Standards**

Refer to the online course to complete this Activity.

## **Secure Device Management (10.2.4)**

---

In this topic, you will learn how secure device management techniques are used to protect data and assets.

### **Risk Management (10.2.4.1)**

---

Risk management involves the selection and specification of security controls for an organization. It is part of an ongoing organization-wide information security program that involves the management of the risk to the organization or to individuals associated with the operation of a system.

Risk management is an ongoing, multistep, cyclical process, as shown in Figure 10-21.

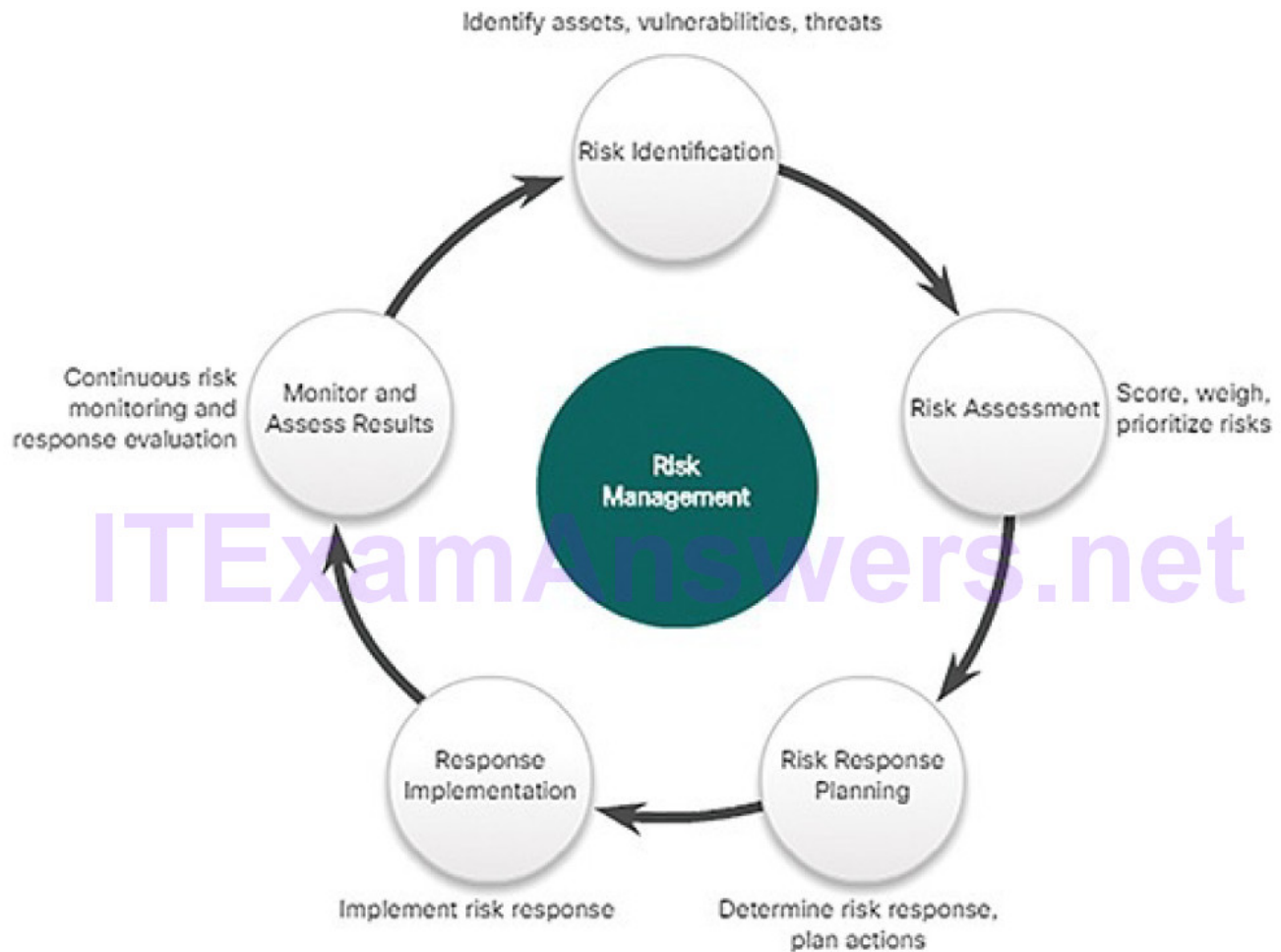


Figure 10-21 Risk Management

Risk is determined as the relationship between threat, vulnerability, and the nature of the organization. It first involves answering the following questions as part of a risk assessment:

- Who are the threat actors who want to attack us?
- What vulnerabilities can threat actors exploit?
- How would we be affected by attacks?
- What is the likelihood that different attacks will occur?

NIST Special Publication 800-30 describes risk assessment as:

...the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur.

A mandatory activity in risk assessment is the identification of threats and vulnerabilities and the matching of threats with vulnerabilities in what is often called threat-vulnerability (T-V) pairing. The T-V pairs can then be used as a baseline to indicate risk before security controls

are implemented. This baseline can then be compared to ongoing risk assessments as a means of evaluating risk management effectiveness. This part of risk assessment is referred to as determining the inherent risk profile of an organization.

After the risks are identified, they may be scored or weighted as a way of prioritizing risk reduction strategies. For example, vulnerabilities that are found to have corresponded with multiple threats can receive higher ratings. In addition, T-V pairs that map to the greatest institutional impact will also receive higher weightings.

There are four potential ways to respond to risks that have been identified, based on their weightings or scores:

**Risk avoidance:** Stop performing the activities that create risk. It is possible that as a result of a risk assessment, it is determined that the risk involved in an activity outweighs the benefit of the activity to the organization. If this is found to be true, then it may be determined that the activity should be discontinued.

**Risk reduction:** Decrease the risk by taking measures to reduce vulnerability. This involves implementing management approaches discussed earlier in this chapter. For example, if an organization uses server operating systems that are frequently targeted by threat actors, risk can be reduced through ensuring that the servers are patched as soon as vulnerabilities have been addressed.

**Risk sharing:** Shift some of the risk to other parties. For example, a risk-sharing technique might be to outsource some aspects of security operations to third parties. Hiring a security as a service (SECaaS) CSIRT to perform security monitoring is an example. Another example is to buy insurance that will help to mitigate some of the financial losses due to a security incident.

**Risk retention:** Accept the risk and its consequences. This strategy is acceptable for risks that have low potential impact and relatively high cost of mitigation or reduction. Other risks that may be retained are those that are so dramatic that they cannot realistically be avoided, reduced, or shared.

#### **Activity 10.2.4.2: Identify the Risk Response**

Refer to the online course to complete this Activity.

#### **Vulnerability Management (10.2.4.3)**

---

According to NIST, vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. The expected result is to reduce the time and money spent dealing with vulnerabilities and the exploitation

of those vulnerabilities. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation, and involve considerably less time and effort than responding after an exploitation has occurred.

Vulnerability management requires a robust means of identifying vulnerabilities based on vendor security bulletins and other information systems such as CVE. Security personnel must be competent in assessing the impact, if any, of vulnerability information they have received. Solutions should be identified with effective means of implementing and assessing the unanticipated consequences of implemented solutions. Finally, the solution should be tested to verify that the vulnerability has been eliminated.

The steps in the Vulnerability Management Life Cycle, shown in Figure 10-22, are described below:

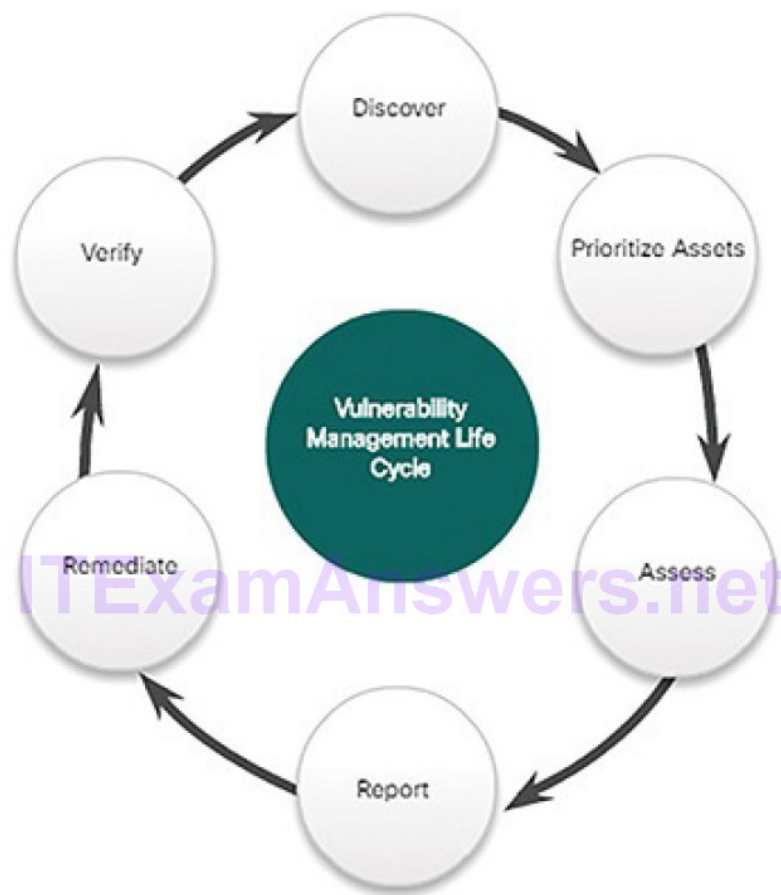


Figure 10-22 Vulnerability Management Life Cycle

**Discover:** Inventory all assets across the network and identify host details, including operating systems and open services, to identify vulnerabilities. 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 risks based on asset criticality, vulnerability, threats, and asset classification.

**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.

#### **Asset Management (10.2.4.4)**

---

Asset management involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise. As part of any security management plan, organizations must know what equipment accesses the network, where that equipment is within the enterprise and logically on the network, and what software and data those systems store or can access. Asset management not only tracks corporate assets and other authorized devices, but also can be used to identify devices that are not authorized on the network.

In publication NISTIR 8011 Volume 2, NIST specifies the detailed records that should be kept for each relevant device. NIST describes potential techniques and tools for operationalizing an asset management process:

- 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 noncompliant authorized assets
- Remediation or acceptance of device state, possible iteration of desired state definition
- Repeat the process at regular intervals, or ongoing

Figure 10-23 provides an overview of this process.

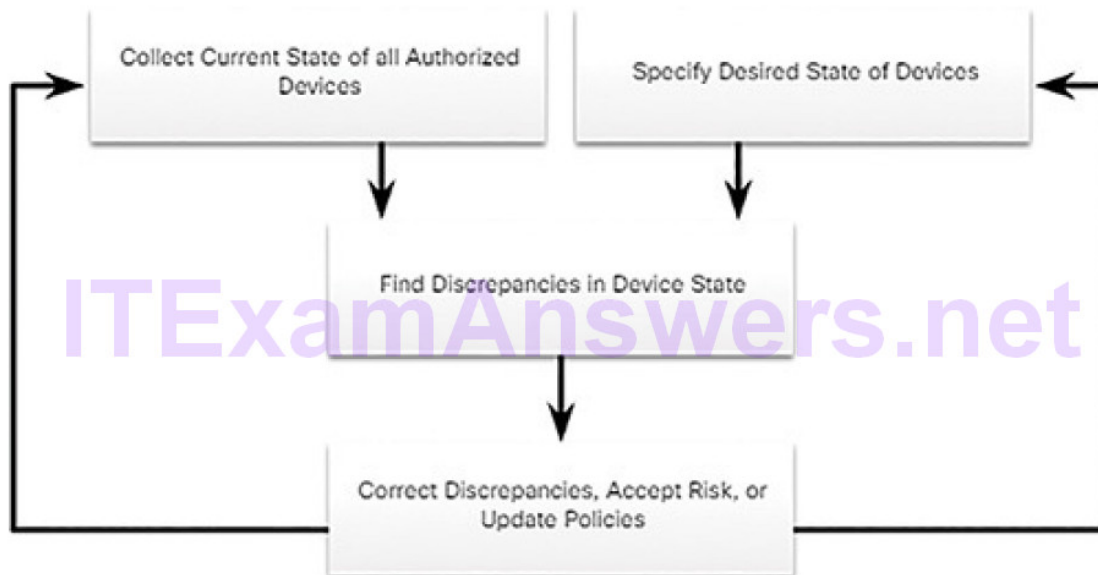


Figure 10-23 An Operational Concept for Asset Management

#### Mobile Device Management (10.2.4.5)

Mobile device management (MDM), especially in the age of BYOD, presents special challenges to asset management. Mobile devices cannot be physically controlled on the premises of an organization. They can be lost, stolen, or tampered with, putting data and network access at risk. Part of an MDM plan is taking action when devices leave the custody of the responsible party. Measures that can be taken include disabling the lost device, encrypting the data on the device, and enhancing device access with more robust authentication measures.

Due to the diversity of mobile devices, it is possible that some devices that will be used on the network are inherently less secure than others. Network administrators should assume that all mobile devices are untrusted until they have been properly secured by the organization.

MDM systems, such as Cisco Meraki Systems Manager, shown in Figure 10-24, allow security personnel to configure, monitor, and update a very diverse set of mobile clients from the cloud.

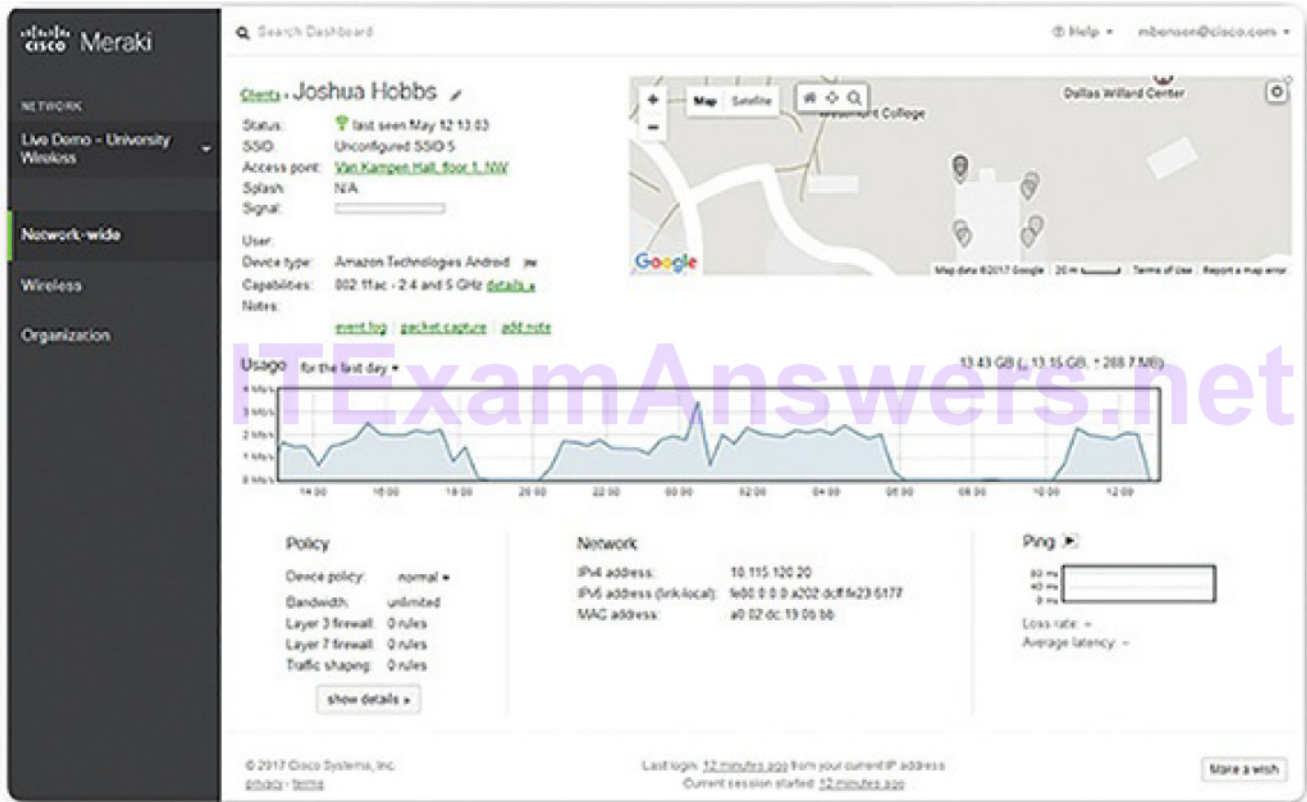


Figure 10-24 Cisco Meraki Systems Manager

### Configuration Management (10.2.4.6)

Configuration management addresses the inventory and control of hardware and software configurations of systems. Secure device configurations reduce security risk. For example, an organization provides many computers and laptops to its workers. This enlarges the attack surface for the organization, because each system may be vulnerable to exploits. To manage this, the organization may create baseline software images and hardware configurations for each type of machine. These images may include a basic package of required software, endpoint security software, and customized security policies that control user access to aspects of the system configuration that could be made vulnerable. Hardware configurations may specify the permitted types of network interfaces and the permitted types of external storage.

Configuration management extends to the software and hardware configuration of networking devices and servers as well. 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.”

For internetworking devices, software tools are available that will back up configurations, detect changes in configuration files, and enable bulk change of configurations across a number of devices.

With the advent of cloud data centers and virtualization, management of numerous servers presents special challenges. Configuration management tools like Puppet, Chef, Ansible, and SaltStack were developed to allow efficient management of servers that enable cloud-based computing.

#### **Enterprise Patch Management (10.2.4.7)**

---

Patch management is related to vulnerability management. Vulnerabilities frequently appear in critical client, server, and networking device operating systems and firmware. Application software, especially Internet applications and frameworks like Acrobat, Flash, and Java, also are frequently discovered to have vulnerabilities. Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, and installing required patches, and verifying that the patches are installed on all required systems. Installing patches is frequently the most effective way to mitigate software vulnerabilities. Sometimes, it is the only way to do so.

Patch management is required by some security compliance regulations, such as SOX and HIPAA. Failure to implement patches in a systematic and timely manner could result in audit failure and penalties for noncompliance. Patch management depends on asset management data to identify systems that are running software that requires patching. Figure 10-25 shows a screenshot of the SolarWinds Patch Manager tool.

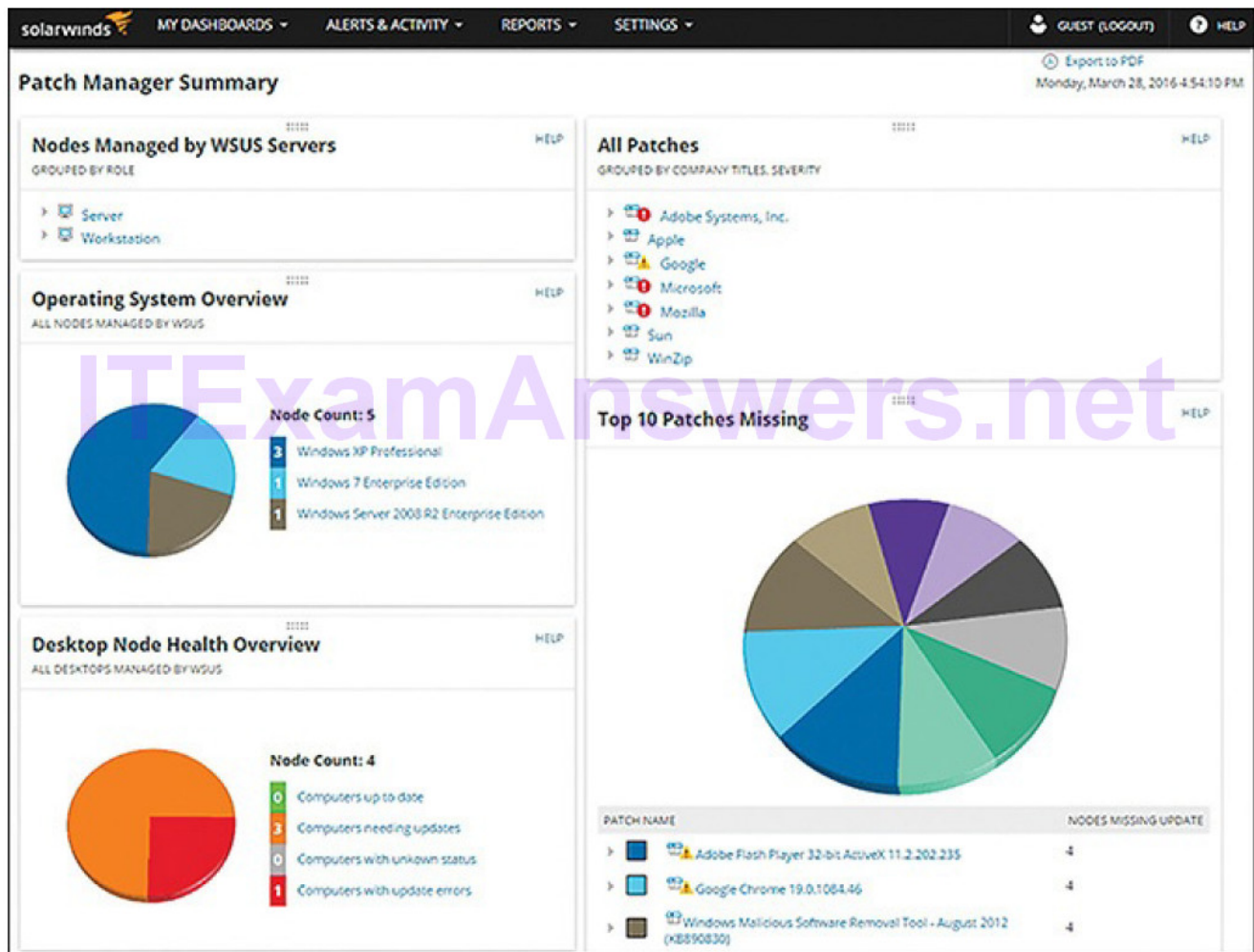


Figure 10-25 SolarWinds Patch Manager

### Patch Management Techniques (10.2.4.8)

At the enterprise level, patch management is most efficiently run from a patch management system. Most patch management systems incorporate a client-centralized server architecture, as do other end point–related security systems. There are three patch management technologies:

**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, determines if patches exist that require installation, and installs the patches (Figure 10-26). The agent runs with sufficient privileges to allow it to install the patches. Agent-based approaches are the preferred means of patching mobile devices.

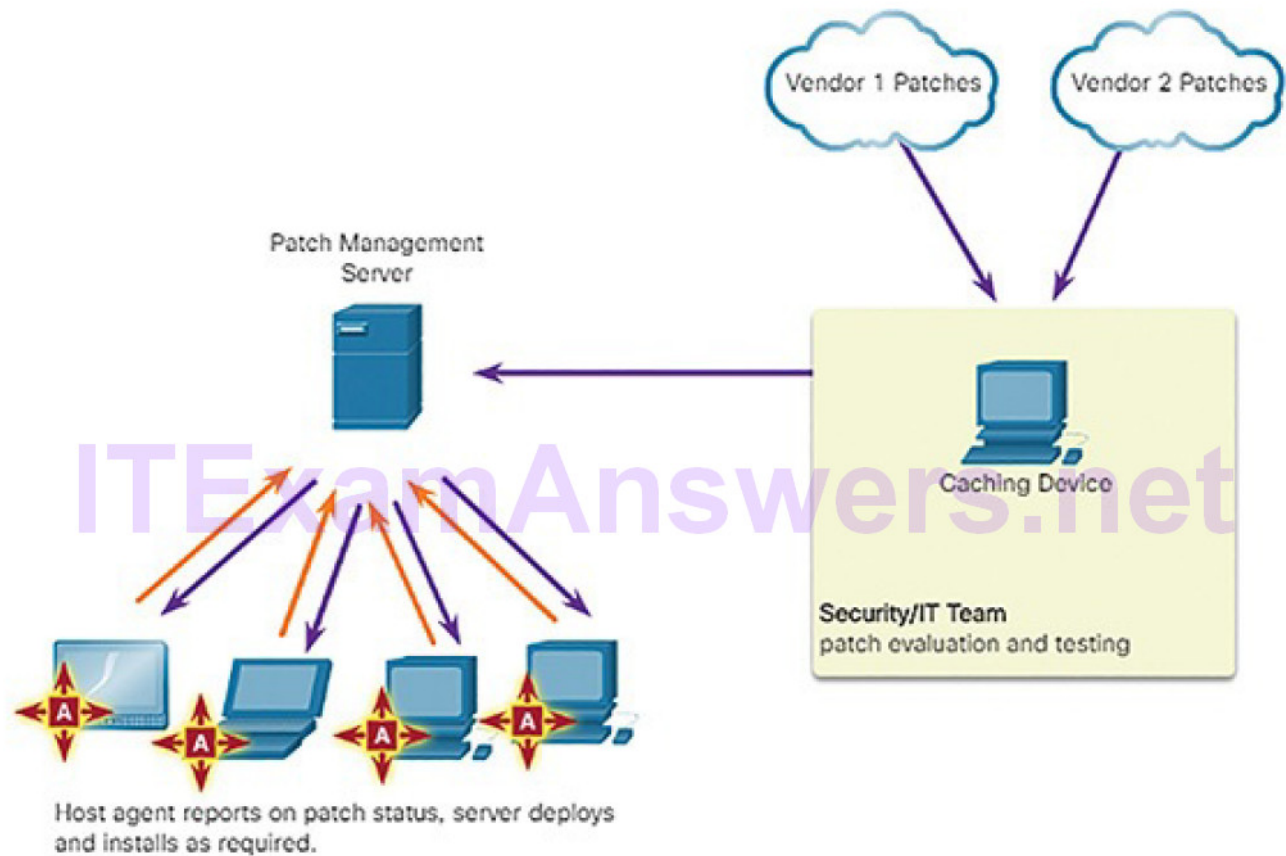


Figure 10-26 Agent-Based Patch Management

**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 (Figure 10-27). Only devices that are on scanned network segments can be patched in this way.

This can be a problem for mobile devices.



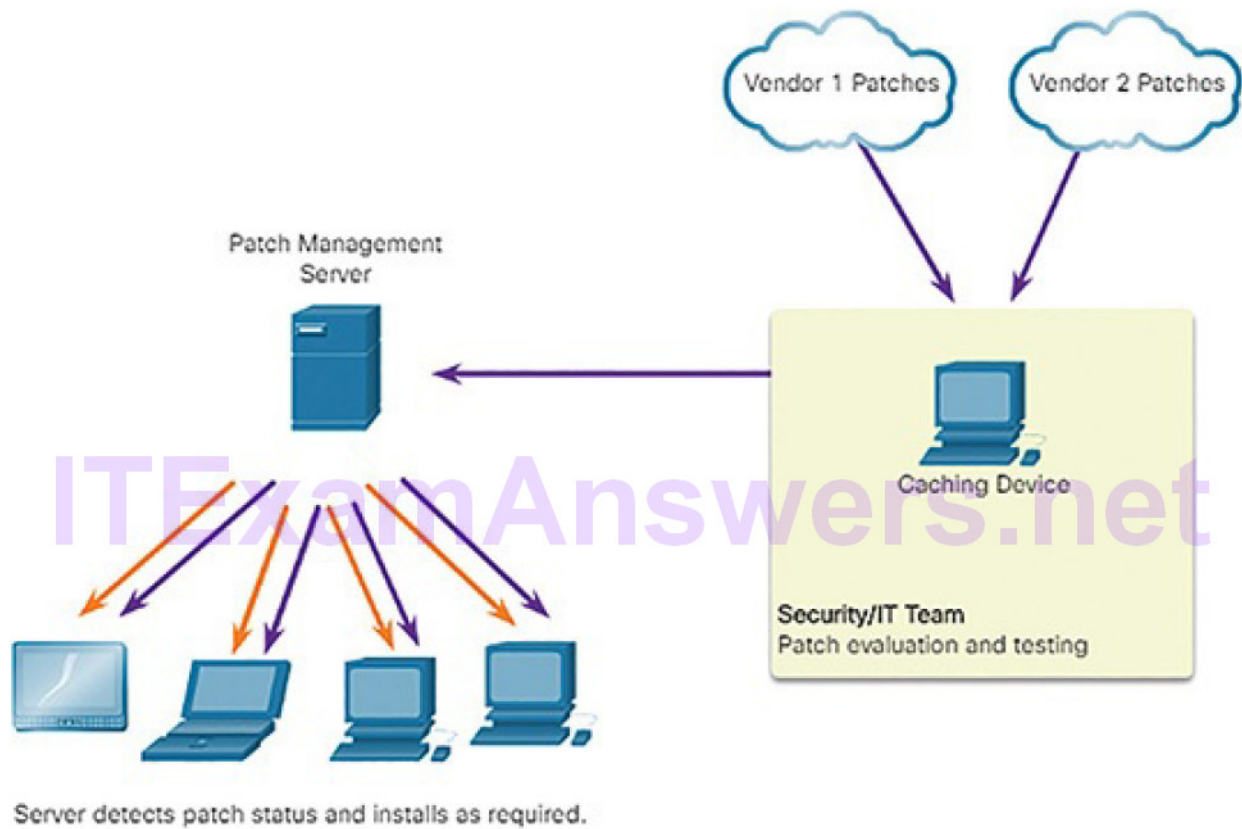


Figure 10-27 Agentless Scanning Patch Management

**Passive network monitoring:** Devices requiring patching are identified through the monitoring of traffic on the network (Figure 10-28). This approach is only effective for software that includes version information in its network traffic.

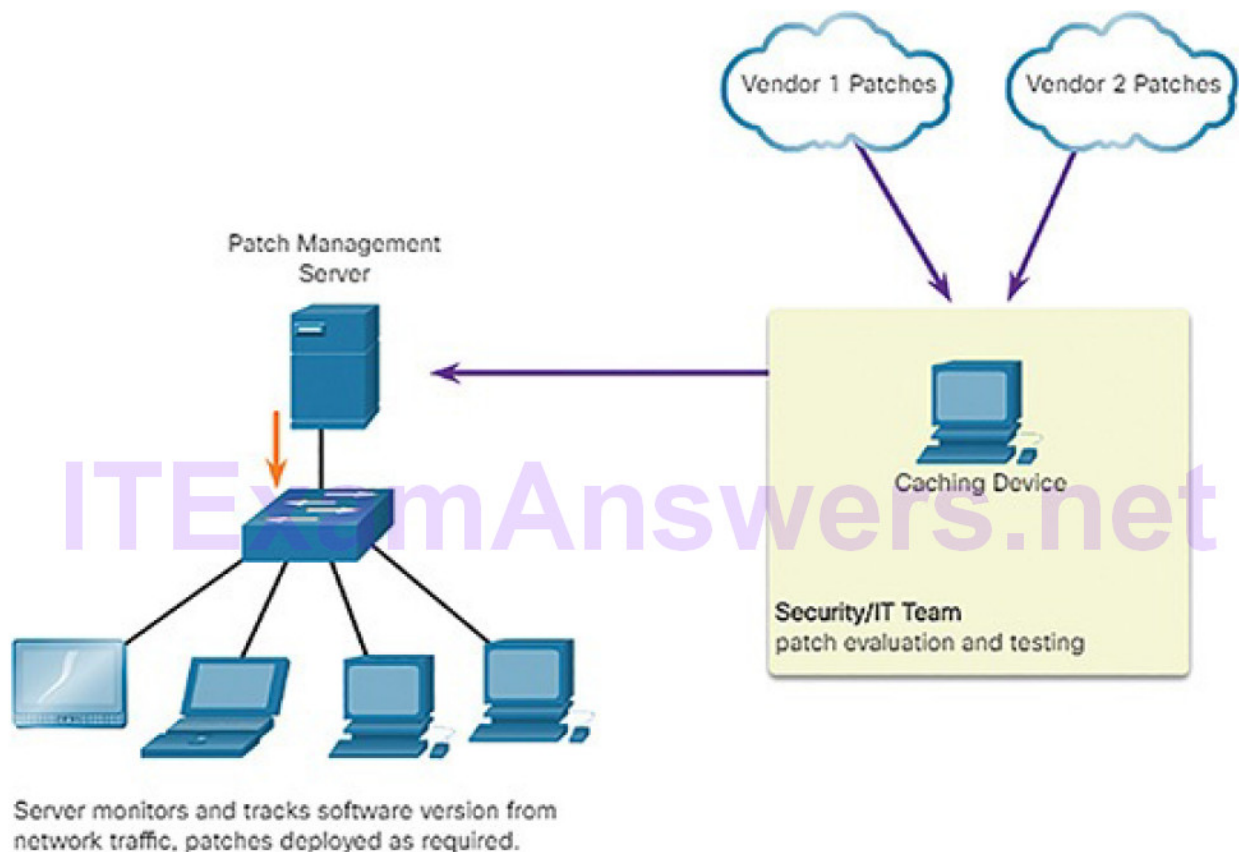


Figure 10-28 Passive Network Monitoring Patch Management

#### Activity 10.2.4.9: Identify Device Management Activities

Refer to the online course to complete this Activity.

### Information Security Management Systems (10.2.5)

In this topic, you will learn how information security management systems are used to protect assets.

#### Security Management Systems (10.2.5.1)

An Information Security Management System (ISMS) consists of a management framework through which an organization identifies, analyzes, and addresses information security risks. ISMSs are not based in servers or security devices. Instead, an ISMS consists of a set of practices that are systematically applied by an organization to ensure continuous improvement in information security. ISMSs provide conceptual models that guide organizations in planning, implementing, governing, and evaluating information security programs.

ISMSs are a natural extension of the use of popular business models, such as Total Quality Management (TQM) and Control Objectives for Information and Related Technologies (COBIT), into the realm of cybersecurity.

An ISMS is a systematic, multilayered approach to cybersecurity. The approach includes people, processes, technologies, and the cultures in which they interact in a process of risk management.

An ISMS often incorporates the “plan-do-check-act” framework, known as the Deming cycle, from TQM. It is seen as an elaboration on the process component of the People-Process-Technology-Culture model of organizational capability, as shown in Figure 10-29.

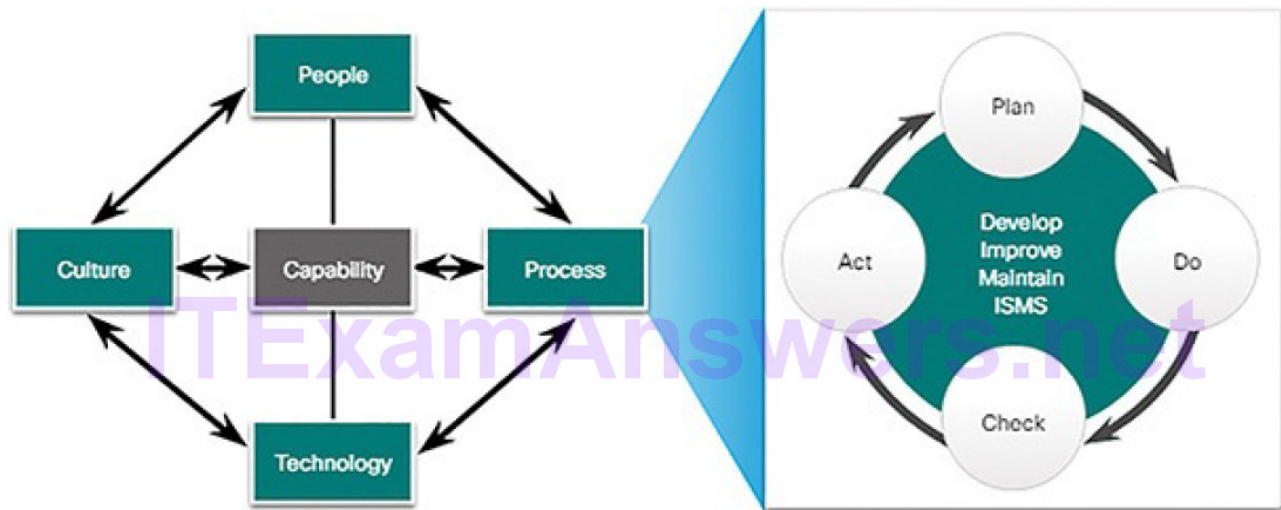


Figure 10-29 A General Model for Organizational Capability

### ISO-27001 (10.2.5.2)

ISO is the International Organization for Standardization. ISO’s voluntary standards are internationally accepted and facilitate business conducted between nations.

ISO partnered with the International Electrotechnical Commission (IEC) to develop the ISO/IEC 27000 family of specifications for ISMSs, as shown in Table 10-2.

Table 10-2 ISO/IEC 27000 Family of Standards

Standard Title and Description	
ISO/IEC 27000	Information security management systems – Overview and vocabulary. Introduction to the standards family, overview of ISMS, essential vocabulary.
ISO/IEC 27001	Information security management systems – Requirements. Provides an overview of ISMS and the essentials of ISMS processes and procedures.
ISO/IEC 27003	Information security management systems – Guidance. Critical factors necessary for successful design and implementation of ISMS. All specification up to the production of implementation plans.

---

ISO/IEC 27004	Information security management – Monitoring, measurement, analysis and evaluation. Discussion of metrics and measurement procedures to assess effectiveness of ISMS implementation.
---------------	--

---

ISO/IEC 27005	Information security risk management. Supports the implementation of ISMS based on a risk-centered management approach.
---------------	---

---

The ISO 27001 Certification is a global, industry-wide specification for an ISMS. Figure 10-30 illustrates the relationship of actions stipulated by the standard with the plan-do-check-act cycle.

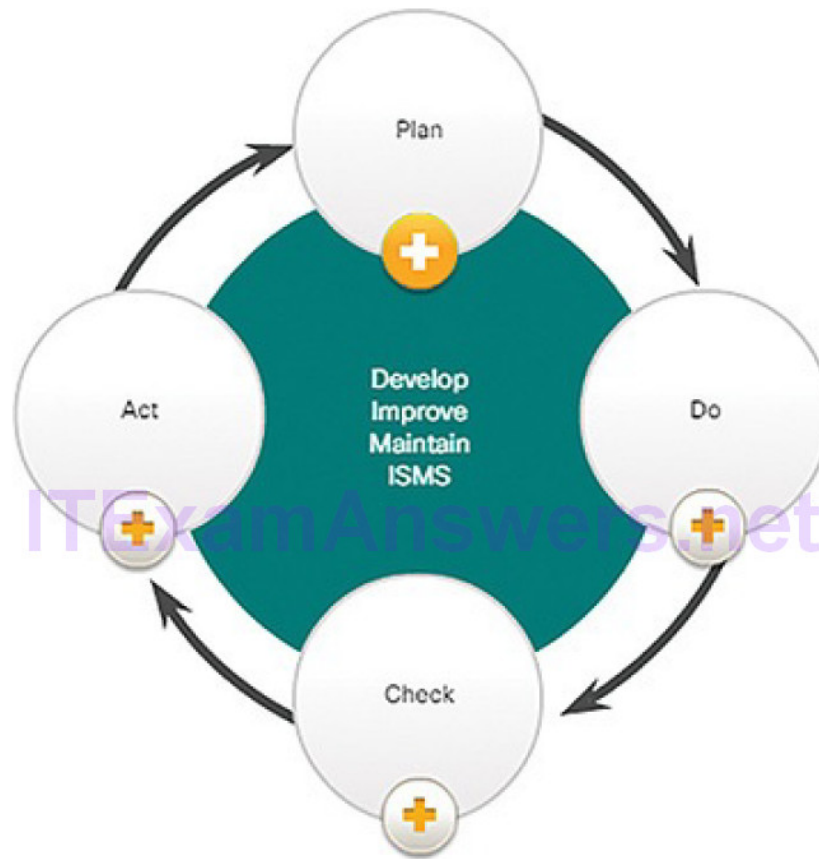


Figure 10-30 ISO 27001 ISMS Plan–Do–Check–Act Cycle

The details of each action are as follows:

### Plan

- Understand relevant business objectives
- Define scope of activities
- Access 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

Certification means an organization's security policies and procedures have been independently verified to provide a systematic and proactive approach for effectively managing security risks to confidential customer information.

### NIST Cybersecurity Framework (10.2.5.3)

---

NIST is very effective in the area of cybersecurity, as we have seen in this chapter. More NIST standards will be discussed later in the course.

NIST has developed the Cybersecurity Framework, which, like ISO/IEC 27000, is a set of standards designed to integrate existing standards, guidelines, and practices to help better manage and reduce cybersecurity risk. The Framework was first issued in February 2014 and continues to undergo development.

The Framework consists of a set of activities suggested to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The core functions, defined in Table 10-3, are split into major categories and subcategories.

Table 10-3 NIST Cybersecurity Framework Core and Functions

Core Function	Description
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.

Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The major categories provide an understanding of the types of activities related to each function, as shown in Table 10-4.

Table 10-4 NIST Cybersecurity Framework Core and Activities

Core Function	Activity
<b>Identify</b>	Asset Management
	Business Environment
	Risk Assessment
	Risk Management Strategy
<b>Protect</b>	Access Control
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
<b>Detect</b>	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
<b>Respond</b>	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements



<b>Recover</b>	Recovery Planning
	Improvements
	Communications

Organizations of many types are using the Framework in a number of ways. Many have found it helpful in raising awareness and communicating with stakeholders within their organization, including executive leadership. The Framework is also improving communications across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. By mapping the Framework to current cybersecurity management approaches, organizations are learning and showing how they match up with the Framework's standards, guidelines, and best practices. Some parties are using the Framework to reconcile internal policy with legislation, regulation, and industry best practice. The Framework also is being used as a strategic planning tool to assess risks and current practices.

#### **Activity 10.2.5.4: Identify the ISO 27001 Activity Cycle**

Refer to the online course to complete this Activity.

#### **Activity 10.2.5.5: Identify the Stages in the NIST Cybersecurity Framework**

Refer to the online course to complete this Activity.

### **Summary (10.3)**

In this chapter, you learned how to investigate endpoint vulnerabilities and attacks. Antimalware for network devices and hosts provides a method for mitigating the impact of attacks. Host-based personal firewalls are stand-alone software programs that control traffic entering or leaving a computer. A host-based intrusion detection system (HIDS) is designed to protect hosts against known and unknown malware. A HIDS is a comprehensive security application that combines the functionalities of antimalware applications with firewall functionality. Host-based security solutions are essential to protecting the expanding attack surfaces.

Cybersecurity analysts and security experts use a variety of tools to perform endpoint vulnerability assessments. Network and device profiling provide a baseline that serves as a reference point for identifying deviations from normal operations. Similarly, server profiling is used to establish the accepted operating state of servers. Network security can be evaluated using a variety of tools and services, including:

- Risk analysis to evaluate the risk posed by vulnerabilities to a specific organization
- Vulnerability assessment, which uses software to scan Internet-facing servers and internal networks for various types of vulnerabilities

- Penetration testing, which uses authorized simulated attacks to test the strength of network security

The 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. The benefits of CVSS include:

- Standardized vulnerability scores that should be meaningful across organizations
- Open framework with the meaning of each metric openly available to all users
- Prioritization of risk in a way that is meaningful to individual organizations

A number of security compliance regulations have emerged, including:

**Federal Information Security Management Act of 2002 (FISMA):** This provides security standards for U.S. government systems and contractors to the U.S. government.

**Sarbanes-Oxley Act of 2002 (SOX):** This provides the requirements for the way in which U.S. corporations control and disclose financial information.

**Gramm-Leach-Bliley Act (GLBA):** This states that financial institutions must secure customer information, protect against threats to customer information, and protect against unauthorized access to customer information.

**Health Insurance Portability and Accountability Act (HIPAA):** This requires that all patient personally identifiable healthcare information be stored, maintained, and transmitted in ways that ensure patient privacy and confidentiality.

**Payment Card Industry Data Security Standard (PCI DSS):** This is a proprietary, non-governmental standard for the secure handling of customer credit card data.

Risk management involves the selection and specification of security controls for an organization. There are four potential ways to respond to risks that have been identified, based on their weightings or scores:

- Risk avoidance, if it is determined that the activity should be discontinued
- Risk reduction, by implementing management approaches to reduce vulnerability
- Risk sharing, to shift risk by outsourcing some aspects of security operations to third parties
- Risk retention and acceptance, for risks that have low potential impact and/or relatively high cost of mitigation or reduction

Risk management tools include:

- Vulnerability management
- Asset management

- Mobile device management
- Configuration management
- Enterprise patch management

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.

## Practice

---

There are no Labs or Packet Tracer activities in this chapter.