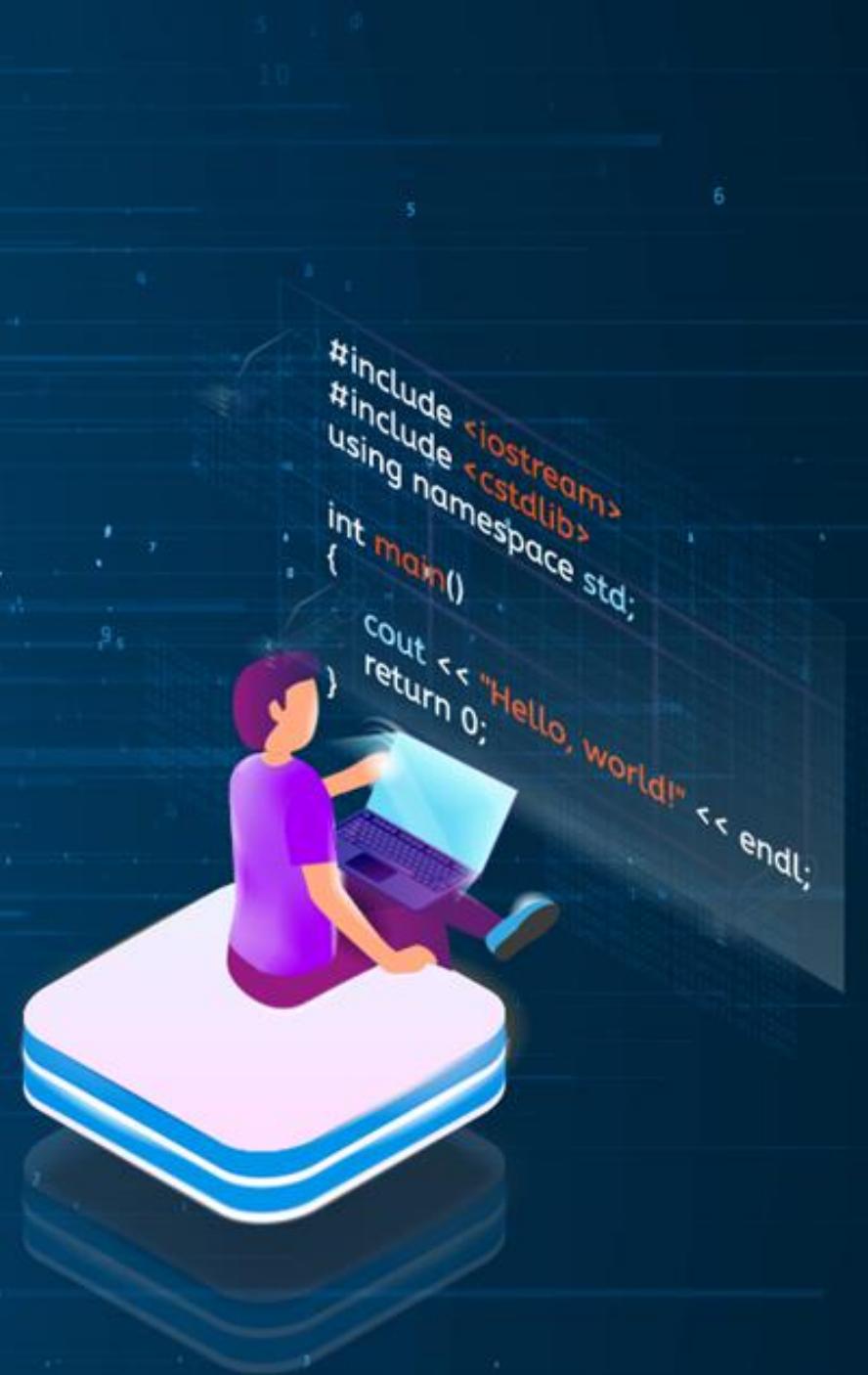




CompTIA Security +

Domain 04: Security Operations



```
#include <iostream>
#include <cstdlib>
using namespace std;

int main()
{
    cout << "Hello, world!" << endl;
    return 0;
}
```

Learning Objectives

By the end of this lesson, you will be able to:

- Apply Common security techniques to computing resources
- Understand the security implications of proper hardware, software, and data asset management
- Understand Vulnerability assessment and Penetration testing process
- Understanding Security Alerting and Monitoring Concepts and Tools
- Understanding Security technologies for protection of enterprise
- Explain and understand Identity access management



Learning Objectives

By the end of this lesson, you will be able to:

- Understand the importance of automation and orchestration related to operation
- Understand incident management
- Understanding data sources to support an investigation

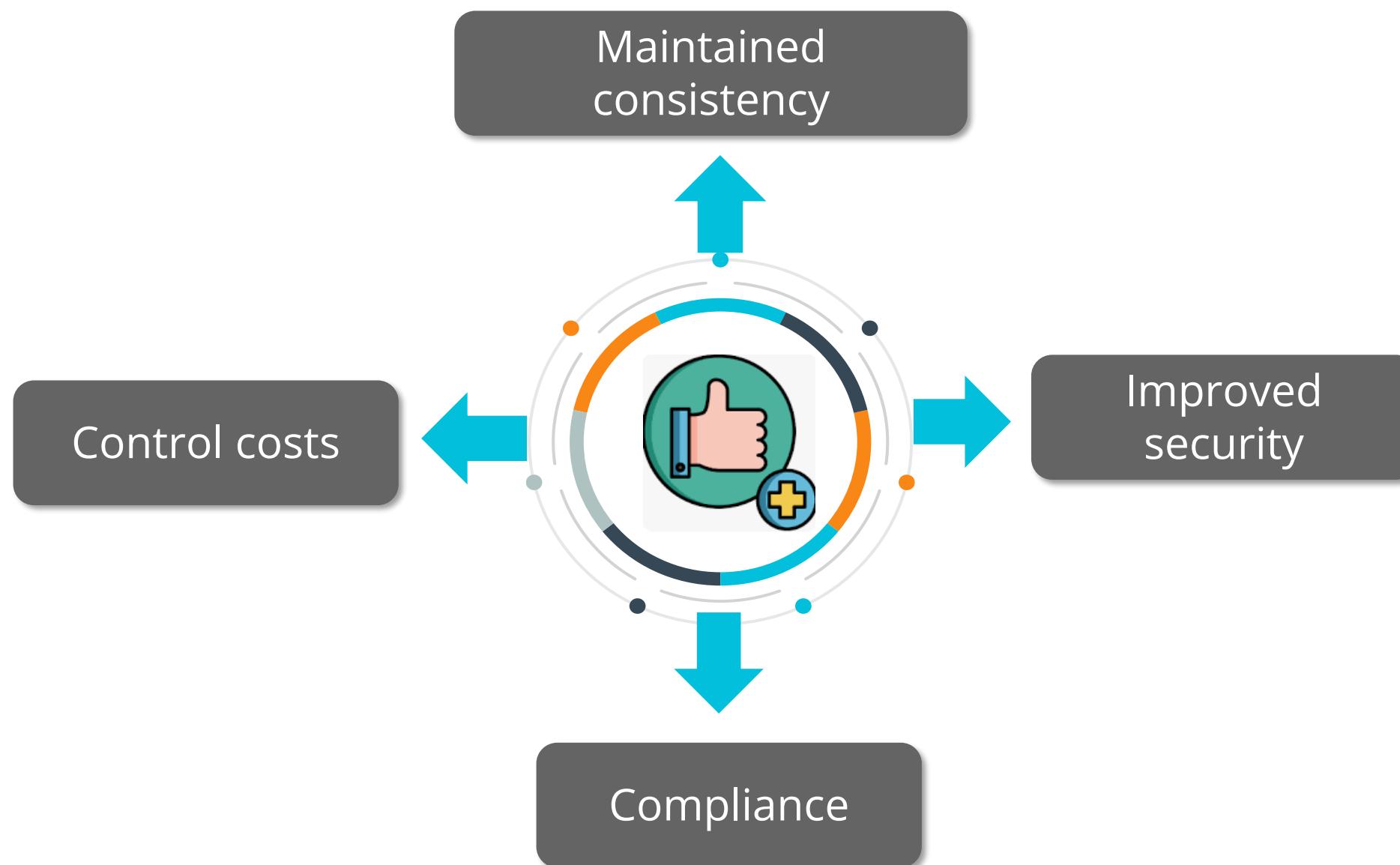


TECHNOLOGY

Establishing Baselines

Baseline

A security baseline is a predefined set of configurations and best practices meticulously designed to create a resilient and secure foundation for computing resources. Key benefits of implementing secure baselines include:



- Implemented secure baselines offer a reliable starting point to harden targets against potential vulnerabilities.
- A security baseline is a defined standard representing a secure and approved configuration or state, serving as a benchmark to compare the current system state.

Types of Baselines

Infrastructure baseline

This is a snapshot of your infrastructure's configuration, including virtual machines, storage buckets, networking settings, and security policies.

Security baseline

This defines the minimum security requirements for your resources. It helps you identify and address potential security risks and ensure compliance with relevant regulations.

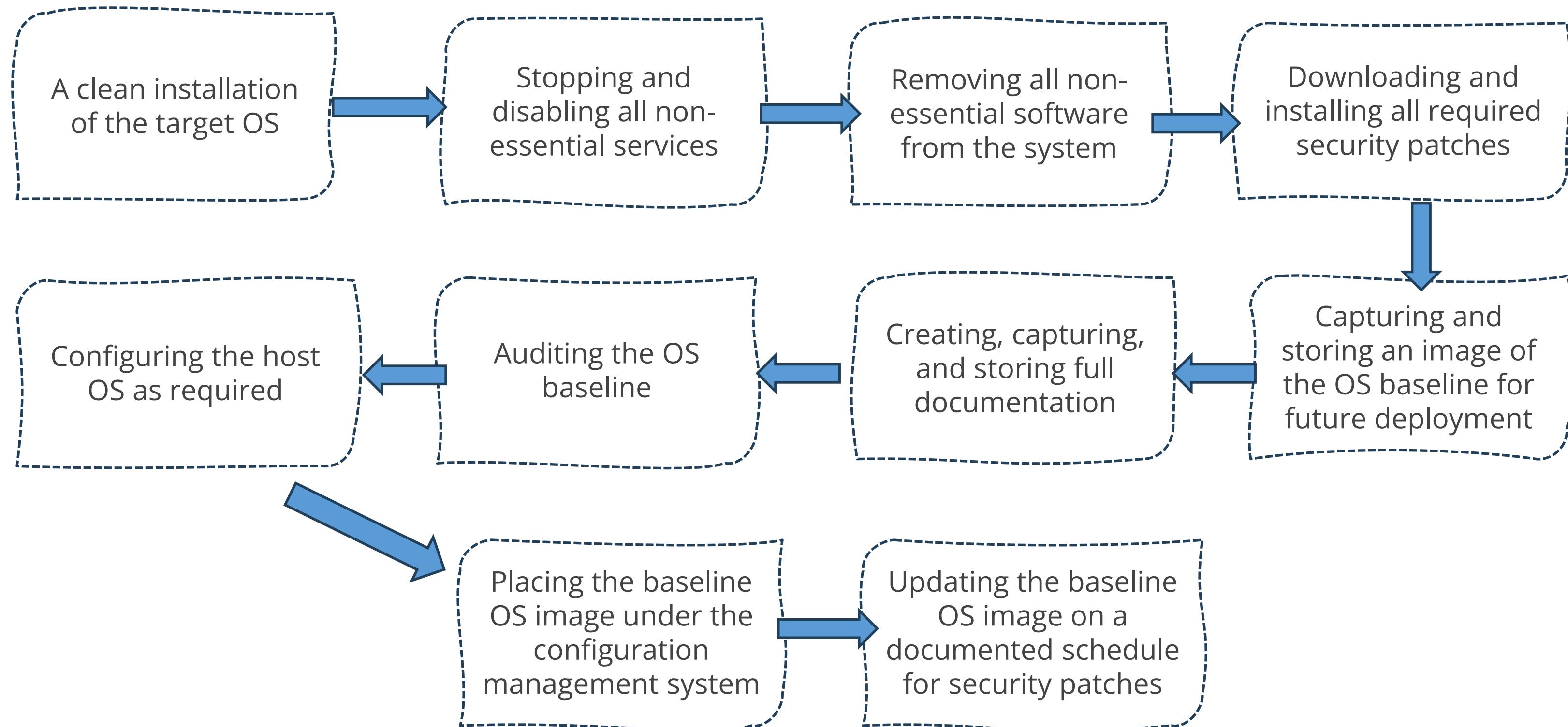
Performance baseline

This measures the typical performance of your applications and infrastructure. You can use this to identify performance bottlenecks, track trends, and measure the impact of changes.

Network baseline

A network baseline is a snapshot of a network's normal operating conditions, including its configuration, performance metrics, and traffic patterns.

Baseline Process



Phases of Establishing Baselines



1



2



3

Establishing baseline

- Center for internet security
- Security technical implementation guide

Deploying baselines

- Microsoft group policy
- Puppet forge

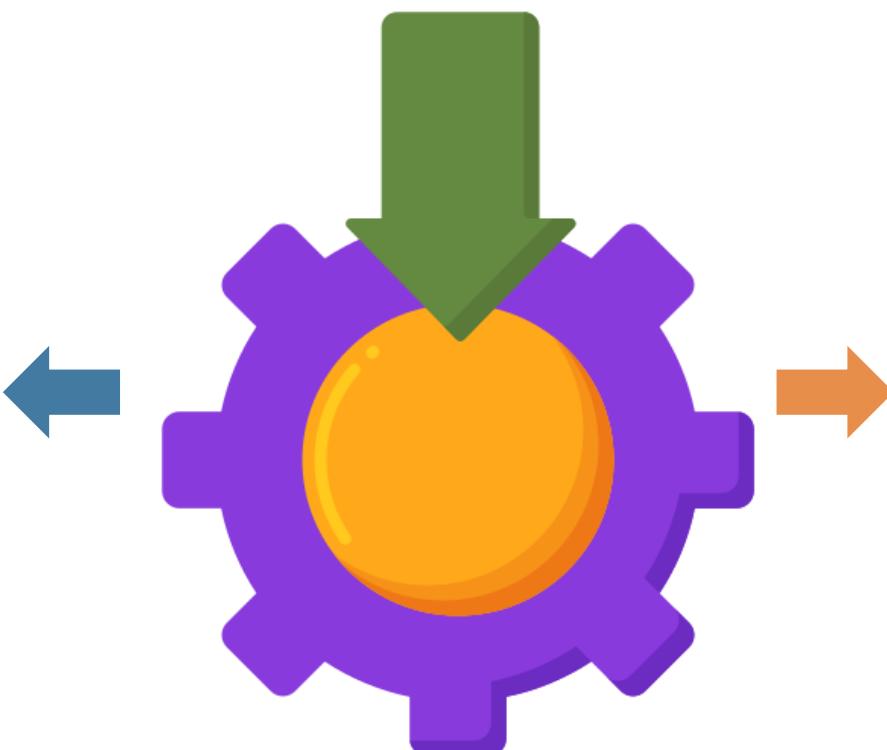
Maintaining baselines

- SCAP compliance checker
- CIS configuration assessment tool

Establishing Baselines

CIS benchmarks

- Widely recognized and respected cybersecurity standards and best practices
- Serve as a foundational security baseline for various technologies, including operating systems, network devices, and applications
- Strengthen an organization's security posture by reducing vulnerabilities



Security Technical Implementation Guide (STIG)

- Comprehensive repository of cybersecurity guidelines and best practices curated by the United States Department of Defense (DoD) Enhances the security posture of DoD information systems and networks
- Implementing STIG recommendations involves a systematic approach to assess systems and networks against the guidelines, identifying vulnerabilities

Deploying Baselines

To effectively deploy security baselines, the following methods are used:

Microsoft group policy

- Feature in Microsoft Windows Server environments for managing configurations for users and computers in an Active Directory domain
- Sets up consistent settings for many devices and users across a network

Puppet

- Versatile platform-agnostic solution providing a repository of pre-built modules and configurations
- Deploys security baselines across a range of operating systems, including Windows, Linux, and macOS
- Flexibility makes it a favored choice for heterogeneous environments

Maintaining Baselines

To ensure security baselines are maintained, the following tools are essential:

SCAP compliance checker

- The Security Content Automation Protocol (SCAP) is a standardized framework for maintaining system security
- Operates by comparing a system's security settings against a predefined checklist of security requirements
- Generates reports highlighting areas of non-compliance for swift corrective actions

CIS configuration assessment tool

- CIS-CAT is designed to evaluate systems and applications against CIS benchmarks curated by the Center for Internet Security (CIS)
- These benchmarks represent a gold standard for secure configurations and best practices across various technologies, from operating systems to web browsers

TECHNOLOGY

Hardening of Devices

Hardening Targets

Hardening your computing infrastructure involves fortifying your IT systems to make them more resistant to cyberattacks.

Core aspects

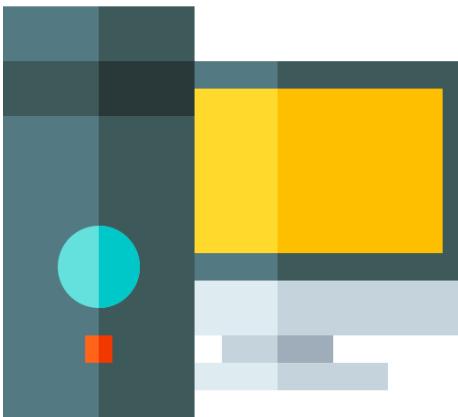
- Proactively reducing vulnerabilities, mitigating risks, and bolstering an organization's overall security posture
- Fortifying the security of devices and systems to protect against potential threats and maintain operational continuity



Technologies That Require Hardening



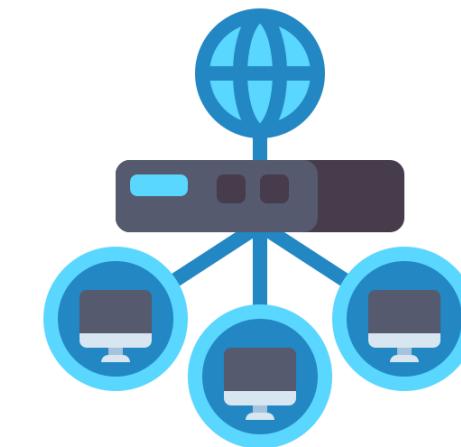
Mobile devices



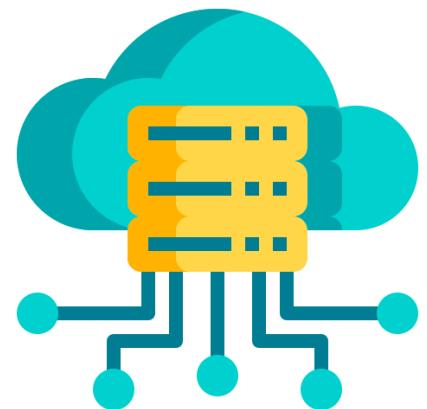
Workstations



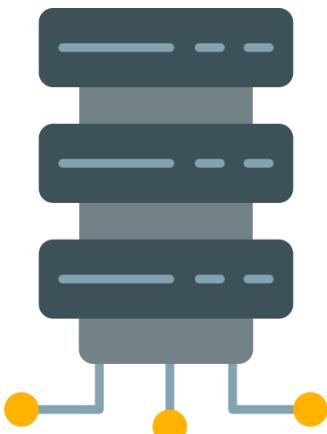
Switches



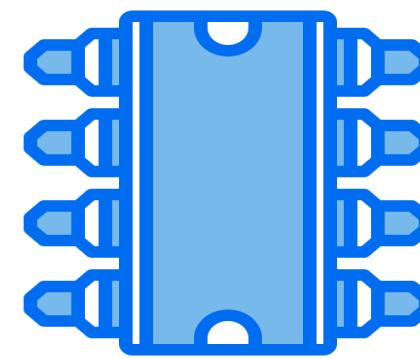
Routers



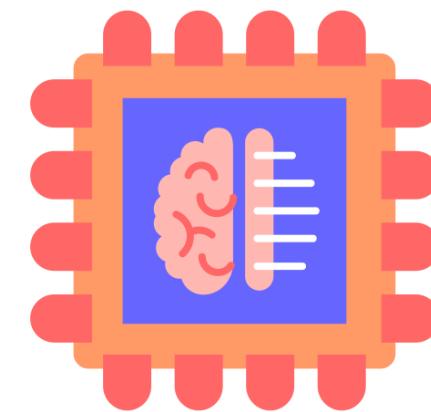
Cloud infrastructure



Servers



Industrial control system

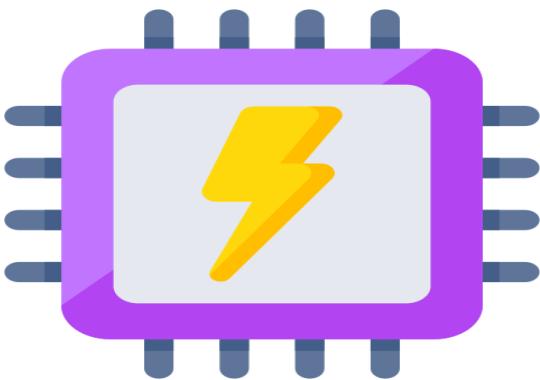


Embedded system

Technologies That Require Hardening



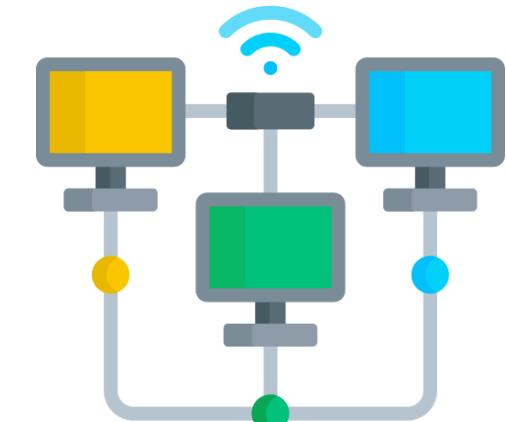
IoT devices



Real-time
operating system



Wireless access
points



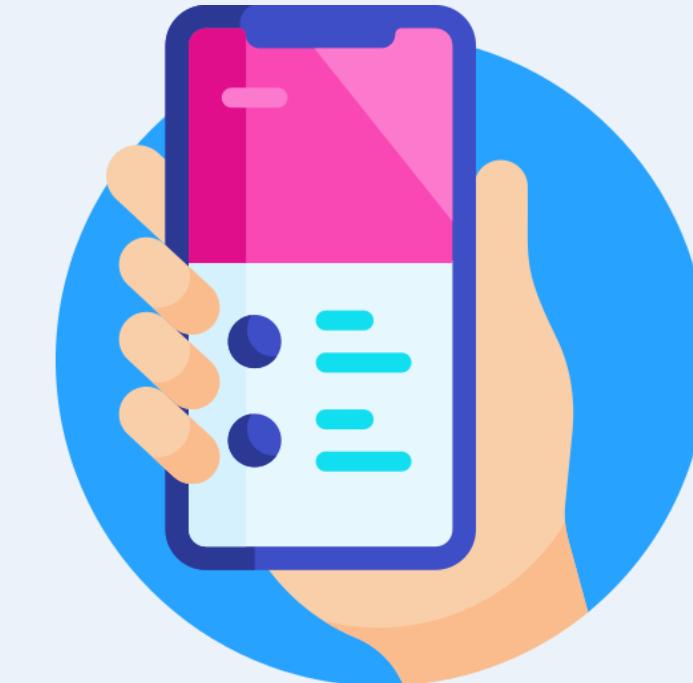
Wired
infrastructure

Mobile Hardening

This involves securing mobile devices and applications to protect against threats like malware, data breaches, and unauthorized access.

Key aspects include:

- Securing mobile devices and applications against threats like malware, data breaches, and unauthorized access
- Enhancing the security of mobile phones to protect sensitive information



Mobile Hardening

To effectively secure mobile devices, implement the following key controls:

Ensure apps are downloaded from trusted sources to minimize the risk of malware

Check and limit the permissions apps request to protect sensitive data

Remove or disable apps that are no longer in use to reduce potential vulnerabilities

Use encryption to protect the data stored on your device

Implement strong authentication methods such as biometrics or two-factor authentication

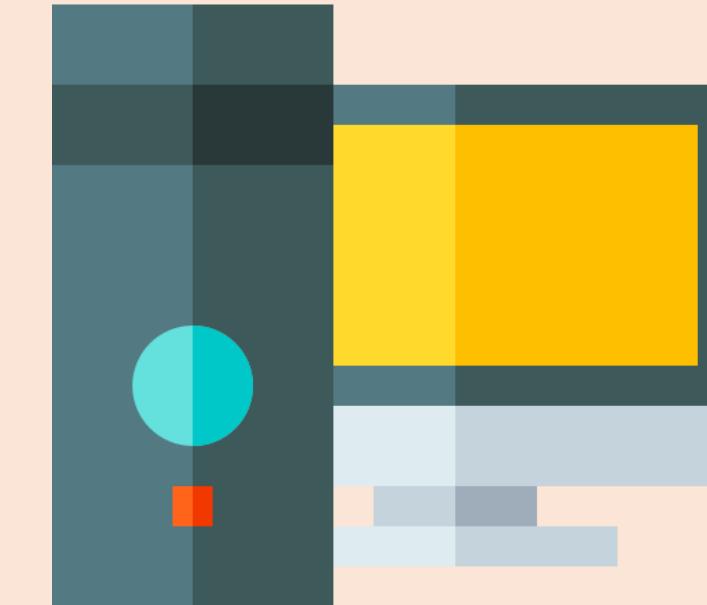
Regularly back up your data to ensure it can be restored in case of loss or damage

Workstation Hardening

It safeguards individual computers (desktops and laptops) against potential threats.

Key aspects include:

- Configuring the operating system, applications, and network settings to minimize vulnerabilities and protect sensitive data



Workstation Hardening

Essential steps to harden workstations include:

-  **Minimize attack surface:** Remove unnecessary software, services, features, and startup programs
-  **Enforce strong passwords:** Implement complex passwords and require regular password changes
-  **Patch management:** Configure automatic updates for your operating system and applications to ensure the latest security patches are applied promptly
-  **Principle of least privilege:** Grant users only the minimum level of access required for their tasks, reducing potential damage if an account is compromised
-  **Secure configuration:** Follow best practice guidelines like CIS Benchmarks to configure your OS securely

Switch Hardening

It involves configuring network switches to minimize vulnerabilities and protect against unauthorized access.

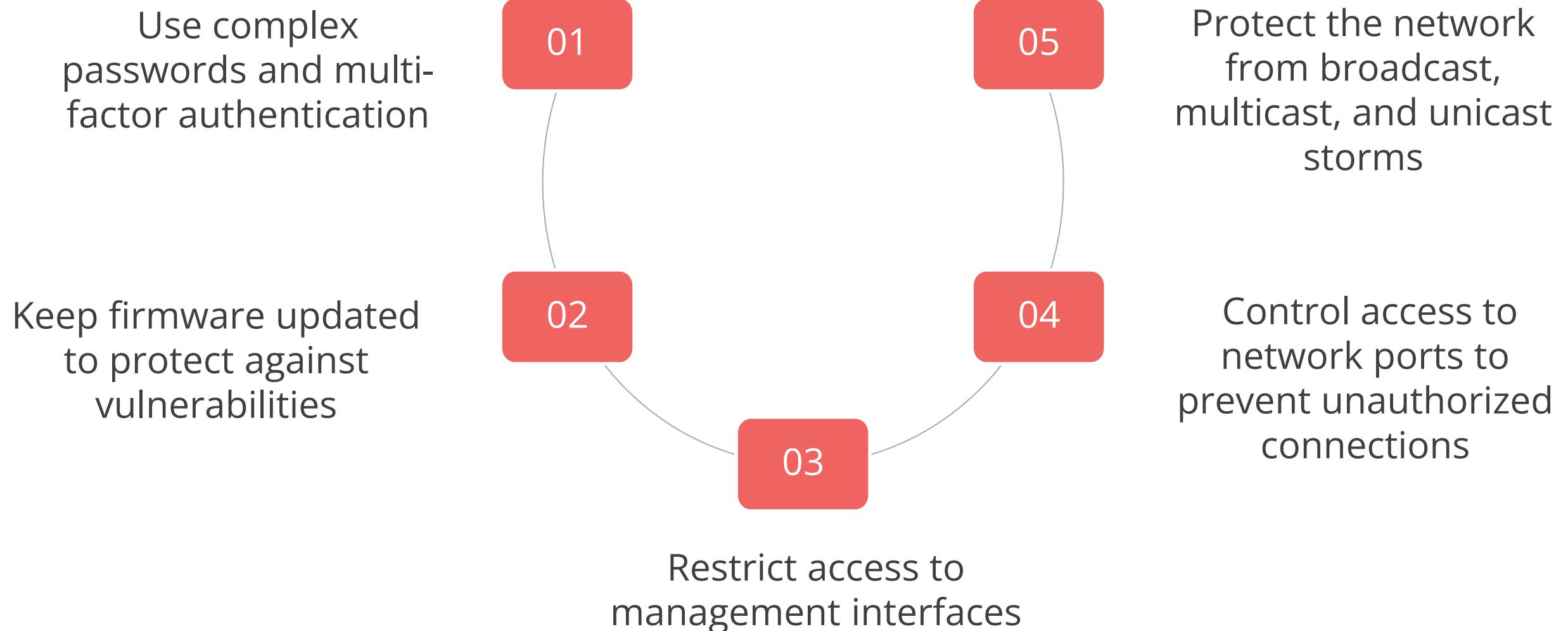
Key aspects include:

- A switch connects multiple computers and other devices within a local area network (LAN)
- Implementing security measures to prevent unauthorized access, data breaches, and other cyberattacks



Switch Hardening

Essential steps for switch hardening include:

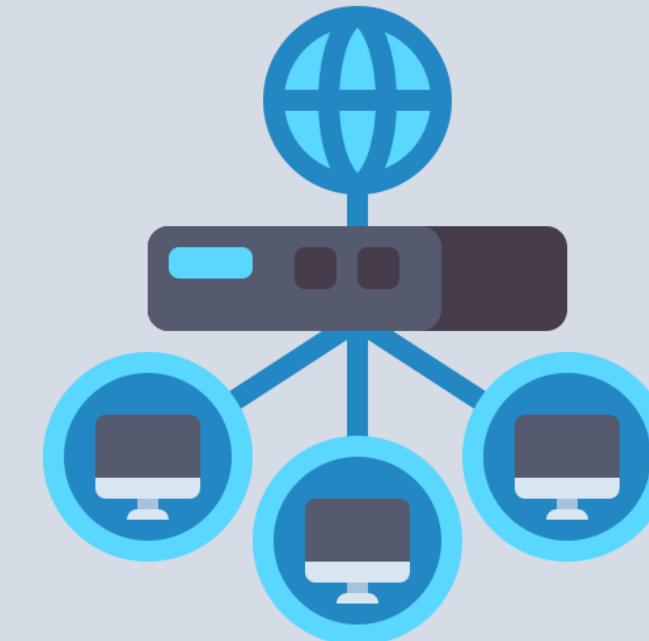


Router Hardening

It is a process of securing network routers against potential vulnerabilities and attacks.

Key aspects include:

- A router is a networking device that forwards data packets between computer networks
- Implementing security measures to protect the router's configuration, data, and services
- Enhancing the security of your network to protect against a wide range of threats



Router Hardening

Essential steps for router hardening include:

- 01 Prevent unauthorized access with complex passwords and multi-factor authentication
- 02 Reduce potential attack vectors by turning off unnecessary features
- 03 Protect against vulnerabilities by keeping firmware up to date
- 04 Secure the router physically to prevent tampering
- 05 Detect and respond to suspicious activities through continuous monitoring and logging

Cloud Hardening

This involves implementing security measures to protect cloud-based systems and applications from vulnerabilities and attacks.

Key aspects include:

- **Securing cloud-based systems and applications:** Implement robust security protocols to reduce vulnerabilities and protect against attacks
- **Protecting data, applications, and infrastructure:** Ensure the confidentiality, integrity, and availability of resources within the cloud environment through comprehensive security measures



Cloud Hardening

Implementing effective cloud hardening controls involves the following measures:

Ensure that only authorized users have access to cloud resources through robust identity and access management practices

Protect sensitive information by encrypting it both when stored and during transmission

Regularly apply security patches to all cloud resources to mitigate vulnerabilities

Implement stringent access controls for management consoles to prevent unauthorized access

Perform continuous security assessments and penetration testing to identify and address potential security weaknesses

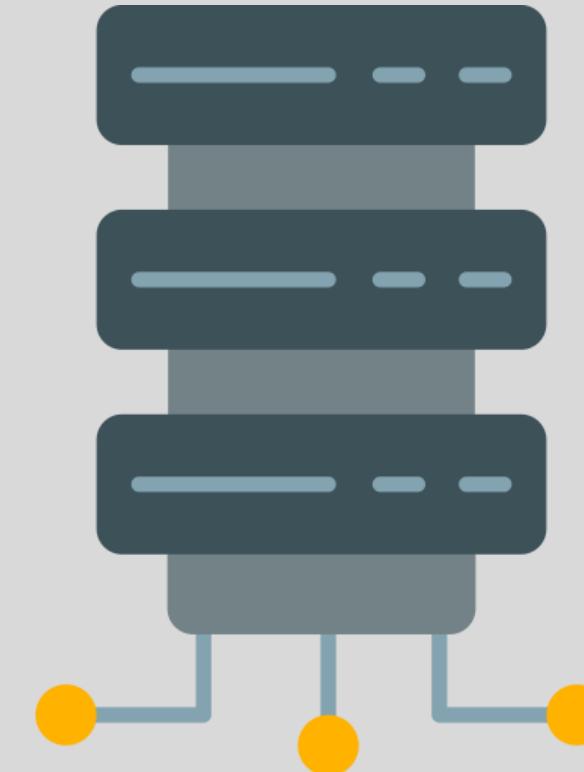
Develop and maintain a comprehensive disaster recovery plan to ensure business continuity in case of a security incident

Server Hardening

It involves securing a server, which is a computer program or device that provides functionality for other programs or devices (clients), to reduce its vulnerability to attacks.

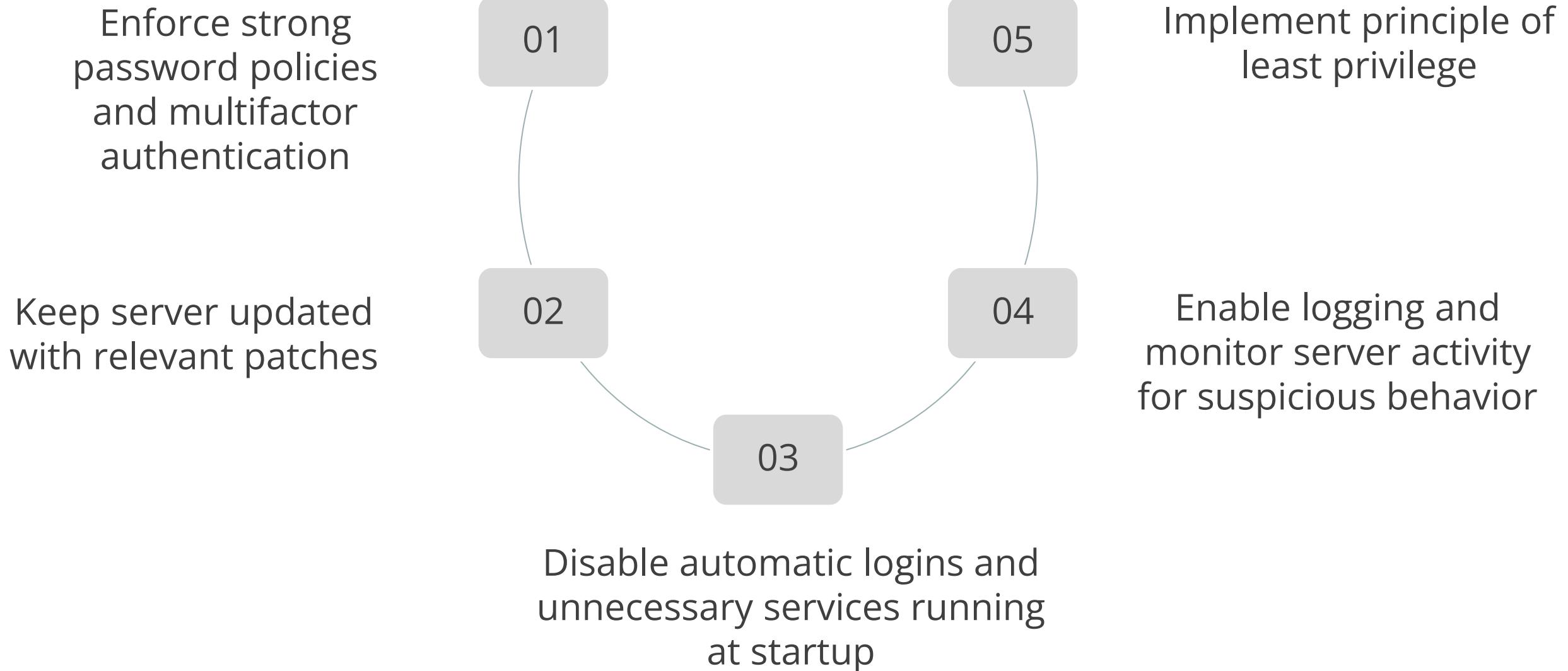
Key aspects include:

- Implementing security measures to protect the server's data, applications, and operating system
- Reducing the risk of cyberattacks and safeguarding valuable assets



Server Hardening

Implementing effective server hardening controls involves the following measures:

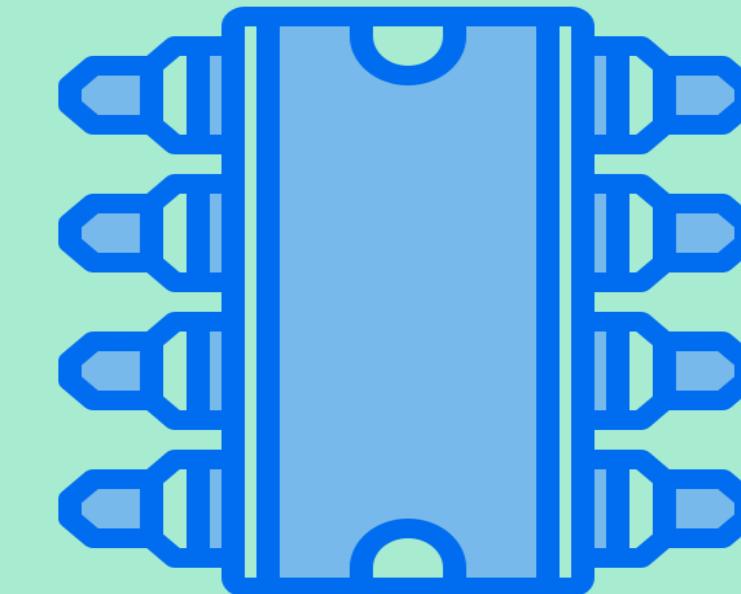


ICS Hardening

ICS hardening refers to the process of securing Industrial Control Systems (ICS) to protect them from cyberattacks. These systems often control critical infrastructure, making their security paramount.

Key aspects include:

- Securing ICS that control critical infrastructure such as power plants, water treatment facilities, and manufacturing processes
- Implementing security measures to protect against cyber threats and ensure the safe and reliable operation of critical systems



ICS Hardening

Implementing effective ICS hardening controls involves the following measures:

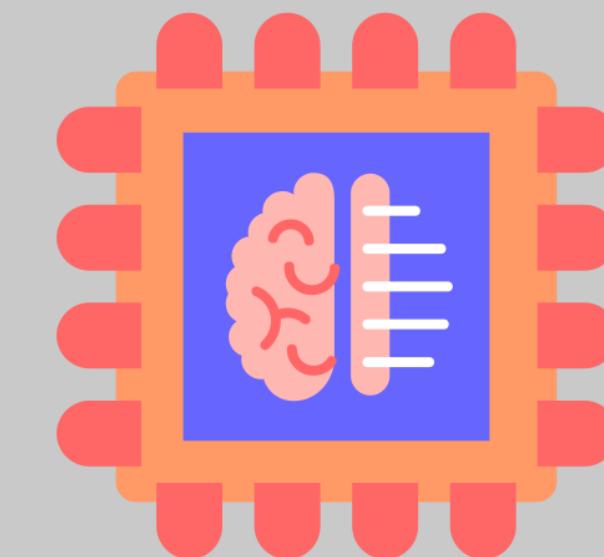
- 01 Establish a strong security perimeter around the ICS network
- 02 Implement network segmentation within the ICS itself to further isolate critical control systems
- 03 Apply rigorous patch management practices to keep ICS devices updated with the latest security fixes
- 04 Develop and enforce a baseline configuration for all ICS devices
- 05 Implement a strict change management process to track and approve any modifications to the ICS environment

Embedded System Hardening

It involves securing specialized computer systems designed for specific functions within larger mechanical or electrical systems against cyber threats.

Key aspects include:

- **Unique approaches required:** Due to their limited resources and specific functionalities, embedded systems need unique security approaches compared to traditional IT systems
- **Benefits:** Implementing these measures enhances security and protects critical infrastructure



Embedded System Hardening

Implementing effective embedded system hardening controls involves the following measures:



Coding standards: Enforce secure coding practices to minimize vulnerabilities introduced during development



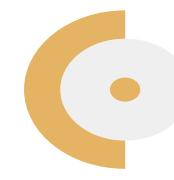
Static code analysis: Utilize static code analysis tools to identify potential vulnerabilities and coding errors early in the development process



Essential functionality: Include only the necessary code and libraries for the embedded system's core operation to reduce the attack surface



Secure boot: Implement secure boot procedures to verify the integrity of firmware before execution, preventing unauthorized code from loading



Code security: Use secure coding practices and code scanning tools to identify and eliminate vulnerabilities in the embedded software

IoT Hardening

It involves securing Internet of Things (IoT) devices and their infrastructure to protect data and maintain system integrity. IoT refers to the network of physical devices, vehicles, home appliances, and other items that connect and exchange data.

Key aspects include:

- **Securing IoT devices:** Implementing security measures to protect these devices from cyber threats
- **Maintaining system integrity:** Ensuring the overall security and reliability of the IoT infrastructure



IoT Hardening

To effectively secure IoT devices and their infrastructure, implement the following key controls:

Reduce the number of entry points for potential attackers by disabling unnecessary features and services

Ensure devices boot only with verified and trusted software to prevent unauthorized code execution

Implement strong authentication and authorization mechanisms to restrict access to IoT devices

Employ encryption and secure communication protocols to protect data in transit

Perform vulnerability assessments and penetration testing to identify and fix security weaknesses

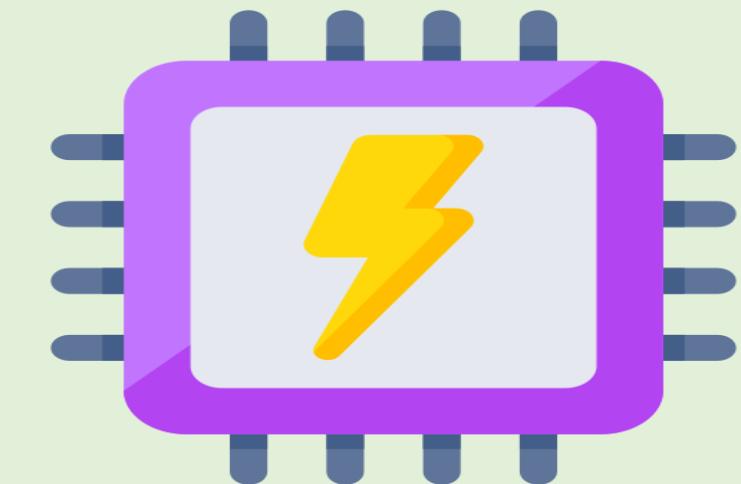
Regularly apply updates and security patches to protect against known vulnerabilities

RTOS Hardening

RTOS (Real-Time Operating System) hardening involves securing these systems designed for tasks with strict time constraints to protect against cyberattacks and maintain reliability.

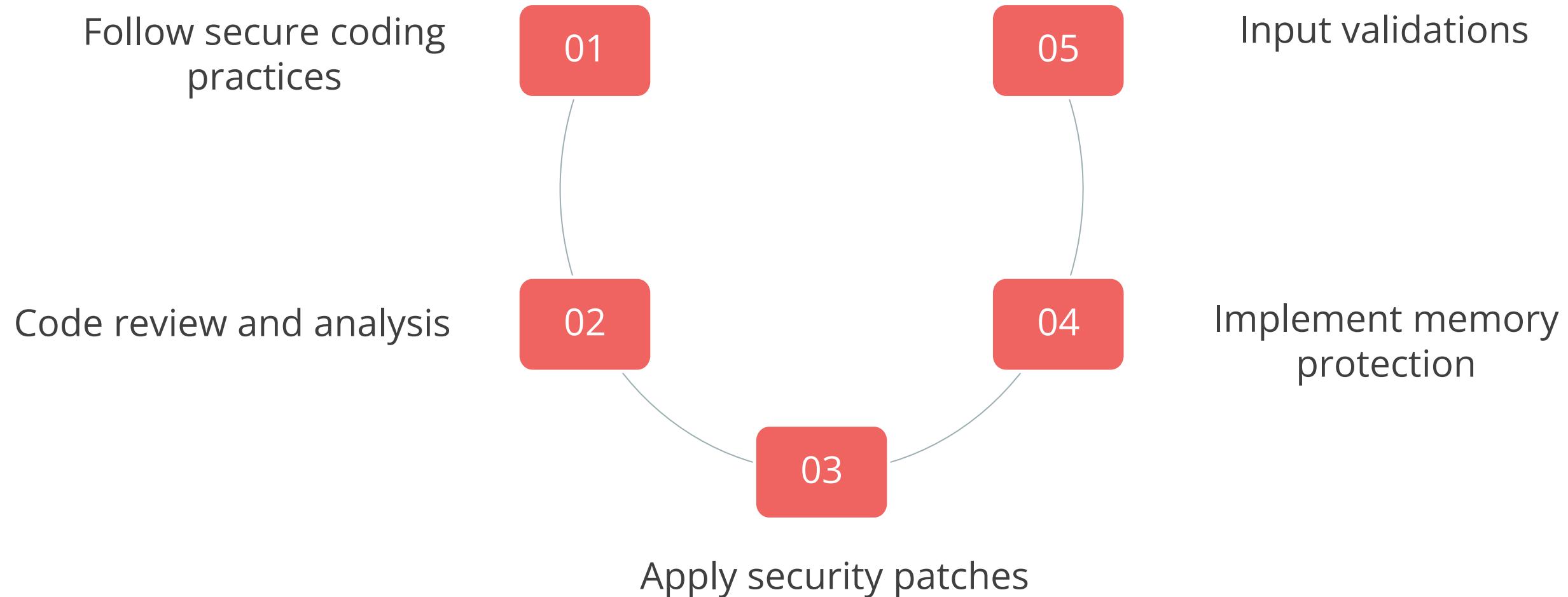
Key aspects include:

- **Specialization:** Unlike general-purpose operating systems like Windows or macOS, RTOS is specialized for real-time tasks
- **Importance:** Securing embedded systems that rely on RTOS is essential for their operation and protection against cyber threats



RTOS Hardening

To effectively secure RTOS (Real-Time Operating Systems), implement the following key controls:

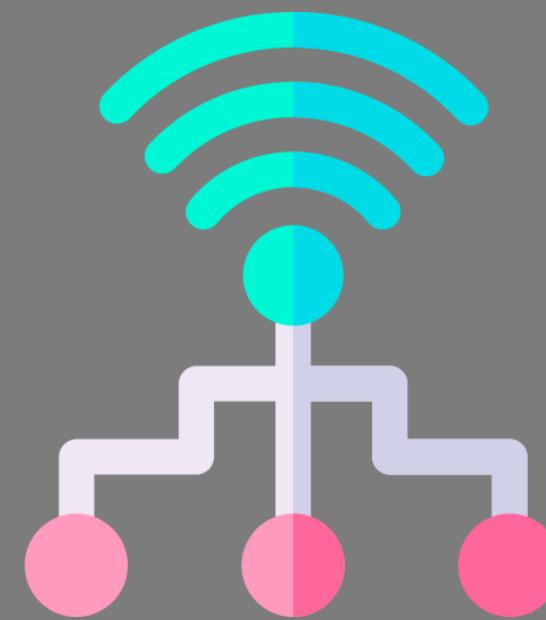


Wireless Hardening

It involves securing wireless networks that transmit information without physical cables to protect against unauthorized access, data breaches, and other cyber threats.

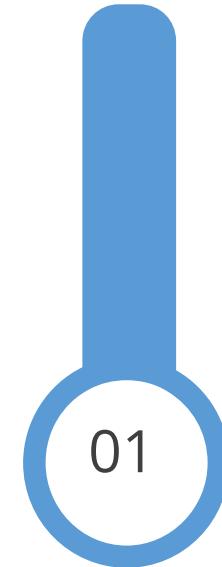
Key aspects include:

- **Importance:** Protects wireless networks from unauthorized access, data breaches, and other cyber threats

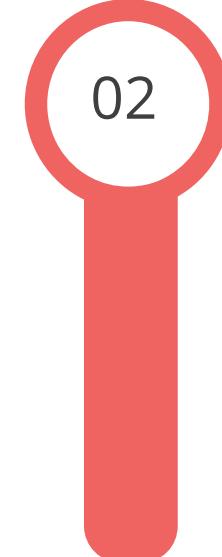


Wireless Hardening

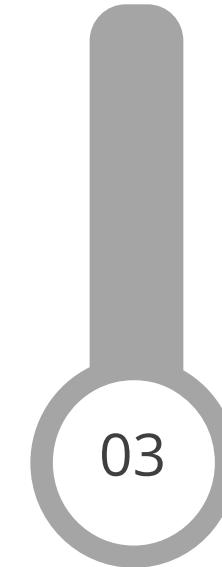
To secure wireless networks, implement the following key controls:



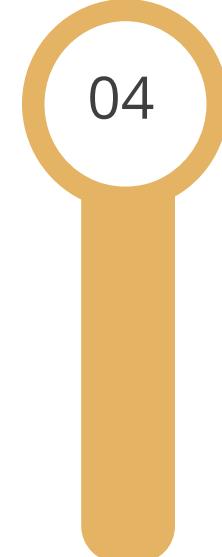
Ensure your network name (SSID) does not reveal sensitive information



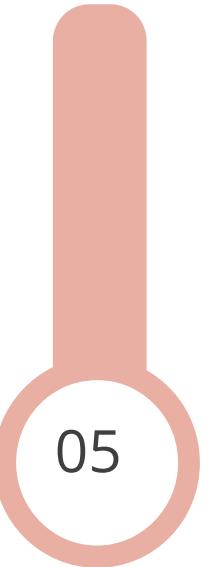
Use robust methods to authenticate users and encrypt data



Limit network access to approved devices



Regularly update firmware to protect against vulnerabilities



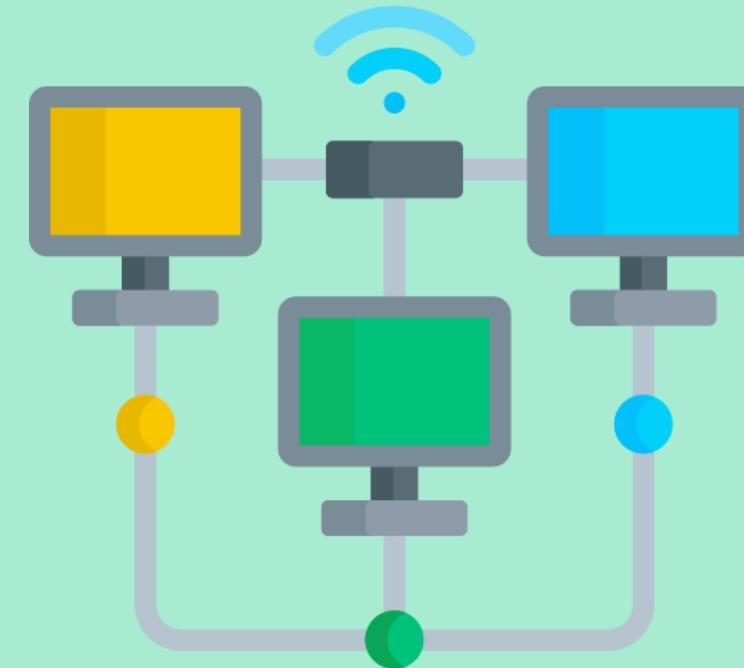
Restrict physical access to network hardware

Network Hardening

Network hardening involves securing a network, which is a group of interconnected devices that share resources and communicate, against unauthorized access and cyberattacks.

Key aspects include:

- **Protecting resources:** Safeguarding the data and devices on the network
- **Preventing cyberattacks:** Implementing measures to defend against malicious activities



Network Hardening

To effectively secure a network, implement the following key controls:

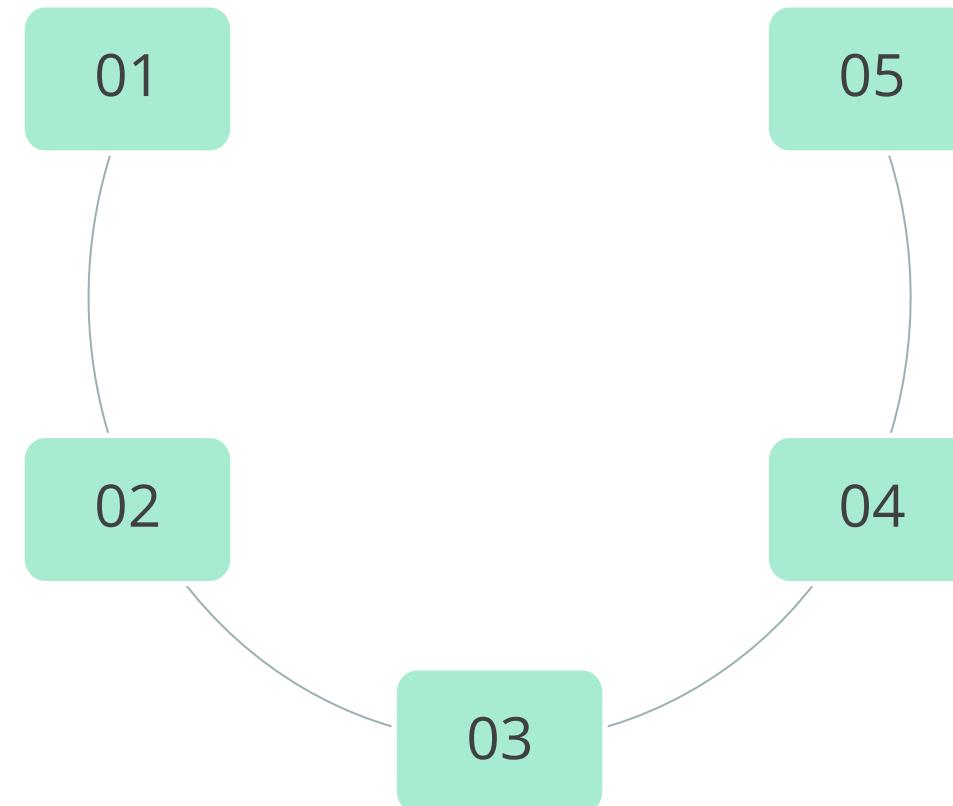
Divide the network into segments to limit the spread of potential threats

Use robust authentication methods to verify the identity of users and devices

Grant users and devices only the minimum access necessary for their tasks

Continuously monitor network traffic to detect and respond to suspicious activities

Regularly identify, assess, and remediate network vulnerabilities



TECHNOLOGY

Wireless Technologies

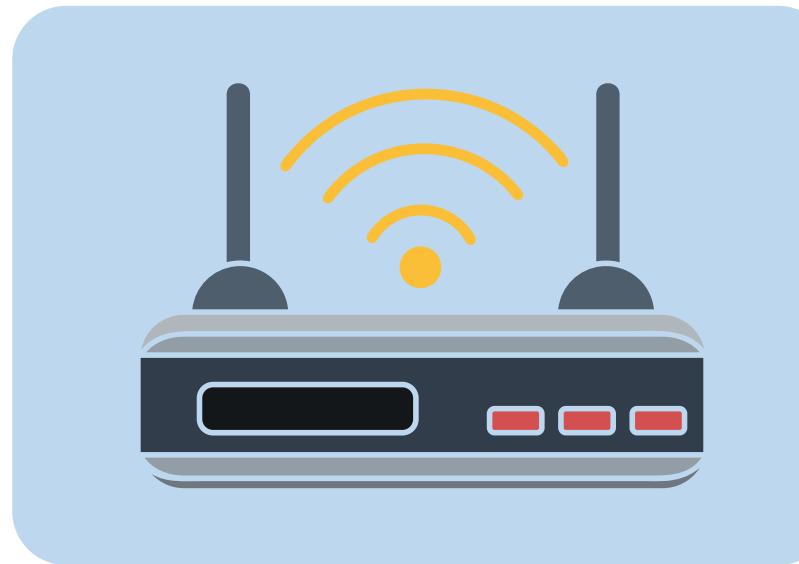
Wireless Technologies

Wireless technology is the fastest-growing area of network connectivity.

The various types of wireless technologies are given below.



Wireless Standards



WLAN Operational Modes

Wireless Technologies

Wireless Network

- A wireless network is a computer network that uses wireless data connections between network nodes
- It is based on 802.11 Standard .
- It is the fastest-growing area of network connectivity.
- In a wireless network , data are carried by electrical wave from one node to another

Wireless Access Point

- In computer networking, a wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows a Wi-Fi device to connect to a wired network.

Wireless Standards

These are essential guidelines and specifications that ensure the interoperability and reliability of wireless communication technologies.

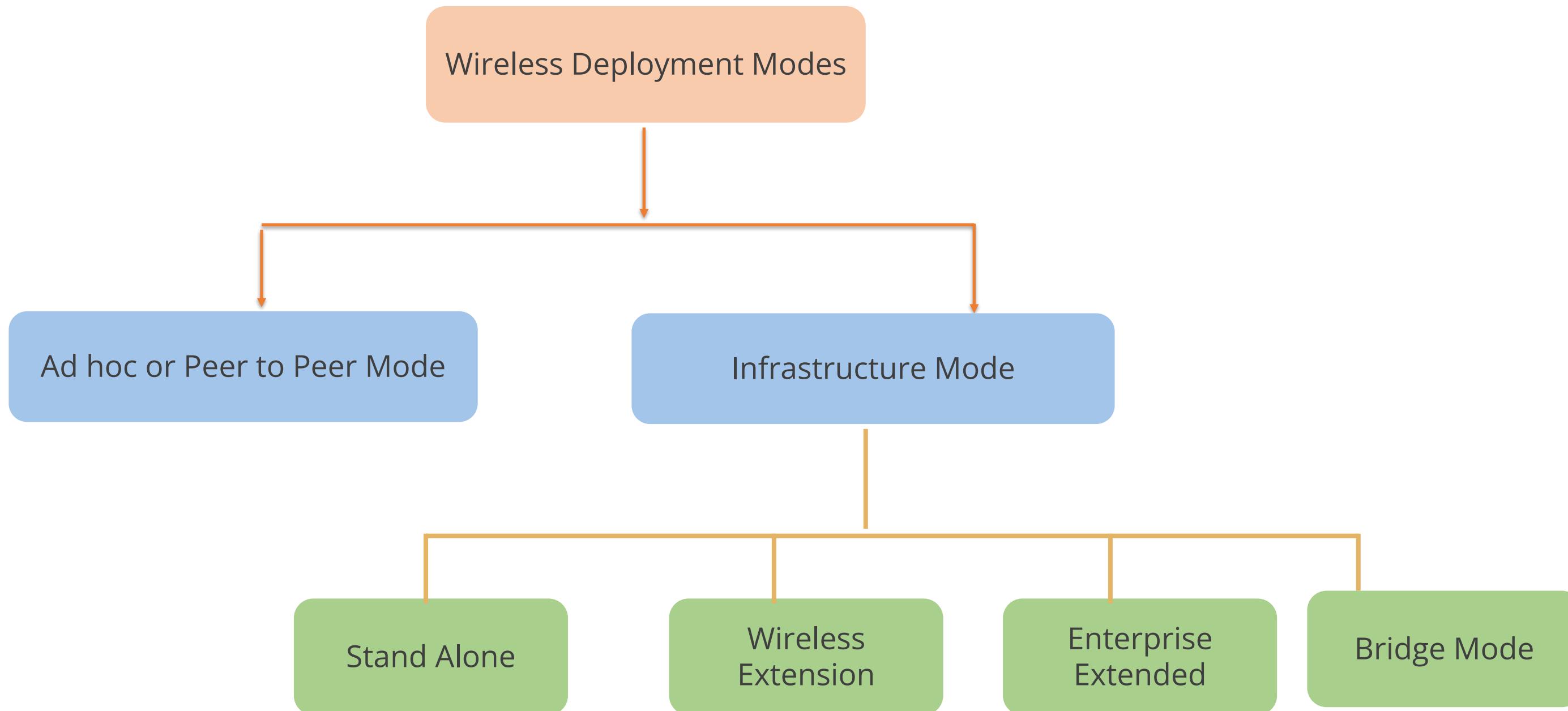
Standard	Year Introduced	Band Frequency	Max Data Transfer	Modulation
802.11a	1999	5 GHz	54 Mbps	DSSS, FHSS
802.11b	1999	2.4 GHz	11 Mbps	OFDM
802.11g	2003	2.4 GHz	54 Mbps	DSSS
802.11n	2009	2.4 & 5 GHz	600 Mbps	OFDM
802.11ac	2013	5 GHz	1.3 Gbps	MIMO-OFDM
802.11ax	2021	2.4, 5 (Wi-Fi 6) 6 GHz (Wi-Fi 6E)	10 Gbps	OFDMA, MU-MIMO

IEEE Wireless Standards

IEEE Wireless Standards:

- IEEE 802.11 refers to a family of specifications for WLANs developed by a working group of the IEEE.
- Wireless standards, primarily governed by the IEEE 802.11 series, define the protocols and specifications for wireless networks. These standards ensure compatibility between different devices and manufacturers, enabling seamless communication.
- It also generically refers to the IEEE Committee for setting wireless LAN standards.

Wireless Deployment Modes



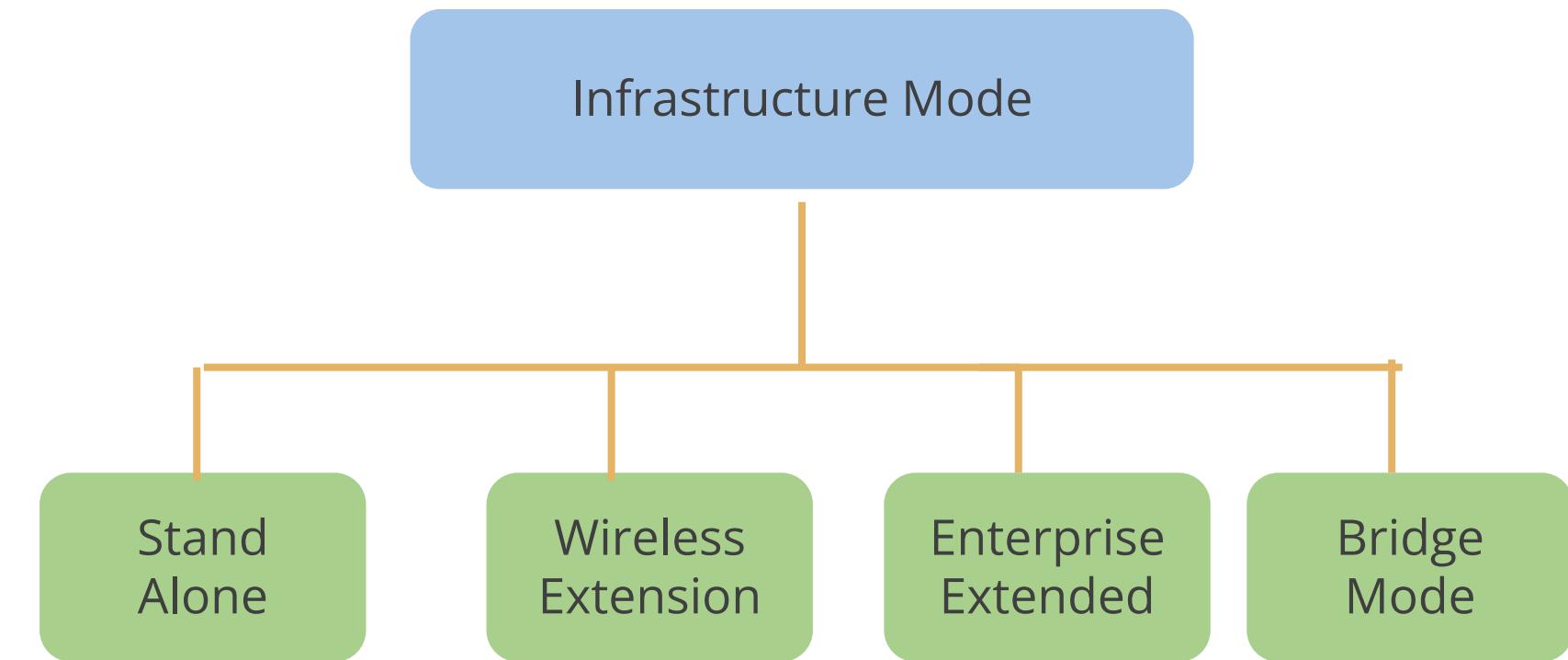
Wireless Deployment Modes: Ad hoc Mode

- It means that any two wireless networking devices, including two wireless network interface cards (NICs), can communicate without a centralized control authority.
- It refers to a wireless network structure where devices can communicate directly with each other.



Wireless Deployment Modes: Infrastructure Mode

Infrastructure mode means that a wireless access point is required, wireless NICs on systems can't interact directly, and the restrictions of the wireless access point for wireless network access are enforced.

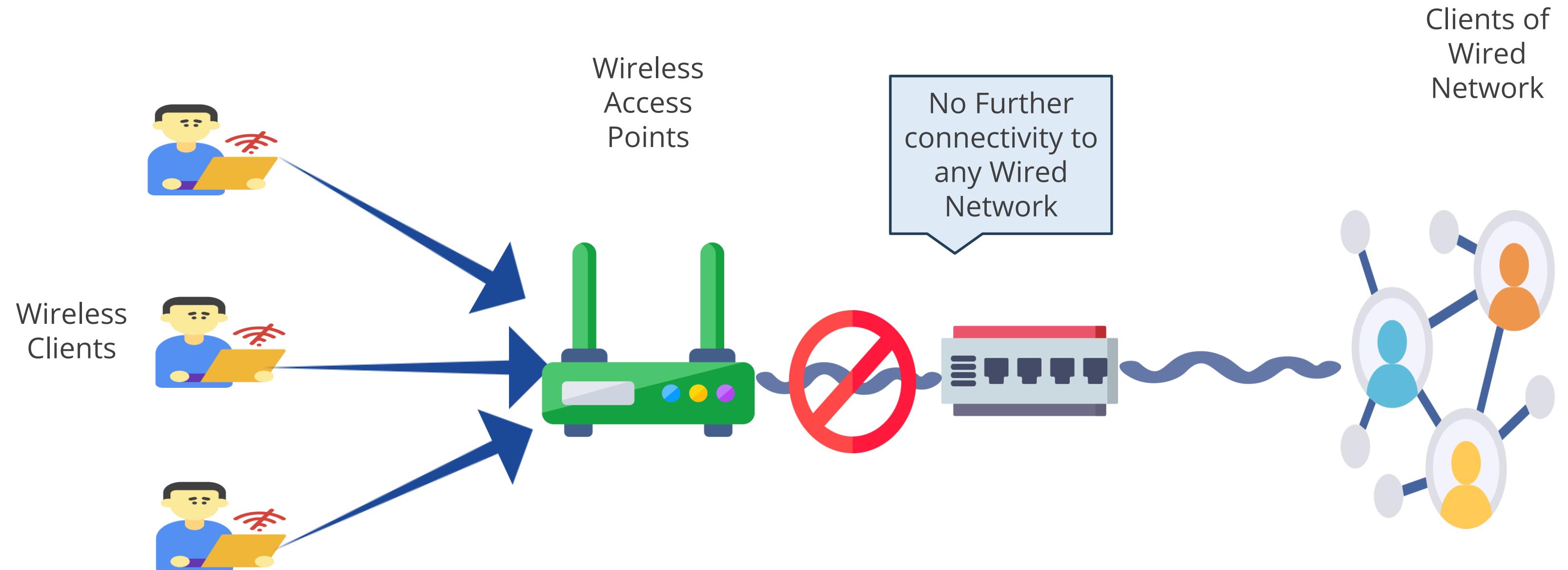


Infrastructure Mode: Standalone Mode

Standalone infrastructure occurs when there is a wireless access point connecting wireless clients but not to any wired resources. The wireless access point serves as a wireless hub exclusively not further connected.



Infrastructure Mode: Standalone Mode

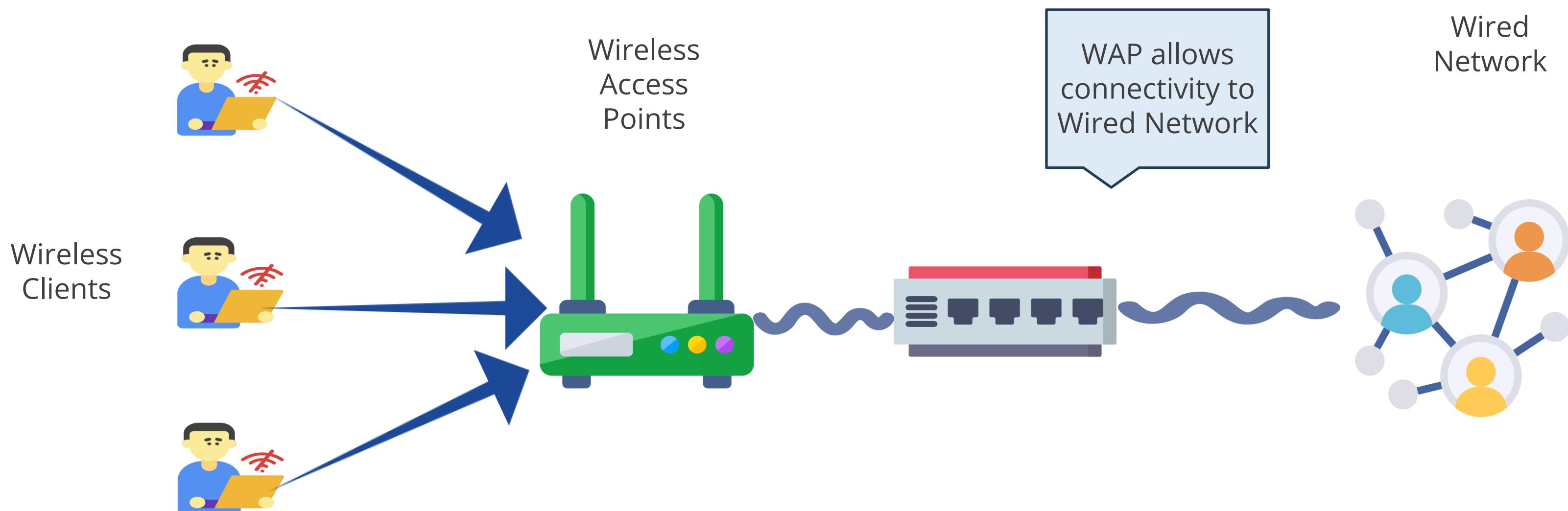


Infrastructure Mode: Wireless Extension Mode

It is a configuration setting in wireless networking that allows a Wi-Fi network to be expanded by connecting multiple access points (APs), effectively extending the coverage area of the network.

It occurs when the wireless access point acts as a connection point to link the wireless clients to the wired network.

Infrastructure: Wireless Extension Mode

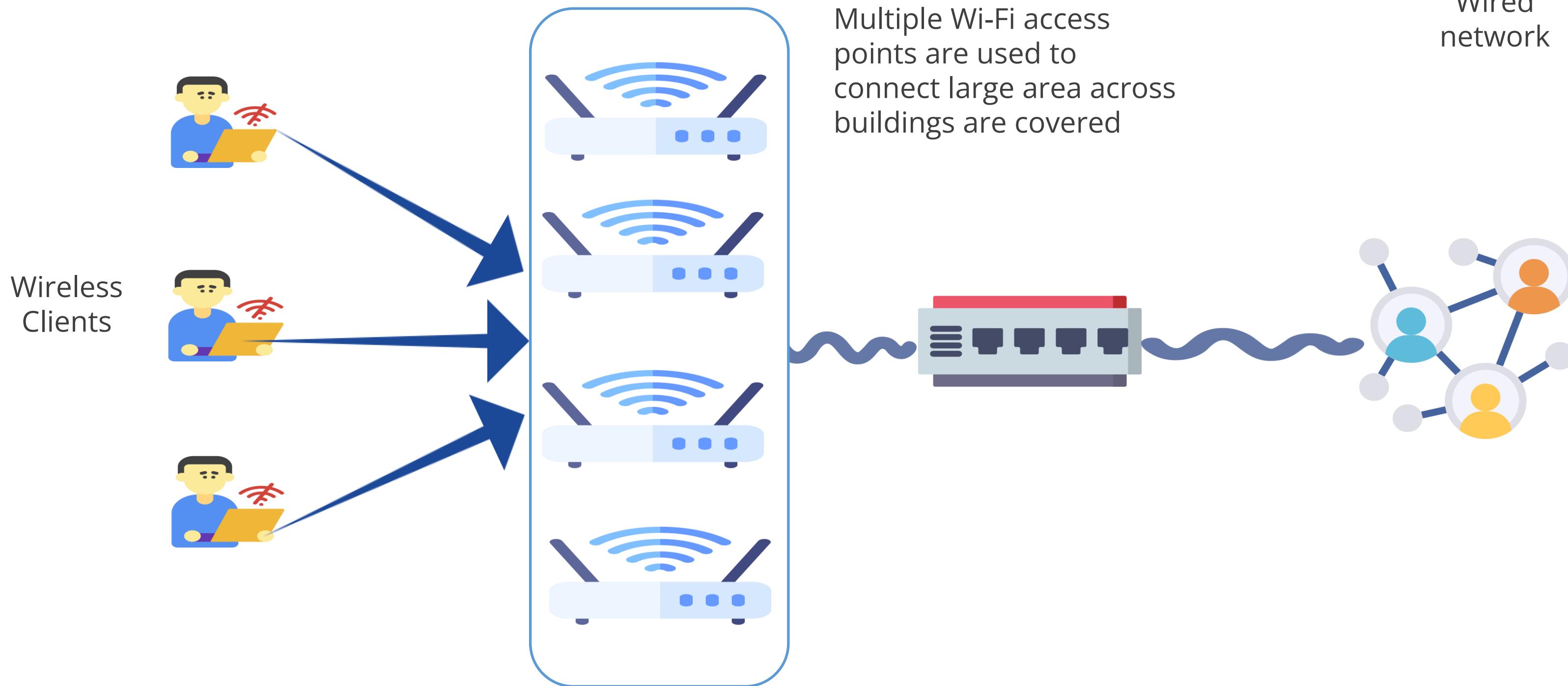


Infrastructure Mode: Enterprise Extension Mode

- Enterprise extended infrastructure occurs when multiple wireless access points (WAPs) connect a large physical area to the same wired network.
- Enterprise extended mode is designed for large-scale Wi-Fi deployments and is typically used in businesses, schools, or other organizations with extensive areas to cover.



Infrastructure Mode: Enterprise Extension Mode



Infrastructure Mode: Bridge Mode

It is a networking configuration that allows two or more network segments to be connected and act as a single network. It essentially bridges two networks, allowing devices on both sides to communicate with each other as if they were on the same local network.

It occurs when a wireless connection is used to link two wired networks. This often uses dedicated wireless bridges and is used when wired bridges are inconvenient, such as when linking networks between floors or buildings.

Infrastructure Mode: Bridge Mode



Service Set Identifier(SSID)

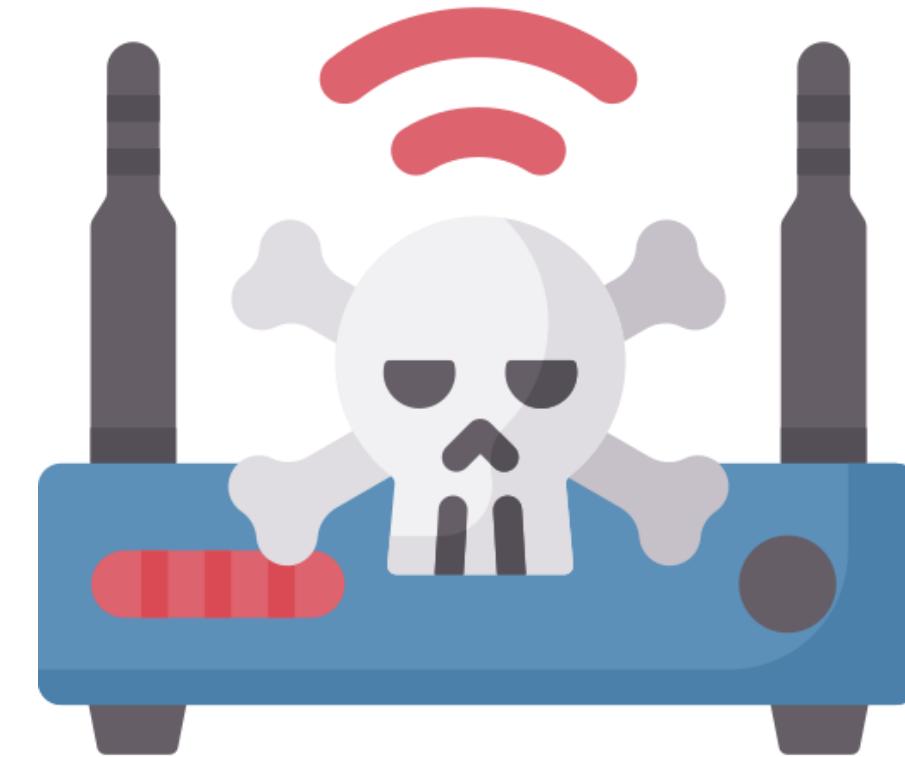
- It is a unique ID that can be made up of case-sensitive letters, numbers, and special characters like dashes, periods, and spaces.
- According to the 802.11 wireless local area networks (WLAN) standard, an SSID can be as long as 32 characters

Securing SSID



Wi-Fi Attacks

Wireless networks are more vulnerable to attacks than wired networks, as data travels through the airwaves as radio waves, making it easier for attackers to intercept or eavesdrop on information.



Wireless Attacks

Evil twin

- An evil twin is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications.
- It tricks them into connecting to a fake Wi-Fi network that appears legitimate, stealing their data or redirecting them to malicious websites

Eavesdropping

- This is a passive attack where attackers use tools like packet sniffers to capture data packets traveling over the airwaves.
- These packets can contain sensitive information such as login credentials, emails, or financial data if not properly encrypted.

Jamming

- Jamming is a denial of service that specifically targets the radio spectrum aspect of wireless.
- Like other DoS attacks can manipulate things behind the scenes, so can jamming on a wireless AP, enabling things such as attachment to a rogue AP

Wireless Attacks

Denial of service attack

- Attackers flood a network with bogus traffic, overwhelming it and making it unavailable to legitimate users. This can disrupt operations for businesses or organizations relying on the network..

Disassociation

- Disassociation attacks against a wireless system are attacks designed to disassociate a host from the wireless access point, and from the wireless network.
- A disassociation attack, also known as a de-authentication attack, targets the connection between a device and a Wi-Fi network and disconnect the users from network

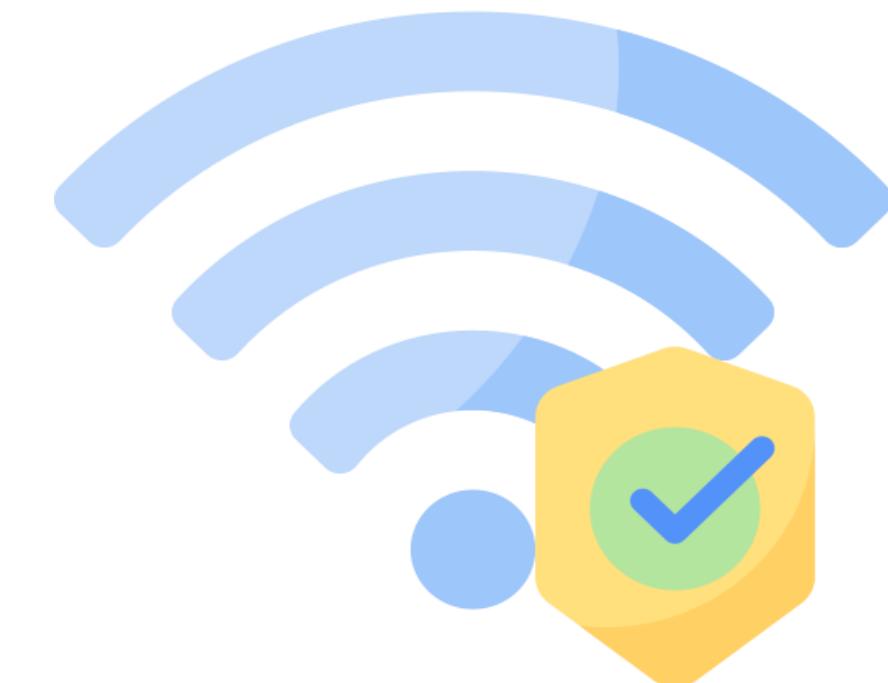
War driving

- It is searching for Wi-Fi wireless networks, usually from a moving vehicle, using a laptop or smartphone.
- It involves slowly driving around an area to locate Wi-Fi signals. This can be done by an individual or with one person driving and others searching for wireless networks.

Wi-Fi Security

It is a multifaceted approach to protecting your wireless network from unauthorized access and data breaches which are discussed further.

It is crucial to safeguard your personal data and prevent unauthorized access to your network.



Wi-Fi Security Measures

The following measures are taken to enhance the Wi-Fi security:

Use of encryption



Use WPA2 authentication

Use antivirus, antispyware
and firewall

Turn off SSID broadcast

Use WPA3 authentication

Wi-Fi Encryption Protocol

- It is a set of rules and procedures used to scramble data transmitted over a wireless network, making it unreadable to unauthorized individuals.
- It is essential for safeguarding your wireless network from unauthorized access and data breaches.



Secure Encryption Protocol

Wired Equivalency Privacy(WEP)

- Wired Equivalent Privacy is defined by the IEEE 802.11 standard.
- WEP was designed with one main goal in mind: to prevent hackers from snooping on wireless data as it was transmitted between clients and access points (APs).
- WEP uses a predefined shared secret key of 40 bits.
- A shared key is static and shared among all wireless access points and device interfaces.
- It uses the RC4 algorithm.

WIFI Protected Access(WPA)

- WPA is an improvement over WEP in that it does not use the same static key to encrypt all communications.
- Instead, it negotiates a unique key set with each host.
- However, a single passphrase is used to authorize the association with the base station (i.e., allow a new client to set up a connection).
- If the passphrase is not long enough, it could be guessed.
- Usually, 14 characters or more for the passphrase are recommended.

Secure Encryption Protocol

Wi-Fi Protected access-2(WPA2)

- It is a new method of securing wireless that was developed and is still considered secure. This is the amendment known as 802.11i, or WPA2.
- WPA2 uses the Advanced Encryption Standard (AES), which is considered much more secure than the encryption used in WEP and WPA (TKIP).
- WPA2 also introduced more seamless roaming, enabling clients to move from one AP to another on the same Wi-Fi network without having to reauthenticate.

Wi-Fi Protected access-3(WPA 3)

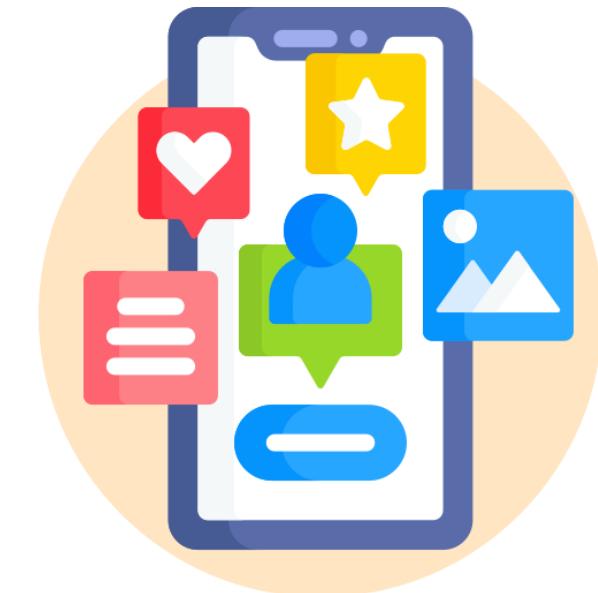
- It also standardizes the 128-bit cryptographic suite and disallows obsolete security protocols.
- WPA3-Personal also uses AES encryption, like WPA3.
- It uses Simultaneous Authentication of Equals (SAE), which is a more secure key exchange method compared to WPA2's PSK mode, making it more resistant to password-cracking attempts.
- SAE also eliminates the reuse of encryption keys, requiring a new code with every interaction.

TECHNOLOGY

Mobile Management and Security

Introduction to Mobile Management

- Involves the administration and control of mobile devices within an organization
- Includes activities such as device provisioning, configuration, security, and compliance
- Encompasses deployment models and security solutions, such as Mobile Device Management, mobile application management, and content management, which will be discussed in detail in the following slides



Mobile Device Security

- Cell phones, tablets, computers, and more have become a dominant part of our everyday lives.
- These devices store information such as contact lists, passwords, emails, texts, and other data.
- These attacks on your mobile device aim to steal private information, including bank details, login credentials, and other sensitive data.
- Mobile device security protects your data from security threats, prevents data breaches, blocks unauthorized access to sensitive information, and mitigates data loss due to user error, theft, or misplacement.



Connection Method

Cellular

- Cellular connections use mobile telephony circuits, typically fourth-generation (4G) or LTE, though some 3G services still exist.
- Cellular networks offer robust nationwide coverage, providing strong signals virtually anywhere with reasonable population density.

WIFI

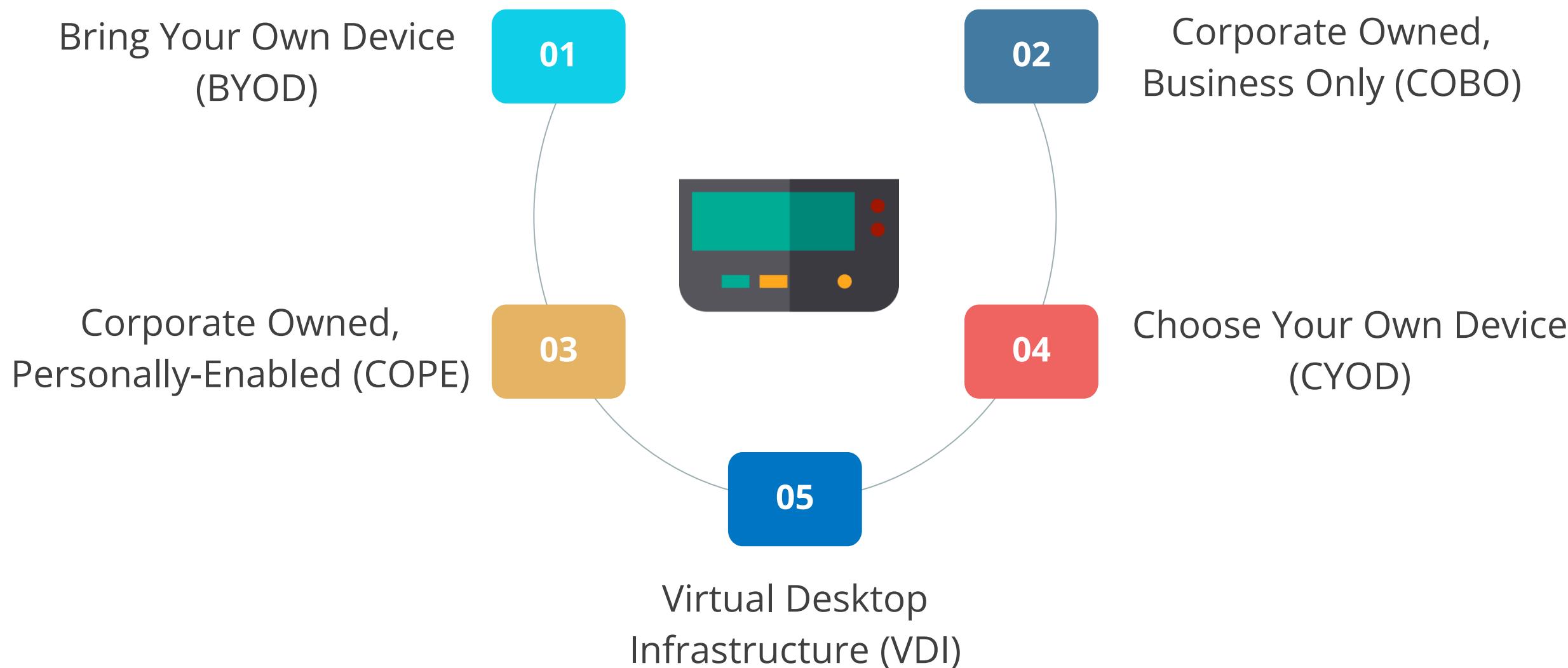
- Wi-Fi refers to the radio communication methods developed under the Wi-Fi Alliance.
- These systems exist on 2.4- and 5-GHz frequency spectrums and are constructed by both the enterprise you are associated with and third parties.

Satellite communication

- SATCOM (satellite communications) is the use of terrestrial transmitters, receivers, and satellites in orbit to transfer signals.
- Satellites are expensive, and for high-density urban areas, both cost and line-of-sight issues make SATCOM a more expensive option.

Mobile Device Deployment Models

A mobile device deployment model explains the process by which employees are supplied with mobile devices and applications. It can be:



Mobile Device Deployment Models

Bring your own device

Allows employees to use personal devices to access organizational networks, work systems, and sensitive data

Corporate owned business only

Provides employees with company-owned devices restricted to company use

Corporate owned, personally-enabled

Gives employees company-owned devices for both business and personal use

Choose your own device

Lets employees select from a list of company-approved devices

Virtual desktop infrastructure

Controls the mobile environment of non-corporate-owned equipment

Enterprise Mobility Management

Enterprise Mobility Management (EMM) is a class of management software that applies security policies for the use of mobile devices and applications in the enterprise.

Provides visibility over use and configuration

Manages enterprise-owned devices and BYOD

Enterprise Mobility Management

The main functions of an EMM product site are as follows:

Mobile Device Management (MDM)

- Involves network enrollment
- Manages device functions

Mobile Application Management (MAM)

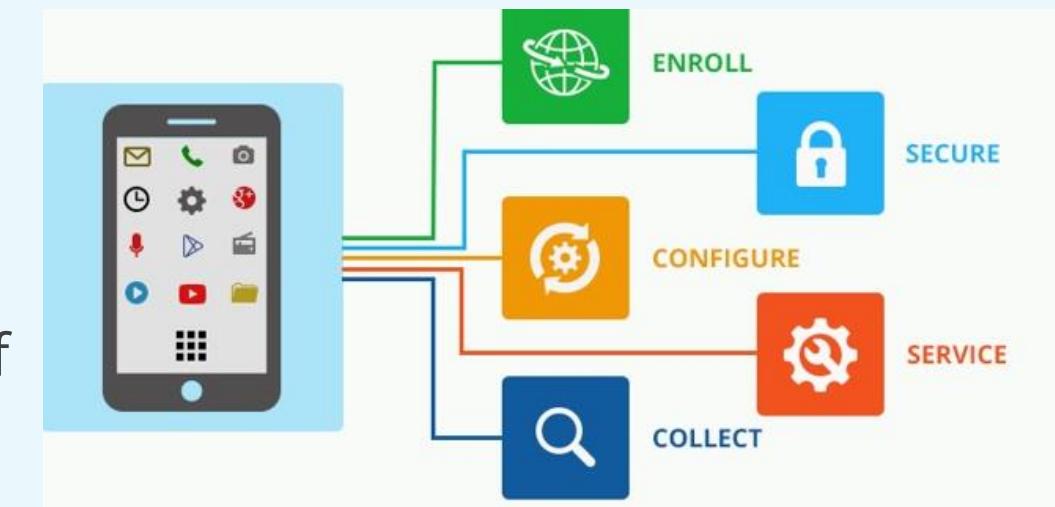
- Involves installing and monitoring corporate apps and data

Unified Endpoint Management (UEM)

- Aims for visibility across PCs, laptops, smartphones, tablets, and even IoT devices

Mobile Device Management

- Manages mobile devices in organizations to access sensitive business data
- Includes storing essential information about mobile devices, deciding which apps can be installed, locating devices, and securing devices if lost or stolen



MDM Policy Controls

**Lock the device
with a strong
password**

**Lock the device
automatically after a
certain period of
inactivity**

**Remotely lock the
device if it is lost or
stolen**

**Encrypt data on the
device**

**Wipe the device
automatically after
a certain number of
failed login attempts**

a

Mobile Access Control Systems

The security and privacy of a smartphone is ensured by the following authentications:



Mobile Access Control Systems

A screen lock mechanism, such as a password, PIN, or pattern, can be used to protect a user's smartphone from any intervention.



Context-aware authentication helps a user unlock the smartphone
in case of password loss.

Remote Wipe

Remote wipe or kill switch is initiated from the enterprise management software.

It sets the device to factory defaults or clears storage if the smartphone is stolen. The remote wipe is triggered when the thief enters the wrong password multiple times.



The thief might be able to prevent the device from receiving the wipe command.

The screenshot shows a web-based management interface for a user named James Pengelly. The left sidebar lists various services: User Info (selected), Exchange, SecuriSync, AppID, Skype for Business, SharePoint, POP/IMAP Mailboxes, and Email Archiving. The main content area is titled 'ActiveSync devices' and displays a table of connected devices:

Device name	Device model	Latest sync date	Wipe	Delete
Outlook for iOS and Android	Outlook for iOS and Android	10/09/2017, 21:38:41	Wipe	Delete
XT1032	XT1032	31/05/2017, 08:49:03	Wipe	Delete
Outlook for iOS and Android	Outlook for iOS and Android	22/05/2017, 04:13:57	Wipe	Delete
Moto G (5)	Moto G (5)	16/05/2017, 14:44:57	Wipe	Delete
White iPad mini	iPad2C5	19/06/2016, 19:19:59	Wipe	Delete
Outlook for iOS and Android	Outlook for iOS and Android	24/08/2015, 22:22:20	Wipe	Delete
unknown	iPhone	12/06/2012, 10:17:06	Wipe	Delete

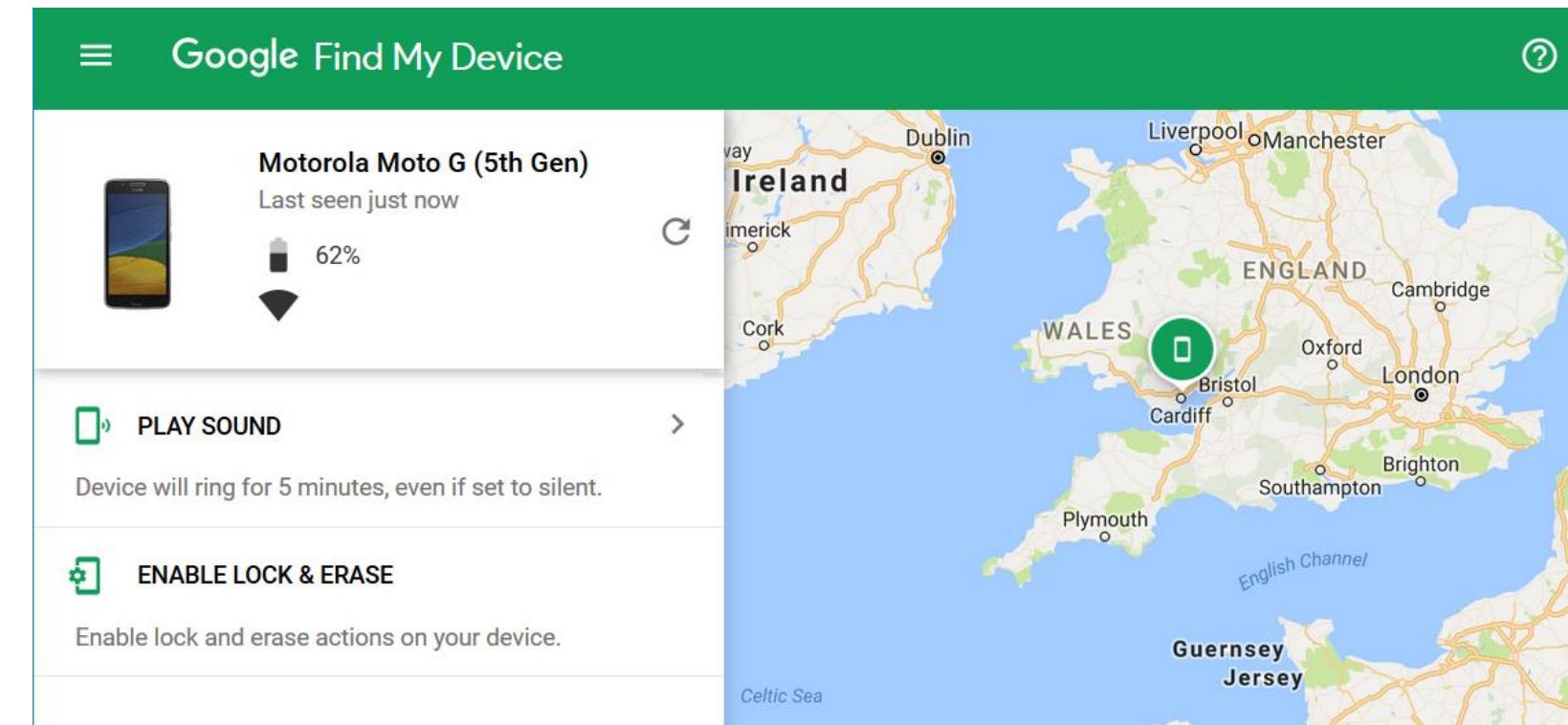
7 items found (7 total)

The screenshot here shows the corporate messaging service by Intermedia.

Geofencing

Geofencing applies location-based policies automatically and helps disable the onboard camera or video through MDM or EMM controls.

Using **Find My Device**
to locate an Android
smartphone



GPS Tagging

Global Positioning System (GPS) tagging refers to the process of including geographical identification metadata in a device.



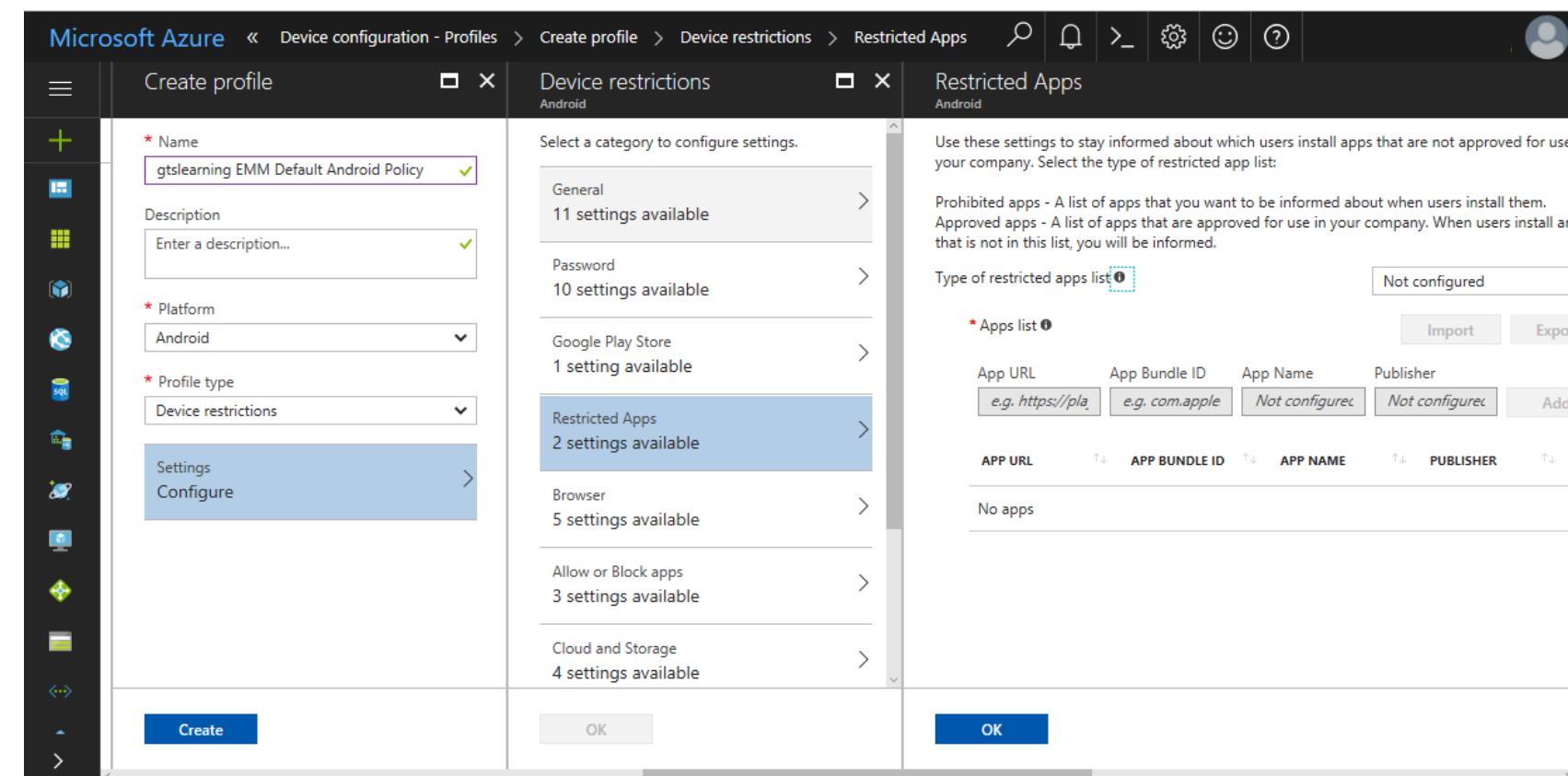
Is highly sensitive and poses a risk to personal information

Helps track movements and assists social engineering

Application Management

MDM or EMM applications use policies to provide better management of devices.

Android allows third-party app stores to install untrusted applications onto a device with the user's consent, a process known as sideloading.



Content Management

Devices are usually privately owned for corporate use and using them for any other tasks creates data ownership and privacy issues.



Containerization sets up a corporate workspace segmented from the employee's private apps and data.



It enforces storage segmentation to ensure data separation.



It helps enforce content management or DLP policies.

Rooting and Jailbreaking

Rooting or jailbreaking mobile devices involves subverting the security measures on the device, posing a risk for the enterprise management agent.

Rooting

- Rooting is the process of gaining administrative privileges (root access) on an Android device
- Usually done on Android devices
- Also known as custom firmware or ROM (Read only memory)

Jailbreaking

- Jailbreaking is the process of removing software restrictions imposed by the manufacturer on a device
- Usually done in iOS by restarting the device with a patched kernel

Carrier unlocking

- Removes the restriction by the network provider, allowing the use of a SIM from another provider
- Performs on both iOS and Android
- Unlocks a device to a single carrier

TECHNOLOGY

Application Security

Application Security

- Involves developing, adding, and testing security features within applications to prevent security vulnerabilities against application threats
- Protects software applications from cyberattacks and data breaches
- Encompasses the entire lifecycle of an application, from the initial design phase to deployment and ongoing maintenance
- Focuses on identifying, mitigating, and preventing various application vulnerabilities that attackers can exploit



Reasons for Software Vulnerabilities



Application Security Controls

Input validations

Secure cookies

Static code analysis

Code signing

Secure coding practices

- Is a critical security measure in software development. It ensures that only expected and authorized data enters your system, protecting against vulnerabilities and improving data integrity
- Prevents attackers from injecting malicious code or unexpected data that could disrupt program flow or compromise the system (e.g., SQL Injection, Cross-Site Scripting (XSS))
- Ensures that data conforms to the expected format (e.g., email address format, date within a specific range)

Application Security Controls

Input validations

Secure cookies

Static code analysis

Code signing

Secure coding practices

- Cookies, also known as HTTP cookies, web cookies, or internet cookies, are small pieces of data created by websites and stored on your device (computer, phone, tablet) by your web browser.
- They act like a little note from the website that helps it remember information about you and your visit.
- Secure cookies are an upgraded version of regular cookies that encrypt the cookie data using HTTPS, ensuring it's unreadable if intercepted during transmission.
- These secure cookies are sent only over HTTPS connections due to the Secure attribute that instructs the browser on this limitation.

Application Security Controls

Input validations

Secure cookies

Static code analysis

Code signing

Secure coding practices

- Is a security testing technique that examines computer code without running it
- Involves meticulously reviewing a recipe to identify potential problems before you start cooking
- Uses tools to parse and analyze the source code of your program, typically written in languages like C++, Java, or Python
- Helps identify issues early in the development process, making them easier and cheaper to fix compared to finding them later in production

Application Security Controls

Input validations

Secure cookies

Static code analysis

Code signing

Secure coding practices

- Verify the authenticity and integrity of software code with code signing, a security practice
- Function as a cryptographic seal, providing assurance regarding the authenticity and reliability of software through code signing
- Ensure the software has not been tampered with and comes from a trusted source with code signing
- Display security warnings in operating systems to alert users when they attempt to install unsigned code, encouraging caution

Application Security Controls

Input validations

Secure cookies

Static code analysis

Code signing

Secure coding practices

- Follow secure coding practices to enhance security and minimize vulnerabilities
- Ensure software is secure, resilient, and less prone to security breaches with these practices
- Prevent the introduction of security weaknesses in the code, making it harder for attackers to exploit the software

TECHNOLOGY

Sandboxing

Sandboxing

It is a technique used to safely evaluate the threat in an isolated test environment (sandbox).

- It tests suspicious programs in isolated environments to prevent harm to the host device.
- It provides effective protection against zero-day attacks and advanced threats.
- Suspicious email attachments are sent to a virtual sandbox for deep analysis of malicious activity.



Sandboxing Flow

Isolation:

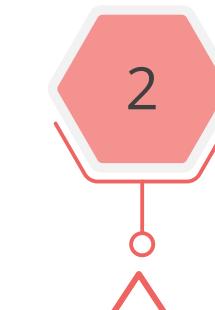
A sandbox creates a segregated environment that mimics a real operating system, allowing suspicious programs to execute without affecting the real system or network.

Analysis:

Security experts can then analyze the activity of the code inside the sandbox.

Protection:

If the code is found to be malicious, it can be prevented from entering the real system, thus stopping a cyberattack in its tracks.



Detonation:

The suspicious code is then detonated within the sandbox, essentially run and its behavior monitored closely.

Threat detection:

By observing the behavior of the code, analysts can identify malicious activities such as attempts to steal data, install malware, or damage the system.

Benefits of Sandboxing

Proactive defense:

Sandboxing allows for the analysis of unknown or zero-day threats that traditional signature-based security might miss.

Safe analysis:

Security professionals can examine potentially risky code without putting the actual system or network at risk.

Improved detection rates:

Sandboxing can uncover sophisticated malware that might bypass traditional security measures.

TECHNOLOGY

Monitoring

Monitoring

It is the process of continuously tracking, analyzing, and managing the performance, health, and availability of the IT infrastructure to keep the systems running smoothly.



Commercial applications such as SolarWinds Security Event Manager and Splunk, offer robust monitoring and alerting solutions for businesses to help them detect and respond to potential security threats.

Assets to monitor in Infrastructure

Hardware performance:

CPU utilization, memory usage, disk space, and network bandwidth

System health:

Uptime, errors, and application response times

Resource utilization:

Monitoring resource usage helps identify potential bottlenecks and plan for future needs.

Security events:

Suspicious login attempts, unauthorized access, and malware activity



Why is Infrastructure Monitoring Important?

Identifies problems proactively

Improves security posture

Optimizes resources better

Enhances capacity planning

Improves system uptime
and performance

Security Implications of Proper Hardware, Software, and Data Asset Management

Effective Asset Management in Cybersecurity

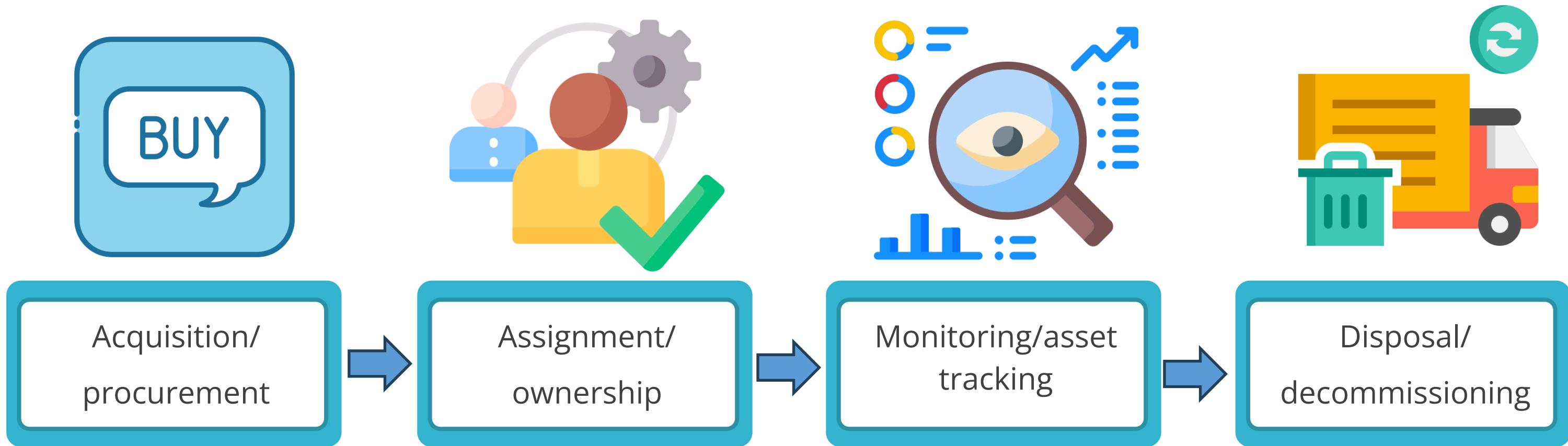
Proper management of hardware, software, and data assets is crucial for maintaining cybersecurity. This section covers:

- **Acquisition and third-party risk assessment:** Evaluating risks associated with acquiring new assets and integrating third-party services
- **Asset assignment and accountability:** Ensuring assets are properly assigned and accountability is maintained
- **Asset disposal and decommissioning:** Guidelines for securely disposing of and decommissioning assets to prevent data breaches



Phases of Asset Management

Proper asset management involves several key phases, each with important security implications:



Acquisition/Procurement

The acquisition or procurement process is the initial phase of asset management, setting the stage for securely handling hardware, software, and data assets:

Strategic evaluation

Begins with a strategic evaluation of an organization's technological needs

Beyond purchasing

Involves more than merely purchasing the required resources

Comprehensive strategy

Ensures that procured items meet the organization's security policies, standards, and compliance requirements

Factors to Consider During Acquisition/Procurement Process

Change management

Vendor selection



Compliance alignment

Risk assessment

Total cost of ownership

Factors to Consider During Acquisition/Procurement Process

Change management

Vendor selection

Total cost of ownership

Risk assessment

Compliance requirement

- When you procure new assets or replace existing ones, submit a case to the Change Advisory Board for purchase and implementation approval.
- Introducing new IT assets can disrupt established workflows and user habits.
- Change management helps prepare users for changes and minimizes resistance to adoption.

Factors to Consider During Acquisition/Procurement Process

Change management

Vendor selection

Total cost of ownership

Risk assessment

Compliance requirement

- Vendor selection is a critical step in successfully acquiring IT assets. Choosing the right vendor can ensure you get high-quality equipment, software, or services that meet your needs and budget.
- It's crucial for quality, cost efficiency, reliability, and compliance.
- Finding the best deal and ensuring the vendor aligns with your organization's security and compliance requirements is essential.

Factors to Consider During Acquisition/Procurement Process

Change management

Vendor selection

Total cost of ownership

Risk assessment

Compliance requirement

- TCO (Total Cost of Ownership) assesses the complete cost of acquiring, owning, and operating an asset over its lifecycle.
- It goes beyond the initial purchase price to include ongoing expenses.
- Hidden costs can significantly impact your budget over time. Consider maintenance costs and replacement parts, not just the purchase price.

Factors to Consider During Acquisition/Procurement Process

Change management

Vendor selection

Total cost of ownership

Risk assessment

Compliance requirement

- Risk assessment is crucial to identify, analyze, and prioritize potential risks.
- It helps develop strategies to mitigate risks and ensure project success.
- Address security considerations at every stage of the acquisition process.
- Comprehensive risk assessment helps identify vulnerabilities and threats.

Factors to Consider During Acquisition/Procurement Process

Change management

- Consider compliance requirements to adhere to relevant laws, regulations, and industry standards.
- Non-compliance can result in fines, legal consequences, and reputational damage.
- Adherence to legal and regulatory requirements is non-negotiable; security and compliance go hand in hand.
- Ensure acquired assets comply with data protection, privacy, and industry-specific regulations.

Vendor selection

Total cost of ownership

Risk assessment

Compliance requirement

Assignment/Ownership

Proper assignment and ownership of assets are crucial for effective asset management.

- Each asset procured or developed should be accounted for and allocated to a data owner.
- Ownership designates the individual or department responsible for an asset from acquisition to decommissioning.
- Establishing ownership ensures responsibility and accountability, impacting the organization's overall security posture.



Activities Flowing Out of Ownership/Assignment Process

Proper ownership and assignment of assets lead to several critical activities:

Asset register:

A comprehensive record of an organization's assets, including details such as location, value, and ownership

Standard naming convention

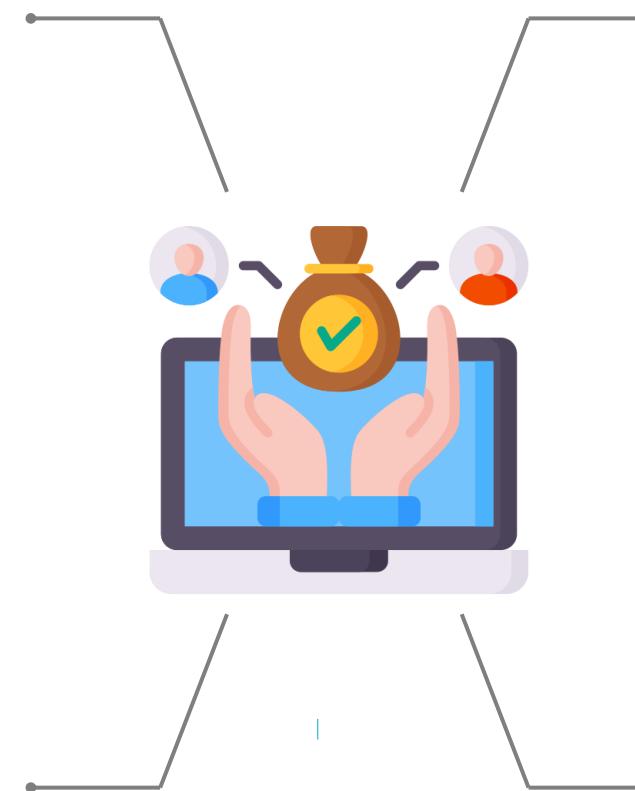
Required to distinguish between different assets

Ownership:

Ensures accountability by assigning specific owners to assets, making it easier to enforce accountability for their condition and usage

Asset classification:

Involves categorizing assets into critical, essential, and non-essential, ensuring appropriate support based on asset value and sensitivity



Monitoring/Asset Tracking

Monitoring and asset tracking are central pillars of effective asset management, vital for maintaining an organization's cybersecurity hygiene:

- Provides continuous visibility into the status, location, and condition of all assets within an organization
- Ensures informed decisions related to security, budgeting, and overall operations



Activities flowing out of Monitoring/Asset Tracking

Inventory

- Maintains a detailed record of all organizational assets, including make, model, software version, and patch level
- Allows for accurate tracking, efficient asset utilization, and cost optimization
- Tools: IBM Maximo, ServiceNow Asset Management

Enumerations

- Takes inventory management a step further
- Each asset should have a distinct identifier for easier tracking and differentiation
- Actively identifies assets within an environment and maps their relationships and dependencies

Tools for Inventory/Enumerations

Mobile Device Management (MDM)

Monitors and tracks mobile devices; can remotely wipe lost or stolen devices

Asset tags

Crucial for inventory management, particularly for physical IT assets

RFID tags

Quickly scan and identify assets in proximity for efficient tracking

GPS and location-based Service

Services like Apple AirTag can track and monitor asset whereabouts

Microsoft intune

Tracks devices enrolled in its MDM platform, including smartphones, tablets, and laptops

Network mapper

Automatically scans a network to detect all connected devices, including desktops, laptops, servers, printers, NAS devices, and other equipment

Disposal/Decommissioning

The disposal/decommissioning phase is the final stage in the life cycle of an asset:

- Involves the systematic removal, decommissioning, and disposal of assets that are no longer in use or have reached the end of their operational life
- Mitigates the risk of unauthorized access and data breaches
- Maintains regulatory compliance
- Ensures no residual data is left on any data drives, especially if the device was used to access classified data



Data Disposal Methods

There are five major ways to destroy data. Each is explained in the following slides:

Erasing →

- Erasing is a simple deletion process.
- The process removes only the catalog reference, not the files.
- Not the best practice to destroy data, because anyone can retrieve the data using widely available tools.

Clearing (overwriting)

Purging

Sanitization

Degaussing

Data Disposal Methods

There are five major ways to destroy data. This slide explains the clearing (overwriting) method:

Erasing

Clearing (overwriting)

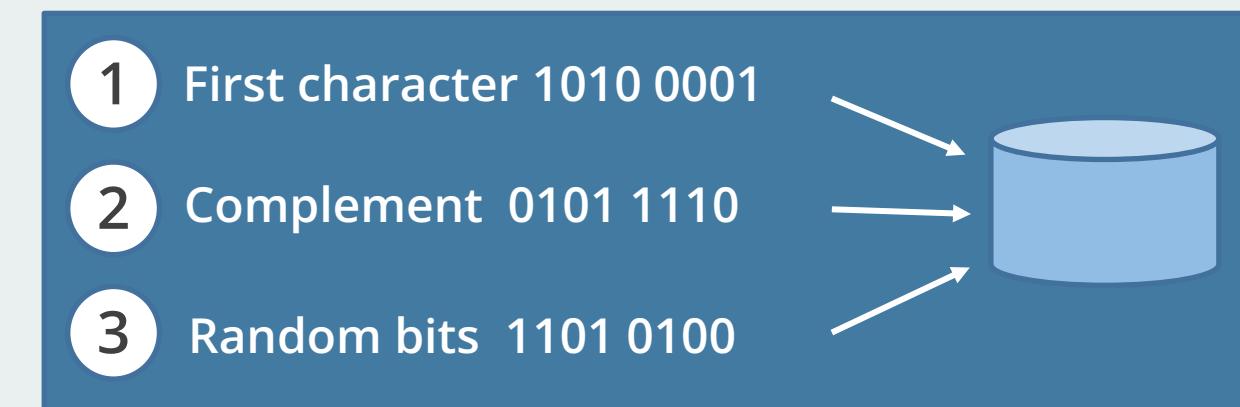
Purging

Sanitization

Degaussing

- Process of preparing the media for reuse with assurance that cleared data cannot be retrieved using traditional means of recovery.
- Unclassified data is written over all the addressable locations on the media.
- Data recovery requires special laboratory techniques.
- This method is used when you want to prepare media for reuse at the same classification level.

The following image illustrates the clearing process:



Data Disposal Methods

This slide explains the purging method:

Erasing

Clearing (overwriting)

Purging

Sanitization

Degaussing

- More intense form of clearing; repeats the clearing process multiple times
- Provides assurance that data cannot be recovered using any known means
- Can be combined with degaussing to completely remove data
- Used when one wants to prepare media for reuse at a lower classification level

Data Disposal Methods

This slide explains the sanitization method:

Erasing

Clearing (overwriting)

Purging

Sanitization

Degaussing

- Sanitization is a combination of processes that ensures data is removed from the system
- It ensures data cannot be recovered by any means
- The process includes ensuring non-volatile memory is erased, and external drives are removed and sanitized to destroy data

Data Disposal Methods

This slide explains the degaussing method:

Erasing

Clearing (overwriting)

Purging

Sanitization

Degaussing

- Generates heavy magnetic fields that realign the magnetic fields in magnetic media; only effective on magnetic media (does not affect CD/DVD/SSD)
 - AC erasure: Medium is degaussed by applying an alternating field that is reduced in amplitude over time
 - DC erasure: Medium is saturated by applying a unidirectional field

Data Destruction Methods

Data destruction is a critical process for ensuring the complete elimination of sensitive information:

- Destruction is the final stage in the life cycle of media and is the most secure method of sanitizing media.
- When destroying media, it is important to ensure that the media cannot be reused or repaired, and that data cannot be extracted from the destroyed media.



Destruction Methods

Various methods can be used to securely destroy data and prevent recovery:

Shredding

Refers to the mechanical shredding of hard drives, disks, or other storage media into small, unreadable pieces.

Incineration

Means burning the asset to ashes, ensuring it cannot be reassembled or used again.

Pulverization

Involves reducing the asset to small pieces by using a sledgehammer, or other means.

Crushing

Applying great force to render the asset unusable.

Chemical decomposition

Involves using chemicals to break down the asset's components.

Pulping

Means turning the paper waste into pulp and is like making papier-mâché.

TECHNOLOGY

Vulnerability Assessment

Vulnerability Assessment

It is the process in which vulnerabilities in IT are identified and the risks of these vulnerabilities are evaluated.

Vulnerability assessment objectives

The main objective of a vulnerability assessment process is to detect and remediate vulnerabilities in a timely fashion.

Vulnerability Assessment

The steps in the process are:

Identify the assets or resources



Identify vulnerabilities or potential threats to each resource



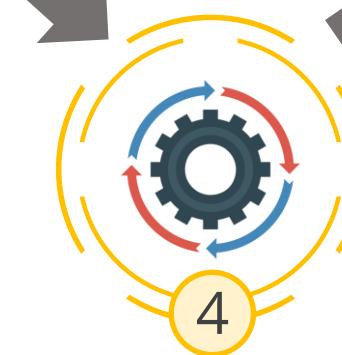
Define and implement ways to minimize the consequences if an attack occurs



Assign a quantifiable level of importance to the identified resources



Develop a strategy to mitigate or eliminate the most serious vulnerabilities in the most valuable resources



Types of Vulnerability Assessments

The three types of vulnerability assessments are:

Personnel testing

- Identify vulnerabilities in standard employee practices and demonstrate social engineering attacks

Physical testing

- Review facility and perimeter protection mechanisms
- Perform physical security vulnerability assessments

System and network testing

- Assess the system using the following methods:
 - Network discovery scan
 - Network vulnerability assessment
 - Web application vulnerability scan

Network Discovery Scan

It is a foundational step in the vulnerability assessment process, providing critical visibility into the network landscape

Network discovery scan

- They search for systems with open ports.
- They do not probe systems for vulnerabilities.



Commonly used tools

- NMAP
- Angry IP Scanner

Network Discovery Scan

There are four network discovery scanning techniques:

TCP SYN scanning

- Sends a single packet to each scanned port with the SYN packet set
- If a response with SYN and ACK flags is received, it indicates the port is open at the sender's end
- This is also called half-open scanning.

TCP connect scanning

- Opens a full connection to a remote system on the specified port
- It is used when the user running the scan does not have the necessary permissions to run a half-open scan

TCP ACK scanning

- Sends a packet with the ACK flag set, indicating that it is part of an open connection

Xmas scanning

- Sends a packet with the FIN, PSH, and URG flags set

Network Vulnerability Scan

It is a vital component of a comprehensive cybersecurity strategy, helping organizations identify, assess, and remediate vulnerabilities to protect their networks and data from potential threats.

Two common problems

- **False-positive:** Reporting a vulnerability without having substantial evidence to prove it or reporting by mistake, leading to a nuisance.
- **False-negative:** Not identifying a vulnerability and failing to report it as a part of the results, leading to a dangerous situation.

Tools used: Tenable Nessus, OpenVAS, Microsoft Baseline Security Analyzer (MBSA), and Retina Network Scanner Community Edition.

Network Vulnerability Scan

Types of scans:

Unauthenticated or non-credentialed scan:

- It is the process of exploring a network or a networked system for vulnerabilities that are accessible without logging in as an authorized user.
- It inspects the security of a target system from an outsider's perspective.

Authenticated or credentialed scan:

- It is a method in which vulnerability testing is performed as a logged-in or authenticated user.
- Authenticated scans help reduce the false-positive and false-negative results.
- Authenticated scans are performed with read-only access to the scanned servers.



Benefits of Network Vulnerability Scan



Identify weak points: Vulnerability scans provide a comprehensive view of potential vulnerabilities within your systems.



Prioritize remediation: By categorizing vulnerabilities based on severity (using CVSS), vulnerability scans help organizations prioritize which issues to address first.



Monitor continuously: Regular scans provide an ongoing assessment of your security posture, allowing you to proactively address emerging threats and vulnerabilities in real-time.

Vulnerability Scanners

They continuously identify, analyze, and report on potential security weaknesses in your IT infrastructure.

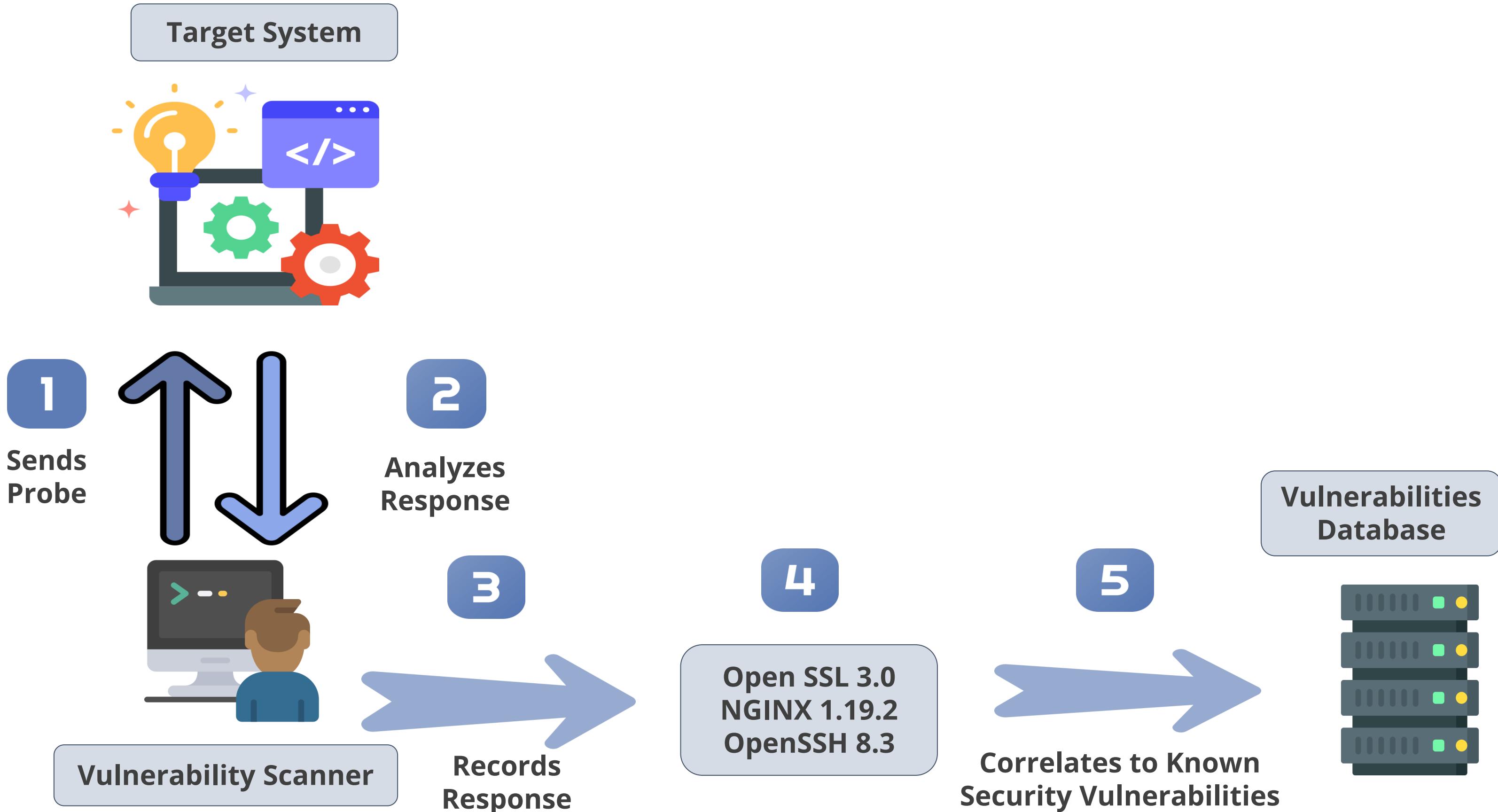


They work by comparing information about the software running on a system (such as version numbers and configurations) against databases of known vulnerabilities.

Vulnerability Scan Process

1. The process begins with the vulnerability scanner directing probes towards the target system.
2. These probes act as requests aimed at various components of the system.
3. Upon receiving these probes, the target system undergoes analysis and responds, providing information about its configuration, software versions, and potential vulnerabilities.
4. The vulnerability scanner, equipped with tools such as Open SSL 3.0, Nginx 1.19.2, and Open SSH 8.3, records and captures these responses.
5. Subsequently, it correlates the acquired data with entries stored in the Common Vulnerabilities and Exposures (CVE) database.

Vulnerability Scan Process



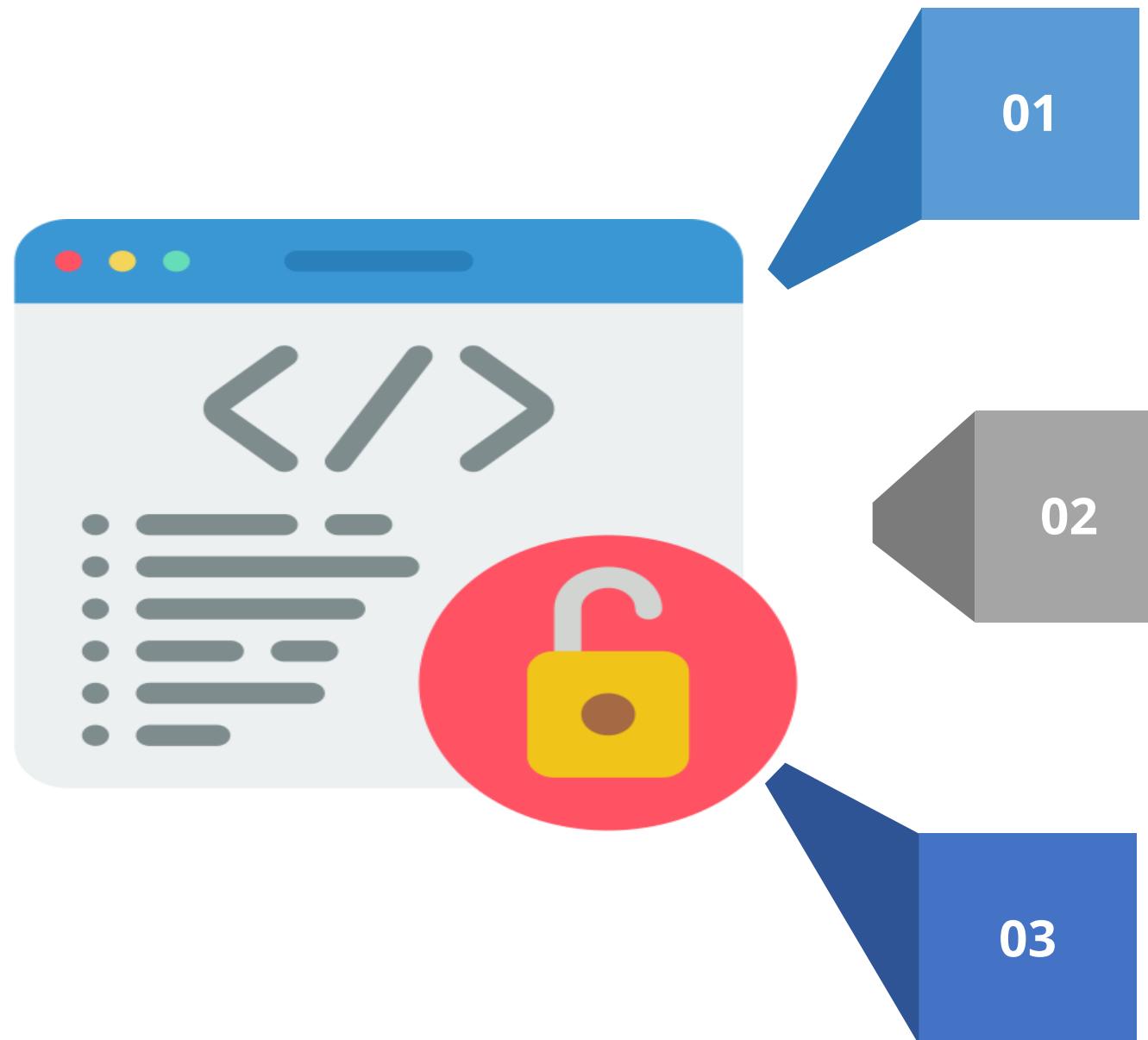
Security Content Automation Protocol (SCAP)

It is a framework that enables compatible vulnerability scanners to see whether a computer adheres to a predefined configuration baseline.



It is a set of specifications and tools that standardize how information about software flaws, security configurations, and vulnerabilities is communicated and exchanged.

SCAP Attributes



Standardized Formats: SCAP defines common formats for expressing information about vulnerabilities, security configurations, and patching information. This ensures different security tools can understand and utilize this data seamlessly.

Automation: SCAP facilitates the automation of vulnerability management tasks, allowing organizations to automate processes like vulnerability scanning, configuration assessment, and patch deployment

Open Source and Vendor-Neutral: SCAP is an open-source and vendor-neutral approach, meaning it's not tied to any specific security product or vendor. This allows for interoperability between different security tools from various vendors

Components of SCAP



Open vulnerability and assessment language:

It is a way to express information about vulnerabilities and system configurations in a structured and machine-readable format facilitating interoperability between different security tools.



Extensible configuration checklist description format:

It is a way to write down security checklists for computers and devices. Having a standard format like XCCDF allows different security tools to understand these checklists.



Common vulnerability scoring system (CVSS):

An industry-standard scoring system for assessing the severity of vulnerabilities. CVSS scores help prioritize which vulnerabilities to address first based on their potential impact

SCAP Benefits

Improved efficiency
Automates vulnerability management tasks, saving time and resources.

Simplified compliance
SCAP helps organizations comply with security regulations and standards that require vulnerability management practices

Enhanced security
Standardized formats ensure consistent and accurate communication of security information, leading to better decision-making

Vendor agnosticism
Allows organizations to leverage different security tools from various vendors without compatibility issues



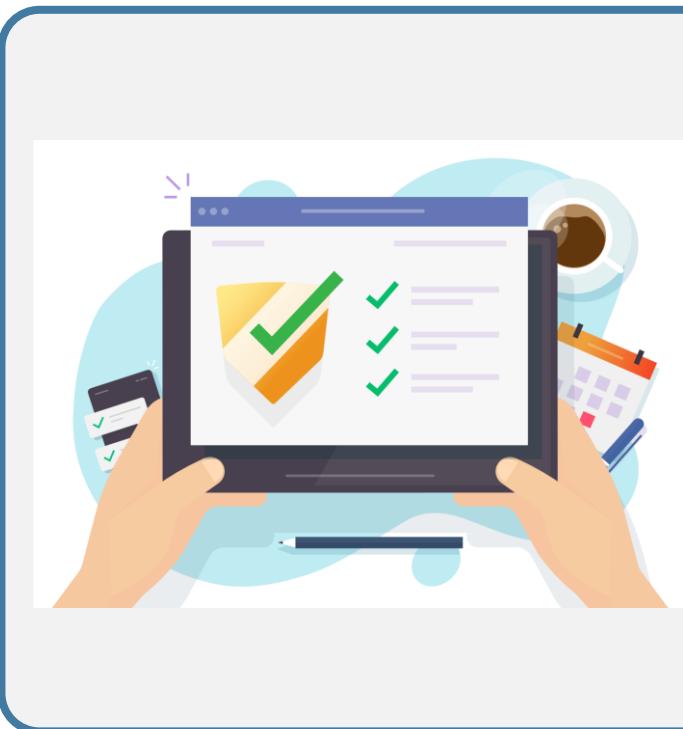
Web Application Vulnerability Scan

It is an automated security tool specifically designed to identify security vulnerabilities in web applications.



Uses special purpose scanners that analyze Web applications for known vulnerabilities

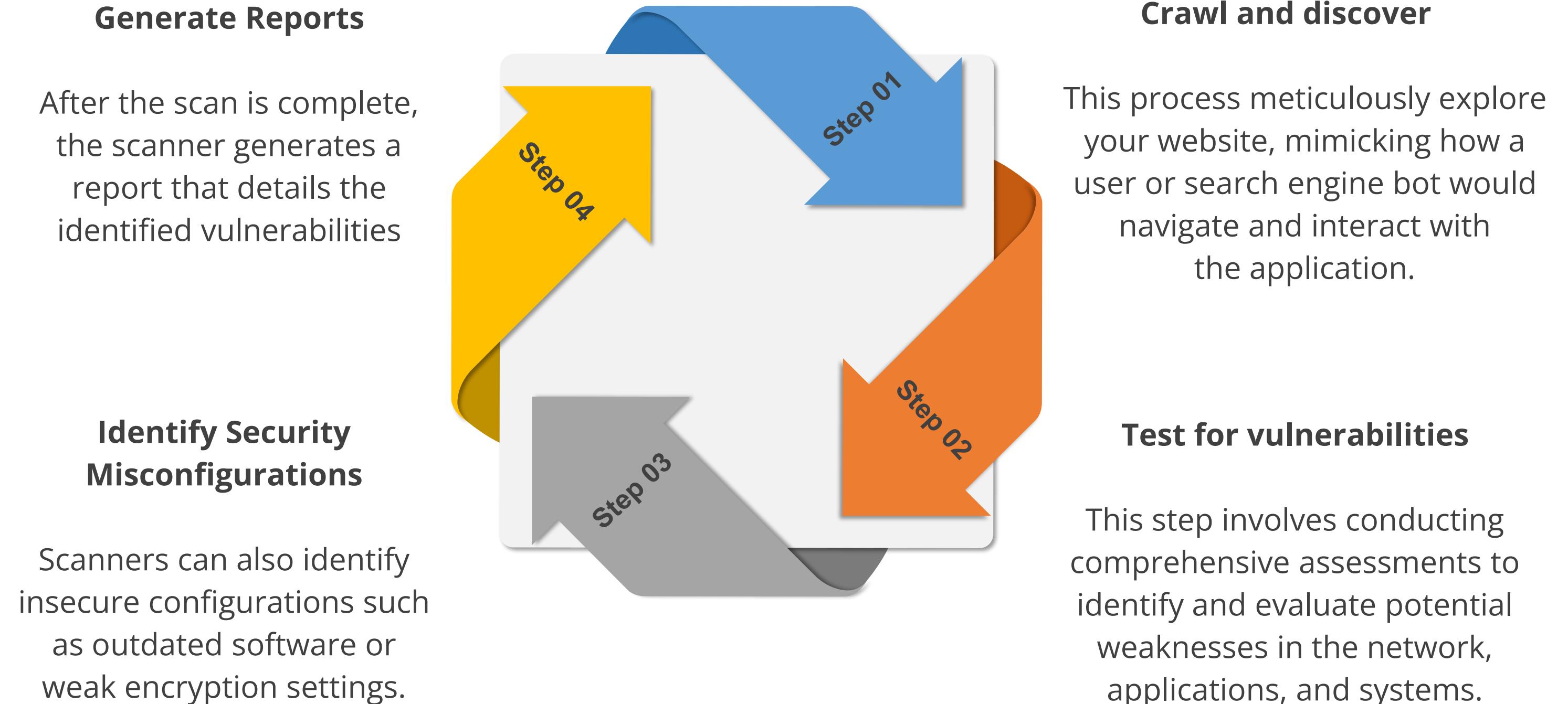
Web Application Vulnerability Scan



Ideal scenarios:

- Conduct an initial scan of all applications
- Examine any new application before moving to production
- Inspect any modified application before it moves to production
- Perform regular and scheduled reviews of all applications

Web Application Vulnerability Scanning Process



Benefits of Web Application Scanners

Proactive Security

Regular scans help identify vulnerabilities before attackers can exploit them, protecting your website and user data

Improved Security Posture

By addressing identified vulnerabilities, you can significantly strengthen the overall security of your web application

Compliance with Regulations

Many regulations and security standards require organizations to regularly scan their web applications for vulnerabilities

Reduced Development Costs

Early detection of vulnerabilities during development is easier and cheaper to fix compared to patching them after a security breach.

Types of Web Application

Static application security test (SAST)

- White-box security test
- Requires source code
- Finds vulnerabilities in the earlier stages of an SDLC
- Less expensive to fix vulnerabilities
- Can't discover runtime- and environment-related issues
- Supports all software

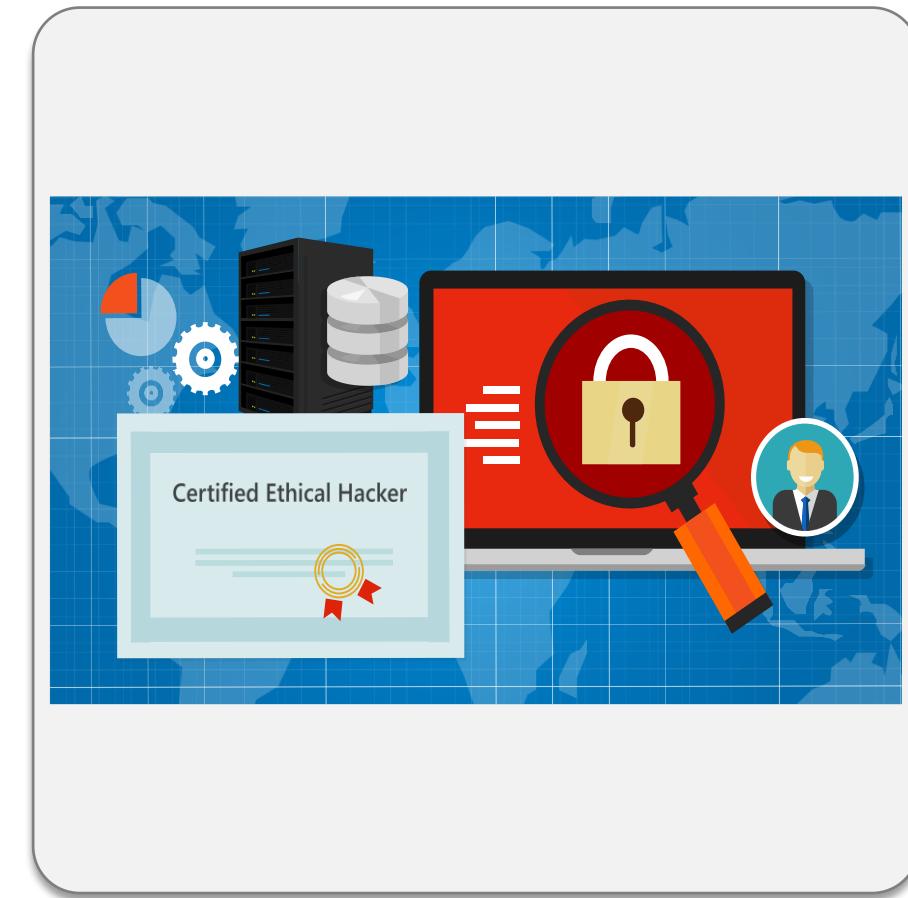
Dynamic application security test (DAST)

- Black-box security test
- Requires a running application
- Finds vulnerabilities towards the later stages of an SDLC
- More expensive to fix vulnerabilities
- Can discover runtime- and environment-related issues
- Predominantly deals with Web apps

Tools required: Acunetix, QualysGuard, and Burp Suite

Penetration Testing

It is also called pen testing or ethical hacking, is the practice of testing a computer system, network, or Web application to find security vulnerabilities that an attacker could exploit.

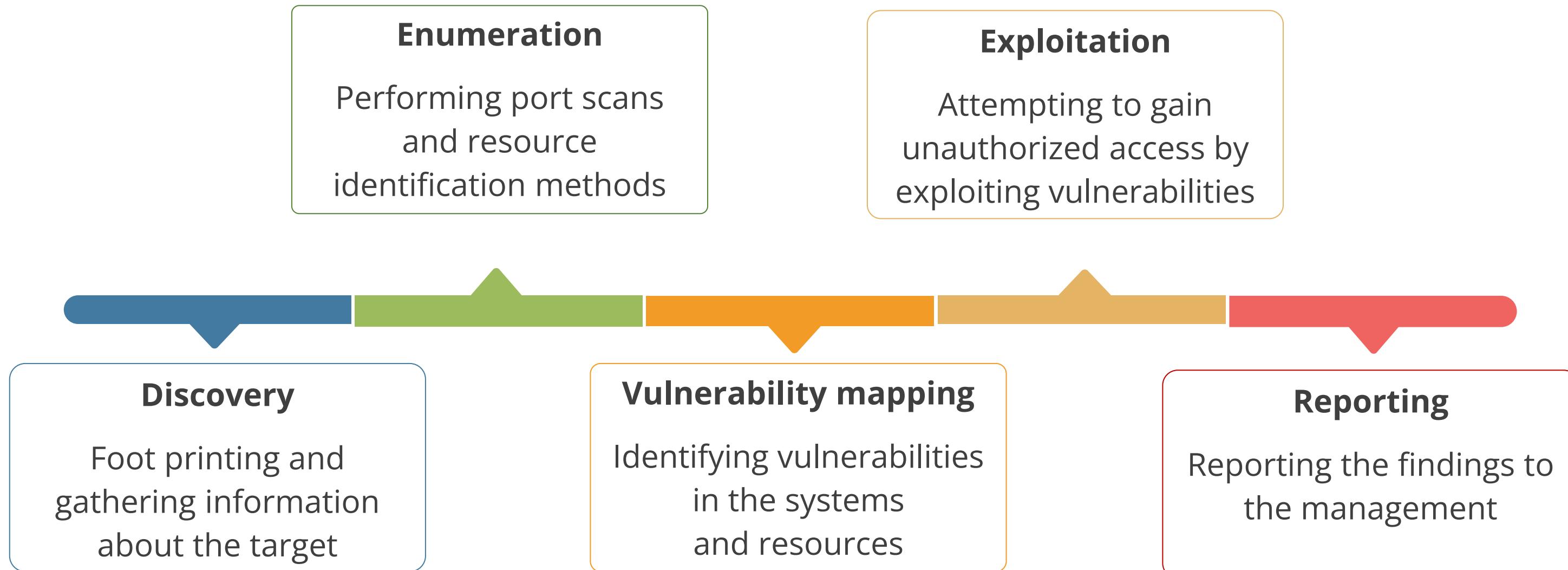


It is the process of determining the true nature and impact of a given vulnerability by exploiting existing vulnerabilities.

Tools required: Metasploit, Kali Linux, and Aircrack-ng

Penetration Testing Process

Phases of penetration testing:



Penetration Testing Types

Black-box testing (zero knowledge)

White-box testing (full knowledge)

Gray-box testing (partial knowledge)

Blind tests

Double blind types

Targeted

- The tester has no prior knowledge of the internal design or features of the system.
- It is the most accurate method to simulate an external attacker.
- It will probably not detect all vulnerabilities.
- The testing team may inadvertently impact another system.

Penetration Testing Types

Black-box testing (zero knowledge)

White-box testing (full knowledge)

Gray-box testing (partial knowledge)

Blind tests

Double blind types

Targeted

- The tester has complete knowledge of the internal system.
- It allows the test team to target specific internal controls and features.
- It may yield a more complete result.
- It may not be representative of an external hacker.

Penetration Testing Types

Black-box testing (zero knowledge)

White-box testing (full knowledge)

Gray-box testing (partial knowledge)

Blind tests

Double blind types

Targeted

- Some information about internal working is given to the tester.
- It helps guide their tactics toward areas that need to be thoroughly tested.
- This approach mitigates the risks of the other two models.

Penetration Testing Types

Black-box testing (zero knowledge)

White-box testing (full knowledge)

Gray-box testing (partial knowledge)

Blind tests

Double blind types

Targeted

- The tester only has publicly available data to work with.
- The network security team has prior knowledge of this test to defend against an attack.

Penetration Testing Types

Black-box testing (zero knowledge)

White-box testing (full knowledge)

Gray-box testing (partial knowledge)

Blind tests

Double blind types

Targeted

- It is also known as stealth assessment.
- It is a blind test to both the tester as well as the security team.
- It is used to evaluate the security levels and responses of the security team.
- It is a realistic demonstration of the likely success or failure of an attack.

Penetration Testing Types

Black-box testing (zero knowledge)

White-box testing (full knowledge)

Gray-box testing (partial knowledge)

Blind tests

Double blind types

Targeted

- It involves external and internal parties carrying out a focused test on specific areas of interest.

Vulnerability Disclosure and Incentive Programs

Programs designed to identify, report, and remediate security vulnerabilities, often providing incentives or recognition to those who responsibly disclose them.

Below are two important programs under this category:

Responsible Disclosure
Program

Bug Bounty Program

Responsible Disclosure Program

It is a framework that encourages the ethical reporting of security vulnerabilities.



It outlines the procedures for external security researchers to report vulnerabilities they have discovered in a company's software or systems.

Bug Bounty Program

It is a specialized type of responsible disclosure program that offers financial incentives to security researchers for discovering and reporting software vulnerabilities.



Organizations host these programs to crowd source the identification of security flaws in their software, systems, or online services.

TECHNOLOGY

System and Process Audit

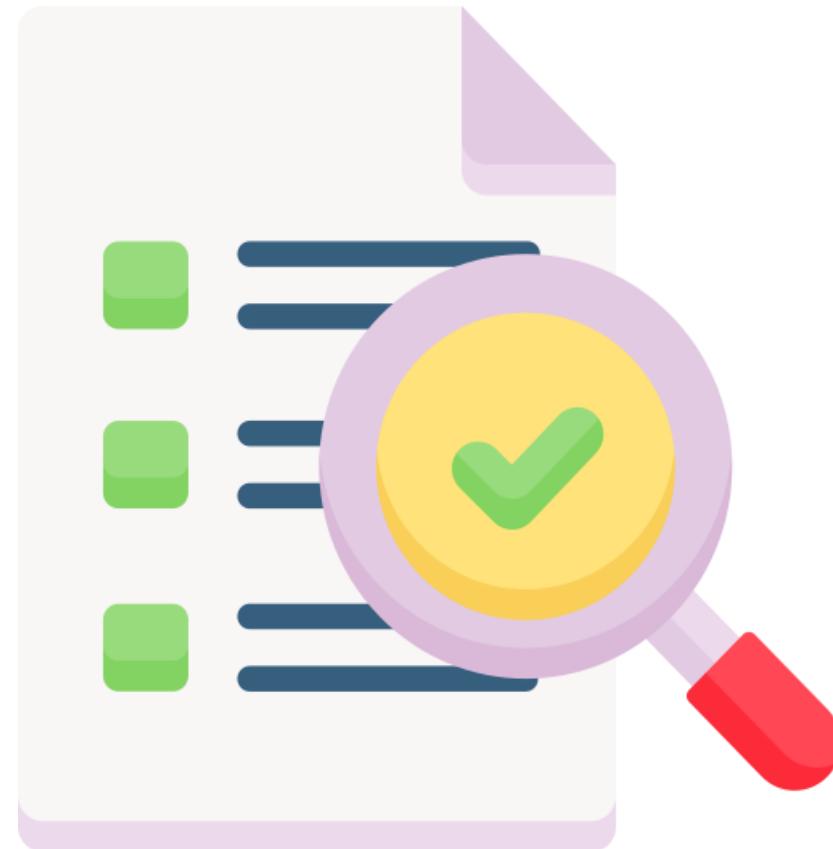
What Is Audit?

- It is a systematic, repeatable process, where a competent, independent professional evaluates one or more controls, interviews personnel, obtains and analyzes evidence, and develops a written opinion on the effectiveness of the control(s).
- The purpose of a risk audit is to provide reasonable assurance that adequate risk controls exist and are operationally effective.

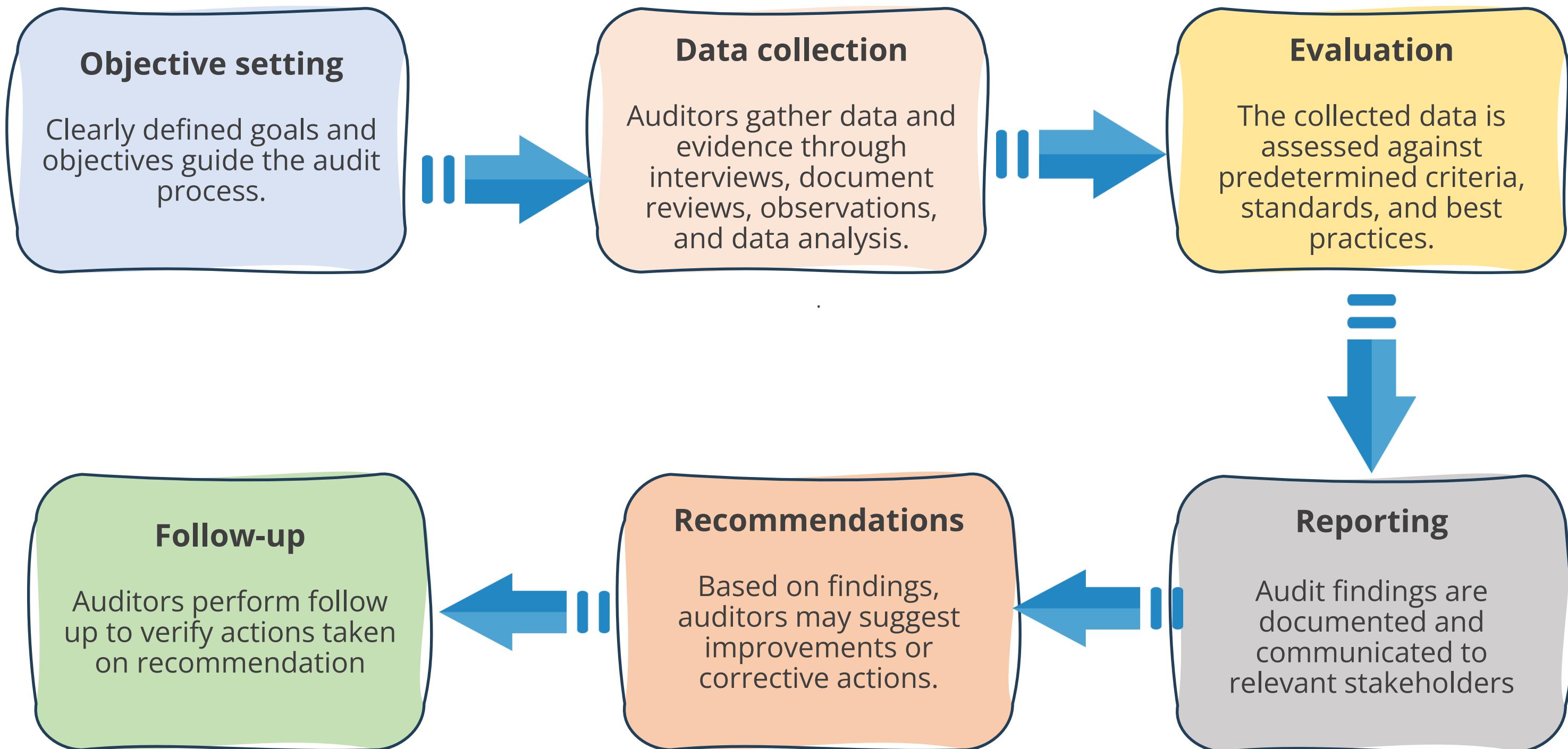


System and Process Audit

- A System and process audits are systematic evaluations conducted to assess the effectiveness, efficiency, security, and compliance of an organization's operational systems, workflows, and protocols with applicable regulations.
- These audits delve deep into the intricate workings of an organization to identify areas for improvement, verify compliance, and mitigate risks.



System and Process Audit



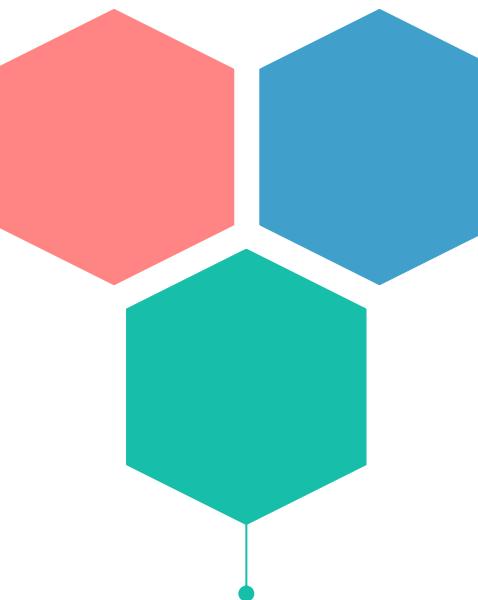
Why System and Process Audit matters?

Identify inefficiencies

Audits uncover bottlenecks, redundancies, and inefficiencies within processes, allowing organizations to streamline operations.

Ensure Compliances

Organizations must adhere to various regulations and industry standards. Audits help verify compliance and avoid legal consequences.



Enhance quality

By evaluating processes and systems, audits lead to improved product and service quality.

Vulnerability Analysis

It is a central component in cybersecurity that balances data collection and actionable decision-making.



Analysis transforms raw data about vulnerabilities and threats into comprehensive insights.

Confirmation of Vulnerabilities

It involves a rigorous process to validate suspected vulnerabilities. Analysts confront false positives and false negatives, reflecting the accuracy of prior vulnerability assessments.

False positive:

A false positive can act as a smokescreen, hiding a real issue by overwhelming a security team with false alarms.

False negative:

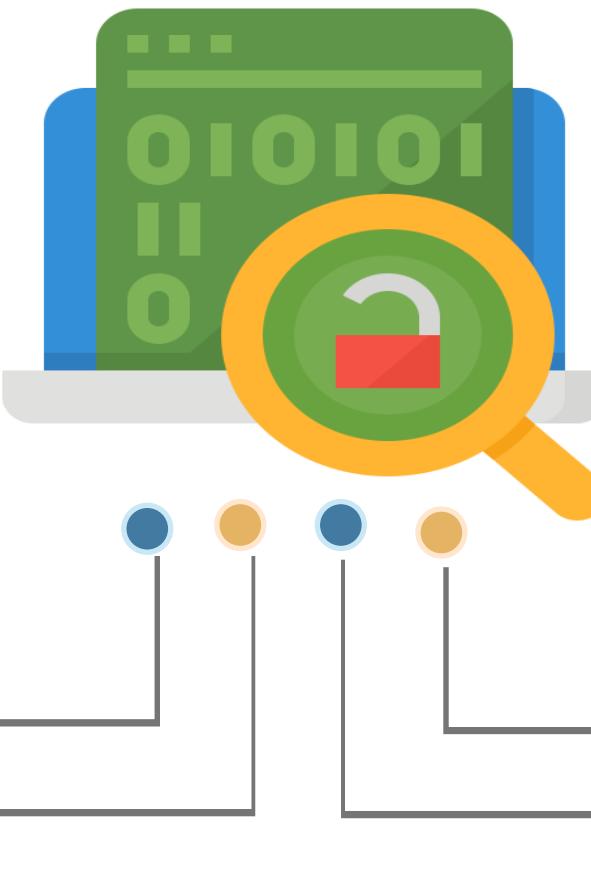
A false negative could be even more damaging, serving as a ticking time bomb for unauthorized access to critical systems.

Vulnerability Classification

It refers to the organized categorization of identified vulnerabilities within a system or application, usually based on criteria such as the nature of a vulnerability, the level of risk it poses, the component affected, or the potential impact



Vulnerability Classification Factors



Exposure Factor:
It quantifies the potential loss percentage from a successful attack.

Environmental Variable:
Environmental variables like infrastructure, industry, and regulations influence the urgency of addressing vulnerabilities..

Industry Impact:
Different sectors face unique cybersecurity challenges; financial institutions protect customer data, and healthcare protects health data.

Risk Tolerance:
It is the level of risk an organization can bear. It combines vulnerability assessment with the organization's capacity to handle risk.

Prioritization

It is the process of categorizing vulnerabilities based on their potential impact and the severity of the risk they pose.



It is a complex juggling act that requires a deep understanding of cybersecurity principles and the organization's operational intricacies.

Common Vulnerability Scoring System (CVSS)

- It is a multifaceted tool that provides a robust mechanism for assessing vulnerabilities in a standardized way.
- It quantifies the nature and severity of software vulnerabilities, aiding security professionals and organizations in making informed decisions about risk mitigation.
- It is a standardized system for assessing the severity of vulnerabilities, according to factors such as the impact, exploitability, and ease of remediation.

Score	Rating
9.0-10.0	Critical
7.0-8.9	High
4.0-6.9	Medium
0.1-3.9	Low

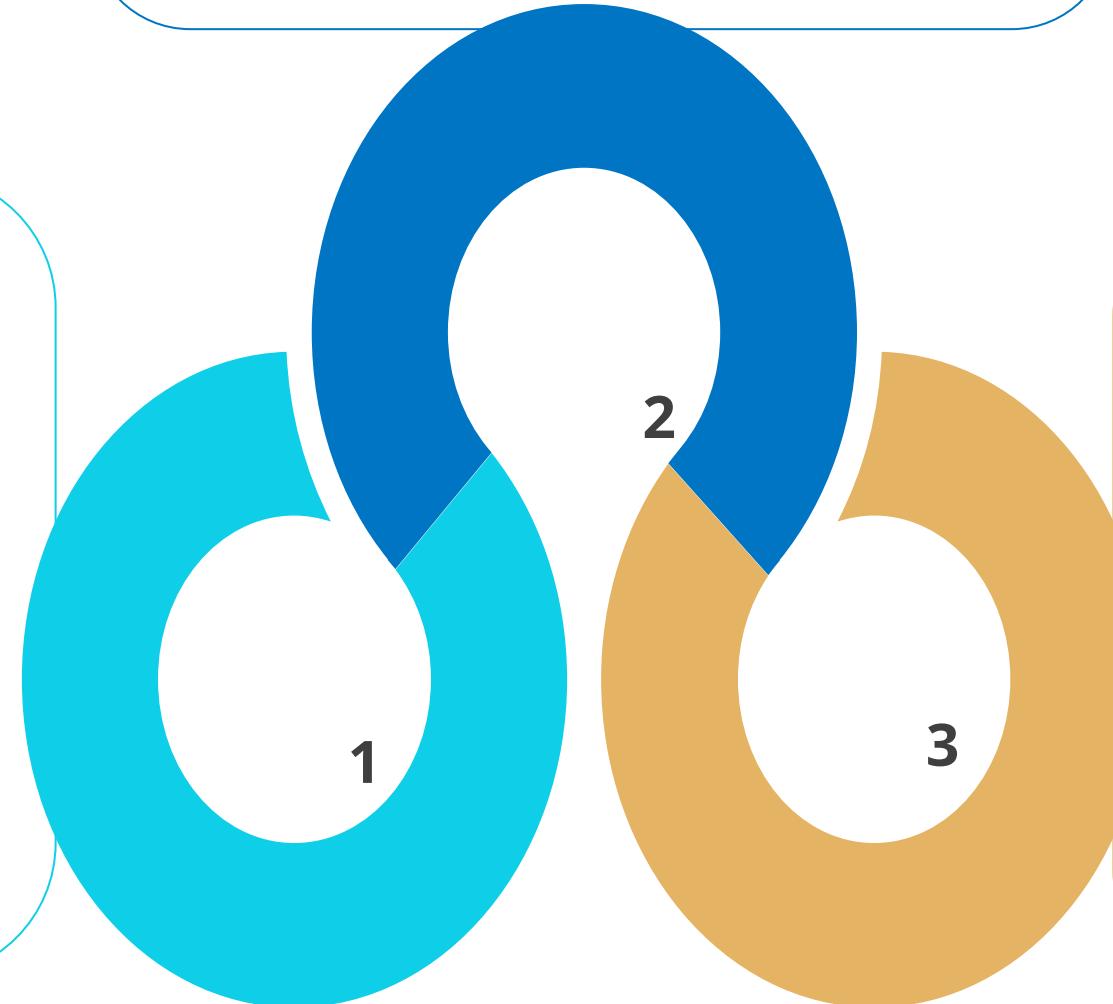
CVSS Scoring

Temporal Metric:

This layer examines the attributes of a vulnerability that may change over time, including exploit code maturity, remediation level, and report confidence.

Base Metrics:

These are inherent qualities of the vulnerability, like how it can be exploited and the potential impact on confidentiality, integrity, and availability. These metrics are independent of any specific system or environment.



Environmental group:

This layer allows an organization to tailor CVSS scores based on specific environmental characteristics, providing a customized risk assessment.

Common Vulnerabilities and Exposures (CVE)

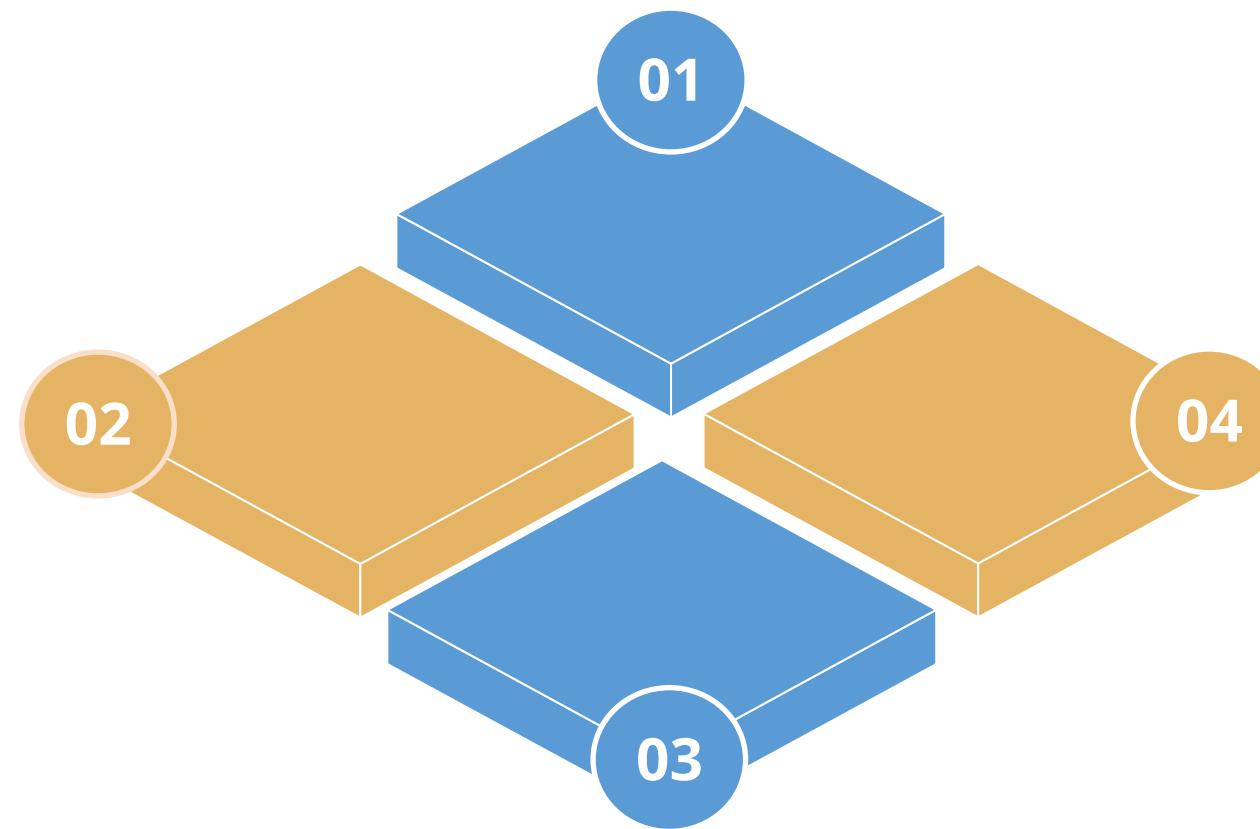
The CVE program identifies and catalogues publicly disclosed cybersecurity vulnerabilities, aiming to standardize their identification and improve communication and collaboration among cybersecurity professionals, software vendors, and other stakeholders.



CVE Details

Severity Score:

An indication of the vulnerability's severity using a scoring system like CVSS (Common Vulnerability Scoring System).



Description:

A detailed explanation of the vulnerability, its potential impact, and affected systems

Public References:

Links to additional resources like exploit code, vendor advisories, or mitigation strategies.

CVE ID:

A unique identifier in the format CVE-YYYY-NNNN (e.g., CVE-2023-4567).

Vulnerabilities Response and Remediation

Patching

It involves regularly updating software, applications, and systems to address known vulnerabilities. Timely patching is crucial, as it bolsters an organization's defense by closing security gaps that malicious actors may exploit.

Insurance

It serves as a financial safety net, providing coverage for potential losses resulting from cyber incidents.

Segmentation

It is a strategic approach to minimize the impact of a cyber breach. It involves dividing a network into isolated segments, limiting lateral movement for attackers, and containing potential breaches.

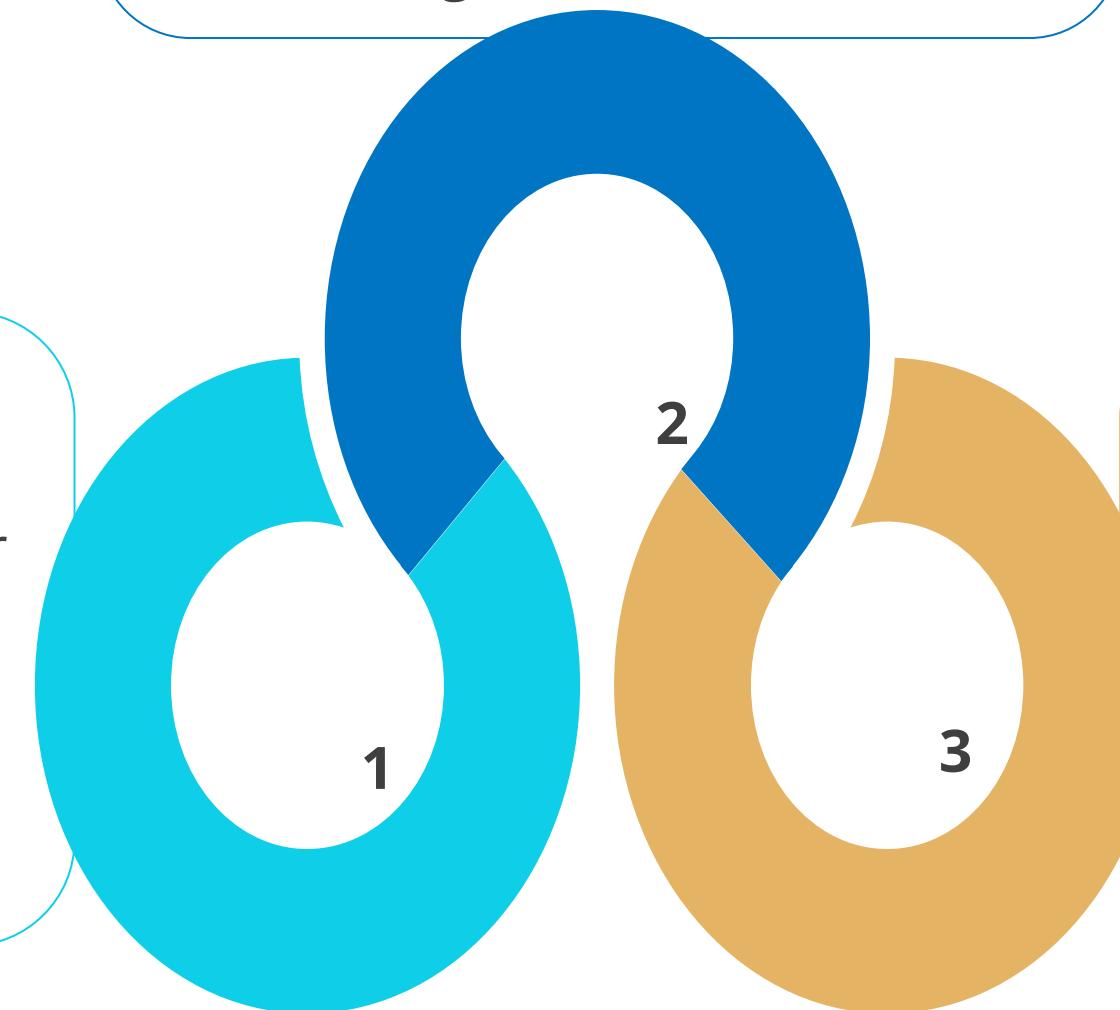
Validation of Remediation

Verification:

In the context of validation of remediation, involves ongoing monitoring and assurance that vulnerabilities remain mitigated over time.

Rescan:

It involves running vulnerability scans again after applying patches or making other changes. It's a way of proving that remediation efforts have worked.

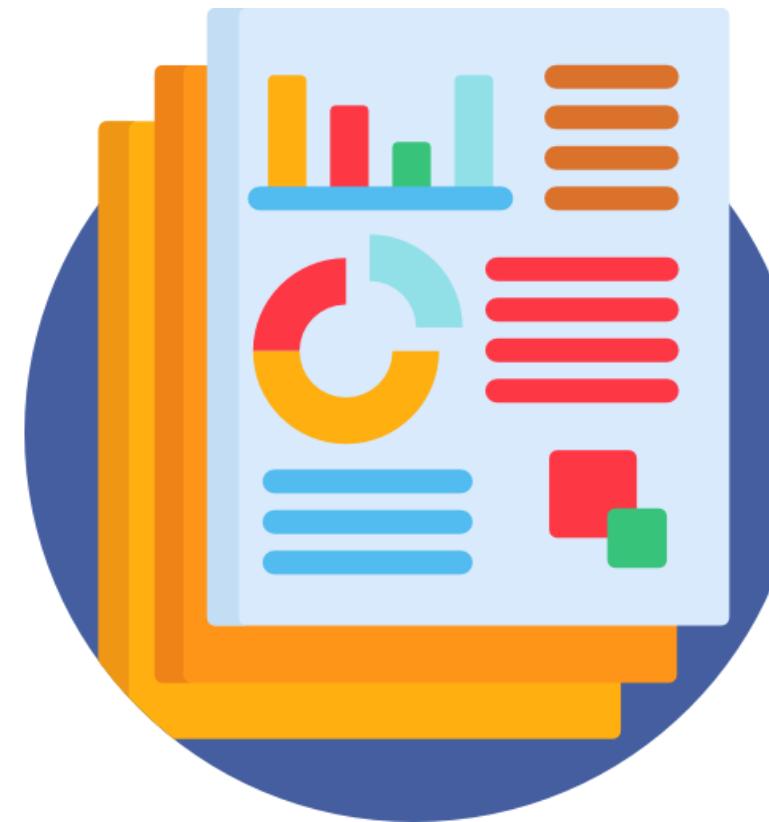


Audit:

It offers a thorough manual review by an independent third party or internal team, unlike automated rescans.

Reporting

It is a formal document that details security weaknesses in software applications, systems, or components.



These reports are generated by vulnerability scanning systems and serve as actionable insights and organizational memory for cybersecurity efforts.

Components of Reporting

Vulnerability overview

This is a summary of the current vulnerability landscape, including the total number of vulnerabilities, their severity distribution, and trends over time.

CVSS score

These relate detailed information on the varying levels of severity for identified vulnerabilities, and those of the highest priority that require immediate attention should be highlighted.

Remediation progress

This is an update on the status of remediation efforts, including the number of vulnerabilities addressed and those still pending.

Risk metric

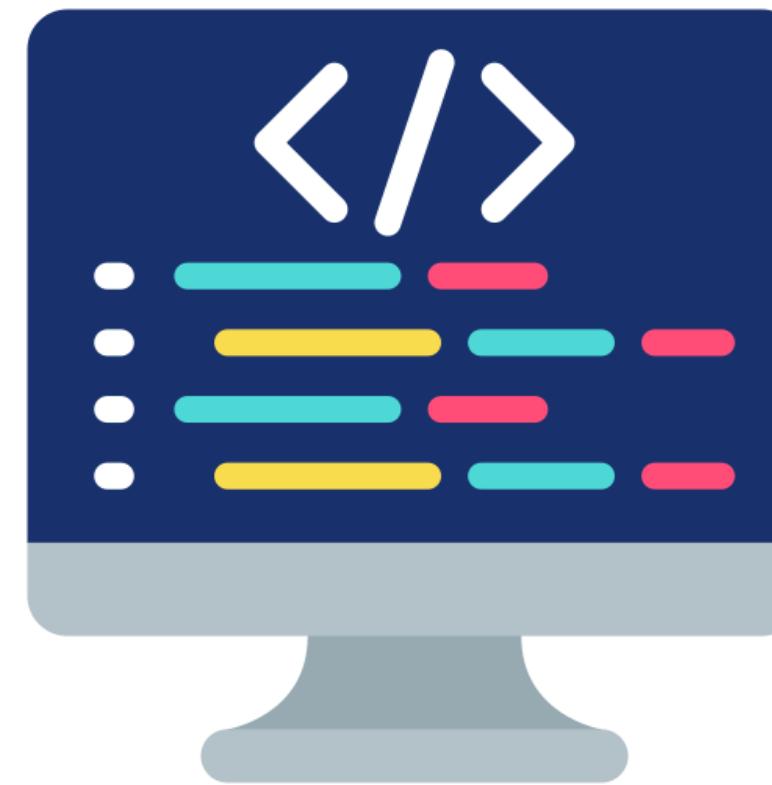
The report should include metrics by which to measure vulnerability management activities that have contributed to reducing the organization's overall cybersecurity risk.

Recommendation

Clear recommendations on the prioritization and allocation of resources for vulnerability remediation efforts should also be provided.

What Is Package

It refers to a software component or module that is used within an application.

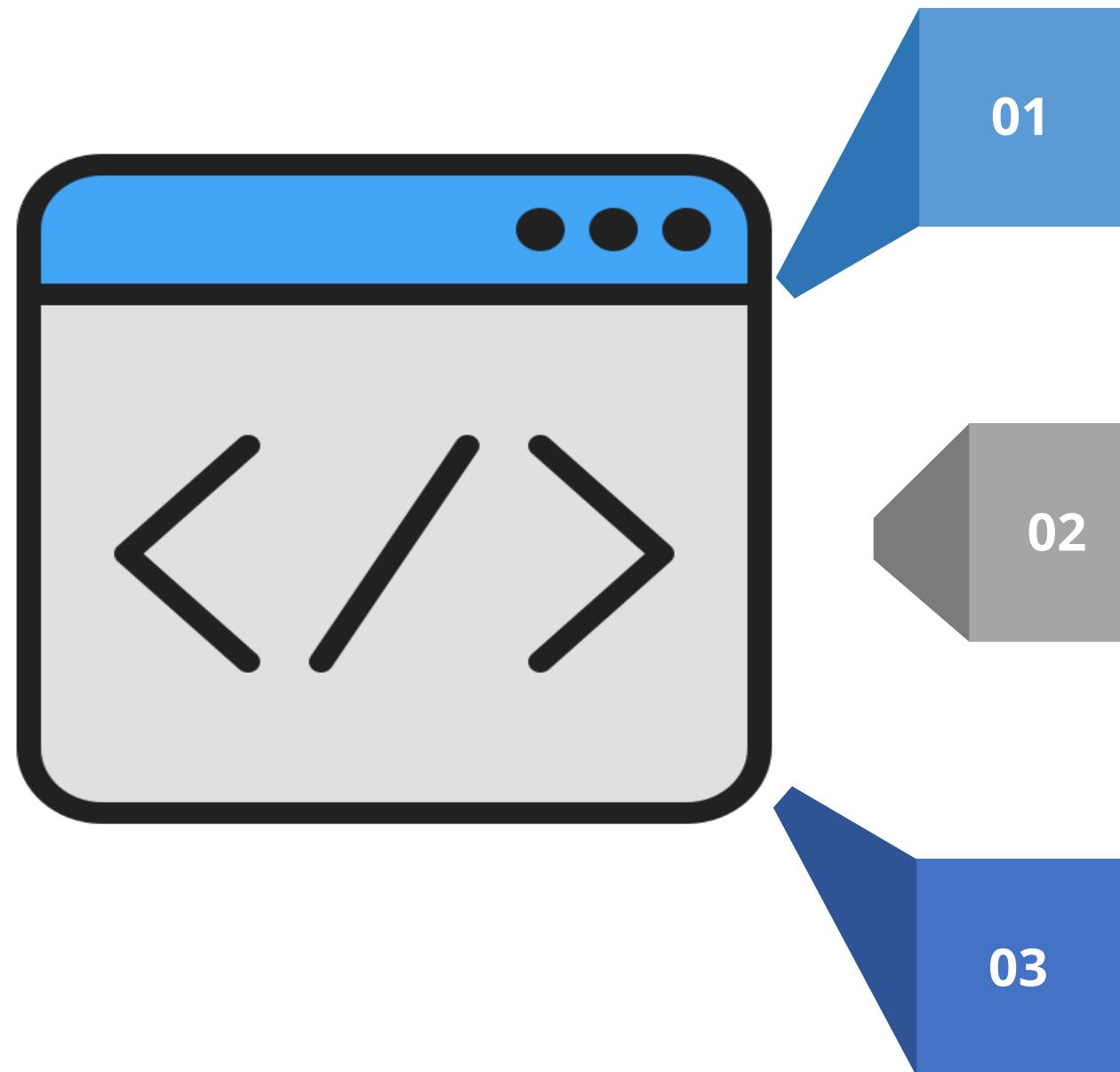


These packages can include libraries, frameworks, plugins, or other pieces of code that are integrated into an application to provide specific functionality.

Package Monitoring

- It involves continually surveilling third-party software packages and libraries that an application incorporates.
- It refers to monitoring the status and management of software packages within the application itself.
- Complexity arises because some organizations use many of these packages without understanding the security ramifications.
- Imagine it as keeping tabs on the health and performance of the building blocks that make your application work.

Attributes to Be Monitored



Installation and updates: Tracks the installation status of different packages within the application

Package dependencies: Applications often rely on other software packages to function properly. Package monitoring ensures all the necessary dependencies are met and any conflicts between packages are identified

Package health: Monitors the health and functionality of the software packages. This might involve checking for errors, compatibility issues, or resource usage.

Package Monitoring Implementation Tools



Package managers

Many languages and frameworks have package managers for installation, updates, and dependency management, with monitoring features.

Examples include npm (Node.js) and pip (Python).

Application monitoring tools

Application package monitoring tools focus on monitoring the software packages used within an application.

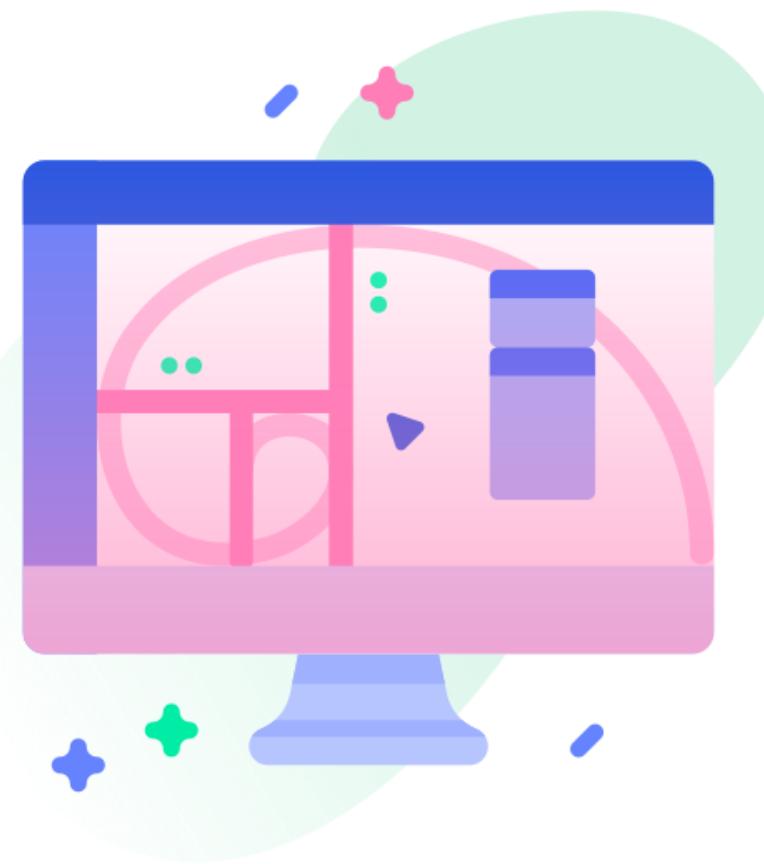
For example:
NPM (Node Packet Manager), SNYK.

Custom monitoring scripts

Developers can write custom scripts to track specific package-related metrics and generate alerts for potential issues.

Software Component Analysis (SCA)

It is used in application security to analyze software components.



It helps developers identify and address risks in third-party components to build secure, compliant, and robust applications

Functionalities of SCA

Component identification: SCA tools meticulously examine your application's codebase to identify all the software components used. These components can include libraries, frameworks, and other pre-written modules.

Risk analysis: Once the components are identified, SCA tools analyze them for potential risks.

Security vulnerabilities: They check if the identified components have known security weaknesses that attackers could exploit.

License compliance: SCA tools verify that the licenses of the used components are compatible with your project's licensing terms.

Outdated components: They identify components with outdated versions that might lack security patches or bug fixes.

SCA Benefits

Improved security posture

By identifying and addressing vulnerabilities in third-party components, SCA helps you build more secure applications.

Enhanced license compliance

SCA ensures you're using components according to their license terms, avoiding potential legal issues

Reduced development costs

Proactive identification of vulnerabilities or licensing conflicts can prevent costly remediation efforts later in the development process.

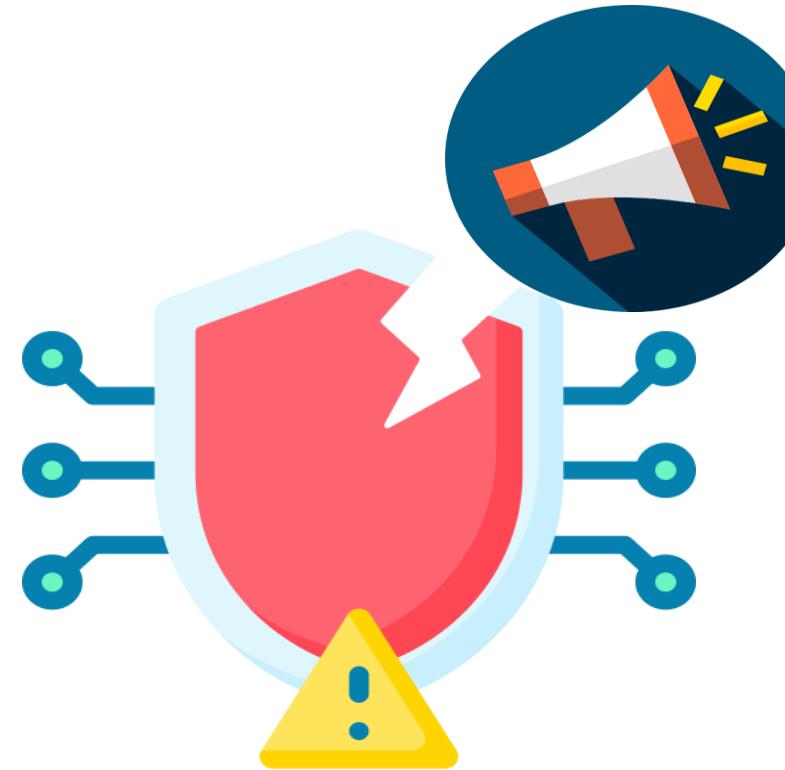
Streamline development process

SCA tools can automate many aspects of component analysis, saving developers time and effort



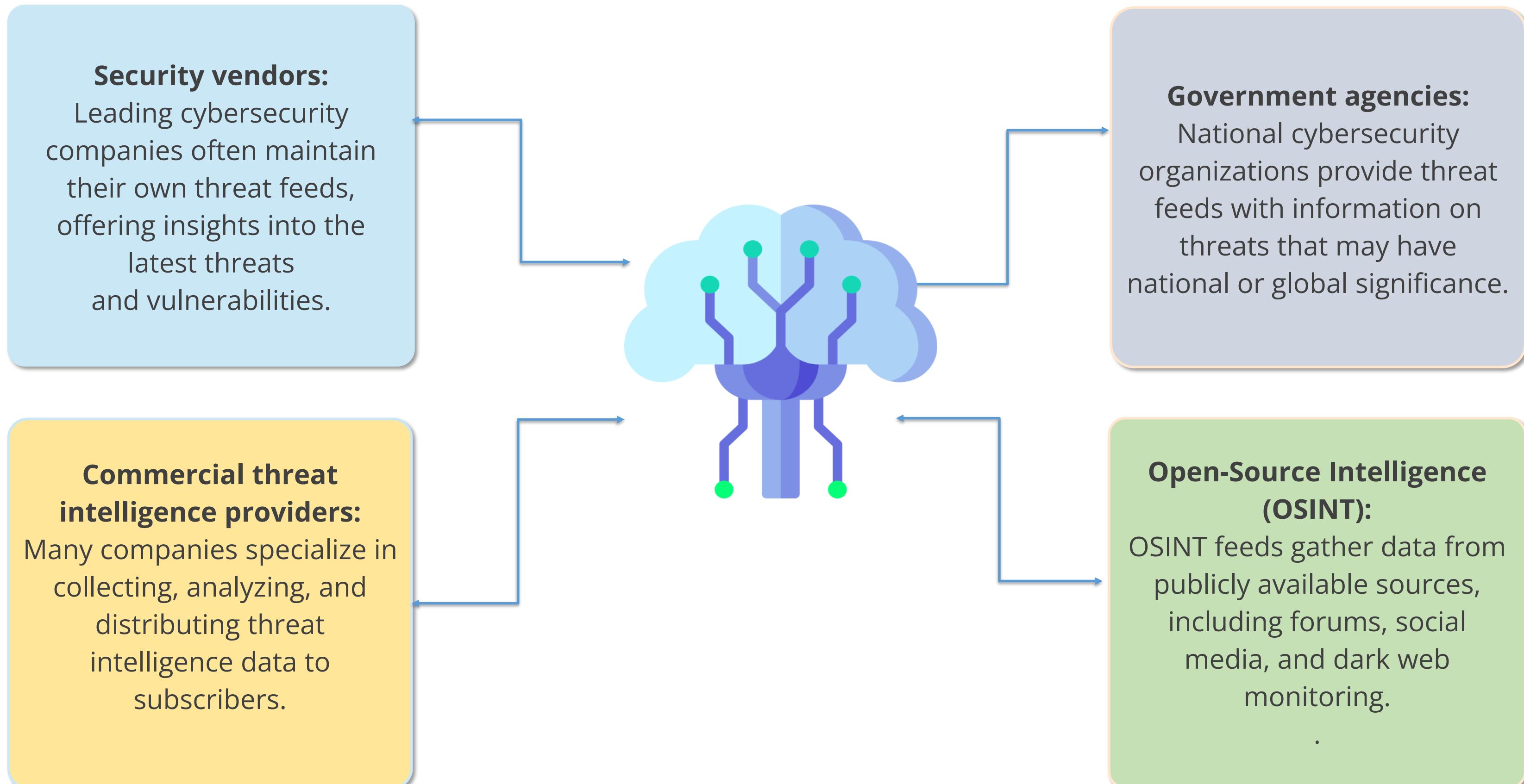
Threat Feeds

They are continuous data streams that provide information about the latest cyber threats and suspicious activities, serving as a valuable resource for security teams to detect and prevent cyberattacks.



They are crucial for security teams, providing real-time information to proactively defend against cyberattacks.

Types of Threat Feeds



OSINT

- OSINT stands for Open-Source Intelligence. It is the practice of gathering and analyzing information from publicly available sources to gain valuable insights.
- It is a powerful technique for gathering valuable information from publicly available sources.
- By effectively using OSINT, individuals and organizations can gain insights, make informed decisions, and achieve their goals
- Think of it like detective work using only publicly available clues

OSINT Sources

Websites and forums

Public websites, forums, and social media can reveal potential vulnerabilities, hacker discussions, and emerging threats.

News and media

News outlets report on data breaches, cyberattacks, and vulnerabilities, offering insights into the latest developments.

Government reports

Government agencies, like US-CERT, release reports on vulnerabilities and threats.

Blogs and research paper

Security researchers share their findings in blogs and research papers, offering insights into vulnerabilities and exploitations.

Proprietary or Third-Party Feeds

- It is a specialized channel that may require a subscription. Unlike OSINT, these feeds are curated and may include analysis of a threat's impact.
- For instance, a bank could subscribe to a service like Recorded Future or FireEye to get tailored data on threats aimed explicitly at financial institutions.
- It involves numerous vendors, including industry stalwarts such as FireEye, Symantec, and Recorded Future.
- These vendors offer a vast array of threat data feeds and reports that organizations can use to fortify their defenses.



Third-Party Source of Intelligence

Structured Threat Information Expression(STIX)

- STIX is a standardized language and format for representing structured threat information.
- It provides a common ground for expressing and sharing threat intelligence consistently.
- Organizations and vendors can use STIX to package and exchange data on threats, vulnerabilities, and incidents.

SHODAN

- It is a search engine for the Internet of Things (IoT) and connected devices. SHODAN scans the web, indexing information about internet-connected devices and services, including open ports, vulnerabilities, and configurations.
- SHODAN's data can be invaluable for organizations seeking to understand their external attack surface.

Information-Sharing Organization (ISO)

- Information-sharing organizations and groups such as information sharing, and analysis centers (ISACs) serve as hubs where companies can contribute and receive threat information.
- Their primary mission is to facilitate the exchange of threat intelligence, insights, and best practices among members.
- ISOs serve as a nexus for collective wisdom to transform this intelligence into actionable defense strategies.



Data Shared by ISA

Indicators of Compromise (IOCs): This is the information left by cyber attackers. IOCs include malicious IP addresses, malware signatures, and suspicious URLs.

Tactics, Techniques, and Procedures (TTPs): ISOs offer a deeper understanding of the methods employed by threat actors, including attack patterns and behavior.

Incident data: This refers to narratives of past and ongoing cyber incidents, offering context and actionable insights to defenders.

Different Cyber Sharing Agencies

Cyber Threat Alliance

CTA is a coalition of cybersecurity organizations and companies that work together to share cyber threat intelligence and improve global defenses against cyber threats.

Automated Indicator Sharing(AIS)

AIS is a program led by the US government that enables the sharing of cyber threat indicators and defensive measures with authorized organizations.

Forum of Incident Response and Security Teams

FIRST is a global organization that brings together incident response and security teams from various industries and regions.

Information Sharing and Analysis center(ISACs)

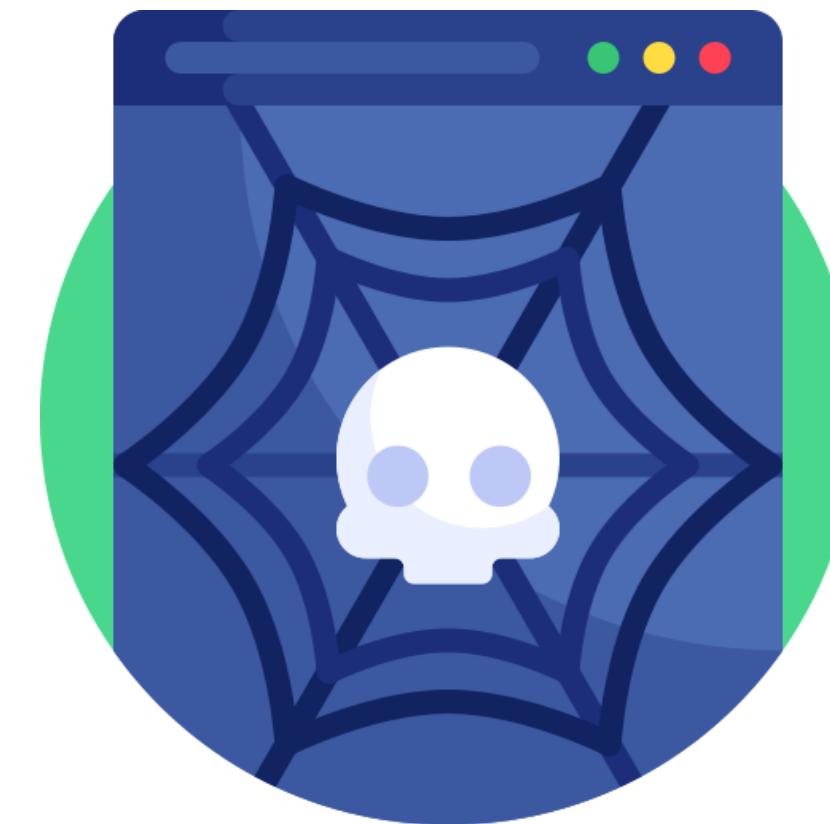
ISACs are sector-specific organizations that focus on sharing cyber threat intelligence within specific industries or critical infrastructure sectors.

Multi-State information Sharing and Analysis Center

Secure and reliable access to applications from anywhere, on any device.

Dark Web

It is known for its anonymity and association with illicit activities, and It can only be accessed using specialized software, with the Tor network being the most well-known.



It is a hidden part of the internet that isn't indexed by traditional search engines.

Dark Web

Anonymity:

The dark web prioritizes anonymity, accessed through software like Tor that anonymizes internet traffic.

Hidden addresses:

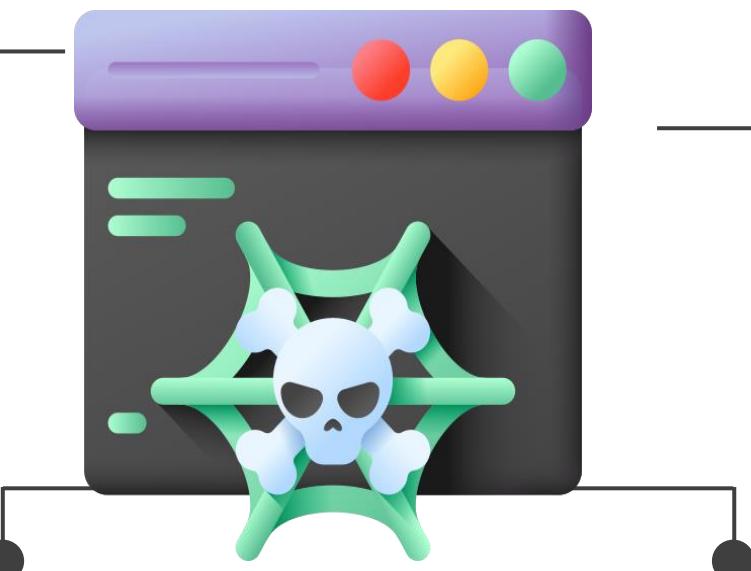
Websites on the dark web use ".onion" addresses instead of ".com" or ".net," and are not indexed by search engines.

Special software for access:

The dark web requires special software, as traditional browsers like Chrome or Firefox cannot access it.

Content:

Security researchers share their findings in blogs and research papers, offering insights into vulnerabilities and exploitations.



Scanning Local VM Using Nessus



Duration: 10 Min.

Problem Statement:

As a cybersecurity analyst, you are tasked with conducting vulnerability scans on a local Windows virtual machine using Nessus. This involves installing and configuring Nessus, scanning the target machine for vulnerabilities, and generating a report that visualizes the identified vulnerabilities and the necessary patches. The aim is to assess the security posture of the system and prioritize remediation efforts to enhance its security.

Note: Refer to the demo document for detailed steps:
[01_Scanning_Local_VM_using_Nessus](#)

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Install the Nessus vulnerability scanner
2. Configure Nessus
3. Prepare for scanning
4. Conduct a vulnerability scan
5. Review scan results

Security Alerting and Monitoring Concepts and Tools

Monitoring and Alerting of Systems and Infrastructure

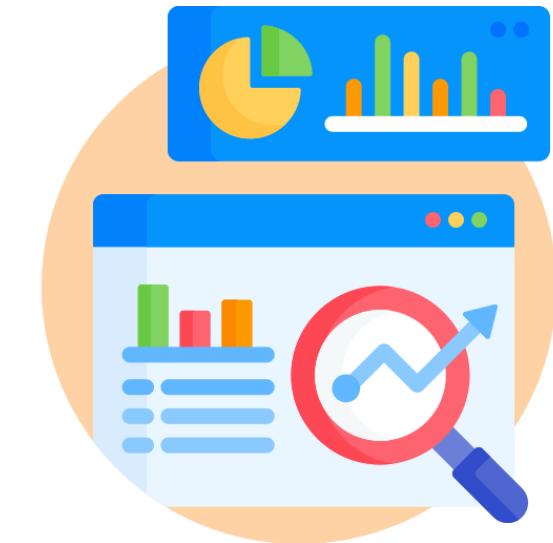
Monitoring IT systems involves the continuous tracking and analysis of various aspects of an organization's IT infrastructure, including hardware, software, network performance, security, and application functionality.

- Monitoring computing resources involves the continuous oversight of an organization's IT assets to ensure they operate within expected parameters.
- This process includes the tracking of systems, applications, and infrastructure, each presenting its own set of challenges and essential metrics.



Monitoring Computing Resources

- Security alerting and monitoring safeguard digital assets and sensitive information, involving continuous observation and analysis to identify and respond to security threats in real time.
- The goal is to minimize the risks of data breaches, unauthorized access, and system vulnerabilities.

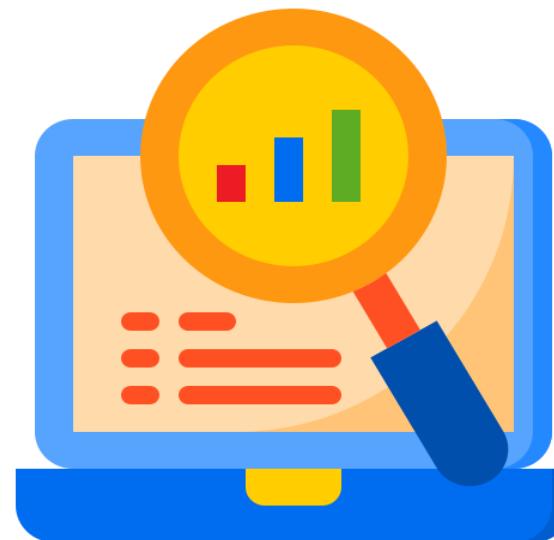


Things to Be Monitored

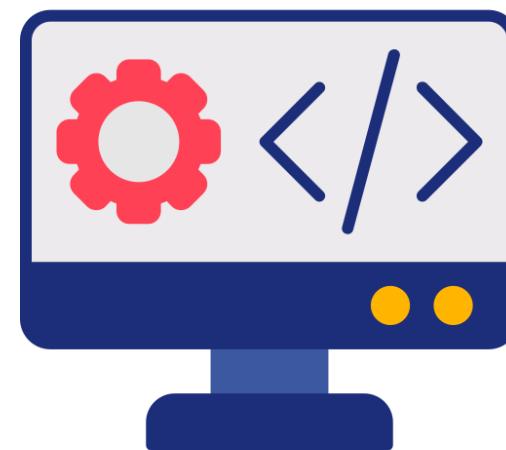
The goal is to minimize the risks of data breaches, unauthorized access, and system vulnerabilities by closely reviewing the following:



Security logs



System monitoring



Application monitoring



Infrastructure monitoring

Things to Be Monitored

Security logs

- Security logs record all authorized and unauthorized access to resources and privileges.
- These logs serve a dual function: acting as an audit trail of user actions and offering preemptive warning against potential intrusion attempts when regularly monitored.
- The security of a network heavily relies on the comprehensive and timely review of these logs.

System monitoring

- Systems refer to the servers, workstations, and endpoints that make up an organization's network.
- Monitoring systems involves keeping a vigilant eye on performance metrics such as CPU usage, memory utilization, and network traffic.
- By establishing baselines and thresholds, security teams can detect anomalies that might indicate a security breach or system failure.

Things to Be Monitored

Application monitoring

- Applications are software programs that enable users to perform various tasks on their computers and devices. Monitoring applications involves tracking their performance, availability, and security.
- Security teams use specialized tools to monitor application logs, error messages, and user activity.
- Anomalies in application behavior, such as unexpected data access or a sudden surge in traffic, can indicate a security incident.

Infrastructure monitoring

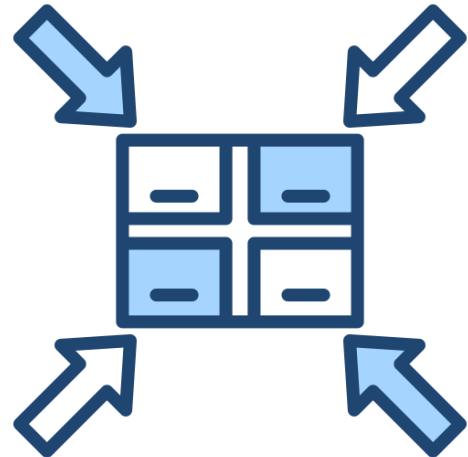
- Infrastructure encompasses the network components, databases, and cloud services that support an organization's digital operations.
- Monitoring infrastructure involves ensuring the integrity and availability of these critical resources with tools including network monitoring software, database activity monitoring, and cloud security solutions.
- Security teams rely on comprehensive monitoring to detect and respond to potential infrastructure vulnerabilities and issues.

What Is Logging?

- Logging is the process of recording information about system events, errors, warnings, and other relevant data for later analysis.
- Logging is essential for identifying and resolving issues by analyzing past logs, aiding in performance monitoring, and ensuring adherence to regulations by maintaining audit trails.



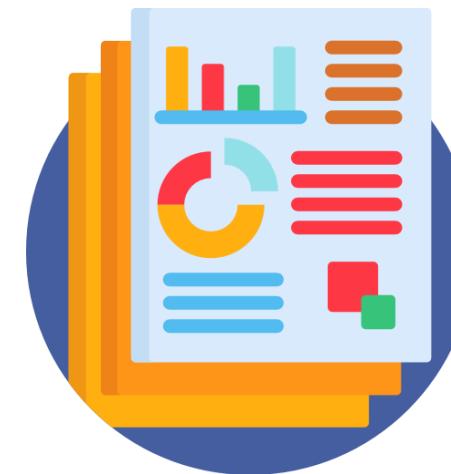
Core Logging Activities



Aggregate logs



Log alerts



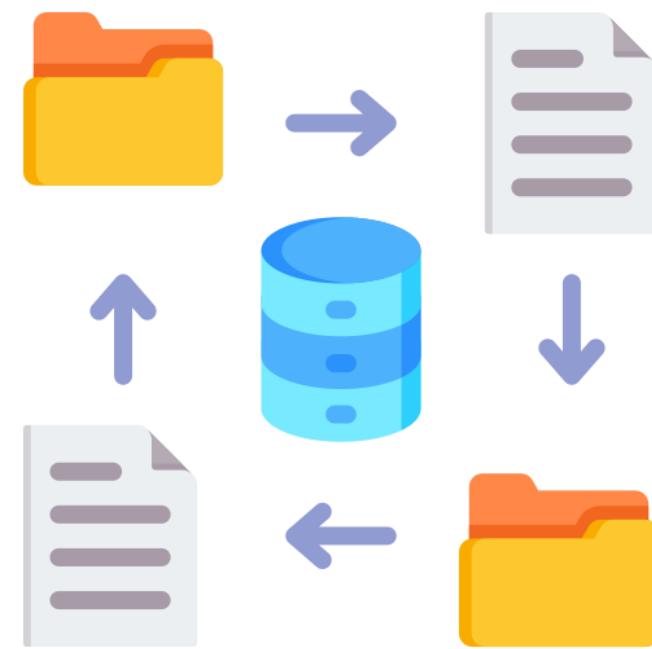
Generate reports



Archive data

Log Aggregation

- Log aggregation involves gathering disparate log data from various sources, such as servers, applications, databases, and network devices, and bringing the data into a single, centralized repository for examination.
- Specialized tools like syslog-ng and rsyslog manage and process log data, enabling real-time analysis and generating comprehensive reports.



Log Alerts

- Log alerts are automatic notifications triggered by specific conditions within log data. They serve as a real-time early warning system, notifying IT professionals of potential issues, security threats, or system anomalies.
- Rules and thresholds within security systems trigger notifications when specific conditions or events occur.
- Timely alerts empower cybersecurity professionals to investigate and mitigate threats, with IDSs, IPSs, and SIEM solutions notifying administrators of suspicious or unauthorized activities.



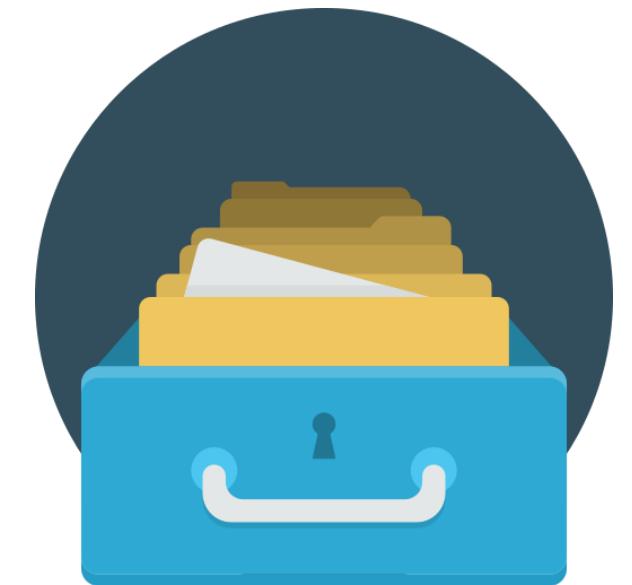
Reporting

- Reporting in cybersecurity translates technical information into a format that can be understood by both technical and senior management teams.
- For the technical team, it includes detected vulnerabilities and recommended actions. For senior management, it addresses potential business impact.
- Executive reports cover projected financial costs, potential reputational damage, and strategic risk mitigation recommendations.



Archiving

- Involves the secure storage of historical data, such as logs and reports, for long-term retrieval and analysis.
- Acts like a well-organized filing cabinet, allowing you to quickly find documents when you need to revisit an old case or validate compliance during an audit.
- Requires deciding what to archive and the duration, considering legal requirements and potential future analysis.
- Uses strong encryption to ensure data integrity, safeguarding information from tampering or accidental deletion.



Alert Response and Remediation or Validation

- Alert response and remediation are crucial in IT operations, ensuring a timely and effective response to potential issues identified by monitoring systems.
- It also serves as an alarm system for the Security Operations Center (SOC) to prompt necessary measures to prevent potential attacks. The following actions can be taken in response to alerts:



Quarantine



Alert tuning

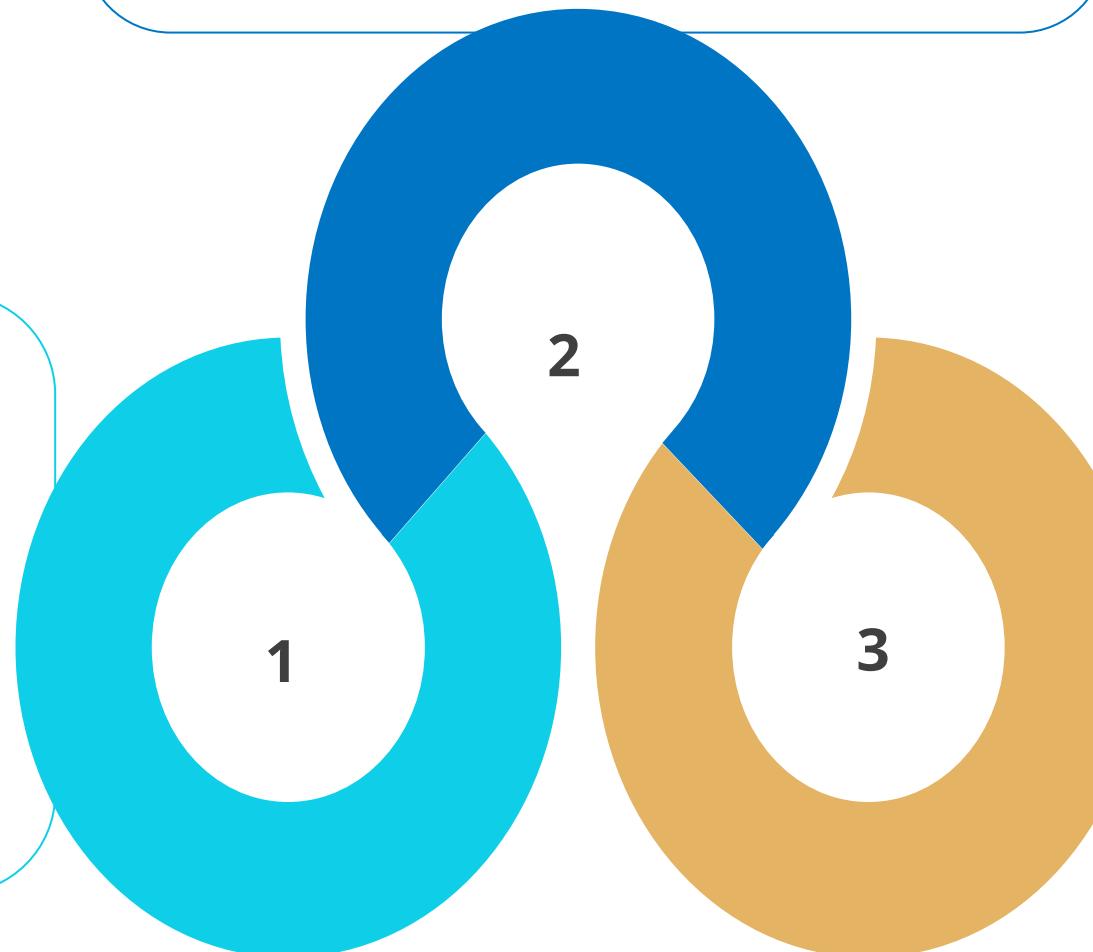
Quarantine

- Isolates potentially compromised systems or devices from the network to prevent further infection or compromise of other network assets.
- Applies to endpoints, servers, or network segments and is often used in response to alerts indicating potential malware infections or suspicious activity.



Key Activities of Quarantine

Automated response
Security tools are configured to automatically quarantine systems when specific conditions or alerts are triggered.



Manual intervention
Manual intervention is required to assess the situation before initiating quarantine.

Isolation duration
Isolation duration determines how long a system should remain in quarantine based on the severity of the alert and the steps taken for remediation.

Alert Tuning

- Optimizes security alerts to reduce noise, improve accuracy, and ensure that only actionable alerts are generated.
- Involves adjusting the thresholds, rules, and parameters used by security monitoring tools to trigger alerts that provide accurate assessments.
- Aims to strike the right balance between alert accuracy and coverage.



Tools for Logging and Monitoring



Security Content Automation
Protocol (SCAP)



Intrusion Detection System or Intrusion
Prevention System (IPS or IDS)



Antivirus



NetFlow

Tools for Logging and Monitoring



Vulnerability scanner



Data loss prevention



Simple Network Management Protocol
(SNMP)



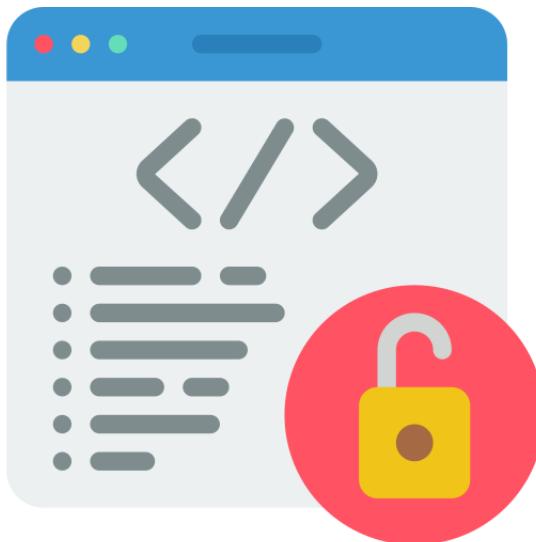
Security Information and Event
Management (SIEM)

Security Content Automation Protocol

- Enables compatible vulnerability scanners to determine whether a computer adheres to a predefined configuration baseline.
- Standardizes how information about software flaws, security configurations, and vulnerabilities is communicated and exchanged.
- Provides a common language for security tools and systems to share information about potential security risks.



SCAP Attributes



01

Standardized formats: Defines common formats for expressing information about vulnerabilities, security configurations, and patching information, ensuring different security tools can understand and utilize this data seamlessly

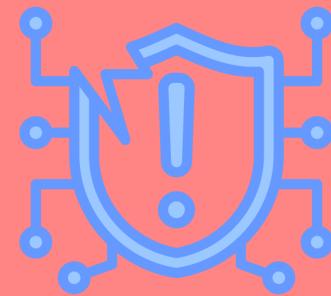
02

Automation: Facilitates the automation of vulnerability management tasks, allowing organizations to automate processes like vulnerability scanning, configuration assessment, and patch deployment

03

Open source and vendor-neutral: Is open-source and vendor-neutral, meaning it is not tied to any specific security product or vendor, allowing for interoperability between different security tools from various vendors

Components of SCAP



Open vulnerability and assessment language

Expresses information about vulnerabilities and system configurations in a structured, machine-readable format, facilitating interoperability between different security tools



Extensible configuration checklist description format

Provides a standard format like XCCDF for writing security checklists for computers and devices, allowing different security tools to understand these checklists

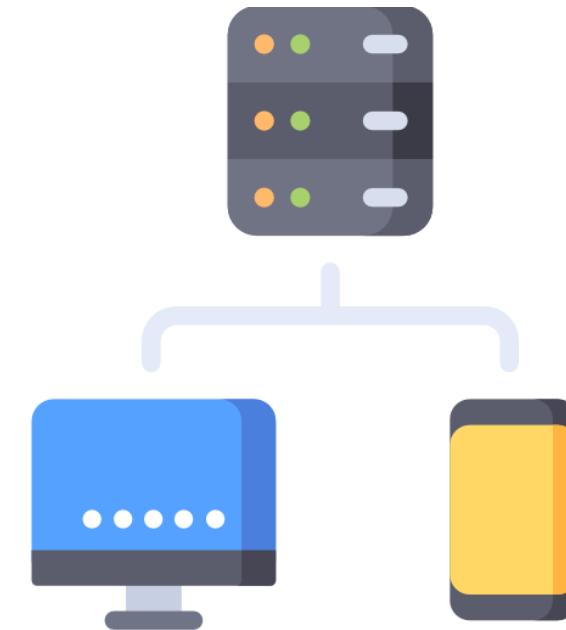


Common vulnerability scoring system (CVSS):

Uses an industry-standard scoring system to assess the severity of vulnerabilities, helping prioritize which vulnerabilities to address first based on their potential impact

What Is SNMP?

- SNMP stands for Simple Network Management Protocol
- It is a widely used protocol for managing and monitoring network devices like routers, switches, firewalls, printers, and more
- SNMP acts as a communication tool that allows network administrators to collect valuable information about their network devices and identify potential issues



Components of SNMP

SNMP agents

Software modules or processes running on network devices like routers, switches, servers, and IoT devices

SNMP managers

Centralized systems for monitoring and managing network devices, initiating SNMP requests to gather information from agents, and configuring and controlling devices

SNMP traps

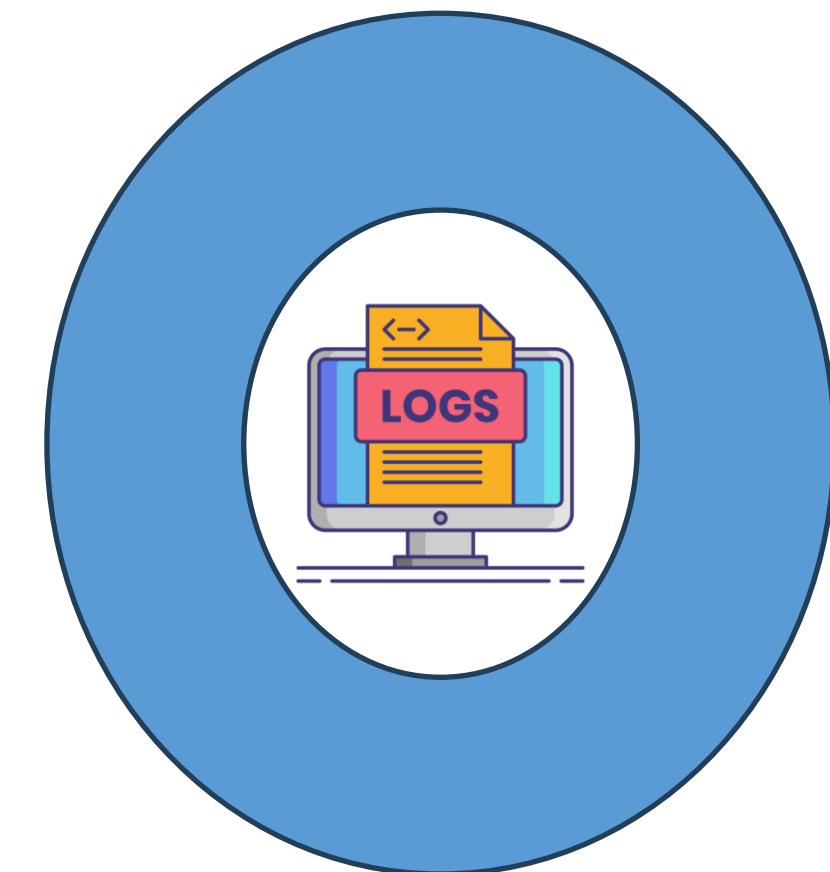
Asynchronous notifications sent by SNMP agents to managers without a prior request, informing managers of specific events or conditions like hardware failures, high resource utilization, or security issues

Management information base

MIB specifies the type of information that can be monitored or managed on a device, with each piece of information assigned a unique identifier called an Object identifier (OID)

SNMP Traps in Details

- Traps are alert messages sent from an SNMP-enabled device to a management station or system, to indicate a significant event or change in the device's status
- Unlike a polling mechanism, traps are initiated by the devices themselves and provide immediate notification without the delay of a polling cycle
- Currently, version 3 (v3) is preferred and recommended because versions 1 (v1) and 2 (v2) exchange traps in clear text, which is not secure. Details about v3 are described in the next slide



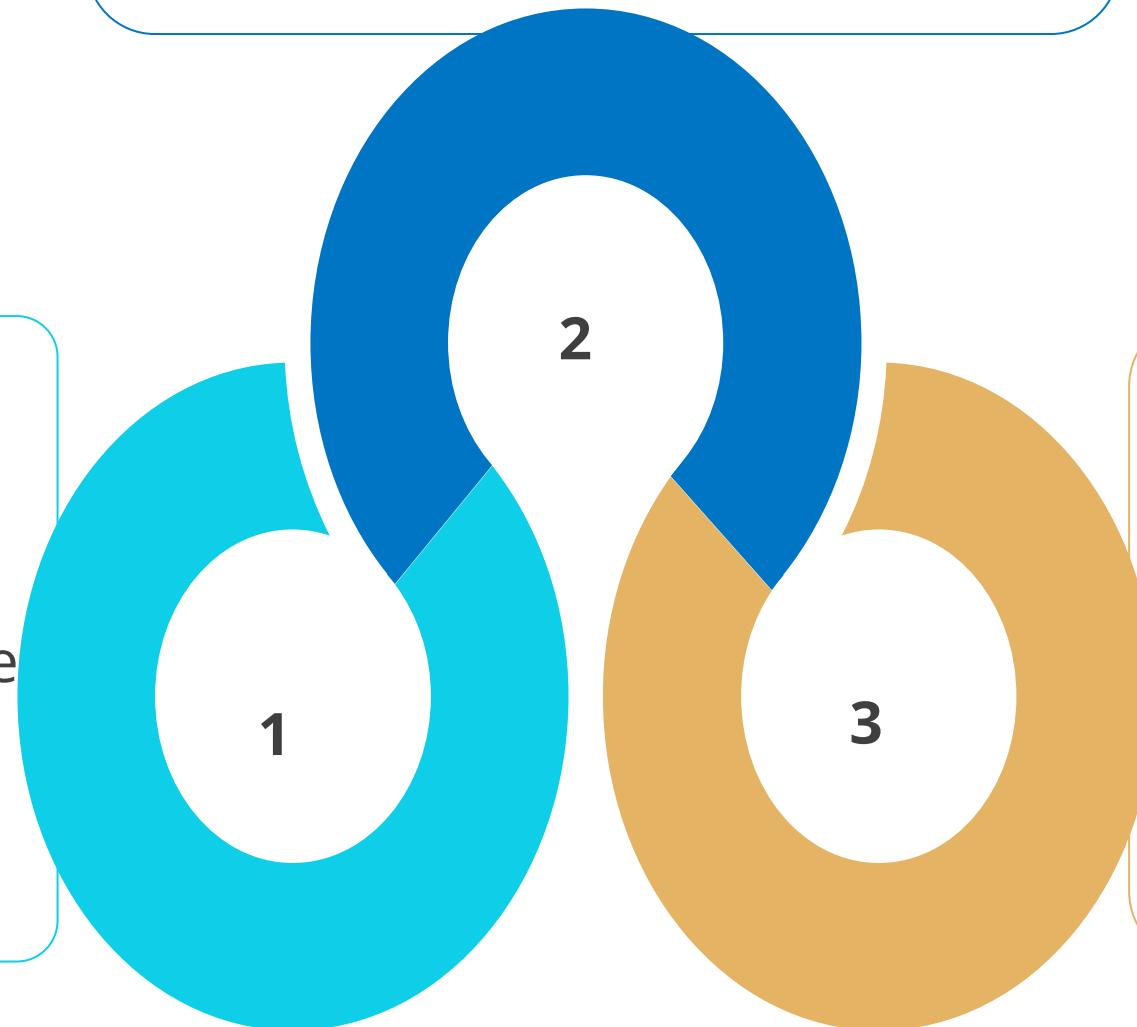
Attributes of SNMPv3

Authentication

Implements authentication protocols, such as HMAC-MD5 or HMAC-SHA, to confirm that a trap originates from a legitimate source

Message integrity

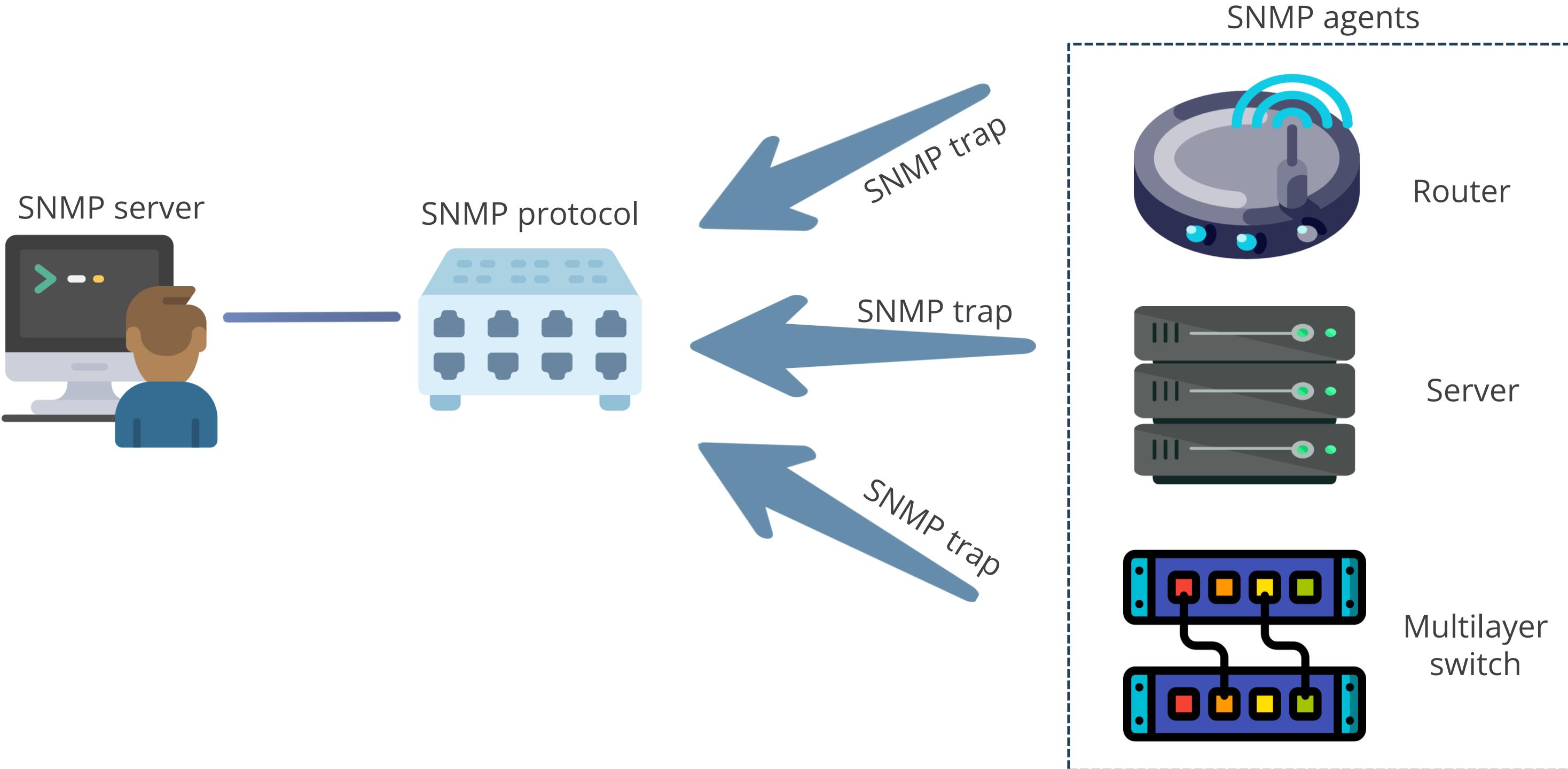
Includes a checksum within a trap message to ensure that the data has not been altered during transmission



Encryption

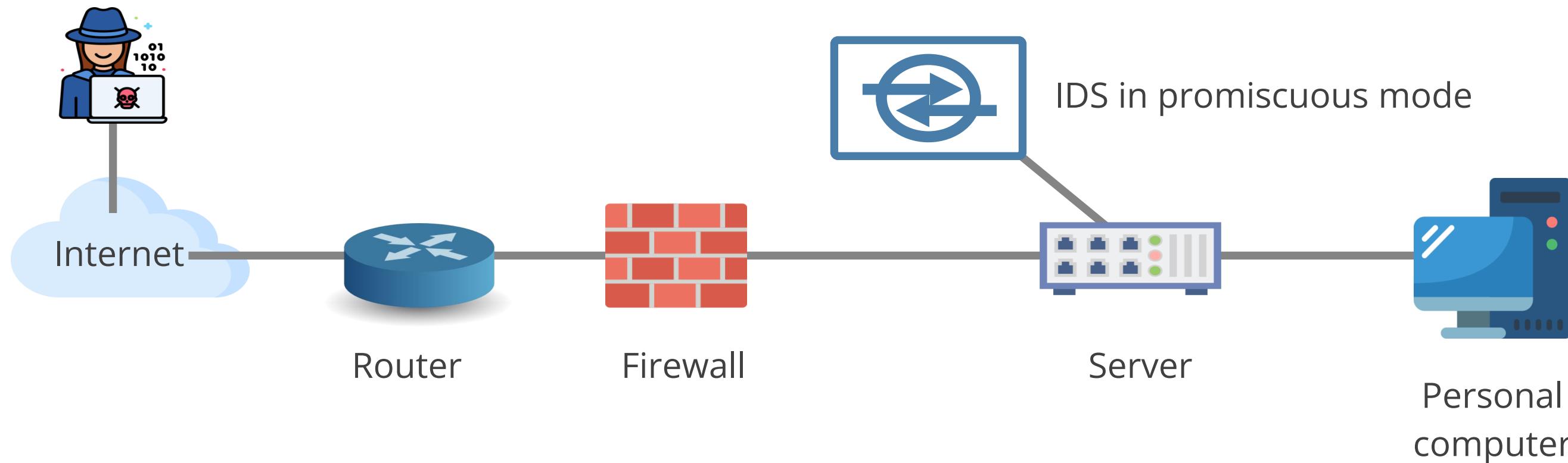
Maintains the confidentiality of the content of a trap by encrypting messages using protocols like AES

SNMP



Intrusion Detection System

- IDS continuously monitors the environment and detects and alerts on malicious attempts to gain unauthorized access
- It can only detect, not prevent, and it operates in promiscuous mode



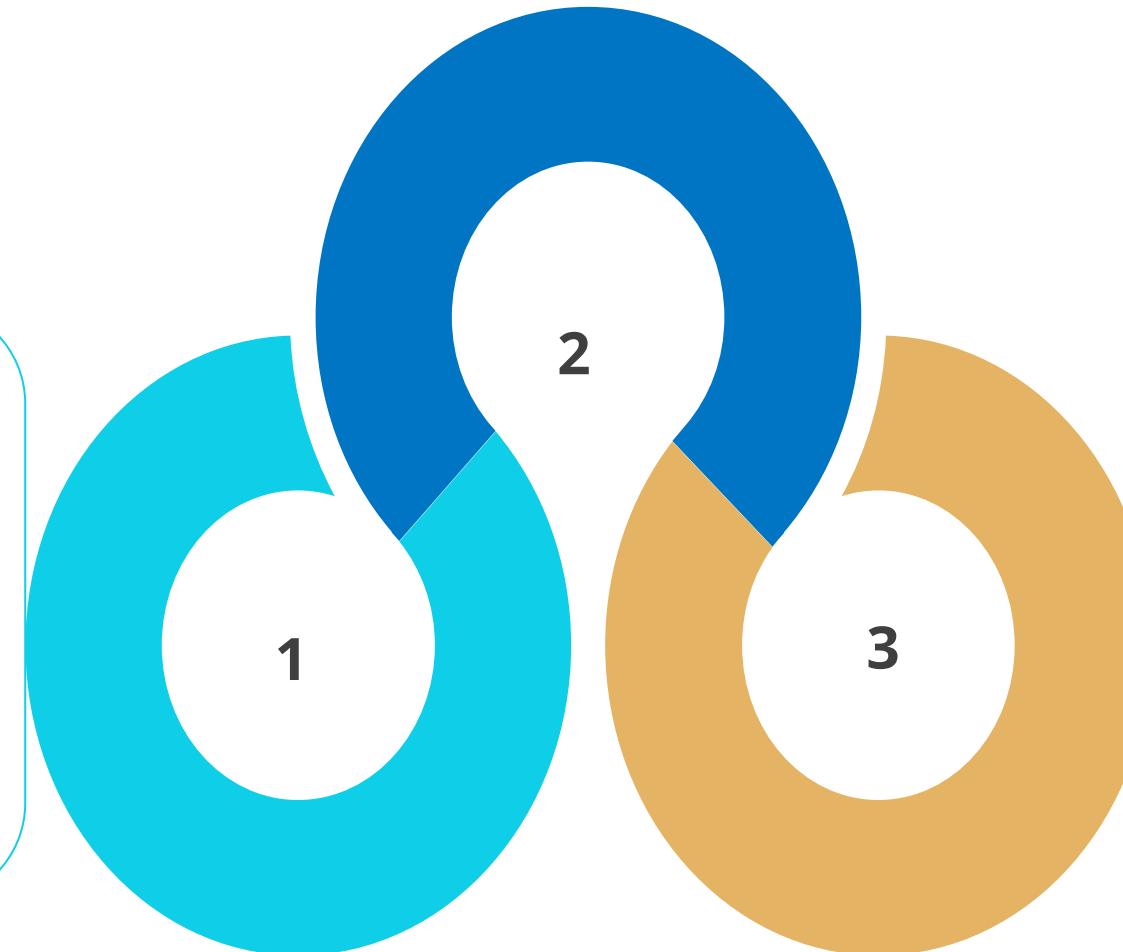
Functions of IDS

Alerts and notification

Generates alerts or notifications when a potential threat is detected, allowing security teams to investigate and respond to incidents promptly. Uses sensors and collectors to gather information to raise the alert

Traffic analysis

Inspects network traffic in real-time, examining data packets for unusual patterns, signatures, or behaviors that may indicate a security threat

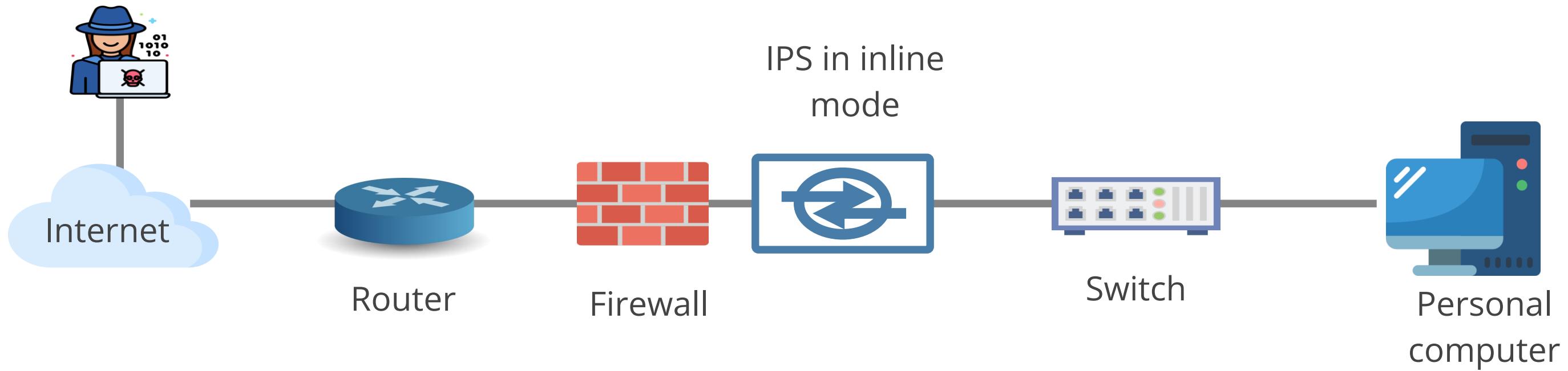


Passive role

Serves as an early warning system, providing insights into potential security breaches without actively blocking or preventing attacks

Intrusion Prevention System

Intrusion Prevention System (IPS) is a technology that monitors the environment and responds automatically when malicious attempts to gain unauthorized access are detected.



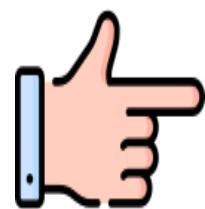
Functioning of IPS



Real-time analysis and actions: An IPSs continuously analyze network traffic (much like NIDSs) but with the added ability to take immediate action, rather than simply monitor and generate alerts.



Blocking threats: It can take proactive steps to block or prevent malicious activity, such as dropping suspicious packets or blocking access to specific IP addresses.



Policy enforcement: It can enforce security policies and rules defined by administrators, ensuring that network traffic complies with security guidelines.



Alerting and reporting: It also generate alerts and reports, giving administrators visibility into the security events occurring within the network.

Security Information and Event Management

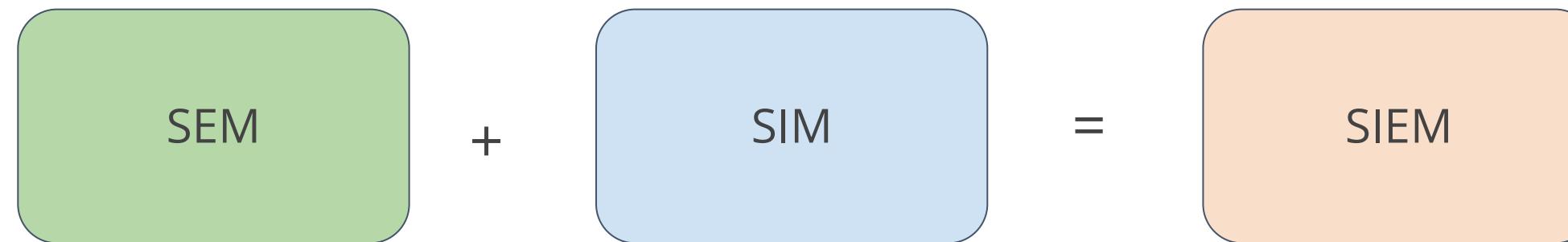
Security Information and Event Management (SIEM) solutions offer real-time monitoring and analysis of events as well as tracking and logging of security data for compliance or auditing purposes.



Security Information and Event Management

Security Information and Event Management

Security Event Management (SEM) provides real-time monitoring of events by correlating and analyzing data from different security sensors in the system.



Security Information Management (SIMs) provide long-term storage and management of such event data.

SIEM Process

Collect data from various sources (network devices, servers, firewalls, and IDS or IPS)



Normalize and aggregate the collected data

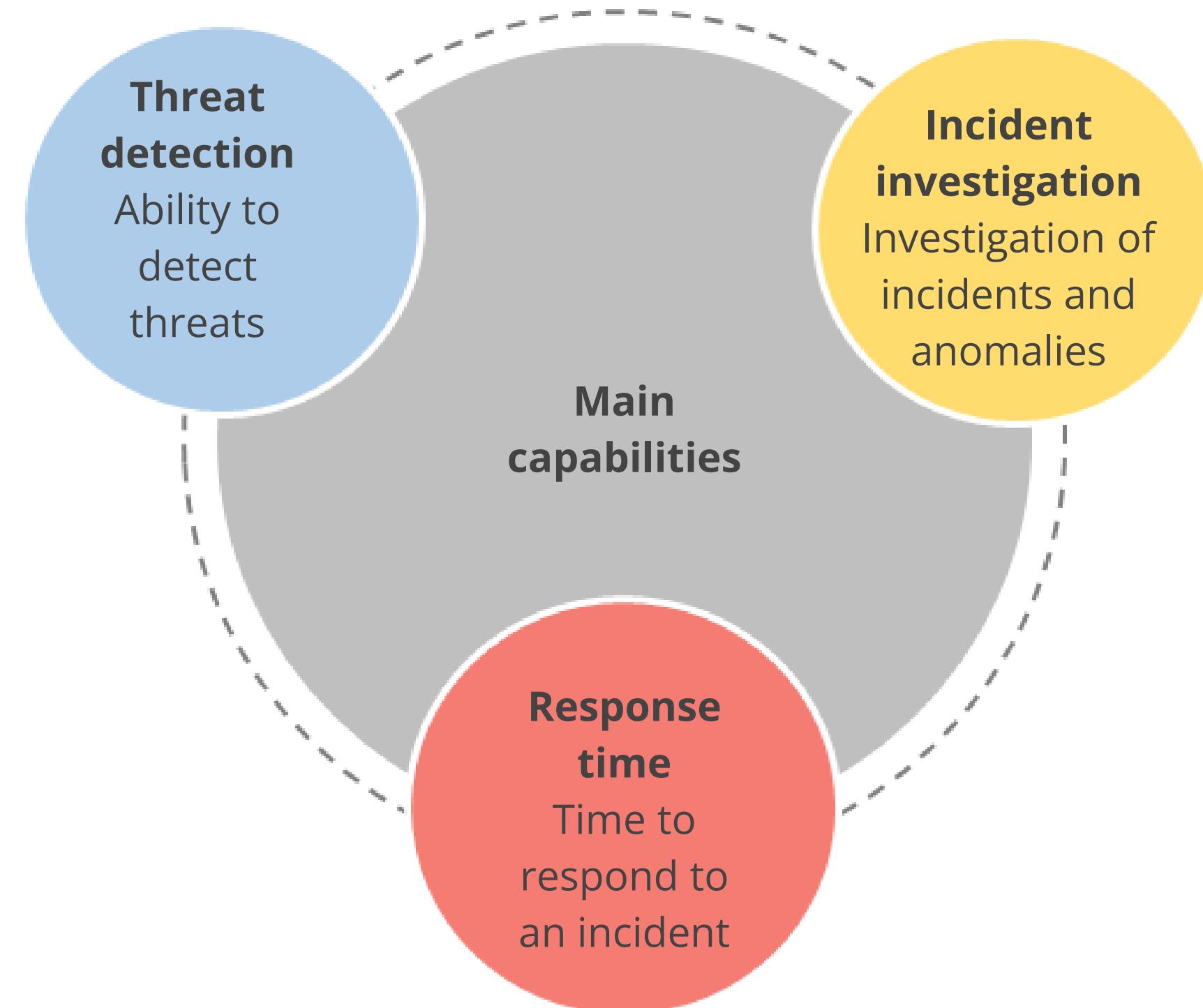


Analyze the data and identify the threats



Pinpoint security breaches and enable organizations to investigate the alerts

SIEM Capabilities



SIEM Capabilities

Aggregation

Provides a centralized repository to gather information from various systems across the environment.

Normalization

Processes logs into a meaningful, structured format to extract and interpret data efficiently across different sources.

Correlation

Recognizes patterns to connect the dots and correlate events from various data sources.

SIEM Capabilities

Reporting

Provides tools to visualize data and events in your environment.

Real-time monitoring

Provides real-time monitoring and threat detection across the organization's infrastructure, enabling rapid responses to potential data breaches.

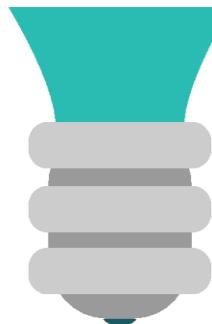
Data Loss Prevention

DLP involves implementing controls and practices to ensure that data is accessible only to authorized users and systems.



The goals of a DLP strategy are to manage risk, maintain regulatory compliance, and demonstrate due diligence by the application and data owners.

DLP should be integrated as part of the risk management approach.



DLP focuses on external parties.

DLP Architecture

Data in motion

- This is also referred to as network-based DLP or gateway DLP.
- In this topology, the monitoring engine is deployed near the organizational gateway to monitor outgoing protocols such as hypertext transfer protocol (HTTP), hypertext transfer protocol secure (HTTPS), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

Data at rest

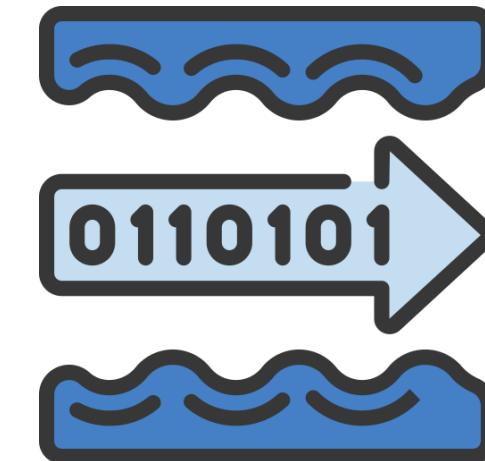
- This is also referred to as storage-based data.
- In this topology, the DLP engine is installed where the data is at rest, usually one or more storage subsystems, as well as file and application servers.
- This topology is effective for data discovery and tracking usage but may require integration with network-based or endpoint-based DLP for policy enforcement.

Data in use

- This is also referred to as client or endpoint based.
- The DLP application is installed on a user's workstations and endpoint devices.
- This topology offers insights into how users utilize the data, with the ability to add protection that network DLP may not be able to provide.

NetFlow

- NetFlow, originally developed by Cisco, is a protocol used for collecting and monitoring network traffic data.
- It enables network administrators to understand the source, destination, volume, and paths of traffic flow across their networks.
- This understanding is vital for security tasks, such as detecting anomalies, profiling traffic, and monitoring network performance.
- While Cisco initiated NetFlow, it has been standardized as IPFIX by the Internet Engineering Task Force (IETF), as documented in RFC 7011, RFC 7015, and RFC 5103.



Antivirus

- Antivirus software, also known as anti-malware, is a computer program used to prevent, detect, and remove malware. It was originally developed to detect and eliminate computer viruses.
- Antivirus software continuously scans for malware indicators, suspicious activities, and emerging threats.
- Once the antivirus algorithms detect a virus characterized by a distinct signature pattern, they can initiate predefined actions such as deleting or quarantining the virus, all configured within the antivirus console.

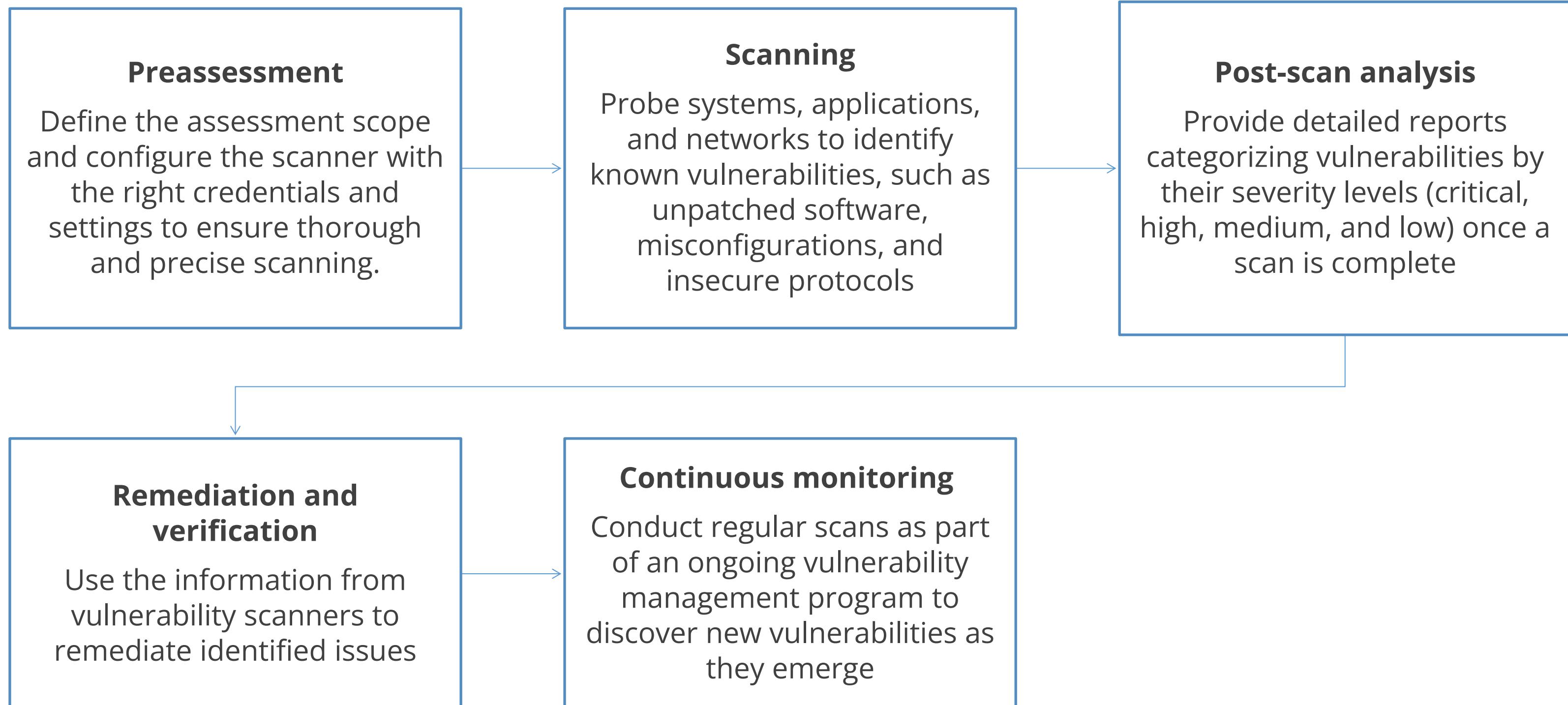


Vulnerability Scanners

- Vulnerability scanners automate the identification of weaknesses in systems and networks, acting as digital sentinels constantly searching for vulnerabilities.
- Tools like Nessus and OpenVAS play a critical role in proactive defense, scanning for known vulnerabilities.



Vulnerability Scanning Stages



Agent and Agentless in Data Gathering

Agent based

- Uses software agents on individual devices or endpoints within a network
- Gathers information about the device's performance, configuration, and security
- Transmits logged data to a SIEM server for analysis



Agentless

- Operates without the need for specialized agent deployment on endpoints
- Relies on existing protocols and interfaces to gather data from devices and systems remotely
- Uses sensors and collectors on the network to gather information

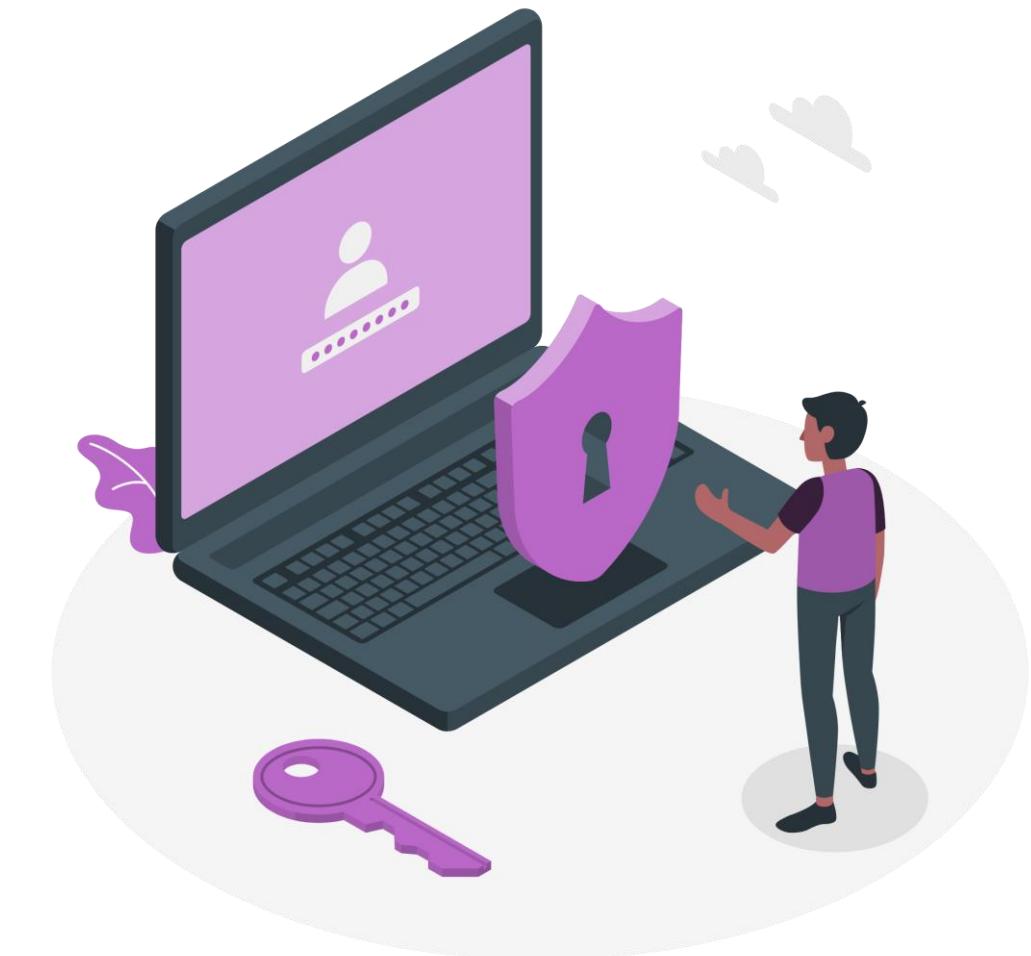
TECHNOLOGY

Modifying Enterprise capabilities to Enhance Security

Technologies for Enhancing Modern Enterprise Security

In the modern business environment, characterized by a dispersed workforce, cloud technology, and persistent cyber threats, it's crucial to integrate various security technologies. Key components of an effective security strategy include:

- Strong security framework: Integrating various technologies to protect against diverse threats
- Comprehensive security strategy: Combining multiple technologies to address the specific needs of your organization



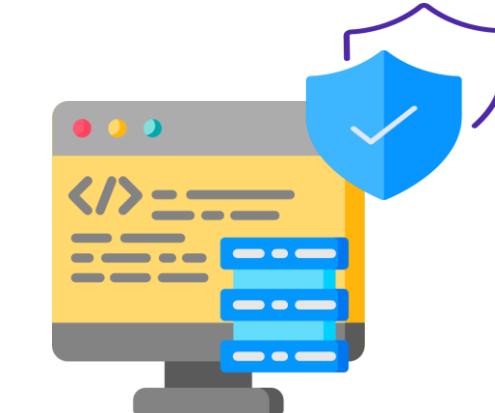
Technologies for Enhancing Modern Enterprise Security



Firewalls



Unified threat management



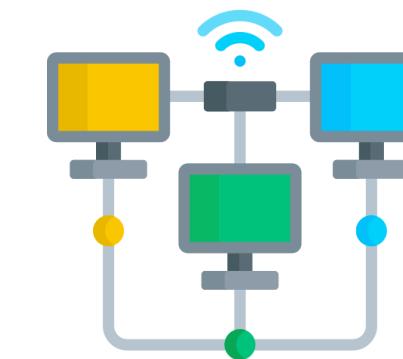
Web application firewall



Intrusion detection system



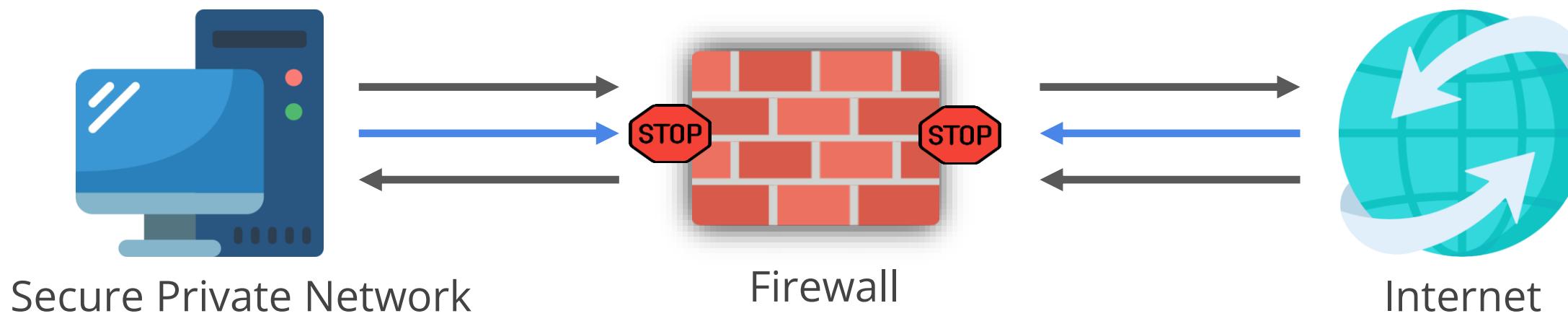
Intrusion prevention system



Zones

Firewall

- Firewall has been the first line of defense in network security for over 25 years. It is located at the intersection of two networks, usually a private and a public network such as the internet.
- A firewall completely isolates your computer from the Internet by checking each data packet as it reaches either side of the firewall.



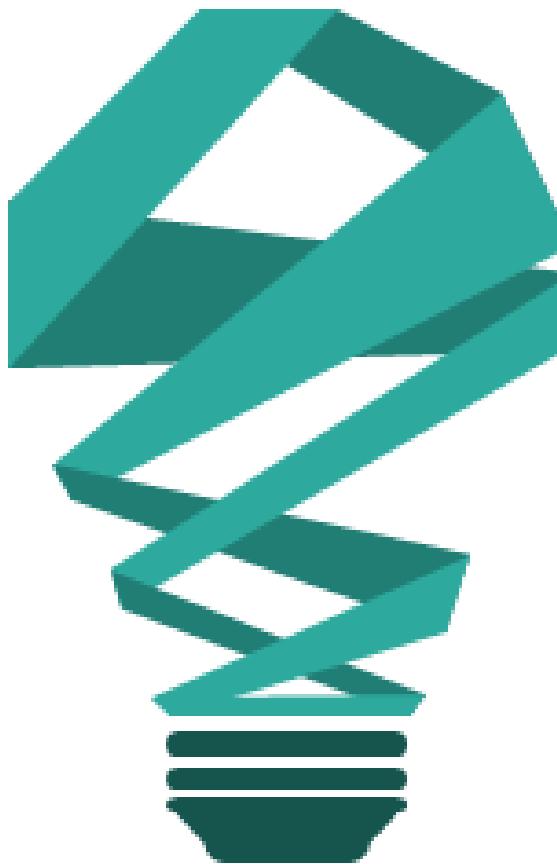
Firewall

A firewall is a crucial network security device that controls incoming and outgoing network traffic based on predetermined security rules. Key features of firewalls include:

- **Traffic analysis and control:** Determines whether specific traffic should be allowed or blocked
- **Types:** Can be hardware, software, or a combination of both, enforcing network security policies
- **Network segregation:** Restricts access from one network to another
- **Operational layers:** Functions from Layer 3 to Layer 7 of the OSI model



How does a firewall work



Filtering: Firewalls examine network traffic based on predefined rules

Blocking: Suspicious or malicious traffic is blocked

Allowing: Safe and authorized traffic is permitted.

Unified Threat Management

Unified Threat Management (UTM) integrates multiple security functions into a single platform, providing comprehensive protection and simplifying security management. Key aspects of UTM include:

- **Centralized security:** Combines multiple security functions, eliminating the need for separate standalone appliances
- **Threat protection:** Safeguards against threats, malware, and network attacks from a single point
- **Efficiency and cost-effectiveness:** Simplifies security management, reduces costs, and enhances overall protection



Components of UTM

Firewall: Protects the network from unauthorized access

Antivirus/Anti-malware: Protects against malicious software.

VPN: Provides secure remote access

Content filtering: Blocks or allows specific types of content

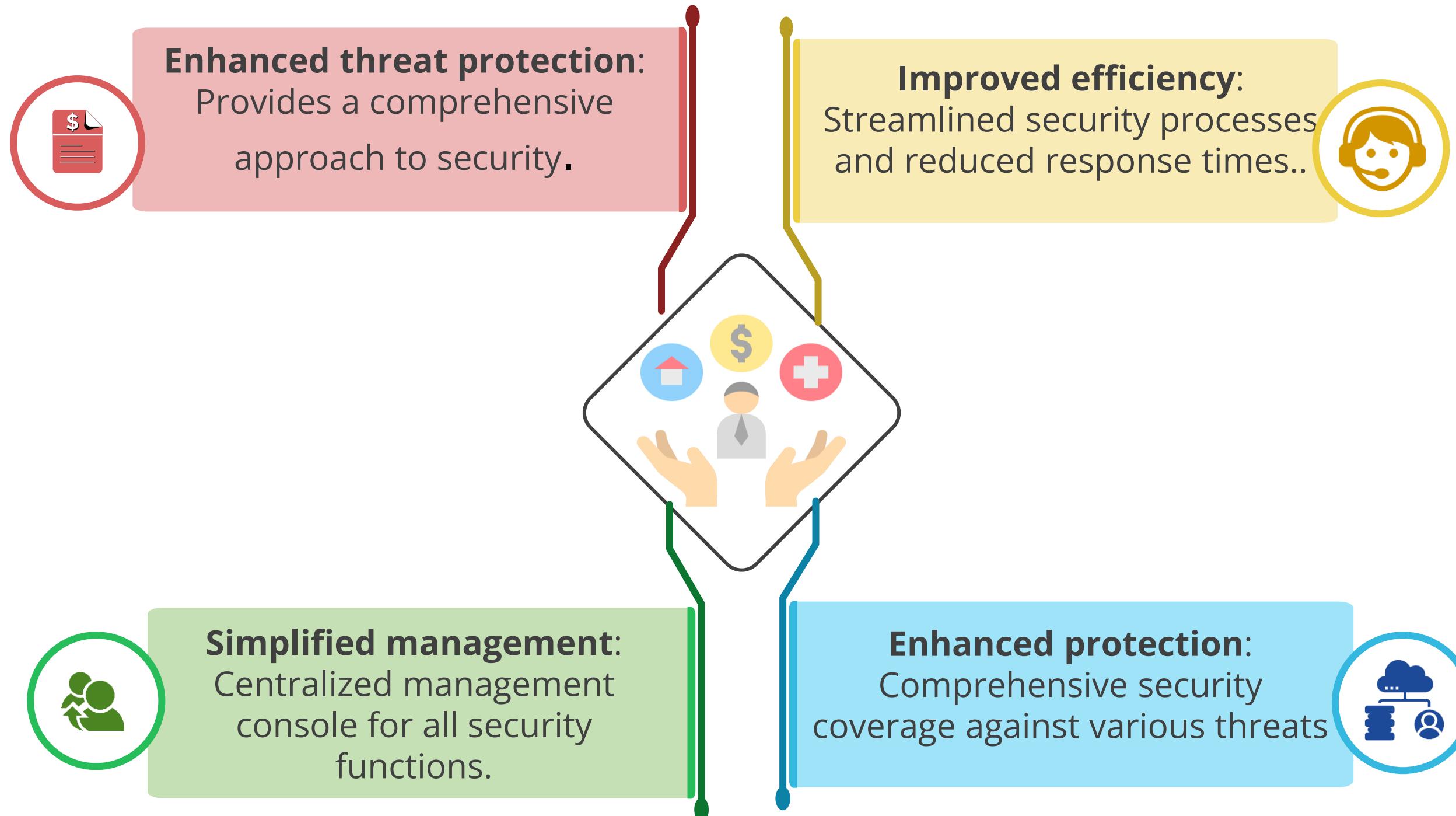


Intrusion Prevention System (IPS): Detects and prevents network attacks.

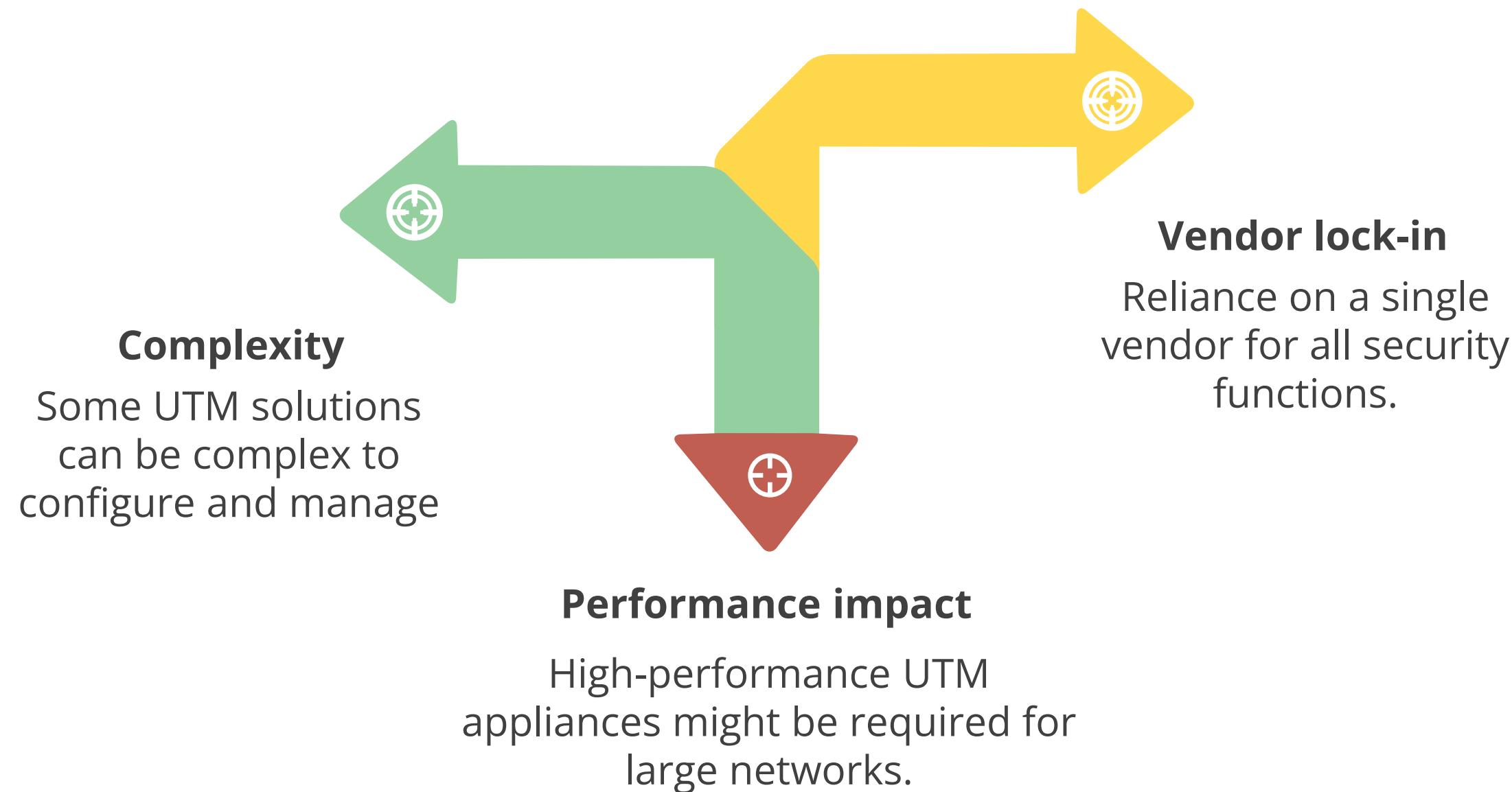
Spam filtering: Blocks unwanted email

Web filtering: Controls access to websites based on content or user policies.

Benefits of Unified Threat Management



Limitations of UTM



Next-Generation Firewall (NGFW) Evolution Over UTM

The Next-Generation Firewall (NGFW) is an advanced firewall that enhances traditional security measures with additional features. Key characteristics of NGFWs include:

- **Deep-packet inspection:** Conducts thorough analysis of data packets to identify threats
- **Application-level inspection:** Monitors and controls applications to prevent intrusions
- **External intelligence integration:** Utilizes threat intelligence from external sources for improved security



Key Features of Next Generation Firewall



Application control: identifies and controls applications running on the network, allowing administrators to block or restrict specific apps



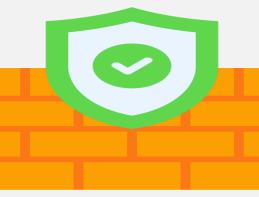
Intrusion Prevention System (IPS): Detects and prevents network attacks, providing an additional layer of protection.



Advanced Threat Protection (ATP): Utilizes techniques like sandboxing and behavioral analysis to identify and block advanced threats like malware and ransomware.

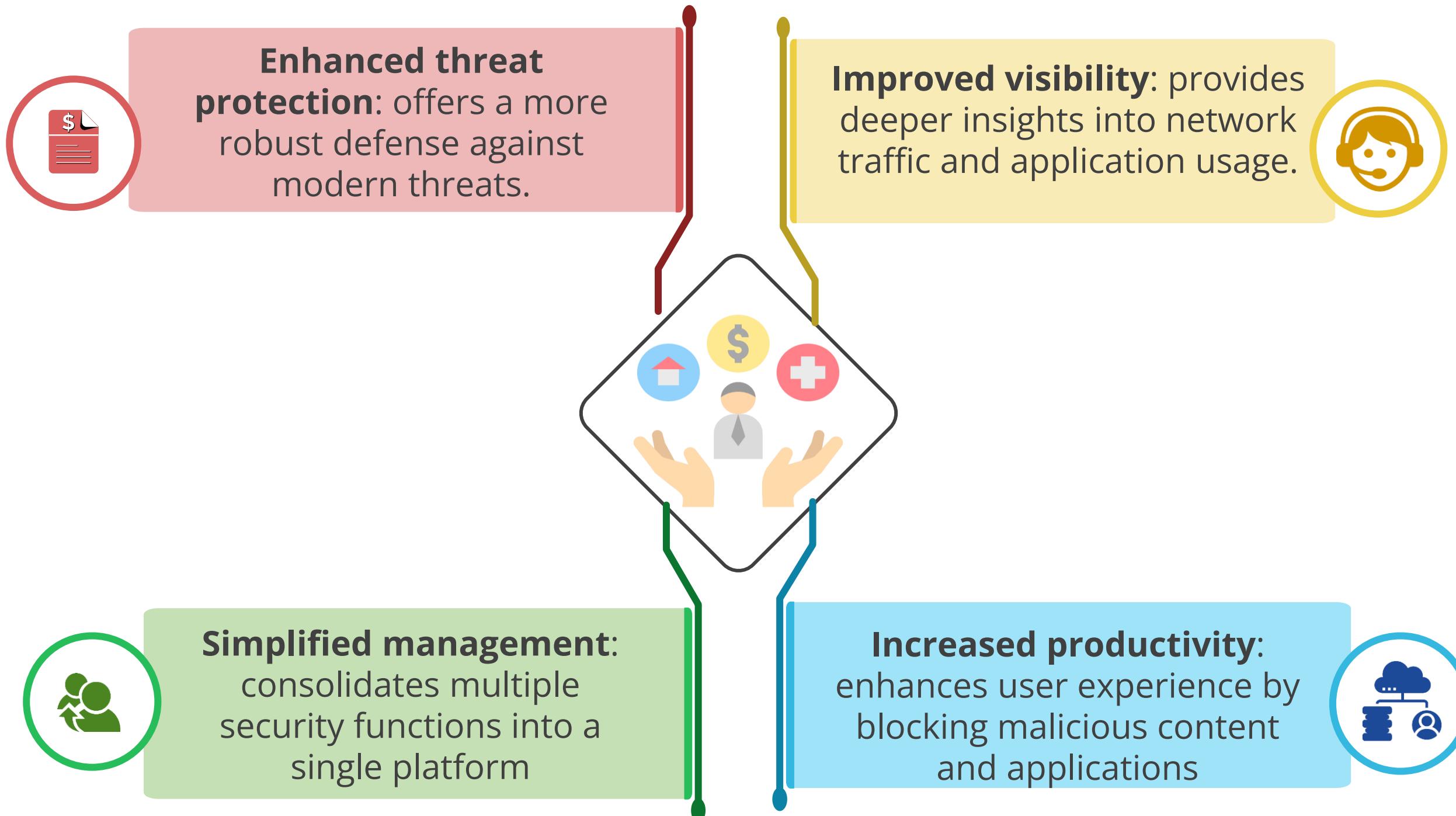


User identity and context awareness: enhances security by considering user identity, location, and device information



Unified Threat Management (UTM): Often includes additional security features like web filtering, spam filtering, and VPN

Benefits of Next Generation Firewall



UTM and NGFW

S.No	Feature	UTM	NGFW
1	Focus	Comprehensive security suite	Advanced threat protection
2	Performance	Lower	Higher
3	Scalability	Limited	High
4	Management	Centralized	Complex
5	Cost	Lower initial investment	Higher initial investment
6	Ideal for	Small to medium-sized businesses	Large organizations

UTM vs. NGFW: Key Takeaways

Choosing between Unified Threat Management (UTM) and Next-Generation Firewall (NGFW) depends on your organization's specific needs. Key takeaways include:

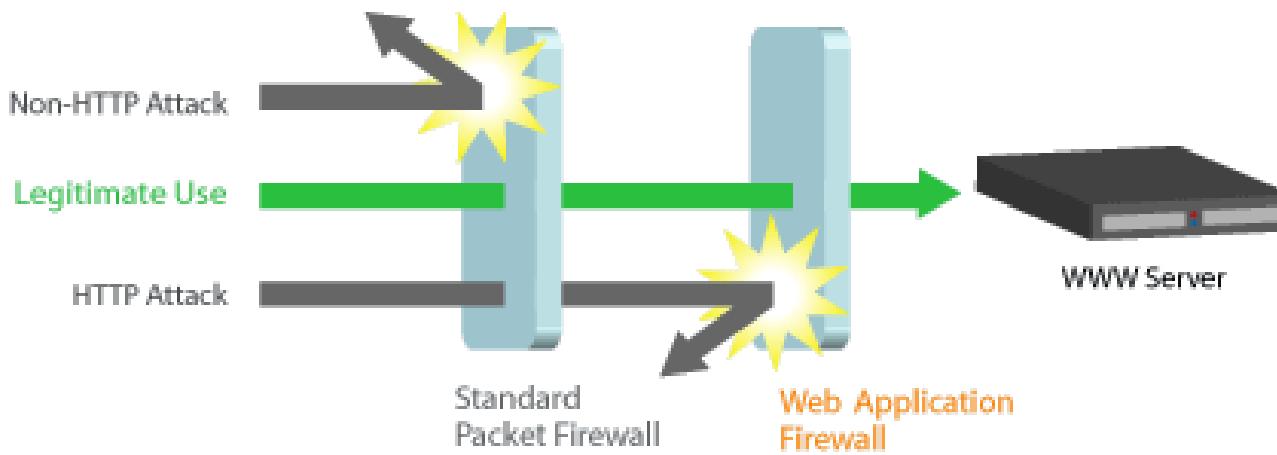
- **Ease of management and cost:** If you prioritize easy management and a lower initial investment, UTM might be sufficient
- **Advanced protection and performance:** For advanced threat protection and high performance, NGFW is the better option
- **Feature overlap:** Many NGFWs now offer some UTM capabilities and vice versa, providing flexibility in your security strategy

TECHNOLOGY

Web Application Firewall

Web Application Firewall (WAF)

It filters and monitors HTTP traffic to protect web applications from attacks such as cross-site forgery, cross-site scripting (XSS), file inclusion, and SQL injection.



It operates through rules or policies to filter out malicious traffic.

Types of WAF

Network based WAF

Deployed at the network level, inspecting traffic before it reaches the application server

Host based WAF

Installed directly on the web server, providing granular control over application-specific traffic

Cloud based WAF

Offered as a cloud service, providing scalability and ease of deployment

WAF Technologies

Signature based detection

- This traditional approach relies on a database of known attack signatures, comparing incoming traffic patterns against them.
- Signature databases are regularly updated to include new threats.

Anomaly detection

- Analyzes traffic patterns to detect deviations from normal activity, indicating potential malicious intent.
- Techniques include statistical analysis, machine learning, and behavioral profiling.

Positive model(Whitelist)

- Only allows traffic matching pre-defined criteria, essentially creating a "safe list" for authorized requests.
- Offers strong protection against unknown threats and misconfigurations.

Negative model(Blacklist)

- Blocks traffic matching known attack signatures, essentially creating a block list of malicious patterns.
- Easier to implement than whitelists.

TECHNOLOGY

Intrusion Detection and Prevention System

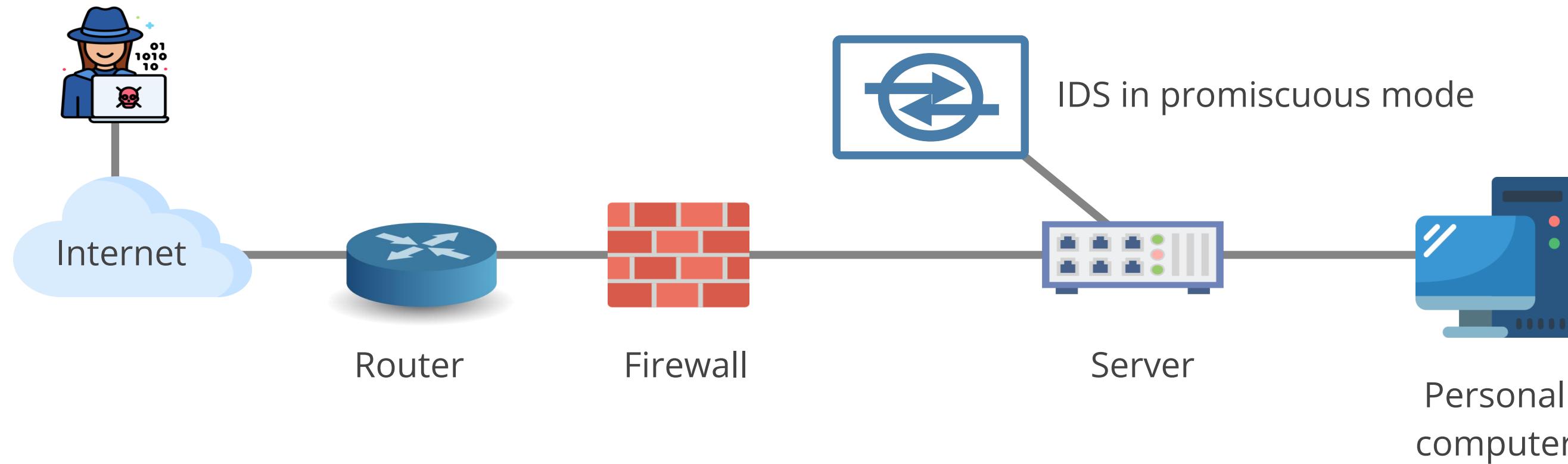
Intrusion

- It refers to any unauthorized access, unauthorized attempt to access or damage, or malicious use of information systems.
- It may compromise the confidentiality, integrity, and availability of the information assets.



Intrusion Detection System (IDS)

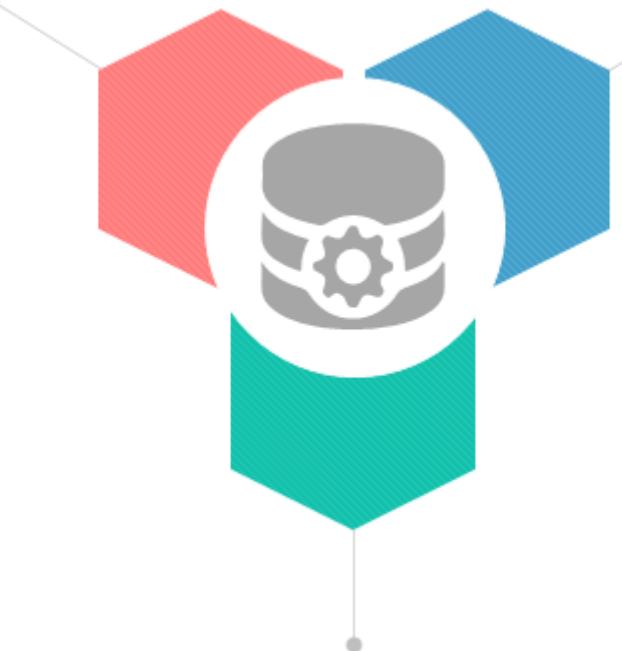
It is a solution that continuously monitors the environment and detects and alerts malicious attempts to gain unauthorized access.



Main Functions of IDS

It gathers and analyzes information from within a computer or a network to identify violations of the security policy, including unauthorized access and misuse.

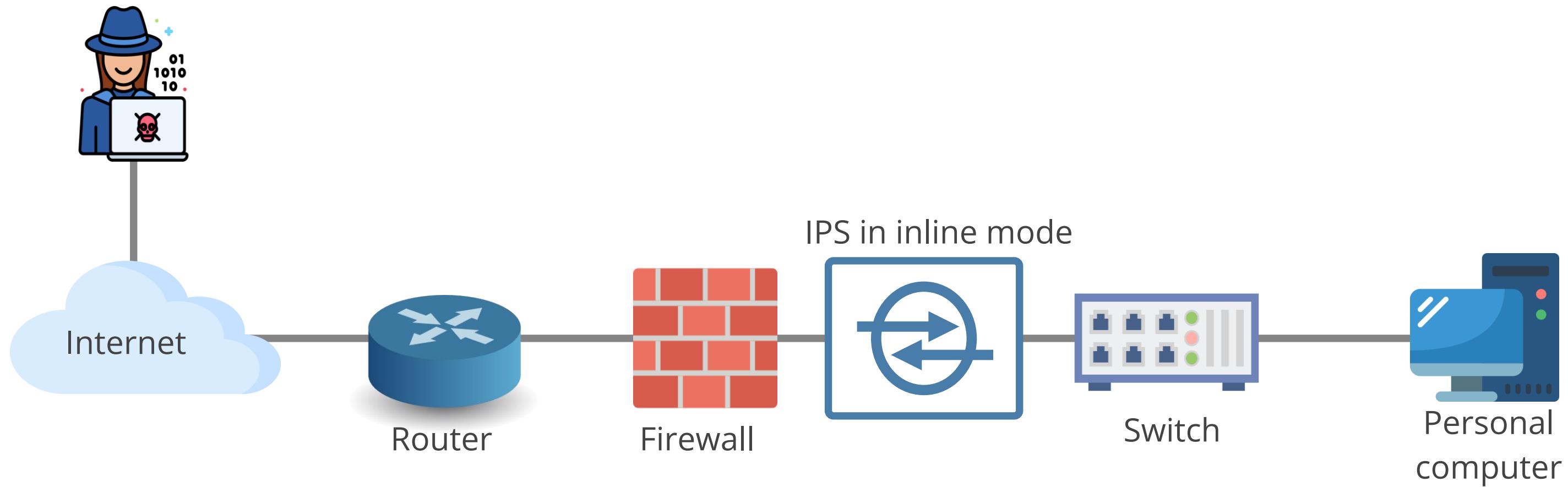
It is also referred to as a **packet sniffer**, which intercepts packets traveling via various communication media and protocols, usually TCP/IP.



It evaluates traffic for suspected intrusions and raises the alarm upon detecting such intrusions.

Intrusion Prevention System (IPS)

It is a technology that monitors the environment and responds automatically when malicious attempts to gain unauthorized access are detected.



Trend Analysis in IPS/IDS

AI and machine level integrations

Convergence with security suites

Cloud based IDS/IPS

Focus on network behavioral analysis

Zero-trust architecture

IOT and OT protections

- Traditional IDS/IPS relied on signature-based detection, which struggles with novel attacks. IDS/IPS solutions integrate with machine learning and AI.
- These technologies empower systems to autonomously analyze and identify anomalous patterns, enabling the rapid detection of previously unknown threats.
- This allows for better detection of zero-day attacks and advanced persistent threats (APTs)..

Trend Analysis in IPS/IDS

AI and machine level integrations

Convergence with security suites

Cloud based IDS/IPS

Focus on network behavioral analysis

Zero-trust architecture

IOT and OT protections

- Modern IDS/IPS are being integrated with broader security suites that offer a unified platform for various security functionalities like firewalls, anti-malware, and SIEM (Security Information and Event Management).
- This consolidation simplifies security management and streamlines threat response

Trend Analysis in IPS/IDS

AI and machine level integrations

Convergence with security suites

Cloud based IDS/IPS

Focus on network behavioral analysis

Zero-trust architecture

IOT and OT protections

- The rise of cloud computing has led to a surge in cloud-based IDS/IPS solutions.
- These offer scalability, flexibility, and easier deployment for organizations leveraging cloud infrastructure.
- Additionally, cloud-based threat intelligence sharing improves overall threat detection capabilities

Trend Analysis in IPS/IDS

AI and machine level integrations

Convergence with security suites

Cloud based IDS/IPS

Focus on network behavioral analysis

Zero-trust architecture

IOT and OT protections

- Modern IDS/IPS go beyond just inspecting packet data.
- They employ NBA techniques to analyze overall network traffic patterns and identify deviations from normal behavior.
- This helps detect sophisticated attacks that attempt to blend in with legitimate traffic

Trend Analysis in IPS/IDS

AI and machine level integrations

Convergence with security suites

Cloud based IDS/IPS

Focus on network behavioral analysis

Zero-trust architecture

IOT and OT protections

- The zero-trust concept assumes that threats can exist both outside and inside a network.
- This is driving IDS/IPS solutions to take a more holistic approach.
- These systems now scrutinize traffic not only at the perimeter but also within the network, ensuring continuous monitoring and threat containment.

Trend Analysis in IPS/IDS

AI and machine level integrations

Convergence with security suites

Cloud based IDS/IPS

Focus on network behavioral analysis

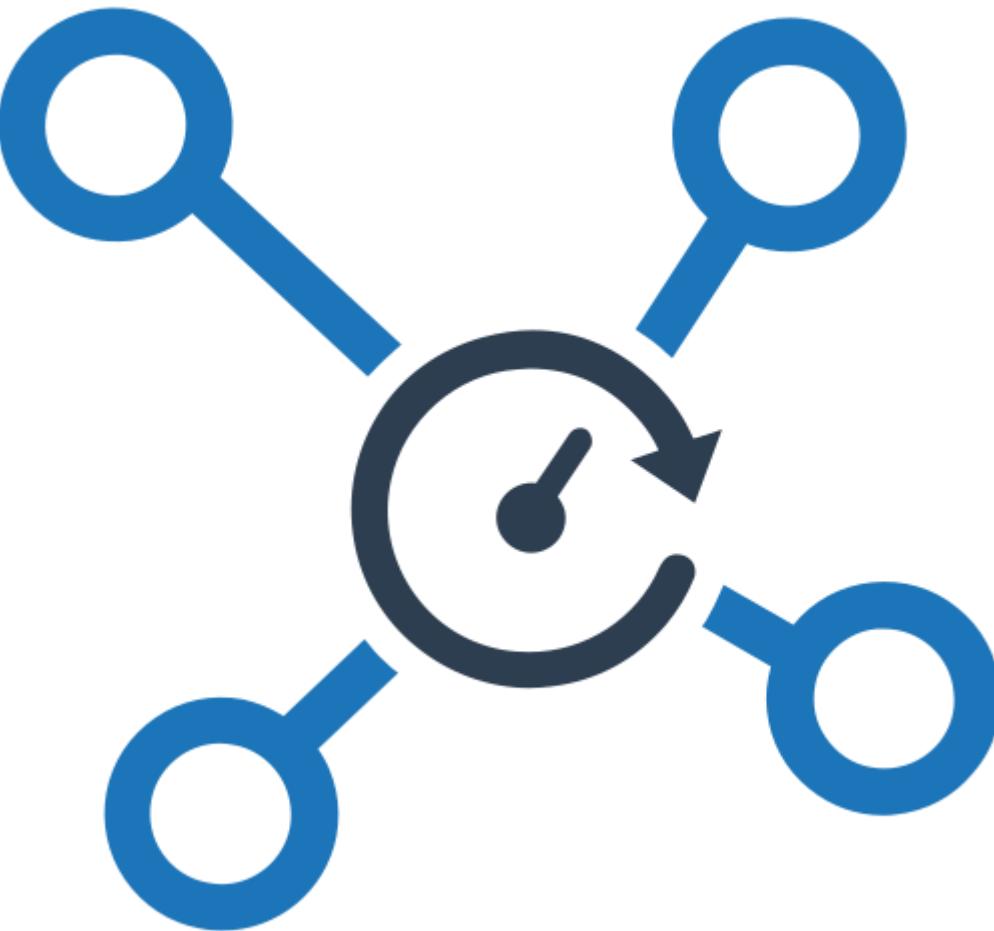
Zero-trust architecture

IOT and OT protections

- With the proliferation of IoT devices and operational technology (OT), IDS/IPS solutions are extending their reach to secure these traditionally vulnerable areas.
- They now provide deep packet inspection and anomaly detection for IoT and OT environments.

Zones

- They serve as logical or physical boundaries, dividing a network into smaller, more manageable, and secure sections. –
- They also isolate different network parts, creating a barrier to prevent potential attackers from moving laterally. If a threat actor breaches one zone, they will have difficulty accessing other zones containing critical resources.



Type of Zones

Wide area network

It is an external public network that covers a wide geographical area. This is considered an untrusted zone

Local area network (LAN)

It is a network covering a small location such as a building or a company with staff working in close proximity. This is seen as a trusted zone.

Screened subnet

It is a company-owned boundary layer designed to protect against external hackers. It serves as a neutral zone for data accessible to both trusted and untrusted sources.

TECHNOLOGY

OSI, TCP/IP, and Protocols

Introduction to Secure Network Architecture and Design



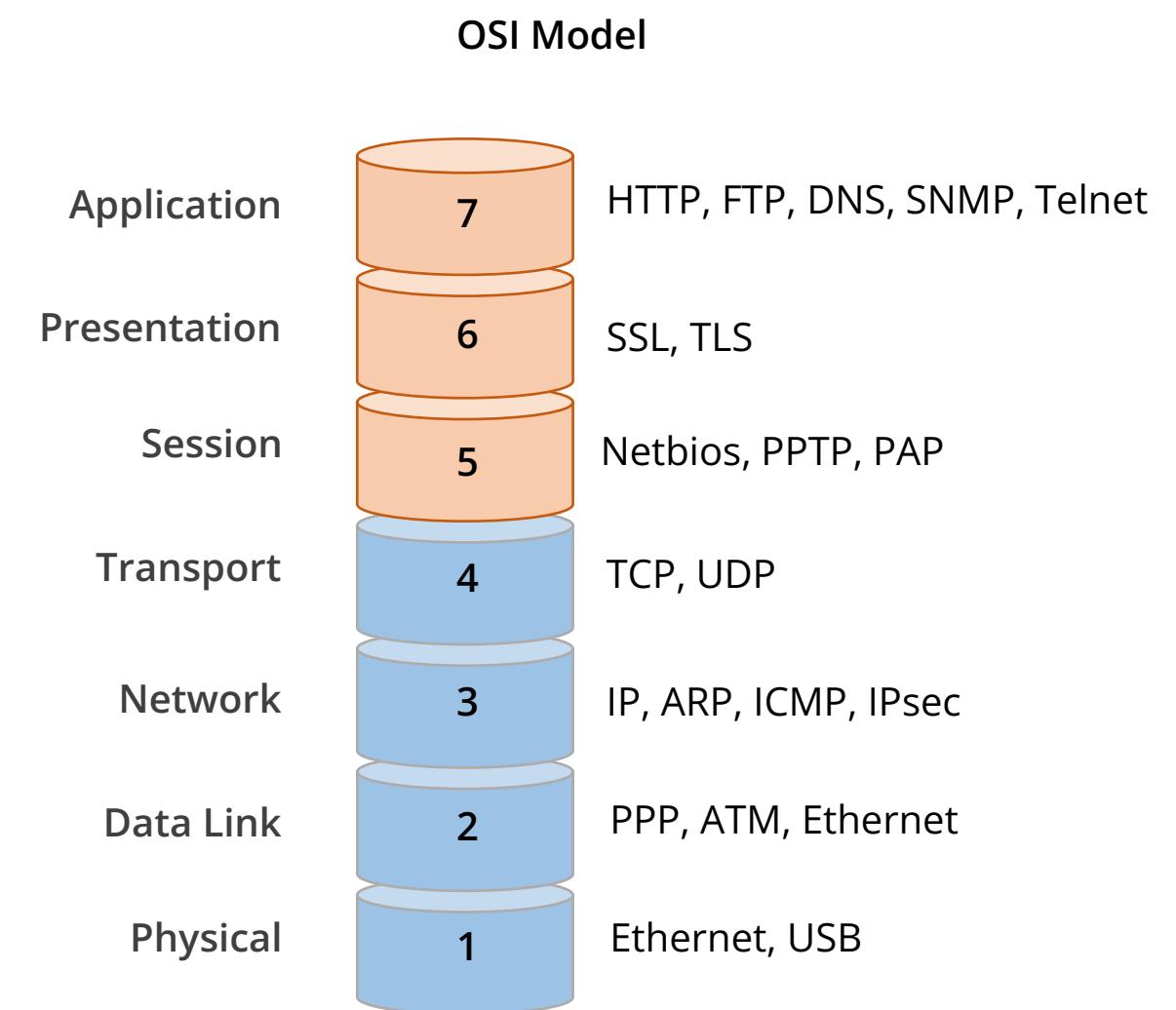
Various communication protocols define communication.

- OSI and TCP/IP models are the most popular models.
- Communication is divided into different layers by both models.
- Security is more efficiently addressed using the layered approach.
- The protocols can be grouped into stacks or suites.

Open Systems Interconnection (OSI)

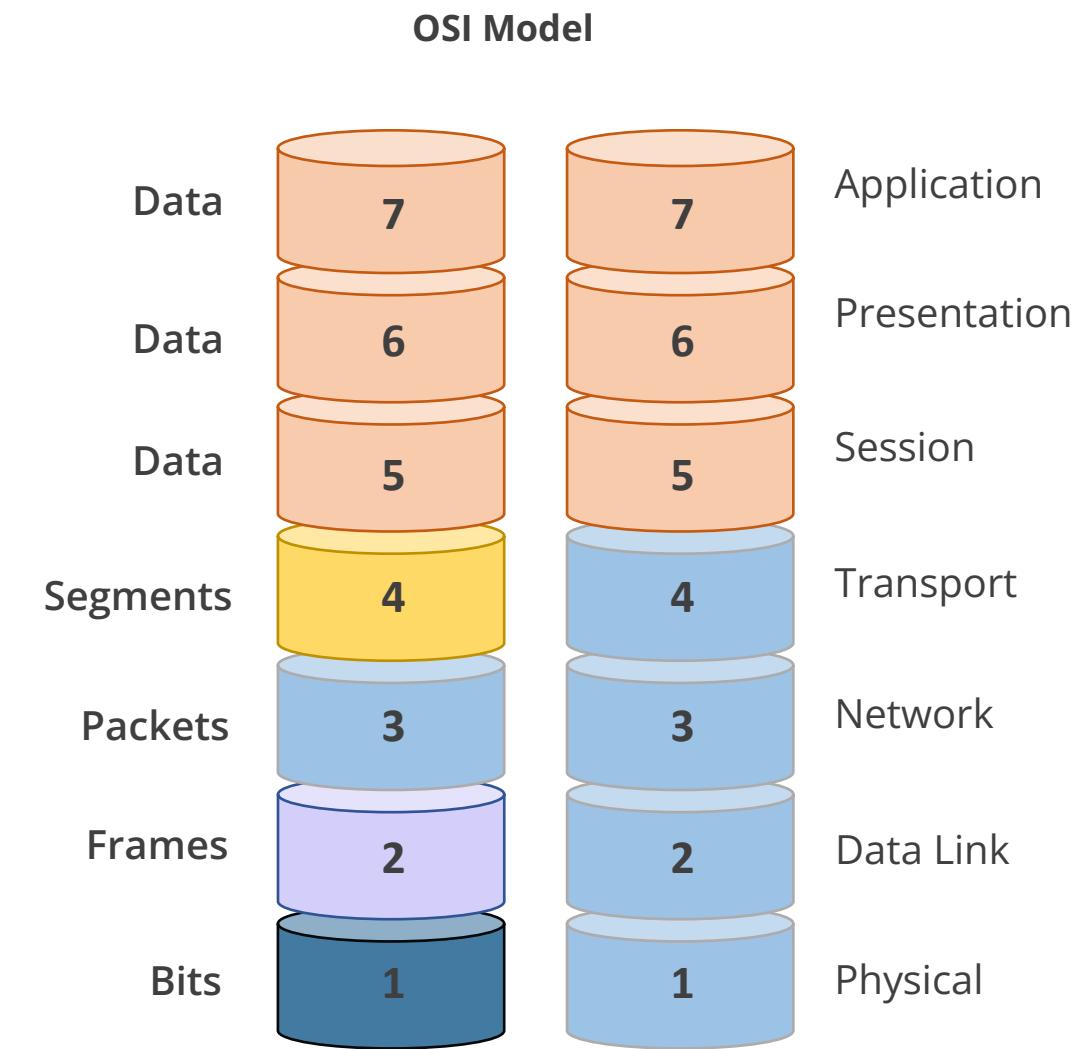
This is a standard model for network communications and allows dissimilar networks to communicate.

- OSI describes how data and network information are communicated from one computer to another.
- Each layer communicates with the same layer's software or hardware on other computers.



Open Systems Interconnection (OSI)

- The four lower layers (transport, network, data link, and physical) manage end-to-end data flow through the network.
- The three upper layers of the OSI model (application, presentation, and session) focus more on application services.
- Data is encapsulated with the necessary protocol information as it moves down the layers before network transit.



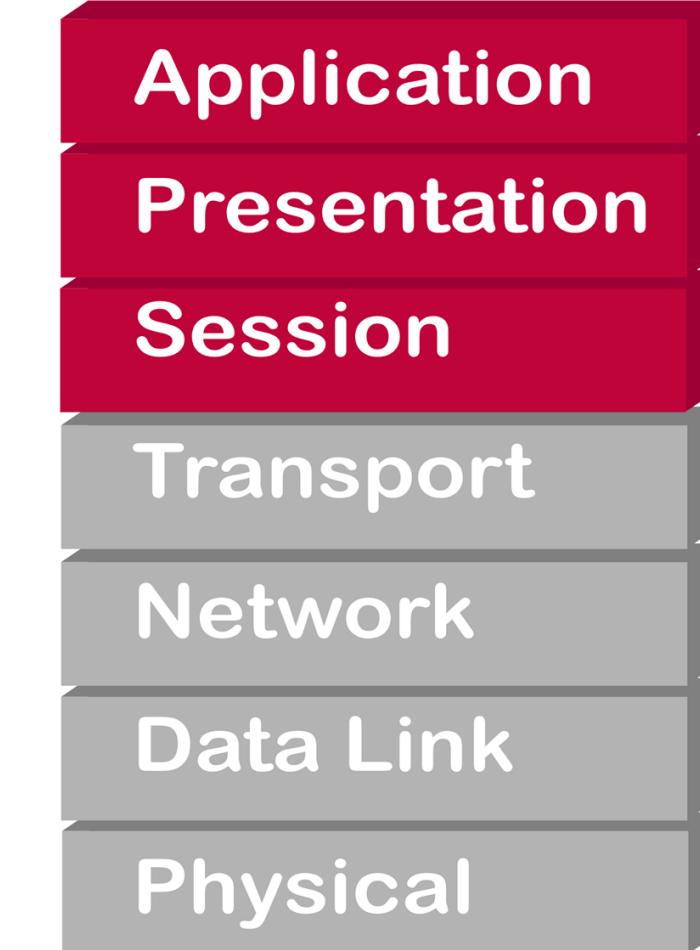
Open Systems Interconnection (OSI)

7	Application	This is like the contents of the letter itself - the information you want to communicate. This is the data that the user interacts with, like your email or web browser.
6	Presentation	This layer is like the person who opens the letter and translates it into a language you understand. It changes the data into a format that the receiving computer can understand.
5	Session	This layer is like making sure the mail is delivered to the correct mailbox. It establishes, maintains, and ends communication with the receiving device.
4	Transport	This layer acts like a security check. It ensures that the data arrives safely without any errors, just like ensuring your letter is not damaged when it arrives.
3	Network	This layer is like the post office system that determines the best route for the letter. This layer finds the best path for the data to reach its destination.
2	Data link	This layer is like the sorting process at the post office. It prepares the data for transport on the physical layer by packaging it up and adding a delivery address.
1	Physical	Like a mail truck, this layer is responsible for the actual delivery of data. In a computer, it is the physical parts like the cables and wires that carry the data from one computer to another.

Working of the OSI Model

Data is sent from a source computer to a destination computer.

- Each protocol operates in a specific layer.
- Each protocol in the source computer has a specific task assigned.
- When the data packet reaches the destination computer, it moves up through the model.
- Each protocol detaches and examines only the data attached by its counterpart at the source computer.
- Each layer at the destination handles only the data packaged by its counterpart on the sending side.



Working of the OSI Model

The following illustration explains how data travels in the OSI model:

1. Data travels down the stack.



Host A	
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

2. Data travels through the network.



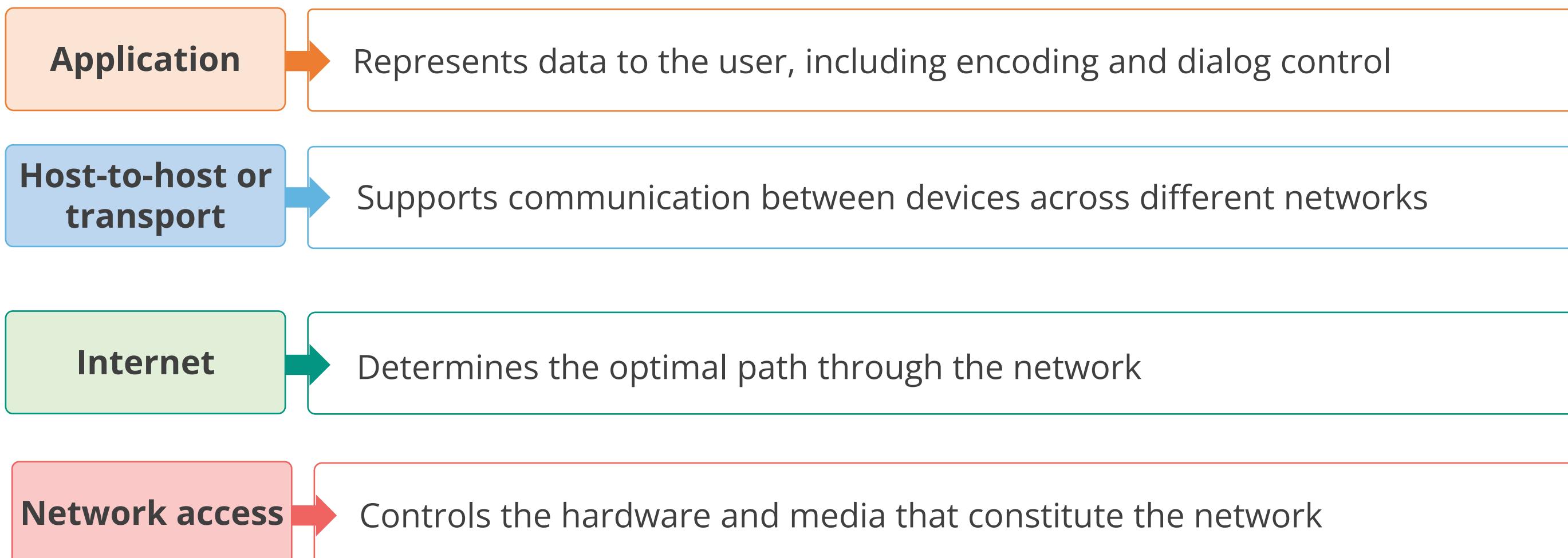
Host B	
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

3. Then, data travels up the receiving stack.



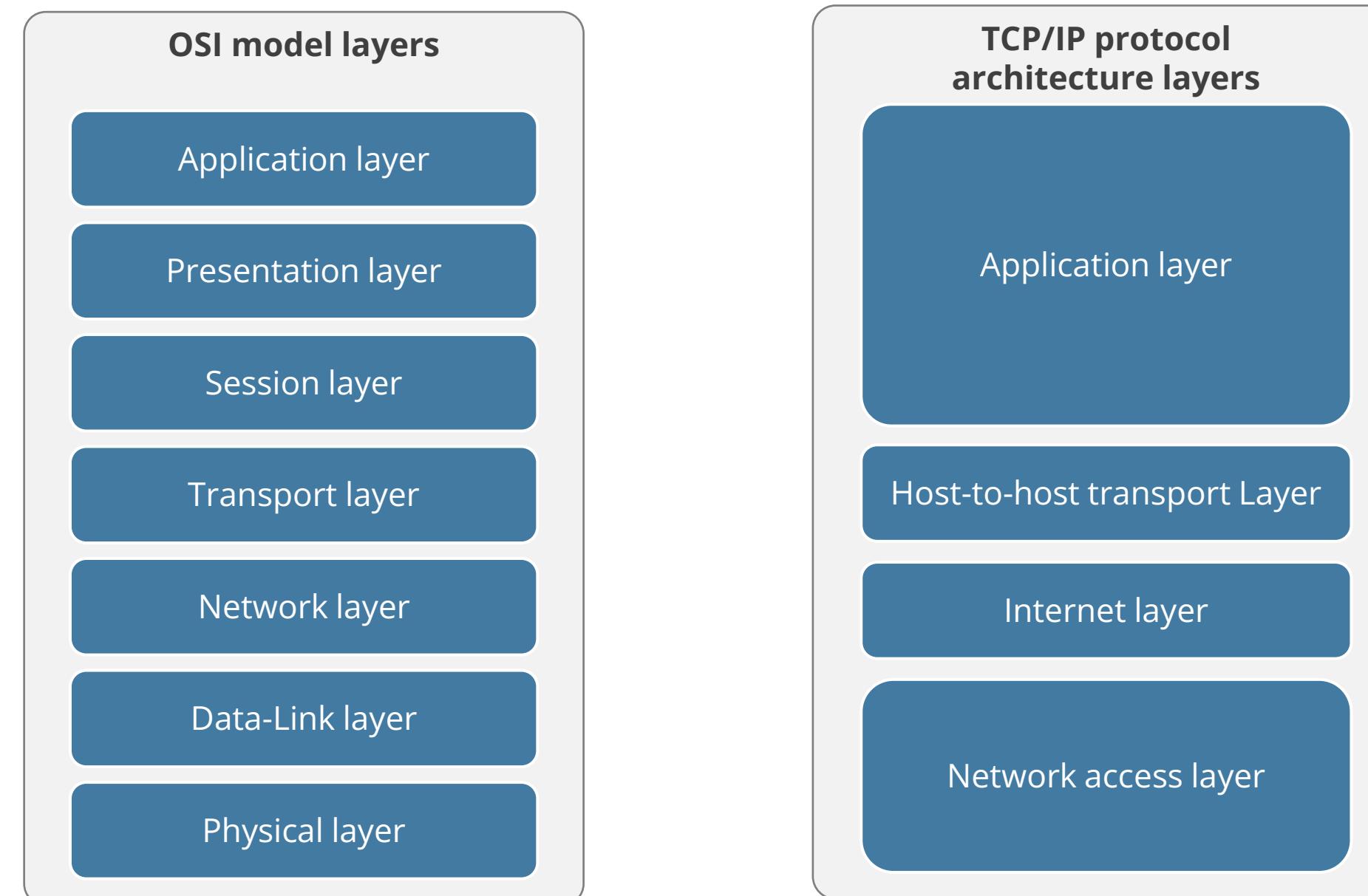
Transmission Control Protocol or Internet Protocol (TCP/IP) Model

TCP/IP is the common name for the suite of protocols originally developed by the Department of Defense (DoD).



Comparison of OSI and TCP/IP Models

The TCP/IP model is very similar to the OSI model; however, it has fewer layers.



Types of Network Protocols

Transmission Control Protocol (TCP)

User Datagram Protocol (UDP)

Internet Protocol (IP)

Address Resolution Protocol (ARP)

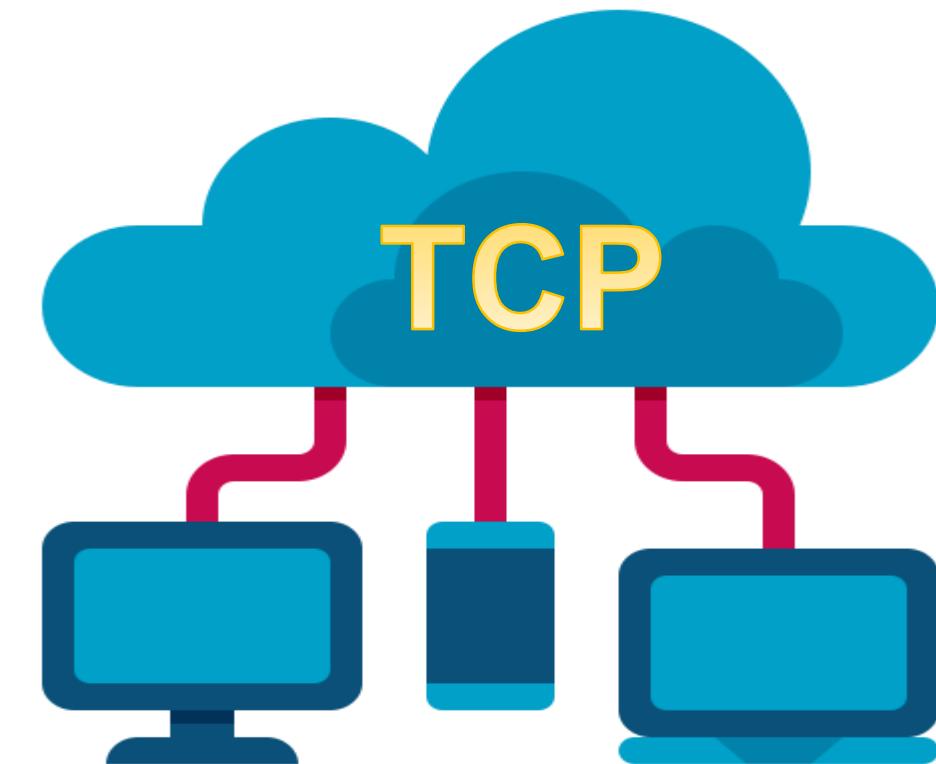
Internet Control Message Protocol (ICMP)

Transmission Control Protocol (TCP)

TCP provides a complete duplex and reliable connection.

Reliable data transport is addressed by TCP to ensure that the following goals are achieved:

- An acknowledgment is sent back to the sender.
- Any unacknowledged segments are retransmitted.
- Segments are reassembled in their correct order.
- It maintains a manageable data flow.
- The types of ports are reserved or well-known ports (0 to 1023), registered ports (1024 to 49151), and dynamic ports (49152 to 65535).
- Examples of applications that use TCP: HTTP, FTP, and Telnet.



TCP is costly in terms of network overhead and is slower than UDP.

TCP Flags

TCP flags are control bits in the TCP header that provide crucial information about network connection states. They play a key role in establishing, managing, and terminating TCP connections.

SYN (Synchronize):

Used to initiate a connection

ACK (Acknowledge):

Confirms the receipt of data

FIN (Finish):

Indicates the end of the data transmission from one side of the connection

RST (Reset):

Abruptly terminates an existing connection

PUSH (Push):

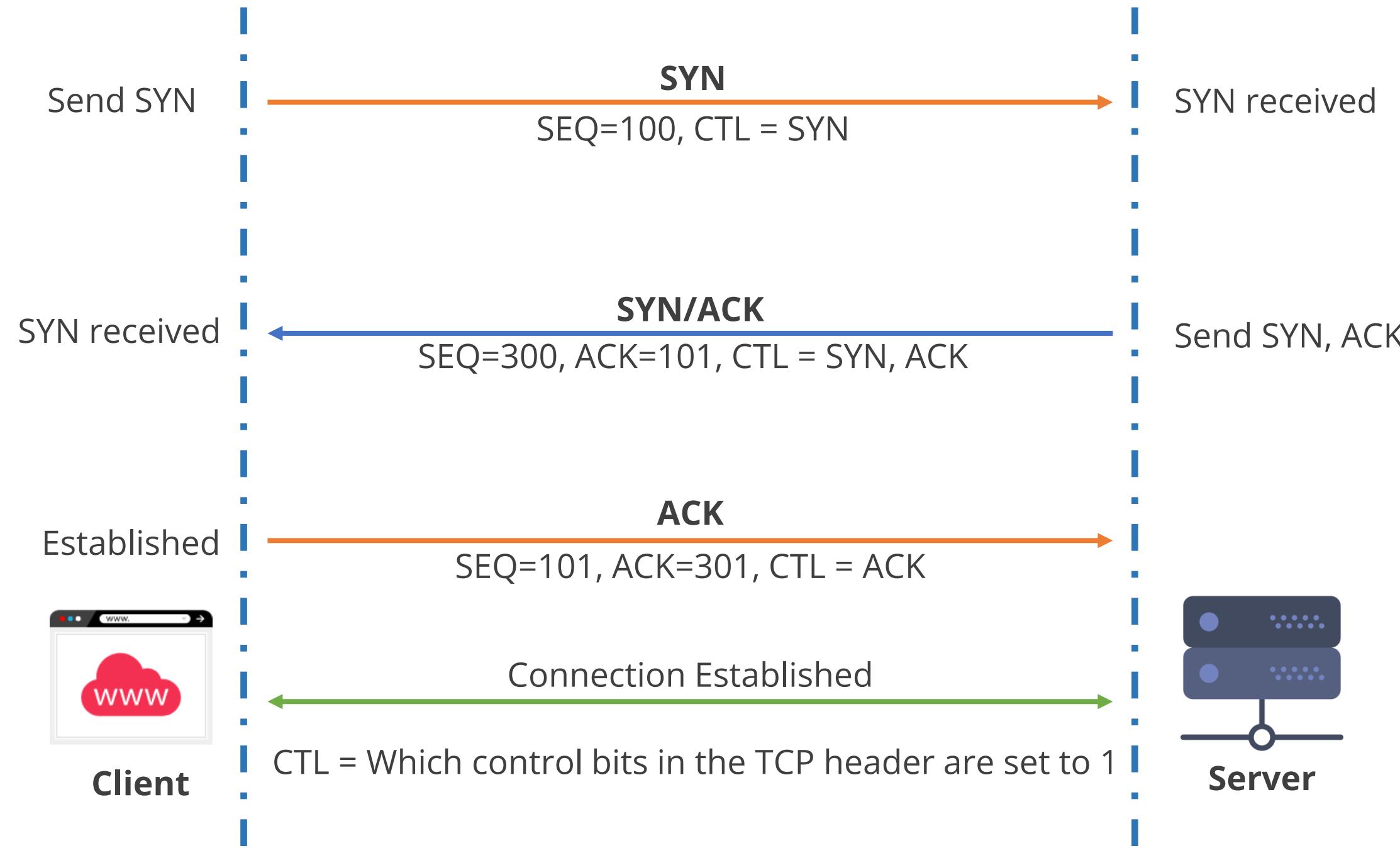
Requests the immediate delivery of data

URG (Urgent):

Indicates that urgent data follows in the packet

TCP Handshake Process

A TCP three-way handshake is used to create a connection between a local host or client and server.



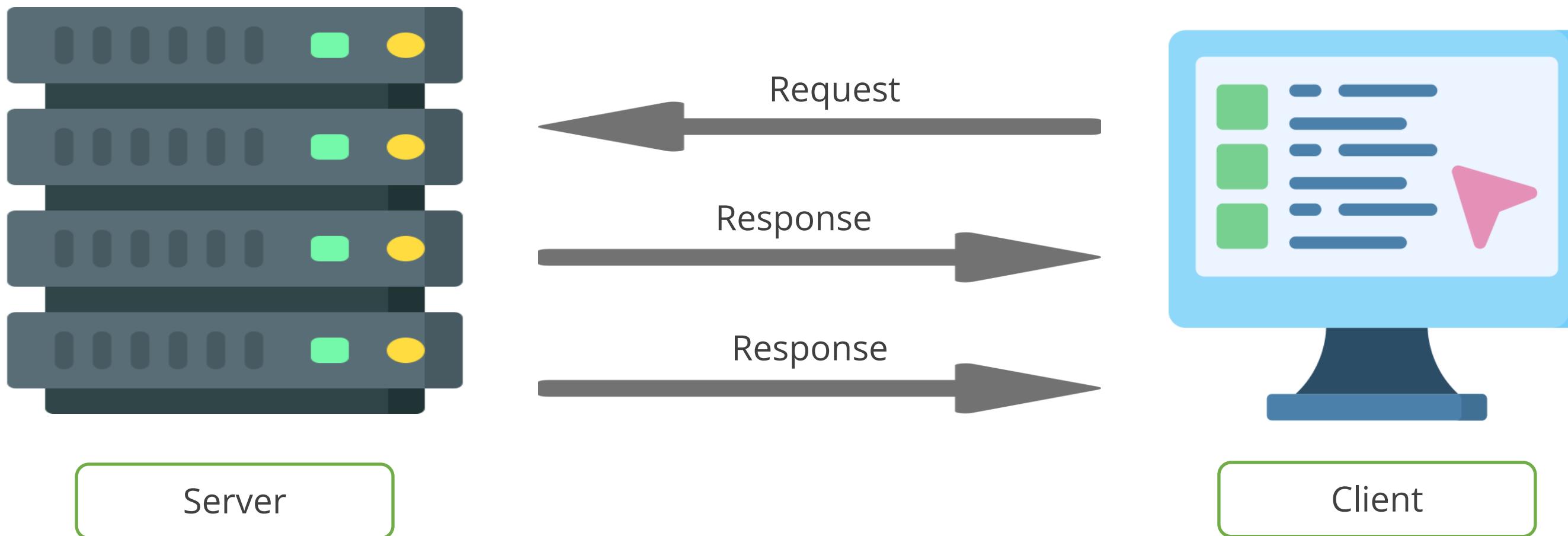
User Datagram Protocol (UDP)

UDP is not very similar to TCP.

- It gives only 'best effort' delivery.
- It is referred to as an unreliable protocol.
- It is considered a connectionless protocol.
- Examples of applications that use UDP: DNS, TFTP, and VoIP.



User Datagram Protocol (UDP)

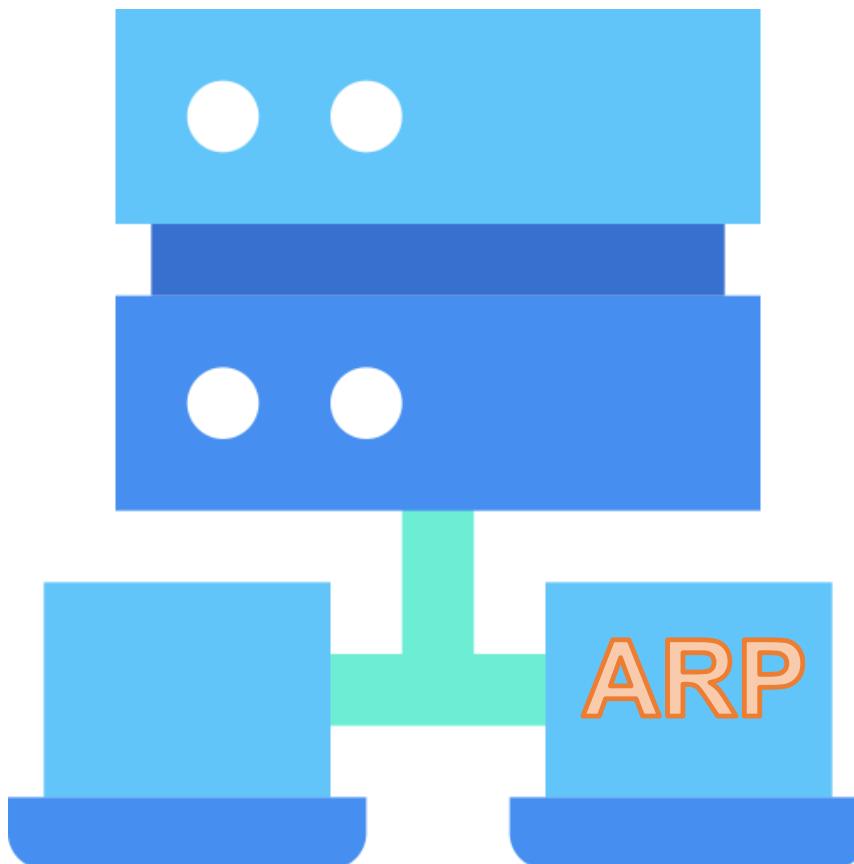


TCP vs. UDP

	TCP	UDP
Connection	TCP establishes connection between the computers before transmitting the data.	UDP sends data directly to the destination computer without checking if the system is ready to receive it.
Speed	Connection-oriented protocol	Connectionless protocol
Reliability	Slow	Fast
Header size	Highly reliable	Unreliable
Acknowledgement	20 bytes	8 bytes
	It takes acknowledgement of data and has the ability to re-transmit if the user requests.	It neither takes acknowledgement nor re-transmits the lost data.

What Is ARP?

ARP stands for Address Resolution Protocol.

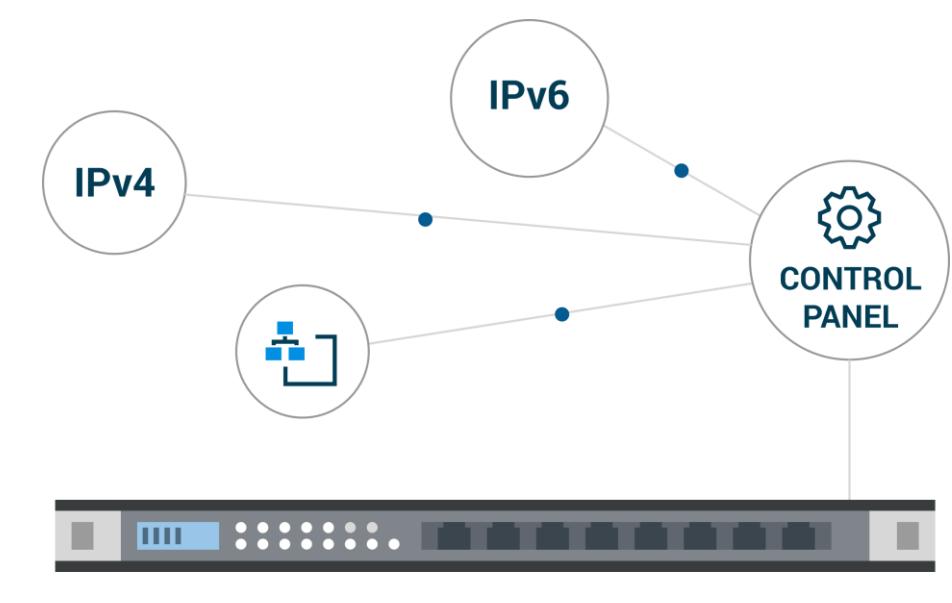


- It is a crucial protocol in networking, especially on LANs, such as the home or office networks.
- ARP translates logical IP addresses, which identify devices on a network, into physical addresses.
- These physical addresses are called media access control (MAC) addresses and are embedded into every network interface card (NIC).

Internet Protocol (IP)

Internet Protocol is a network layer protocol, which handles addressing and routing.

IP specifies the packet format or datagrams and the addressing scheme.

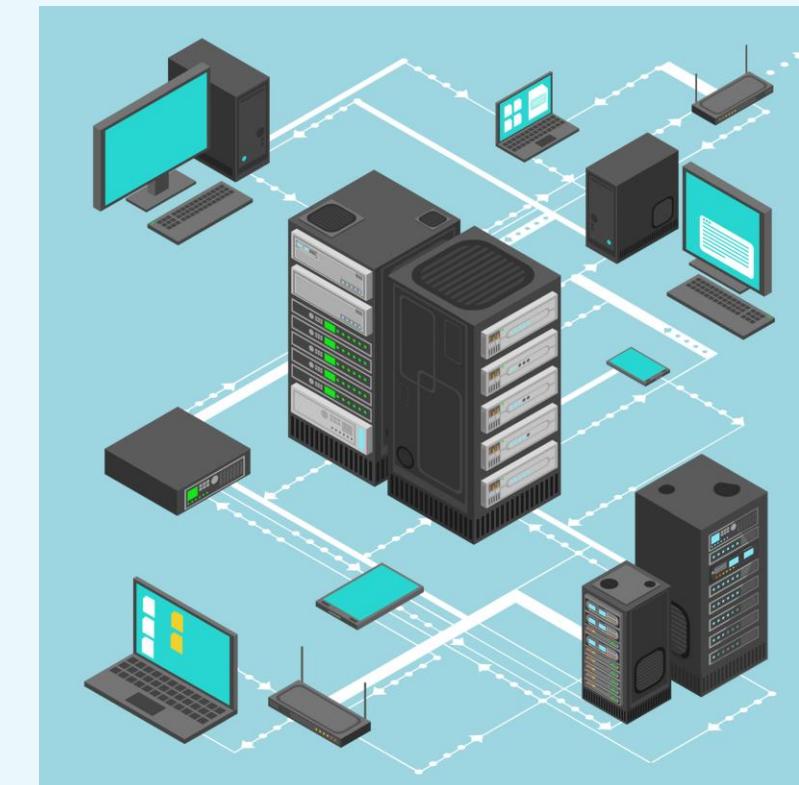


The two types of IP versions are IPv4 (32-bit address) and IPv6 (128-bit address).

Internet Control Message Protocol (ICMP)

ICMP is a management and messaging protocol for IP.

- Its primary function is to send messages between network devices.
- It can inform hosts of a better route to a destination.
- Ping is an ICMP utility used to check the connectivity of devices on a network.



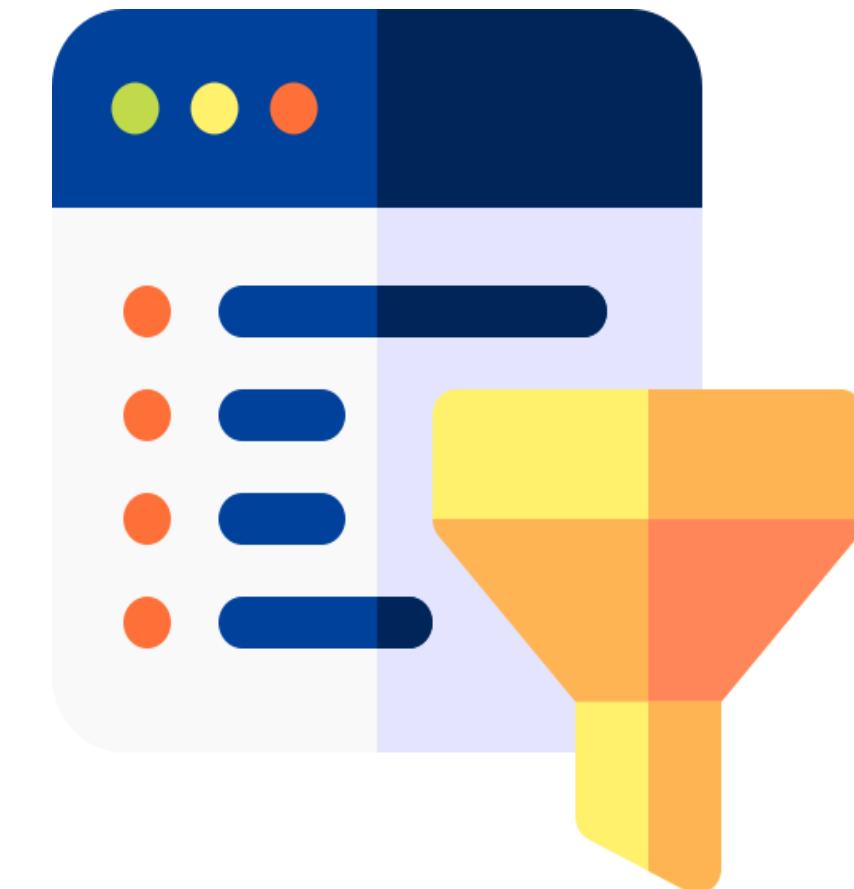
TECHNOLOGY

Web Filtering Technologies

Web Filtering

It refers to technology that monitors and controls which websites users can access on a network.

- It acts like a digital gatekeeper, allowing access to some sites and blocking others based on predefined criteria.
- Web filtering is an essential tool for managing internet access and promoting online safety.
- However, it is crucial to carefully consider the filtering approach and ensure it aligns with your specific needs and ethical considerations.



Web Filtering Technologies

Agent-based filtering

- Agent-based filtering deploys software agents on individual devices to enforce internet filtering rules, ensuring compliance with organizational policies.
- It offers real-time protection at the host and application level, safeguarding every aspect of the network.

Centralized proxy filtering

- Centralized proxy servers act as intermediaries, intercepting and scrutinizing each internet request, applying filtering rules, and allowing only approved traffic.

Universal resource locator

- URL scanning analyzes the web addresses you visit, comparing them against a database of known malicious sites.
- If it detects a match, it raises the alarm, ensuring you don't navigate into dangerous territory.

Web Filtering Technologies

Content categorization

- Web filtering systems classify websites into categories such as 'news,' 'social media,' or 'shopping.'
- This helps organizations control access by allowing or blocking entire categories, ensuring users remain productive and safe.

Block rules

- Block rules allow administrators to specify which websites or content types are off-limits.
- If a user attempts to access a blocked resource, the web filter redirects them away from danger.

Reputation-based filtering

- Reputation-based filtering assesses the trustworthiness of websites based on their history.
- If a website has a bad reputation for hosting malware or engaging in malicious activities, this filter protects users from harm.

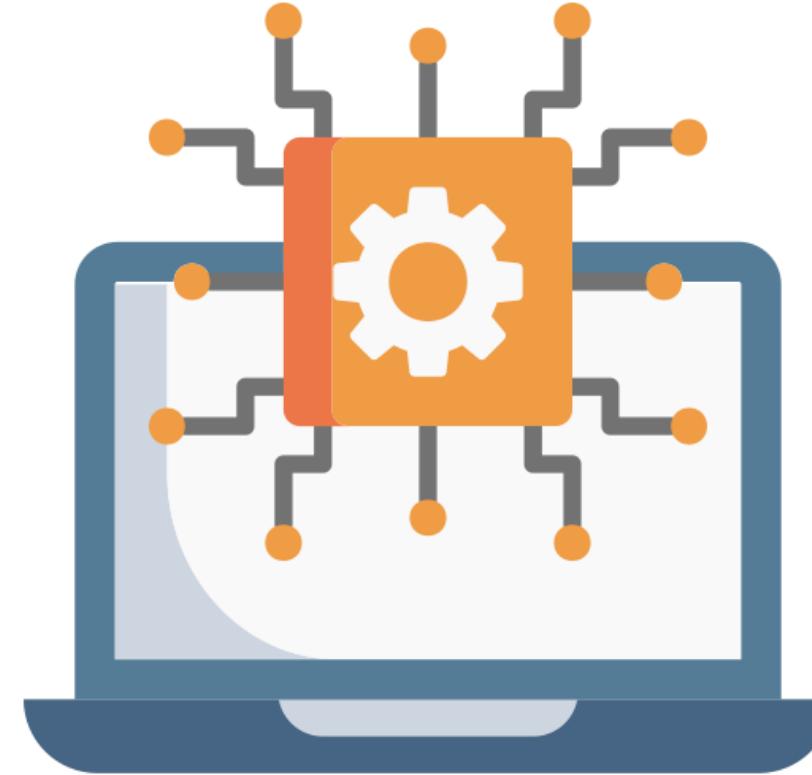
TECHNOLOGY

Operating System Security

Operating System (OS) Security

This involves taking steps to protect an operating system from unauthorized access, data breaches, malware infections, and other threats.

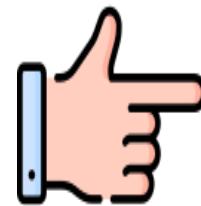
It is crucial for overall computer security, ensuring the system's stability, integrity, and confidentiality.



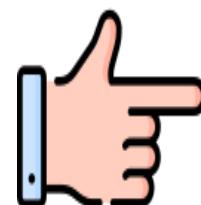
Operating System Security



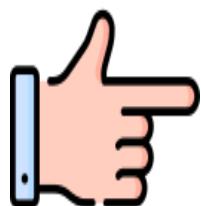
Keep the system updated: OS hardening starts with regular updates. Ensure your OS, software, and applications are up to date with the latest security patches.



User Account Control: UAC ensures that actions requiring administrative privileges are authorized. It prompts users for consent or administrator credentials, preventing malware from executing unnoticed.



Minimize attack surface: Disable or remove unnecessary services and software, as each running service or application is a potential entry point for attackers.



Implement strong authentication: Strengthen user authentication with strong, complex passwords. Enforce policies that require password changes at regular intervals.

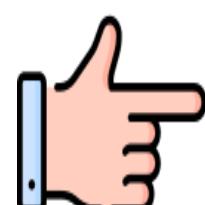
Operating System Security



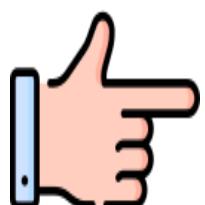
Employ access controls: Follow the principle of least privilege by limiting user and application access to only what is necessary for specific tasks. Regularly review and audit user permissions to prevent unauthorized access.



Enable firewall protections: Activate a firewall to filter incoming and outgoing network traffic, allowing only trusted connections and services to block potential attack vectors.



Encrypt data: Implement encryption for sensitive data both at rest and in transit. Use Full Disk Encryption (FDE) to encrypt data at rest. Other technologies include BitLocker (Windows), FileVault (macOS), and LUKS (Linux).



Monitor and log activities: Enable system logging and monitoring to keep an eye on system activities. Analyze logs regularly to detect anomalies or signs of potential threats.

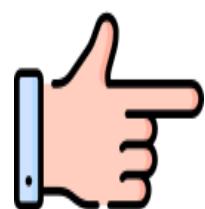
Operating System Security



Patch management: Establish a robust patch management process. Regularly review vendor security advisories and apply patches promptly.



Educate users: Human error is a significant security risk. Train users on best practices, security policies, and the importance of vigilance.



Back up the data: Regularly back up your data and system configurations. In the event of a security incident or data loss, having a reliable backup can be a lifesaver.

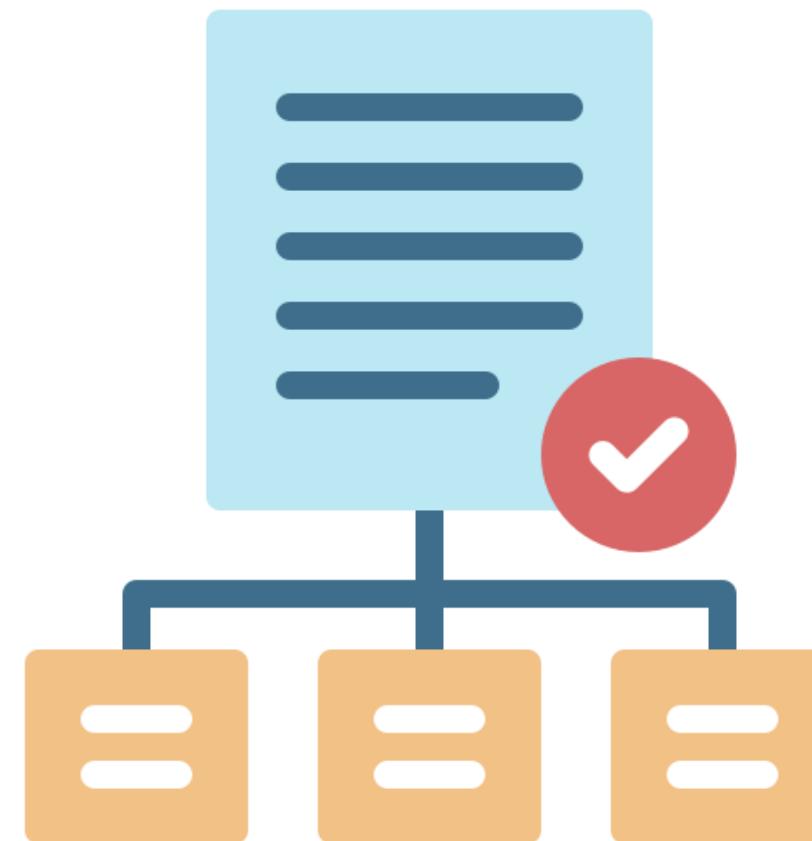


Disaster recovery plan: Develop a comprehensive disaster recovery plan. Know how to restore your system quickly and efficiently in case of a breach or catastrophic failure.

Group Policy

This is used to uniformly apply security settings and automate software installations or updates across a network.

- It can also customize users' desktops to establish a standardized baseline for the organization.
- It is not limited to security settings; it can also automate software installation and updates across a network.
- This ensures that all users have consistent software versions and configurations.



Security-Enhanced Linux (SELinux)

This is a robust security mechanism that provides fine-grained access control.

- It maintains a security policy for system resources and enforces it through kernel-level controls and user-space utilities.
- It follows the principle of least privilege, ensuring that each process and user can only access necessary resources.
- It adds an extra layer of security by enforcing access based on predefined policies, regardless of file ownership or user permissions.



TECHNOLOGY

Email Security

Email Security

Email is a digital method used to exchange messages and attachments between people and organizations over the internet or computer networks.

- Email security encompasses methods and technologies that protect accounts, information, and users from threats.
- It guards against unauthorized access, phishing, and spam, acting like a shield for your inbox.



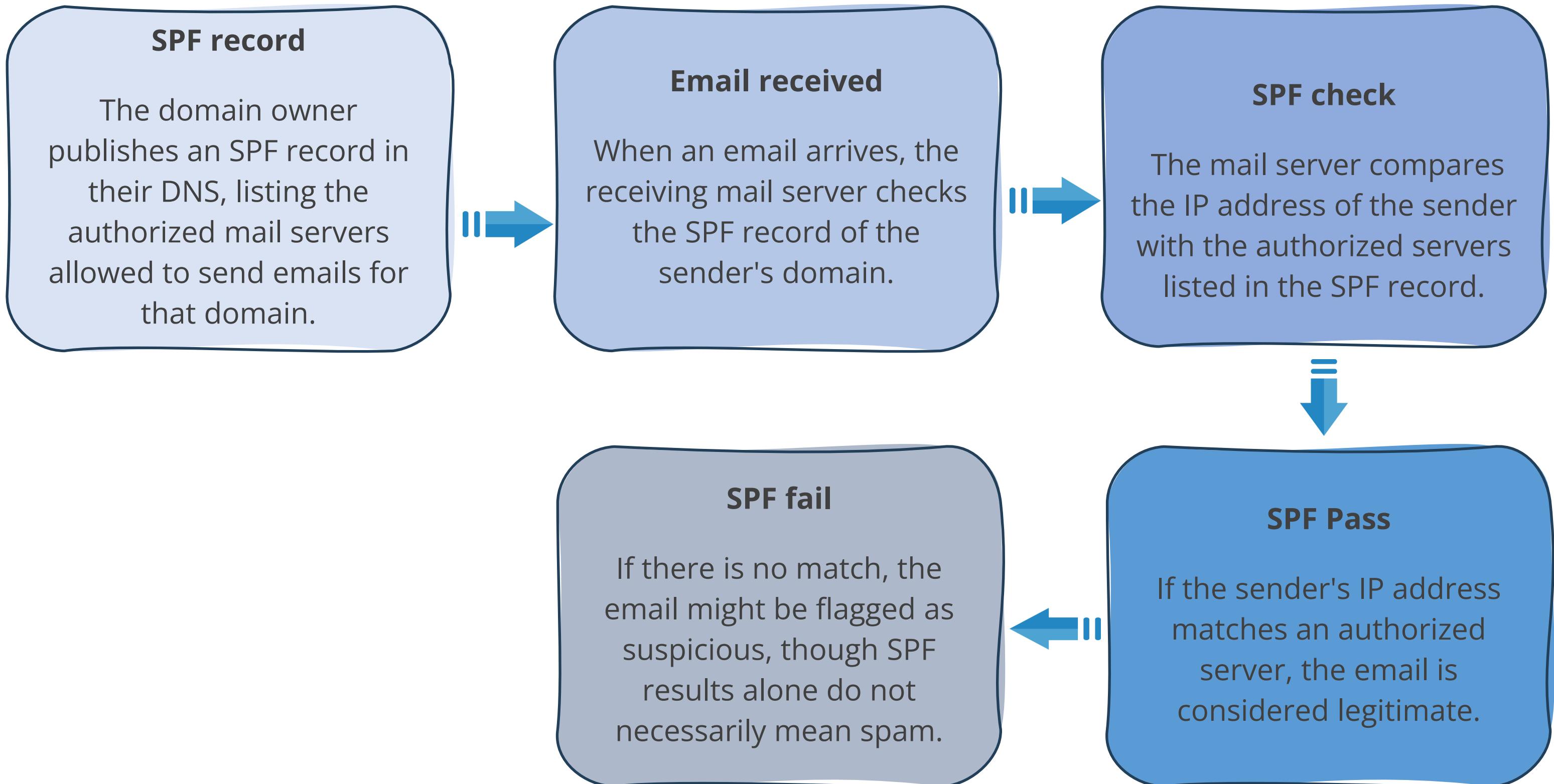
What Is the Sender Policy Framework (SPF)?

It is an email authentication protocol designed to combat email spoofing, a tactic commonly used in phishing attacks.

- SPF acts as a whitelist for email senders.
- The domain owner (the owner of the email address, like '@example.com') publishes an SPF record in their Domain Name System (DNS).
- This record specifies which email servers are authorized to send emails on behalf of that domain.
 - If the IP address of an email server from which they receive email is in the SPF records, then it is legitimate.



How Does SPF Work?



What Is DomainKeys Identified Email (DKIM)?

It is an email authentication protocol that works with SPF to enhance email security.

- It adds cryptographic verification to prevent tampering.
- This method allows senders to digitally sign their emails, and recipients' servers validate these signatures for authenticity.



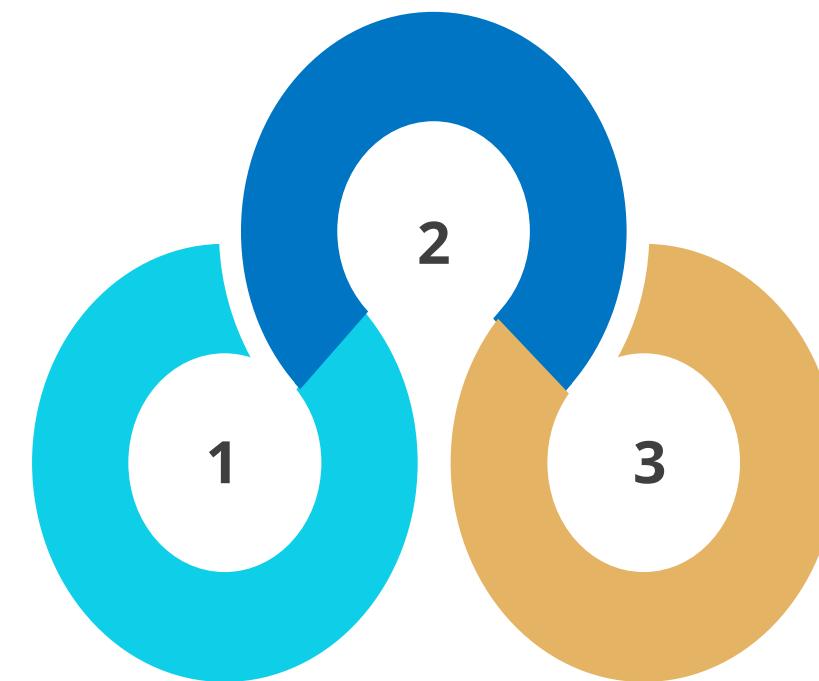
DKIM Process

Verification

When the receiving mail server gets the email, it retrieves the sender's public key from the DNS record and uses it to verify the digital signature.

Digital signing

When you send an email through a DKIM-enabled server, a digital signature is added using a cryptographic key pair: a private key on the sending server and a public key in the domain's DNS records.



Authentication

If verification is successful, it means the signature matches the sender's domain, and the email is likely authentic, ensuring it originated from the claimed domain.

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

This is an email authentication protocol that enhances email security.

- It works alongside SPF and DKIM to specify how mail servers should handle failed authentication.
- It empowers domain owners to dictate actions when authentication fails and instructs email receivers on handling unauthenticated messages.
- It acts as the final layer of defense in the email authentication trio, alongside SPF and DKIM.



How DMARC Works

SPF check

The receiving mail server uses SPF to validate that the email is from an IP address listed in the DNS records of the sending domain. If the sending IP address is not listed in the SPF record, the email fails this check.

DKIM check

The receiving mail server uses DKIM to verify the email header's digital signature against the sender's public DNS key. If the signature does not match, the email fails this check.

DMARC policy retrieval

The receiving mail server retrieves the DMARC policy from the sending domain's DNS records, which specifies actions if SPF or DKIM checks fail.

Reporting

DMARC allows the sender to specify an email address for receiving DMARC verification reports.

Policy enforcement

Based on the DMARC policy, the receiving mail server decides whether to deliver the email to the recipient's inbox, send it to the spam folder, or reject it outright.

Secure/Multipurpose Internet Mail Extensions (S/MIME)

This is a widely used standard for securing email communication through digital signatures and encryption.

- It utilizes a public-key cryptography system to achieve this.
- Encryption: When sending a secure email using S/MIME, the recipient's public key encrypts the email content, making it unreadable to anyone without the corresponding private key.
- Digital signatures: S/MIME also allows for digitally signing emails using your private key to create a unique signature attached to the email.



Pretty Good Privacy (PGP)

This is software that encrypts and decrypts emails, files, and even entire disk partitions.

- It offers versatile cryptographic privacy and authentication for various types of data.
- This secure email method revolves around a pair of keys: a public key, which is openly shared, and a private key, closely guarded by the user.

- To send an encrypted message, the sender uses the recipient's public key.
- Only the recipient, with the corresponding private key, can decrypt the message.
- This method does not rely on PKI infrastructure.



Email Gateway

An email gateway acts as a security checkpoint for email communications, scanning all incoming and outgoing emails for potential threats.

- Email gateways serve as a crucial line of defense against various email threats, such as spam, malware, and phishing attacks.
- Gateways allow policies to be created based on attachments, malicious URLs, and content to prevent them from entering your mail server.
- They can also use data loss prevention to stop personally identifiable information (PII) and sensitive data from leaving the network via email.



File Integrity Monitoring (FIM)

This is a security process that continuously checks and verifies the integrity of critical system files, applications, and databases to alert administrators of any unauthorized changes or corruption.

- FIM safeguards systems by establishing a baseline of normal file and system configurations.
- It continuously monitors these parameters in real-time, promptly alerting the security team or IT administrators to unauthorized changes.
- FIM helps mitigate threats early, ensures compliance with regulations, detects insider threats, protects critical assets, and provides valuable forensic assistance after security incidents.
- Use native tools built into Windows by running the sfc/scannow command with admin privileges.



DNS Filtering

DNS filtering is a security technique that manages internet access by evaluating and filtering DNS requests.

- It blocks or permits access to specific websites or content categories based on established policies, enhancing network security and compliance.
- DNS filtering leverages the DNS to control and restrict internet access on a network.



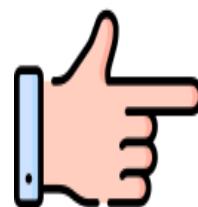
DNS Filtering Functions



Block access to malicious sites: Prevents access to malicious websites, stopping users from stumbling upon phishing or malware sites.



Filter content: Enables organizations to enforce content policies, restrict access to specific website categories, boost productivity, and mitigate legal risks.



Enhance privacy: Offers a layer of privacy protection by blocking access to websites that might track or collect user data without consent, thus safeguarding personal information.



Reinforce security: Blocks access to malicious domains, reducing the risk of cyberattacks and data breaches.

User and Entity Behavior Analytics (UEBA)



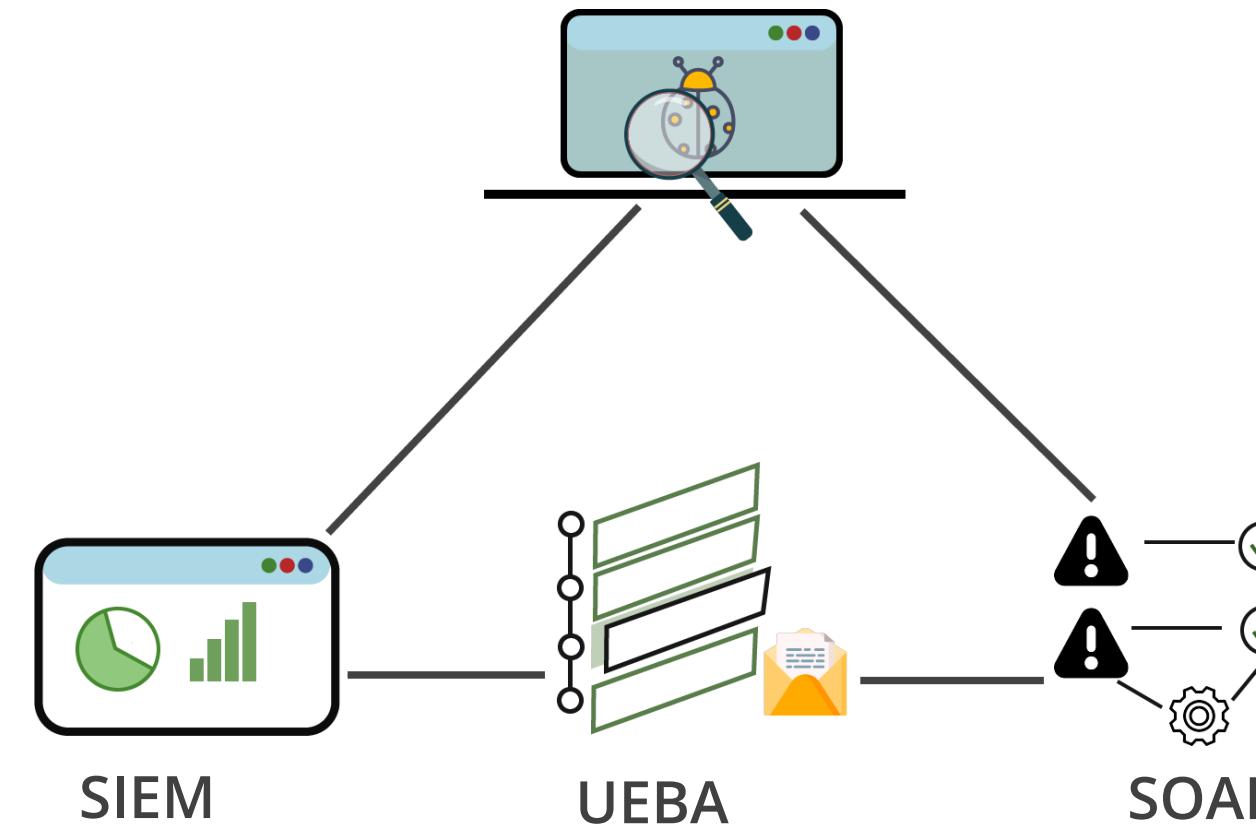
This is a cyber threat detection technology that uses machine learning and deep learning to model the behavior of users and devices on corporate networks.



It can identify abnormal behavior, determine if it has security implications, and alert the security team accordingly.

User and Entity Behavior Analytics (UEBA)

Malware event



- SIEM (Security information and event management)
- SOAR (Security orchestration, automation, and response)

User and Entity Behavior Analytics (UEBA)

User

UEBA technology can monitor user behavior for any peculiar or suspicious activity.

Entity

This technology can monitor entities other than users, such as routers, servers, applications, or even IoT devices.

Behavior

It establishes a baseline of normal behavioral profiles and patterns, then identifies anomalies that deviate from that baseline, which have security significance.

Analytics

The analytics tools based on AI and machine learning algorithms do not require signatures or human intervention and provide automated, accurate threat and anomaly detection.

Antivirus, Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR)

Antivirus

Antivirus software, also called anti-virus software, is a program designed to protect the computer from malicious software (malware) such as viruses, worms, Trojan horses, spyware, and ransomware.

Antivirus software is essential for protecting the computer from various malware threats. By blocking malware, it helps keep your computer secure and running smoothly.



Antivirus Functioning

Scanning

Antivirus software scans the computer for malware. This can be done in real-time as you access files or through periodically scheduled scans.

Detection

When the antivirus software detects malware, it identifies the specific threat.

Removal

It then quarantines or removes the malware from the system.

Prevention

Some antivirus programs also include features to prevent malware from infecting the computer in the first place. This might involve blocking malicious websites or suspicious email attachments.

Endpoint Detection and Response (EDR)

It is a cybersecurity technology that protects individual devices within a network from cyberattacks.

- This solution focuses on desktops, laptops, servers, mobile devices, and other devices connected to the corporate network.
- EDR systems are equipped with advanced monitoring and detection capabilities to identify potential threats by seeking out suspicious behavior.



EDR Functioning

Data collection

EDR solutions continuously collect data from endpoints, including system logs, file changes, network activity, and application behavior.

Detection

Using a combination of signature-based and behavior-based analysis, EDR identifies anomalies and potentially malicious activities. It compares the collected data against known threat indicators and behavioral patterns.

Alerting

When EDR identifies suspicious activity or potential threats, it creates alerts for security personnel to investigate. The alerts are ranked by severity to help prioritize responses.

Response

EDR empowers security teams to respond swiftly to threats. It provides tools to isolate compromised endpoints, contain threats, and remove malicious software.

Benefits of EDR

Enhanced threat detection

EDR goes beyond traditional antivirus by looking for unusual activity patterns that might indicate an attack, even if it's not previously known malware.

Improved business response

EDR provides the data and insights needed to quickly identify and respond to security incidents, minimizing potential damage.

Advanced threat hunting

Security teams can use EDR tools to proactively hunt for threats within their network, even if they haven't triggered any specific alerts.

Improved visibility

EDR provides a comprehensive view of endpoint activity across the network, helping security teams identify vulnerabilities and improve their overall security posture..

Antivirus vs. EDR

Feature	Antivirus	EDR
Focus	Blocking known malware threats	Detecting and responding to all threats
Detection method	Signature-based detection	Anomaly-based and behavior detection
Response capabilities	Limited - May quarantine or remove threats	More advanced - can isolate endpoints, block processes, etc.
Visibility	Limited to individual files	Provides a broader view of endpoint activity

Extended Detection and Response (XDR)

This is an advanced security solution that expands upon EDR.

- While EDR focuses on securing individual devices, XDR takes a broader approach by extending threat detection and response capabilities across the entire IT infrastructure.
- XDR covers a wider range of security data sources, providing a comprehensive view of the organization's digital environment and enabling security teams to detect and respond to threats across the entire attack surface.



XDR Functioning

Unified visibility

XDR integrates data from various security tools across the network, providing a comprehensive view of potential security threats.

Advanced analytics

XDR uses advanced analytics to correlate data from various sources, enabling it to detect complex threats and connections that EDR might miss.

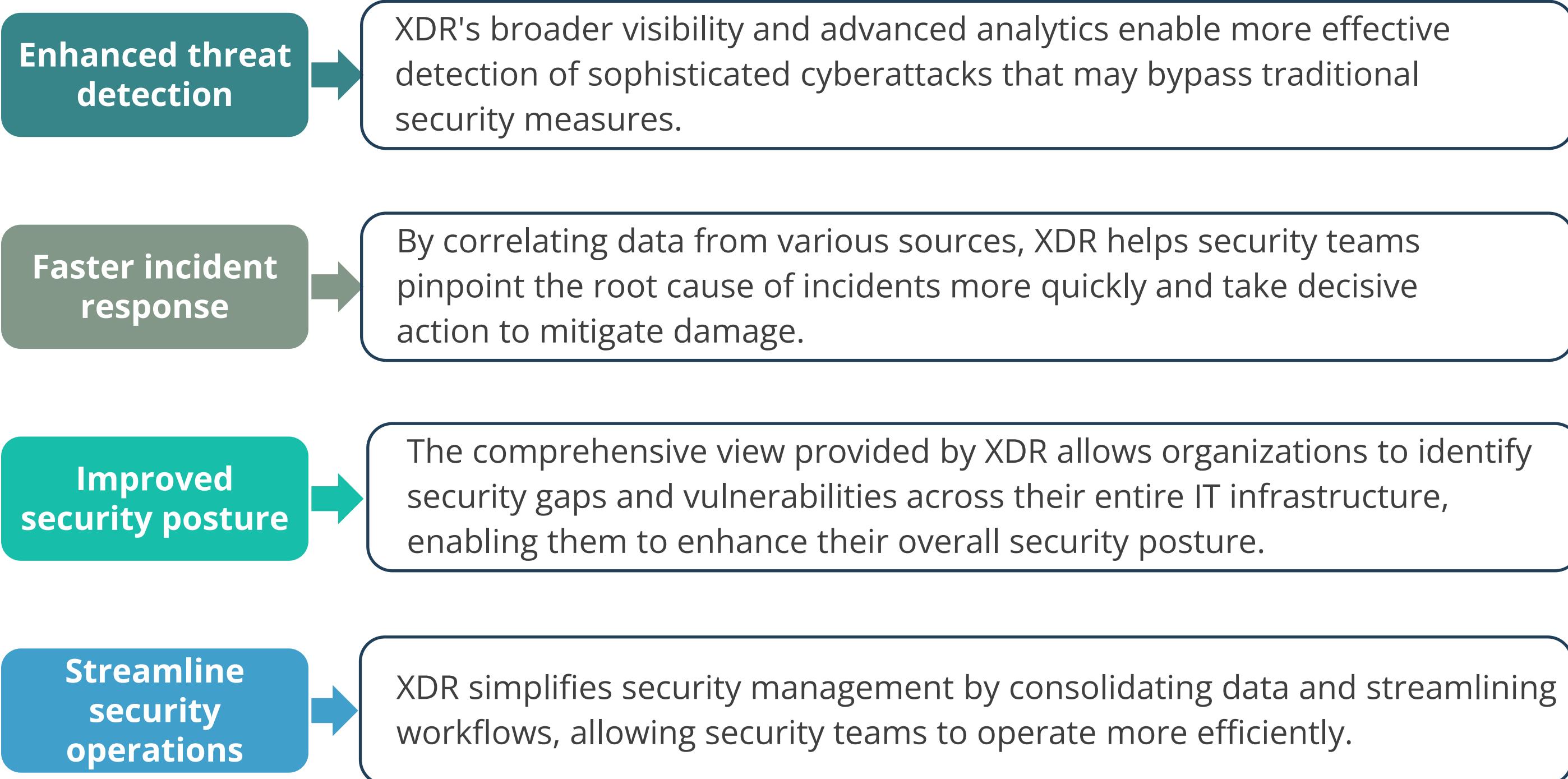
Improved threat hunting

Security teams can use XDR to proactively hunt for threats across the entire network environment, enabling early detection and faster response to emerging threats.

Simplified management

XDR simplifies security management for IT teams by consolidating security data into a single platform, allowing them to view security posture, investigate incidents, and manage responses from a central location.

Benefits of XDR



TECHNOLOGY

Secure Protocols

Secure Communication Protocol

Protocols act as a common language allowing different components to communicate using a known set of commands.

- A secure protocol is a set of rules governing how data is securely transmitted between parties.
- It involves encryption to scramble data and authentication to verify identities.
- They have built-in security mechanisms to enforce security by default.



Secure Protocols

DNSSEC

- Domain Name System Security Extensions (DNSSEC) is a set of extensions to the DNS protocol that, using cryptography, enables origin authentication of DNS data, authenticated denial of existence, and data integrity, but does not extend to availability or confidentiality.

SSH

- The Secure Shell Protocol (SSH) is an encrypted remote terminal connection program used for remote connections to a server.
- SSH uses asymmetric encryption but generally requires an independent source of trust with a server, such as manually receiving a server key, to operate.
- It uses TCP port 22 as its default port.

Secure Protocols

S/MIME

- Multipurpose Internet Mail Extensions (MIME) is a standard for transmitting binary data via e-mail.
- Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of MIME data in e-mails.
- S/MIME offers cryptographic protections to e-mails and is built into most modern e-mail software to facilitate interoperability.

SRTP

- The Secure Real-time Transport Protocol (SRTP) is a network protocol for securely delivering audio and video over IP networks.
- It uses cryptography to provide encryption, message authentication, integrity, and replay protection to the RTP data.

Secure Protocols

LDAPS

- Lightweight Directory Access Protocol (LDAP) is the primary protocol for transmitting directory information.
- By default, LDAP traffic is transmitted insecurely.
- LDAP traffic can be made secure by using SSL/TLS, known as LDAP Secure (LDAPS). Commonly, LDAP is enabled over SSL/TLS by using a certificate from a trusted certificate authority (CA).
- LDAPS communication occurs over port TCP 636.

SNMPv3

- The Simple Network Management Protocol version 3 (SNMPv3) is a standard for managing devices on IP-based networks.
- It was developed specifically to address the security concerns and vulnerabilities of SNMPv1 and SNMPv2.
- SNMP is an application layer protocol, part of the IP suite of protocols, and can be used to manage and monitor devices, including network devices, computers, and other devices connected to the IP network.
- All versions of SNMP require ports 161 and 162 to be open on a firewall.

Secure Protocols

IMAPS

- Internet Message Access Protocol (IMAP), does not secure data, including login credentials, by default.
- IMAP over SSL/TLS (IMAPS) uses SSL/TLS to encrypt the communication channel between the email client and the mail server.

HTTPS

- HTTPS stands for Hypertext Transfer Protocol Secure.
- It encrypts communication between your browser and the website you are visiting, making the data unreadable to eavesdroppers.

Secure Protocols

FTPS

- File Transfer Protocols Secure (FTPS) is the implementation of FTP over an SSL/TLS secured channel.
- It supports complete FTP compatibility and provides encryption protections enabled by SSL/TLS.
- FTPS uses TCP ports 989 and 990.

SFTP

- SSH File Transfer Protocol (SFTP) is the use of FTP over an SSH channel.
- This leverages the encryption protections of SSH to secure FTP transfers.
- Because SFTP relies on SSH, it uses TCP port 22.

Configuring Proton VPN



Duration: 10 Min.

Problem Statement:

As a network security specialist, you are tasked with configuring Proton VPN to secure traffic routing and verify IP addresses. The goal is to ensure the confidentiality and integrity of data transmitted over the network by encrypting internet traffic and masking the user's IP address. This setup aims to enhance privacy, prevent unauthorized data access, and protect against online threats.

Note: Refer to the demo document for detailed steps:
02_Configuring_Proton_VPN

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Install Proton VPN

Implementing Network Segmentation and VLANs



Duration: 10 Min.

Problem Statement:

As a network engineer, you are tasked with demonstrating the process of implementing network segmentation and VLANs using Cisco Packet Tracer. The objective is to enhance network security and management by creating isolated virtual networks within a single physical infrastructure. This involves configuring VLANs to segregate network traffic, thereby reducing the attack surface and improving overall network performance and security.

Note: Refer to the demo document for detailed steps:
[03_Implementing_Network_Segmentation_and_VLANS](#)

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

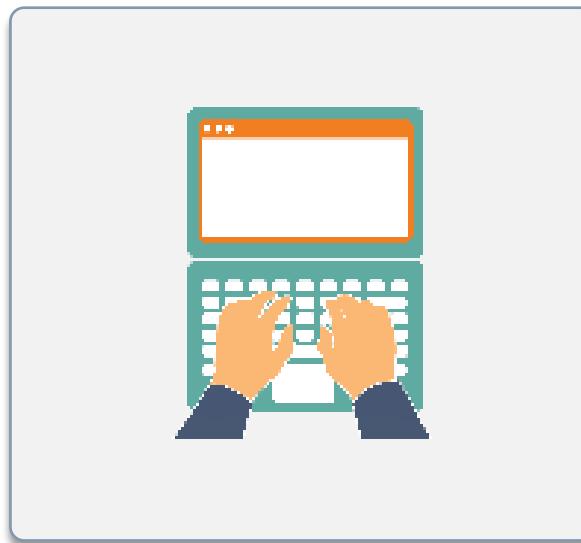
1. Install the Cisco Packet Tracer
2. Load Sample Network and Connect Devices
3. Assign IP Addresses and Verify Initial Connectivity
4. Create VLANs
5. Assign Ports to VLANs and Verify Configuration

Implementing and Maintaining Identity and Access Management

Access, Subject, Object, and Access Controls

The terms access, subject, object, and access controls are defined as follows:

Access



The transfer of data between subjects and objects

Subject



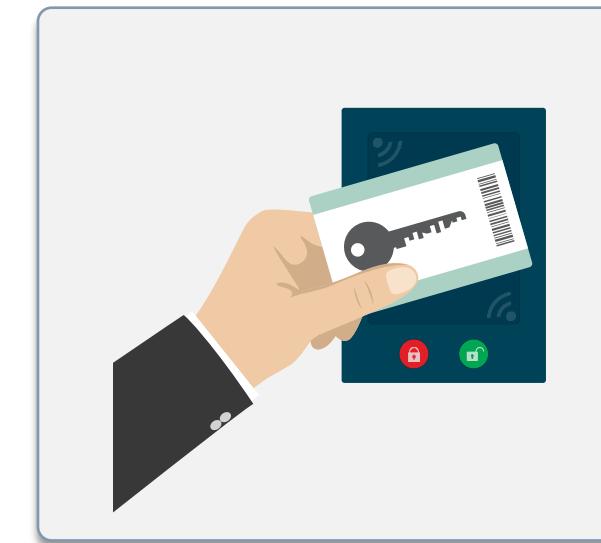
An active component that requires access to an object or the data within it

Object



A passive component that contains data or information

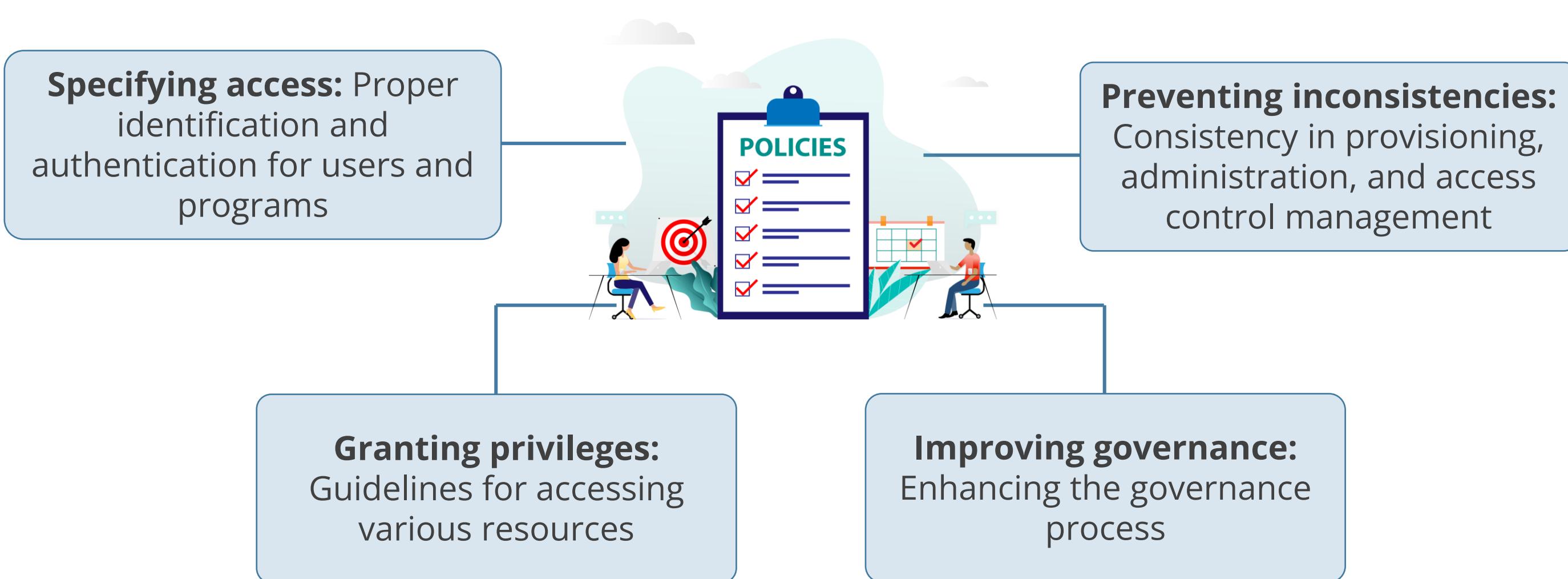
Access control



The security feature that manages how a user or system interacts with and communicates with other systems and resources

Identity and Access Management Policy

An effective access control program in an organization begins with establishing identity and access management policies. These policies include:



Identity Management

It involves the use of products to identify, authenticate, and authorize users through automated means. The goals include:

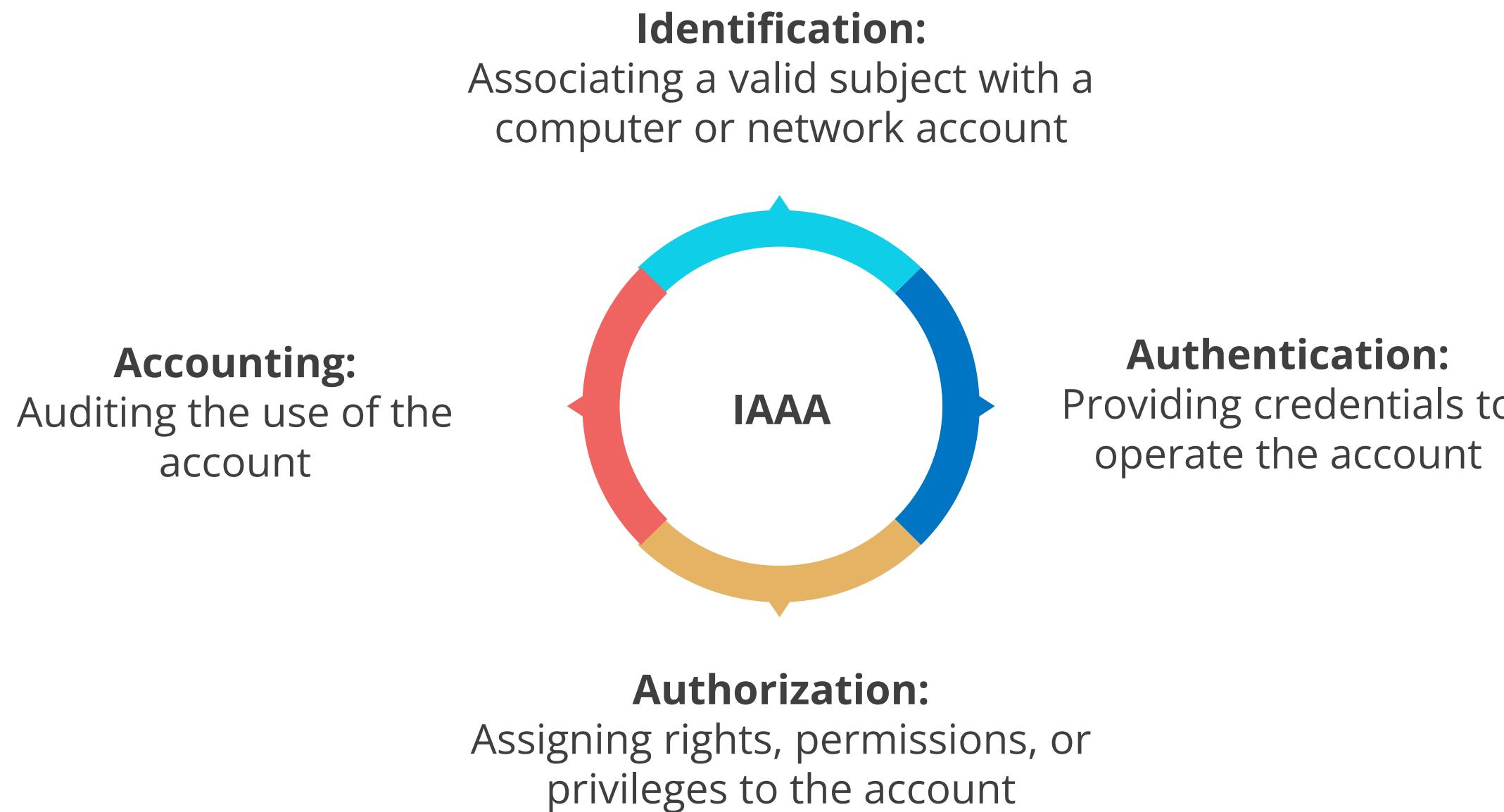
Increasing security and productivity



Reducing cost, downtime, and repetitive tasks

Identity and Access Management

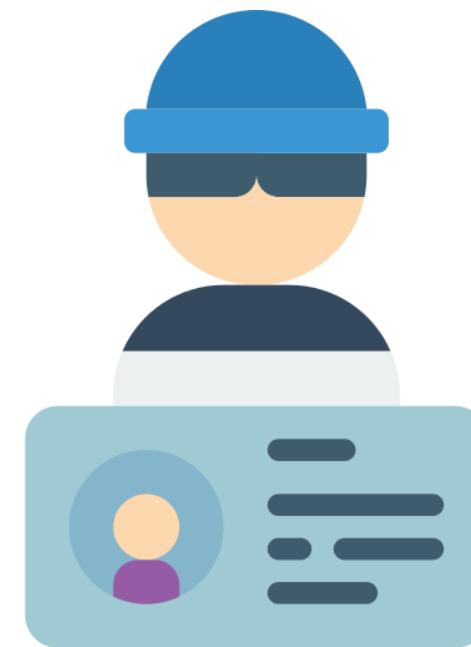
An IAM system consists of four main processes:



Identification



The process of an individual claiming or professing an identity



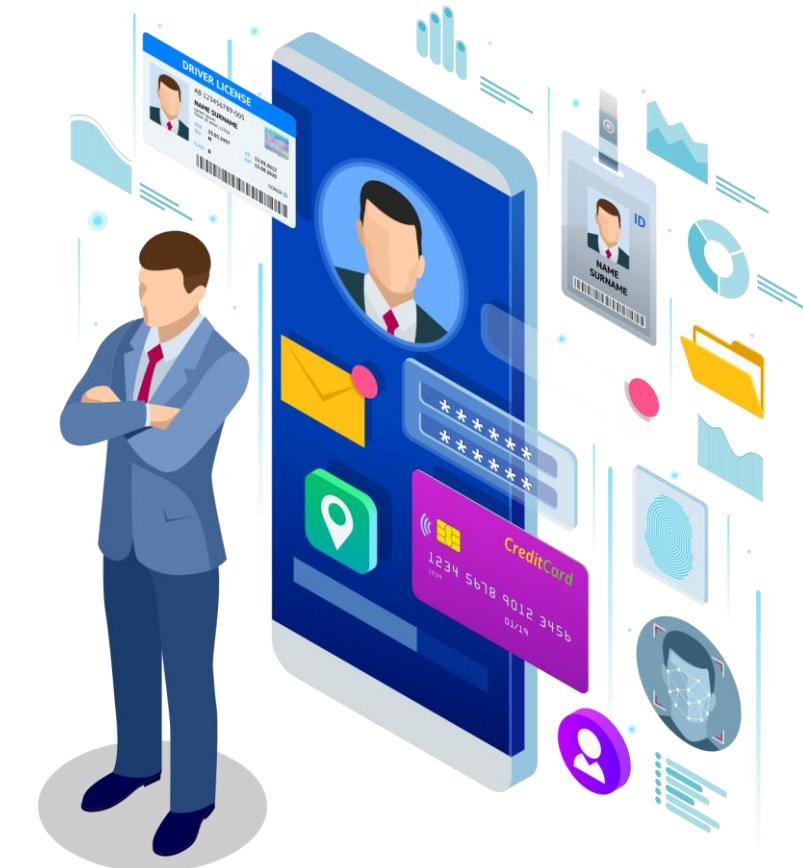
To begin authentication, authorization, and accountability procedures, a subject must submit an identity to the system.

Identification Methods

To authorize applications to access sensitive resources, digital identification methods are used.

Common types include:

- Username
- User ID
- Account number
- Personal Identification Number (PIN)
- Identification badge
- MAC address
- IP address
- Email address
- Radio Frequency Identification (RFID)



Guidelines for User Identification

Three important security characteristics of identity are:

Uniqueness

- User identification must be unique.

Non-descriptiveness

- The user's role or job function should not be exposed by the identity (ID).

Secure issuance

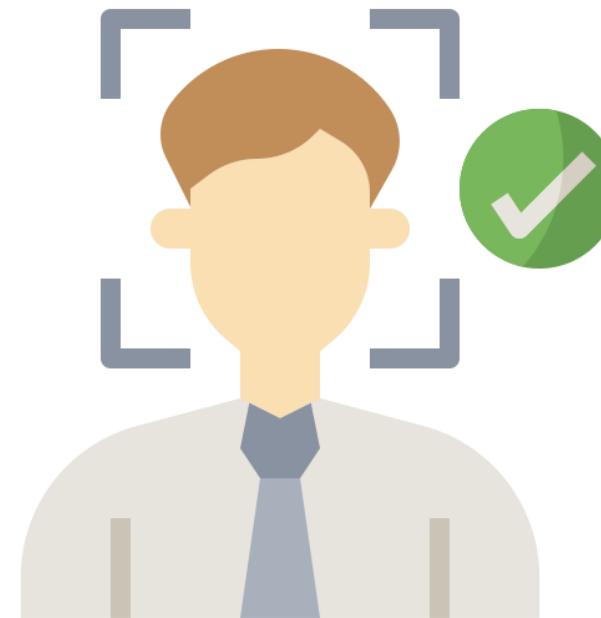
- The ID issuing process must be well-documented and secure.

Authentication



It involves comparing one or more criteria to a database of legitimate identities, such as user accounts, to validate the subject's identity.

Comparing criteria to a database of legitimate identities



Validating the subject's identity

An example of identification and authentication is the use of a username and password. Users identify themselves with usernames and authenticate with passwords.

Authorization



It is the process of granting access to an object after the subject has been properly identified and authenticated.

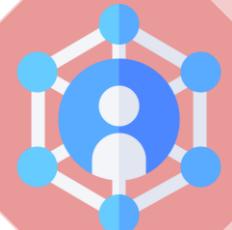
Granting access to an object



Identification and authentication of the subject

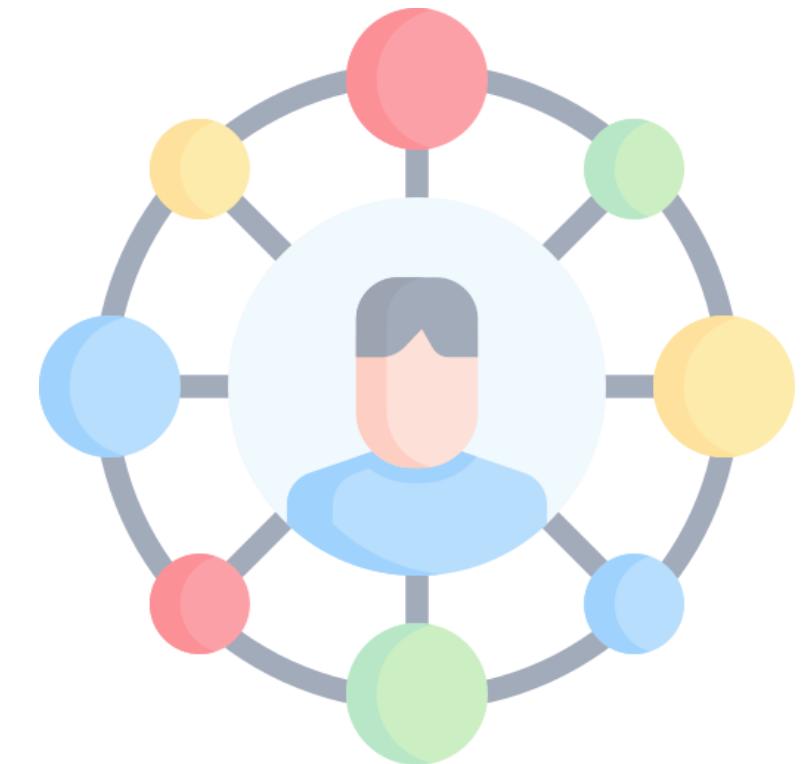
For example, CRUD operations: create, read, update, and delete

Accounting



It refers to a system's ability to associate users and processes with their actions.

Associating users with their actions



Associating processes with their actions

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA)



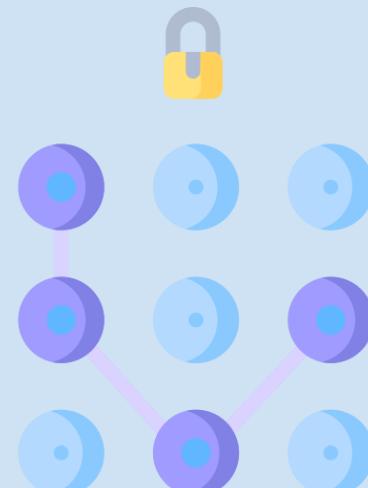
Multi-factor authentication is a type of authentication that necessitates the use of more than one different authentication factor in order to be successful.



Multi-Factor Authentication (MFA)

Based on the type of authentication, MFA can be categorized into:

Something you know



Something you have



Something you are



Implementing Multi-Factor Authentication (MFA)



Duration: 10 Min.

Problem Statement:

As a security specialist, you are required to implement Multi-Factor Authentication (MFA) to enhance the security of user accounts and sensitive data. The goal is to provide an additional layer of protection by requiring users to verify their identity through multiple factors, such as something they know (password), something they have (security token or smartphone), and something they are (biometric verification). This implementation aims to reduce the risk of unauthorized access and safeguard the organization's digital assets.

Note: Refer to the demo document for detailed steps:
[04_Implementing_Multi-Factor_Authentication_\(MFA\)](#)

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Enable the two-step verification of your Google account

TECHNOLOGY

Type 1 Authentication: Password

Password

It is a secret data usually used to confirm a user's identity.

Problems with passwords

- Insecure
- Easily broken
- Subject to repudiation



Common password attacks

- Dictionary (Crack, John the Ripper)
- Brute force (Lophtcrack)
- Hybrid attack (Dictionary and Brute Force)
- Trojan horse login program (Password sending Trojans)
- Social engineering

The combination of username and password is the most common identification and authentication scheme.

Password Types

Passphrase

- Longer than a password, in the form of a sequence of characters
- I will pass CISSP exam
 - Manchester United is my favorite team
 - A quick brown fox jumps over a lazy dog

Cognitive passwords

- The individual's identity is verified based on opinion or fact-based information
- What is the name of the high school you attended?
 - How many family members do you have?
 - What is your mother's maiden name?

One-time password (OTP)

- Dynamic password will be valid for only one login session or transaction
- An OTP a bank sends to a customer via SMS

Password Management

Using passwords is a common practice for validating a user's identity during the authentication process.

A process governing user passwords should consider the following steps:

Set password length
and time limits

Create policies for
password changes and
resets

Use previous login
dates in banners

Limit unsuccessful
logins

Limit the concurrent
connections

Enable auditing

Password Management

Self service password reset

Any process or technology that allows users who have either forgotten their password or triggered an intruder lockout to authenticate with an alternate factor and repair their own problem without calling the help desk.

Assisted password reset

Any process or technology that allows users who have either forgotten their password or triggered an intruder lockout to get their password reset with the help of the help desk.

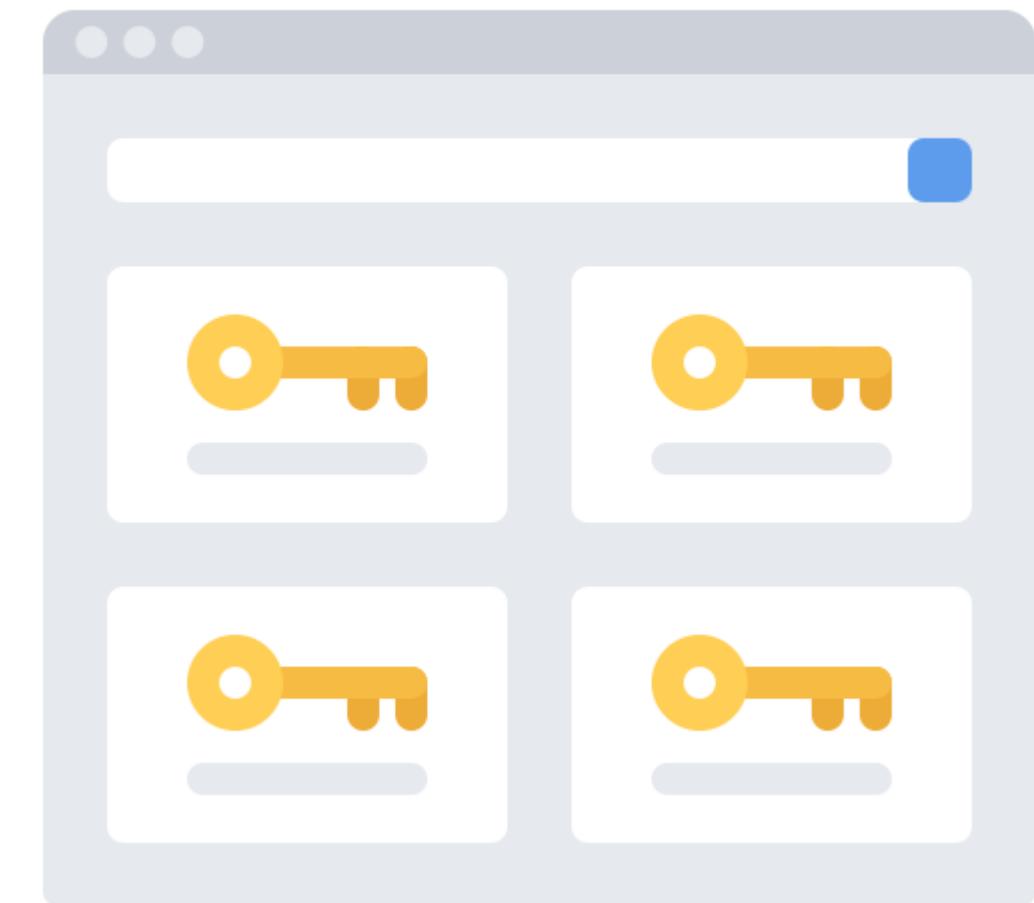
Password synchronization

A process, usually supported by software such as password managers, through which a user maintains a single password across multiple IT systems.

Password Manager

It is a software application that securely stores and manages your login credentials for various online accounts and applications.

- Password managers encrypt passwords and other sensitive data (such as credit card numbers or notes) using robust encryption algorithms.
- They can generate complex, random passwords that are nearly impossible to guess or crack.
- Many password managers offer cross-device syncing, allowing you to access your passwords from any device you use, whether it's your computer, phone, or tablet.



TECHNOLOGY

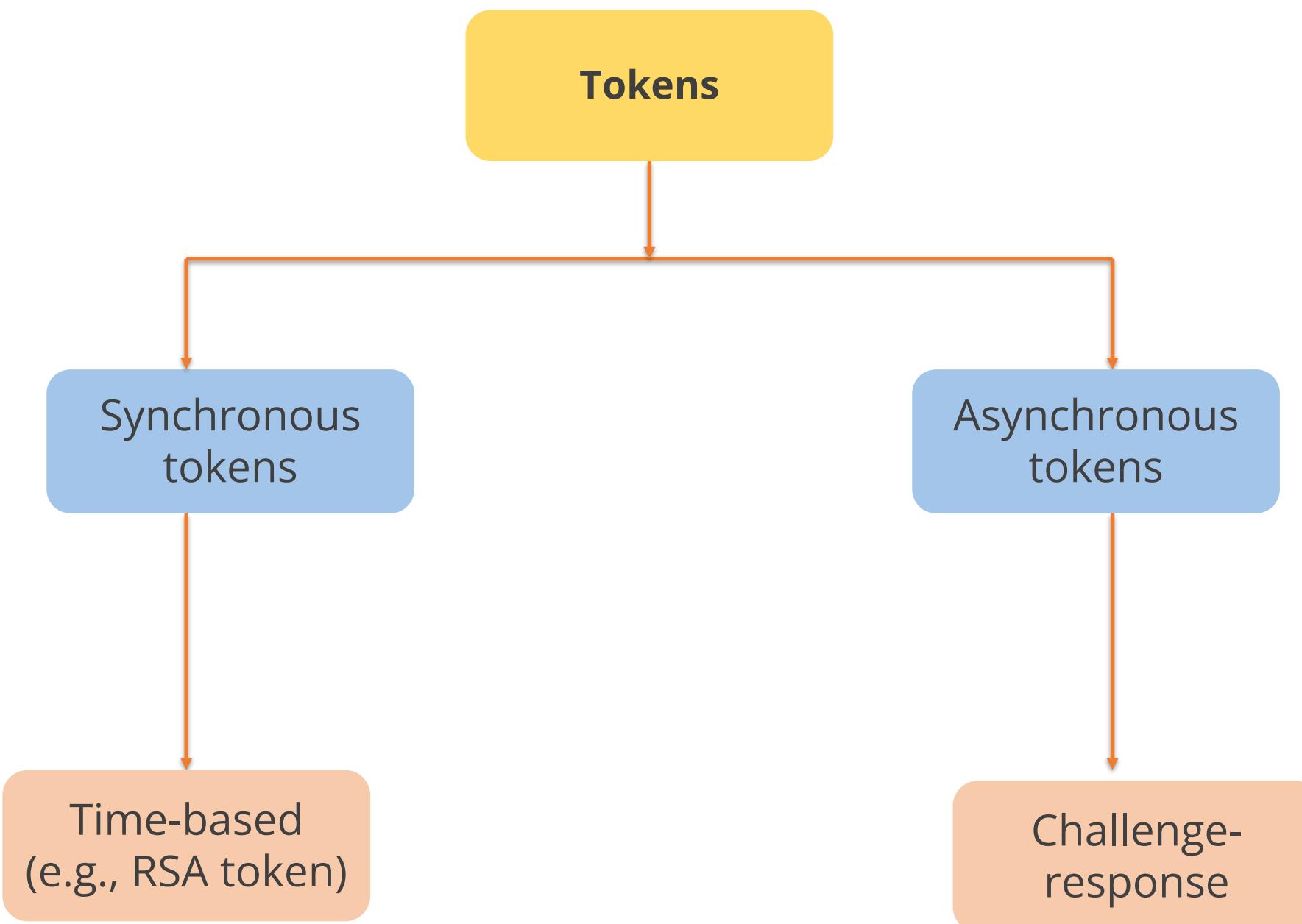
Type 2 Authentication: Tokens

Tokens

- Tokens prove user identity and authenticate to a system or application.
- They can be software-based or hardware-based.
- Attackers can compromise security by gaining control of the token and impersonating the owner, potentially compromising the authentication protocol.
- Tokens must be secured to prevent being cloned, damaged, lost, or stolen.



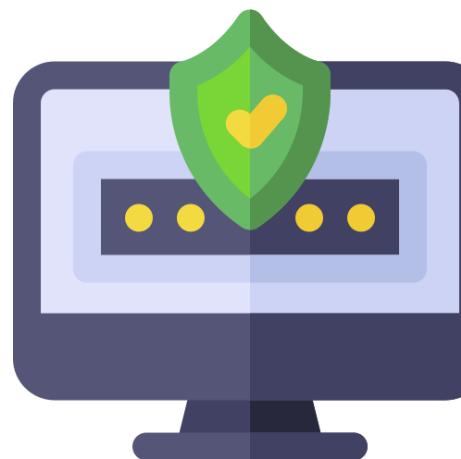
Types of Token



Time-Based One-Time Password



A time-based one-time password (TOTP) uses a cryptographic hash function to combine a secret key and a timestamp, creating an encrypted string for multi-factor authentication.



Time-Based One-Time Password



01

A secret key is agreed upon and shared between the user and the server.

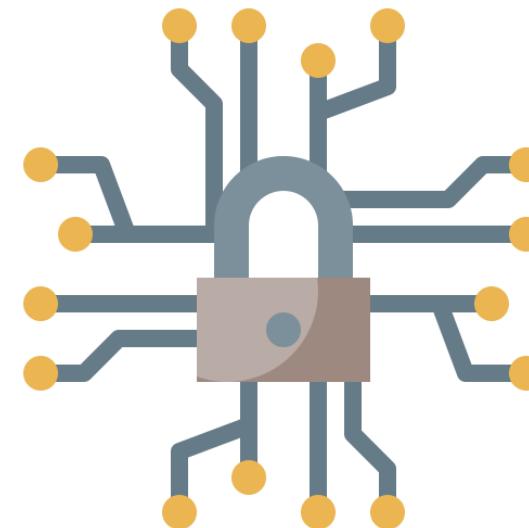
02

The internal clock between the user's device and the server must be synchronized.

03

The clock is based on Unix time, which counts the seconds since January 1, 1970, 00:00:00 UTC.

Time-Based One-Time Password



04

The number of seconds is rounded to 30 seconds by default.

05

The algorithm generates a hash value from the rounded number and the pre-shared secret key.

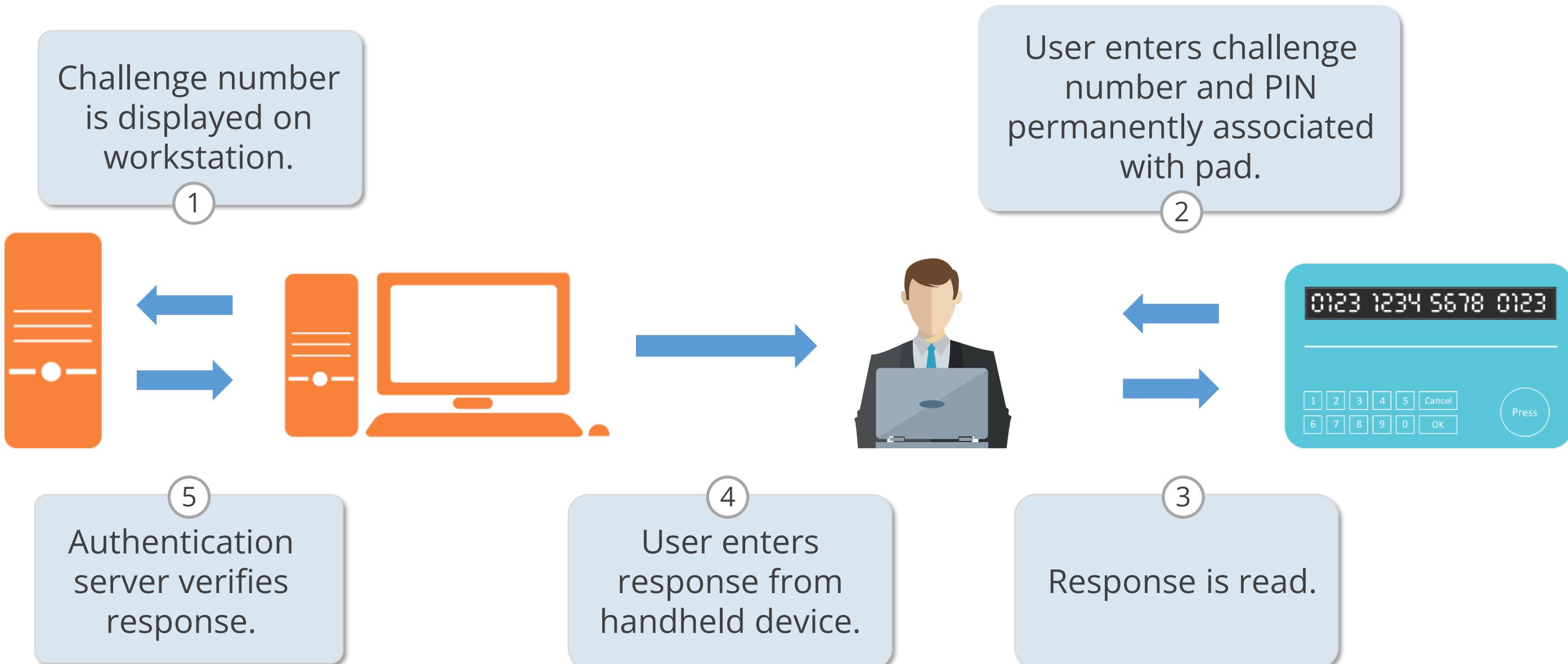
06

The passcode from the user's device must match the server's passcode associated with the user's device.

Token Device: Asynchronous

Challenge-response is used to authenticate a user.

Example: Grid Cards.



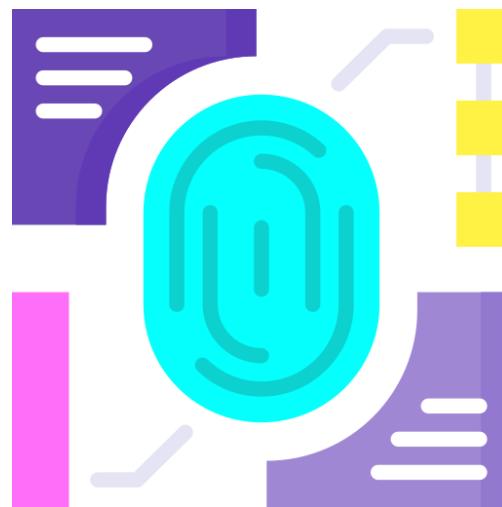
TECHNOLOGY

Type 3 Authentication: Biometric

Biometrics



Verifies a person by analyzing the individual's unique physiological or behavioral characteristics, making it one of the most effective and accurate methods of verifying identification



Belongs to the **something you are** category

Biometric Authentication

Enrollment is the first step in setting up biometric authentication, done by scanning the selected biometric information.

Steps used in the scanning process:



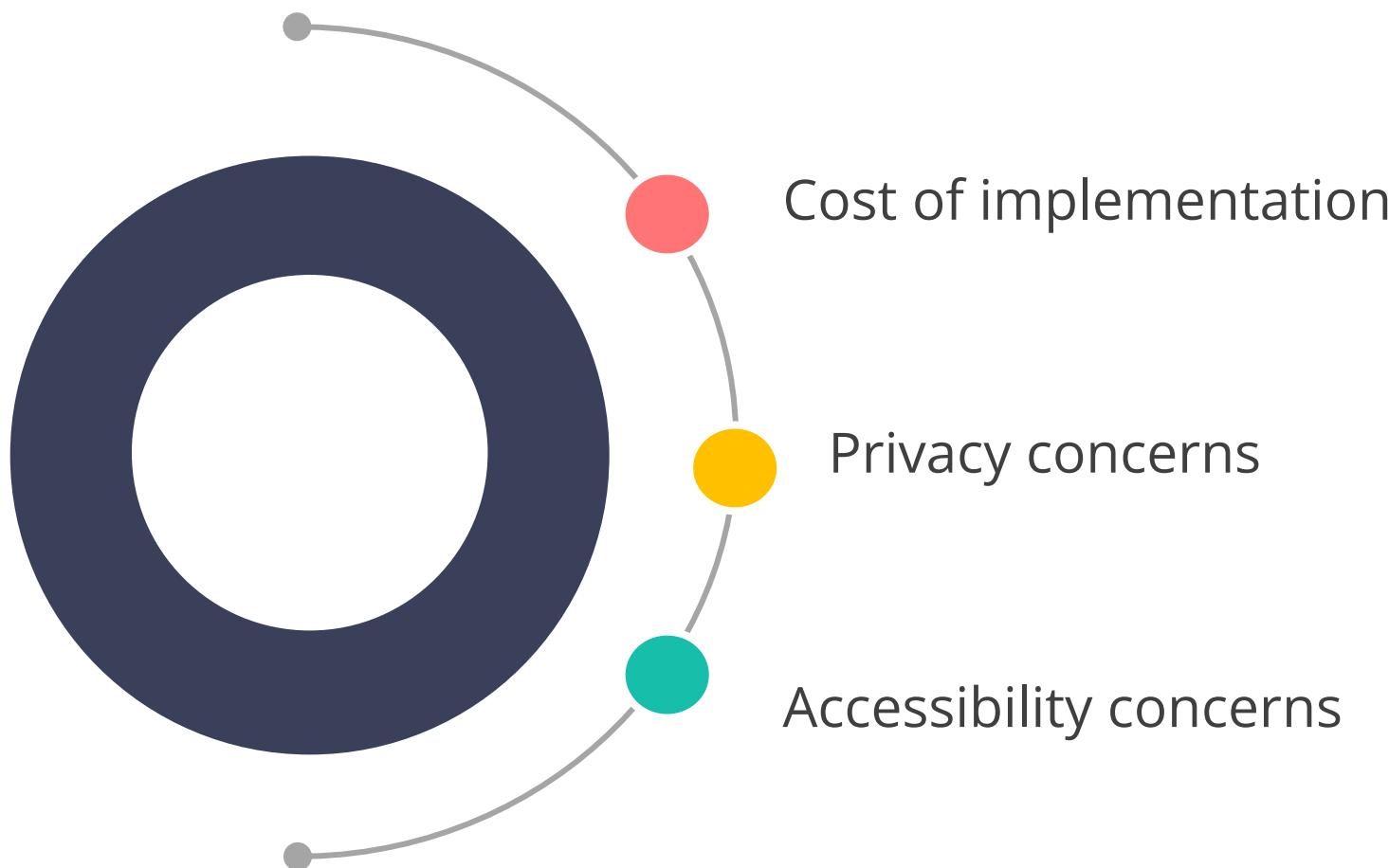
Obtain biometric samples from the target using the sensor module.



Record features that uniquely identify the target in the sample using the feature extraction module.

Efficacy Rates and Considerations

Factors to be considered when implementing biometric authentication are:



Biometrics: Characteristics

Biometrics, based on individuals' physiological and behavioral characteristics, is one of the most effective and accurate methods for verifying identification.

Acceptance

- Refers to user acceptance of the biometric system
- Depends on the privacy intrusiveness and psychological or physical discomfort

Throughput rate

- Also called the biometric system response time
- Refers to the time taken to process an authentication request

Enrollment time

- Refers to the time taken by the biometric system to register and create an account for the first time

Biometric Authentication

Patterns used to identify people biometrically are:

Physical

- Fingerprints
- Iris and facial recognition

Behavioral

- Voice recognition
- Typing pattern matching

Biometrics

The following are some common types of biometrics:

Keyboard pattern
recognition



Facial scan



Retina scan



Iris scan



Voice pattern
recognition



Fingerprint



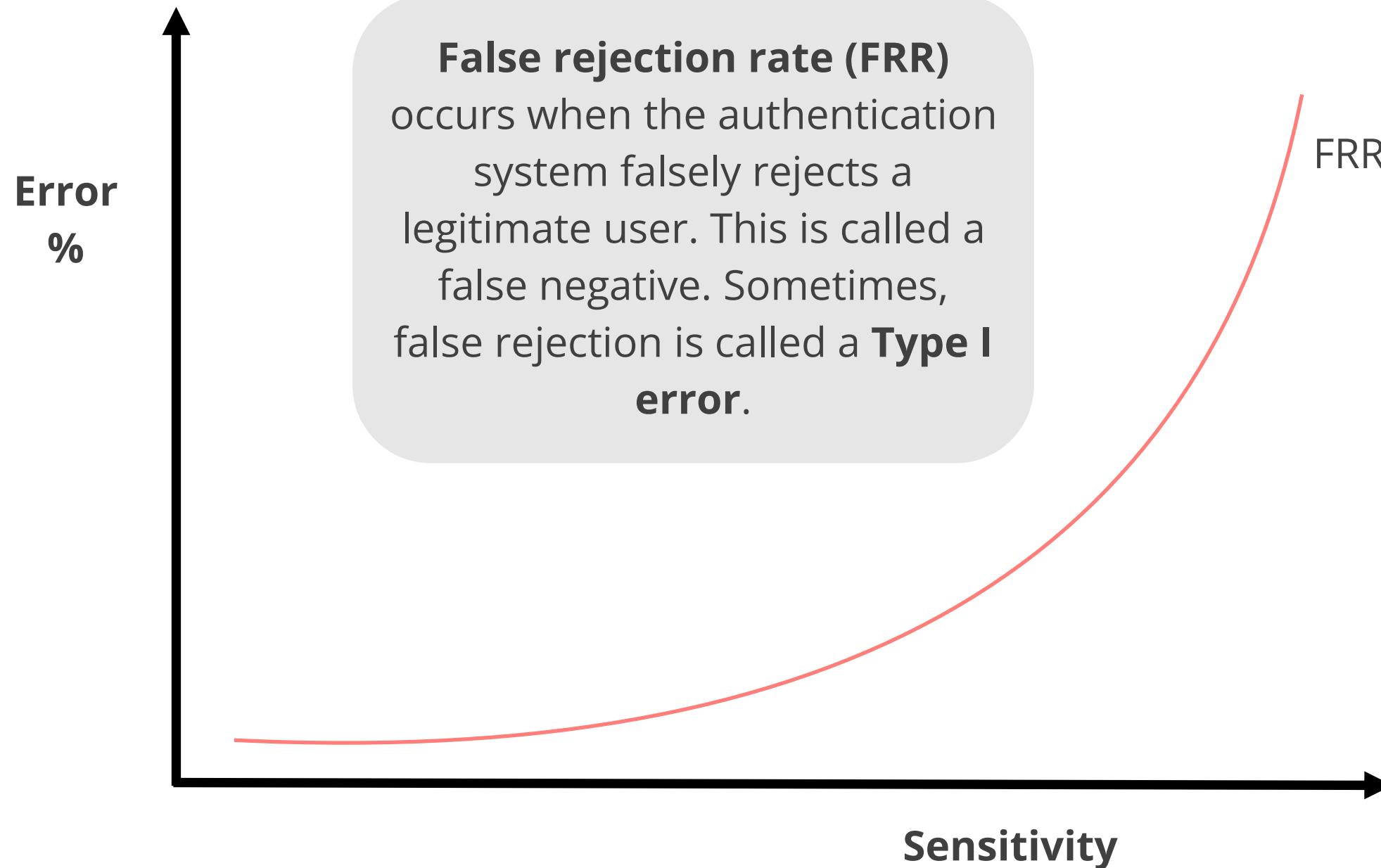
Signature scan



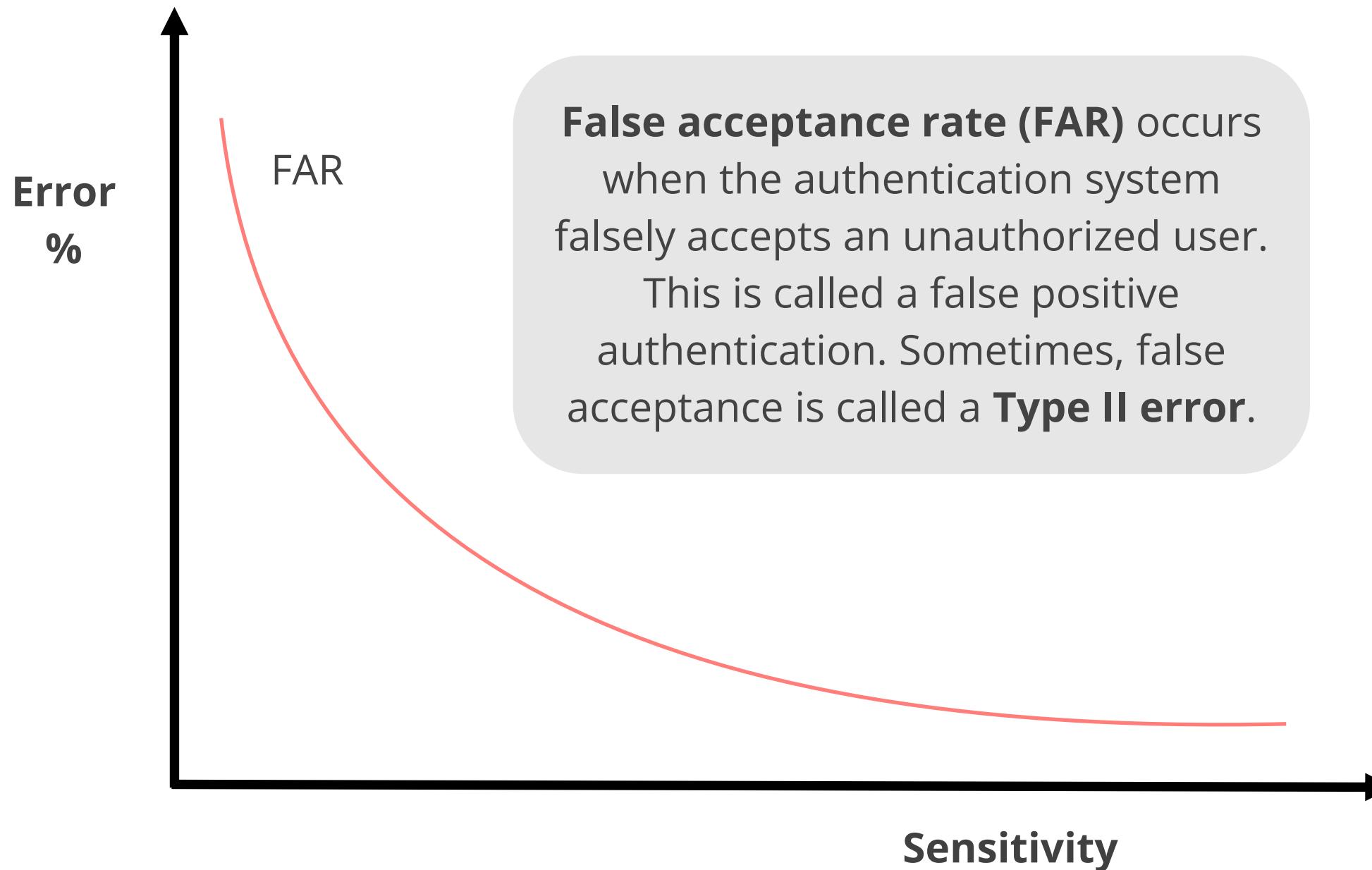
Palm scan



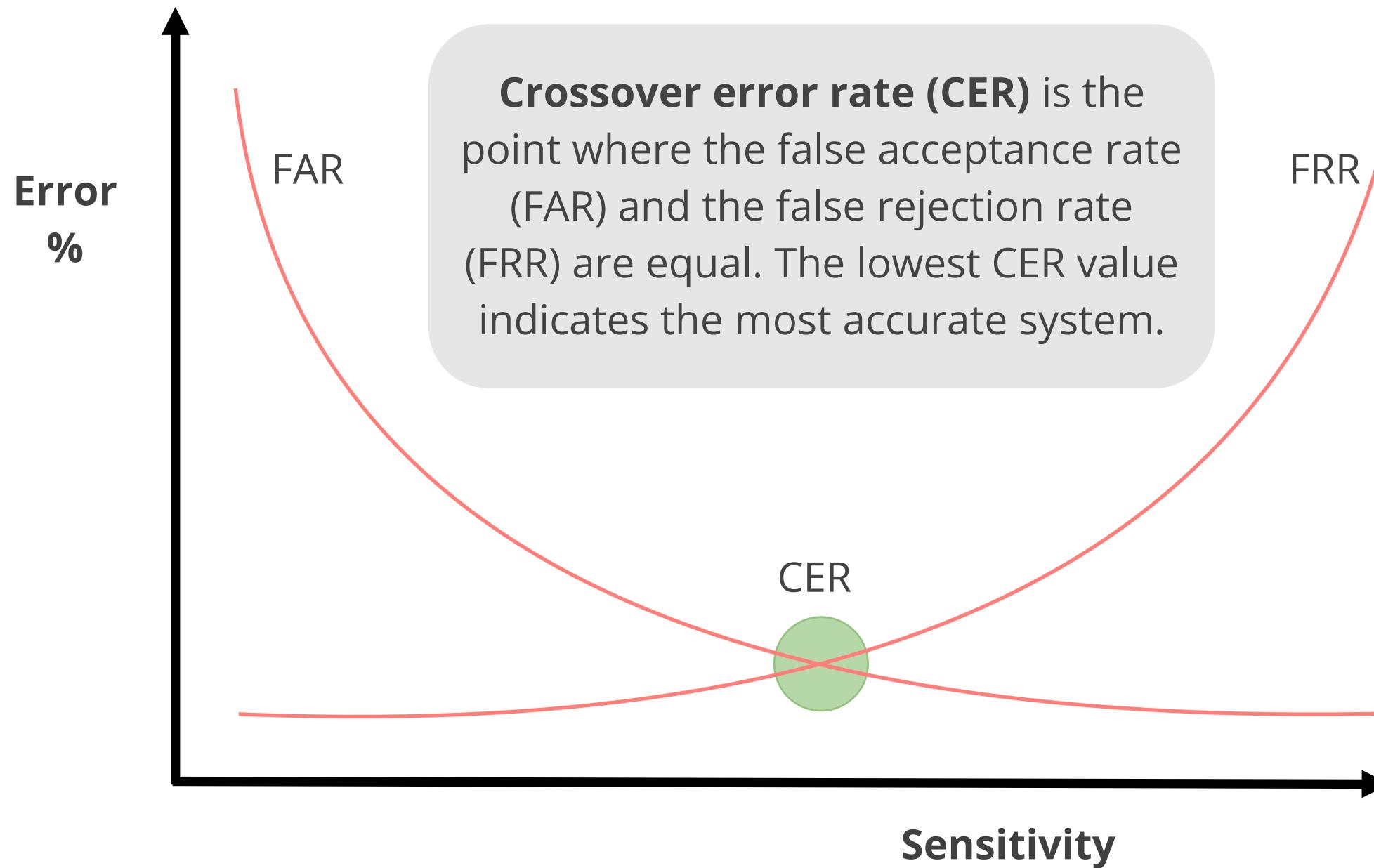
Errors in Access Control



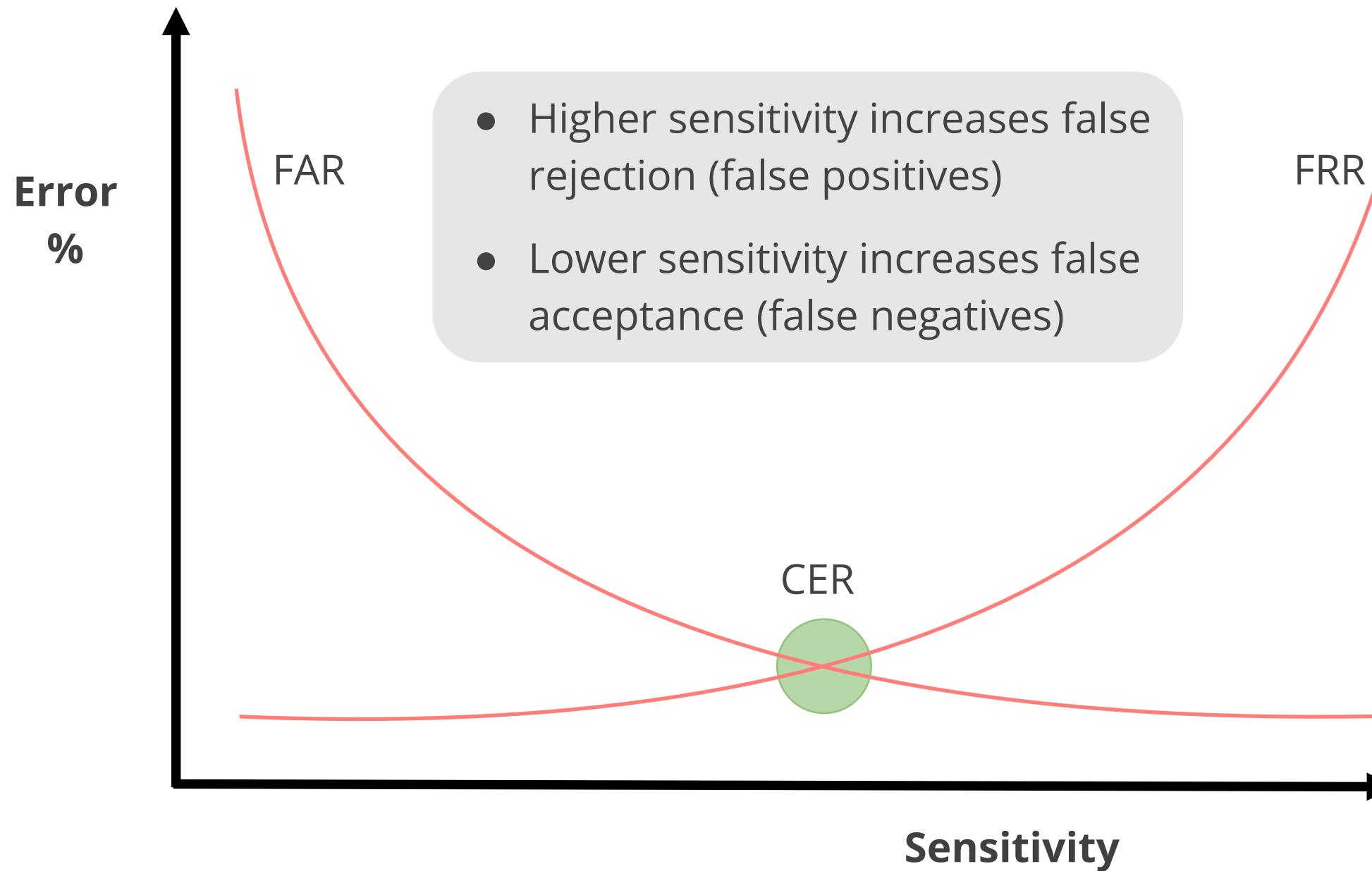
Errors in Access Control



Errors in Access Control



Errors in Access Control



Biometric and Behavioral Technologies

Certain biometric and behavioral technologies can be used for purposes other than login authentication:

Biometric identification

Matches people to a database rather than having them perform identity verification themselves

Continuous authentication

Verifies that the logged-in user is still operating the device

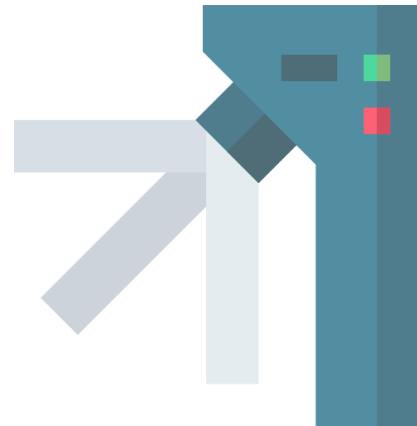
TECHNOLOGY

Passwordless Authentication

Passwordless Authentication



Passwordless authentication allows users to log into a system without entering a password or any other knowledge-based secret.



Users input public identification and provide secure proof of identity through a registered device or token to complete the procedure.

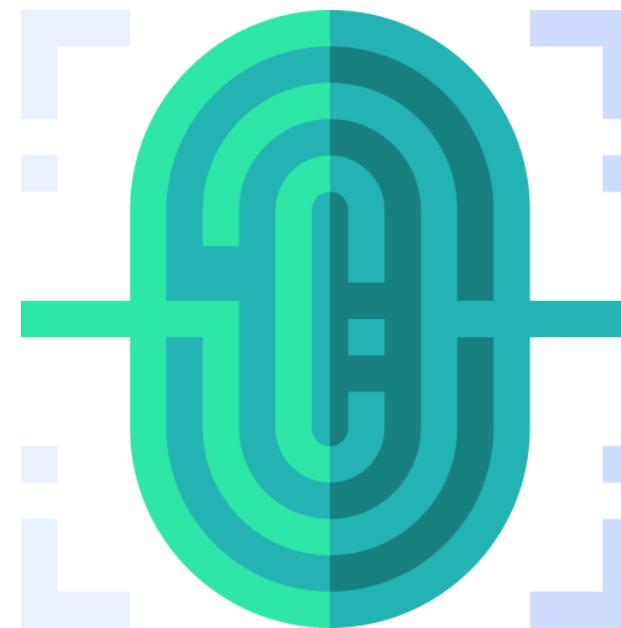
Passwordless Authentication



Why Passwordless?

- Presents usernames and passwords as the most common and insecure forms of authentication
- Shows that over two-thirds of people reuse passwords across sites
- Reports that eighty-one percent of successful cyber attacks in 2018 were due to compromised usernames or passwords, according to a Verizon report

Passwordless Authentication



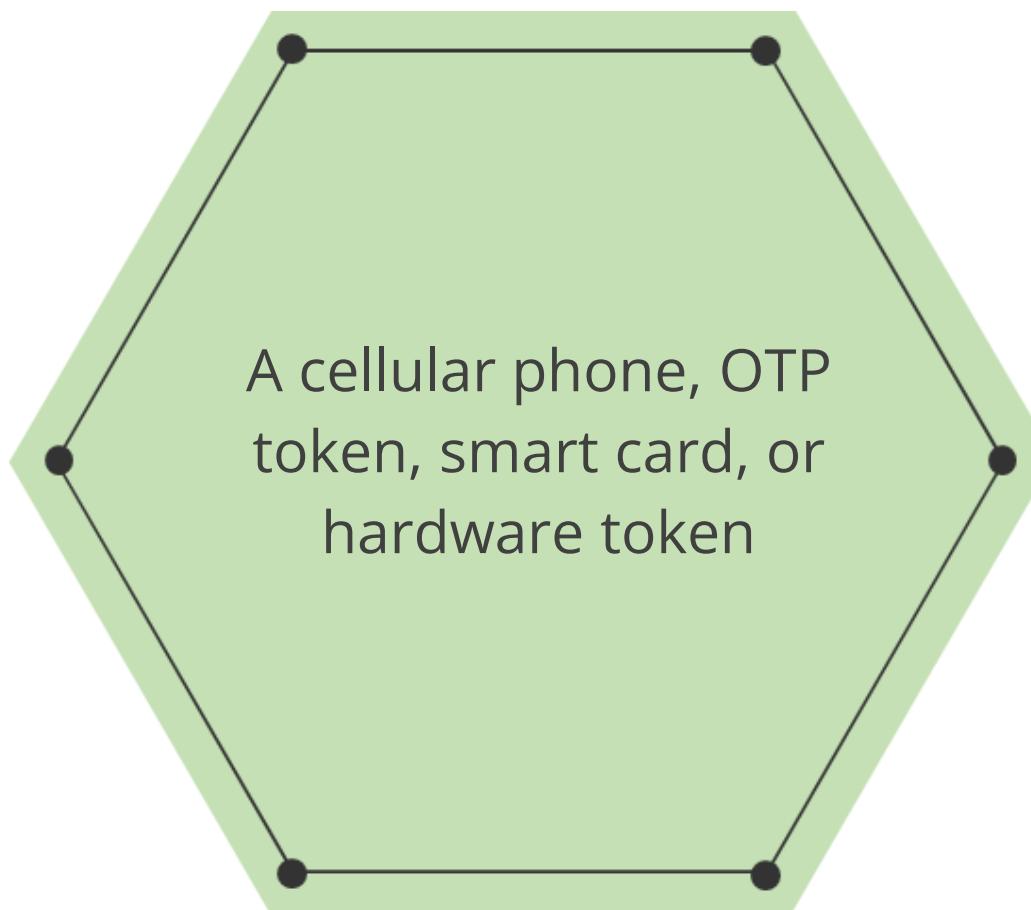
Why Passwordless?

- Reduces risk by 99.9%
- Adds an additional layer of protection with MFA
- Does not require a memorized secret

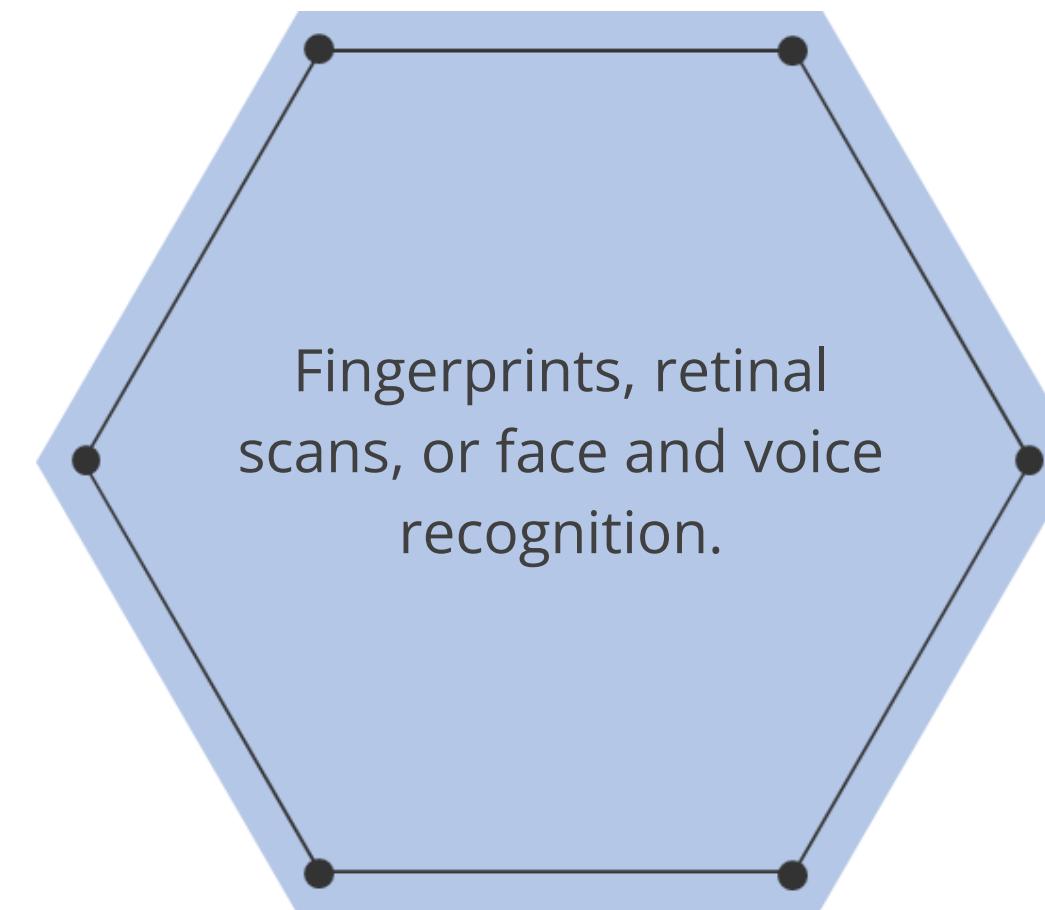
Passwordless Authentication

The user's identity can be proved using an alternative factor such as:

Something you have



Something you are



Benefits



- Eliminates the need for end users to create, manage, or remember passwords
- Highlights the fragility of passwords and their role in security violations, promoting passwordless security as a better option
- Reduces the headache for IT departments in resetting lost passwords

TECHNOLOGY

Authorization and Accounting

Access Criteria

An organization should grant access privileges to subjects based on their level of trust and need-to-know basis.

Access criteria include the following:

Transaction

Access is based on user privileges to perform specific commands and functions on data.



Roles

Access is granted depending on the role or job function in the organization.



Groups

Create user groups and assign rights and privileges to these groups.



Location

Access is given based on the location of the user.



Time

Access is granted depending on the time of the day.



Authorization Concepts

Authorization is based mainly on the following concepts.

Need-to-know principle

According to this principle, the subject is given access to specific information depending on their job, duties, and requirements.

Authorization creep

Authorization creep occurs when an employee moves from one department to another and is assigned new access rights without reviewing and removing old permissions.

Access control list (ACL)

An access control list specifies the subjects granted access and the operations allowed on objects.

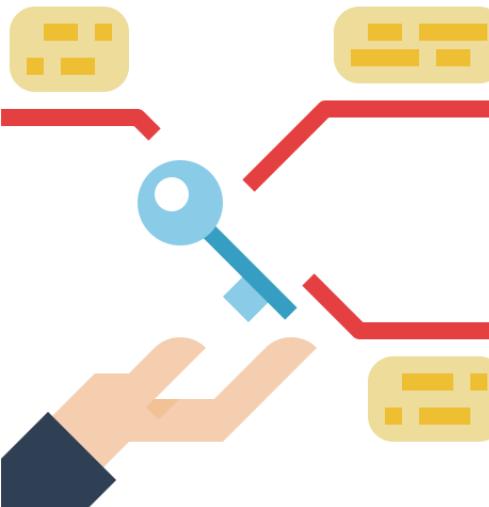
Default to zero

Access controls should start with zero access, allowing the administrator to grant access based on the organization's security policy.

Least Privilege



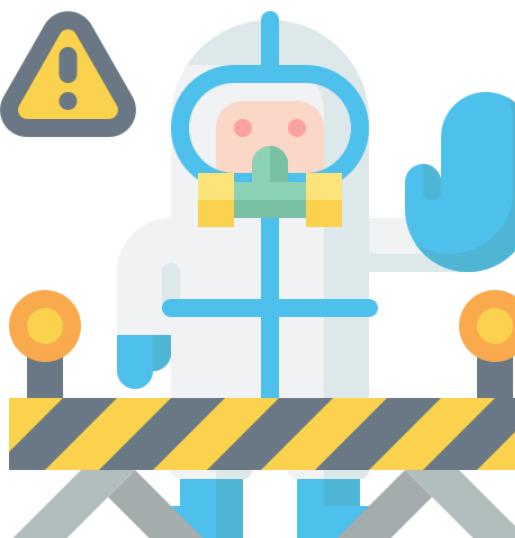
According to the concept of least privilege, users should be given only the minimum access necessary to accomplish their tasks.



Least Privilege



This guarantees that users cannot execute any tasks that are not part of their allocated duties. For example, less than 1% of Google employees get to set foot inside their data centers.



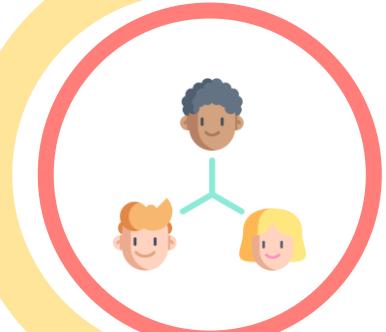
Need-to-Know



The **need-to-know** principle ensures that users are granted access only to the information necessary to complete their work tasks.



Separation of Duties



The **separation of duties** principle ensures that the sensitive tasks are split into the tasks performed by more than one person.



Separation of Duties



Separation of duties is an internal control that creates a system of checks and balances to prevent fraud and errors.



Accountability

Accountability ensures users are responsible for their actions and enforces security policies. The following provides an overview of items and actions that can be audited and logged:

System-level events

- System or computer performance
- Successful and unsuccessful login attempts
- Timestamps of the login attempts

Application-level events

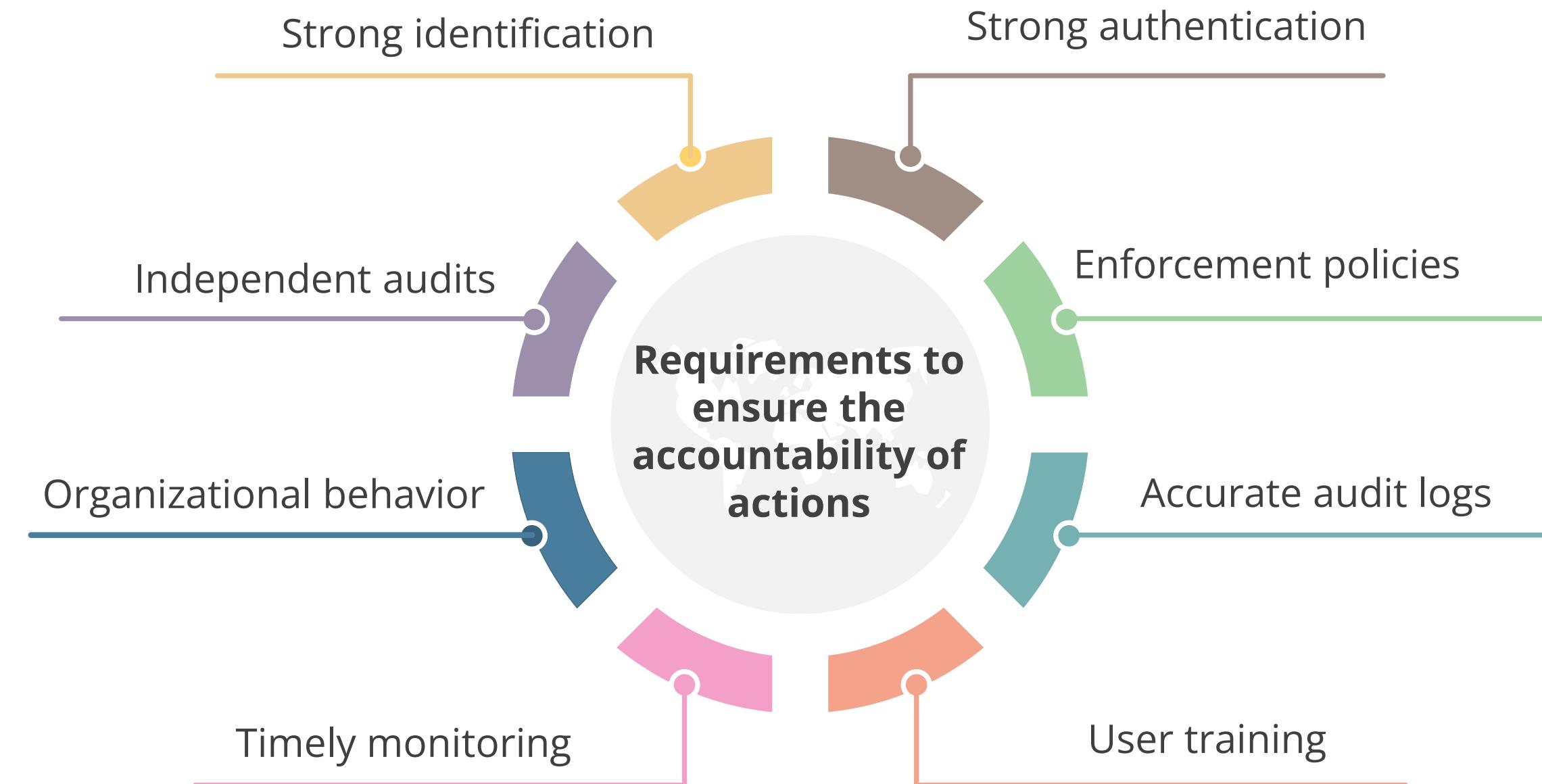
- Error messages
- File modifications

User-level events

- Identification and authentication attempts
- Commands used

Accountability

Non-repudiation ensures that users, processes, and actions are held accountable for their impacts.



TECHNOLOGY

Federation Identity Management

Federated Identity Management (FIM)

Federated identity

- Is a portable identity, and along with its associated entitlements, can be used across business boundaries
- Allows a user to be authenticated across multiple IT systems and enterprises
- Is based on linking a user's otherwise distinct identity at two or more locations without the need to synchronize or consolidate directory information



Federated Identity Management (FIM)

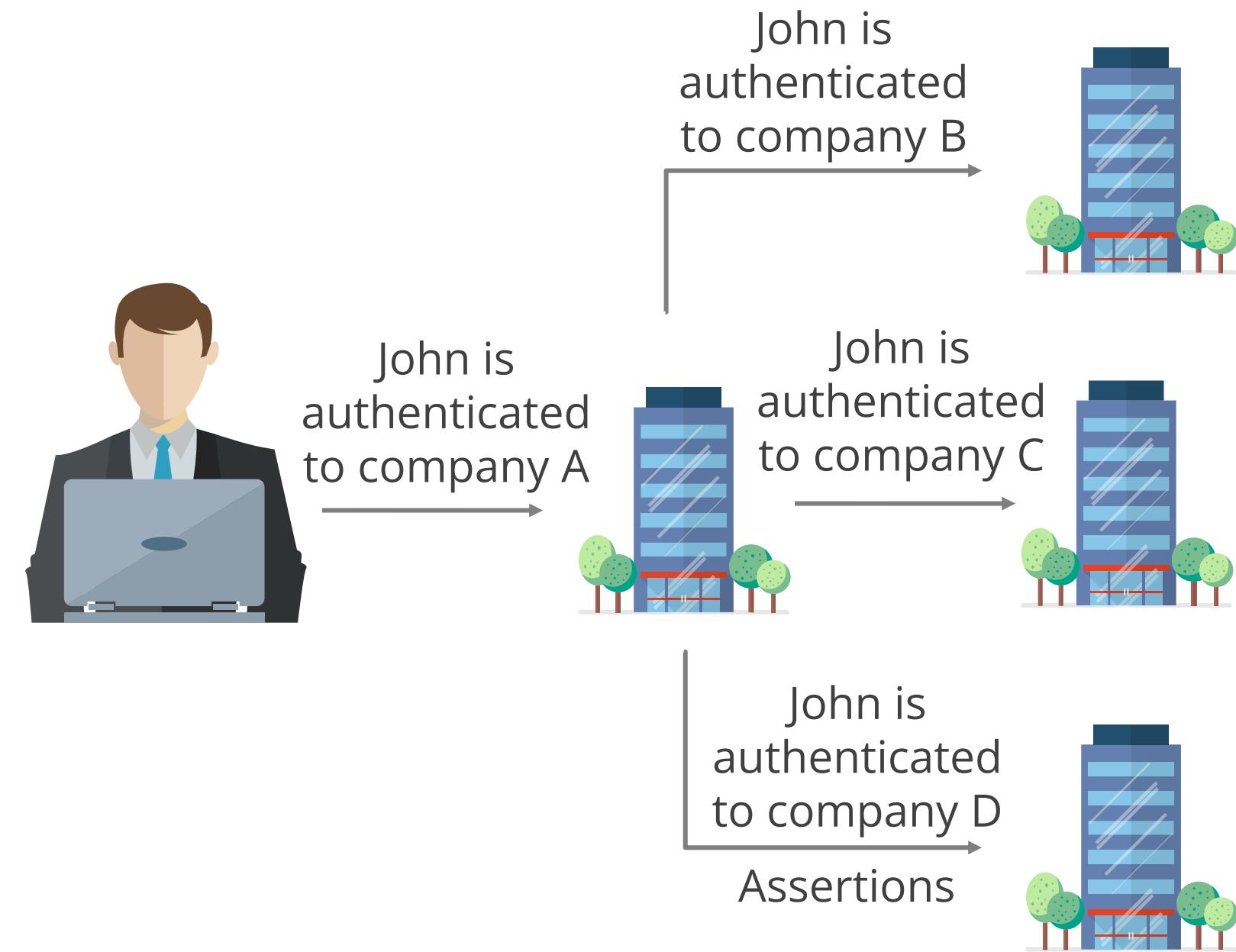
Federated identity management

- Addresses the identity management issues that arise when multiple organizations need to share the same applications and users between them
- Requires each organization in the federation to subscribe to a common set of policies, standards, and procedures for the provisioning and management of user identification, authentication, and authorization information
- Establishes a trust relationship among participating organizations



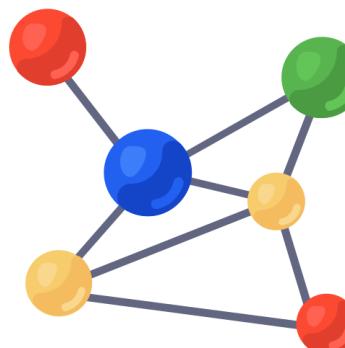
Federated Identity Management (FIM): Example

- When you book a flight on Expedia, the website asks if you also want to book a hotel room. If you click **Yes**, you could then be directed to the Hilton Hotel website, which provides information on the hotel closest to the airport you are flying into.
- You don't have to log in again to book a room. You logged in on the Expedia website, and that website sent your information to the Hilton website, all of which happened transparently.

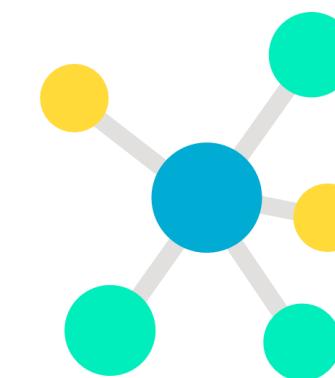


Types of Federated Identity Management

Cross certification model



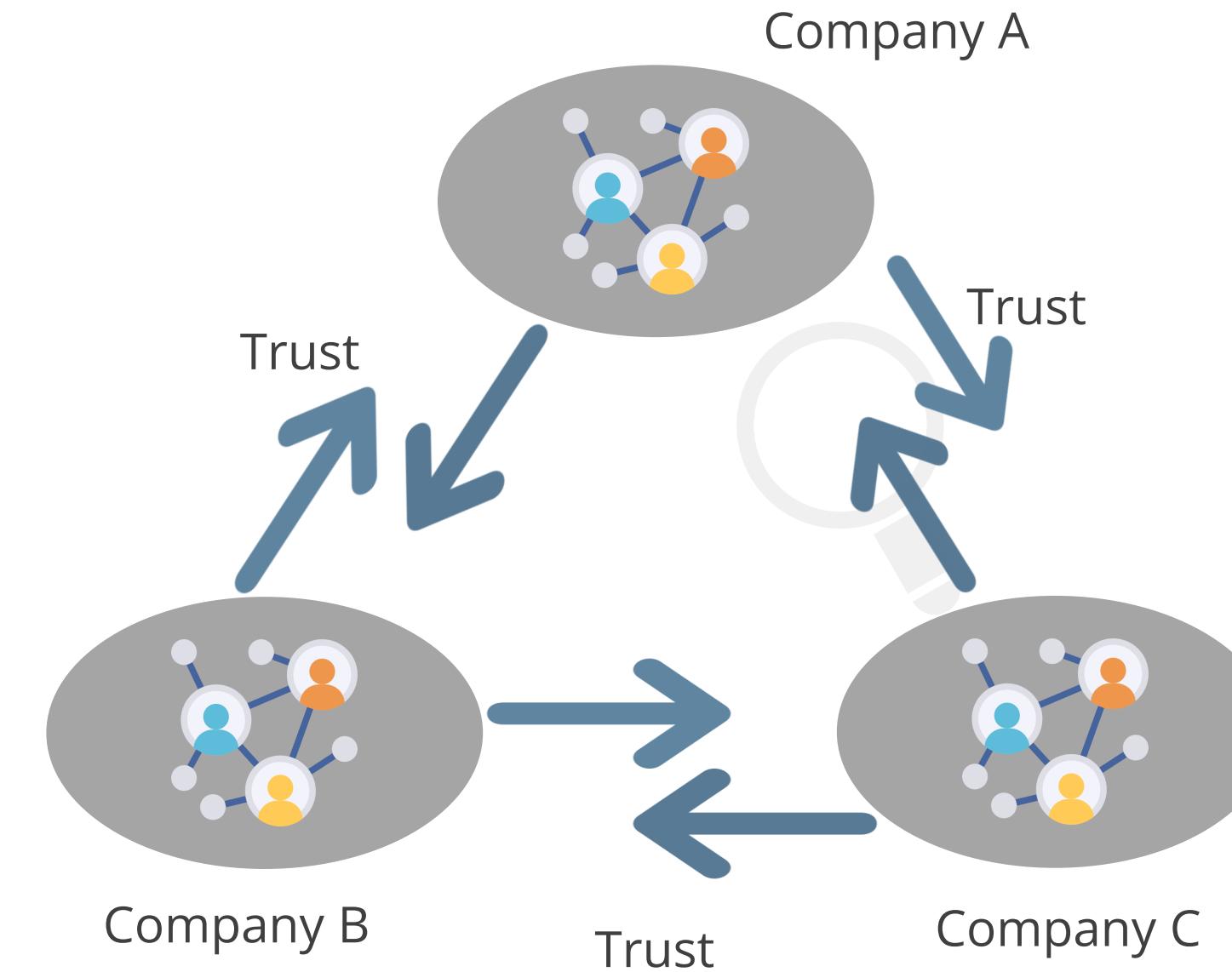
Trusted third party



Federated Management Models

Cross certification model

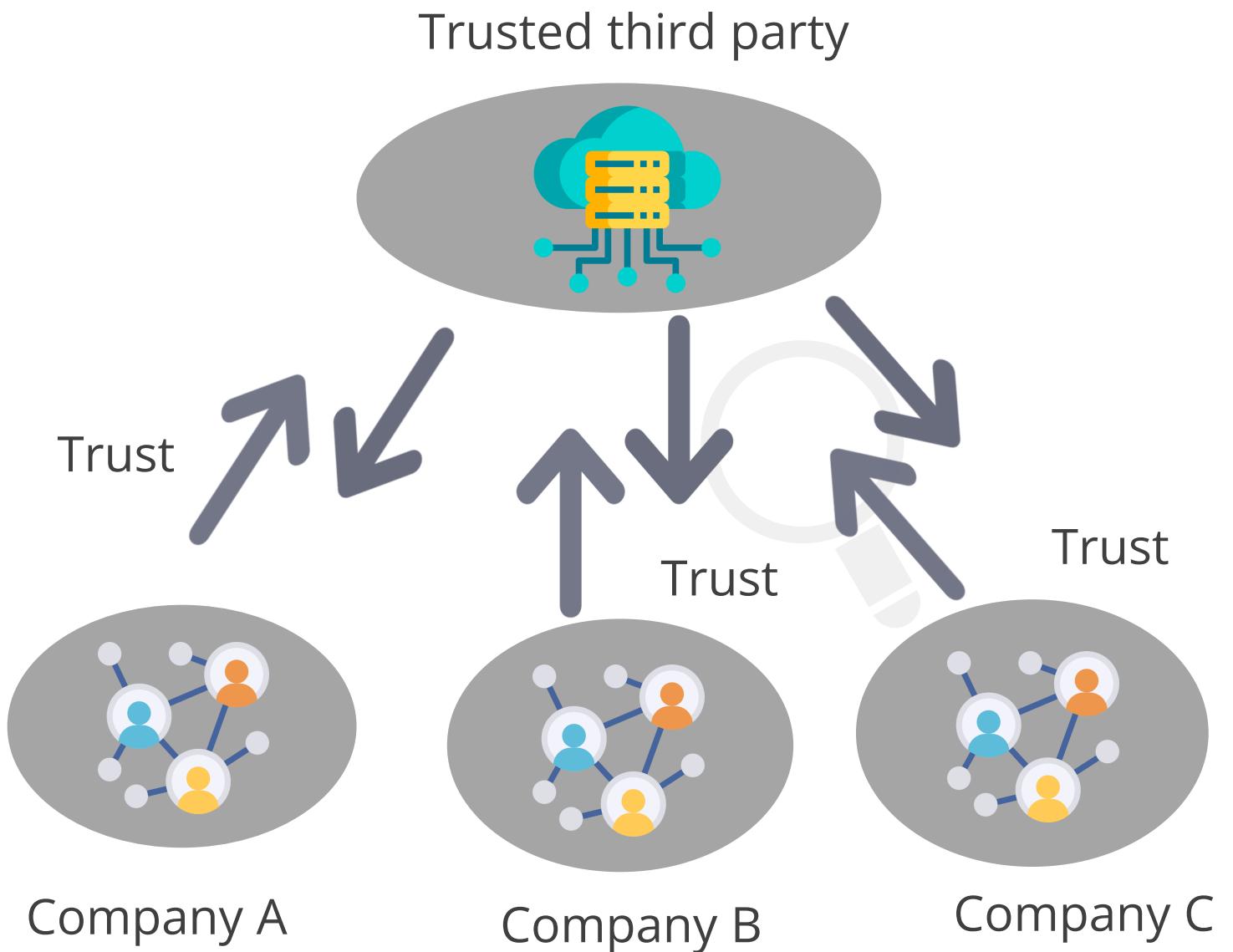
- Certifies every other participating organization
- Manages trust relationships, which become difficult as the number of participating organizations increases
- Plays the roles of both identity provider and service provider, depending on communication



Federated Management Models

Trust third party

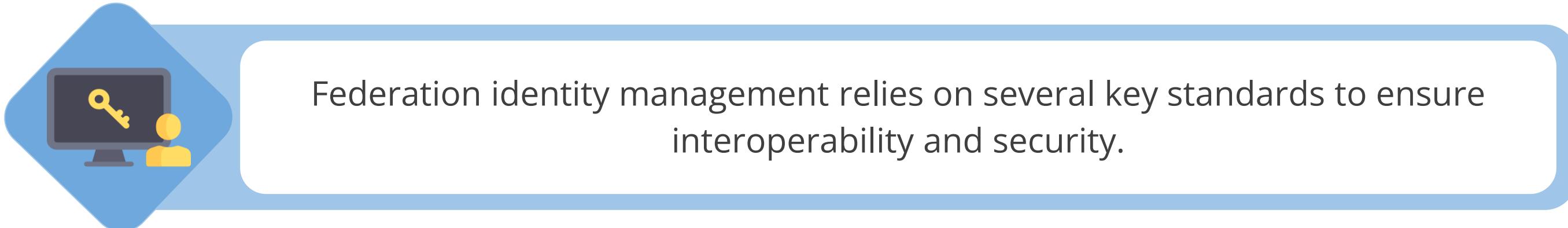
- Subscribes to the standards and practices of a trusted third party, which manages the verification and due diligence process for all participating organizations
- Considers the participating organizations trustworthy after verification by the third party
- Acts as a trusted entity or bridge between participating organizations for identity verification purposes
- Serves as the identity provider in the trusted third-party certification model, with other organizations serving as service providers



TECHNOLOGY

Federation Identity Management Standards

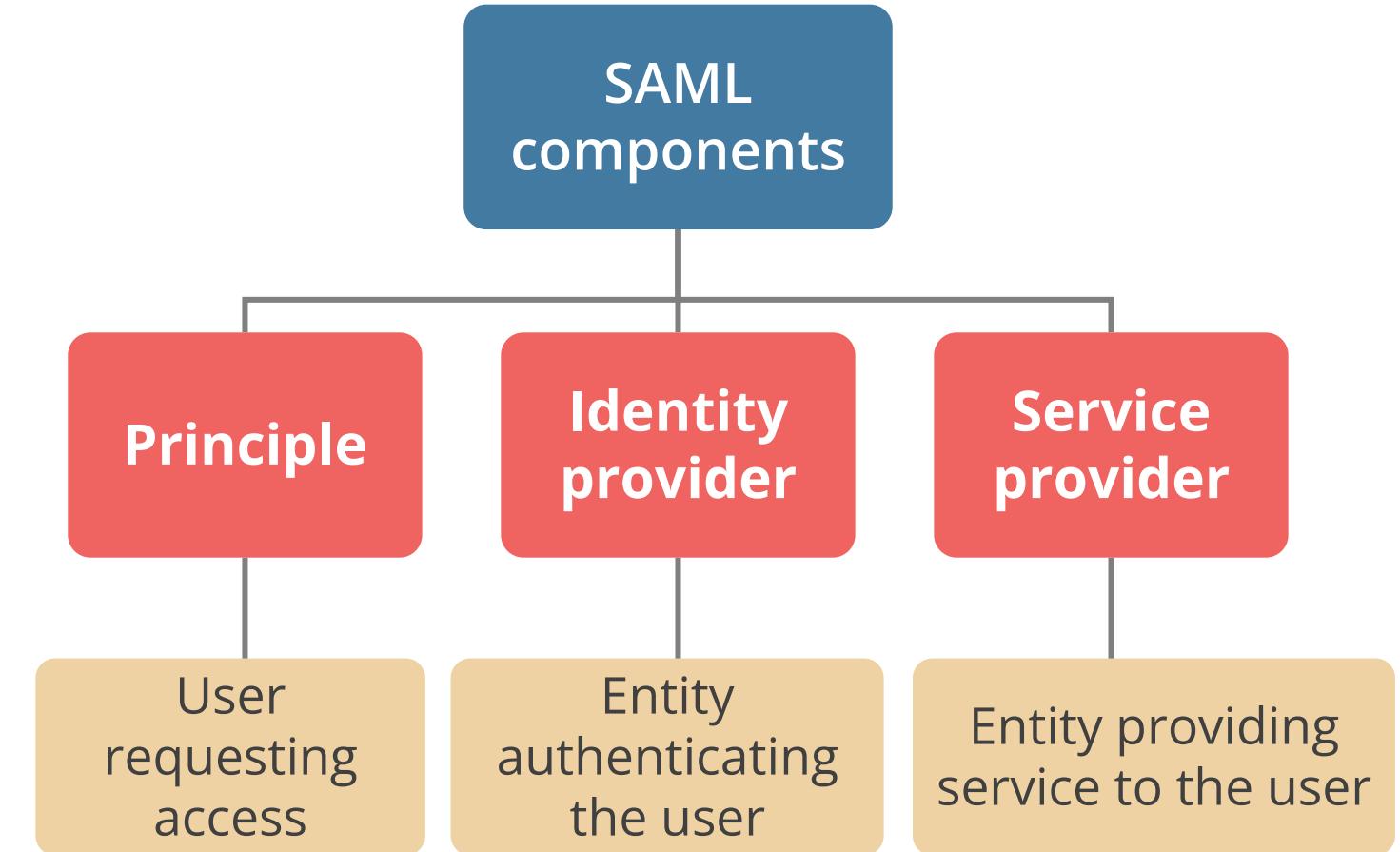
Federation Identity Management Standards



Security Assertion Markup Language (SAML)

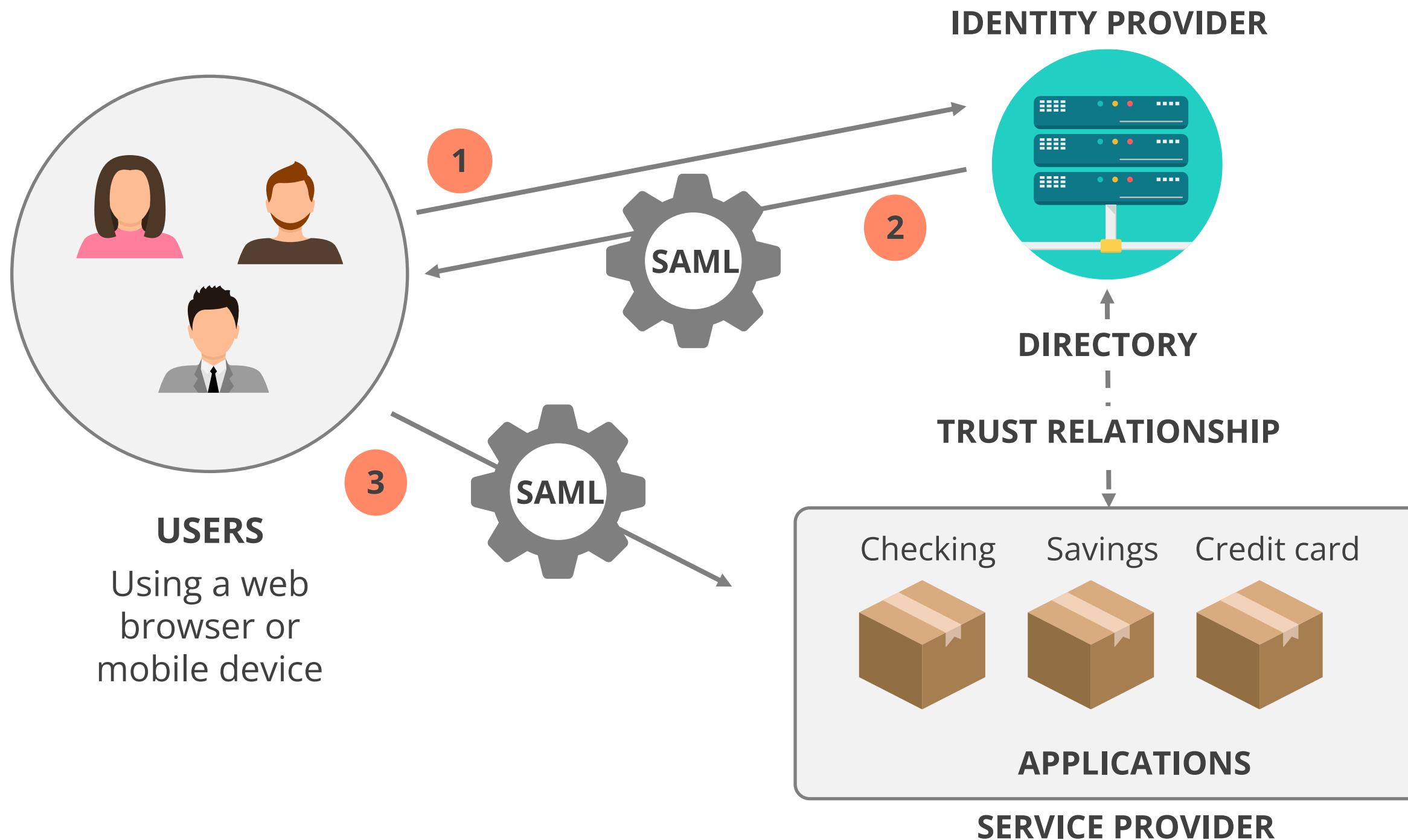
Security assertion markup language

- Allows the exchange of authentication and authorization data between security domains as an XML standard
- Provides the authentication pieces to the federated identity management systems
- Uses SAML and SPML for access needs in federated identity systems
- Offers SSO capabilities to access different browsers
- Relies on TLS for message confidentiality and digital signatures for message integrity, lacking a security mode



Security Assertion Markup Language (SAML)

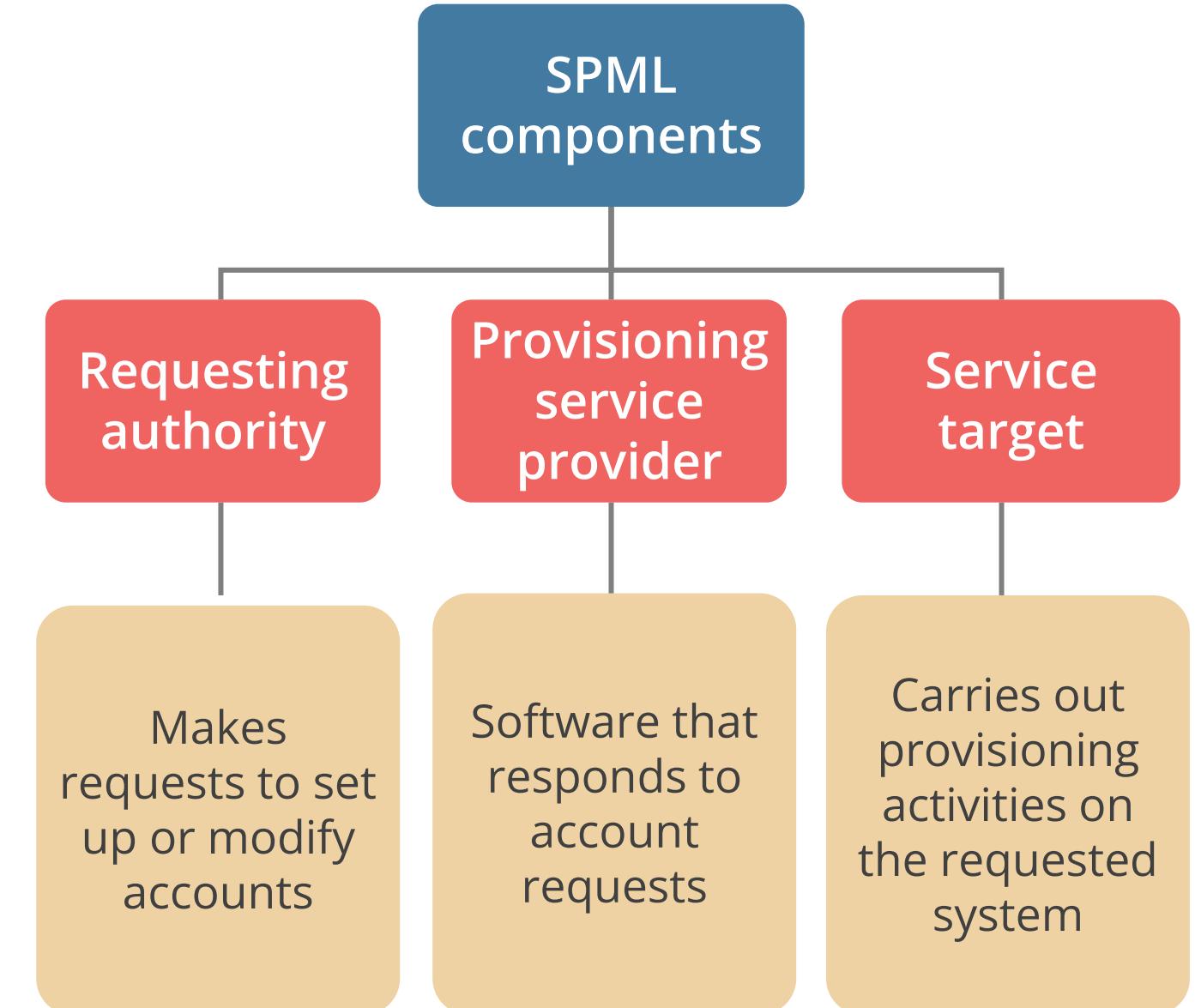
The diagram below will help you understand SAML.



Service Provisioning Markup Language (SPML)

Service provisioning markup language

- Exchanges provisioning data between applications within one organization or across different organizations
- Automates user management and access entitlement configuration across multiple provisioning systems
- Integrates and inter-operates service provisioning requests across various platforms



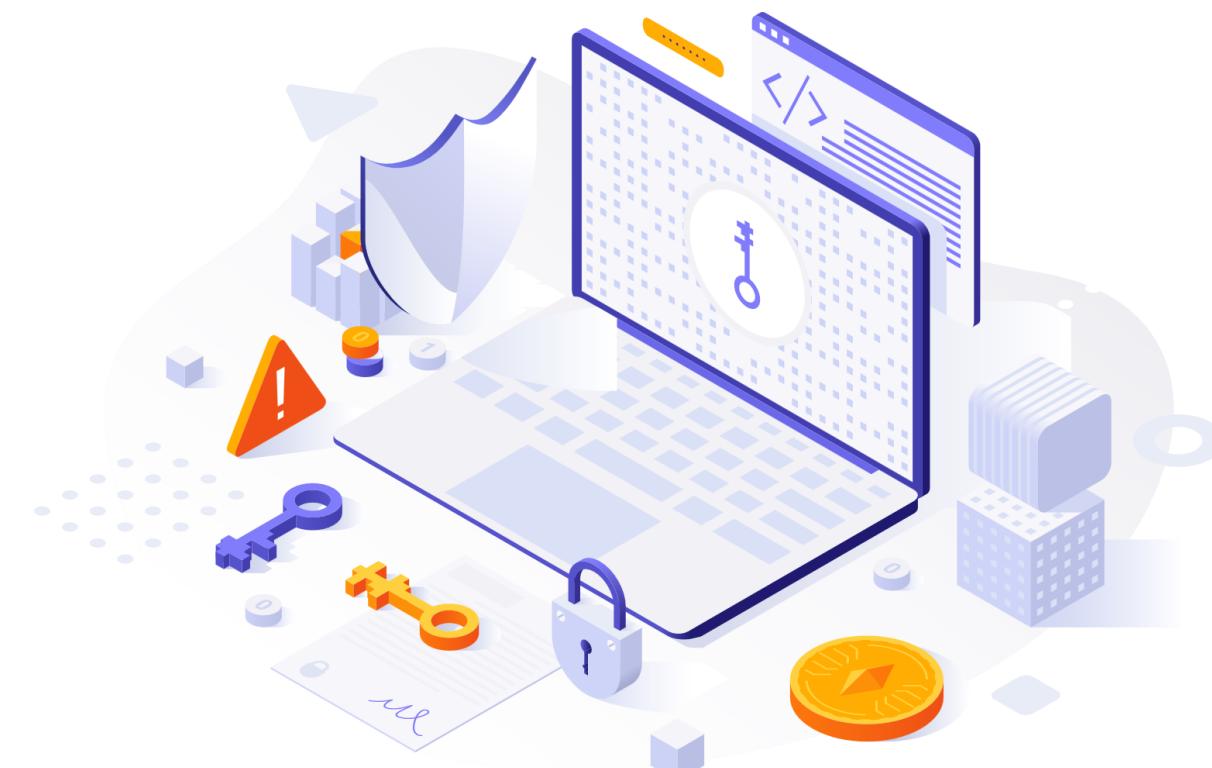
OpenID Connect

OpenID

- Allows you to use an existing account to sign in to multiple websites without needing to create new passwords
- Enables you to share information like your name or email address with the websites you visit, while controlling how much information is shared
- Ensures that only your identity provider receives your password, which then confirms your identity to the websites you visit
- Prevents other websites from ever seeing your password, eliminating the risk of compromising your identity on unscrupulous or insecure websites

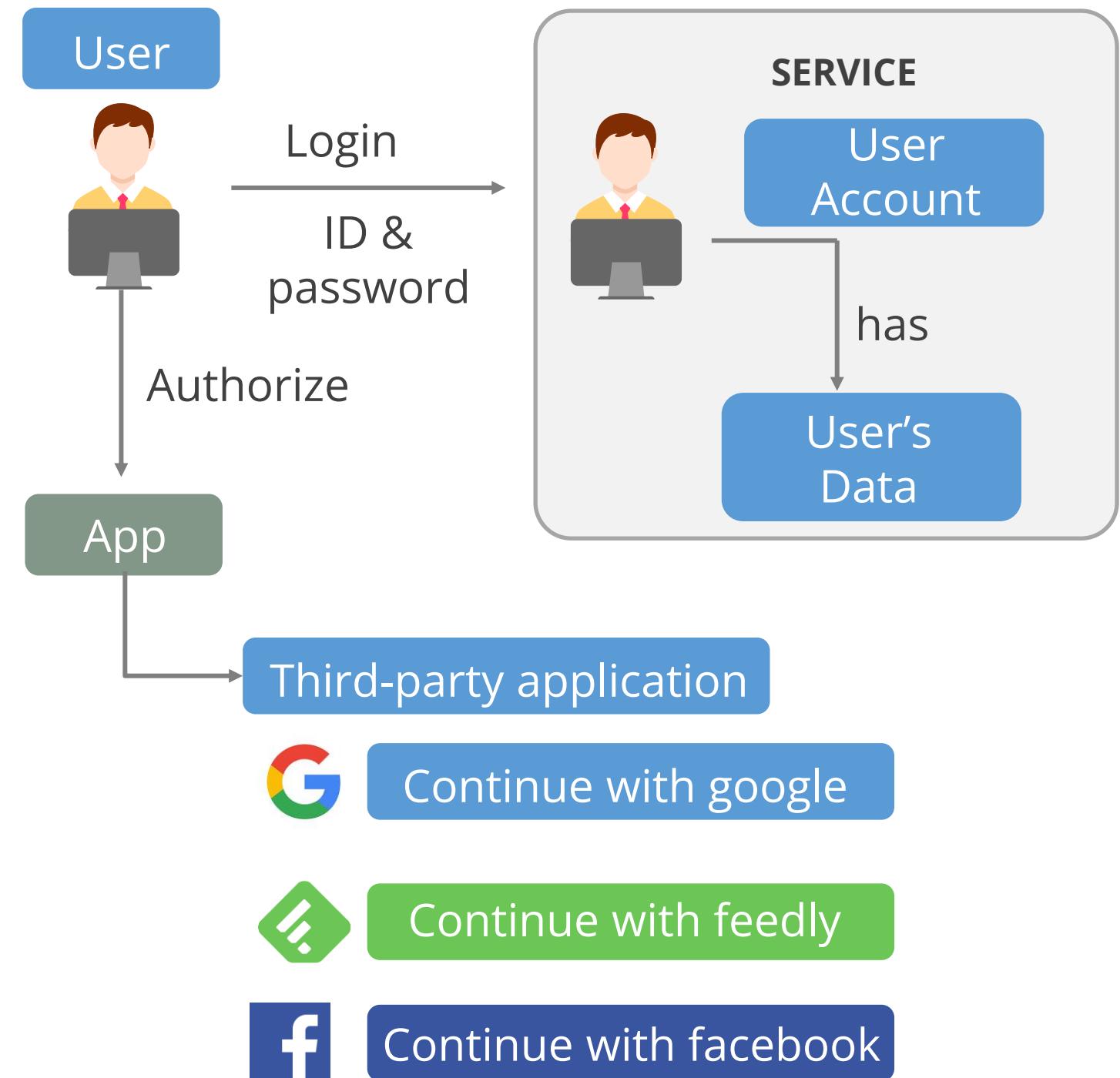
OAuth

- OAuth is an open-standard authorization protocol or framework that describes how unrelated servers and services can safely allow authenticated access to their assets without sharing the initial, related, and single login credentials.
- In authentication parlance, this is known as secure, third-party, user-agent, and delegated authorization.



OAuth: Example

- The simplest example of OAuth is when you log in to a website, and it offers you one or more options to log in using another website or service login.
- You then click on the button linked to the other website. That website authenticates you, and the website you were originally connecting to logs you in using the permission obtained from the second website.



Difference between SAML, OAuth, and OpenID

	SAML 2.0	OAuth2.0	OpenID connect
Purpose	Authorization and authentication	Authorization	Authentication
History	Developed by OASIS in 2001	Developed by Twitter and Google in 2006	Developed by the OpenID Foundation in 2004
Data format	XML	JSON	JSON
Use case	SSO for enterprise applications	-	SSO for consumer applications

TECHNOLOGY

Single Sign-On

Single Sign-On (SSO)

This technology allows users to log in to multiple applications with just one set of credentials.

- With SSO, the user enters credentials only once to gain access to all the corporate resources to which they are entitled.
- Imagine having a master key for your house that unlocks all the doors - SSO is like that for your digital life.



Single Sign-On (SSO)

Pros	Cons
Users have one password for all enterprise systems and applications.	Difficult to implement
Only one strong password needs to be remembered and used	Centralized point of failure
User accounts can be easily created on hire and modified or deleted on dismissal.	Potential data compromise

Single Sign On (SSO)

SSO technologies:

Kerberos

The Kerberos authentication protocol uses a key distribution center, tokens or tickets, and symmetric key cryptography.

SESAME

The Secure European System for Applications in a Multivendor Environment (SESAME) authentication protocol uses asymmetric cryptography.

Dumb terminal

Thin clients' or dumb terminals' access control, processing, and storage depend on a central server.

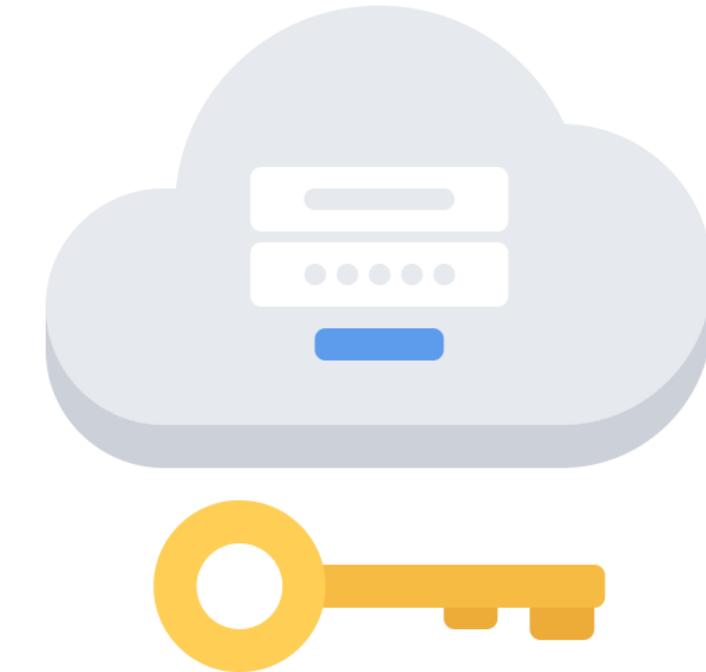
Script-based sign on

An organization can implement its SSO solution by developing a script.

Kerberos



Kerberos is an authentication protocol that offers a single sign-on solution for distributed environments.



It uses a client/server model based on tickets to allow nodes to securely interact on an insecure network and confirm their identity to one another.

Key Features of Kerberos



Single Sign on Kerberos is an open protocol that allows users to authenticate only once to access multiple resources within a Kerberos realm.

Strong Encryption It uses Advanced Encryption Standard (AES) symmetric-key cryptography to protect data confidentiality and integrity

Mutual Authentication- Both the client and the server are authenticated, ensuring the identity of both parties

Key Features of Kerberos



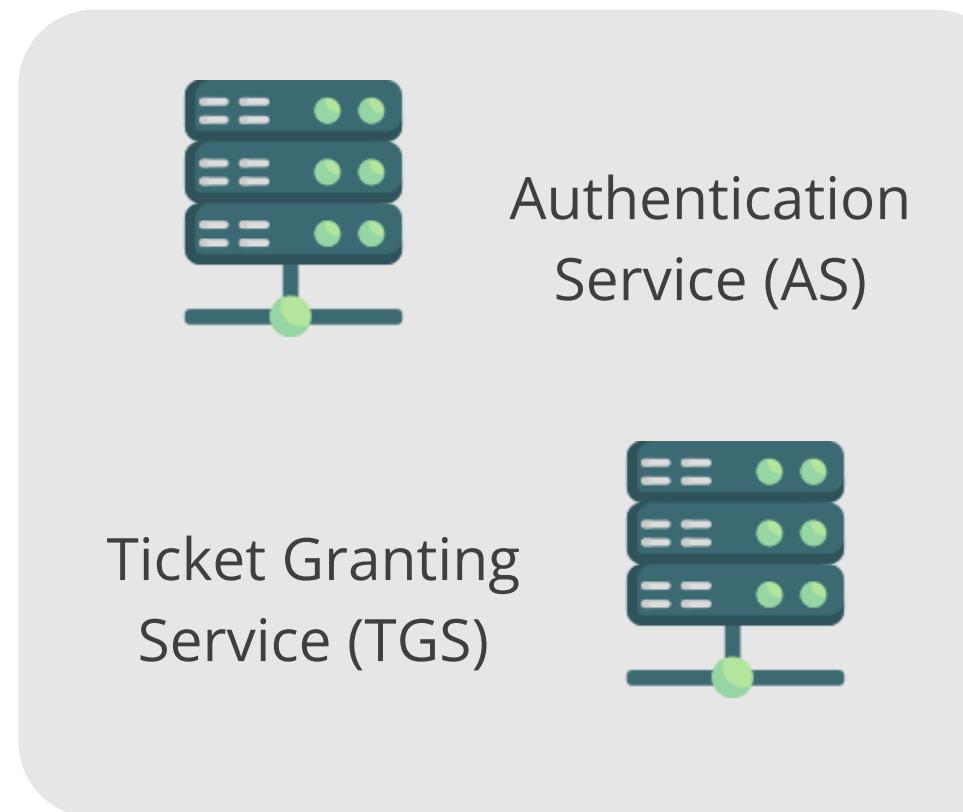
Ticket-Based Authentication: Uses tickets for access, reducing password transmission

Centralized Management- It uses a Key Distribution Center (KDC) which allows Centralized management of user credentials and ticket issuance.

Scalability: Can handle large numbers of users and services

Key Distribution Center (KDC)

It is a central authentication server in the Kerberos protocol, responsible for issuing tickets that allow users to access network services.



- AS handles initial authentication and issues the TGT.
- The AS is the first component in the Kerberos authentication process. It verifies user credentials. and issues a TGT to authenticate the client.
- TGS issues service tickets (ST) based on presented TGT.
- The TGS validates TGT and issues service tickets, which are used for accessing the services.

It is a trustworthy third party that offers authentication services.

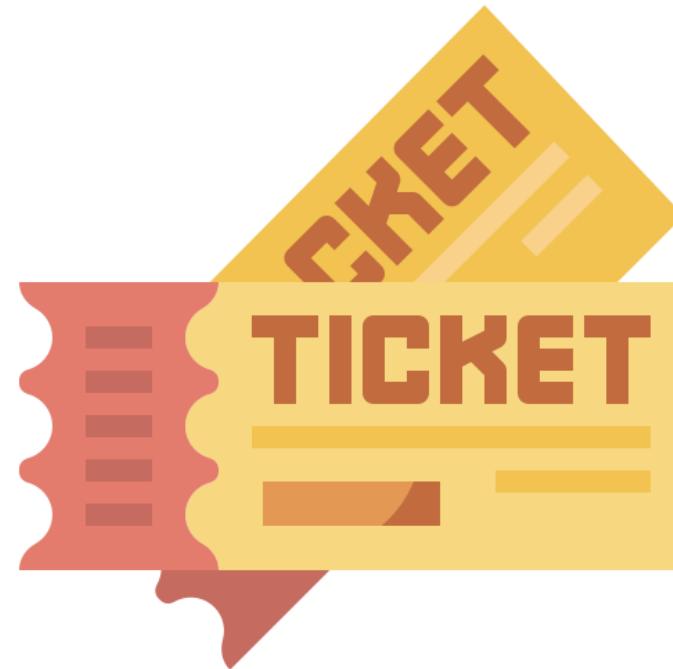
Ticket-Granting Ticket (TGT)



- A TGT verifies that a subject has been verified by a KDC and is authorized to request tickets for access to other objects.
- A TGT contains a symmetric key, an expiry period, and the user's IP address, and is encrypted with the TGS secret key.
- When seeking tickets to access objects, subjects present the TGT.

Service Ticket

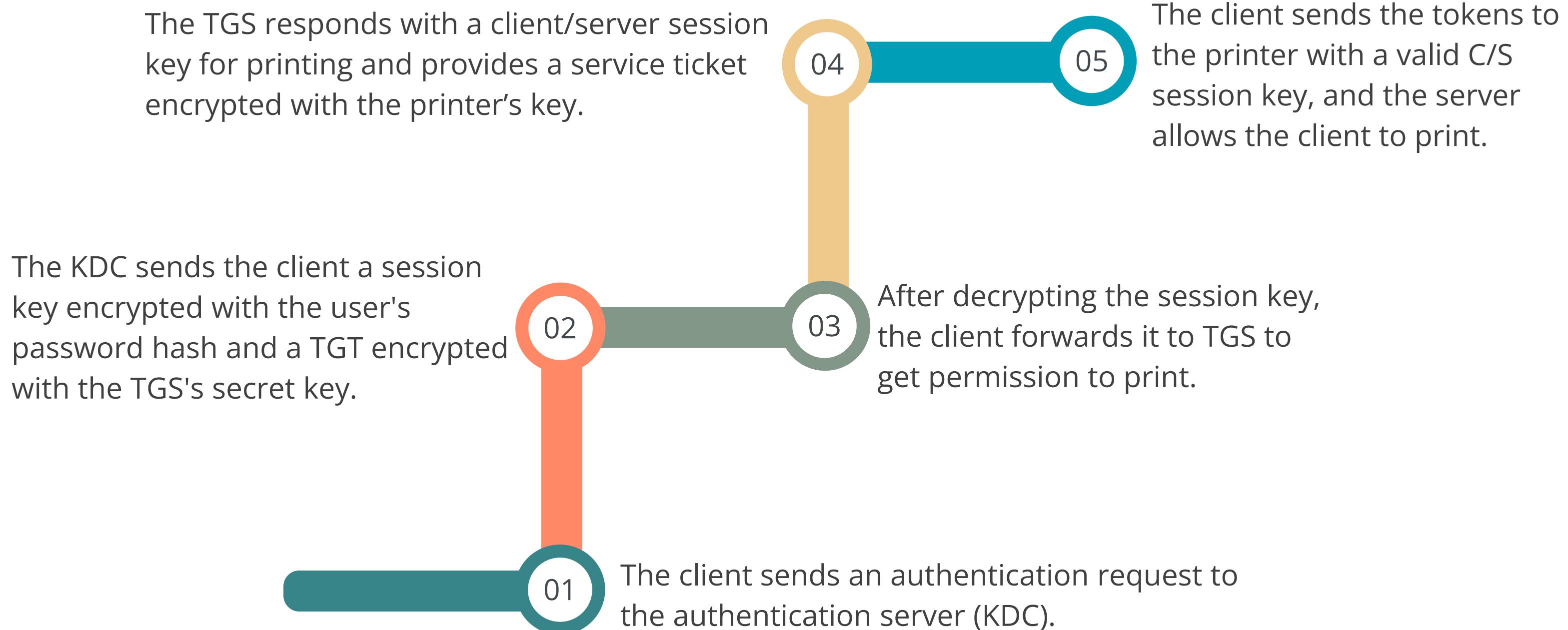
It is an encrypted message that proves a subject is authorized to access an object.



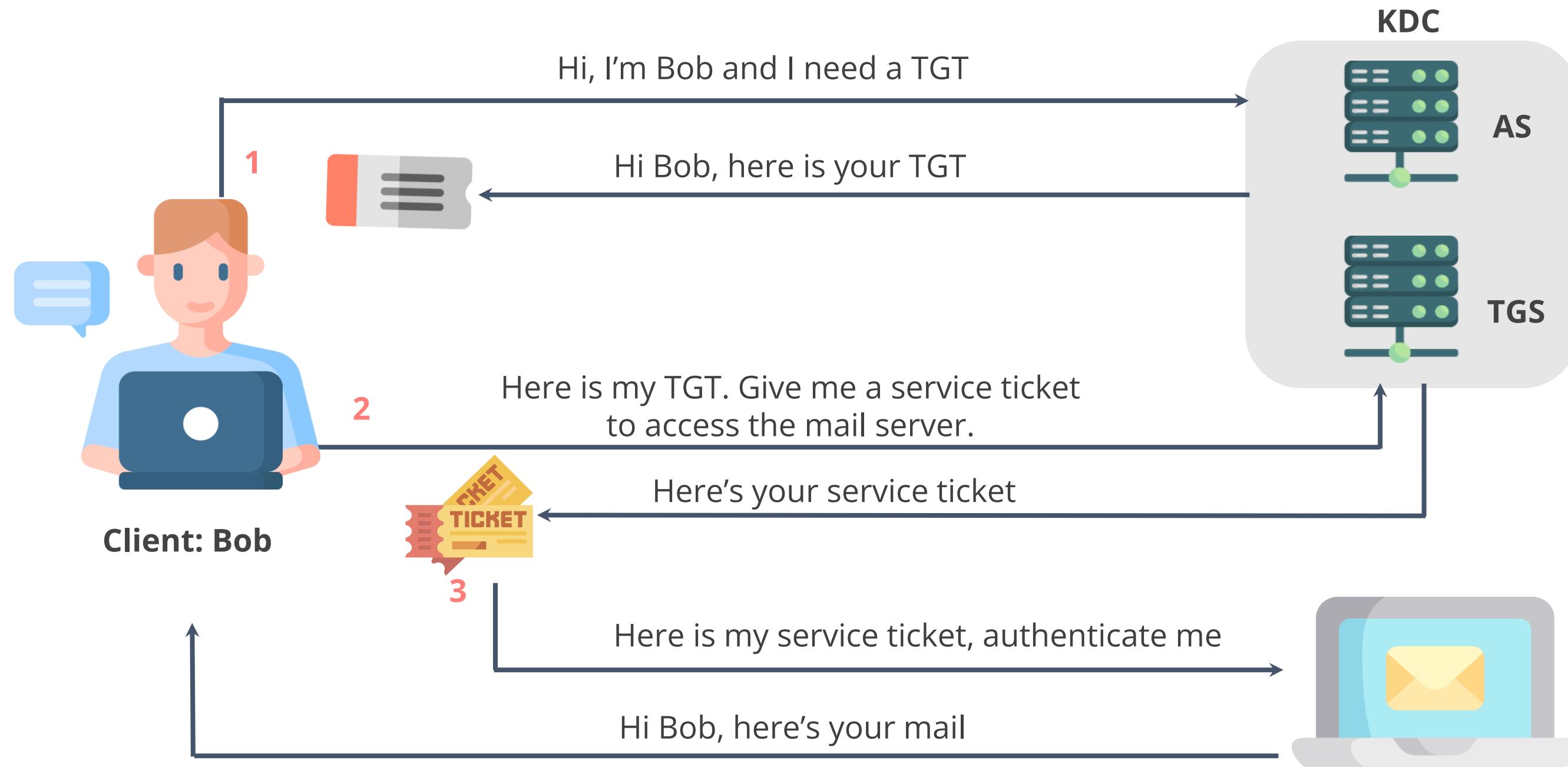
- Kerberos issues service tickets to subjects who seek access to objects.
- Kerberos service tickets feature a set of lifetime and usage constraints.
- The client must request a renewal or a new service ticket to continue communicating with any server after the current ticket expires.

Kerberos Steps

When a user wishes to log on to the network and access a print server, the following steps are performed:



Kerberos Authentication Process



Weakness of Kerberos

Can be a single point of failure



Leads to the compromise of the secret key for every system on the network if compromised

Vulnerable to password guessing

Requires all client and server clocks to be synchronized within five minutes

Difference Between FIM and SSO

Federated identity management (FIM)

- FIM enables a single credential to access multiple applications and resources across multiple organizations.
- FIM provides SSO.

Single sign-on (SSO)

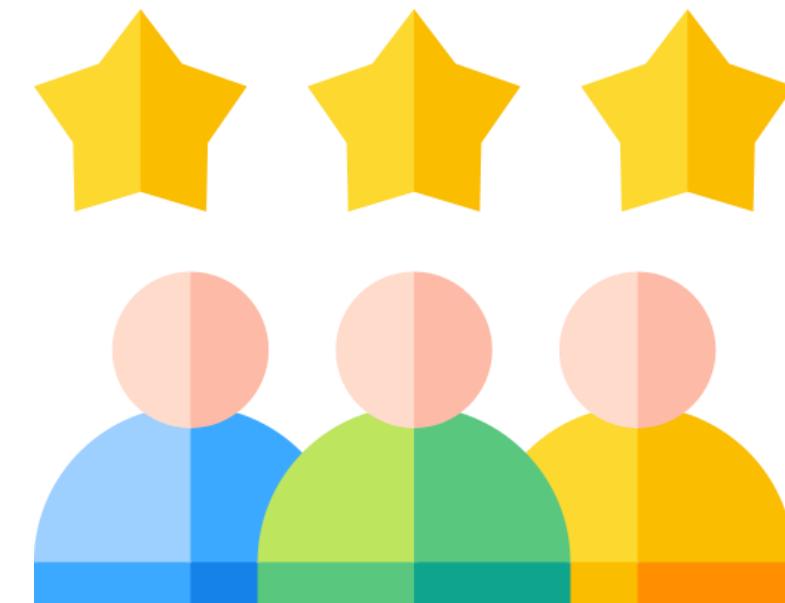
- SSO enables a single credential to access multiple applications and resources within one organization.
- SSO does not necessarily provide FIM.

TECHNOLOGY

Privilege Access Management

Privileged Access Management (PAM)

- PAM, also known as privileged identity management (PIM) or privileged account management, is a cybersecurity strategy that aims to secure access to vital systems and resources within an organization's IT environment.
- These accounts have elevated permissions that allow them to make significant changes to systems and data.
- If compromised by unauthorized users, the damage can be severe.



Just-in-Time (JIT)

JIT access control is a security practice that grants users elevated privileges only when necessary for a specific task and for a limited period.

- It is a cornerstone of privileged access management (PAM) and aligns with the principle of least privilege.
- By adopting JIT access control, organizations can significantly enhance their security posture and protect sensitive data.



Just-in-Time (JIT)

JIT enables organizations to grant users on-demand and privileged access to applications or systems for a predetermined period of time on an as-needed basis.

The requests can be verified against a pre-approval policy or reviewed by an administrator who has the power to grant or deny the requests for short-term privileged access.

JIT access can be provided using ephemeral certificates

JIT enforces the security principle of least privilege by providing users the least amount of access to perform the required job for the minimum duration necessary.

Business Scenario

Kevin was concerned about the security of the cloud virtual machines and wanted to reduce the risk of privileged access abuse and lateral movement by threat actors.

He learned about just-in-time (JIT) access, which enables always-on access by enforcing time-based restrictions based on behavioral and contextual parameters.

After he enabled the JIT feature on the VMs, he created a policy that determines the ports to be protected, how long ports remain open, and the approved IP addresses from which these ports can be accessed.

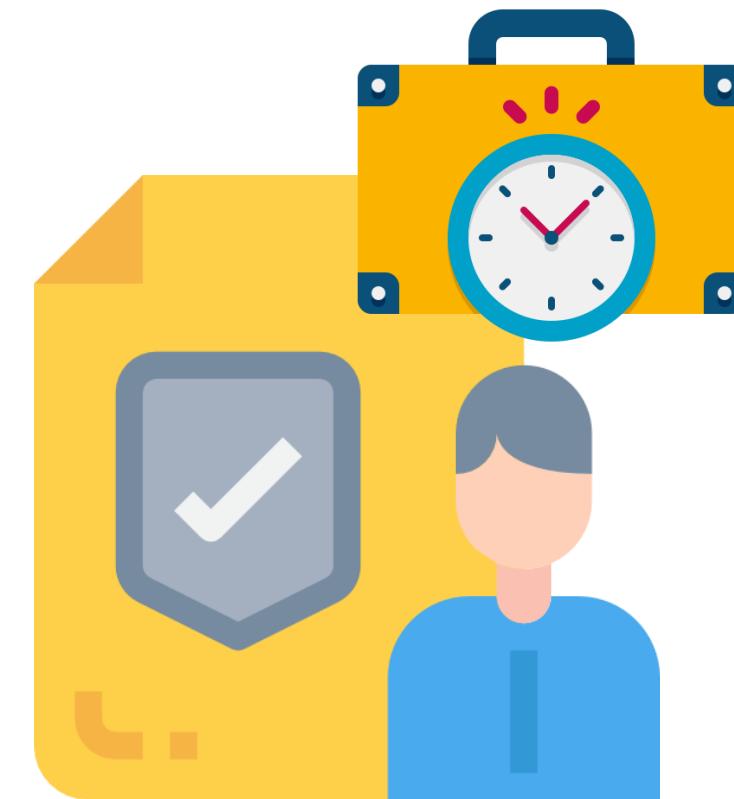
He enabled just-in-time access to lock down the virtual machines at the network level by blocking inbound traffic to management ports such as 22 (SSH) and 3389 (RDP).

The JIT access allowed Kevin to control the access and reduce the attack surface to his virtual machines by allowing need-based access for a limited period.

Ephemeral Credentials

Ephemeral credentials are temporary access keys that offer extra security by minimizing the window of opportunity for attackers.

- They are short-term, one-time-use credentials often used by IT administrators for specific projects.
- These credentials are secure because they only work for a limited time, making it difficult for attackers to exploit them.



Password Vaulting

- Password vaulting, or password management, securely stores and manages login credentials for online accounts and applications.
- It involves removing administrative and privileged accounts from the Active Directory environment and storing them in password vaults, typically software solutions.
- When a request for PAM is authorized, the ticket is released for the approved period.



Implementing and Managing Authorization Mechanisms

Access Control Model

An access control model is a framework that dictates how subjects access objects.

- Each model type uses different methods to control how subjects access objects.
- An organization's business and security goals will help determine which access control model it should use.
- These models are built into the core or the kernel of different operating systems and possibly their supporting applications as well.
- The way a subject accesses an object is guided by an access control model.

Types of access control models

Discretionary access control (DAC)

Mandatory access control (MAC)

Role-based access control (RBAC)

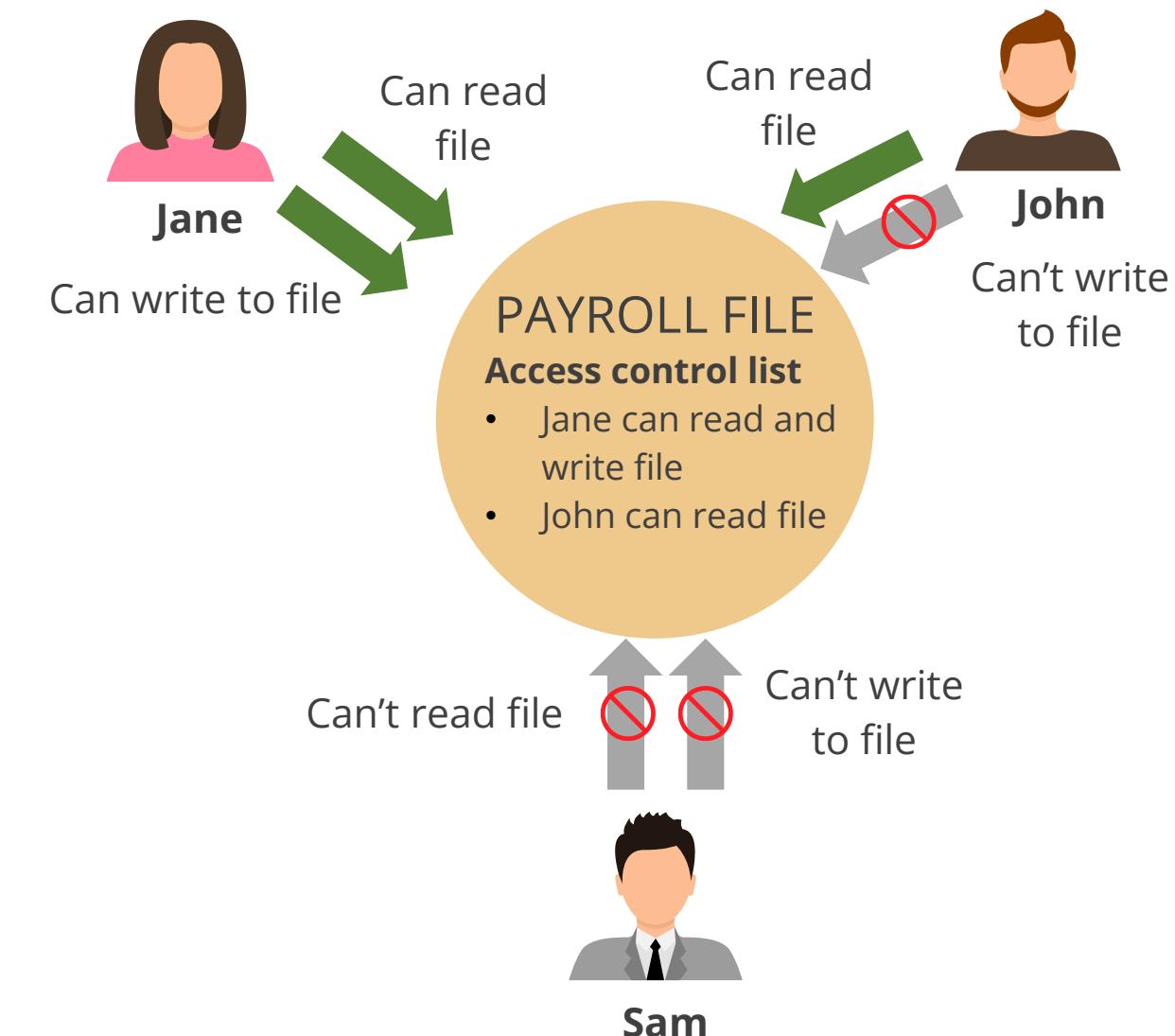
Rule-based access control

Attribute-based access control (ABAC)

Risk-based access control

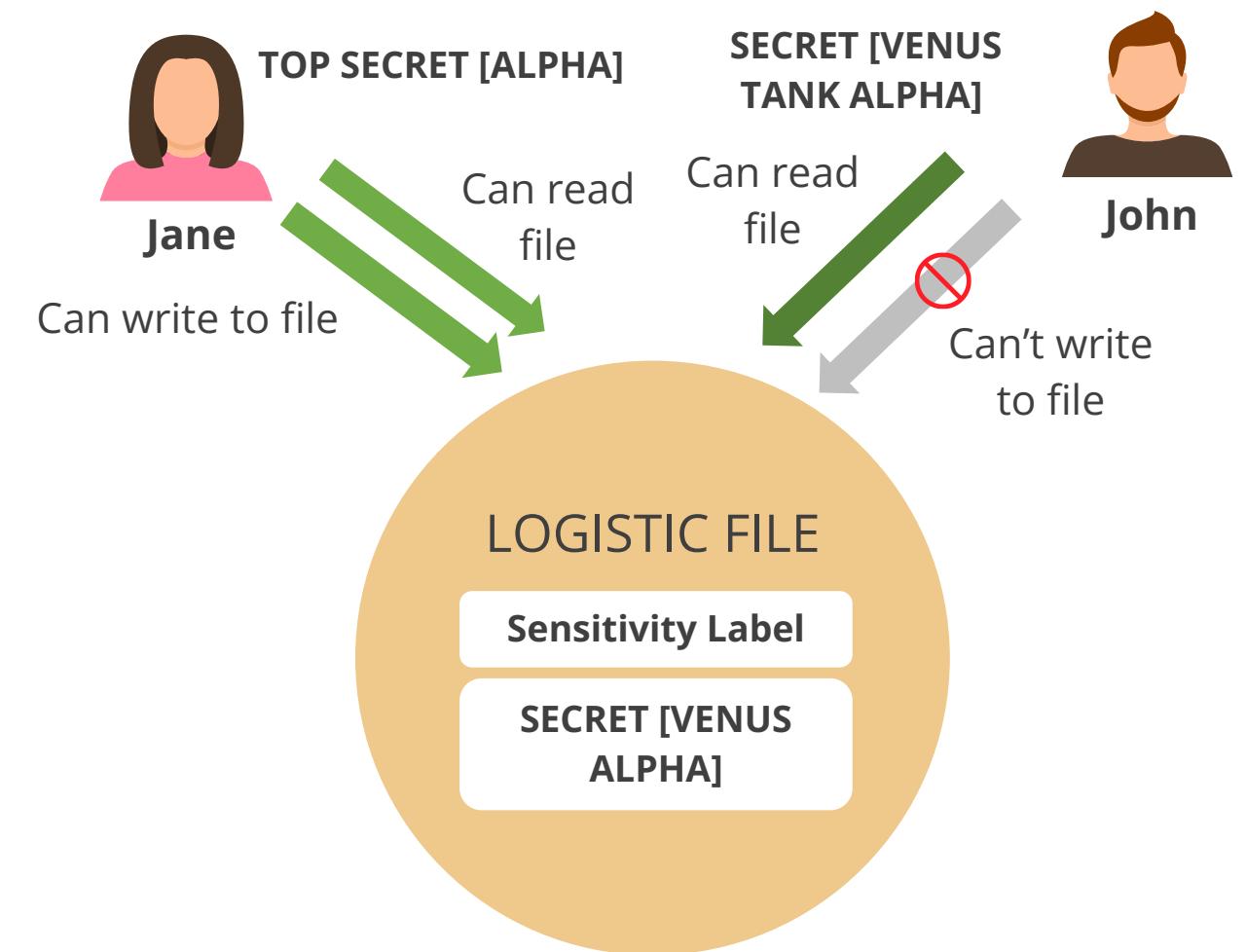
Discretionary Access Control (DAC)

- Access to resources is determined by data owners.
- Access control depends on the owner's discretion and the authorization granted to users.
- Access control lists (ACLs) are used to enforce the security policy.



Mandatory Access Control (MAC)

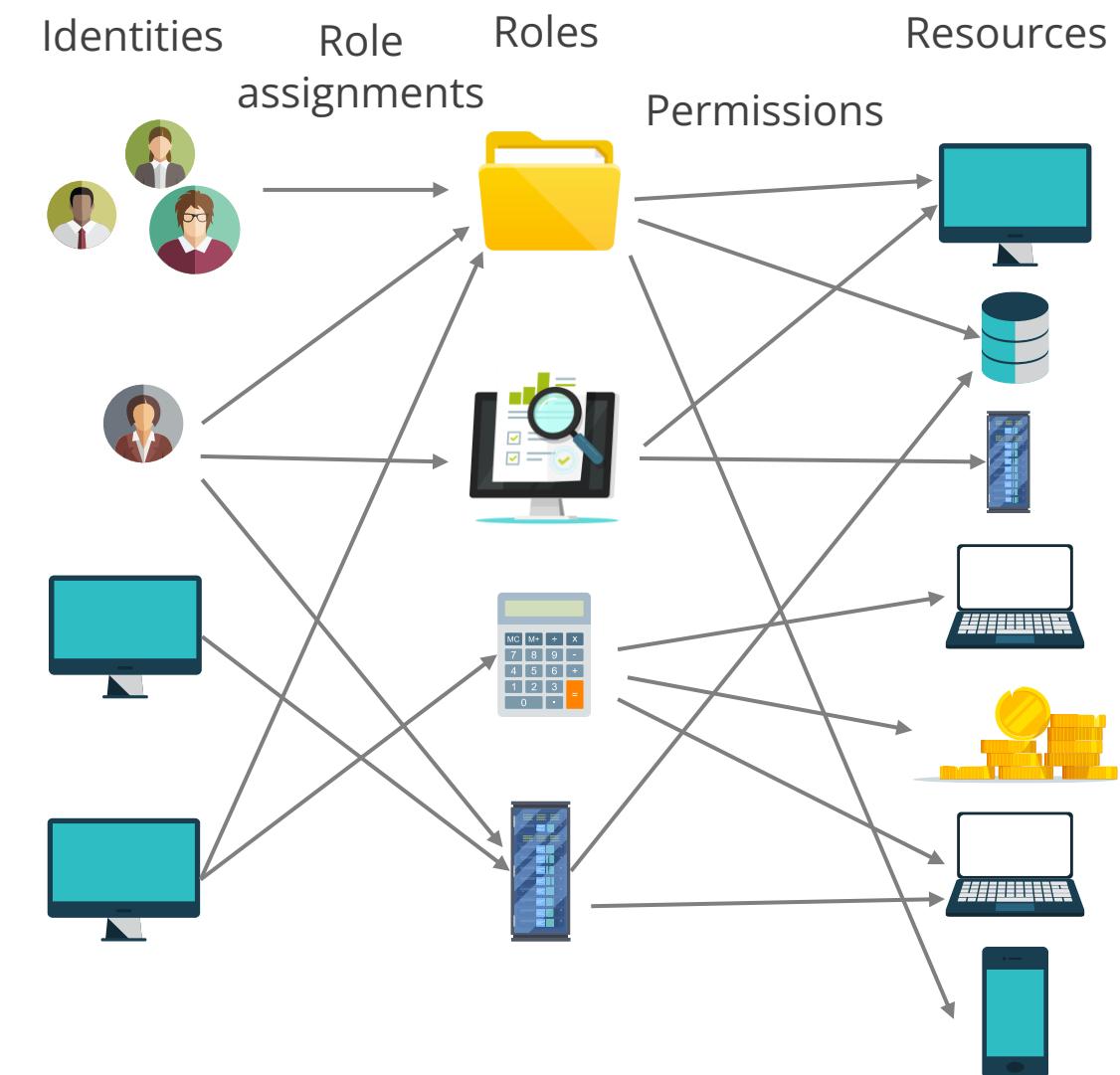
- The system's security policy is enforced by the operating system using security labels.
- Resources have security labels containing data classification, and the users have security clearances.
- This model is used when information classification and confidentiality are important.



Role-Based Access Control (RBAC)

RBAC is a widely used approach to restricting access to computer systems and networks.

- It defines different roles within a system and assigns permissions to those roles.
- Users are assigned roles based on their job functions or needs.
- This approach simplifies access management and ensures that users only have the access they need to perform their jobs.



Rule-Based Access Control (RBAC)

Access requests are evaluated against predefined rules that determine the access to be granted.

The rules are in the form of *if or then statements*.

They are not necessarily identity-based; they can apply to all users or subjects regardless of their identities.

Example: Routers and firewalls use rules to filter incoming and outgoing traffic within an ACL, as defined by an administrator. The firewall examines all traffic and only allows traffic that meets one of the rules.

Attribute-Based Access Control (ABAC)

'An access control method where requests to perform operations on objects are granted or denied based on attributes of the subject, attributes of the object, environment conditions, and specified policies.'

~ NIST

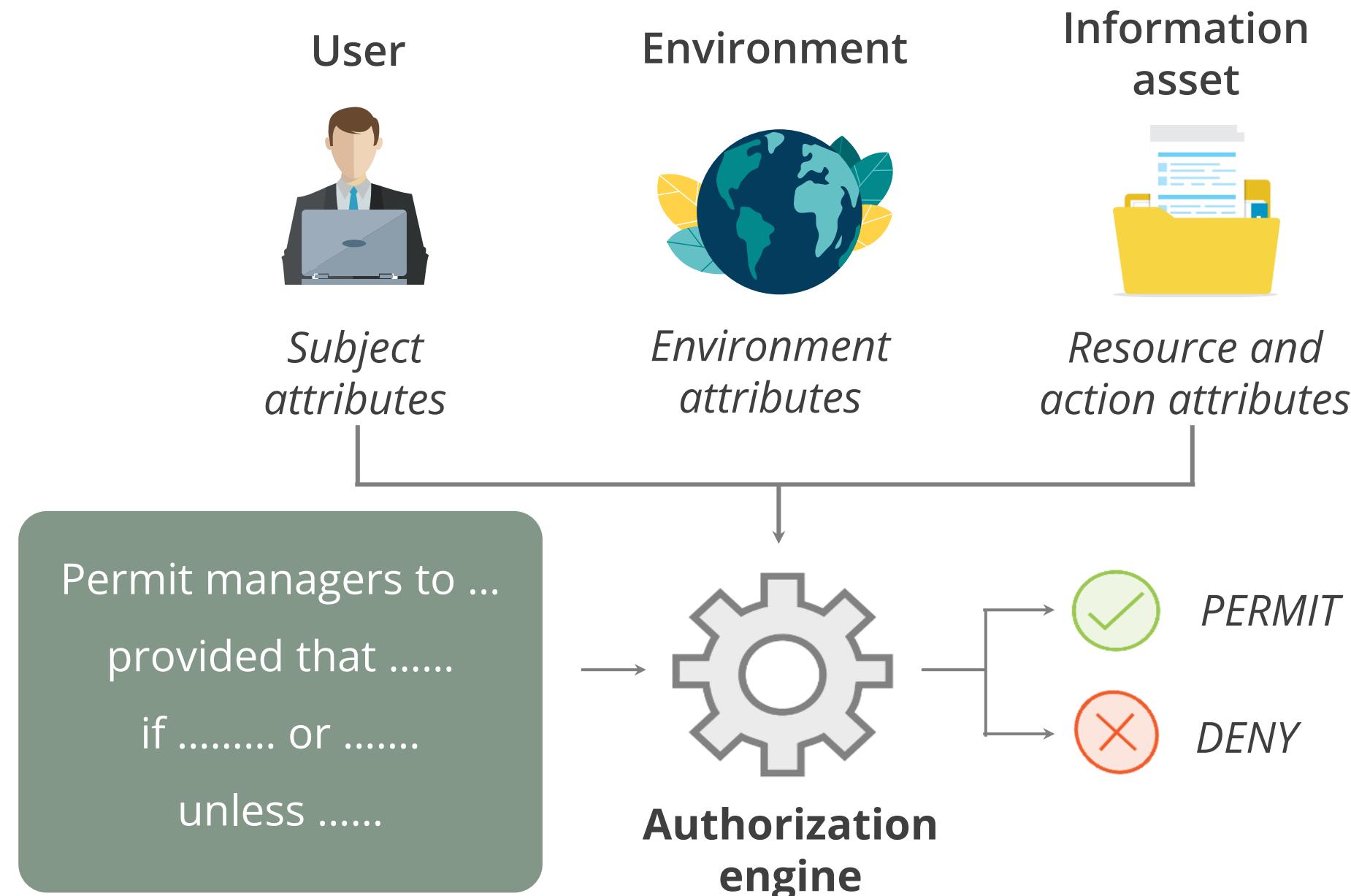
Granular policies can be established by combining these attributes to grant or deny access.



Attributes provide details for building authorization policies, such as who wants access to what, from where, when, and why.

Attribute Based Access Control (ABAC)

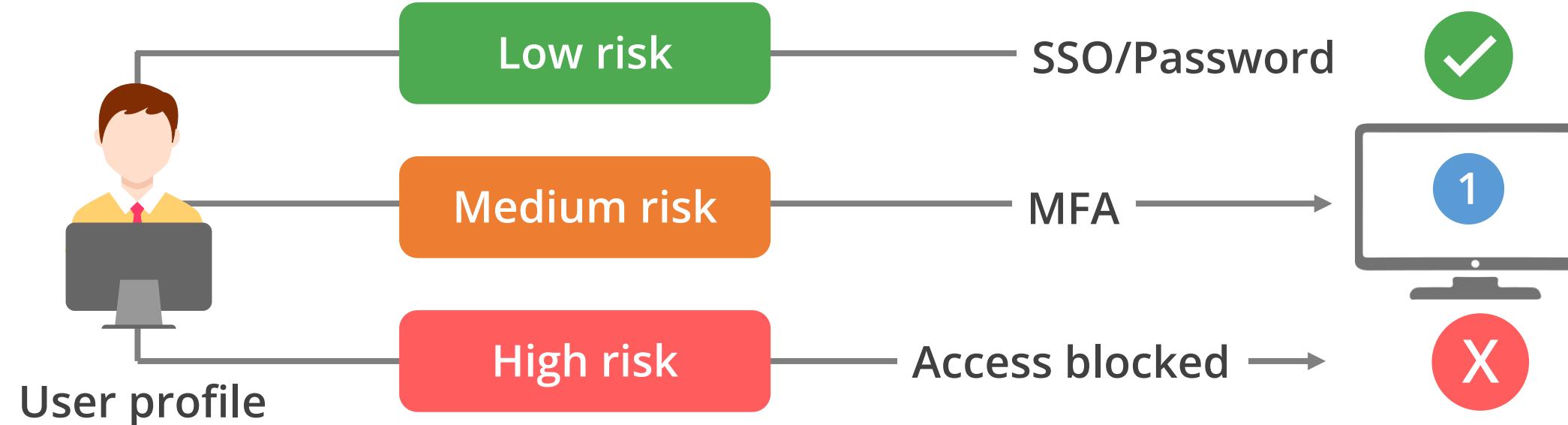
The following diagram describes the ABAC principle.



Risk-Based Access Control

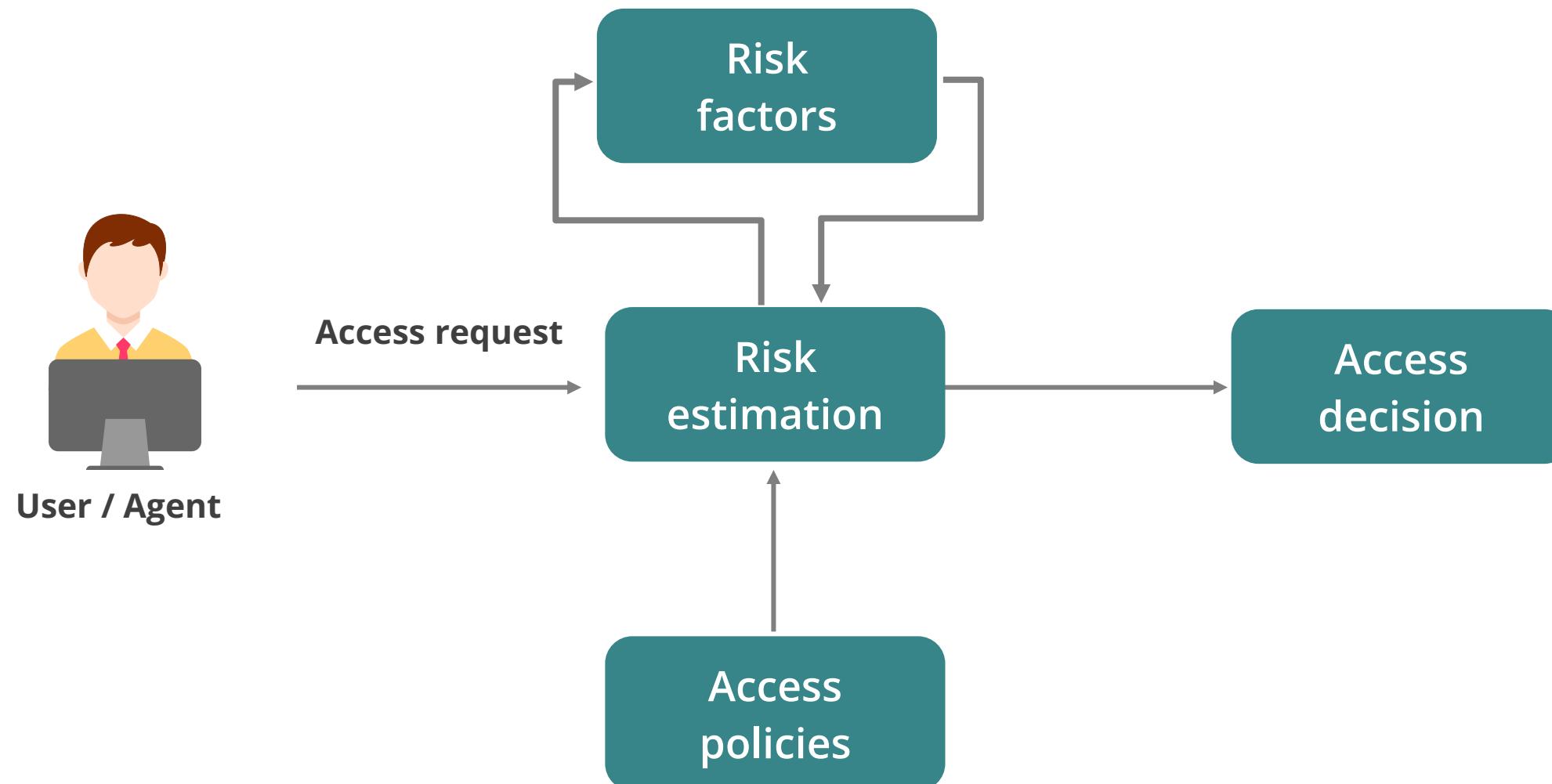
This is a dynamic authentication method that takes into account the security risk value related to each access request as a criterion to determine access decisions.

- Users authenticating from known devices, locations, and networks with a low-risk score could be automatically signed in.
- Suspicious users are required to provide additional credentials using MFA.
- Access requests with a high-risk score would be denied.



Risk-Based Access Control

Main elements of a risk-based access control model:



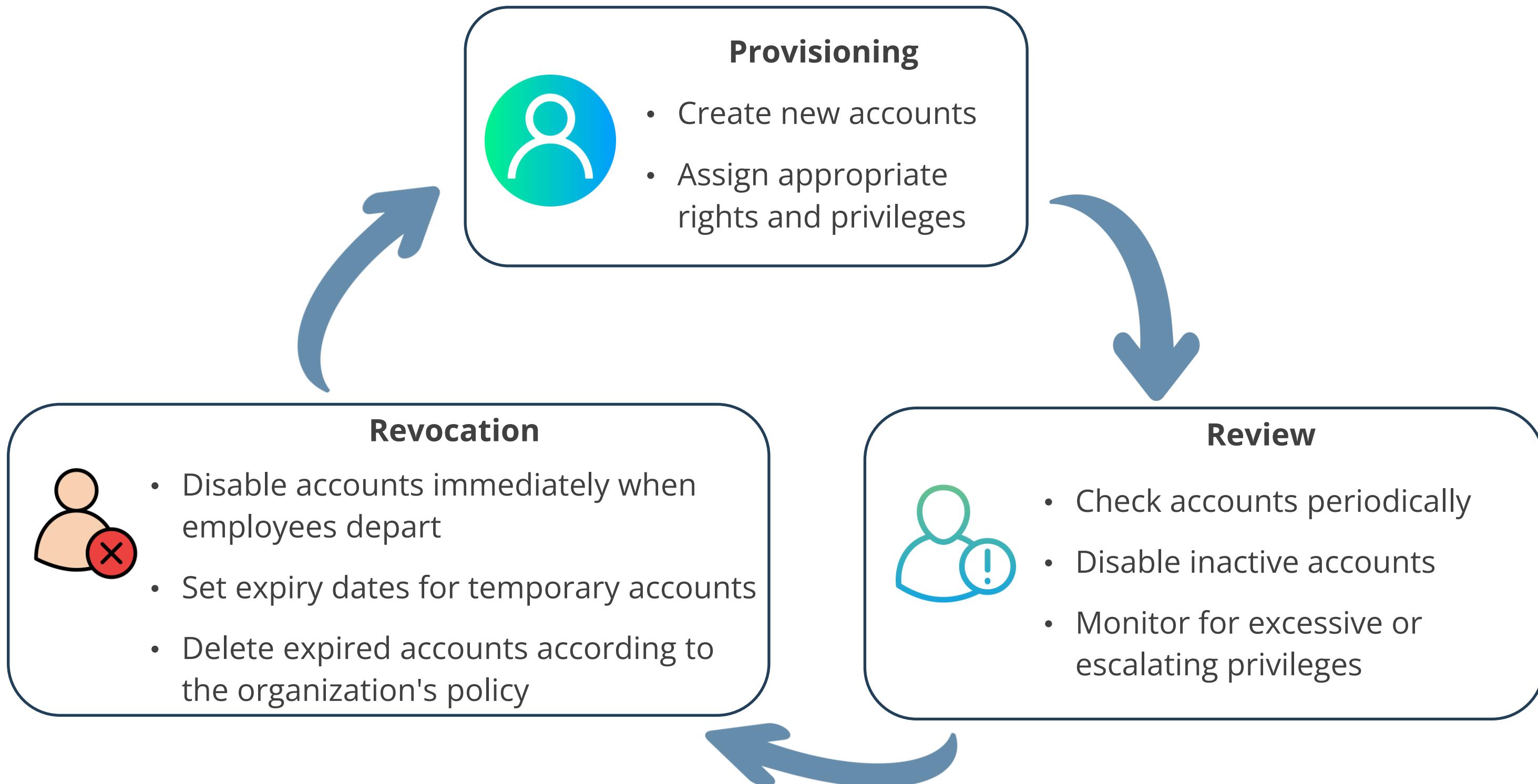
Manage the Identity and Access Provisioning Lifecycle

Identity Proofing

- Confirms a person's identity to ensure the authenticity and legitimacy of their actions
- Acts as a foundational step in identity and access management, helping organizations prevent fraudulent activities
- Requires presenting certain forms of evidence such as a passport, driver's license, or Social Security number (SSN) for identification



Identity and Access Provisioning Process



Account Access Review

- Reviews access rights periodically for all employees and vendors to identify excessive or escalating privileges
- Creates service accounts specifically for use by services, applications, and virtual machines
- Grants elevated privileges and access to business-critical applications and data to service accounts
- Dictates policies to determine when accounts should be reviewed, deactivated, or deleted
- Conducts regular reviews or audits of service accounts to identify unusual behaviors that may indicate a breach or misuse



Privileged Accounts

- Defines accounts with more privileges than normal user accounts
- Includes highly privileged accounts like administrator (Windows) or root (Unix/Linux)
- Allows normal users to temporarily gain root privileges using the sudo command (Unix/Linux)
- Creates accounts specifically for services, applications, and virtual machines
- Assigns full administrative privileges without considering the principle of least privilege, posing a security risk if compromised

Privilege Escalation



Occurs when a malicious user gains higher levels of permissions, access, or privileges than they have been assigned

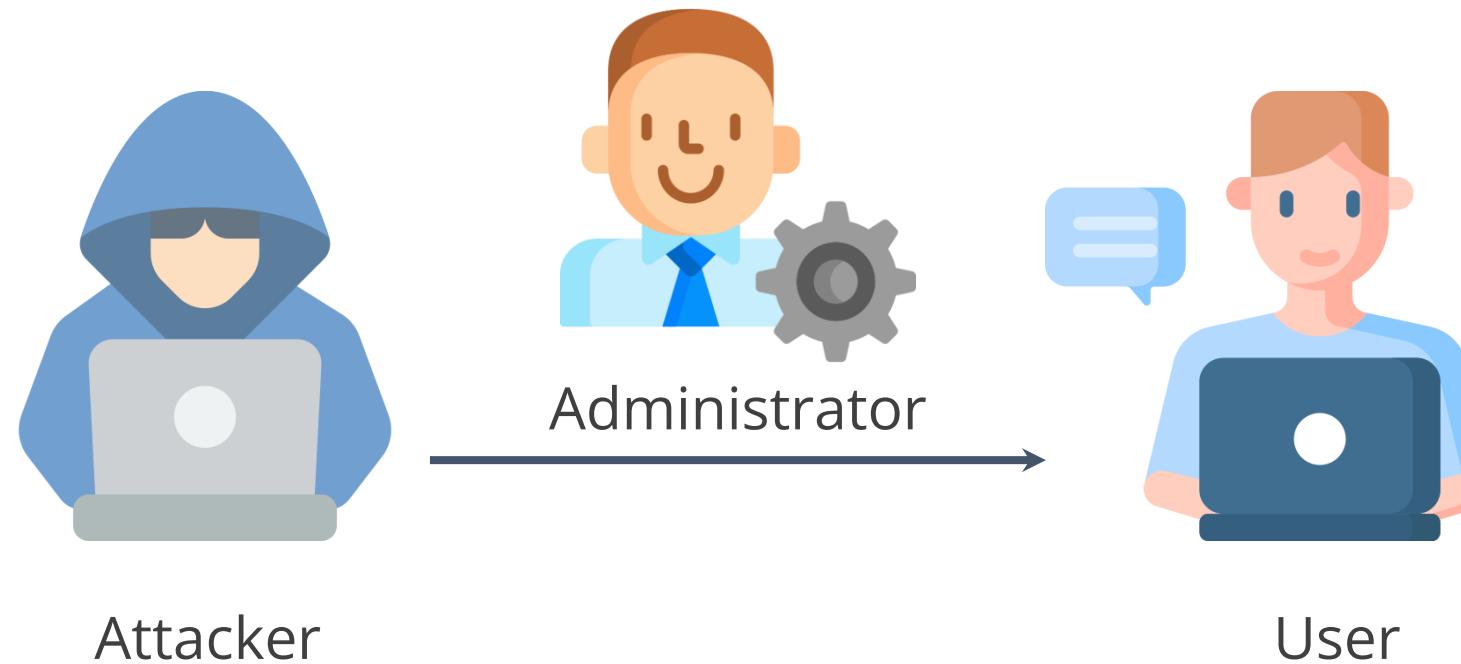


Happens due to administrative oversight, identity theft, or credential compromise

Horizontal Privilege Escalation



Occurs when an attacker gains rights and privileges of another user with similar privileges



Is referred to as **account takeover**

Vertical Privilege Escalation



Occurs when an attacker gains access to an account and tries to elevate its privileges



Is also known as a privilege elevation attack, moving from low to high privileged access

Countermeasures



- Use multi-factor authentication
- Minimize the number and scope of the privileged accounts
- Follow the principle of least privilege

Countermeasures



- Enables continuous monitoring of privileged accounts and keeps detailed logs of activities
- Analyzes privileged accounts to identify and address risks, threats, sources, and attacker intents
- Prevents sharing of privileged accounts and credentials

Active Directory



Active Directory (AD) is a proprietary directory service developed by Microsoft for Windows domain networks.



Active Directory

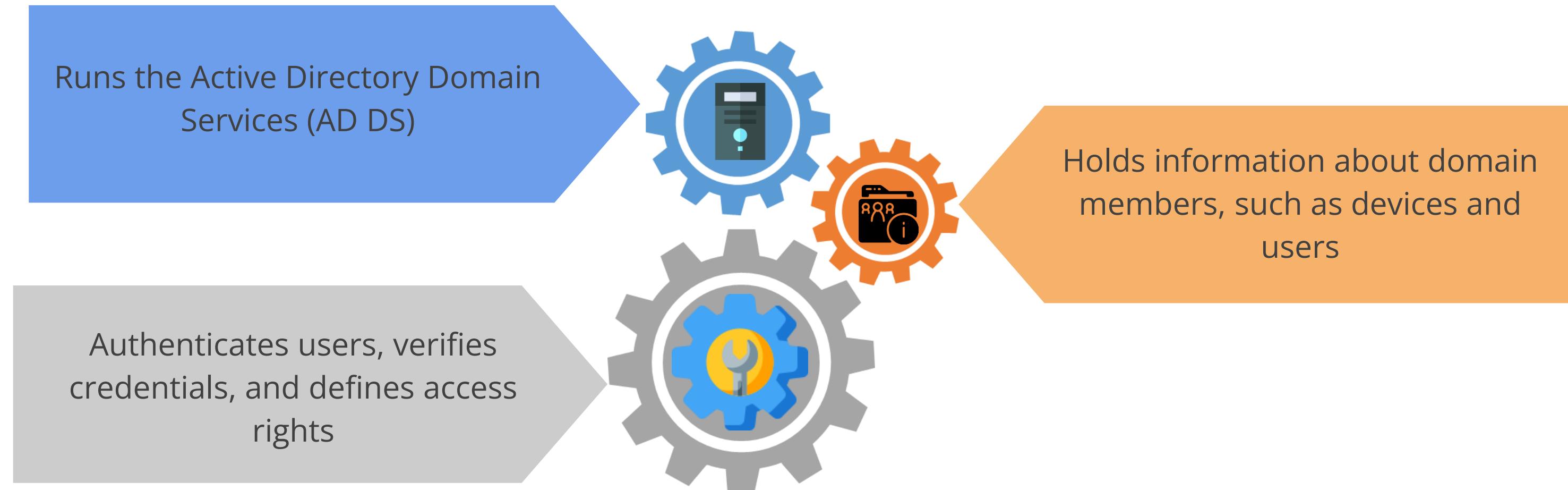


Includes Active Directory in Windows Server operating systems, enabling administrators to manage permissions and access to resources

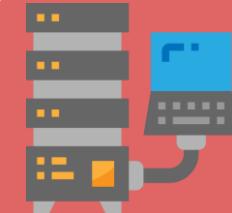


Uses Microsoft's version of Kerberos, DNS, and Lightweight Directory Access Protocol (LDAP) versions 2 and 3

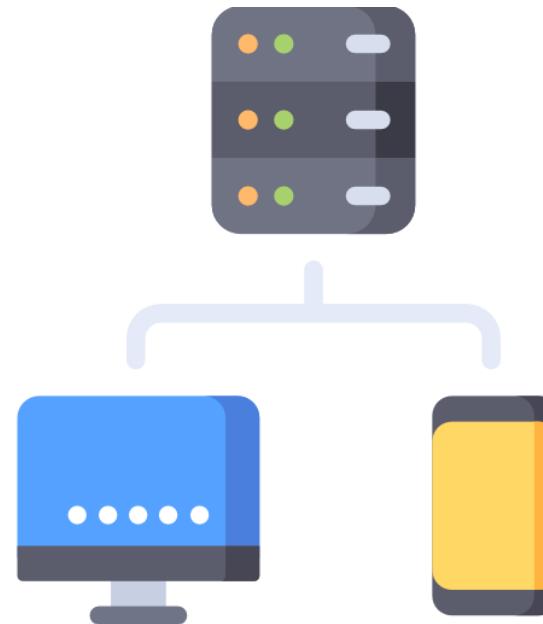
Domain Services



Lightweight Directory Access Protocol



Based on the ITU-X.500's Directory Access Protocol standard, the Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, and industry-standard directory service.

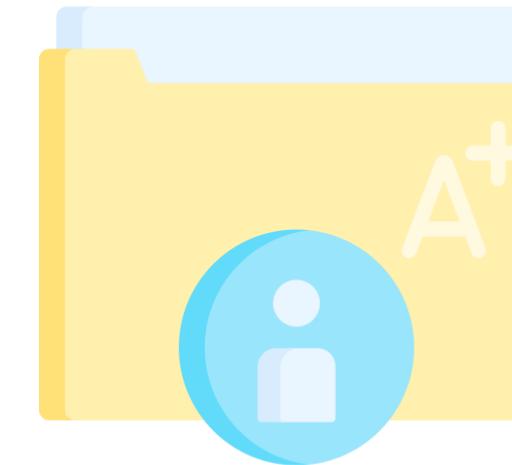


The LDAP directory service operates on a client-server model.

Lightweight Directory Access Protocol

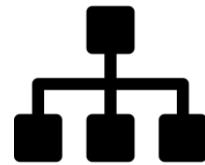


LDAP is used to access and manage distributed directory information services over an Internet Protocol (IP) network.

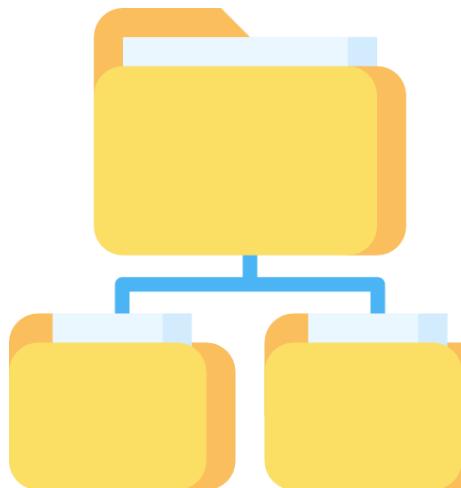


Is often used for authentication and storing information about users, groups, and applications

LDAP Directory Structure



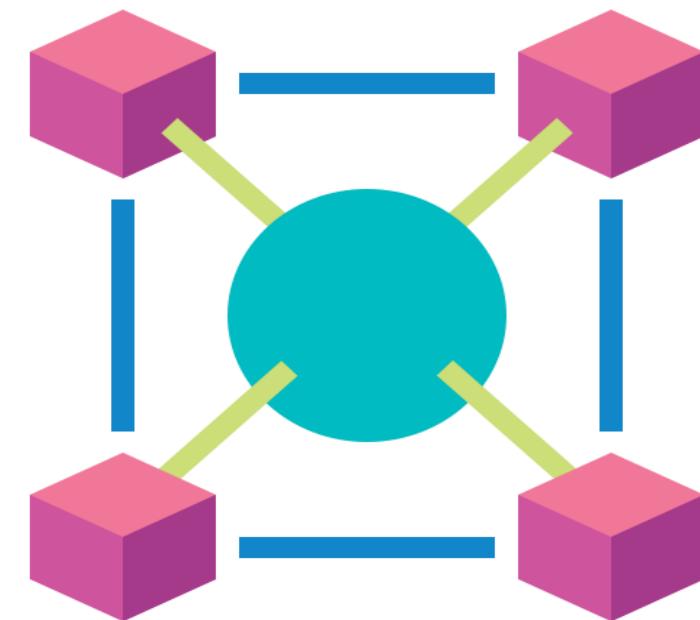
The root entry in an LDAP directory is the highest item in a directory, which is a hierarchical tree structure.



The organization that owns the directory is usually represented by the root entry.

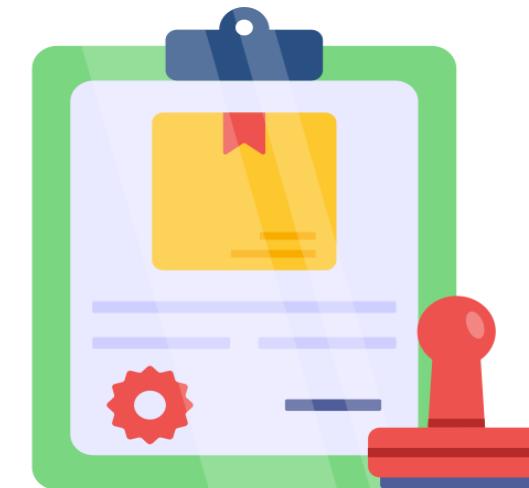
Interoperability

- Interoperability is the ability of different platforms, systems, or technologies to work together seamlessly or exchange and use information in a compatible and effective manner.
- Within IAM, this specifically refers to systems, and not all systems will interoperate in this manner.
- For instance, web applications that normally use OAuth cannot use Kerberos authentication.



Attestation

- Attestation is the process of verifying and confirming that access privileges assigned to users are accurate, complete, and aligned with their current roles and responsibilities.
- It is the process of reviewing and confirming that users have the right access to perform their jobs securely while minimizing the risk of unauthorized access or data breaches.



Attestation Methods

Certificates

Certificates, issued by trusted Certificate Authorities (CAs), function as digital passports, confirming the legitimacy of entities and ensuring secure, encrypted communication across networks.

Tokens

Tokens, frequently employed in OAuth, provide a secure means to confirm user identity and privileges, granting controlled access to valuable resources.

Attestation Methods

Federation

Federation serves as a mechanism to establish cross-domain trust, enabling seamless resource sharing among diverse organizations, confirming user identities, and facilitating SSO capabilities.

Microsoft active directory

Microsoft AD is a powerful directory service tailored for Windows domain networks. It confirms attestation by managing user data, safeguarding valuable resources, and enforcing policies to uphold the integrity and security of networked environments.

Access Control Best practices

Denies access to systems for undefined users or anonymous accounts

Limits and monitors the use of administrator and other powerful accounts

Suspends or delays access capability after a specific number of unsuccessful logon attempts

Removes obsolete user accounts as soon as users leave the company

Enforces strict access criteria

Enforces need-to-know and least-privilege practices

Suspends inactive accounts after 30 to 60 days

Disables unnecessary system features, services, and ports

Replaces default password settings on accounts

Removes redundant IDs, accounts, and role-based accounts from resource access lists

Enforces strong password requirements

Ensures that if the same message is encrypted with the same key and sent twice, its ciphertext is the same

Installing Active Directory and Creating a User



Duration: 10 Min.

Problem Statement:

As a system administrator, you are tasked with installing Active Directory on a Windows Server and creating a user account to manage organizational resources. The objective is to establish a centralized directory service that facilitates user and resource management, enhances security, and streamlines administrative tasks within the organization. This setup will enable secure access control and efficient management of networked resources and user permissions.

Note: Refer to the demo document for detailed steps:
[05_Installing_Active_Directory_and_Creating_a_User](#)

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Install Active Directory Domain Services (AD DS)
2. Create a user under the active directory

Configuring Logon Hours in Active Directory



Duration: 10 Min.

Problem Statement:

As an IT administrator, you are tasked with creating a step-by-step guide for configuring logon hours in Active Directory. The purpose is to enhance security and access control by implementing Attribute-Based Access Control (ABAC). This guide will help ensure that users can only access network resources during authorized hours, thereby reducing the risk of unauthorized access and improving overall security management.

Note: Refer to the demo document for detailed steps:
[06_Configuring_Logon_Hours_in_Active_Directory](#)

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Open a Virtual Machine using the Remote Desktop Connection
2. Open Active Directory Users and Computers
3. Create and Locate the User Account
4. Open User Properties and Set Logon Hours
5. Configure Logon Hours
6. Apply and Close

Importance of Automation and Orchestration Related to Secure Operations

Automation and Scripting

Automation

- Application of technology to perform tasks with minimal human intervention
- Involves technologies from simple scripts to complex software programs and robotic systems

Scripting

- Specific type of automation using programming languages
- Automates tasks within a computer operating system or application
- Scripts are sets of instructions executed step-by-step by the computer

Use Cases of Automations

User provisioning

Ensures user accounts are created, configured, and granted access rights swiftly and accurately

Resource provisioning

Allows allocation and deallocation of resources such as virtual machines, storage, and network resources as needed

Guard rail

- Establishes guard rails by enforcing predefined policies and configurations
- Ensures systems and resources operate within specified parameters to reduce misconfigurations

Security groups

- Enables creation and management of security groups
- Defines who can access specific resources or services

Ticket creation

Enhances IT support and incident response through automated ticket creation and tracking

Enabling/Disabling services and access

Automates the enabling or disabling of services and access within systems

Escalation

- Triggers predefined escalation procedures in critical incidents
- Ensures high priority calls are raised and dealt with immediately

Integration and APIs

Links together tools and systems for streamlined automation and complex process management

Advantages of Automation

Efficiency/Time-saving

Saves time and provides efficiency

Allows time to be used in other productive work

Enforce baseline

Ensures systems consistently adhere to predefined baselines and configurations

Standard infrastructure configurations

Assists in standardizing infrastructure configurations (e.g., firewalls, server environments)

Scaling in a secure manner

Enables seamless scaling of resources while maintaining security

Reaction time

- Ensures threat detection and response are lightning-fast
- Identifies, assesses, and acts upon security incidents in real-time, reducing potential damage

Workforce multiplier

- Automates complex, multi-step processes
- Reduces the time workers spend on boring tasks

Other Considerations for Automation

Complexity

- Streamlines operations but adds management complexity
- Requires carefully designed and maintained workflows
- Becomes more intricate as security needs evolve

Costs

- Involves upfront costs for implementing automation tools and training
- Benefits include efficiency gains and improved security
- Crucial to evaluate long-term cost-benefit analysis for determining what should be automated and how

Other Considerations for Automation

Single point of failure

- Relying on a single automation system for critical security functions creates a single point of failure
- Diversifying automation reduces operational risks

Ongoing supportability

- Needing ongoing support, maintenance, and updates prevents outdated or vulnerable systems
- Assessing sustainability and alignment with a long-term security strategy maintains effectiveness

TECHNOLOGY

Incident Response Activities

Incident Management



Event

Any observable occurrence in a system or a network



Incident

Any event that negatively affects the company and impacts its security posture



Incident response

A practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future references

Incident Response Goals

The goals of incident response are:

Reduce the potential impact
to the organization

Deter attacks through
investigation and prosecution



Provide management with
sufficient information

Maintain or restore business
continuity

Defend against future attacks

Incident Response Team

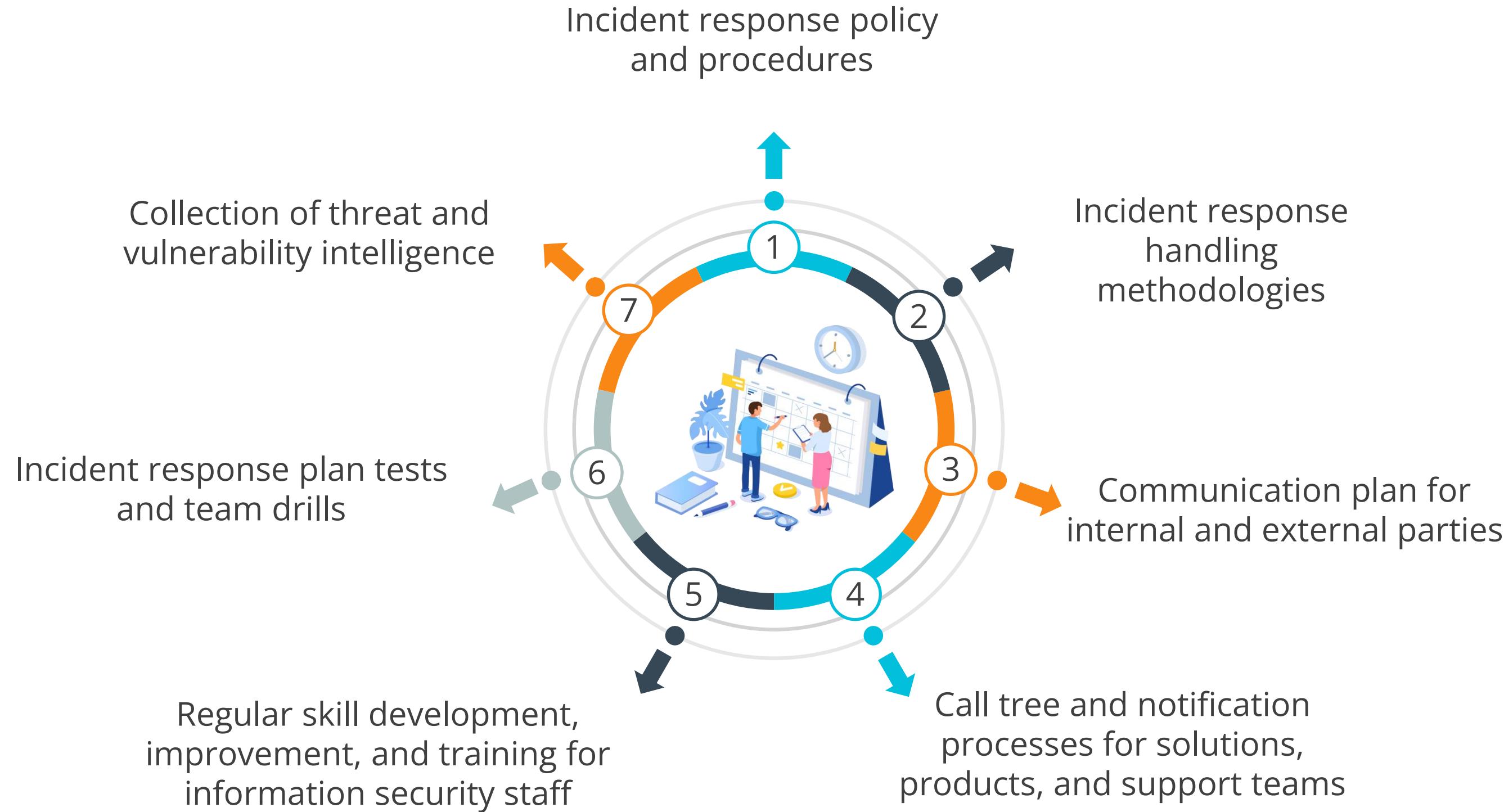
An incident response team is a group of people who prepare for and respond to emergencies.

Basic checklist of an incident response team

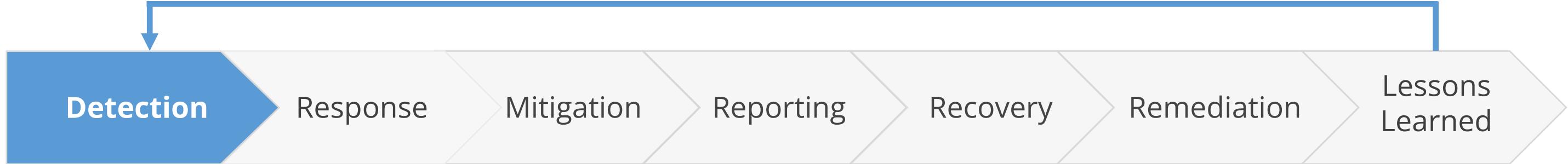
- A list of outside agencies and resources to contact or report to
- An outlined list of roles and responsibilities
- A call tree to contact the defined roles and outside entities
- A detailed procedure to secure and preserve evidence
- A list of items that should be included in the report for the management and the courts
- A description of how different systems should be treated in a particular situation



Incident Management: Planning and Preparation

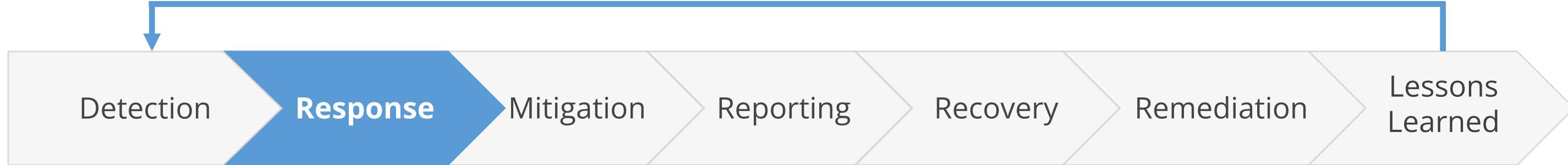


Incident Response Life Cycle



- Automated detection capabilities: Network-based and host-based Intrusion Detection Systems (IDPS), antivirus software, and log analyzers
- Manual detection: Issues reported by end users

Incident Response Life Cycle



The response process includes:

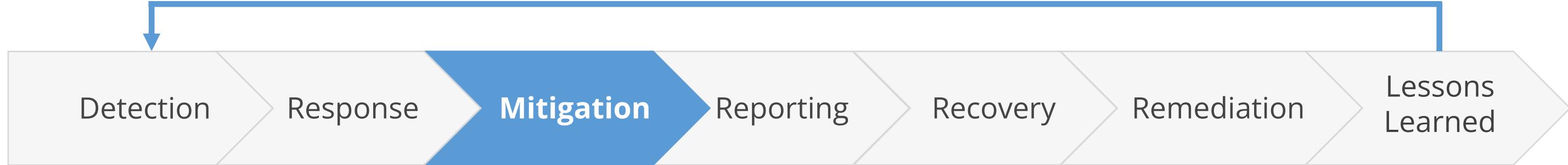
Triage: Ensures that only valid alerts are escalated for further investigation. This step helps in identifying and discarding false positives

Severity assessment: Gathers information to evaluate the severity and set priorities for incident handling

Categorization: Classifies incidents by their severity, potential risk, source, rate of growth, and potential for containment

Root cause analysis: Focuses on identifying the underlying cause of the incident

Incident Response Life Cycle



Objectives of mitigation include:

- **Asset prioritization:** Focuses first on critical assets, followed by less critical ones
- **Containment and isolation:** Limits exposure to prevent further damage
- **Forensic analysis:** Ensures forensic samples are taken before mitigation efforts begin

Incident Response Life Cycle



Effective reporting should include:

Current Status: Updates on the incident's progress (new, in progress, under investigation, or resolved)

Summary: Concise overview of the incident

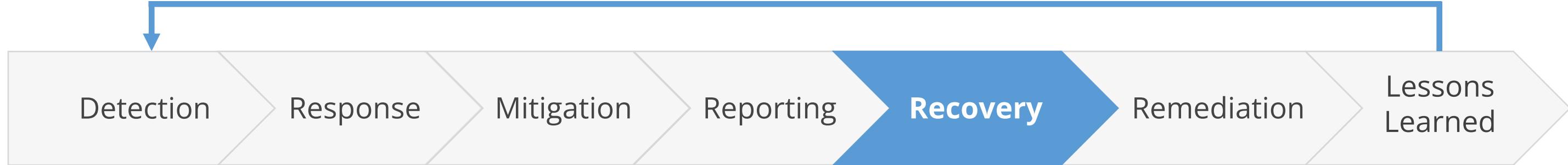
Detailed Documentation: Actions performed, chain of custody (if applicable), and impact assessment

Evidence: Comprehensive list of evidence gathered

Communications: Remarks from incident handlers

Next Steps: Planned actions following the incident report

Incident Response Life Cycle



The recovery process aims to restore systems to operational status and includes:

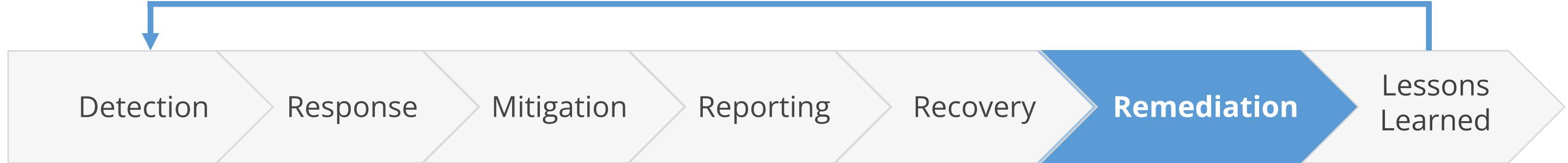
Hardware repair/replacement: Addressing physical and operational damage to hardware

System software reinstallation: Reinstalling or reconfiguring operating systems and applications

Data restoration: Recovering data from backup media to ensure no information loss

Program cleanup: Removing any unwanted programs and data introduced during the incident

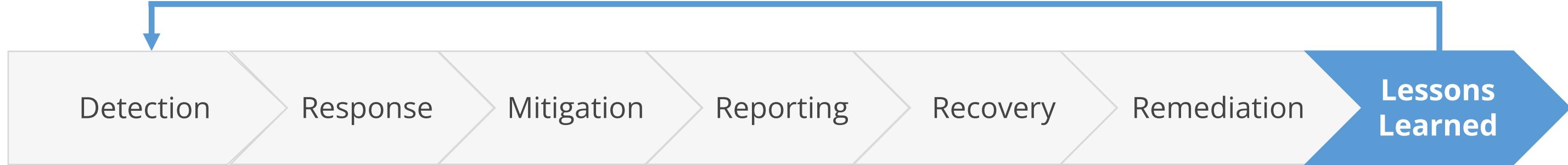
Incident Response Life Cycle



Key aspects of remediation include:

- **System repair:** Fixes to affected systems and software
- **Communication:** Updates and instructions to all affected parties
- **Analysis:** Confirming that the incident is fully contained and unlikely to reoccur
- **Preventive measures:** Adjusting policies and protections to prevent future incidents

Incident Response Life Cycle



Important considerations for lessons learned include:

- **Review meetings:** Regularly scheduled to discuss the handling and outcome of incidents.
- **Documentation:** Detailed follow-up reports that serve as references for future incident response efforts.
- **Continuous improvement:** Using insights gained to enhance the incident response plan.

Incident Response Training

Training programs are integral to the Business Continuity Plan (BCP) and Disaster Recovery (DR), ensuring that all employees are prepared for incident response activities.

Trainings ensure employees:



Types of Security Training

Various trainings conducted include:



Security awareness training:

Educes on the latest cyber threats and prevention methods.



Call tree training:

Ensures employees understand security policies and incident response actions align with organizational policies.

Incident Handling and Simulation Training

Focused training includes:



Incident handling:

Comprehensive training from incident onset to resolution



Simulation and drills:

Provides practical experience through controlled simulations and drills

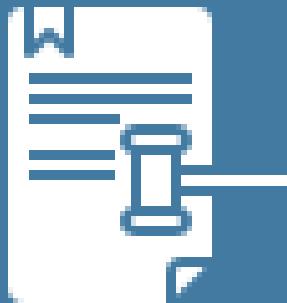
Communication and Legal Training

Advanced training sessions cover:



Communication skills:

Focuses on practical skills for interacting with stakeholders and collaboration within teams.



Legal and regulatory compliance:

Includes training on the legal and regulatory aspects of incident management.

Incident Response Testing

Checklist walkthroughs

A basic review to ensure all steps in the plan are documented and accounted for

Tabletop exercises

Team members gather around a table to discuss their roles and responses to a simulated incident scenario

Parallel simulations

Conducted alongside normal operations, allowing the team to test their response without impacting real systems

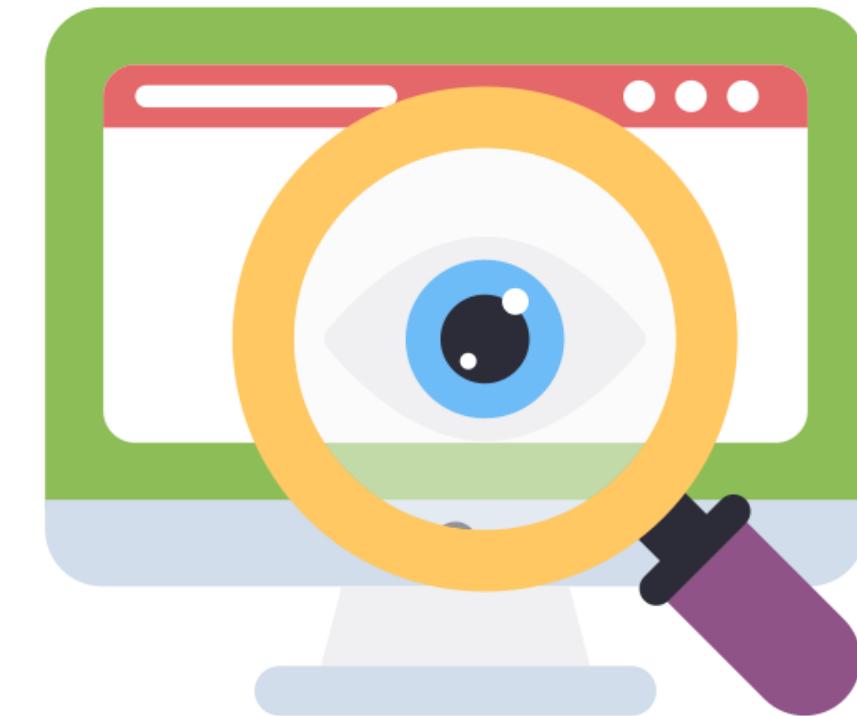
Full-interrupt simulations

These halt normal operations to simulate a real-world incident scenario.

Root Cause Analysis

Root Cause Analysis (RCA) is a problem-solving technique designed to identify the underlying causes of problems rather than just addressing the symptoms. Key aspects of RCA include:

- **Identifying underlying causes:** Focuses on discovering the fundamental issues that lead to problems
- **Preventing recurrence:** Aims to prevent future issues by systematically addressing the root causes



Root Cause Analysis

Exploring the significance of root cause analysis includes:

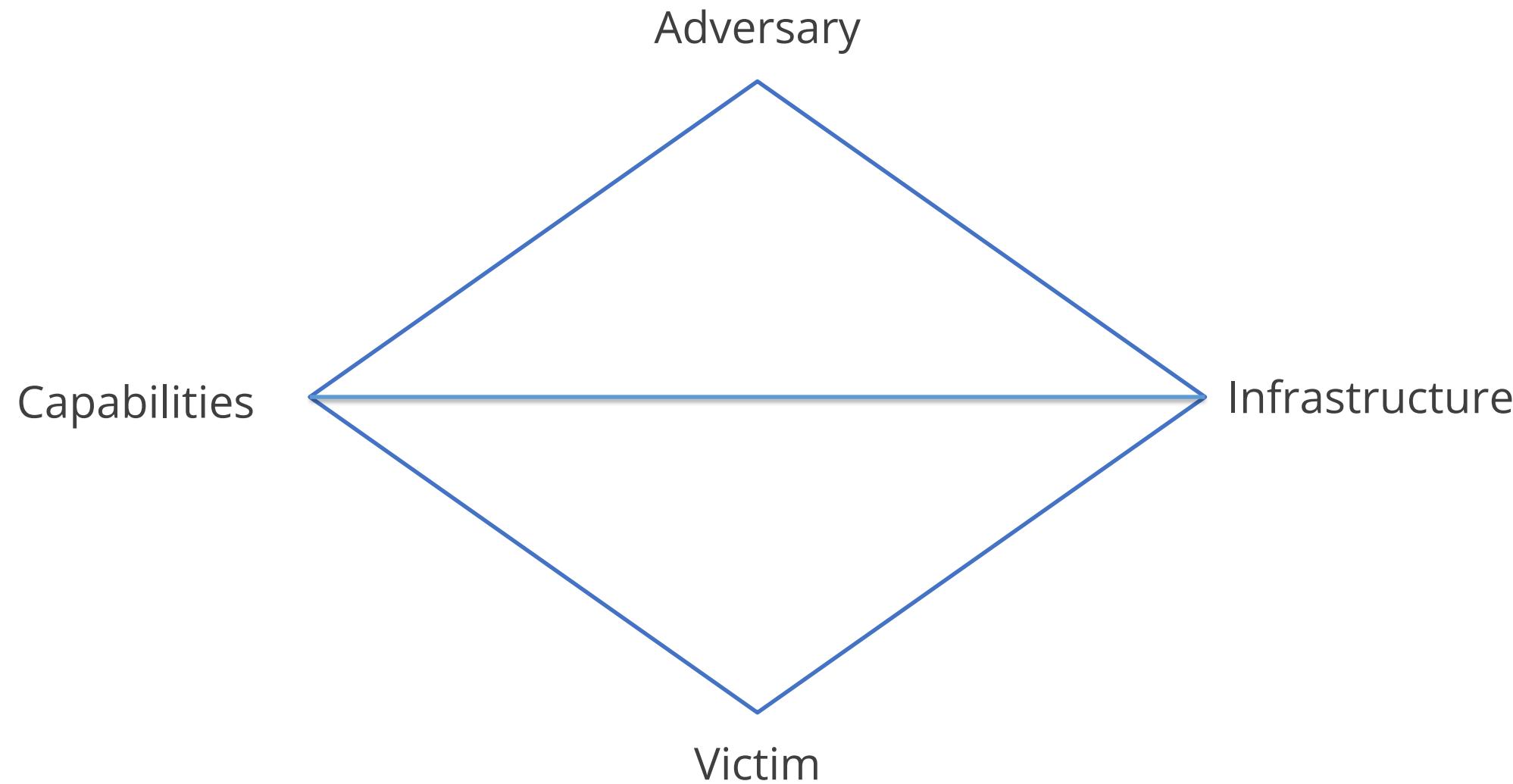
- **Systematic process:** Root Cause Analysis (RCA) is a systematic approach to identifying the underlying causes of an incident.
- **Strategic decisions:** By understanding these causes, organizations can make informed decisions to strengthen their systems and enhance resilience.
- **Continuous improvement:** RCA provides deep insights into problems, promoting improvements in future incident responses.



Diamond Analysis of Intrusion



The Diamond Model is a framework used in cybersecurity to analyze and investigate cyberattacks. The model examines intrusions through four interconnected facets include



Diamond Analysis

Adversaries

This facet represents the attacker or threat actor responsible for the intrusion. Analysts aim to understand the motivations, resources, capabilities, and affiliations of the adversary.

Capabilities

This area explores the technical skills and tools used by the adversary to exploit vulnerabilities and achieve their objectives.

Parallel simulations

This refers to the methods and pathways by which the attacker reaches the victim. This could include channels like USB, email, IP address, or remote access.

Full-interrupt simulations

These halt normal operations to simulate a real-world incident scenario.

MITRE ATT&CK Framework

It is a globally recognized resource for understanding cyber adversaries' tactics and techniques. It serves as a comprehensive knowledge base of attacker behavior, allowing defenders to proactively anticipate and thwart cyber threats.

This framework empowers cybersecurity professionals with crucial insights to address and mitigate evolving threats.



MITRE Attack



Adversarial:
Looks at the behavior of potential groups and provides information about the adversaries and the group to which they belong

Tactics:
Represents the different stages of an attack, such as reconnaissance, initial access, execution, persistence, privilege escalation, and exfiltration

Techniques:
Specifies the methods attackers use within each tactic. For instance, social engineering, phishing emails, and exploiting vulnerabilities are all techniques used for initial access

Common knowledge:
This is the documentation relating to the attackers' tactics and techniques made publicly available online

Cyber Kill Chain

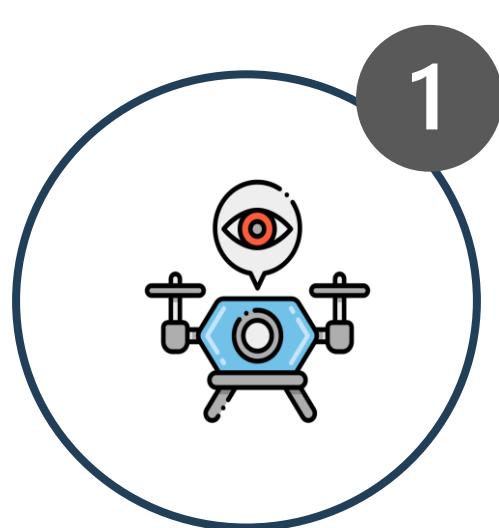
The cyber kill chain is a foundational cybersecurity concept derived from the military kill chain. It outlines the various stages a cyber attacker typically follows to infiltrate a system and achieve their goals.

Understanding these stages empowers security teams to:

- Implement preventative measures and disruption strategies at each point
- Identify what attackers need to accomplish to succeed, aiding defense planning
- Provide a structured view of an attack, enhancing visibility and analyst understanding



Cyber Kill Chain



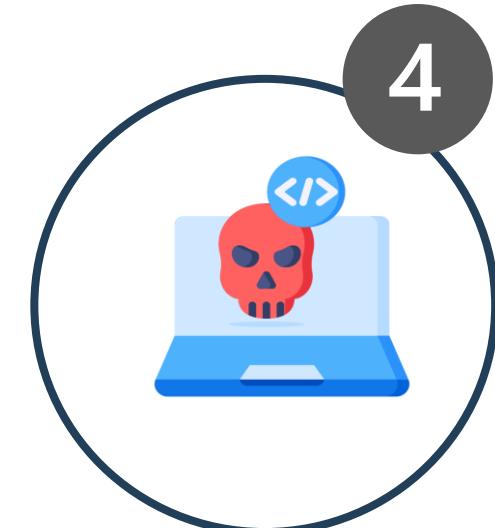
Reconnaissance



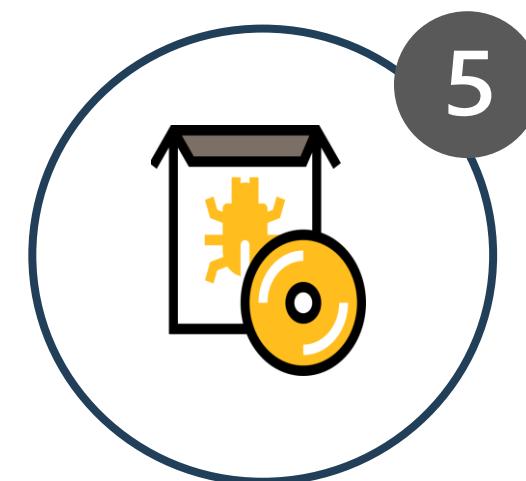
Weaponization



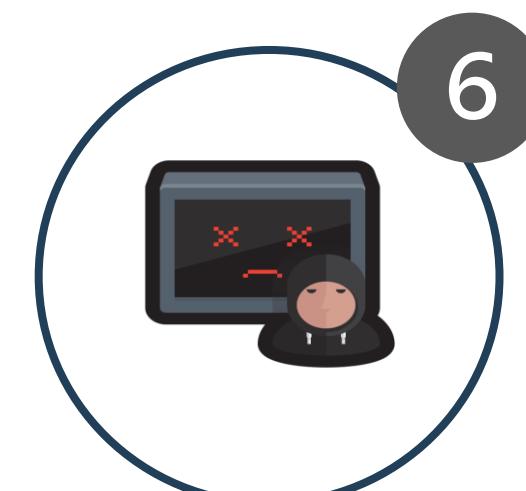
Delivery



Exploitation



Installation



Command and
control



Action on
objectives

Threat Hunting



Threat hunting involves:
Planning, collecting, processing, analyzing, and disseminating information that poses a threat to an organization. This knowledge is then applied to mitigate the threat.

The value of threat hunting includes:

- Detecting threats early and minimizing potential damage
- Enhancing adaptability by allowing security measures to quickly adjust to new types of attacks

Benefits of threat hunting:

- Processing threat data to better understand attackers
 - Responding faster to incidents
- Proactively getting ahead of the attacker's next move

TECHNOLOGY

Digital Forensics

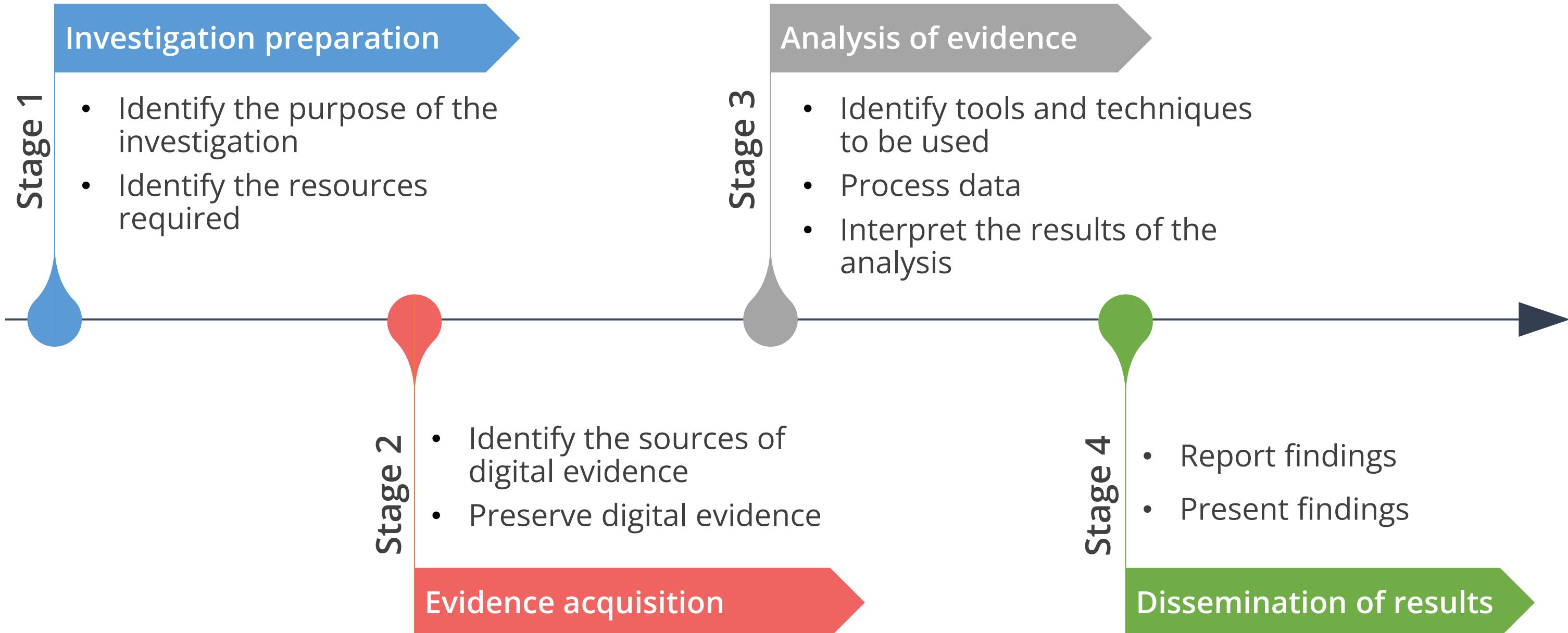
Digital Forensics

Digital forensics, sometimes known as digital forensic science, is a branch of forensic science that involves the recovery and investigation of material found in digital devices, often in relation to cyber crimes.



The goal of digital forensics includes:
Examining digital media in a forensically sound manner
Identifying, preserving, recovering, analyzing, and presenting facts and opinions about the digital information

Forensic Process



Forensic Investigation Guidelines

Best practices according to Forensic Australian Computer Emergency Response Team include:

- Minimize handling or corruption of the original data
- Account for any changes and keep detailed logs of your actions
- Comply with the five rules of evidence
- Do not exceed knowledge and take the aid of experts and specialists if required
- Follow local security policies and obtain written permission
- Capture an accurate image of the system as possible
- Be prepared to testify
- Ensure actions are repeatable
- Work fast and proceed from volatile to persistent evidence
- Do not run any programs on the affected system



Forensic Disk Controller or Write Blocker

Forensic disk controller

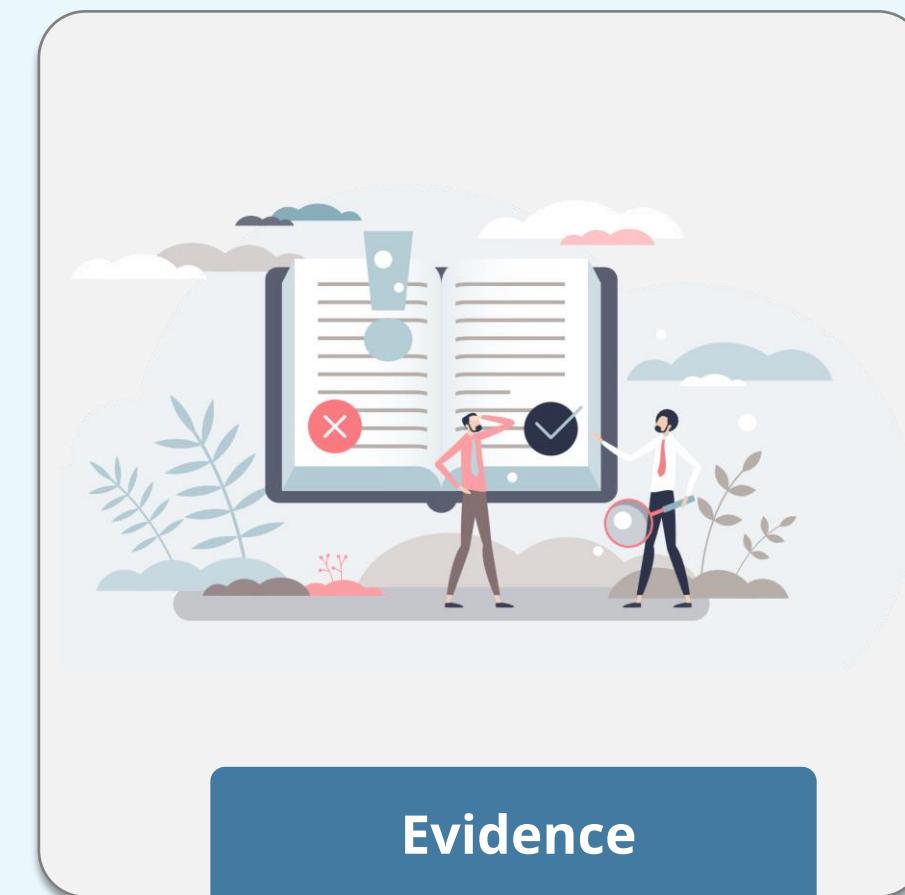
- A forensic disk controller or a hardware write-block device is a specialized type of computer hard disk controller designed for gaining read-only access to computer hard drives without risking damage to the drive's contents.
- The device is called a forensic disk controller because its most common application is in investigations where a computer hard drive may contain evidence.

Functions of a forensic disk controller

- A hardware write-block (HWB) device will not transmit a command to a protected storage device that modifies the data on the storage device.
- An HWB device will return the data requested by a read operation.
- An HWB device will return without modification any access-significant information requested from the drive.
- Any error condition reported by the storage device to the HWB device will be reported to the host.

Evidence

- The available body of facts or information indicating whether a belief or proposition is true or valid
- Evidence, broadly construed, is anything presented in support of an assertion
- Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party may use at a trial in court

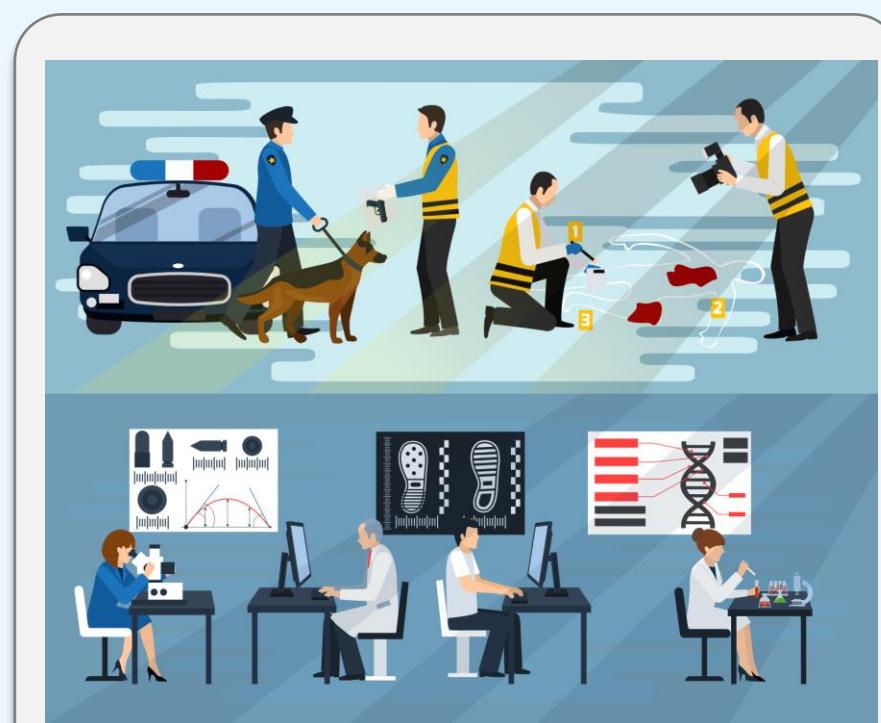


Evidence

Evidence

Evidence is relevant when:

- It is related to the crime
- It can provide information describing the crime
- It can provide information regarding the motives of the perpetrator
- It can verify what has occurred
- It can determine the time of occurrence of the crime



Evidence

Acquisition of Evidence

It involves collecting data from various sources, including modern digital devices like USB flash drives and computers, as well as traditional paper-based documents such as letters and bank statements.

Recording the time includes:

Record time offset: Capture the regional time setting or time zone when gathering evidence from computers.

Time normalization: Convert evidence collected across multiple time zones into a common time zone (such as GMT) to create a chronological sequence.



Order of Evidence Capturing



CPU cache:

This fast but volatile memory is used by the CPU and can provide critical insights.



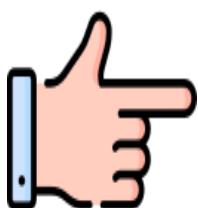
Random Access Memory(RAM):

Volatile memory running applications holds valuable information.



Swap/Page file/Virtual memory:

Used when RAM is exhausted, these are areas of a hard drive used instead of RAM, but much slower.



Hard drive:

Data at rest is the least volatile and is captured after volatile memory. This is where data is saved to the hard drive.

Admissible Evidence

There are three basic requirements for evidence to be introduced in a court of law. To be considered admissible evidence, it must meet all three of these requirements, as determined by the judge prior to being discussed in an open court:

Relevant:

The evidence must be relevant to determining a fact

Material:

The fact that the evidence seeks to determine must be material, that is, related to the case

Competent:

The evidence must be competent, which means it must have been obtained legally. Evidence resulting from an illegal search would be inadmissible because it is not competent

Types of Evidence

Testimonial evidence

It consists of the testimony of a witness, either verbal testimony in court or written testimony in a recorded deposition. Testimonial evidence must not be hearsay evidence.

Hearsay evidence

It is third-party information with hardly any proof of reliability or accuracy. It is secondhand evidence in the form of oral or written statements.

Real evidence

It consists of physical items that may be brought into a court of law. In common criminal proceedings, this may include items such as a murder weapon, clothing, or other physical objects.

Types of Evidence

Documentary evidence

It includes any written items brought into court to prove a fact at hand. This type of evidence must be authenticated, and original documents need to be produced.

Conclusive evidence

It is irrefutable and cannot be contradicted, overriding all other evidence.

Best evidence

It is the original or primary evidence, providing the most reliability. An example would be a signed contract.

Chain of Custody

- In legal context, it refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.
- Chain of custody shows how the evidence was collected, analyzed, transported, and preserved to be presented in court.

EVIDENCE			
Submitting Agency	_____		
Date Collected	_____	Time	_____
Item #	_____	Case #	_____
Collected By	_____		
Description of Evidence	_____		
Location Where Collected	_____		
Type of Offense	_____		
CHAIN OF CUSTODY			
Rec. From	_____	By	_____
Date	_____	Time	_____
Rec. From	_____	By	_____
Date	_____	Time	_____
Rec. From	_____	By	_____
Date	_____	Time	_____

Chain of Custody

Major components of the Chain of Custody

- Location of evidence when it was obtained
- Time at which evidence was obtained
- Identification of individual(s) who discovered evidence
- Identification of individual(s) who secured evidence
- Identification of individual(s) who controlled evidence and maintained possession of that evidence

EVIDENCE			
Submitting Agency	_____		
Date Collected	_____	Time	_____
Item #	_____	Case #	_____
Collected By	_____		
Description of Evidence	_____		
Location Where Collected	_____		
Type of Offense	_____		
CHAIN OF CUSTODY			
Rec. From	_____	By	_____
Date	_____	Time	_____
Rec. From	_____	By	_____
Date	_____	Time	_____
Rec. From	_____	By	_____
Date	_____	Time	_____

Legal Hold

It is also known as a litigation hold, is a process used to preserve electronically stored information (ESI) and physical documents that might be relevant in a potential lawsuit or investigation.

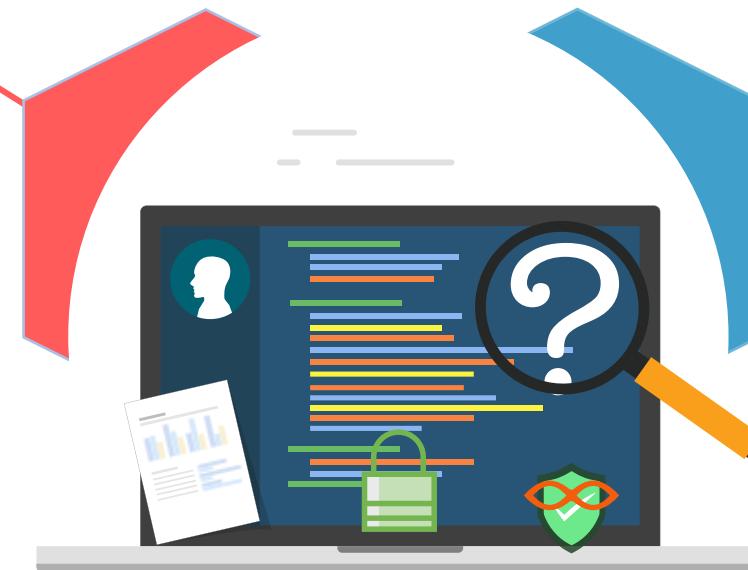
- The primary purpose of a legal hold is to prevent spoliation of evidence, which is the destruction, alteration, or loss of evidence that could be used in legal proceedings.
- A legal hold can be triggered by a court order or by an organization's anticipation of litigation.
- Legal holds apply to all potentially relevant electronic and physical information. This includes emails, documents, spreadsheets, voicemail recordings, chat logs, and social media posts.



E-Discovery

Electronic discovery, also called e-discovery, refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

This discovery process applies to both paper records and electronic records.



Electronic discovery process facilitates the processing of electronic information for disclosure.

TECHNOLOGY

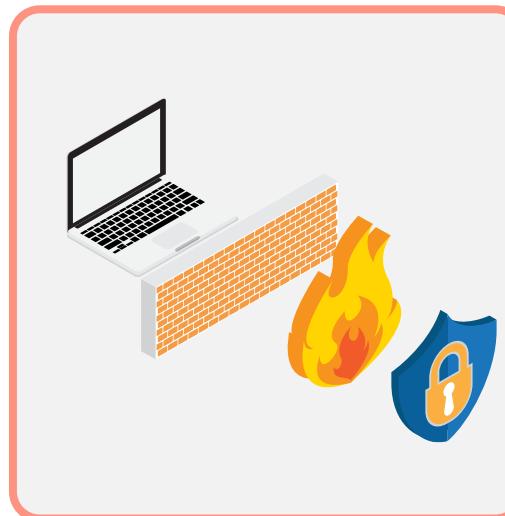
Use of Data Sources to Support Investigations

What Are Logs?



In IT, an event log is a basic resource that provides information about network traffic, system traffic, and other conditions.

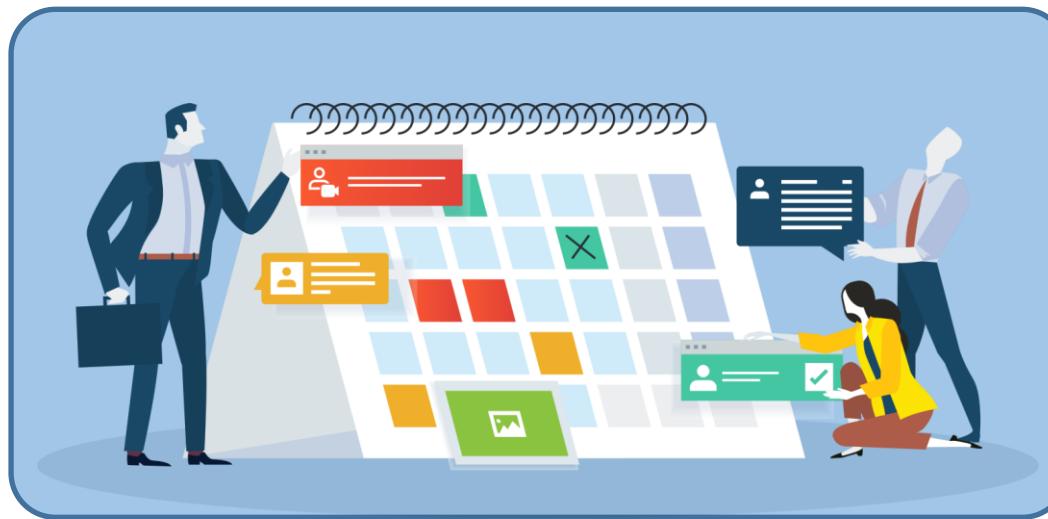
An event log stores this data for retrieval by security professionals or automated security systems to help IT administrators manage various aspects such as security, performance, and transparency.



Besides records related to computer security, logs are generated from many other sources such as antivirus software, firewalls, intrusion detection systems, and prevention systems.

Log Management and Review

Log management involves the collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archiving, and disposal of the large volumes of log data created within an information system.



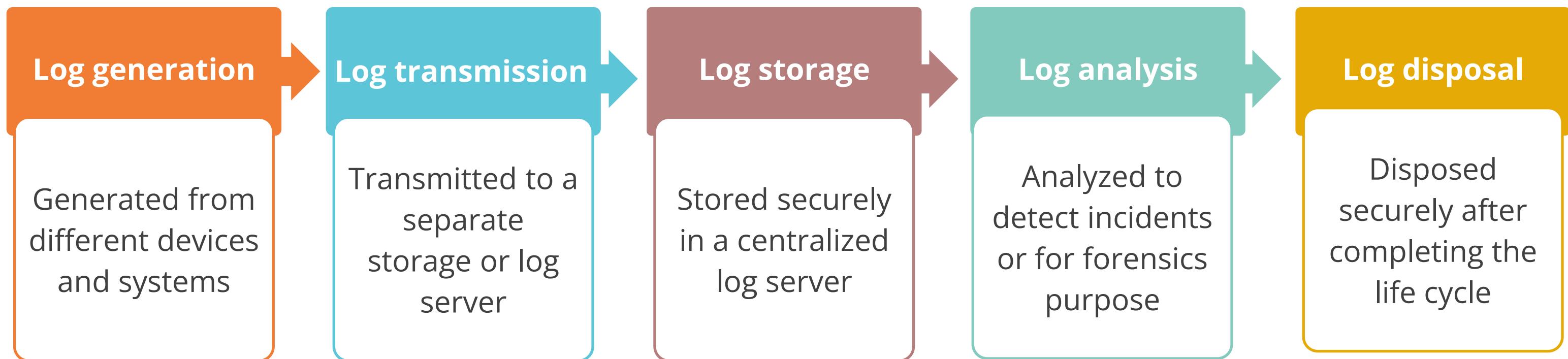
System logs are examined to detect security events or verify effectiveness of security controls.

A key requirement for an effective log review is time synchronization across all log sources.

NTP is the protocol for time synchronization (UDP 123).

Log Management Phases

Log management involves the following steps:



Log Tampering Prevention

It is vital to maintain the integrity of log data. Here are the methods to prevent it from being tampered:

Remote logging

Placing a log file into another device will protect it from being tampered with in a compromised system

Simplex communication

- Using one-way communication between the reporting devices and the central log repository
- This is accomplished by severing the receive pairs on an Ethernet cable.

Replication

Make multiple copies and keep them in different locations

Write-once media

Use write-once media to prevent unauthorized modifications to log files

Cryptographic hash

A powerful technique for ensuring unauthorized modifications are easily noticed.

Log Management: Advantages and Challenges

Advantages

- Ensuring confidentiality, integrity, and availability of logs
- Forensic investigations
- Auditing
- Identifying security incidents, fraud, and operational issues
- Establishing baselines

Challenges

- Managing large quantities of logs from various sources
- Addressing discrepancies in log content, timestamps, and formats

Log Management: Best Practices

- Establish log management policies and procedures
- Prioritize requirements for log management process
- Define roles and responsibilities
- Create and maintain log management infrastructure
- Support the staff responsible for log management



Different Types of Logs

Firewall logs

- Firewall logs hold information about incoming and outgoing traffic, including the source and destination IP addresses, ports, and protocols.
- These logs allow investigators to identify unauthorized access attempts, track potential intrusions, and recognize patterns of malicious activity.

Application logs

- Application logs include the events happening within the software systems.
- They capture details about user interactions, errors, and events within applications.
- When investigating issues or breaches related to a specific application, these logs provide critical context that helps analysts pinpoint the root cause of the problem and understand user behavior.

Different Types of Logs

Endpoint logs

- Endpoints, such as computers and mobile devices, generate logs documenting user activities, system changes, and security events.
- These logs are invaluable when investigating incidents involving compromised devices or suspicious user behavior.
- The domain name system (DNS) log file shows every website the user visits, making it particularly useful when reviewing the activity of an end user who visited malicious sites.

OS-specific security logs

- Operating systems (like Windows, macOS, or Linux) maintain security logs that record system events and security-related activities.
- These logs provide detailed information about the health and security of the OS, invaluable in the detection of anomalies, vulnerabilities, or unauthorized access.

Different Types of Logs

IDS/IPS logs

- IDS/IPS logs record data on network traffic and patterns.
- By analyzing these logs, investigators can identify and respond to potential threats in real-time, safeguarding the network from intruders and suspicious activities.

Network logs

- Network logs record data flow across a networks, including connections, data transfers, and errors.
- These logs are instrumental in identifying network breaches, tracking data leaks, and understanding the overall health and performance of network infrastructure.

Different Types of Logs

DNS log files

- A DNS log file records websites and devices that have been visited in addition to failed DNS resolutions.
- These are all warning signs that may indicate intrusion attempts on the system.

Metadata

- Metadata refers to information about data, such as file attributes, access times, user interactions, and, for photos, the location of the picture.
- Metadata enhances the investigative process by revealing the who, what, when, and where behind digital activities.

Web server log files

- The web server log file captures the connections to the web server itself.
- It lists the visitor's source IP addresses, status codes, and web pages or web applications visited.

Types of Windows Logs

Event logs

These logs are the heartbeat of the Windows system, recording events such as system startups, shutdowns, application errors, and security-related incidents. Event Viewer, a built-in tool, provides access to this data.

Application logs

These logs store information about software programs. Developers often use these logs to diagnose issues, but they can also be invaluable for troubleshooting application-specific problems.

Security logs

These logs store data such as failed login attempts, access control changes, and other security events that may provide information on an attempted security breach

Types of Windows Logs

System logs

System logs document system-level events and errors. They are indispensable for identifying and addressing hardware and driver issues.

Setup logs

When you install or upgrade software or hardware components, setup logs record the process. These logs can be handy when troubleshooting installation problems.

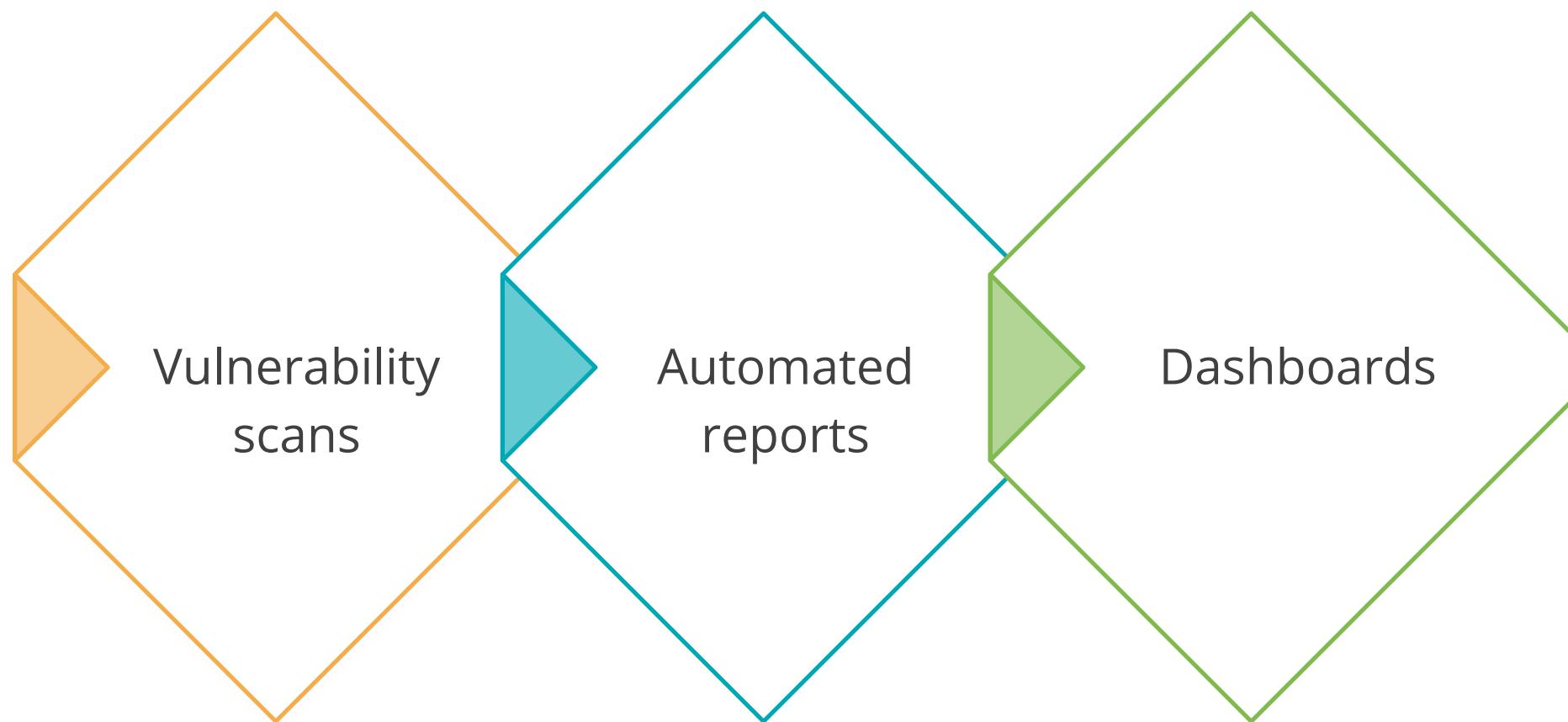
Data Sources

Data sources are the various tools and methods used to collect, analyze, and present information that supports an investigation.

- These sources can range from vulnerability scans that identify weak points in a network to dashboards that provide real-time analytics.
- Understanding how to leverage these data sources effectively is crucial in a comprehensive approach to cybersecurity.



Data Sources



Data Sources: Vulnerability Scans

Vulnerability scans are systematic examinations of networks, systems, or applications to identify and evaluate security weaknesses or flaws that attackers could exploit.

These scans utilize specialized software tools to probe systems for known vulnerabilities, such as unpatched software, insecure configurations, and unprotected systems.

It provides insights into potential security gaps that require remediation to strengthen the overall security posture.

Data Sources: Automated Reports

Automated reports serve as a network's eyes and ears, offering a synthesized view of various security metrics and events.

Automated reports like these enable you to spot irregularities and take corrective action swiftly, thereby minimizing the risk and impact of security incidents

Security information and event management (SIEM) systems, such as Splunk or IBM QRadar, often generate these reports.

Data Sources: Dashboards

A dashboard is a user interface that organizes and presents information in an easy-to-read format, often using graphs, charts, and gauges.

The centralized display aggregates data from multiple sources, providing a real-time overview of an organization's network and security status.

Dashboards allow for prompt responses to threats and efficient monitoring of system health and performance.

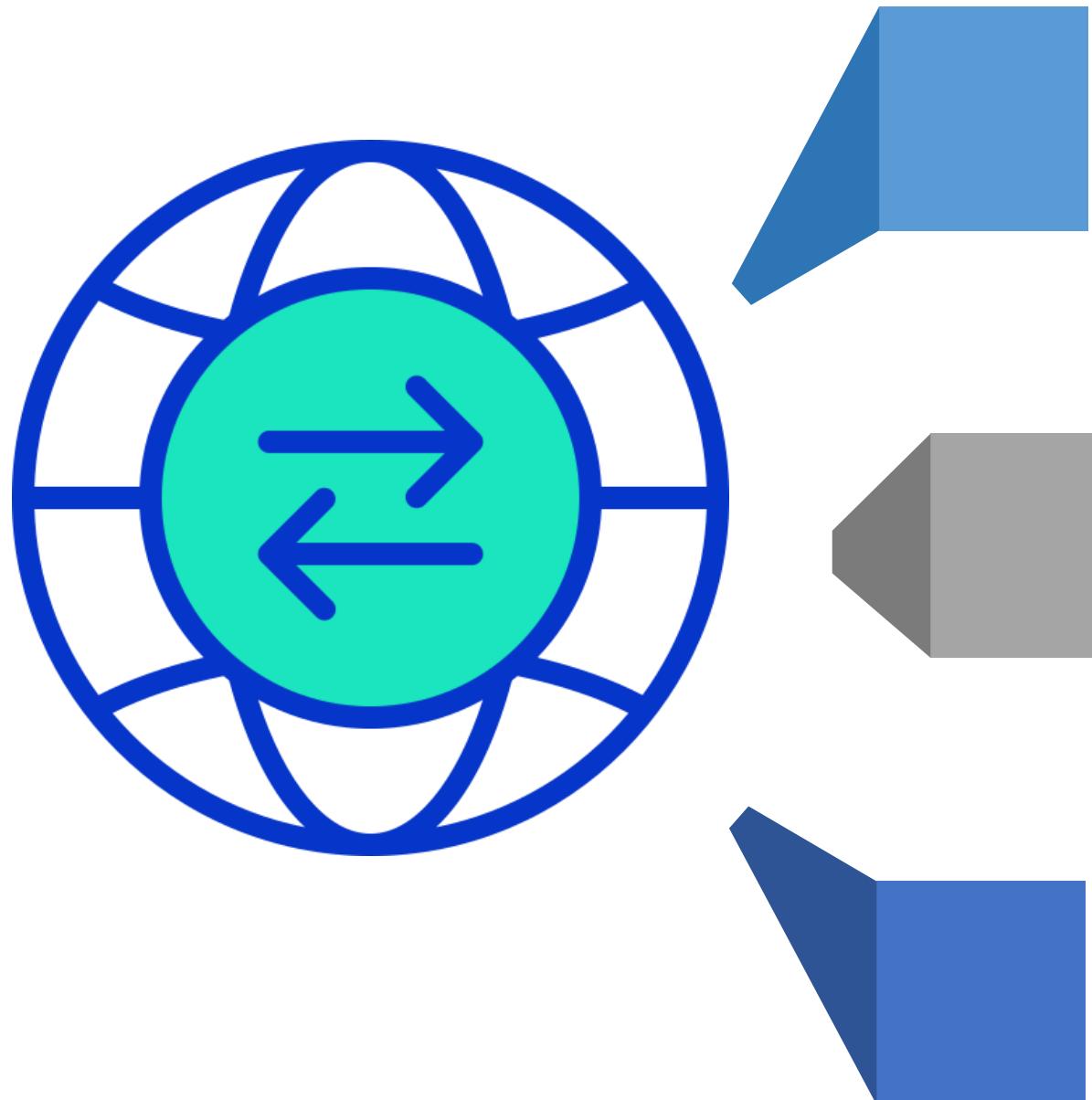
They are pivotal in managing the complex flow of information in cybersecurity operations.

Packet Captures

- Packets are the data that runs up and down our network.
- By capturing packets, cybersecurity administrators can analyze what is happening on the organization's network.
- The tools used can be called packet sniffers or protocol analyzers, with common examples being Wireshark or the Linux-based Tcpdump.
- A trace can be conducted by capturing packets, i.e., saving the data in a packet capture (PCAP) form for later analysis.



Use Cases of Packet Captures



Forensics and incident response: PCAPs can be invaluable for forensic analysis of security incidents because they allow investigators to reconstruct events and identify the source of an attack.

Deep analysis: PCAPs provide highly detailed and specific information about network traffic, which can be used to analyze network behavior in depth.

Baseline creation: It involves establishing a record of normal network traffic patterns. Network administrators can then use this baseline as a reference to compare against current traffic on their network.

Using Event Viewer to Implement Logging and Forensic Analysis



Duration: 10 Min.

Problem Statement:

As a network administrator, you are tasked with implementing logging and forensic analysis using Event Viewer. The objective is to maintain a secure and well-monitored network environment by tracking system events, user activities, and potential security incidents. This implementation aims to enhance the organization's ability to detect, investigate, and respond to unauthorized activities and security breaches effectively.

Note: Refer to the demo document for detailed steps:

[07_Using_Event_Visualizer_to_Implement_Logging_and_Forensic_Analysis](#)

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Use Event Viewer to view successful and failed login
2. Set up a group policy to log the failed login attempts
3. Create a user and add it to the administrator group
4. View the port status and name resolution using netstat and nslookup

Implementing encryption solutions for data at rest using AESCrypt



Duration: 10 Min.

Problem Statement:

As a security engineer, you are tasked with implementing encryption solutions for data at rest using AESCrypt. The objective is to protect sensitive information from unauthorized access, ensuring its confidentiality, integrity, and security during storage and transmission. This implementation aims to safeguard data against potential breaches and comply with security best practices and regulatory requirements.

Note: Refer to the demo document for detailed steps:
[08_Implementing_encryption_solutions_for_data_at_rest_using](#)

Assisted Practice: Guidelines

Steps to be followed are:

1. Install AESCrypt
2. Create a text file and encrypt it using AESCrypt

Using ROHOS Disk Encryption



Duration: 10 Min.

Problem Statement:

As a cybersecurity specialist, you are tasked with demonstrating the process of using ROHOS Disk Encryption to create and manage encrypted virtual drives. The goal is to ensure the protection of sensitive data stored on local systems and portable devices. This involves setting up secure encrypted storage that guards against unauthorized access and data breaches, thereby maintaining data confidentiality and security.

Note: Refer to the demo document for detailed steps:
[09_Using_ROHOS_Disk_Encryption](#)

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Install ROHOS disk encryption software
2. Utilize ROHOS disk encryption software

Key Takeaways

- Hardening techniques are important within organizations for the security of devices within the organization.
- Lifecycle management plays an important role in the security of assets in the organization.
- Security testing is essential for the timely discovery of vulnerabilities, management, and remediation.
- Network security devices play an instrumental role in establishing and managing the security of the enterprise.
- Identity and access management is essential for ensuring that the right people access the right resources in the right manner at the right time.



Key Takeaways

- Automation is essential for the efficient and timely delivery of services in an optimum manner.
- Incident management plays an instrumental role in handling incidents on time, lessening their impact, and eradicating the incidents.
- Digital forensics, chain of custody, and e-discovery are essential for investigation and forensics.
- Mitre framework and cyber kill chain are essential methodologies and frameworks to handle attacks and incidents.
- Log management and types of logs play an important role in the timely detection of attacks and incidents, and they are important in operations.

