Cyber Threat Management course

Governance

IT security governance determines who is authorized to make decisions about cybersecurity risks within an organization. It demonstrates accountability and provides oversight to ensure that any risks are adequately mitigated and that security strategies are aligned with the organization's business objectives and are compliant with regulations.

IT security governance should not be confused with IT security management, which defines and implements the controls that an organization needs to have in place to mitigate risks.
Similarly, **data governance** in particular determines who is authorized to make decisions about data within an organization.

There are several key roles in good data governance programs.

- **Data owner:** A person who ensures compliance with policies and procedures, assigns the proper classification to information assets, and determines the criteria for accessing information assets.
- **Data controller:** A person who determines the purposes for which, and the way in which, personal data is processed.
- **Data processor:** A person or organization who processes personal data on behalf of the data controller.
- **Data custodian:** A person who implements the classification and security controls for the data in accordance with the rules set out by the data owner. In other words, data custodians are responsible for the technical control of the data.
- **Data steward:** A person who ensures that data supports an organization's business needs and meets regulatory requirements.
- **Data protection officer:** A person who oversees an organization's data protection strategy.

Cybersecurity Policies

A cybersecurity policy is a high-level document that outlines an organization's vision for cybersecurity, including its goals, needs, scope and responsibilities. Specifically, it:

- Demonstrates an organization's commitment to security.
- Sets the standards of behavior and security requirements for carrying out activities, processes and operations, and protecting technology and information assets within an organization.

- Ensures that the acquisition, use and maintenance of system operations, software and hardware is consistent across the organization.
- Defines the legal consequences of policy violations.
- Gives the security team the support they need from senior management.

There are various types of cybersecurity policies. Let’s find out more about some of the most common ones.

- Master Cybersecurity policy: The blueprint for an organization’s cybersecurity program, this policy serves as the strategic plan for implementing cybersecurity controls.
- System-specific policy: This type of policy is developed for specific devices or computer systems and aims to establish standardization for approved applications, software, operating system configurations, hardware and hardening countermeasures within an organization.
- Issue-specific policy: This type of policy is developed for certain operational issues, circumstances or conditions that may require more detailed requirements and directions.

Types of Security Policies

An organization needs to establish clear and detailed security policies that all employees are aware of. It is critical that these policies also have the support of the senior management team.

Let’s find out more about some of the security-related policies that an organization may have in place.

- **Identification and authentication policy: Specifies** who should be permitted access to network resources and what verification procedures are in place to facilitate this.
- **Password policy:** Defines minimum password requirements, such as the number and type of characters used and how often they need to be changed.
- **Acceptable use policy:** Highlights a set of rules that determine access to and use of network resources. It may also define the consequences of policy violations.
- **Remote access policy:** Sets out how to remotely connect to an organization’s internal network and explains what information is remotely accessible.
- **Network maintenance policy:** Outlines procedures for updating an organization’s specified operating systems and end-user applications.
- **Incident handling policy:** Provides guidance on how to report and respond to security-related incidents within an organization.
- **Data policy:** Sets out measurable rules for processing data within an organization, such as specifying where data is stored, how data is classified (high, medium, low, confidential, public or private), and how data is handled and disposed of.
- **Credential policy:** Enforces the rules for composing credentials, such as the minimum and maximum length of a password.

- **Organizational policy:** Provides guidance for how work should be carried out in an organization. Examples might include change management, change control or asset management policies.

The Ethics of Cybersecurity

Ethics of a Cybersecurity Specialist

Ethics is the little voice in your head that tells you what is right and what is wrong, guiding you to make the right decisions. As a cybersecurity specialist, you need to understand both the law and an organization's interests in order to be able to make such decisions.

Ethics can be viewed from many different perspectives.

- During the nineteenth century, philosophers Jeremy Bentham and John Stuart Mill articulated the theory of **utilitarian ethics**. This is based on the guiding principle that the consequence of an action is the most important factor in determining if the action is moral or not. For example, an action that maximizes the greatest good for the greatest amount of people is an ethical choice.
- The **rights approach** is guided by the principle which states that an individual has the right to make their own choices, which cannot be violated by another person's decision. This decision must respect and consider the fundamental rights of the individual. These fundamental rights include the right to truth, privacy, safety and for society to apply laws fairly to all members of society.
- The **common good approach** proposes that ethical actions are those that benefit the entire community. It challenges individuals to recognize and pursue the values and goals shared with other members of a community.

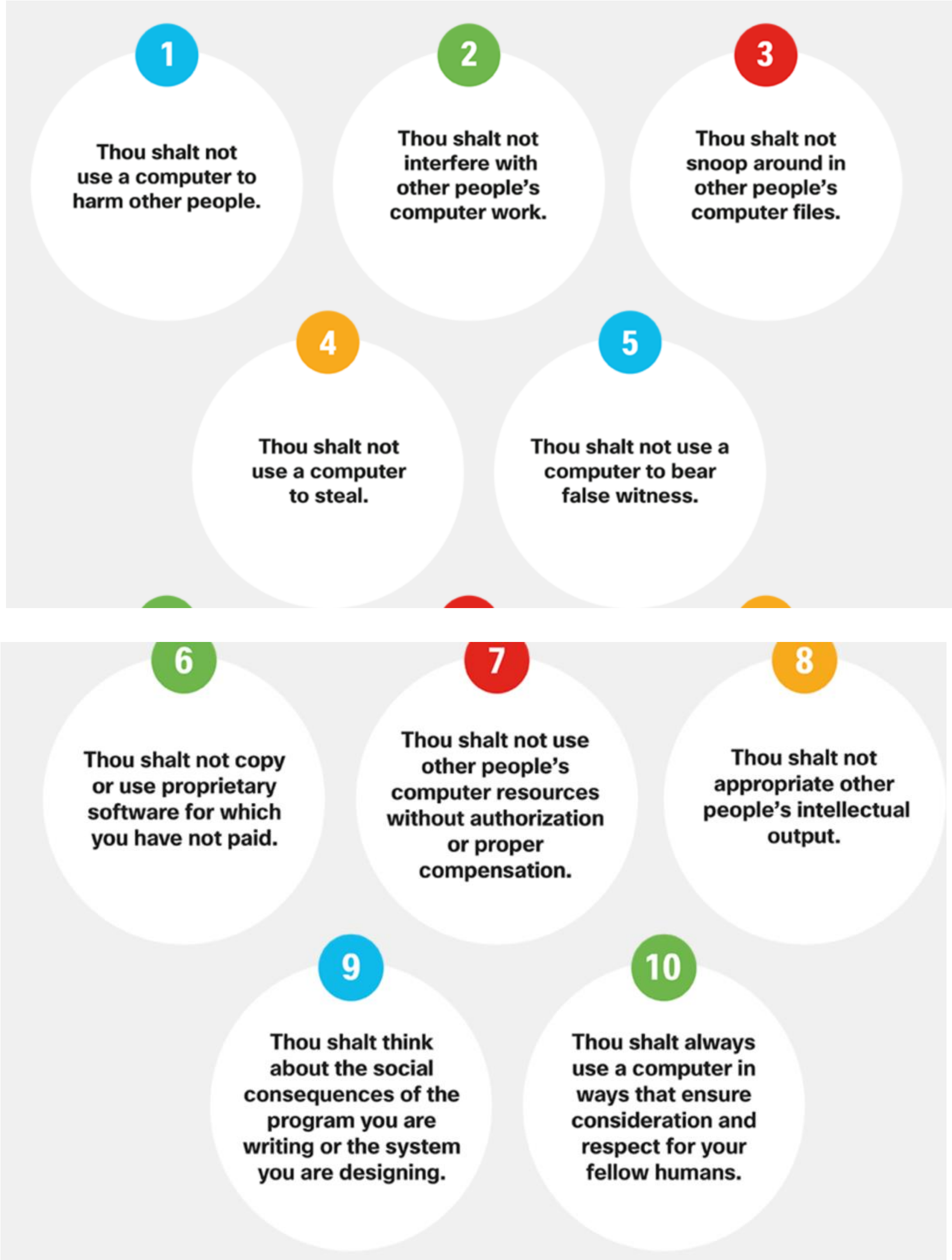
"As a cybersecurity specialist, there will often be no obvious answer to the ethical issues you come across. The right course of action will depend on the situation and the ethical perspective you use to guide your decision."

The Ten Commandments of Computer Ethics

Based in Washington, DC, the Computer Ethics Institute is a resource for identifying, assessing and responding to ethical issues throughout the information technology industry.

It was one of the first organizations to recognize the ethical and public policy issues arising from the rapid growth of the information technology field.

They created the **ten commandments of computer ethics** presented here.


1
Thou shalt not use a computer to harm other people.
2
Thou shalt not interfere with other people's computer work.
3
Thou shalt not snoop around in other people's computer files.
4
Thou shalt not use a computer to steal.
5
Thou shalt not use a computer to bear false witness.
6
Thou shalt not copy or use proprietary software for which you have not paid.
7
Thou shalt not use other people's computer resources without authorization or proper compensation.
8
Thou shalt not appropriate other people's intellectual output.
9
Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10
Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Cybercrime

Cybercrime falls into three categories:

1. **Computer-targeted crime** is where a computer is the target of criminal activity. Examples include malware attacks, hacking or denial of service attacks.
2. **Computer-assisted crime** occurs when a computer is used to commit a crime, such as theft or fraud.
3. **Computer-incidental crime** is where a computer provides information that is incidental to an actual crime. For example, a computer is used to store illegally downloaded videos, not the actual tool used to commit the crime.

There are lots of tools connected to the internet — many of which do not require a great deal of expertise to use — that are contributing to the exponential growth of cybercrime. In fact, cybercrime is growing much faster than the ability of the legal system to create the laws and regulations that prohibit it.

There are several agencies working to combat cybercrime, including the Federal Bureau of Investigation Internet Crime Complaint Center (IC3), InfraGard, and Software and Information Industry Association (SIIA) in the U.S.

The Twelve Domains of Cybersecurity

ISO/IEC 27000 is a series of information security standards or best practices to help organizations improve their information security. Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (ICO), the ISO 27000 standards set out comprehensive information security management system (ISMS) requirements. An ISMS consists of all of the administrative, technical and operational controls that address information security within an organization.

The ISO 27000 standard is represented by twelve independent domains. These twelve domains provide the basis for developing security standards and effective security management practices within organizations, as well as helping to facilitate communication between organizations.

1. **Risk assessment:** This is the first step in the risk management process, which determines the quantitative and qualitative value of risk related to a specific situation or threat.
2. **Security policy:** This document addresses the constraints and behaviors of individuals within an organization and often specifies how data can be accessed, and what data is accessible by whom.
3. **Organization of information security:** This is the governance model set out by an organization for information security.
4. **Asset management:** This is an inventory of and classification scheme for information assets within an organization.
5. **Human resources security:** This refers to the security procedures in place that relate to employees joining, moving within and leaving an organization.
6. **Physical and environmental security:** This refers to the physical protection of an organization’s facilities and information.
7. **Communications and operations management:** This refers to the management of technical security controls of an organization’s systems and networks.
8. **Information systems acquisition, development and maintenance**: This refers to security as an integral part of an organization’s information systems.
9. **Access control:** This describes how an organization restricts access rights to networks, systems, applications functions and data in order to prevent unauthorized user access.

10. **Information security incident management:** This describes an organization’s approach to the anticipation of and response to information security breaches.
11. **Business continuity management:** This describes the ability of an organization to protect, maintain and recover business-critical activities following a disruption to information systems.
12. **Compliance:** This describes the process of ensuring conformance with information security policies, standards and regulations.

The structure of this ISO cybersecurity model differs from the Open System Interconnection (OSI) model in that it is a peer model that uses domains rather than layers to describe the security categories. Each domain has a direct relationship with the other domains. It is important for cybersecurity specialists to be aware of and understand both of these models.

Control Objectives and Controls

These twelve domains are made up of **control objectives** (ISO 27001) and **controls** (ISO 27002). Let’s find out the difference.

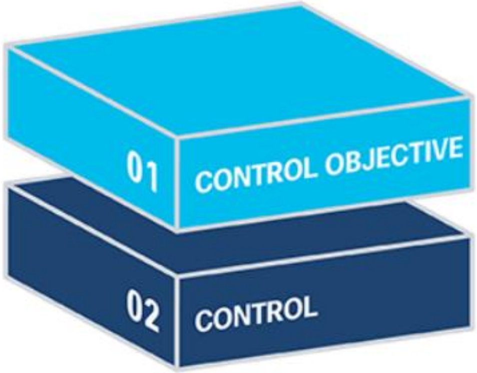
Control Objectives

Control objectives define the high level requirements for implementing a comprehensive information security management system within an organization, and usually provide a checklist to use during an ISMS audit.

Passing this audit indicates that an organization is ISO 27001 compliant and provides partners with confidence in the security of the organization’s data and operations.

Controls

Controls set out how to accomplish an organization’s control objectives. They establish guidelines for implementing, maintaining and improving the management of information security in an organization.

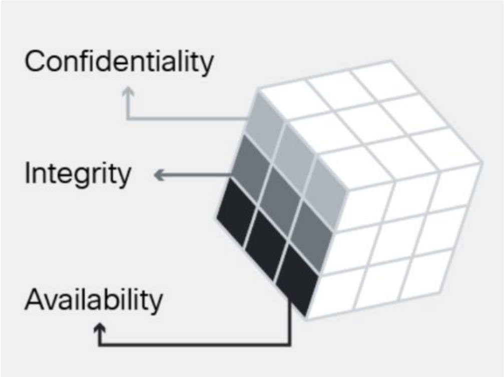


For example:

An organization's **control objective** is to control access to networks by using the appropriate authentication mechanisms for users and equipment.

A relevant **control**, therefore, is to use strong passwords consisting of at least eight characters and a combination of upper and lowercase letters, numbers and symbols.

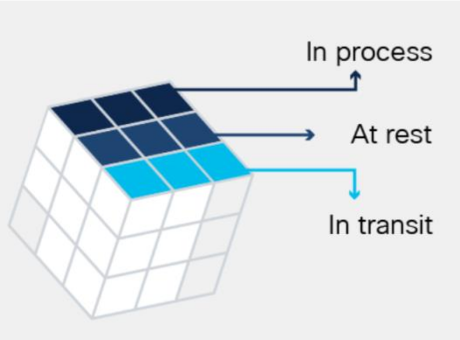
ISO 27000 and the CIA Triad



ISO 27000 is a universal framework that is applicable to every type of organization. In order to use it effectively, an organization must identify which domains, control objectives and controls apply to its environment and operations. Most organizations do this by producing a statement of applicability (SOA) which allows it to tailor the available control objectives and controls to best meet its priorities around confidentiality, integrity and availability.

*"Different organizations will prioritize confidentiality, integrity and availability differently. For example, data **Confidentiality** and **Availability** are the highest priorities at **Google**, while Integrity is a lower priority (Google does not verify user data). **Amazon** places higher emphasis on **Availability**, for if the website is not available, there are no sales. Amazon may therefore direct more resources into ensuring that there are enough servers available to handle customer purchases. "*

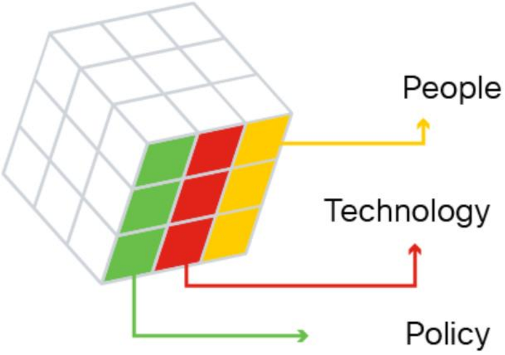
ISO 27000 and the States of Data



The ISO controls specifically address security objectives for data in each of the three states: in process, at rest (in storage) and in transit.

The responsibility for identifying and implementing the relevant controls may lie with different groups across an organization. For example, a network security team may be responsible for controls that ensure the confidentiality, integrity and availability of all data being transmitted (data in transit), programmers and data entry analysts for data being processed (in process) and hardware support specialists for stored data (at rest/in storage).

ISO 27000 and Safeguards



The ISO controls also provide technical direction for control objectives that relate to the cybersecurity policies, procedures and guidelines set out by senior management within an organization.

For example, let’s imagine that a senior management team establishes a policy to protect all data coming into or going out of an organization. The responsibility for implementing and configuring the networks, systems and equipment to be able to fulfill the policy directives will fall to the appropriate IT professionals within the organization, not the senior management team.

The National Cybersecurity Workforce Framework

The National Institute of Standards and Technologies (NIST) created the National Cybersecurity Workforce Framework to support organizations seeking cybersecurity professionals. The framework organizes cybersecurity work into seven categories, outlining the main job roles, responsibilities and skills needed for each one.

Summary of the main cybersecurity functions in each category.

- **Operate and maintain:** Provides the support, administration and maintenance required to ensure effective and efficient IT system performance and security.
- **Protect and defend:** Identifies, analyzes and mitigates threats to internal systems and networks.
- **Investigate:** Investigates cybersecurity events and/or cyber attacks involving IT resources.
- **Collect and operate:** Provides specialized denial and deception operations and collection of cybersecurity information.
- **Analyze:** Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
- **Oversee and govern:** Provides leadership, management, direction or development and advocacy so an organization may effectively conduct cybersecurity work.
- **Securely provision:** Conceptualizes designs, procures or builds secure IT systems.

The CIS Critical Security Controls

The Center for Internet Security (CIS) developed a set of critical security controls to help organizations with different levels of resources and expertise at their disposal to improve their cyber defenses.

- **Basic controls:** Organizations with limited resources and cybersecurity expertise available should implement:

  - Inventory and control of hardware assets
  - Inventory and control of software assets
  - Continuous vulnerability management
  - Controlled use of administrative privileges
  - Secure configurations for hardware and software
  - Maintenance, monitoring and analysis of audit logs

- **Foundational controls:** Organizations with moderate resources and cybersecurity expertise available should implement the basic controls as well as:
    - Email and web browser protections
    - Malware defense
    - Limitation and control of network ports, protocols and services
    - Data recovery capabilities
    - Secure configurations for network devices
    - Boundary defense
    - Data protections
    - Controlled access based on the ‘need to know’ principle
    - Wireless access control
    - Account monitoring and control
- **Organizational controls:** Organizations with significant resources and cybersecurity expertise available should implement the basic and foundational controls, as well as:
    - A security awareness and training program
    - Application software security
    - Incident response and management
    - Penetration tests and red team exercises (simulated attack exercises to gauge an organization’s security capabilities)

“CIS has also developed https://www.cisecurity.org/cis-benchmarks . With over 100 configuration guides and checklists for various platforms, this resource can help any organization securely configure a system, as well as mitigate any security vulnerabilities.

The Cloud Controls Matrix

The Cloud Security Alliance (CSA) provides security guidance to any organization that uses cloud computing or wants to assess the overall security risk of a cloud provider.

Their Cloud Controls Matrix (CCM) is a cybersecurity control framework that maps cloud-specific security controls to leading standards, best practices and regulations. It is composed of 197 control objectives that are structured in 17 domains covering all aspects of cloud technology, including governance and risk management, human resources and mobile security.

The CCM is considered a de-facto standard for cloud security assurance and compliance.

Network security testing

Vulnerability Scanners

A vulnerability scanner assesses computers, computer systems, networks or applications for weaknesses. Vulnerability scanners can help to automate security auditing by scanning the network for security risks and producing a prioritized list to address vulnerabilities.

- A vulnerability scanner looks for the following types of vulnerabilities:
  - Use of default passwords or common passwords
  - Missing patches
  - Open ports
  - Misconfigurations in operating systems and software
  - Active IP addresses, including any unexpected devices connected
- Vulnerability scanning is key to identifying vulnerabilities, Misconfigurations and a lack of security controls for organizations with networks that include segments, routers, firewalls, servers and other devices.
- Commonly used vulnerability scanners on the market include Nessus, Retina, Core Impact and GFI LanGuard. Their functions include:
  - Performing compliance auditing
  - Providing patches and update
  - Identifying misconfiguration
  - Supporting mobile and wireless devices
  - Tracking malware
  - Identifying sensitive data

Types of Scans

When evaluating a vulnerability scanner, look at how it is rated for accuracy, reliability, and scalability and reporting. You can choose a software-based or cloud-based vulnerability scanner.

- **Categories**: Vulnerability scanners fall into one of several categories:
  - Network scanners probe hosts for open ports, enumerate information about users and groups and look for known vulnerabilities on the network.
  - Application scanners access application source code to test an application from the inside (they do not run the application).
  - Web application scanners identify vulnerabilities in web applications.
- **Intrusive and Credentialed Scans:** Intrusive scans try to exploit vulnerabilities and may even crash the target, while a non-intrusive scan will try not to cause harm to the target. In a credentialed scan, usernames and passwords provide authorized access to a system, allowing the scanner to harvest more information. Non-credentialed scans are less invasive and give an outsider's point of view. However, all types of scanner can

mistakenly identify a vulnerability where none exists. This is known as a false positive, while not identifying an existing vulnerability is a false negative. Credentialed scans return fewer false positives and fewer false negatives. You need to review all logs and configurations to take care of any vulnerabilities that require attention.

Security Automation

SIEM

Security Information and Event Management (SIEM) systems use log collectors to aggregate log data from sources such as security devices, network devices, servers and applications. Logs can generate many events in a day, so SIEM systems help to reduce event volume by combining similar events to reduce the event data load. SIEM identifies deviations from the norm and then takes the appropriate action.

The goals of a SIEM system for security monitoring are:

- Identify internal and external threats
- Monitor activity and resource usage
- Conduct compliance reporting for audits
- Support incident response

When the SIEM system detects a potential issue, it might log additional information, generate an alert and instruct other security controls to stop an activity's progress. Advanced SIEM systems include user and entity behavior analytics that look for patterns that rely on human sentiment to recognize a threat before it becomes a threat.

The amount of data logged from critical systems is an important consideration when implementing a SIEM system since you need to review the reports generated. SIEM systems are costly to purchase and maintain and are only cost-effective if the organization has millions of events generated in a day.

SOAR

Orchestration Automation and Response (SOAR) tools allow an organization to collect data about security threats from various sources, and respond to low-level events without human intervention. SOAR has three important capabilities:

- Threat and vulnerability management
- Security incident response
- Security operations automation

An organization can integrate SOAR in to its SIEM solution.

Network Security Testing Techniques

Operations Security

Operations security is concerned with the day-to-day practices necessary to first deploy and later maintain a secure system. All networks are vulnerable to attack if the planning, implementation, operations, and maintenance of the network do not adhere to operational security practices.

Operations security starts with the planning and implementation process of a network. During these phases, the operations team analyzes designs, identifies risks and vulnerabilities, and makes the necessary adaptations. The actual operational tasks begin after the network is set up and include the continual maintenance of the environment. These activities enable the environment, systems, and applications to continue to run correctly and securely.

Some security testing techniques are predominantly manual, and others are highly automated. Regardless of the type of testing, the staff that sets up and conducts the security testing should have significant security and networking knowledge in these areas:

- Operating systems
- Basic programming
- Networking protocols, such as TCP/IP
- Network vulnerabilities and risk mitigation
- Device hardening
- Firewalls
- IPSs

Types of Network Tests

Threat actors use reconnaissance techniques to learn about networks as they search for vulnerabilities. Similarly, network testers use reconnaissance to find out what hackers can learn. Active reconnaissance means directly interacting with network systems to gather information using many of the tools that are used in penetration testing and vulnerability assessment. Passive reconnaissance means indirectly learning about the network and network users through searches from information sources that range from Facebook to leaked password details on the dark web. It frequently involves the use of open-source intelligence (OSINT) information resources. Network security testing requires cybersecurity personnel to think like threat actors and discover vulnerabilities before they can be exploited by the real threat actors.

After a network is operational, you must access its security status. Many security tests can be conducted to assess the operational status of the network:

- **Penetration testing -** Network penetration tests, or pen testing, simulate attacks from malicious sources. The goal is to determine the feasibility of an attack and possible consequences if one were to occur. Some pen testing may involve accessing a client's premises and using social engineering skills to test their overall security posture.
- **Network scanning -** Includes software that can ping computers, scan for listening TCP ports, and display which types of resources are available on the network. Some scanning software can also detect usernames, groups, and shared resources. Network administrators can use this information to strengthen their networks.
- **Vulnerability scanning -** This includes software that can detect potential weaknesses in the tested systems. These weaknesses can include misconfiguration, blank or default passwords, or potential targets for DoS attacks. Some software allows administrators to attempt to crash the system through the identified vulnerability.
- **Password cracking -** This includes software that is used to test and detect weak passwords that should be changed. Password policies must include guidelines to prevent weak passwords.
- **Log review -** System administrators should review security logs to identify potential security threats. Filtering software to scan lengthy log files should be used to help discover abnormal activity to investigate.
- **Integrity checkers -** An integrity checking system detects and reports on changes in the system. Most of the monitoring is focused on the file system. However, some checking systems can report on login and logout activities.
- **Virus detection -** Virus or antimalware detection software should be used to identify and remove computer viruses and other malware.

Note: Other tests, including Wardialing and Wardriving, are considered to be legacy, but should still be accounted for in network testing.

Network Security Testing Tools

There are many tools available to test the security of systems and networks. Some of these tools are open source while others are commercial tools that require licensing.

Software tools that can be used to perform network testing include:

- **Nmap/Zenmap -** This is used to discover computers and their services on a network, therefore creating a map of the network.
- **SuperScan -** This port scanning software is designed to detect open TCP and UDP ports, determine what services are running on those ports, and to run queries, such as whois, ping, traceroute, and hostname lookups.
- **SIEM (Security Information Event Management) -** This is a technology used in enterprise organizations to provide real time reporting and long-term analysis of security events.

- **GFI LANguard -** This is a network and security scanner which detects vulnerabilities.
- **Tripwire -** This tool assesses and validates IT configurations against internal policies, compliance standards, and security best practices.
- **Nessus -** This is a vulnerability scanning software, focusing on remote access, misconfigurations, and DoS against the TCP/IP stack.
- **L0phtCrack -** This is a password auditing and recovery application.
- **Metasploit -** This tool provides information about vulnerabilities and aids in penetration testing and IDS signature development.

Note: Network testing tools evolve at a rapid pace. The preceding list includes legacy tools, and its intent is to provide an awareness of the different types of tools available.

Nmap and Zenmap

Nmap is a commonly used, low-level scanner that is available to the public. It has an array of excellent features which can be used for network mapping and reconnaissance.

The basic functionality of Nmap allows the user to accomplish several tasks, as follows:

- **Classic TCP and UDP port scanning -** This searches for different services on one host.
- **Classic TCP and UDP port sweeping -** This searches for the same service on multiple hosts.
- **Stealth TCP and UDP port scans and sweeps -** This is similar to classic scans and sweeps, but harder to detect by the target host or IPS.
- **Remote operating system identification -** This is also known as OS fingerprinting.

Advanced features of Nmap include protocol scanning, known as Layer 3 port scanning. This feature identifies Layer 3 protocol support on a host. Examples of protocols that can be identified include GRE and OSPF.

While Nmap can be used for security testing, it can also be used for malicious purposes. Nmap has an additional feature that allows it to use decoy hosts on the same LAN as the target host, to mask the source of the scan.

Nmap has no application layer features and runs on UNIX, Linux, Windows, and OS X. Both console and graphical versions are available. The Nmap program and Zenmap GUI can be downloaded from the internet.

SuperScan

SuperScan is a Microsoft Windows port scanning tool. It runs on most versions of Windows and requires administrator privileges.

SuperScan version 4 has a number of useful features:

- Adjustable scanning speed
- Support for unlimited IP ranges
- Improved host detection using multiple ICMP methods
- TCP SYN scanning
- UDP scanning (two methods)
- Simple HTML report generation
- Source port scanning
- Fast hostname resolution
- Extensive banner grabbing capabilities
- Massive built-in port list description database
- IP and port scan order randomization
- A selection of useful tools, such as ping, traceroute, and whois
- Extensive Windows host enumeration capability

Tools, such as Nmap and SuperScan, can provide effective penetration testing on a network and determine network vulnerabilities while helping to anticipate possible attack mechanisms. However, network testing cannot prepare a network administrator for every security problem.

SIEM

Security Information Event Management (SIEM) is a technology used in enterprise organizations to provide real time reporting and long-term analysis of security events. SIEM evolved from two previously separate products: Security Information Management (SIM) and Security Event Management (SEM). SIEM can be implemented as software, integrated with Cisco Identity Services Engine (ISE) or as a managed service.

SIEM combines the essential functions of SIM and SEM to provide:

- **Correlation -** Examines logs and events from disparate systems or applications, speeding detection of and reaction to security threats.
- **Aggregation -** Aggregation reduces the volume of event data by consolidating duplicate event records.
- **Forensic analysis -** The ability to search logs and event records from sources throughout the organization provides more complete information for forensic analysis.
- **Retention -** Reporting presents the correlated and aggregated event data in real-time monitoring and long-term summaries.

SIEM provides details on the source of suspicious activity, including:

- User information (name, authentication status, location, authorization group, quarantine status)
- Device information (manufacturer, model, OS version, MAC address, network connection method, location)
- Posture information (device compliance with corporate security policy, antivirus version, OS patches, compliance with mobile device management policy)

Using this information, network security engineers can quickly and accurately assess the significance of any security event and answer the critical questions:

- Who is associated with this event?
- Is it an important user with access to intellectual property or sensitive information?
- Is the user authorized to access that resource?
- Does the user have access to other sensitive resources?
- What kind of device is being used?
- Does this event represent a potential compliance issue?

Penetration Testing

Penetration testing, or pen testing, is a way of testing the areas of weaknesses in systems by using various malicious techniques. A penetration test simulates methods that an attacker would use to gain unauthorized access to a network and compromise the systems and allows an organization to understand how well it would tolerate a real attack.

It’s important to note that pen testing is not the same as vulnerability testing, which only identifies potential problems. Pen testing involves hacking a website, network or server with an organization’s permission to try to gain access to resources using various methods that real-life black hat hackers would use.

One of the primary reasons why an organization would use pen testing is to find and fix vulnerabilities before the cybercriminals do. Penetration testing is a technique used in ethical hacking.

Different Levels of Penetration Testing

Penetration testing (pen testing) can be conducted at various levels based on the amount of information and access provided to the testers. The main levels include:

1. **Black Box Testing**
   - The tester has no prior knowledge of the target system.
   - Simulates an external attack (e.g., from a hacker with no insider access).
   - Focuses on discovering vulnerabilities from an outsider’s perspective.

2. **White Box Testing (or Clear Box Testing)**
    - The tester has full knowledge of the system, including source code, architecture, and credentials.
    - Simulates an internal attack or a deep security audit.
    - Allows for thorough testing of internal logic, design flaws, and hidden vulnerabilities.
3. **Gray Box Testing**
    - The tester has partial knowledge or limited access (e.g., user-level credentials).
    - Simulates an attack from a user with some level of access (e.g., a disgruntled employee or a contractor).
    - Balances realism with depth by targeting both internal and external weaknesses.

Penetration Phases

There are four phases that make up a penetration test.

Phase 1: Planning: This phase establishes the rules of engagement for conducting the test. It involves defining the scope, goals, timeline, and legal permissions. Both the tester and the organization agree on what systems can be tested, the testing methods, and how potential risks will be managed.

Phase 2: Discovery: Reconnaissance is conducted to gather as much information as possible about the target. This includes:

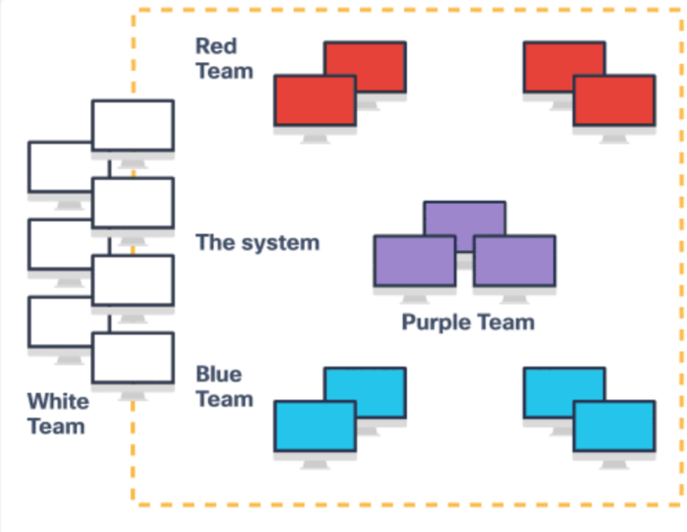
- **Passive techniques**: These involve collecting data without directly interacting with the target system. Known as footprinting, examples include examining DNS records, social media, and public websites.
- **Active reconnaissance**: This involves direct interaction with the system, such as network scanning, to identify open ports, services, and vulnerabilities.

Phase 3: Attack: Using the information gathered, the tester attempts to exploit identified vulnerabilities to gain access. This phase includes:

- Escalating privileges to gain deeper access
- Lateral movement across systems
- Installing tools or creating backdoors (persistence)
- Cleaning up any traces to avoid detection and preserve the integrity of the test

Phase 4: Reporting: the tester compiles and delivers a detailed report to the organization. It includes a summary of the testing process, vulnerabilities discovered, methods used to exploit them, potential impact, and recommended remediation steps to improve security posture.

Exercise Types

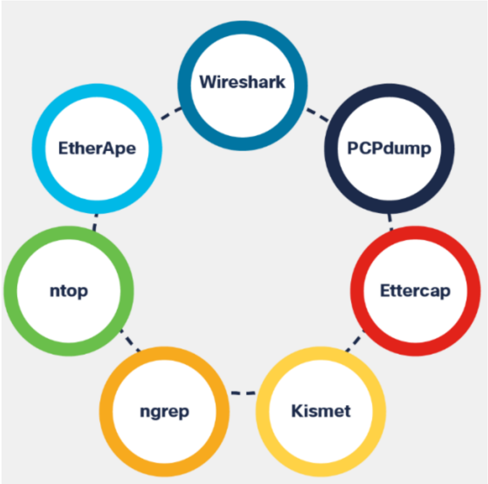


Some organizations create competing teams to conduct penetration exercises that are longer than a penetration test. For instance, in such a scenario, there can be three or four teams:

- **The red team** is the adversary, trying to attack the system while remaining unnoticed.
- **The members of the blue team** are the defenders and they try to thwart the efforts of the red team.
- **The white team** is a neutral team that defines the goals and rules and oversees the exercise. Members of the white team are less technical but possess knowledge about governance and compliance. The white team is the referee of this exercise.
- Sometimes, there is also a **purple team,** where members of the red and blue team work together to identify vulnerabilities and explore ways to improve controls.

"Yet other organizations may conduct a bug bounty program. This is a formalized effort to identify any bugs that might lead to a vulnerability. Bug bounty programs are usually open to the public and involve applications/results delivered online and, possibly, a monetary reward."

Packet Analyzer



Packet analyzers, or packet sniffers, intercept and log network traffic. They perform the below functions — either for legitimate purposes like troubleshooting or illegitimate purposes such as compromising data:

- Network problem analysis.
- Detection of network intrusion attempts.
- Isolation of exploited systems.
- Traffic logging.
- Detection of network misuse.

Protocol Analyzer Output

Sniffing is like eavesdropping on someone.

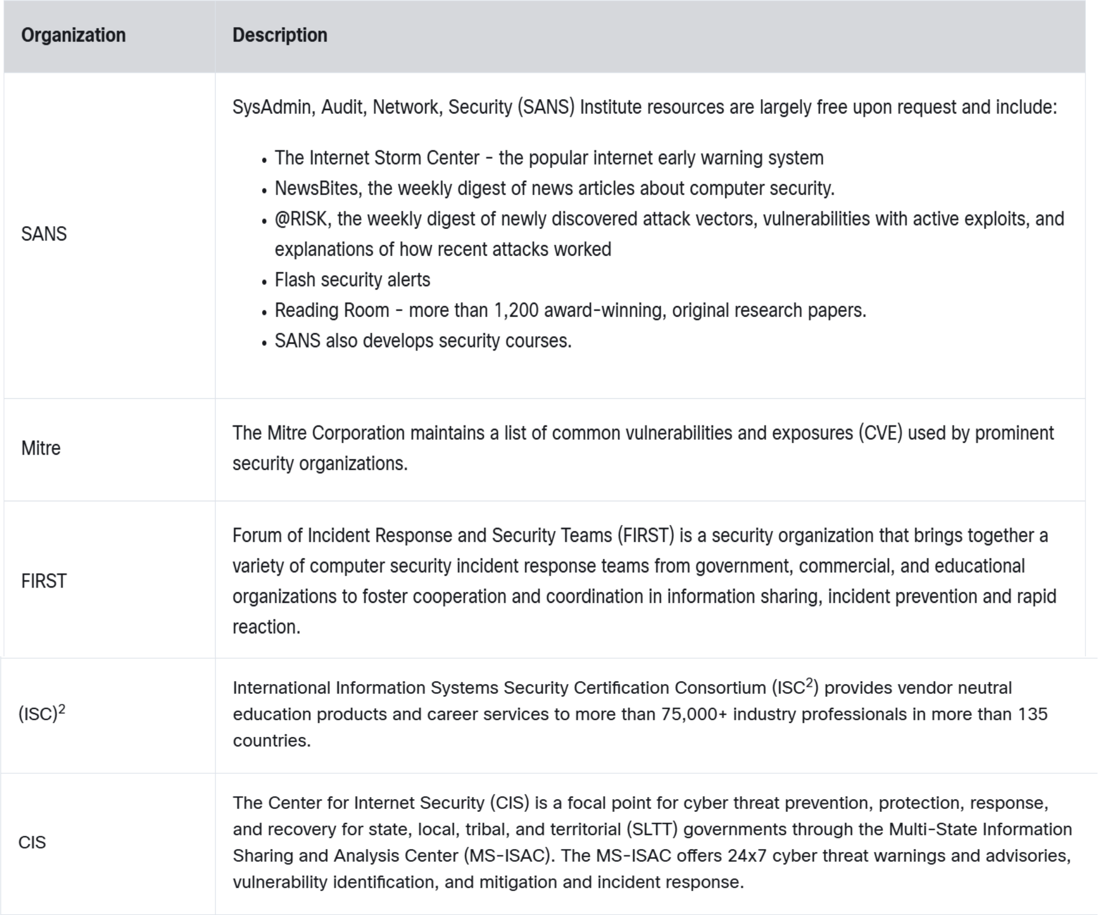
It occurs when someone is examining all network traffic as it passes through their NIC, independent of whether the traffic is addressed to them or not. Criminals accomplish network sniffing using software, hardware, or a combination of the two.

The image shows how sniffing can view all network traffic or target a specific protocol, service or even string of characters such as a login or password. Some network sniffers observe all traffic and modify some or all of the traffic as well.

Note: Physical security is important in preventing the introduction of sniffers to the internal network but sniffing is not only used for malicious purposes. It is also used by network administrators, who can analyze network traffic, identify bandwidth issues and troubleshoot other network issues using sniffers.

Threat intelligence

Network Intelligence Communities



Organization	Description
SANS	SysAdmin, Audit, Network, Security (SANS) Institute resources are largely free upon request and include: • The Internet Storm Center - the popular internet early warning system • NewsBites, the weekly digest of news articles about computer security. • @RISK, the weekly digest of newly discovered attack vectors, vulnerabilities with active exploits, and explanations of how recent attacks worked • Flash security alerts • Reading Room - more than 1,200 award-winning, original research papers. • SANS also develops security courses.
Mitre	The Mitre Corporation maintains a list of common vulnerabilities and exposures (CVE) used by prominent security organizations.
FIRST	Forum of Incident Response and Security Teams (FIRST) is a security organization that brings together a variety of computer security incident response teams from government, commercial, and educational organizations to foster cooperation and coordination in information sharing, incident prevention and rapid reaction.
$(ISC)^2$	International Information Systems Security Certification Consortium (ISC^2) provides vendor neutral education products and career services to more than 75,000+ industry professionals in more than 135 countries.
CIS	The Center for Internet Security (CIS) is a focal point for cyber threat prevention, protection, response, and recovery for state, local, tribal, and territorial (SLTT) governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC). The MS-ISAC offers 24x7 cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

To remain effective, a network security professional must:

- **Keep abreast of the latest threats –** This includes subscribing to real-time feeds regarding threats, routinely perusing security-related websites, following security blogs and podcasts, and more.
- **Continue to upgrade skills –** This includes attending security-related training, workshops, and conferences.

Note: Network security has a very steep learning curve and requires a commitment to continuous professional development.

Cisco Cybersecurity Reports

Resources to help security professionals stay abreast of the latest threats are the Cisco Annual Cybersecurity Report and the Mid-Year Cybersecurity Report. These reports provide an update on the state of security preparedness, expert analysis of top vulnerabilities, factors behind the explosion of attacks using adware, spam, and more.

Cybersecurity analysts should subscribe to and read these reports to learn how threat actors are targeting their networks, and what can be done to mitigate these attacks.

Search the internet to locate and download Cisco Cybersecurity Reports from the Cisco website.

Security Blogs and Podcasts

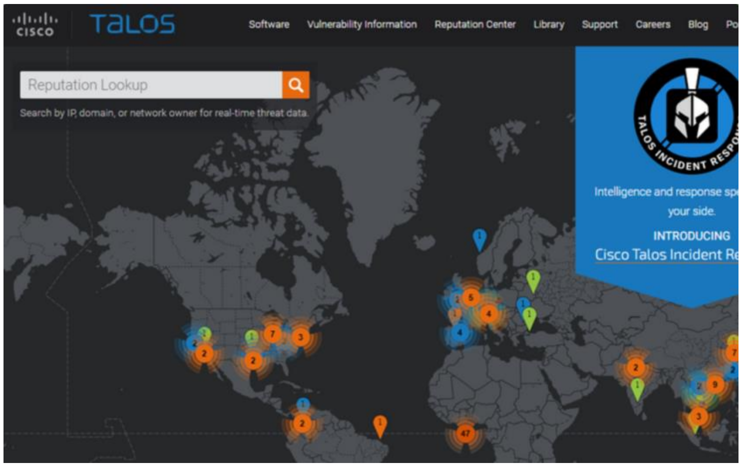
Another method for keeping up-to-date on the latest threats is to read blogs and listen to podcasts. Blogs and podcasts also provide advice, research, and recommended mitigation techniques.

There are several security blogs and podcasts available that a cybersecurity analyst should follow to learn about the latest threats, vulnerabilities, and exploits.

Cisco provides blogs on security-related topics from a number of industry experts and from the Cisco Talos Group. Search for Cisco security blogs to locate them. You can also subscribe to receive notifications of new blogs by email. Cisco Talos also offers a series of over 80 podcasts that can be played from the internet or downloaded to your device of choice.

Cisco Talos

Threat intelligence services allow the exchange of threat information such as vulnerabilities, indicators of compromise (IOC), and mitigation techniques. This information is not only shared with personnel, but also with security systems. As threats emerge, threat intelligence services create and distribute firewall rules and IOCs to the devices that have subscribed to the service.



Search by IP, domain, or network owner for real-time threat data.

Intelligence and response sp your side.

One such service is the Cisco Talos Threat Intelligence Group, shown in the figure. Talos is one of the largest commercial threat intelligence teams in the world, and is comprised of world-class researchers, analysts and engineers. The goal of Talos is to help protect enterprise users, data, and infrastructure from active adversaries. The Talos team collects information about active, existing, and emerging threats. Talos then provides comprehensive protection against these attacks and malware to its subscribers.

Cisco Security products can use Talos threat intelligence in real time to provide fast and effective security solutions. Cisco Talos also provides free software, services, resources, and data. Talos maintains the security incident detection rule sets for the Snort.org, ClamAV, and SpamCop network security tools.

FireEye

FireEye is another security company that offers services to help enterprises secure their networks. FireEye uses a three-pronged approach combining security intelligence, security expertise, and technology.

FireEye offers SIEM and SOAR with the Helix Security Platform, which uses behavioral analysis and advanced threat detection and is supported by the FireEye Mandiant worldwide threat intelligence network. Helix is cloud-hosted security operations platform that combines diverse security tools and threat intelligence into a single platform.

The FireEye Security System blocks attacks across web and email threat vectors, and latent malware that resides on file shares. It can block advanced malware that easily bypasses traditional signature-based defenses and compromises the majority of enterprise networks. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats.

Search for FireEye on the internet and view the security intelligence resources it offers.

Automated Indicator Sharing

The U.S. Department of Homeland Security (DHS) offers a free service called Automated Indicator Sharing (AIS). AIS enables the real-time exchange of cyber threat indicators (e.g., malicious IP addresses, the sender address of a phishing email, etc.) between the U.S. Federal Government and the private sector.

AIS creates an ecosystem where, as soon as a threat is recognized, it is immediately shared with the community to help them protect their networks from that particular threat.

Search the internet for “DHS AIS” service to learn more.

Common Vulnerabilities and Exposures (CVE) Database

The United States government sponsored the MITRE Corporation to create and maintain a catalog of known security threats called Common Vulnerabilities and Exposures (CVE). The CVE serves as a dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities.

The MITRE Corporation defines unique CVE Identifiers for publicly known information-security vulnerabilities to make it easier to share data.

Search the internet for “Mitre Corporation” and view information about CVE

Threat Intelligence Communication Standards

Network organizations and professionals must share information to increase knowledge about threat actors and the assets they want to access. Several intelligence sharing open standards have evolved to enable communication across multiple networking platforms. These standards enable the exchange of cyber threat intelligence (CTI) in an automated, consistent, and machine readable format.

Three common threat intelligence sharing standards include the following:

- **Structured Threat Information Expression (STIX) -** This is a set of specifications for exchanging cyber threat information between organizations. The Cyber Observable Expression (CybOX) standard has been incorporated into STIX.
- **Trusted Automated Exchange of Indicator Information (TAXII) –** This is the specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support STIX.
- **CybOX -** This is a set of standardized schema for specifying, capturing, characterizing, and communicating events and properties of network operations that supports many cybersecurity functions.

These open standards provide the specifications that aid in the automated exchange of cyber threat intelligence information in a standardized format. Search the internet to learn more about STIX, TAXII, and CybOX.

The Malware Information Sharing Platform (MISP) is an open source platform for sharing indicators of compromise for newly discovered threats. MISP is supported by the European Union and is used by over 6,000 organizations globally. MISP enables automated sharing of IOCs between people and machines by using STIX and other export formats.

Threat Intelligence Platforms

As we have seen, there are many sources of threat intelligence information, each of which may have its own data format. Accessing and using multiple threat intelligence sources can be very time-consuming. To help cybersecurity personnel make the best use of threat intelligence, threat intelligence platforms (TIP) have evolved.

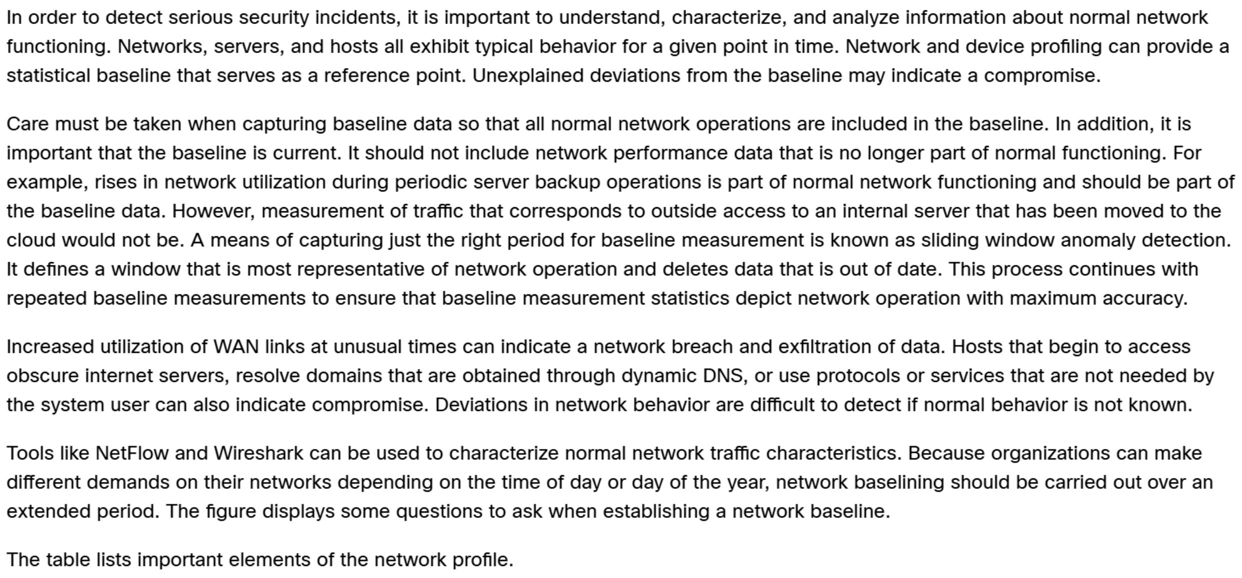
A threat intelligence platform centralizes the collection of threat data from numerous data sources and formats. There are three major types of threat intelligence data. The first is indicators of compromise (IOC). The second is tools, techniques, and procedures (TTP). The third is reputation information about internet destinations or domains. The volume of threat intelligence data can be overwhelming, so the threat intelligence platform is designed to aggregate the data in one place and--most importantly--present the data in a comprehensible and usable format.

Organizations can contribute to threat intelligence by sharing their intrusion data over the internet, typically through automation. Many threat intelligence services use subscriber data to enhance their products and to keep current with the constantly changing immerging threat landscape.

Honeypots are simulated networks or servers that are designed to attract attackers. The attack-related information gathered from honeypots can then be shared with threat intelligence platform subscribers. However, hosting honeypots can itself be a risk. Basing a honeypot in the cloud isolates the honeypot from production networks. This approach is an attractive alternative for gathering threat intelligence.

Endpoint Vulnerability assessment

Network Profiling



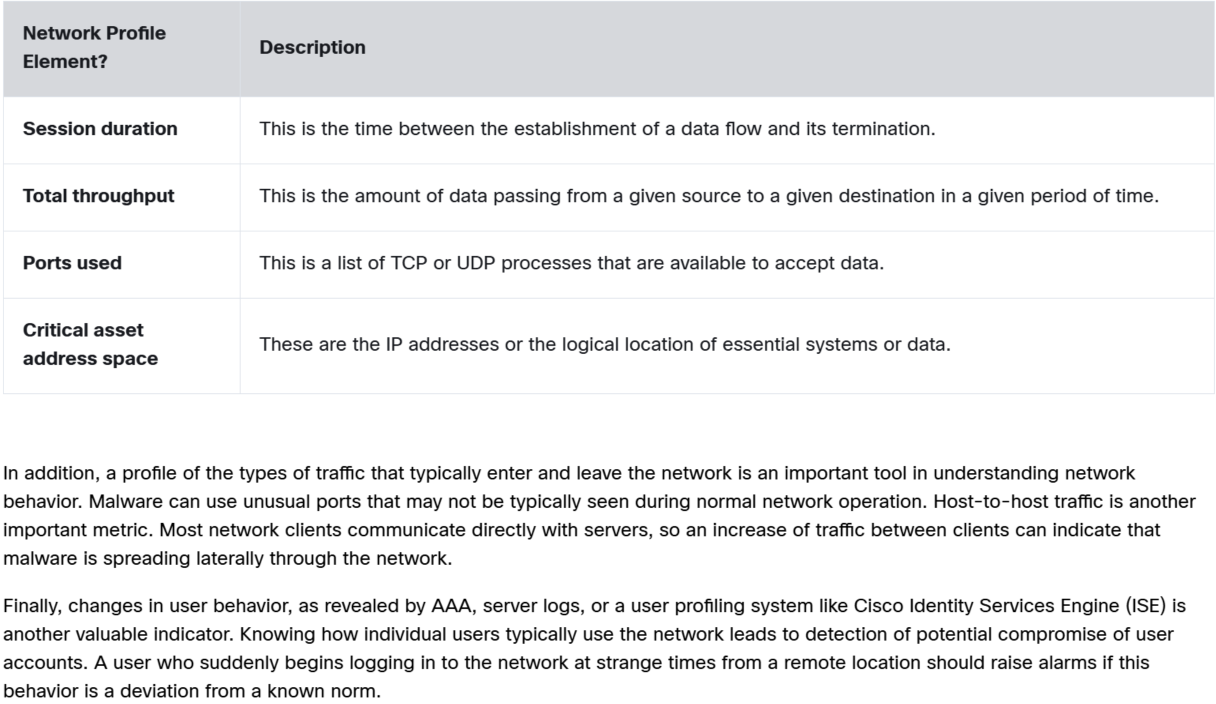
In order to detect serious security incidents, it is important to understand, characterize, and analyze information about normal network functioning. Networks, servers, and hosts all exhibit typical behavior for a given point in time. Network and device profiling can provide a statistical baseline that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

Care must be taken when capturing baseline data so that all normal network operations are included in the baseline. In addition, it is important that the baseline is current. It should not include network performance data that is no longer part of normal functioning. For example, rises in network utilization during periodic server backup operations is part of normal network functioning and should be part of the baseline data. However, measurement of traffic that corresponds to outside access to an internal server that has been moved to the cloud would not be. A means of capturing just the right period for baseline measurement is known as sliding window anomaly detection. It defines a window that is most representative of network operation and deletes data that is out of date. This process continues with repeated baseline measurements to ensure that baseline measurement statistics depict network operation with maximum accuracy.

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. The figure displays some questions to ask when establishing a network baseline.

The table lists important elements of the network profile.

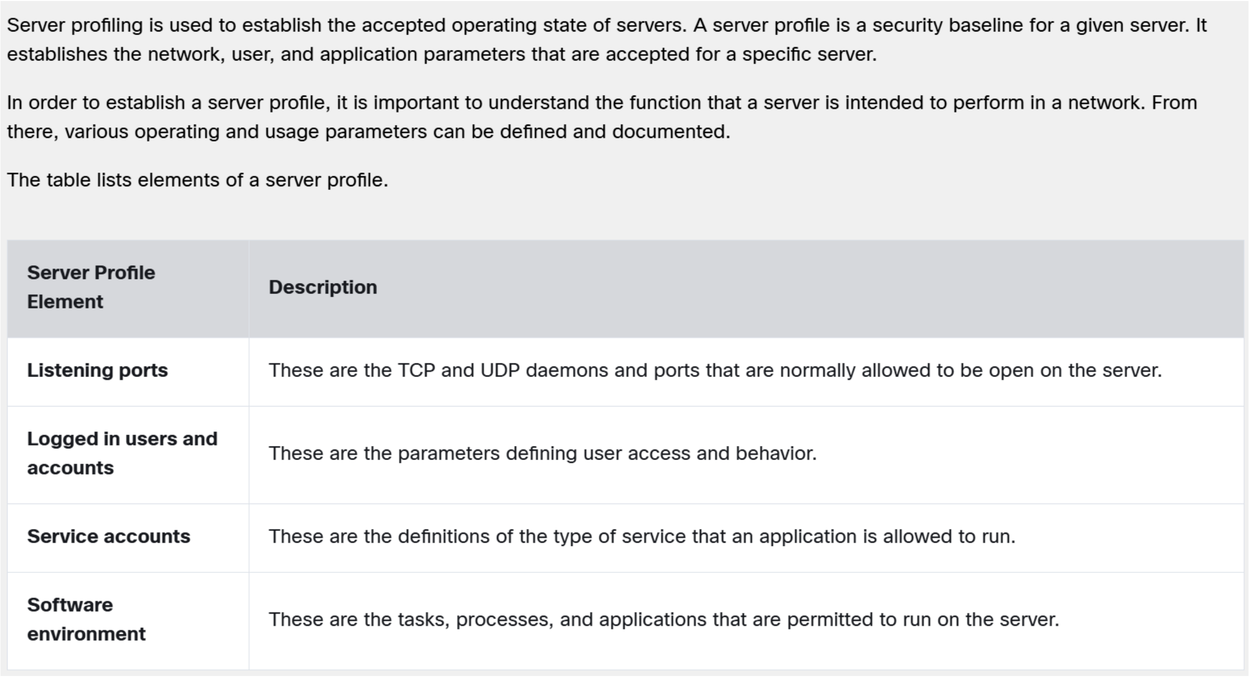


Network Profile Element?	Description
Session duration	This is the time between the establishment of a data flow and its termination.
Total throughput	This is the amount of data passing from a given source to a given destination in a given period of time.
Ports used	This is a list of TCP or UDP processes that are available to accept data.
Critical asset address space	These are the IP addresses or the logical location of essential systems or data.

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



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.

The table lists elements of a server profile.

Server Profile Element	Description
Listening ports	These are the TCP and UDP daemons and ports that are normally allowed to be open on the server.
Logged in users and 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.
Software environment	These are the tasks, processes, and applications that are permitted to run on the server.

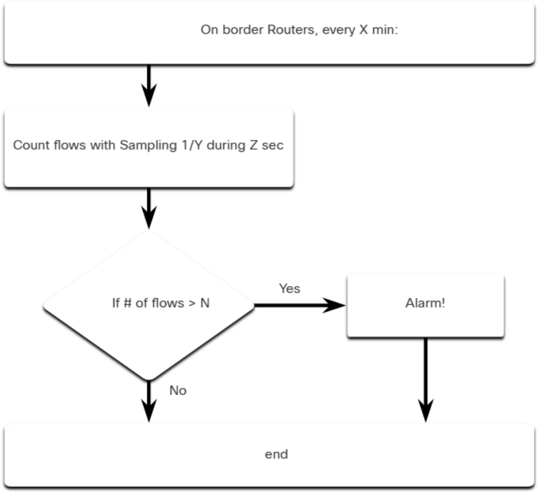
Network Anomaly Detection

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. One approach to detection of network attacks is the analysis of this diverse, unstructured data using Big Data analytics techniques. This is known as network behavior analysis (NBA).

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. In addition, network behavior can be analyzed for known network behaviors that indicate compromise.

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

The figure illustrates a simplified version of an algorithm designed to detect an unusual condition at the border routers of an enterprise.


On border Routers, every X min:
Count flows with Sampling 1/Y during Z sec
If # of flows > N
Yes
Alarm!
No
end

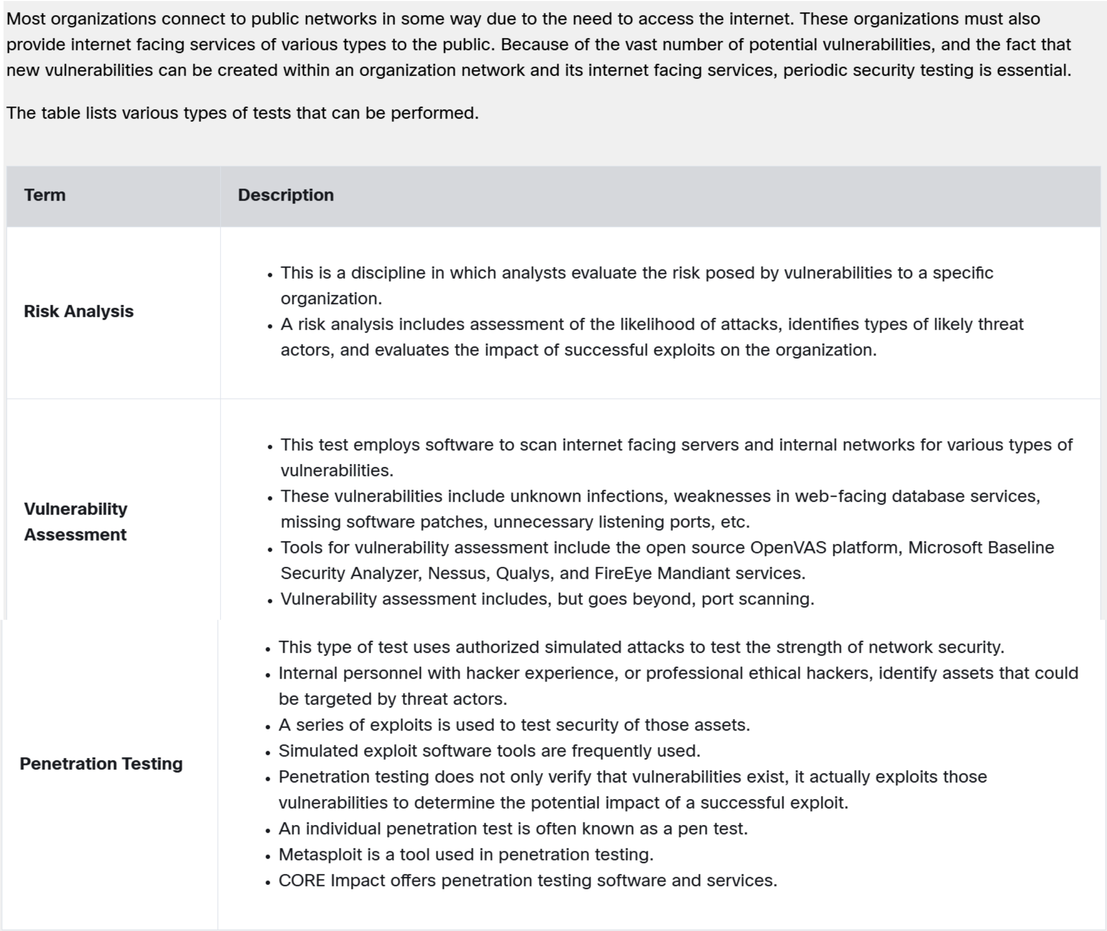
For example, the cybersecurity analyst could provide the following values:

- X = 5, Y = 100, Z = 30. And 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.

In addition to statistical and behavioral approaches to anomaly detection is rule-based anomaly detection. Rule-based detection analyzes decoded packets for attacks based on pre-defined patterns.

Network Vulnerability Testing

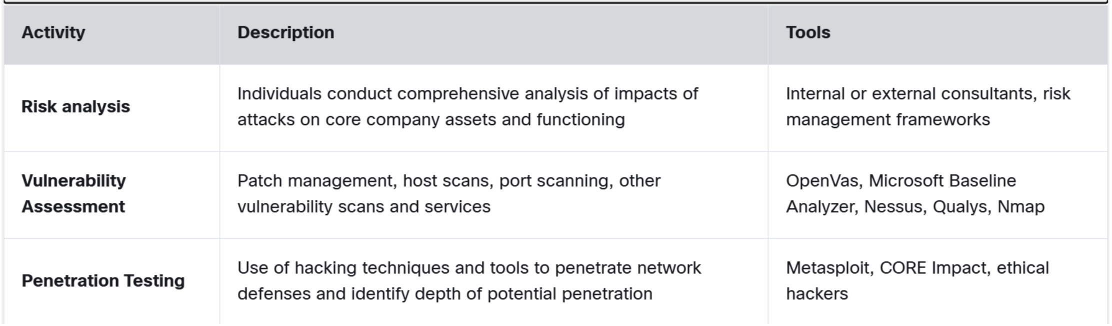


Most organizations connect to public networks in some way due to the need to access the internet. These organizations must also provide internet facing services of various types to the public. Because of the vast number of potential vulnerabilities, and the fact that new vulnerabilities can be created within an organization network and its internet facing services, periodic security testing is essential.

The table lists various types of tests that can be performed.

Term	Description
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.

The table lists examples of activities and tools that are used in vulnerability testing.



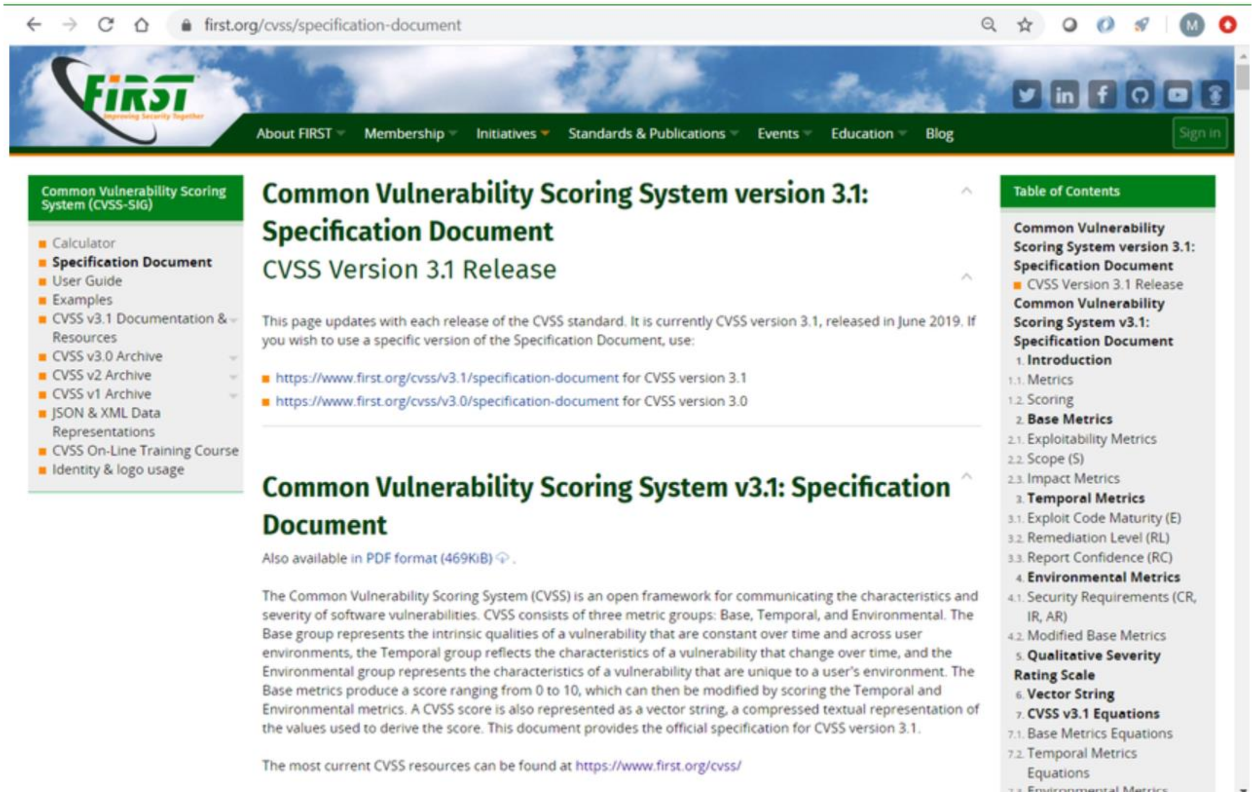
Activity	Description	Tools
Risk analysis	Individuals conduct comprehensive analysis of impacts of attacks on core company assets and functioning	Internal or external consultants, risk management frameworks
Vulnerability Assessment	Patch management, host scans, port scanning, other vulnerability scans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

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is a risk assessment tool that is 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. The Version 3 standard was developed with contributions by Cisco and other industry partners. Version 3.1 was released in June of 2019. The figure displays the specification page for the CVSS at the FIRST website.


first.org/cvss/specification-document
FIRST
Improving Security Together
About FIRST
Membership
Initiatives
Standards & Publications
Events
Education
Blog
Sign in
Common Vulnerability Scoring System (CVSS-SIG)
Calculator
Specification Document
User Guide
Examples
CVSS v3.1 Documentation & Resources
CVSS v3.0 Archive
CVSS v2 Archive
CVSS v1 Archive
JSON & XML Data Representations
CVSS On-Line Training Course
Identity & logo usage
Table of Contents
Common Vulnerability Scoring System version 3.1: Specification Document
CVSS Version 3.1 Release
Common Vulnerability Scoring System v3.1: Specification Document
1. Introduction
1.1. Metrics
1.2. Scoring
2. Base Metrics
2.1. Exploitability Metrics
2.2. Scope (S)
2.3. Impact Metrics
3. Temporal Metrics
3.1. Exploit Code Maturity (E)
3.2. Remediation Level (RL)
3.3. Report Confidence (RC)
4. Environmental Metrics
4.1. Security Requirements (CR, IR, AR)
4.2. Modified Base Metrics
5. Qualitative Severity Rating Scale
6. Vector String
7. CVSS v3.1 Equations
7.1. Base Metrics Equations
7.2. Temporal Metrics Equations

Common Vulnerability Scoring System version 3.1: Specification Document

CVSS Version 3.1 Release

This page updates with each release of the CVSS standard. It is currently CVSS version 3.1, released in June 2019. If you wish to use a specific version of the Specification Document, use:

- https://www.first.org/cvss/v3.1/specification-document for CVSS version 3.1
- https://www.first.org/cvss/v3.0/specification-document for CVSS version 3.0

Common Vulnerability Scoring System v3.1: Specification Document

Also available in PDF format (469KiB) .

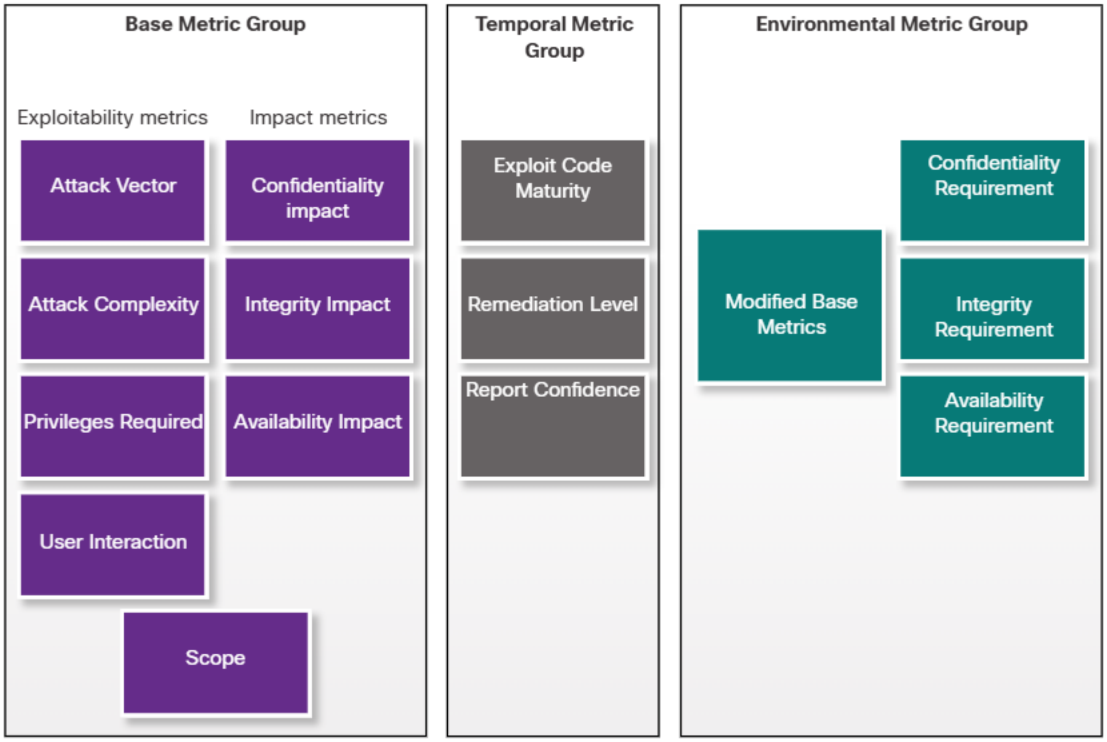
The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 3.1.

The most current CVSS resources can be found at https://www.first.org/cvss/

CVSS Metric Groups

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 that grants and manages access and privileges to users.



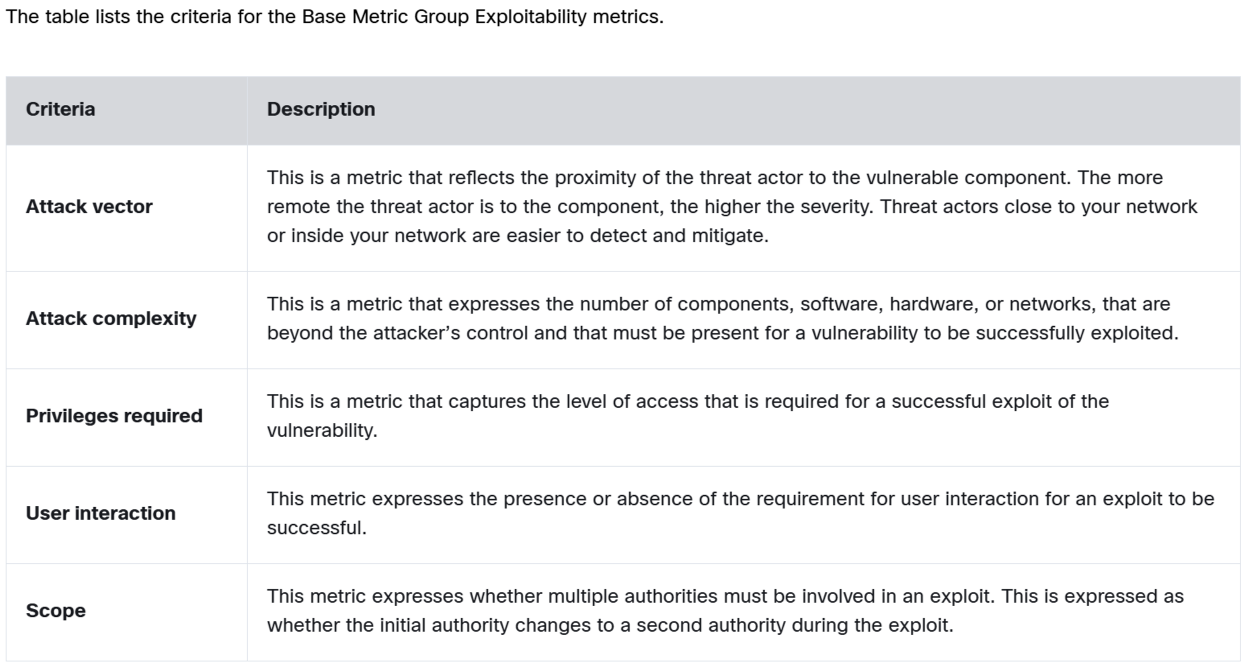
As shown in the figure, the CVSS uses three groups of metrics to assess vulnerability.

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

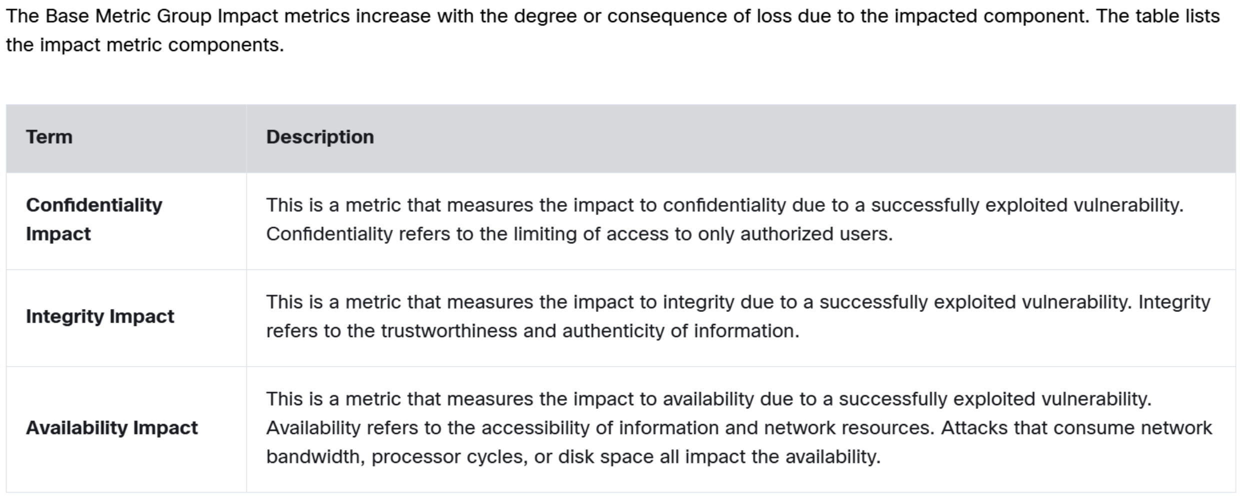
Temporal Metric Group: This measures the characteristics of a vulnerability that may change over time, but not across user environments. Over time, the severity of a vulnerability will change as it is detected and measures to counter it are developed. The severity of a new vulnerability may be high, 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 rate consequences within an organization and allow adjustment of metrics that are less relevant to what an organization does.



The table lists the criteria for the Base Metric Group Exploitability metrics.

Criteria	Description
Attack vector	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	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 for a vulnerability to be successfully exploited.
Privileges required	This is a metric that captures the level of access that is required for a successful exploit of the vulnerability.
User interaction	This metric expresses the presence or absence of the requirement for user interaction for an exploit to be successful.
Scope	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.



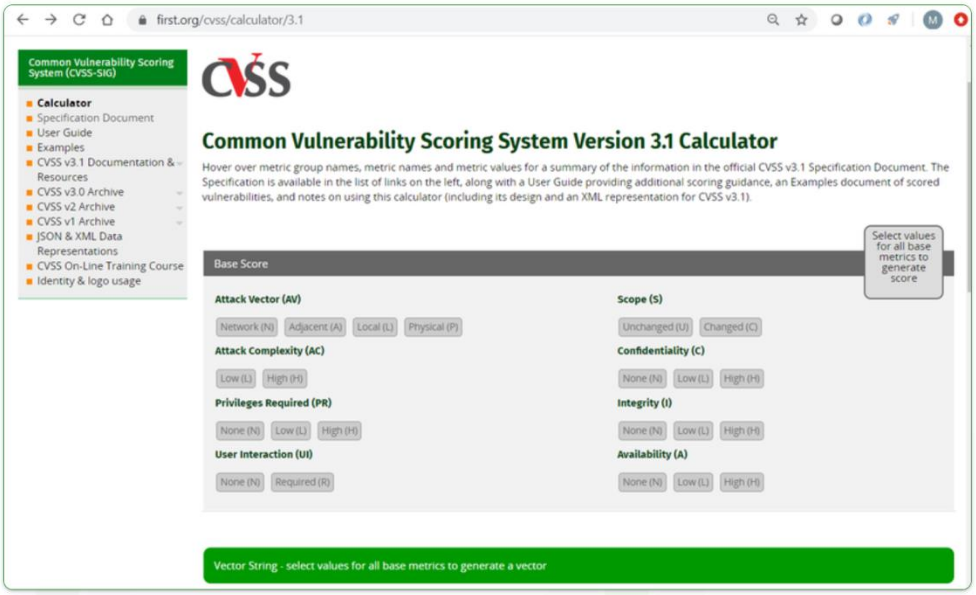
The Base Metric Group Impact metrics increase with the degree or consequence of loss due to the impacted component. The table lists the impact metric components.

Term	Description
Confidentiality Impact	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	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	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

The CVSS Base Metrics Group is designed as a way to assess security vulnerabilities that are 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 v3.1 Calculator, shown in the figure.



Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- CVSS v3.1 Documentation & Resources
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 3.1 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.1).

Base Score

Select values for all base metrics to generate score

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)

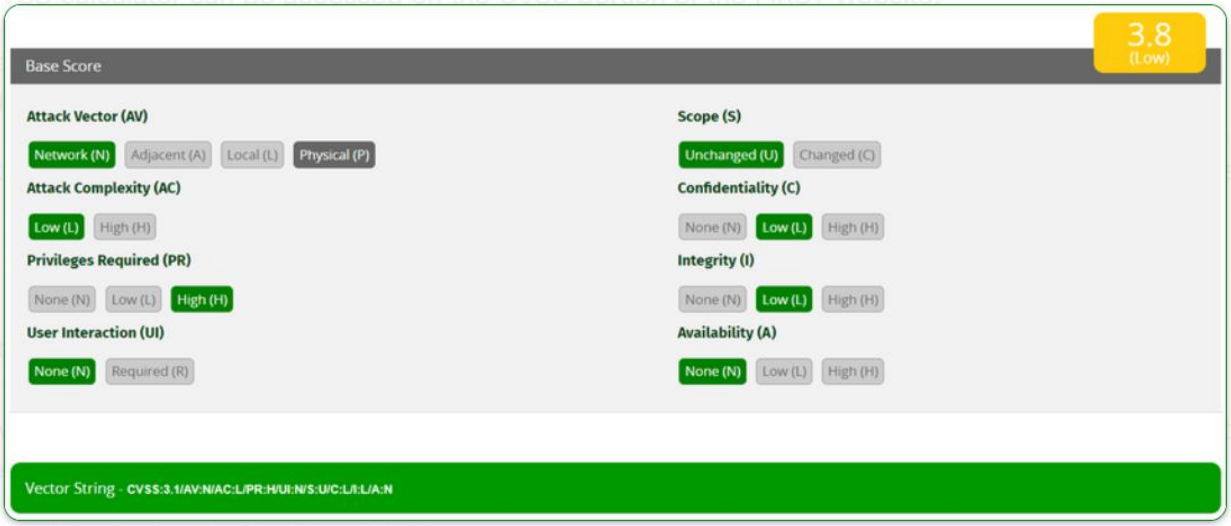
Vector String - select values for all base metrics to generate a vector

The calculator is like questionnaires 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 explains each metric and metric value is displayed by hovering the mouse over each. Choices are made by choosing one of the values for the metric. Only one choice can be made per metric.

The CVSS calculator can be accessed on the CVSS portion of the FIRST website.

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 the figure.



Base Score

3.8
(Low)

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)

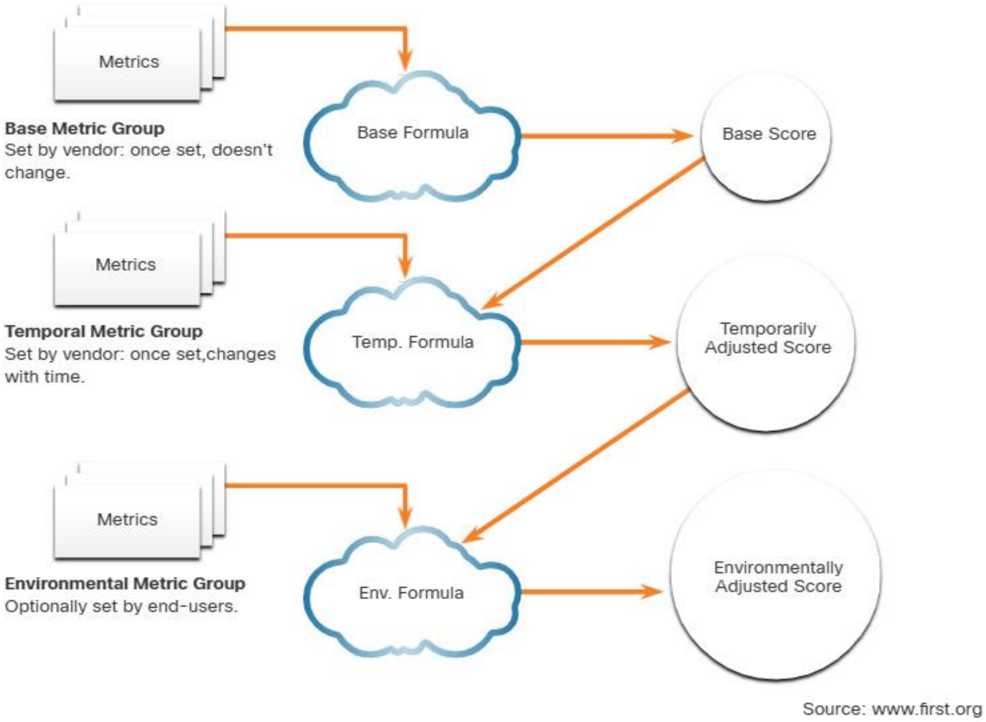
Confidentiality (C)
None (N) [✓ Low (L)] High (H)

Integrity (I)
None (N) [✓ Low (L)] High (H)

Availability (A)
[✓ None (N)] Low (L) High (H)

Vector String - CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

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 the figure.


Metrics
Base Metric Group
Set by vendor: once set, doesn't change.
Base Formula
Base Score
Metrics
Temporal Metric Group
Set by vendor: once set,changes with time.
Temp. Formula
Temporarily Adjusted Score
Metrics
Environmental Metric Group
Optionally set by end-users.
Env. Formula
Environmentally Adjusted Score

Source: www.first.org

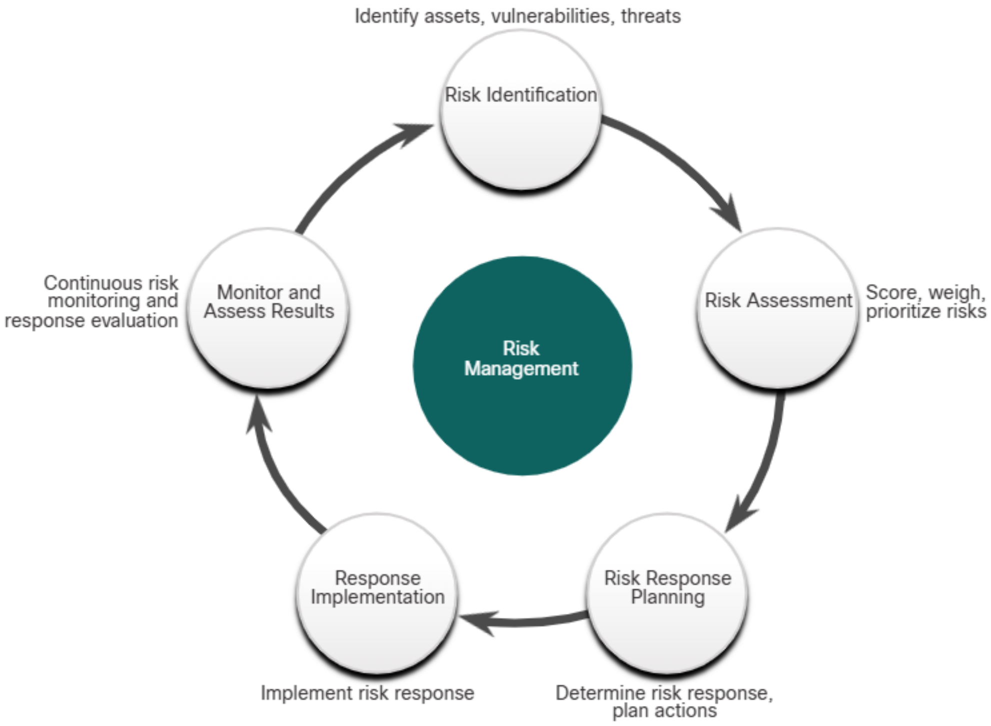
Secure Device Management

Risk Management

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, multi-step, cyclical process, as shown in the figure.

A Risk Management Process


Identify assets, vulnerabilities, threats
Risk Identification
Risk Assessment
Score, weigh, prioritize risks
Risk Response Planning
Determine risk response, plan actions
Response Implementation
Implement risk response
Monitor and Assess Results
Continuous risk monitoring and response evaluation
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?

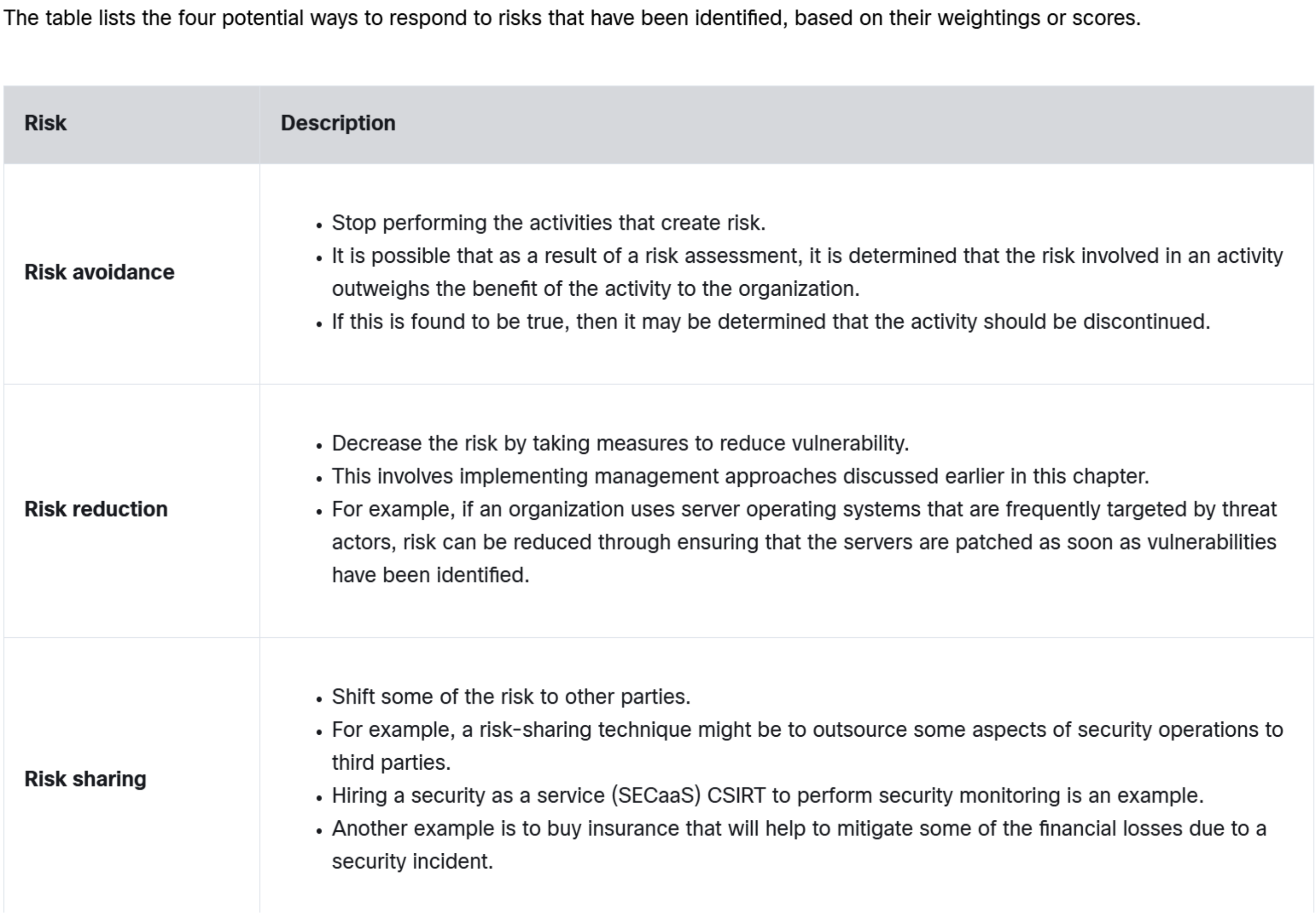
NIST Special Publication 800-30 describes risk assessment as:

...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.

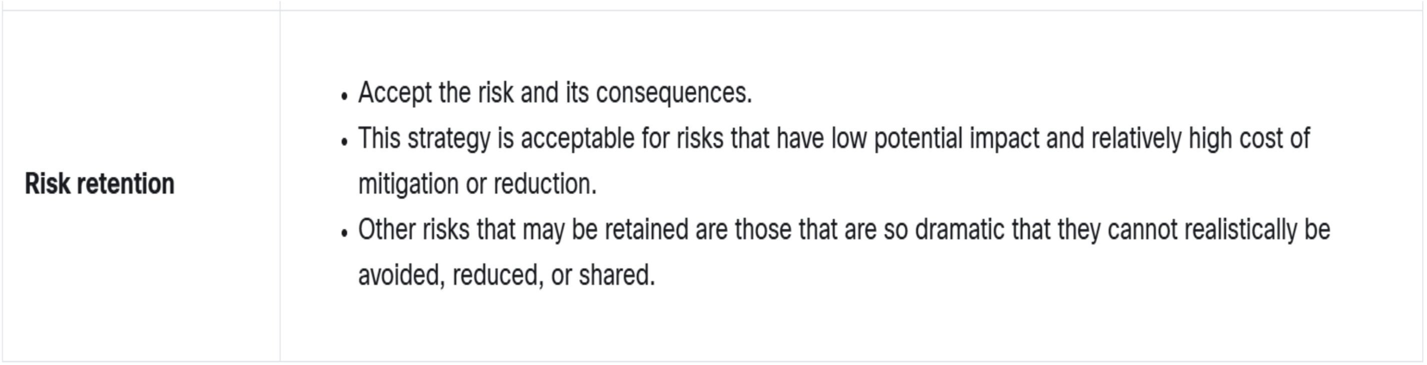
The full publication is available for download from NIST.

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.



The table lists the four potential ways to respond to risks that have been identified, based on their weightings or scores.



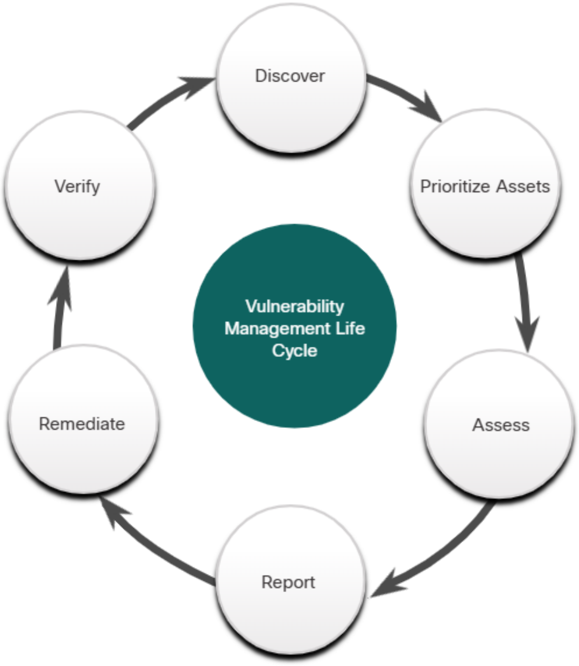
Risk	Description
Risk avoidance	• Stop performing the activities that create risk. • It is possible that as a result of a risk assessment, it is determined that the risk involved in an activity outweighs the benefit of the activity to the organization. • If this is found to be true, then it may be determined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

Vulnerability Management

According to NIST, vulnerability management is a security practice that is 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 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.

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. Conduct additional scans if necessary to confirm that vulnerabilities have been properly resolved.

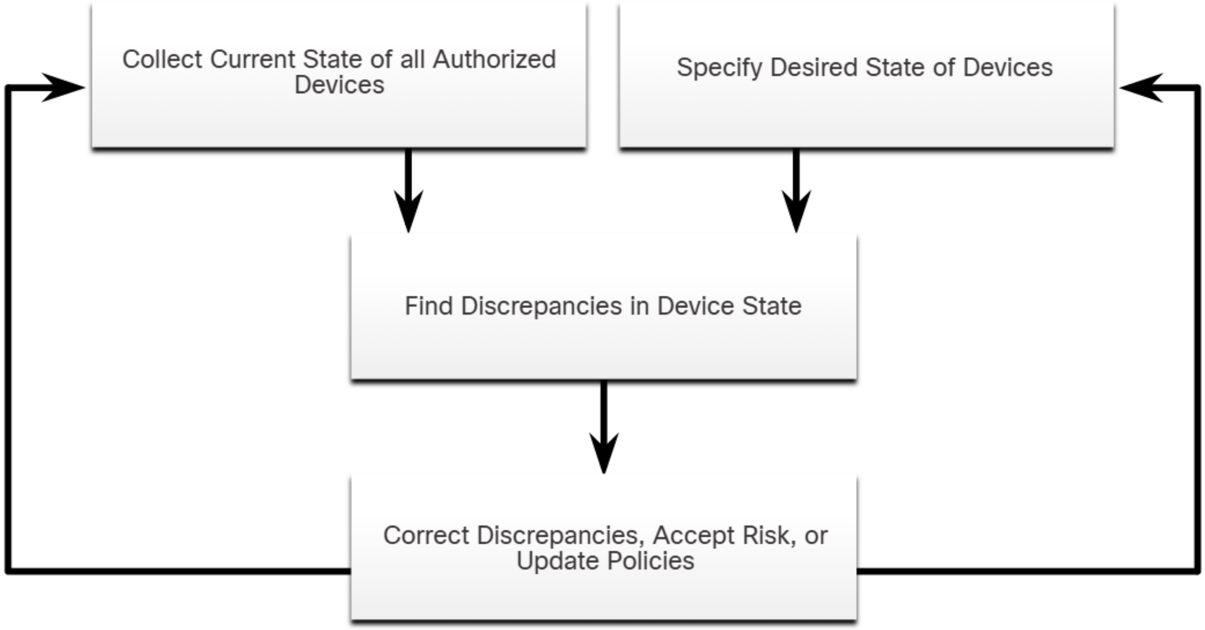
Asset Management

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.

NIST specifies in publication NISTIR 8011 Volume 2, 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 non-compliant authorized assets
- Remediation or acceptance of device state, possible iteration of desired state definition
- Repeat the process at regular intervals, or ongoing

The figure provides an overview of this process.

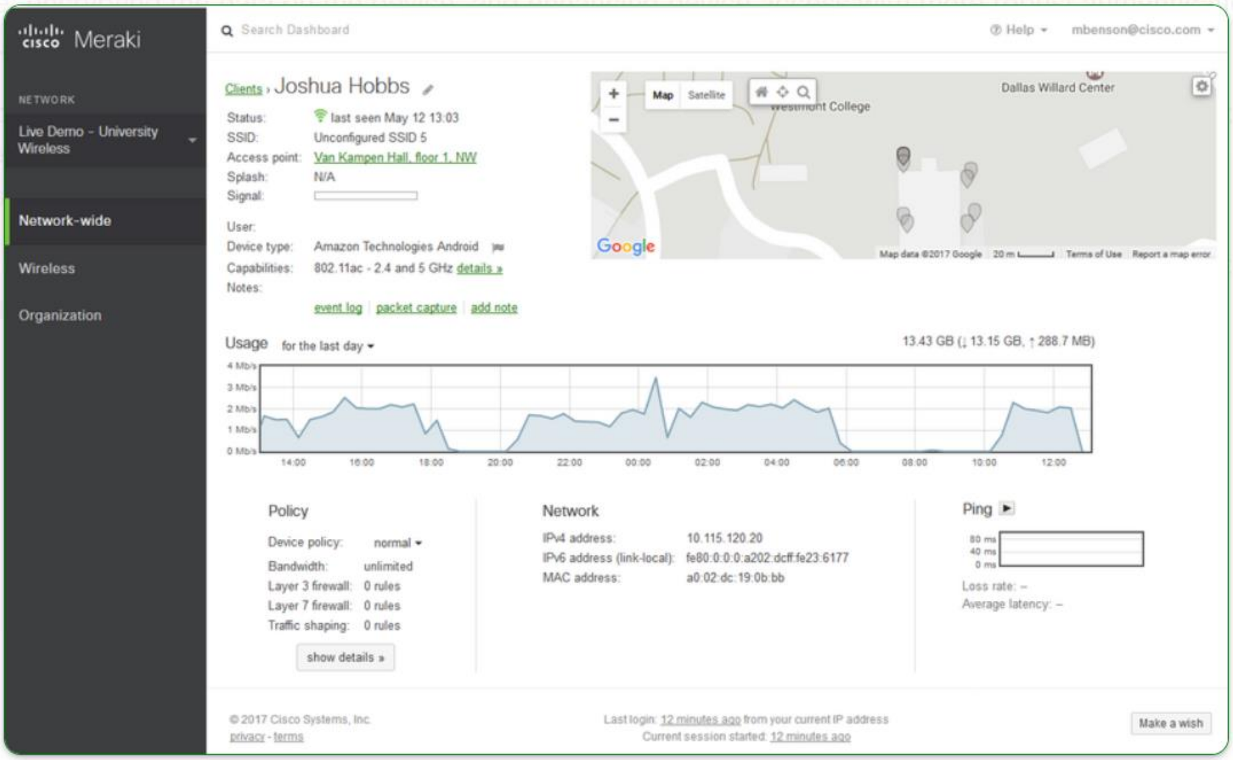

Collect Current State of all Authorized Devices
Specify Desired State of Devices
Find Discrepancies in Device State
Correct Discrepancies, Accept Risk, or Update Policies

Mobile Device Management

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 acting 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 the figure, allow security personnel to configure, monitor and update a very diverse set of mobile clients from the cloud.



Clients › Joshua Hobbs

Status: last seen May 12 13:03
SSID: Unconfigured SSID 5
Access point: Van Kampen Hall, floor 1, NW
Splash: N/A
Signal:
User:
Device type: Amazon Technologies Android
Capabilities: 802.11ac - 2.4 and 5 GHz details »
Notes:

13.43 GB (↓ 13.15 GB, ↑ 288.7 MB)

Policy

Device policy: normal
Bandwidth: unlimited
Layer 3 firewall: 0 rules
Layer 7 firewall: 0 rules
Traffic shaping: 0 rules

Network

IPv4 address: 10.115.120.20
IPv6 address (link-local): fe80:0:0:0:a202:dcff:fe23:6177
MAC address: a0:02:dc:19:0b:bb

Loss rate: –
Average latency: –

© 2017 Cisco Systems, Inc.

Last login: 12 minutes ago from your current IP address
Current session started: 12 minutes ago

Configuration Management

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.

NIST Special Publication 800-128 on configuration management for network security is available for download from NIST.

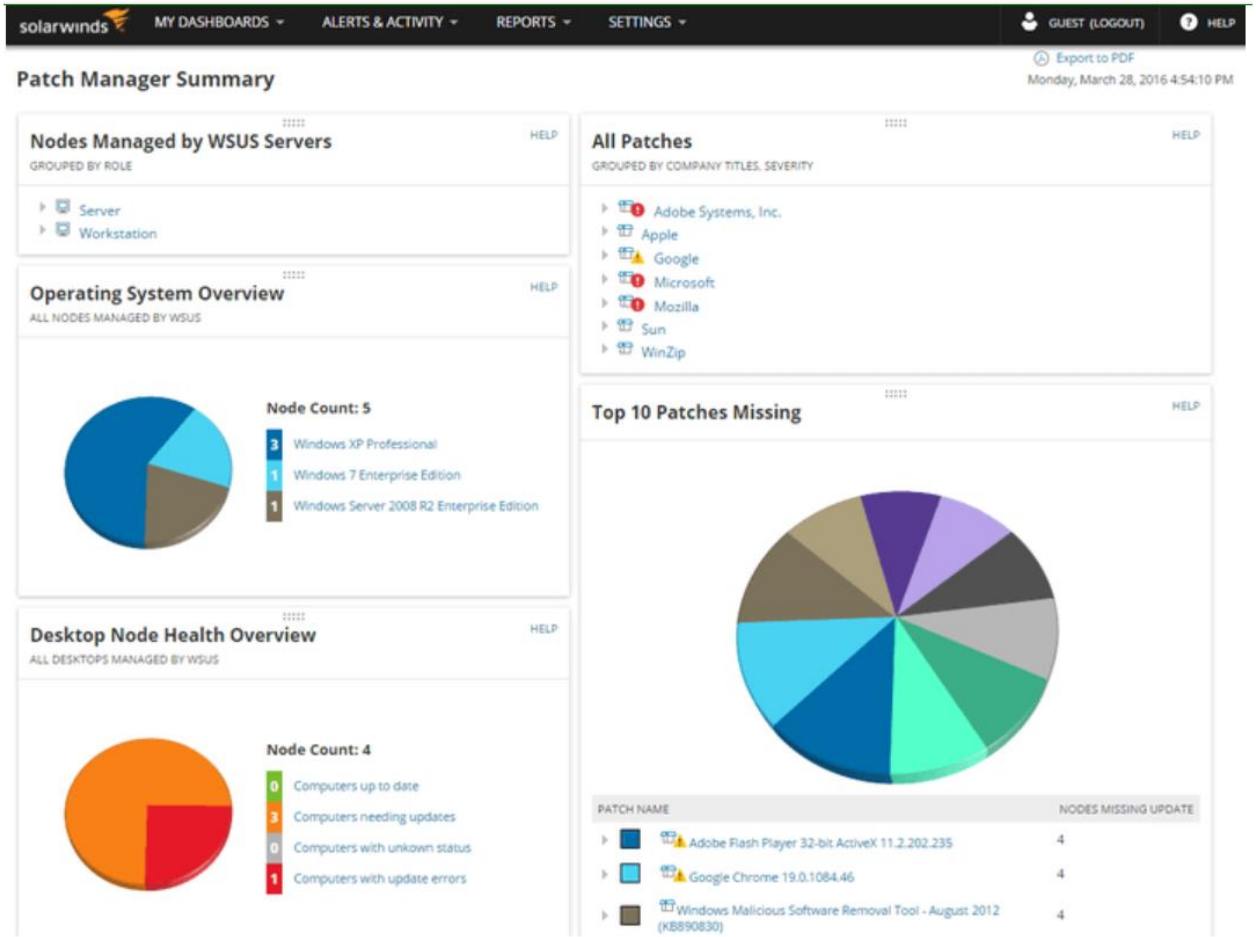
For internetworking devices, software tools are available that will backup configurations, detect changes in configuration files, and enable bulk change of configurations across a number of devices.

With the advent of cloud data centers and virtualization, management of numerous servers presents special challenges. Tools like Puppet, Chef, Ansible, and SaltStack enable efficient management of servers that are used in cloud-based computing.

Enterprise Patch Management

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, installing, and verifying that the patch is installed on all required systems. Installing patches is frequently the most effective way to mitigate software vulnerabilities. Sometimes, they are the only way to do so.

Patch management is required by some compliance regulations, such as Sarbanes Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA). Failure to implement patches in a systematic and timely manner could result in audit failure and penalties for non-compliance. Patch management depends on asset management data to identify systems that are running software that requires patching. Patch management software is available from companies such as SolarWinds and LANDesk. Microsoft System Center Configuration Manager (SCCM) is an enterprise-level tool for automated distribution of patches to a large number of Microsoft Windows workstations and servers.



Patch Manager Summary

Monday, March 28, 2016 4:54:10 PM

Nodes Managed by WSUS Servers

GROUPED BY ROLE

- Server
- Workstation

Operating System Overview

ALL NODES MANAGED BY WSUS

Node Count: 5

3	Windows XP Professional
1	Windows 7 Enterprise Edition
1	Windows Server 2008 R2 Enterprise Edition

Desktop Node Health Overview

ALL DESKTOPS MANAGED BY WSUS

Node Count: 4

0	Computers up to date
3	Computers needing updates
0	Computers with unkown status
1	Computers with update errors

All Patches

GROUPED BY COMPANY TITLES, SEVERITY

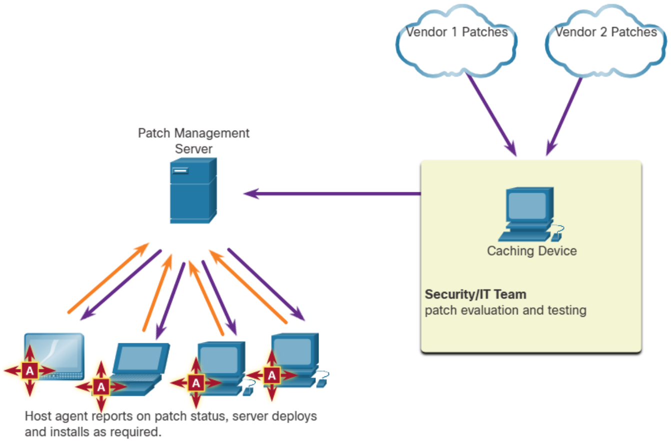
- Adobe Systems, Inc.
- Apple
- Google
- Microsoft
- Mozilla
- Sun
- WinZip

Top 10 Patches Missing

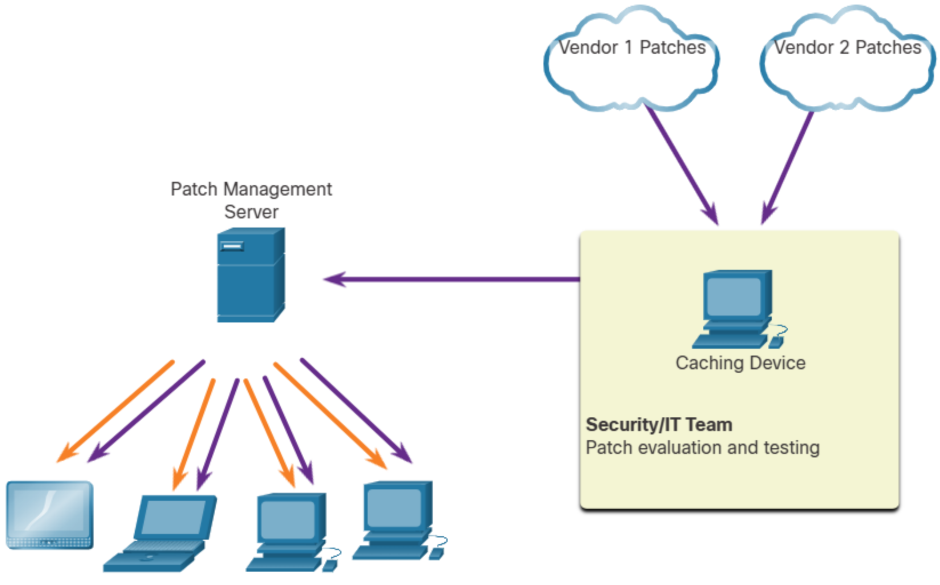
PATCH NAME	NODES MISSING UPDATE
Adobe Flash Player 32-bit ActiveX 11.2.202.235	4
Google Chrome 19.0.1084.46	4
Windows Malicious Software Removal Tool - August 2012 (KB890830)	4

Patch Management Techniques

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

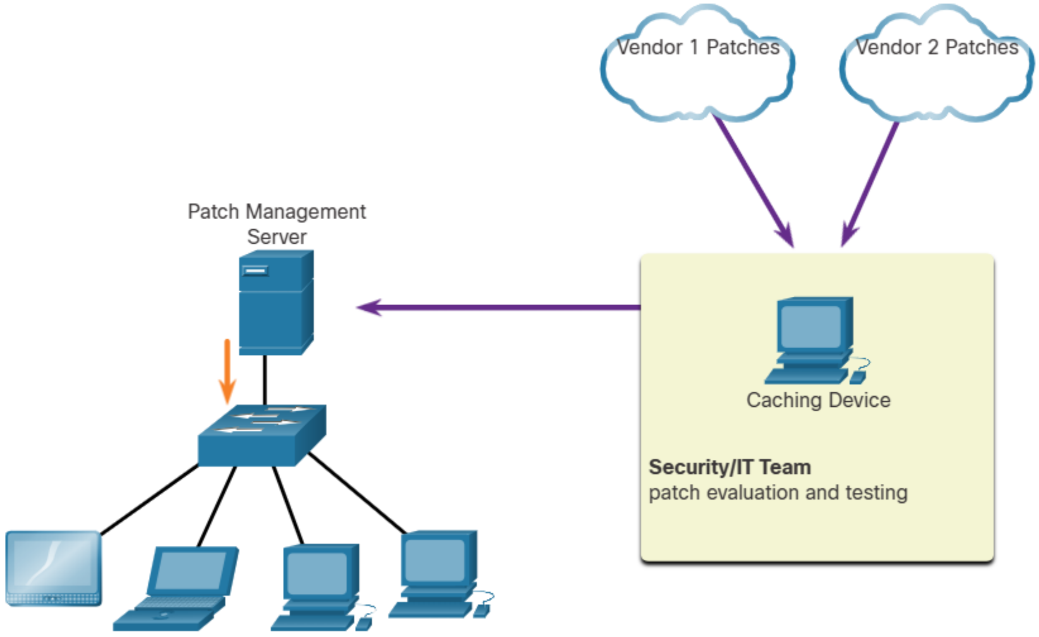

Vendor 1 Patches
Vendor 2 Patches
Patch Management Server
Caching Device
Security/IT Team
patch evaluation and testing
A
A
A
A
Host agent reports on patch status, server deploys and installs as required.

- **Agentless scanning:** Patch management servers scan the network for devices that require patching. The server determines which patches are required and installs those patches on the clients. Only devices that are on scanned network segments can be patched in this way. This can be a problem for mobile devices.



Server detects patch status and installs as required.

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



Server monitors and tracks software version from network traffic, patches deployed as required.

Risk management and security controls

Risk Types

Risk is the probability of loss due to a threat — a malicious act or unexpected event — that damages information systems or organizational assets.

Risk impact is the damage incurred by an event which causes loss of asset(s) or disruption of service(s). The goal of risk management is to reduce these threats to an acceptable level and to implement controls to maintain that level.

Let’s learn more about the ever-changing levels of threat that an organization must continually identify and assess.

Negligence means that no actions or controls are taken to lower risk. The threat is very high, and the cost of an incident could be catastrophic.

Exercising due care can help lower the level of risk. The risk still exists but these reasonable steps lower a potential loss.

Exercising due diligence involves taking reasonable steps to eliminate risk. Some risks still exist, but multiple controls are implemented to prevent potential loss.

Risk can be internal, external, or both. Its impact can ripple through the whole organization and affect other external entities.

Promoting risk awareness within the organization helps employees to develop an understanding of what risks exist, their potential impact and how the organization can manage those risks.

The Risk Management Process

Risk management is a formal process that measures the impact of a threat and the cost to implement controls or countermeasures to mitigate that threat.

Risk cannot be eliminated completely but it can still be managed to an acceptable level. All organizations accept some risk and the cost of a counter measure should not be more than the value of the asset being protected.

Stages of the risk management process:

- **Frame the risk:** identify the threats through the organization that increase risk. Threats identified include loss or damage of processes and products, attacks, potential failure or disruption of services, harm to be organization’s reputation, legal liability, and loss of intellectual property.
- **Assess the risk:** once risk has been identified, it is assessed and analyzed to determine the severity that the threat poses. Some threats can bring the entire organization to a standstill while other threats are merely minor inconveniences. Risk can be prioritized by actual financial impact or a scaled impact on the organization’s operation.
- **Respond to the risk** Develop an action plan to reduce overall organization risk exposure. Management ranks and prioritized threats; a team then determines how to respond to each threat. Risk can be eliminated, mitigated, transferred or accepted.
- **Monitor the risk:** continuously review risk reductions due to elimination, mitigation and transfer actions. Not all risks can be eliminated, so threats that are accepted need to be closely monitored. An organization can use a risk register – a software program or cloud service – to record information about identified risks. The risk register contains details about the risk and the controls implemented or response strategies used.

Risk Assessment

Threat Source Types

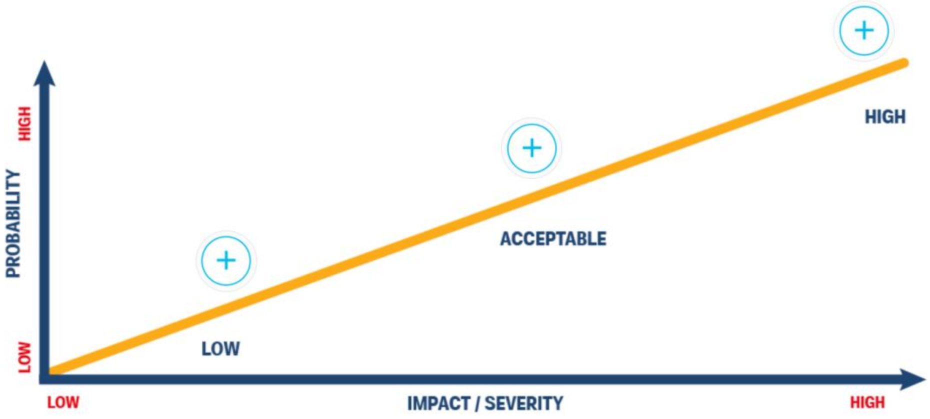
Threat assessment is the foundation for risk assessment. A threat is the potential that a vulnerability will be identified and exploited, while a threat vector is the path that an attacker utilizes to impact the target.

Threat source types are categorized as follows, and can be internal or external.

- **Adversarial:** Threats from individuals, groups, organizations or nations.
- **Accidental:** Actions that occur without a malicious intent.
- **Structural:** Equipment and software failures.
- **Environmental:** External disasters that can be either natural or human-caused, such as fires and floods.

Risk Assessment Methodology

Organizations assess and examine their operational risks by performing a risk assessment to ensure their risk management meets all their business objectives.



- **Low:** Trying to determine the probability of an attack by a human threat source can be difficult and may involve assessing skill level, motive, opportunity and size.
- **Acceptable**: When assessing vulnerability, factors such as ease of discovery, exploitability, and awareness and intrusion detection play a part. Use a combination of estimation and historical data to provide the most accurate probability of an event occurring.
- **High:** Finally, determine the magnitude of the impact. A simple measure of impact can range from very low to very high or from an insignificant impact to a catastrophic impact.

Risk Analysis

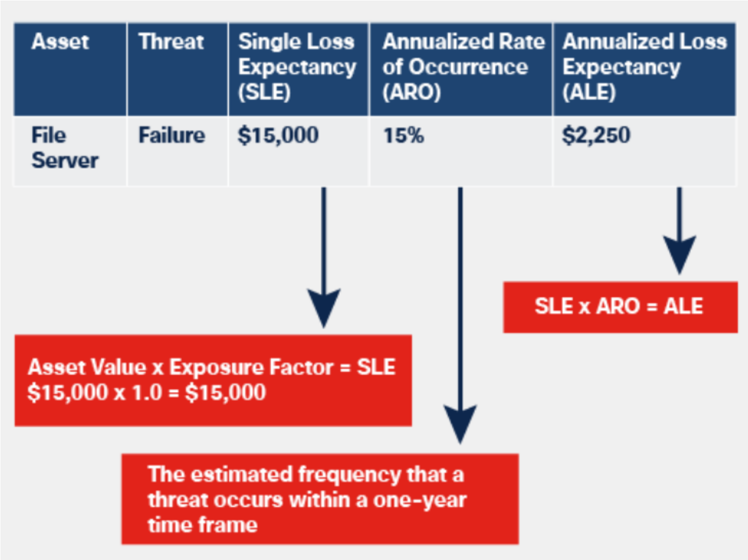
Risk analysis examines the dangers posed by natural and human-caused events to the assets of an organization. A user performs an asset identification to help determine which assets to protect.

A risk analysis has four goals:

1. Identify assets and their value.
2. Identify vulnerabilities and threats.
3. Quantify the probability and impact of the identified threats.
4. Balance the impact of the threat against the cost of the countermeasure.

Let’s learn more about the two approaches to risk analysis.

- **Quantitative risk analysis:** A quantitative risk analysis assigns numbers to the risk analysis process. In this example, the **asset value** is the replacement cost of the file server (the asset). The value of an asset can also be measured by the income gained through the use of the asset. The **exposure factor (EF)** is a subjective value expressed as a percentage of the file server lost due to a particular threat. If total loss occurs, the EF equals 1.0 (100%). The **annualized rate of occurrence (ARO)** is the probability that a loss will occur during the year. An ARO can be greater than 100% if a loss can occur more than once a year. The calculation of the **annual loss expectancy (ALE)** gives management some guidance on what an organization should spend to protect the file server.



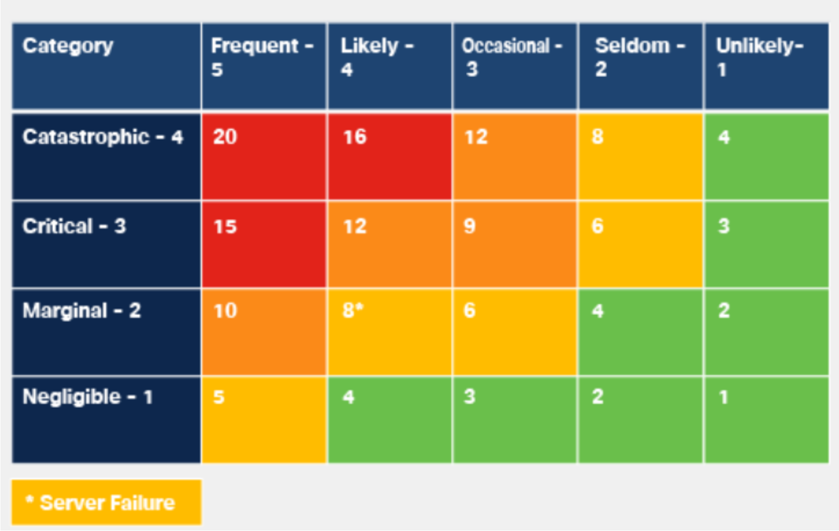
Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)
File Server	Failure	$15,000	15%	$2,250

SLE x ARO = ALE

Asset Value x Exposure Factor = SLE
$15,000 x 1.0 = $15,000

The estimated frequency that a threat occurs within a one-year time frame

- Qualitative risk analysis: Qualitative risk analysis uses opinions and scenarios plotting the likelihood of a threat against its impact. For example, a server failure may be likely, but its impact may only be marginal. A risk matrix is a tool that helps prioritize risks to determine which ones the organization needs to develop a response for. The results can be ranked and used as a guide to determine whether the organization takes any action. When the risk matrix is color-coded, as shown here, it is referred to as a risk heat map.



Category	Frequent - 5	Likely - 4	Occasional - 3	Seldom - 2	Unlikely- 1
Catastrophic - 4	20	16	12	8	4
Critical - 3	15	12	9	6	3
Marginal - 2	10	8*	6	4	2
Negligible - 1	5	4	3	2	1

* Server Failure

Risk Mitigation

Mitigation involves reducing the likelihood or severity of a loss from threats. Many technical controls mitigate risk, including authentication systems, file permissions and firewalls.

Organizations must understand that risk mitigation can have both positive and negative impacts on the organization. Good risk mitigation finds a balance between the negative impact of countermeasures and controls and the benefit of risk reduction.

The most common ways to militate against risk:

- **Accept the risk and periodically reassess:** A short-term strategy is to accept the risk necessitating the creation of contingency plans for that risk. People and organizations have to accept risk on a daily basis.
- **Reduce the risk by implementing controls**: Modern methodologies reduce risk by developing software incrementally, and by providing regular updates and patches to address vulnerabilities and Misconfigurations.
- **Avoid the risk by totally changing the approach:** A good risk mitigation plan can include two or more strategies.
- **Transfer the risk to a third party**: Outsourcing services, purchasing insurance and purchasing maintenance contracts are all examples of risk transfer. Hiring specialists to perform critical tasks to reduce risk can be a good decision and yield greater results with less long-term investment.

Security Controls

Control Types

The inherent risk of a system is the risk that the system poses inherently — without any people, process or technology controls in place. Security controls are safeguards or countermeasures that an organization implements to avoid, detect, counteract or minimize security risks to organizational assets.

- **Administrative controls:** Administrative controls consist of procedures and policies that an organization puts into place when dealing with sensitive information. These controls determine how people act.
- **Technical controls:** Technical controls involve hardware and/or software implemented to manage risk and provide protection.
- **Physical controls:** Physical controls are mechanisms such as fences and locks deployed to protect systems, facilities, personnel and resources. Physical controls physically separate people or other threats from systems.

Functional Security Controls

The functional use of a specific safeguard or counter measure will help determine the reason for choosing and implementing it. Let's find out more about the functional security controls.

- **Preventive controls**: Preventive security controls stop unwanted and unauthorized activity from happening and/or apply restrictions for authorized users. For example, assigning user specific privileges on a system is a preventive control, as it puts limits in place to prevent certain users from accessing and performing unauthorized actions. A firewall that blocks access to a port or service that cybercriminals can exploit is also a preventive control.
- **Deterrent controls**: A deterrent aims to discourage something from happening. Cybersecurity professionals and organizations use deterrents to limit or mitigate an action or behavior — but deterrents cannot stop them completely. Deterrent controls discourage cybercriminals from gaining unauthorized access to information systems and sensitive data. They can be effective at discouraging many different types of attacks on systems, as well as data theft and spreading malicious code.
- **Detective controls**: Access control detection identifies different types of unauthorized activity. Detective controls are not a preventive measure and instead focus on the discovery of a security breach after it has occurred. All detective systems have several things in common. They look for unusual or prohibited activity and can be very simple, such as a motion detector or security guard, or complex, such as an intrusion detection system. Detective controls may also provide methods to record or alert system operators of potential unauthorized access incidents.
- **Corrective controls**: Corrective controls counteract something undesirable by restoring the system back to a state of confidentiality, integrity and availability. They can also restore systems to normal after unauthorized activity occurs. Organizations will implement corrective access controls after a system experiences a threat. Examples include security policies, alarms, antivirus software, intrusion detection systems, mantraps and business continuity planning.
- **Recovery controls**: Recovery security controls restore resources, functions and capabilities back to a normal state after a violation of a security policy. Recovery controls can repair damage, in addition to stopping any further damage. These controls have more advanced capabilities over corrective access controls. Examples of recovery controls include backup/restore operations, fault tolerance drive systems, server clustering, and database shadowing.
- **Compensative controls:** Compensative controls provide options to other controls to bolster enforcement in support of a security policy. A compensative control can also be a substitution used in place of a control that is not possible under the circumstances. Perhaps an organization is not able to have a guard dog so, instead, it deploys a motion detector with a spotlight and a barking sound.Examples of compensative security controls

include security policies, personnel supervision, monitoring and work task procedures that are used in the absence of the ideal control an organization would have put in place.

Controls and Compliance

The Center for Internet Security (CIS) has created a mapping of its 18 critical security controls to some of the common compliance frameworks. This provides helpful guidance to security professionals who are working to create and maintain compliance with the required frameworks.

A Google search on **site:cisecurity.org mapping and compliance** returns a page in which the CIS provides guidance regarding security controls that are relevant to essential industry compliance frameworks such as PCI DSS, the NIST Cybersecurity Framework, FISMA, HIPAA, GDPR, and ISO/IEC 27001. Useful links and references are provided to illustrate how the CIS controls enable compliance with the different frameworks.

In addition, members of the CIS gain access to the CIS-CAT Pro controls guidance and assessment tool that provides assistance in assessing compliance through the mappings of the CIS controls to the individual compliance frameworks.

Digital forensics and incident analysis and response

Digital Forensics

Now that you have investigated and identified valid alerts, what do you do with the evidence? The cybersecurity analyst will inevitably uncover evidence of criminal activity. In order to protect the organization and to prevent cybercrime, it is necessary to identify threat actors, report them to the appropriate authorities, and provide evidence to support prosecution. Tier 1 cybersecurity analysts are often the first to uncover wrongdoing. Cybersecurity analysts must know how to properly handle evidence and attribute it to threat actors.

Digital forensics is the recovery and investigation of information found on digital devices as it relates to criminal activity. Indicators of compromise are the evidence that a cybersecurity incident has occurred. This information could be data on storage devices, in volatile computer memory, or the traces of cybercrime that are preserved in network data, such as pcaps and logs. It is essential that all indicators of compromise be preserved for future analysis and attack attribution.

Cybercriminal activity can be broadly characterized as originating from inside of or outside of the organization. Private investigations are concerned with individuals inside the organization. These individuals could simply be behaving in ways that violate user agreements or other non-criminal conduct. When individuals are suspected of involvement in criminal activity involving the theft or destruction of intellectual property, an organization may choose to involve law enforcement authorities, in which case the investigation becomes public. Internal users could also have used the organization’s network to conduct other criminal activities that are unrelated to the organizational mission but are in violation of various legal statutes. In this case, public officials will carry out the investigation.

When an external attacker has exploited a network and stolen or altered data, evidence needs to be gathered to document the scope of the exploit. Various regulatory bodies specify a range of actions that an organization must take when various types of data have been compromised. The results of forensic investigation can help to identify the actions that need to be taken.

For example, under the US HIPAA regulations, if a data breach has occurred that involves patient information, notification of the breach must be made to the affected individuals. If the breach involves more than 500 individuals in a state or jurisdiction, the media, as well as the affected individuals, must be notified. Digital forensic investigation must be used to determine which individuals were affected, and to certify the number of affected individuals so that appropriate notification can be made in compliance with HIPAA regulations.

It is possible that the organization itself could be the subject of an investigation. Cybersecurity analysts may find themselves in direct contact with digital forensic evidence that details the conduct of members of the organization. Analysts must know the requirements regarding the preservation and handling of such evidence. Failure to do so could result in criminal penalties for the organization and even the cybersecurity analyst if the intention to destroy evidence is established.

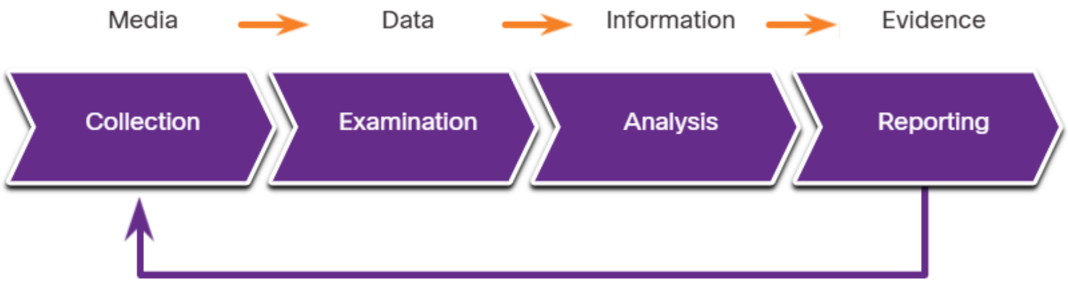
The Digital Forensics Process

It is important that an organization develop well-documented processes and procedures for digital forensic analysis. Regulatory compliance may require this documentation, and this documentation may be inspected by authorities in the event of a public investigation.

NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response is a valuable resource for organizations that require guidance in developing digital forensics plans. For example, it recommends that forensics be performed using the four-phase process.

The following describes the four basic phases of the digital evidence forensic process.

The Digital Evidence Forensic Process



Step 1. Collection: This is the identification of potential sources of forensic data and acquisition, handling, and storage of that data. This stage is critical because special care must be taken not to damage, lose, or omit important data.

Step 2. Examination: This entails assessing and extracting relevant information from the collected data. This may involve decompression or decryption of the data. Information that is irrelevant to the investigation may need to be removed. Identifying actual evidence in large collections of data can be very difficult and time-consuming.

Step 3. Analysis This entails drawing conclusions from the data. Salient features, such as people, places, times, events, and so on should be documented. This step may also involve the correlation of data from multiple sources.

Step 4. Reporting: This entails preparing and presenting information that resulted from the analysis. Reporting should be impartial and alternative explanations should be offered if appropriate. Limitations of the analysis and problems encountered should be included. Suggestions for further investigation and next steps should also be made.

Types of Evidence

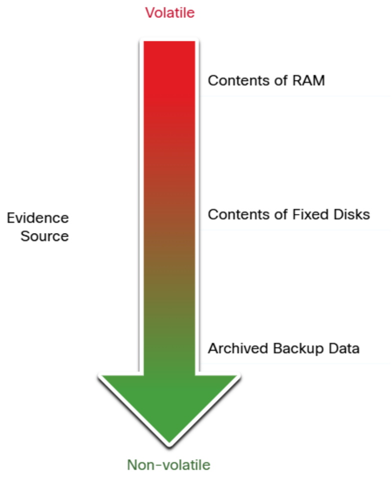
In legal proceedings, evidence is broadly classified as either direct or indirect. Direct evidence is evidence that was indisputably in the possession of the accused, or is eyewitness evidence from someone who directly observed criminal behavior. Evidence is further classified as:

- **Best evidence**: This is evidence that is in its original state. This evidence could be storage devices used by an accused, or archives of files that can be proven to be unaltered.
- **Corroborating evidence**: This is evidence that supports an assertion that is developed from best evidence.
- **Indirect evidence**: This is evidence that, in combination with other facts, establishes a hypothesis. This is also known as circumstantial evidence. For example, evidence that an individual has committed similar crimes can support the assertion that the person committed the crime of which they are accused.

Evidence Collection Order

IETF RFC 3227 provides guidelines for the collection of digital evidence. It describes an order for the collection of digital evidence based on the volatility of the data. Data stored in RAM is the most volatile, and it will be lost when the device is turned off. In addition, important data in volatile memory could be overwritten by routine machine processes. Therefore, the collection of digital evidence should begin with the most volatile evidence and proceed to the least volatile, as shown in the figure.

Evidence Collection Priority



An example of most volatile to least volatile evidence collection order is as follows:

- Memory registers, caches
- Routing table, ARP cache, process table, kernel statistics, RAM
- Temporary file systems
- Non-volatile media, fixed and removable
- Remote logging and monitoring data
- Physical interconnections and topologies
- Archival media, tape or other backups

Details of the systems from which the evidence was collected, including who has access to those systems and at what level of permissions should be recorded. Such details should include hardware and software configurations for the systems from which the data was obtained.

Chain of Custody

Although evidence may have been gathered from sources that support attribution to an accused individual, it can be argued that the evidence could have been altered or fabricated after it was collected. In order to counter this argument, a rigorous chain of custody must be defined and followed.

Chain of custody involves the collection, handling, and secure storage of evidence. Detailed records should be kept of the following:

- Who discovered and collected the evidence?
- All details about the handling of evidence including times, places, and personnel involved.
- Who has primary responsibility for the evidence, when responsibility was assigned, and when custody changed?
- Who has physical access to the evidence while it was stored? Access should be restricted to only the most essential personnel.

Data Integrity and Preservation

When collecting data, it is important that it is preserved in its original condition. Timestamping of files should be preserved. For this reason, the original evidence should be copied, and analysis should only be conducted on copies of the original. This is to avoid accidental loss or alteration of the evidence. Because timestamps may be part of the evidence, opening files from the original media should be avoided.

The process used to create copies of the evidence that is used in the investigation should be recorded. Whenever possible, the copies should be direct bit-level copies of the original storage volumes. It should be possible to compare the archived disc image and the investigated disk image to identify whether the contents of the investigated disk have been tampered with. For this reason, it is important to archive and protect the original disk to keep it in its original, untampered with, condition.

Volatile memory could contain forensic evidence, so special tools should be used to preserve that evidence before the device is shut down and evidence is lost. Users should not disconnect, unplug, or turn off infected machines unless explicitly told to do so by security personnel.

Following these processes will ensure that any evidence of wrongdoing will be preserved, and any indicators of compromise can be identified.

Attack Attribution

After the extent of the cyberattack has been assessed and evidence collected and preserved, incident response can move to identifying the source of the attack. As we know, a wide range of threat actors exist, ranging from disgruntled individuals, hackers, cybercriminals and criminal gangs, or nation states. Some criminals act from inside the network, while others can be on the other side of world. Sophistication of cybercrime varies as well. Nation states may employ large groups of highly-trained individuals to carry out an attack and hide their tracks, while other threat actors may openly brag about their criminal activities.

Threat attribution refers to the act of determining the individual, organization, or nation responsible for a successful intrusion or attack incident.

Identifying responsible threat actors should occur through the principled and systematic investigation of the evidence. While it may be useful to also speculate as to the identity of threat actors by identifying potential motivations for an incident, it is important not to let this bias the investigation. For example, attributing an attack to a commercial competitor may lead the investigation away from the possibility that a criminal gang or nation state was responsible.

In an evidence-based investigation, the incident response team correlates Tactics, Techniques, and Procedures (TTP) that were used in the incident with other known exploits. Cybercriminals, much like other criminals, have specific traits that are common to most of their crimes. Threat intelligence sources can help to map the TTP identified by an investigation to known sources of similar attacks. However, this highlights a problem with threat attribution. Evidence of cybercrime is seldom direct evidence. Identifying commonalities between TTPs for known and unknown threat actors is circumstantial evidence.

Some aspects of a threat that can aid in attribution are the location of originating hosts or domains, features of the code used in malware, the tools used, and other techniques. Sometimes, at the national security level, threats cannot be openly attributed because doing so would expose methods and capabilities that need to be protected.

For internal threats, asset management plays a major role. Uncovering the devices from which an attack was launched can lead directly to the threat actor. IP addresses, MAC addresses, and DHCP logs can help track the addresses used in the attack back to a specific device. AAA logs are very useful in this regard, as they track who accessed what network resources at what time.

The MITRE ATT&CK Framework

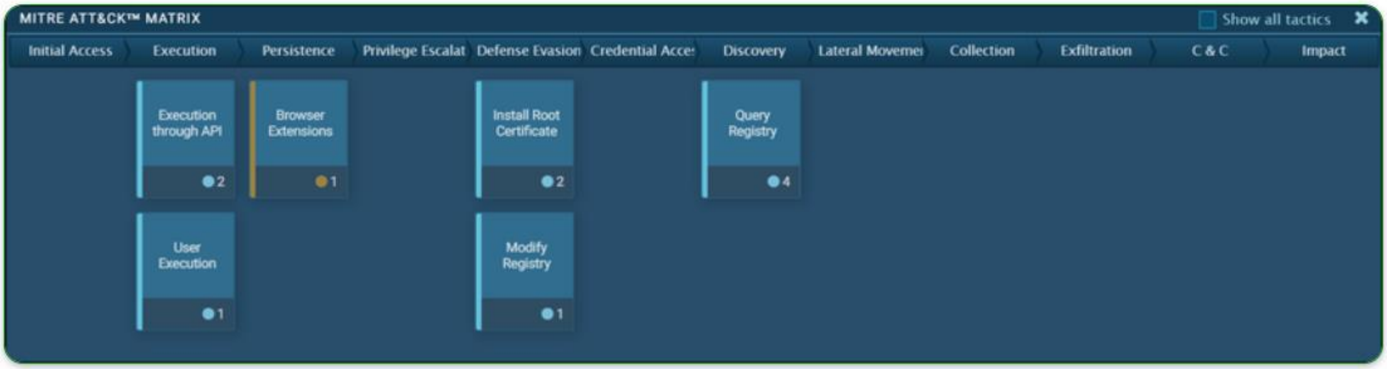
One way to attribute an attack is to model threat actor behavior. The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Framework enables the ability to detect attacker tactics, techniques, and procedures (TTP) as part of threat defense and attack attribution. This is done by mapping the steps in an attack to a matrix of generalized tactics and describing the techniques that are used in each tactic. Tactics consist of the technical goals that an attacker must accomplish in order to execute an attack and techniques are the means by which the tactics are accomplished. Finally, procedures are the specific actions taken by threat actors in the techniques that have been identified. Procedures are the documented real-world use of techniques by threat actors.

The MITRE ATT&CK Framework is a global knowledge base of threat actor behavior. It is based on observation and analysis of real-world exploits with the purpose of describing the behavior of the attacker, not the attack itself. It is designed to enable automated information sharing by defining data structures for the exchange of information between its community of users and MITRE.

The figure shows an analysis of a ransomware exploit from the excellent ANY.RUN online sandbox. The columns show the enterprise attack matrix tactics, with the techniques that are used by the malware arranged under the columns. Clicking the technique then lists details of the procedures that are used by the specific malware instance with a definition, explanation, and examples of the technique.

Note: Do an internet search on MITRE ATT&CK to learn more about this tool.

MITRE ATT&CK Matrix for a Ransomware Exploit



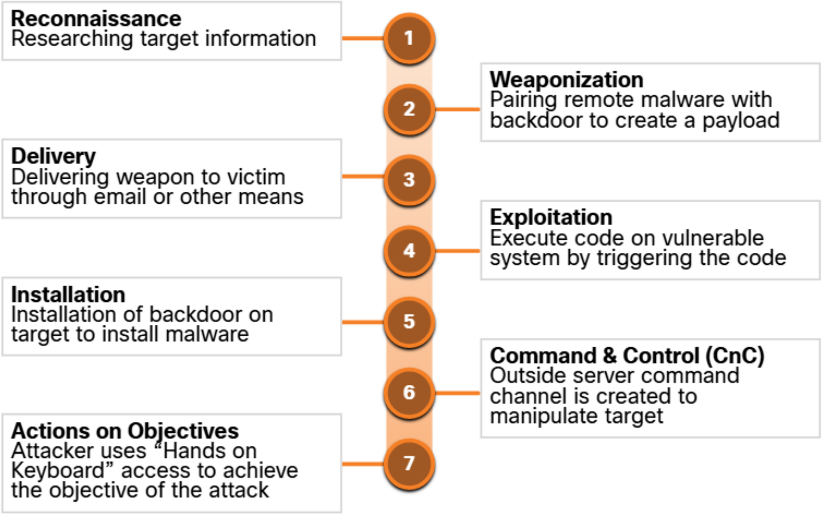
Initial Access	Execution	Persistence	Privilege Escalat	Defense Evasion	Credential Acce:	Discovery	Lateral Moveme	Collection	Exfiltration	C & C	Impact
	Execution through API ● 2	Browser Extensions ● 1		Install Root Certificate ● 2		Query Registry ● 4					
	User Execution ● 1			Modify Registry ● 1							

The Cyber Kill Chain

Steps of the Cyber Kill Chain

The Cyber Kill Chain was developed by Lockheed Martin to identify and prevent cyber intrusions. There are seven steps to the Cyber Kill Chain. Focusing on these steps helps analysts understand the techniques, tools, and procedures of threat actors. When responding to a security incident, the objective is to detect and stop the attack as early as possible in the kill chain progression. The earlier the attack is stopped; the less damage is done and the less the attacker learns about the target network.The Cyber Kill Chain specifies what an attacker must complete to accomplish their goal. The steps in the Cyber Kill Chain are shown in the figure. If the attacker is stopped at any stage, the chain of attack is broken. Breaking the chain means the defender successfully thwarted the threat actor's intrusion. Threat actors are successful only if they complete Step 7

Note: Threat actor is the term used throughout this course to refer to the party instigating the attack. However, Lockheed Martin uses the term "adversary" in its description of the Cyber Kill Chain. Therefore, the terms adversary and threat actor are used interchangeably in this topic.


Reconnaissance
Researching target information
1
Weaponization
Pairing remote malware with backdoor to create a payload
2
Delivery
Delivering weapon to victim through email or other means
3
Exploitation
Execute code on vulnerable system by triggering the code
4
Installation
Installation of backdoor on target to install malware
5
Command & Control (CnC)
Outside server command channel is created to manipulate target
6
Actions on Objectives
Attacker uses "Hands on Keyboard" access to achieve the objective of the attack
7

1. **Reconnaissance**
   - **Description:** The attacker gathers intelligence about the target's network, systems, employees, and vulnerabilities. This can include open-source intelligence (OSINT), social media profiling, domain lookup, and scanning tools.
   - **Goal:** Identify weak points and potential methods of attack without alerting the target.
2. **Weaponization**
   - **Description:** The attacker builds a deliverable malicious payload, often combining an exploit (for a known vulnerability) with a backdoor or remote access tool (RAT).

- **Goal:** Prepare malware that can be embedded in a document, script, or application.

3. **Delivery**
   - **Description:** The attacker sends the payload to the victim using methods such as phishing emails, drive-by downloads, malicious links, or infected USB devices.
   - **Goal:** Ensure the payload reaches the target environment.
4. **Exploitation**
   - **Description:** Once the victim interacts with the malicious payload, the exploit is triggered, taking advantage of a system vulnerability or user behavior.
   - **Goal:** Execute malicious code on the target system.
5. **Installation**
   - **Description:** The attacker installs malware (e.g., keyloggers, ransomware, trojans) on the victim's machine to maintain persistent access.
   - **Goal:** Establish a long-term foothold inside the target environment.
6. **Command and Control (C2)**
   - **Description:** The compromised system connects back to the attacker's infrastructure, allowing the attacker to control the system remotely and receive data.
   - **Goal:** Maintain communication with the infected machine and coordinate the next steps.
7. **Actions on Objectives**
   - **Description:** The attacker achieves their goal, which could be stealing data, disrupting operations, encrypting systems (ransomware), or espionage.
   - **Goal:** Complete the mission without being detected.

Cyber Kill Chain Summary Table

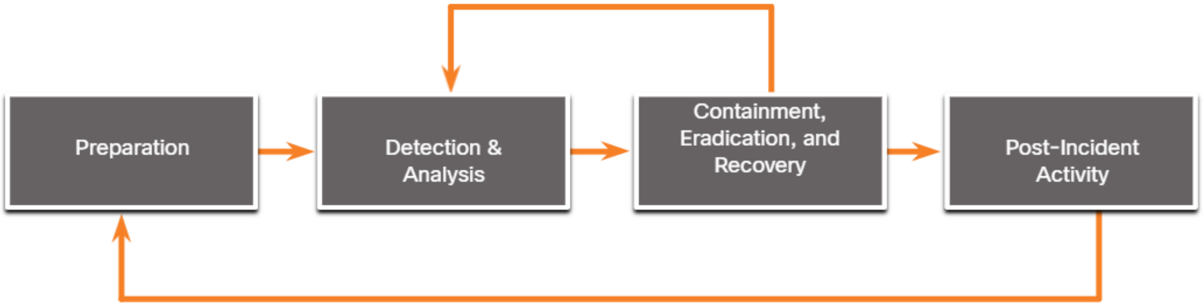
Kill Chain Stage	Attacker Tactics	Defensive Measures
Reconnaissance	- OSINT gathering- Scanning and enumeration	- Threat intelligence- Honeypots- Monitor DNS and traffic patterns
Weaponization	- Crafting malicious payloads- Embedding exploits in documents	- File analysis (sandboxing)- User education on file risks
Delivery	- Phishing emails- Malicious websites- USB drop attacks	- Email filtering- URL reputation services- Endpoint protection
Exploitation	- Triggering exploits via user action or vulnerabilities	- Patch management- Application whitelisting- Host-based intrusion prevention
Installation	- Installing trojans, RATs, or ransomware	- Anti-malware software- Application behavior monitoring- Least privilege
Command and Control	- Opening outbound C2 channels- Using DNS or HTTP for communication	- Network segmentation- Firewall rules- C2 traffic anomaly detection
Actions on Objectives	- Data exfiltration- System sabotage- Credential theft	- Data Loss Prevention (DLP)- Security information and event management (SIEM)- Incident response plans

Establishing an Incident Response Capability

Incident Response involves the methods, policies, and procedures that are used by an organization to respond to a cyberattack. The aims of incident response are to limit the impact of the attack, assess the damage caused, and implement recovery procedures. Because of the potential large-scale loss of property and revenue that can be caused by cyberattacks, it is essential that organizations create and maintain detailed incident response plans and designate personnel who are responsible for executing all aspects of that plan.

The U.S. National Institute of Standards and Technology (NIST) recommendations for incident response are detailed in their Special Publication 800-61, revision 2 entitled "Computer Security Incident Handling Guide," which is shown the figure.

NIST Incident Response Life Cycle



1. Preparation

Purpose:
To establish and maintain the tools, processes, and people necessary to handle incidents efficiently and effectively when they occur.

Detailed Activities:

- **Develop Policies & Response Plans:**
  - Define what constitutes a security incident.
  - Create and regularly update the Incident Response Plan (IRP), including roles, responsibilities, and escalation procedures.
- **Build the Incident Response Team (IRT):**
  - Assign specific roles (incident handler, forensic analyst, communications lead).
  - Include both technical and non-technical staff (e.g., legal, HR, PR).
- **Training and Awareness:**
  - Conduct regular incident response training and tabletop exercises.

    - Raise awareness among employees about how to recognize and report incidents (like phishing).
- **Provisioning Tools and Infrastructure:**
    - Deploy log management tools, Security Information and Event Management (SIEM) systems, forensic tools, and communication systems.
    - Ensure secure backups are available and accessible.
- **Establish Communication Protocols:**
    - Set up secure methods to communicate during incidents (e.g., out-of-band communication).
    - Maintain a contact list for internal teams and external partners.

2. Detection and Analysis

Purpose:
To detect potential security incidents, analyze the information, and determine the scope and impact.

Detailed Activities:

- **Monitoring Systems:**
    - Monitor logs from servers, firewalls, IDS/IPS, antivirus, and cloud systems.
    - Use automated alerting systems and correlation tools to identify unusual patterns.
- **Event and Incident Classification:**
    - Differentiate between benign events and actual incidents.
    - Classify incidents (e.g., DoS, malware infection, insider threat) and prioritize by severity and potential impact.
- **Validate and Investigate:**
    - Confirm the incident with additional evidence.
    - Capture memory, collect logs, and document affected assets and users.
- **Initial Impact Assessment:**
    - Determine the scope (systems affected, data compromised).
    - Start a chain of custody for any evidence that may be used in legal proceedings.
- **Document Everything:**
    - Time of detection, who detected it, and the timeline of all actions taken so far.

3. Containment, Eradication, and Recovery

This phase is often broken down into **three sub-phases**:

A. Containment

Purpose:
Limit the damage and prevent the spread of the incident.

- **Short-term containment:** Immediately isolate affected systems (e.g., take machines off the network).
- **Long-term containment:** Apply more permanent solutions such as disabling accounts, updating firewall rules, or segmentation.
- **Preserve evidence** before any cleanup — for forensic analysis.

B. Eradication

Purpose:
Eliminate the root cause of the incident from the environment.

- **Identify root cause:** Determine how the attacker gained access.
- **Remove malicious components:** Delete malware, disable backdoors, change passwords, patch vulnerabilities.
- **Harden systems:** Apply patches, disable unnecessary services, update configurations.

C. Recovery

Purpose:
Return affected systems to normal operations while ensuring no threats remain.

- **Restore from clean backups.**
- **Monitor systems for recurrence** (e.g., set up increased logging or alerts).
- **Perform integrity checks** on restored systems.
- **Communicate status updates** to stakeholders.

4. Post-Incident Activity (Lessons Learned)

Purpose:
To review the incident, analyze what happened, and improve the response process and security posture.

Detailed Activities:

- **Conduct a post-mortem meeting:**
    - Review the timeline of events.
    - Discuss what went well and what went wrong.
    - Identify gaps in detection, containment, or recovery.
- **Documentation:**

    - Compile a full incident report: nature of the attack, timeline, impacted systems, response actions, and outcome.
- **Update Security Measures:**
    - Apply new policies or controls based on what was learned.
    - Update training materials and IR plans.
- **Compliance and Reporting:**
    - Notify stakeholders or regulatory bodies if required.
    - Ensure logs and evidence are stored securely for future reference or legal use.

Summary Table: NIST Incident Response Life Cycle

Phase	Purpose	Key Activities
1. Preparation	Establish readiness	IR plans, training, tools, communication plans, risk assessments
2. Detection and Analysis	Identify and confirm incidents	Monitoring, incident classification, impact analysis, evidence collection
3. Containment, Eradication, and Recovery	Stop and remove threat, restore systems	Isolate systems, remove malware, recover services, monitor systems
4. Post-Incident Activity	Learn and improve	Debriefs, documentation, policy updates, lessons learned

Incident Data Collection and Retention

By having ‘lessons learned’ meetings, the collected data can be used to determine the cost of an incident for budgeting reasons, as well as to determine the effectiveness of the CSIRT, and identify possible security weaknesses throughout the system. The collected data needs to be actionable. Only collect data that can be used to define and refine the incident handling process.

A higher number of incidents handled can show that something in the incidence response methodology is not working properly and needs to be refined. It could also show incompetence in the CSIRT. A lower number of incidents might show that network and host security has been improved. It could also show a lack of incident detection. Separate incident counts for each type of incident may be more effective at showing strengths and weakness of the CSIRT and implemented security measures. These subcategories can help to target where a weakness resides, rather than whether there is a weakness at all.

The time of each incident provides insight into the total amount of labor used and the total time of each phase of the incident response process. The time until the first response is also important, as well as how long it took to report the incident and escalate it beyond the organization, if necessary.

It is important to perform an objective assessment of each incident. The response to an incident that has been resolved can be analyzed to determine how effective it was. NIST Special

Publication 800-61 provides the following examples of activities that are performed during an objective assessment of an incident:

- Reviewing logs, forms, reports, and other incident documentation for adherence to established incident response policies and procedures.
- Identifying which precursors and indicators of the incident were recorded to determine how effectively the incident was logged and identified.
- Determining if the incident caused damage before it was detected.
- Determining if the actual cause of the incident was identified, and identifying the vector of attack, the vulnerabilities exploited, and the characteristics of the targeted or victimized systems, networks, and applications.
- Determining if the incident is a recurrence of a previous incident.
- Calculating the estimated monetary damage from the incident (e.g., information and critical business processes negatively affected by the incident).
- Measuring the difference between the initial impact assessment and the final impact assessment.
- Identifying which measures, if any, could have prevented the incident.
- Subjective assessment of each incident requires that incident response team members assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked, in order to determine if the owner thinks the incident was handled efficiently and if the outcome was satisfactory.

There should be a policy in place in each organization that outlines how long evidence of an incident is retained. Evidence is often retained for many months or many years after an incident has taken place. In some cases, compliance regulations may mandate the retention period. These are some of the determining factors for evidence retention:

Disaster Recovery Plan

An organization puts its Disaster Recovery Plan (DRP) into action while the disaster is ongoing and employees are scrambling to ensure critical systems are online. The DRP includes the activities the organization takes to assess, salvage, repair and restore damaged facilities or assets. To create the DRP, answer the following questions:

- Who is responsible for this process?
- What does the individual need to perform the process?
- Where does the individual perform this process?
- What is the process?
- Why is the process critical?
  "A DRP needs to identify which processes in the organization are the most critical. During the recovery process, the organization should prioritize the restoration of these mission critical systems."