Certified Information Systems Security Professional (CISSP) Certification Training Course

CISSP® is a registered trademark of (ISC)² ®

Domain 07: Security Operations

Learning Objectives

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

- Utilize investigative processes to ensure compliance during security incidents
- Apply foundational security concepts to maintain system integrity
- Implement disaster recovery (DR) processes to restore services quickly
- Evaluate disaster recovery plans (DRP) to assess their effectiveness in ensuring operational continuity
- Contribute to business continuity (BC) planning to enhance organizational resilience against disruptions

Overview of Investigations and Its Types

Introduction to Investigation

It is a systematic, minute, and thorough attempt to learn the facts about something complex or hidden. It is often conducted in a formal and official manner.

Digital investigation

- It involves investigating crimes using computers and related technologies where evidence exists in digital form or storage.
- It is also known as computer forensics.

Example

Investigation of a bank failure

Investigation: Types

Operational investigation

Criminal investigation

Regulatory investigation

Civil investigation

Operational Investigation

It examines issues related to the organization’s computing infrastructure with the primary goal of resolving the operational issue.

It aims to identify problems or inefficiencies in operations and find ways to optimize workflows, reduce costs, or mitigate risks.

Criminal Investigation

It is typically conducted by law enforcement personnel and examines a violation of criminal law.

It may result in charging a suspect with a crime and prosecuting those charges in a criminal court.

It must have evidence that proves the crime beyond a reasonable doubt.

Regulatory Investigation

It is conducted by government agencies when they believe that an individual or a corporation has violated administrative law.

It varies widely in scope and procedures and is always conducted by government agents.

Civil Investigation

It typically does not involve law enforcement but rather internal employees and outside consultants working on behalf of a legal team.

Most civil cases use the weaker preponderance of evidence standard, rather than the beyond-a-reasonable doubt standard.

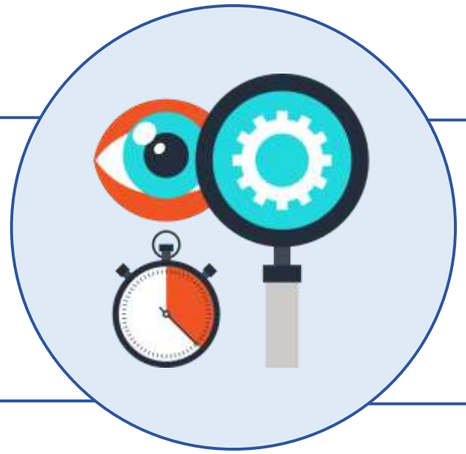
They prepare the evidence necessary to present a case in a civil court resolving a dispute between two parties.

Investigation Challenges

1. It has a compressed time frame for the investigation.
2. It handles intangible information.
3. It is difficult to gather the evidence.
4. It may disrupt normal business operations.
5. Its associated data may be on a computer used for regular business.
6. It requires an expert or a specialist to retrieve the data.
7. It may require working at crime locations spread across different, distant jurisdictions.

Investigation: Primary Activities

An investigation comprises the following primary activities:



1. Identify and gather evidence
2. Examine, analyze, and preserve evidence
3. Establish a chain of custody
4. Present findings

Crime Scene

A crime scene is an environment where potential evidence related to an investigation may exist.

The best practices for handling evidence at a crime scene are:

- Assessing the crime scene
- Securing the environment
- Identifying the evidence
- Determining the potential sources of evidence
- Collecting evidence
- Reducing the degree of contamination

The security professional must understand the crime scene before identifying and collecting evidence.

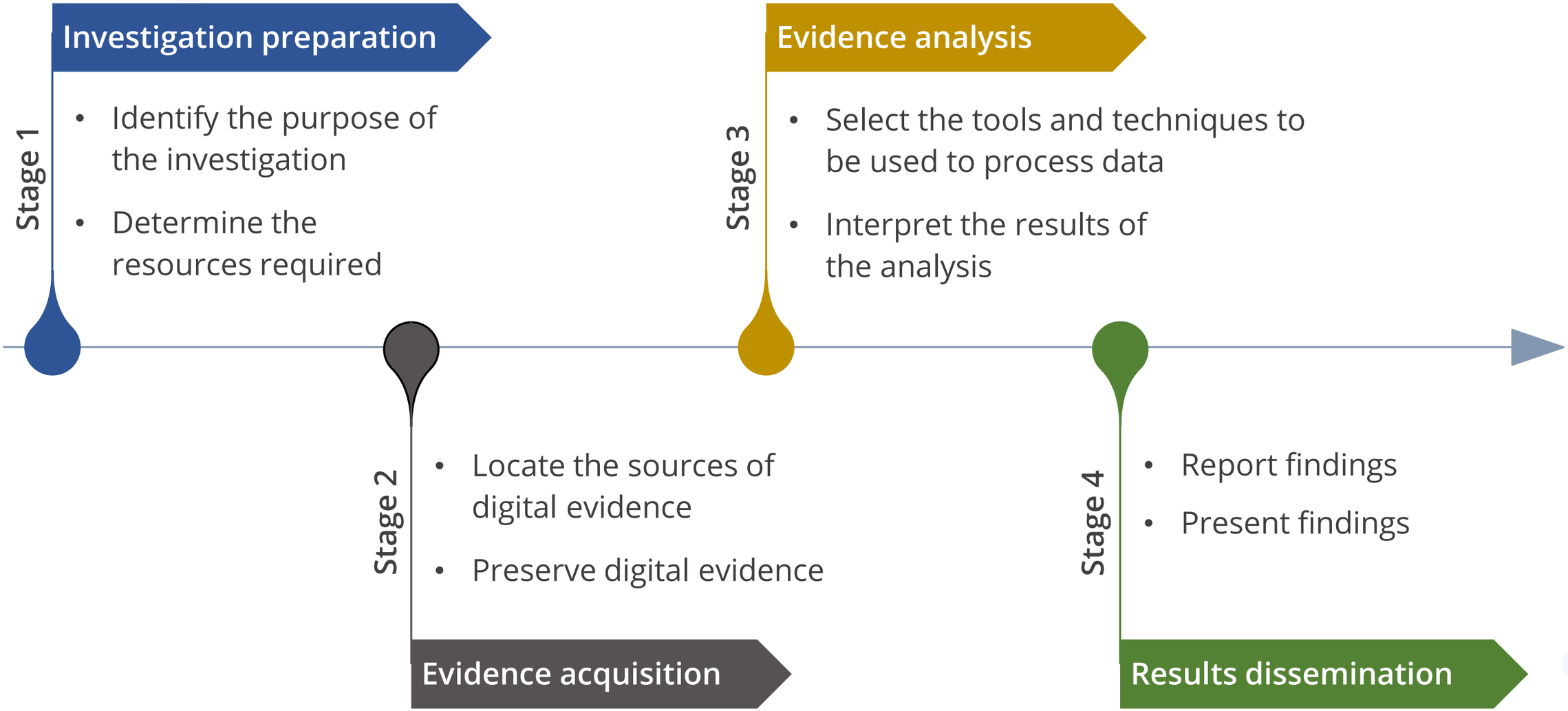
Digital Forensics (Digital Forensic Science)

It is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to cybercrimes.

The goal is to:

- Examine digital media in a sound forensic manner
- Identify, preserve, recover, analyze, and present digital facts and insights related to digital information

Forensic Process



Forensic Investigation Guidelines

The following are the best practices according to the Australian forensic computer emergency response team:

- Minimize handling or corruption of the original data
- Log all changes and maintain detailed records of actions
- Comply with the five rules of evidence
- Avoid exceeding knowledge and consult experts or specialists as necessary
- Follow local security policies and obtain written permission
- Capture the most accurate system image possible
- Be prepared to testify
- Ensure that all actions are repeatable
- Work fast and proceed from volatile to persistent evidence
- Avoid running any programs on the affected system

Forensic Disk Controller or Hardware Write-Block (HWB)

It is a specialized type of computer hard disk controller made to gain read-only access to computer hard drives without the risk of damaging the drive's contents.

The device is named forensic disk controller because its most common application is used in investigations where a computer hard drive may contain evidence.

Forensic Disk Controller or Hardware Write-Block (HWB)

The following are its functions:

- No command transmits to a protected storage device that modifies its data.
- Data requested by a read operation is returned.
- Access-significant information requested from the drive is returned without modification.
- Any error condition reported by the storage device to the HWB device is passed on to the host.

Forensics Investigative Assessment Types

	**Network analysis**	Traffic analysis	Log analysis	Path tracing
	**Media analysis**	Disk imaging	Timeline analysis	Registry analysis	Shadow volume analysis
	**Software analysis**	Reverse engineering	Malicious code review	Exploit review
	**Hardware or embedded device review**	Dedicated appliance attack point review	Firmware and dedicated memory inspections	Embedded operating systems, virtualized software, and hypervisor analysis

Artifacts

It refers to forensic objects that may contain data or evidence relevant to the investigation and can be physical or logical items.

Examples

- Computer
- Network device
- Mobile device
- Event logs
- Registry keys

Investigators must identify and collect artifacts in their custody as evidence.

Evidence

It is the available body of facts or information indicating whether a belief or proposition is valid, and it is presented in support of an assertion.

Digital evidence (electronic evidence) is any probative information stored or transmitted in the digital form that a party may use at a trial in court.

Evidence

An evidence is considered 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


Authentic
01
Accurate
02
Complete
03
Convincing
04
Admissible in the court of law
05
Five rules of evidence

Admissible Evidence

There are three basic requirements for evidence to be introduced in a court of law.

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.

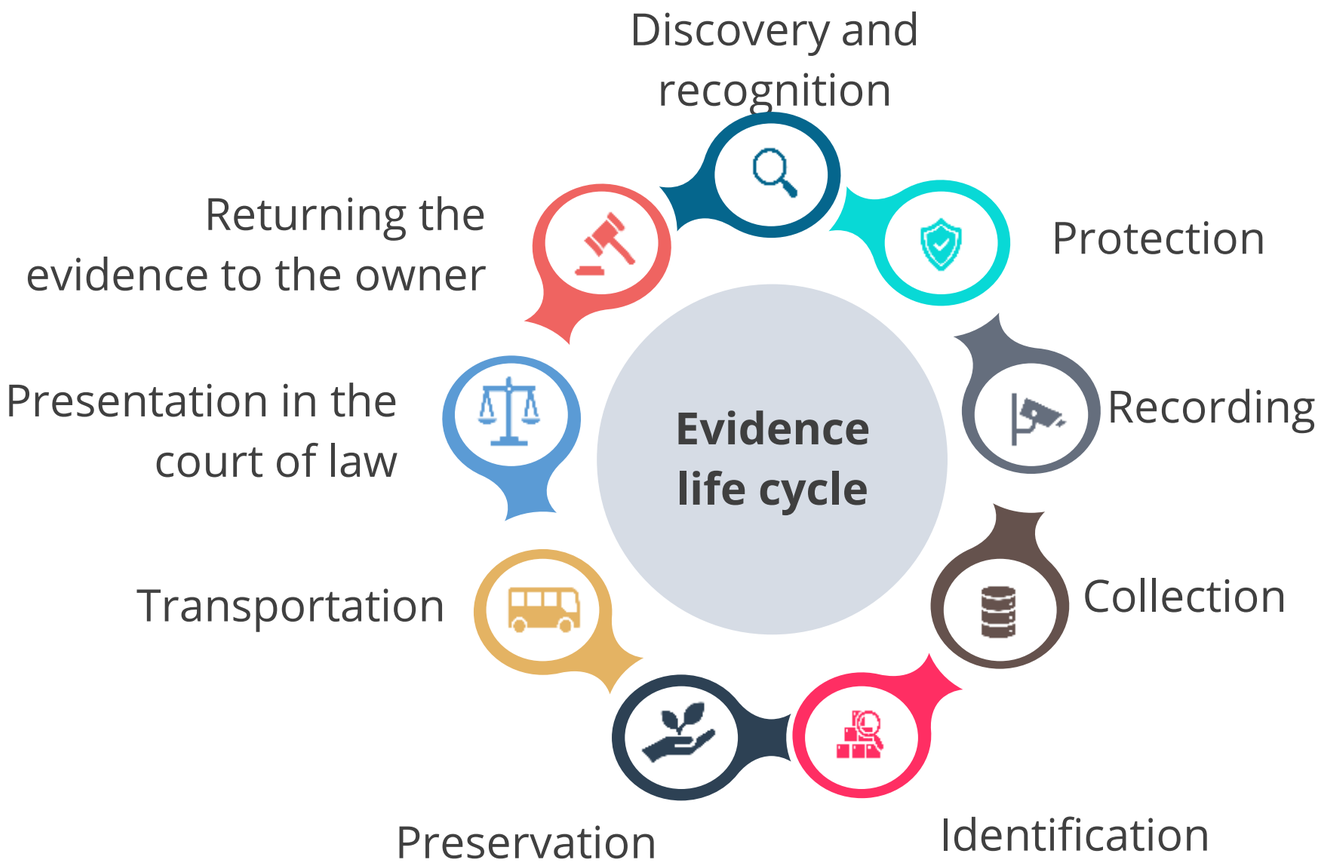
Competent

The evidence must be obtained legally. An evidence from an illegal search is inadmissible due to its incompetence.

The judge determines if the evidence meets these requirements before it can be presented in open court.

Evidence Life Cycle

The gathering, control, storage, and preservation of evidence are extremely critical in any legal investigation.



Types of Evidence

Testimonial evidence

- It is the testimony of a witness, either verbal testimony given in court or written testimony from a recorded deposition.
- It 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.
- It may include items such as a murder weapon, clothing, or other physical objects, in common criminal proceedings.

Types of Evidence

Documentary evidence

- It includes any written items brought into court to prove a fact at hand.
- It must be authenticated, with the original documents required for submission.

Conclusive evidence

It is irrefutable and cannot be contradicted, overriding all other evidence.

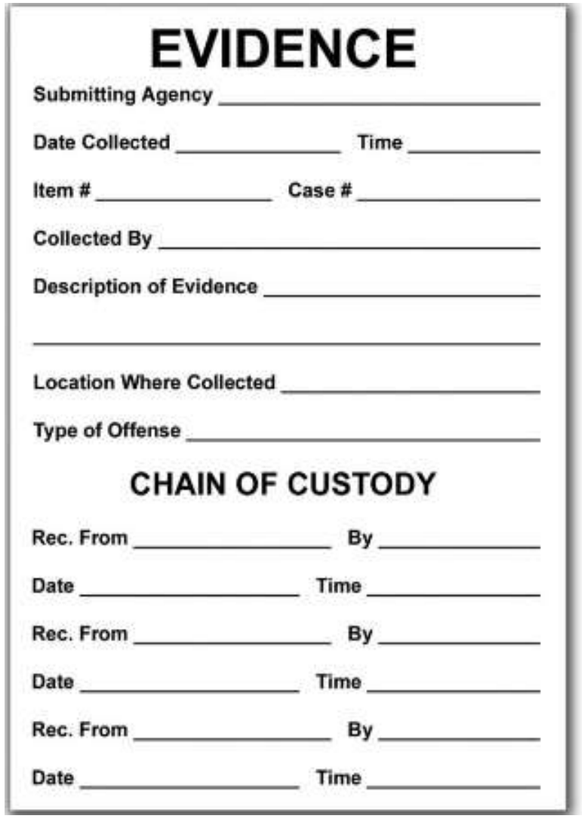
Best evidence

- It is the original or primary evidence, providing the most reliability.
- It may include a signed contract.

Chain of Custody (CoC)

In the 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.

It 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 _____

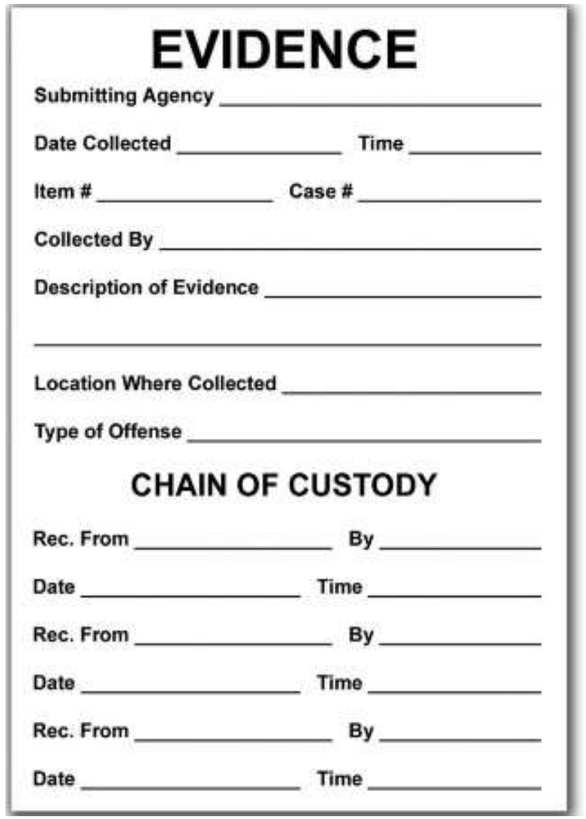
Rec. From _____ By _____

Date _____ Time _____

Chain of Custody (CoC)

The following are its major components:

- 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
- Identification of individual(s) who 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 _____

Evidence Collection Guidelines

The following are the guidelines by the Scientific working group on digital evidence (SWGDE):

- When dealing with digital evidence, one must apply all the general forensic and procedural principles.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When a person needs to access the original digital evidence, that person should be first trained for the purpose.
- All activities involving the seizure, access, storage, or transfer of digital evidence must be documented, preserved, and available for review.
- The individual handling the evidence must be accountable for its management while in their possession.

Electronic Discovery (E-Discovery)

It 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.

It facilitates the processing and disclosure of electronic information.

Legal Hold (Litigation Hold)

It is a process used to preserve electronically stored information (ESI) and physical documents that might be relevant in a potential lawsuit or investigation.

- It prevents spoliation (destruction), alteration, or loss of evidence for legal proceedings.
- It can be triggered by a court order or by an organization's anticipation of litigation.
- It applies to all relevant electronic and physical information, including emails, documents, spreadsheets, voicemails, chat logs, and social media posts.

Quick Check

In a case where law enforcement is struggling to build a case against a hacker, they face challenges due to the nature of the evidence. What makes investigating and prosecuting computer crimes particularly difficult?

A. Backups may be difficult to find.

B. Evidence is mostly intangible.

C. Evidence cannot be preserved.

D. Evidence is hearsay and can never be introduced into a court of law.

Logging and Monitoring Activities

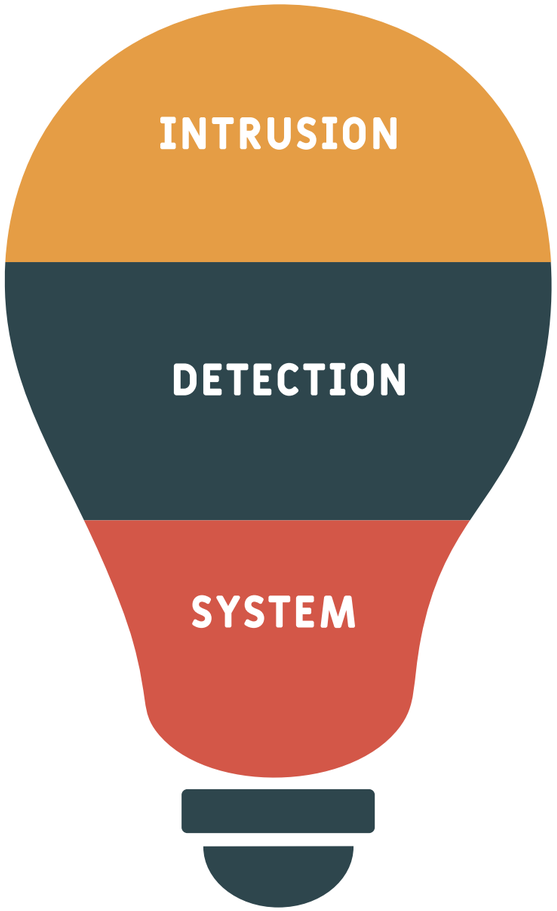
Monitoring of Systems and Infrastructure

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

- It ensures that an organization’s IT assets operate within expected parameters.
- It includes the tracking of systems, applications, and infrastructure, each presenting its own set of challenges and essential metrics.

Intrusion Detection System (IDS)

It detects unauthorized intrusions and suspicious activity in a network, server, or system, and alerts the network administrator.



IDS types

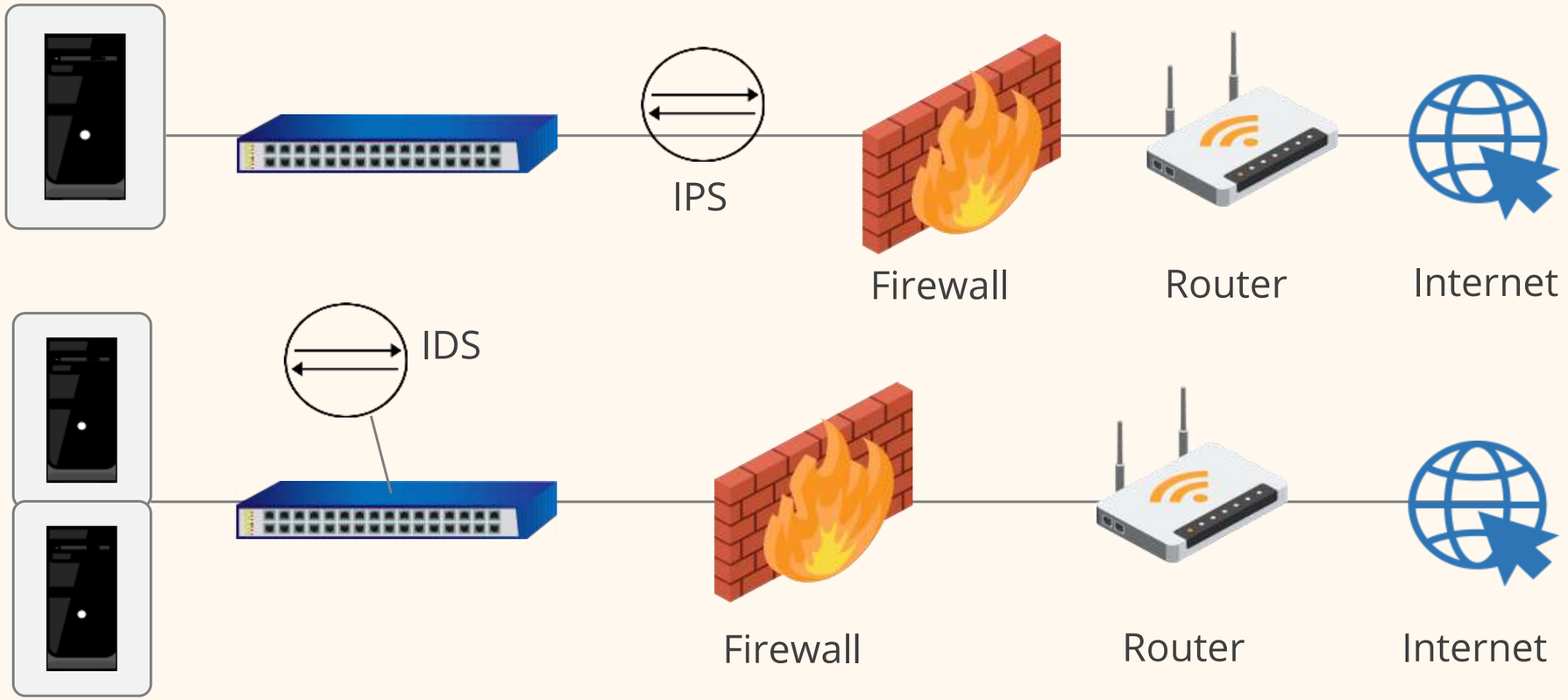
- **Network-based IDS (NIDS):** Detects unauthorized activity through dedicated appliances or systems with a network interface card (NIC) in promiscuous mode and the necessary software installed
- **Host-based IDS (HIDS):** Monitors for malicious or anomalous activity on a workstation or a server

HIDS and NIDS types

- Signature-based
- Statistical anomaly-based
- Rule-based

Intrusion Prevention System (IPS)

It is used to detect and prevent any malicious traffic or activity attempting to gain access to the target.



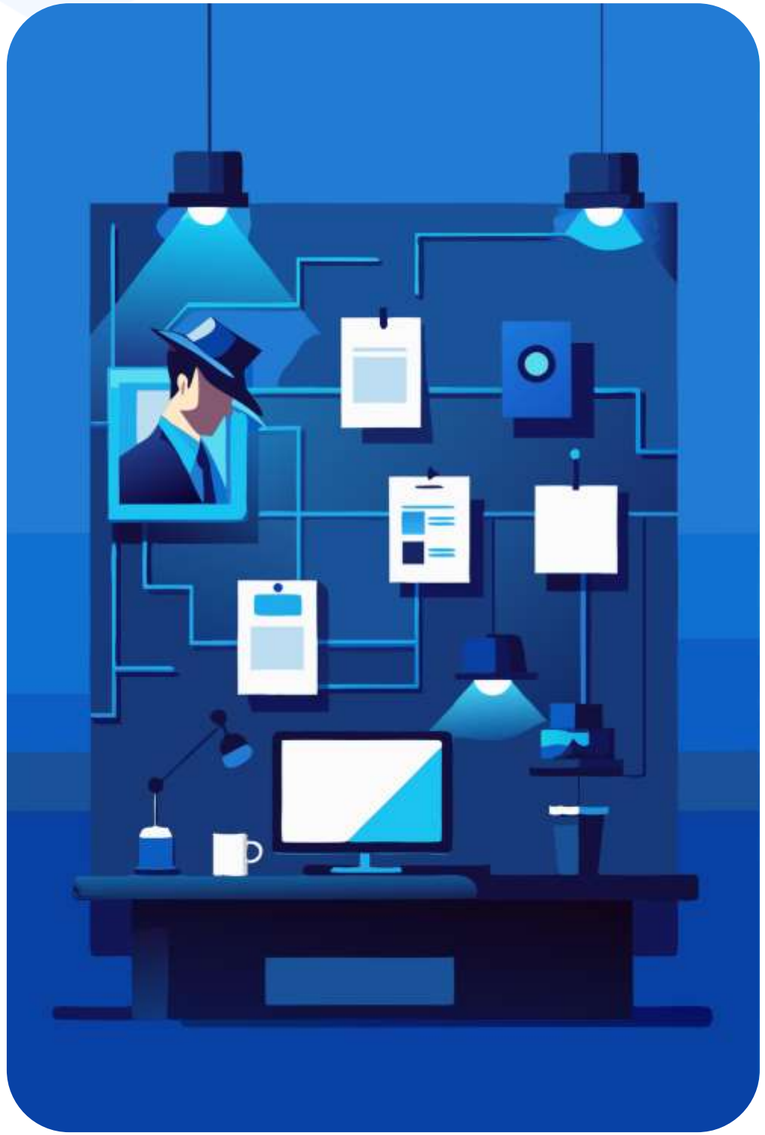
Security Information and Event Management (SIEM)

- It is a term for software products and services combining security information management (SIM) and security event management (SEM).
- This technology provides real-time analysis of security alerts generated by network hardware and applications.

The SIEM system

Security information management (SIM) + Security event management (SEM) = **SIEM**

SIEM Process



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

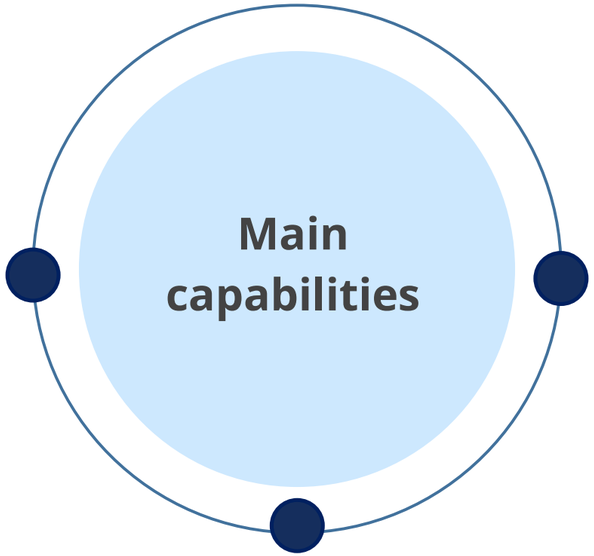
Normalize and aggregate the collected data

Analyze the data and identify the threats

Pinpoint security breaches and enable organizations to investigate the alerts

SIEM Capabilities

Threat detection:
Identifies threats in real-time for quicker responses



Incident investigation:
Uses threat intelligence for faster investigations

Mean time to respond (MTTR):
Shortens response times by streamlining data analysis

SIEM Functionalities

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

Reporting

Provides tools to visualize data and events within the environment

Real-time monitoring

Offers real-time monitoring and threat detection across the infrastructure, enabling rapid responses to data breaches

Continuous Monitoring

The security architect must design and implement a continuous monitoring program that protects the organization's critical information assets.

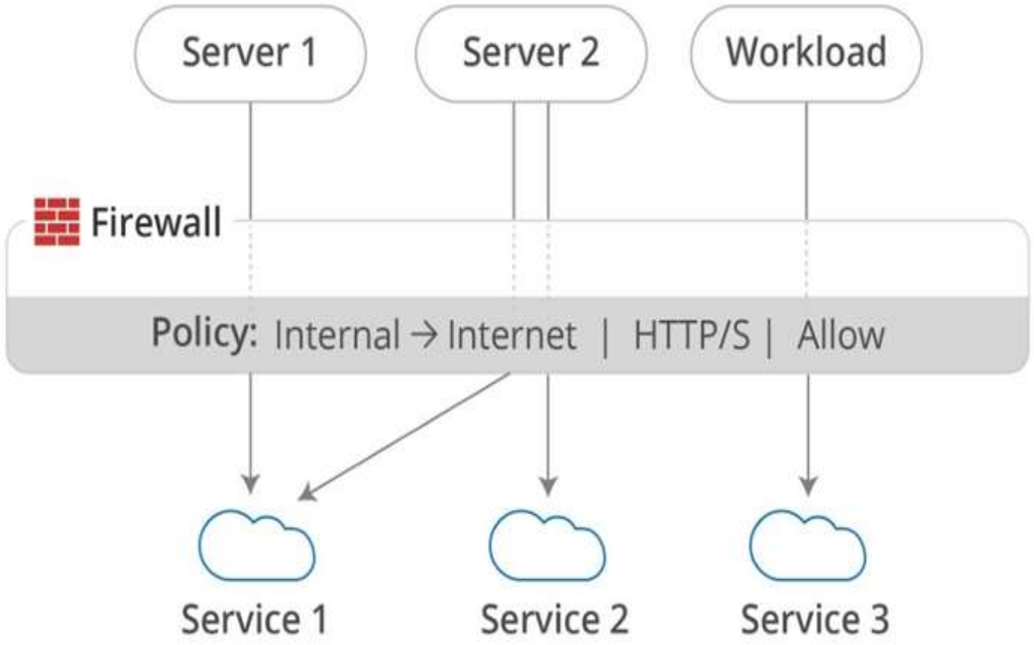
The security practitioner must be familiar with continuous monitoring as a service (CMaaS), offered by agencies such as the General Services Administration (GSA) and the Federal Acquisition Service (FAS).

Egress Filtering

It prevents any unauthorized or malicious traffic from leaving the internal network.

Information flowing from the internal network to the internet is monitored and controlled.

TCP/IP packets leaving the internal network are examined by a router, firewall, or similar edge device.



Example

Payment card industry data security standard (PCI DSS) requires egress filtering from any server in the cardholder environment.

Data Loss or Leak Prevention (DLP)

It helps an organization prevent the loss of its sensitive data.

Data Loss or Leak Prevention (DLP)

Objectives

- Locating and cataloging critical information stored throughout the enterprise
- Monitoring and controlling the sensitive information flow across enterprise networks and end-user systems

Benefits

- Protects sensitive data and intellectual property of an organization
- Meets compliance requirements
- Reduces security breaches

Threat Intelligence

It is the process of planning, collecting, processing, analyzing, and disseminating information that poses a threat to an organization and the application of this knowledge in mitigating the threat.

It collects real-time information from various internal and external sources to identify threats.

It processes threat data to understand attackers, respond faster to incidents, and anticipate their next move.

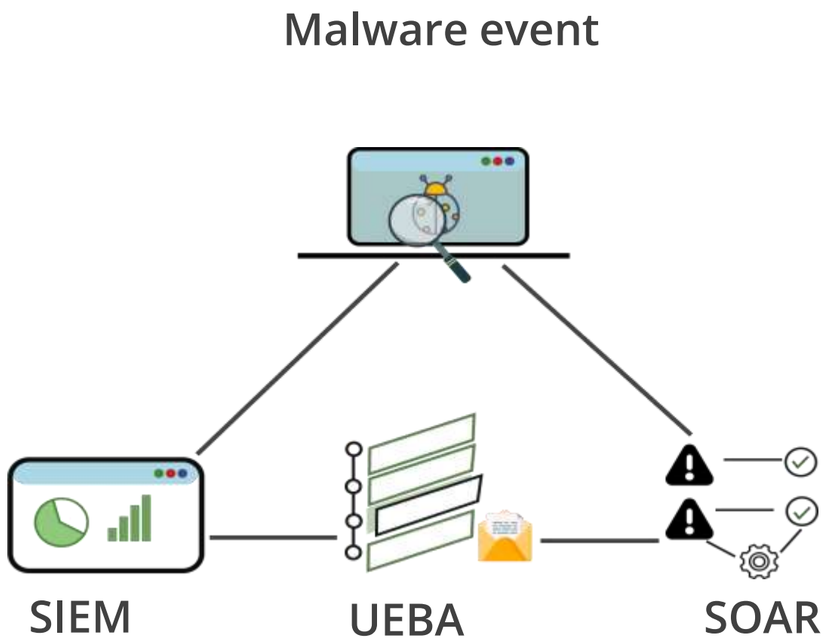
Threat Intelligence

Cyber threat intelligence sources include:

- Open-source intelligence
- Social media intelligence
- Human intelligence
- Technical intelligence
- Intelligence from the deep and dark web

User and Entity Behavior Analytics (UEBA)

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



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

User and Entity Behavior Analytics (UEBA)

UEBA analyzes the following:

User	It can monitor user behavior for any peculiar or suspicious behavior.
Entity	It can track other entities besides users, such as routers, servers, applications, or even IoT devices.
Behavior	It establishes baseline of normal behavioral profiles and patterns and 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 and accurate threat and anomaly detection.

Quick Check

Your organization uses a SIEM tool to monitor its network. During a routine check, you find a series of alerts indicating unusual traffic patterns. What, according to you, will be the first step in handling these alerts?

A. Dismiss the alerts if no complaints have been made

B. Immediately escalate to management

C. Analyze the alerts to identify the source and nature of the traffic

D. Block the traffic until further analysis is complete

Information Technology Infrastructure Library (ITIL) Processes in Security Operations

Introduction to ITIL Process

It is a widely used best practice for IT service management, particularly in security operations centers (SOCs).

It delivers structure, efficiency, and strategic alignment in managing security threats, focusing on incident, problem, change, and service level management.

Change Management

It refers to the process of tracking, approving, and controlling changes to a system through established change control procedures.

It includes identifying, controlling, and auditing all changes made to the system.

Change control:

- Ensures the implementation of change in an orderly manner through formalized testing
- Provides awareness regarding the impending change among users
- Analyzes the effect of the change on the system after implementation
- Reduces the negative impact of the change on the computing services and resources

Change Control Process

The procedures for change implementation and support are:

1. Requesting for a change introduction
2. Approving change
3. Cataloging intended change
4. Testing change
5. Scheduling and implementing change
6. Reporting to the appropriate parties about the change

Change Types

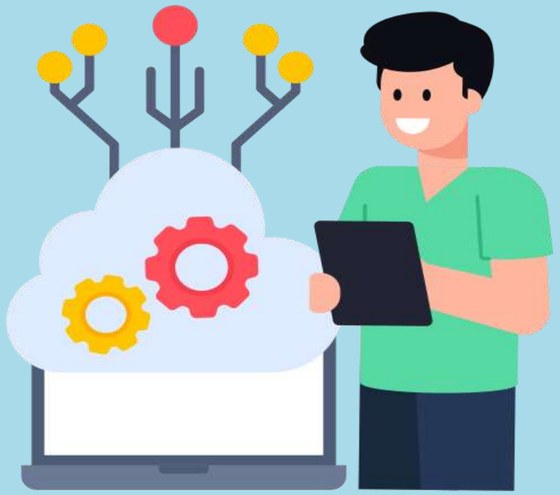
According to ITIL, the following are its types:

Standard change	A pre-authorized change that is low-risk and low-impact, well-understood, fully documented, and can be implemented without requiring additional authorization
Normal change	A change that should follow the change process to ensure that all changes, both minor (low to medium impact) and major (high impact), are scheduled, assessed, and authorized according to a standard procedure
Emergency change	A high-impact and urgent change that must be implemented immediately, bypassing strict adherence to the standard process

Configuration Management (CM)

It is the systematic process of tracking and maintaining detailed information about IT components within an organization.

It ensures that they are set up correctly and that changes are made consistently, including settings, software, and version levels.



Change management defines the reasons for changes, while configuration management details what those changes involve.

Configuration Management

The following are its four key functions:

Defining the desired state

•It establishes the ideal configuration, including installed software, configured settings, and present files.

Tracking the actual state

•It maintains an accurate record of installed and configured IT components.

Enforcing the desired state

•It uses CM tools to restore compliance when actual configurations deviate from the desired state.

Auditing and reporting

•It utilizes CM tools to track system changes and generate compliance report.

Configuration Management

It applies technical and administrative directions to:

Identify and document the functional and physical characteristics of each configuration item

Report the status of change processing and implementation

Manage changes

Patch Management

It is the process of applying proper patches to a system at a specified time using a strategy and plan.

A patch is a piece of software designed to fix problems and update a computer program.

This includes:

- Fixing security vulnerabilities and bugs
- Improving usability and performance

Patch

Types of Patches

Hotfixes

They are small targeted updates that alter the behavior of installed applications in a limited manner.

Service packs

They are comprehensive packages containing all hotfixes and critical updates for improved system stability.

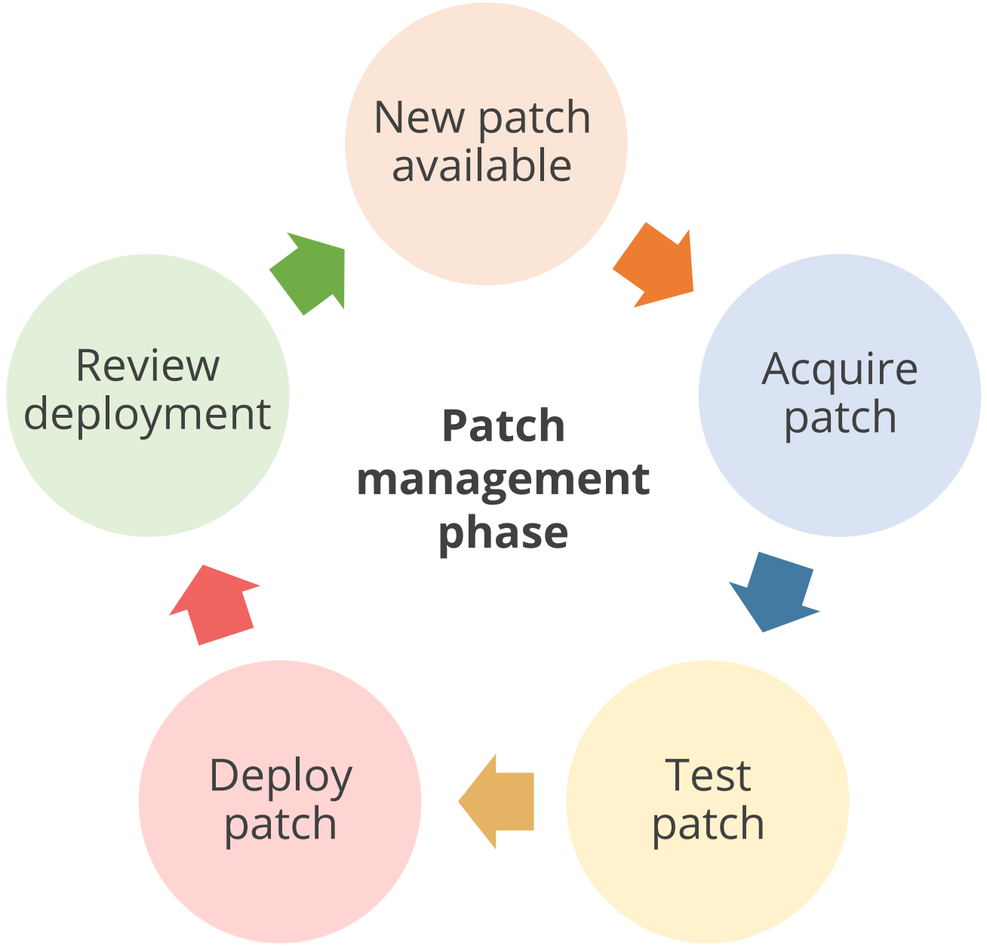
Updates

They address noncritical, non-security-related bug issues and fix specific problems.

Patch Management Activities and Cycle

The activities involve:

- Scheduling and prioritizing patches
- Testing patches
- Tracking change
- Installing and deploying patches
- Auditing and assessment
- Ensuring compliance



Vulnerability Management

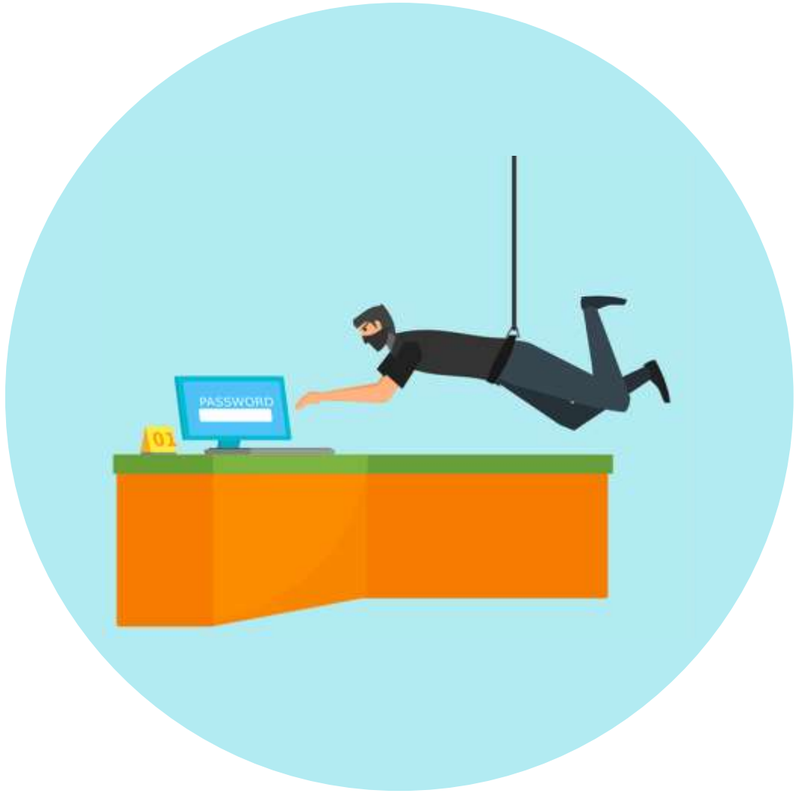
It is the process of identifying, assessing, and mitigating weaknesses in an organization's systems and networks to defend against potential attacks.

It includes:

- Flaws
- System misconfigurations
- Policy failures

Example

Buffer overflow and unpatched system



Given the rising number of cyber threats, understanding these vulnerabilities is crucial for strengthening defenses.

Vulnerability Management

Vulnerabilities can be addressed through various methods:

- Deploying a new code
- Changing hardware
- Applying security patches
- Reconfiguring systems

Real-World Scenario

Equifax data breach

Equifax Inc., an American multinational consumer credit reporting agency, suffered a data breach between May and July 2017 that affected at least 147 million individuals. The leaked data included sensitive PII, social security numbers, birth dates, addresses, and driver's license numbers.

An investigation revealed that Equifax had failed to:

- Implement a policy to ensure that security vulnerabilities were patched
- Failed to segment its database servers to block access to other parts of the network once one database was breached
- Failed to install robust intrusion detection protections for its legacy databases

Real-World Scenario

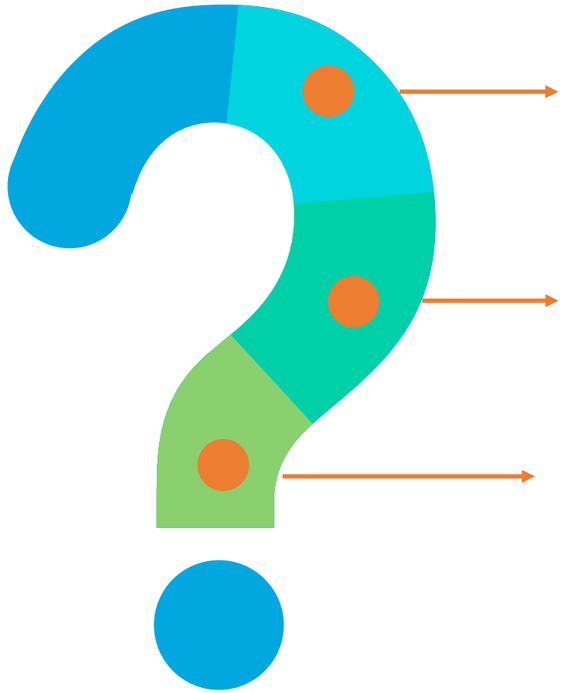
Equifax data breach

Following the massive data breach:

- Equifax’s CIO, CSO, and CEO resigned, highlighting the severity of the incident.
- The company agreed to pay a minimum of $575 million, with the potential to reach up to $700 million, as part of a global settlement.
- The company was mandated to implement a comprehensive information security program to prevent future breaches and protect sensitive data.

Real-World Scenario

How did the Equifax breach happen?



On March 9, 2017, Equifax was made aware of a critical vulnerability in the Apache Struts web framework, but the company failed to apply the patch even after two months.

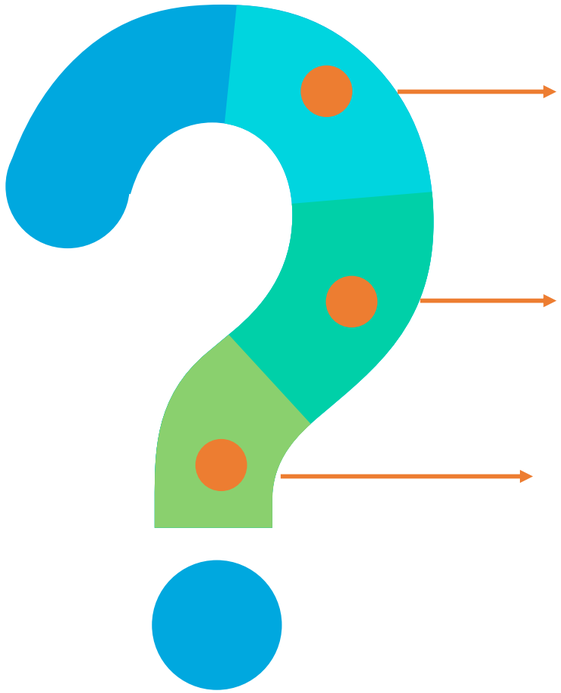
They were initially hacked via an unpatched server housing Equifax's online dispute portal.

After gaining the ability to issue system-level commands on the online dispute portal, the attackers accessed the additional databases as these systems were not isolated or segmented from each other.

The Apache Struts web framework is a commonly used, open-source software suite for developing web applications.

Real-World Scenario

How did the Equifax breach happen?



The attackers gained access to a database that contained unencrypted credentials which allowed them to access other databases containing PII.

They stole data over an encrypted connection and were undetected for months as Equifax had failed to renew the digital certificate of their network detection tool.

Equifax discovered the breach on July 29, 2017, but they didn’t alert the public until September.

Quick Check

A development team is planning to deploy new updates to an existing production system. Which of the following is the most effective in preventing weakness from being introduced into existing production systems?

A. Patch management

B. Configuration management

C. Change management

D. Security baseline

Overview of Incident Management

Incident Management

It is essential for preventing any disruption and minimizing damage and consists of the following components:

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

Any practice of detecting a problem, determining its cause, minimizing the damage, resolving the issue, and documenting each step for future reference

Incident Response Goals

Reduce the potential impact to the organization

Provide management with sufficient information

Deter attacks through investigation and prosecution

Maintain or restore business continuity

Defend against future attacks

Incident Response Team

It is s a group of people who prepare for and respond to emergencies.

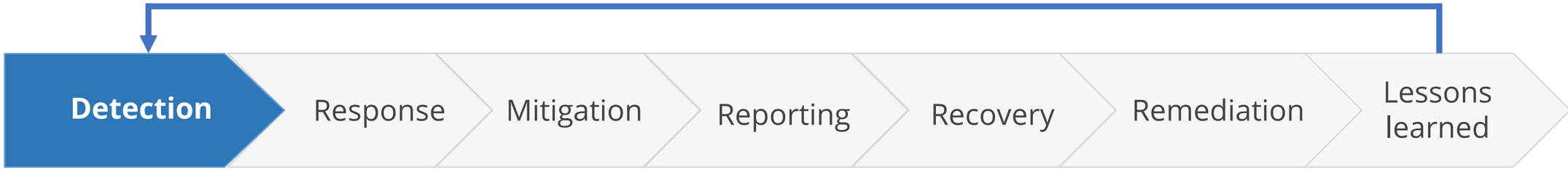
Incidence response checklist:

- A list of outside agencies and resources to contact or report
- 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

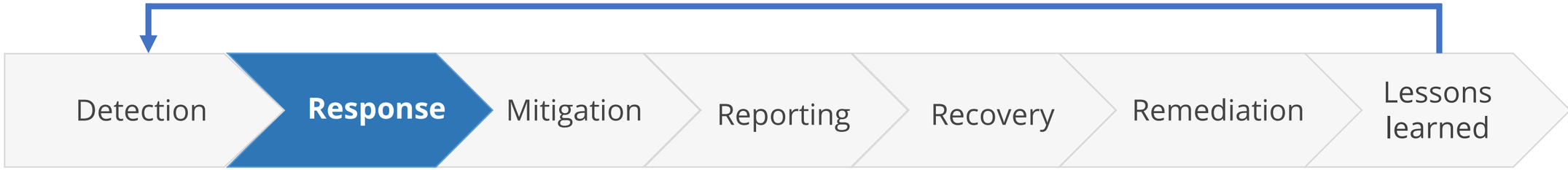
1. Establish incident response policy and procedures
2. Define handling methodologies
3. Create communication plan for internal and external parties
4. Develop call tree and notification processes for solutions, products, and support teams
5. Perform regular skill development, improvement, and training for information security staff
6. Conduct planned tests and team drills
7. Collect threat and vulnerability intelligence

Incident Response Life Cycle



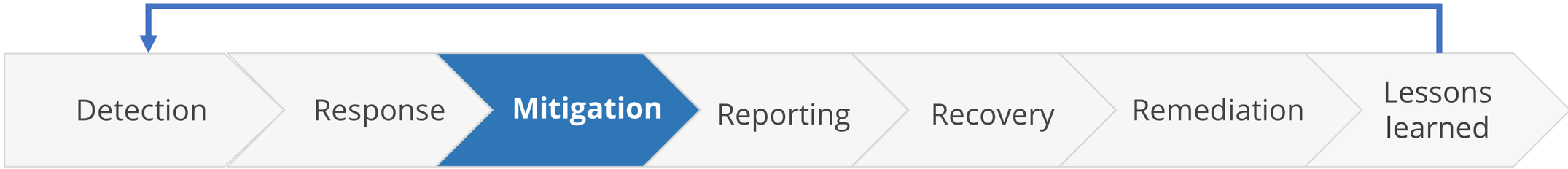
- **Automated detection capabilities** include network-based and host-based IDPSs, antivirus software, and log analyzers.
- **Manual detection** includes problems reported by end users.

Incident Response Life Cycle



- The triage process ensures that only valid alerts are promoted to **investigation or incident** status; false positives or incorrect alerts are identified and removed.
- Information is collected to investigate its severity and set priorities for addressing the incident.
- Incidents are categorized according to their severity level, potential risk, source (internal or external), rate of growth, and ability to contain the damage.
- More data is gathered to determine the root cause of the incident.

Incident Response Life Cycle



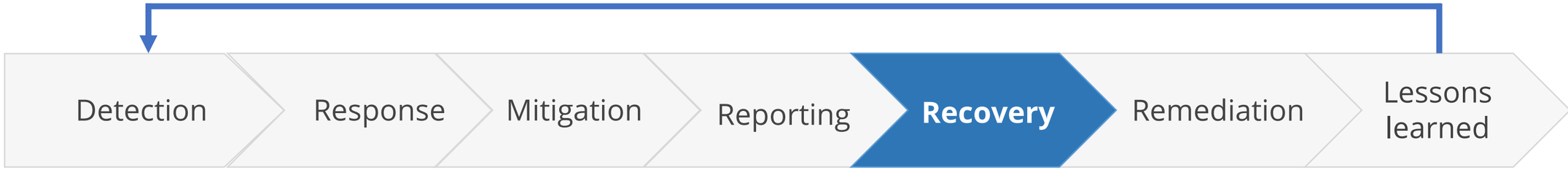
- Its goal is to prevent or minimize any further loss or damage from the incident so that recovery and remediation can begin.
- It prioritizes the most critical assets first, followed by less important assets.
- It utilizes isolation and containment to limit exposure and prevent further damage to the organization.
- It ensures that the response team takes its last forensic samples before commencing mitigation activities.

Incident Response Life Cycle

To handle and resolve incidents in a timely manner, the incident response team must document:

- The current status of the incident (new, in progress, forwarded for investigation, or resolved)
- Summary of the incident
- Related incidents
- Actions performed
- Chain of custody (if applicable)
- Impact assessment report
- List of evidence gathered
- Comments of incident handlers
- Next actions

Incident Response Life Cycle

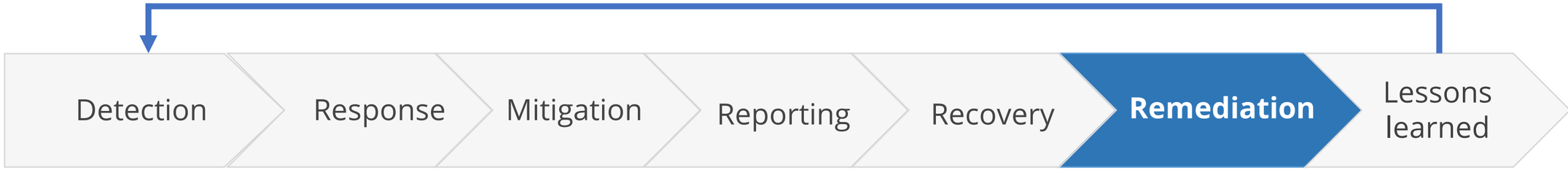


It is the process of restoring a system to its pre-incident condition.

Recovery and repair activities include:

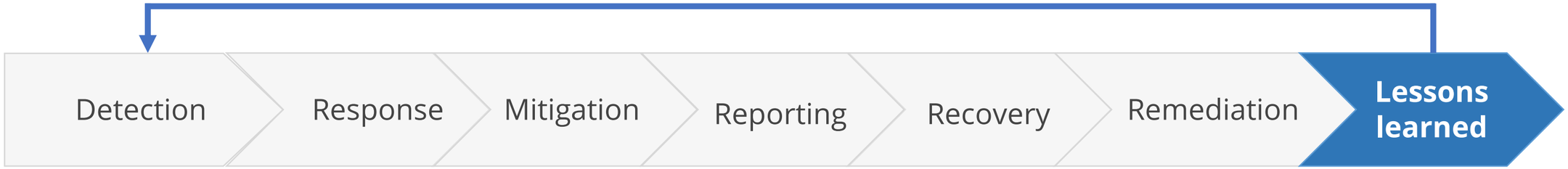
- Repairing or replacing hardware
- Reinstalling or reconfiguring operating system or application software
- Removing unwanted programs and data
- Restoring damaged or missing data from the backup media

Incident Response Life Cycle



- It is the post-incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the incident has been contained.
- It involves measures to ensure that the particular attack will never again be successful against the organization.

Incident Response Life Cycle



- This final stage is often skipped as the business moves back into normal operations but it’s critical to look back and heed the lessons learned.
- Holding a **lessons learned meeting** with all involved parties after a major incident, and periodically after lesser incidents as resources permit, allows for closure by reviewing what occurred, the intervention steps taken, and the effectiveness of those interventions.
- A follow-up report for each incident provides a reference that can be used to assist in handling similar incidents in the future.

Quick Check

After a cybersecurity incident, the response team holds a meeting to reflect on the event. What is their primary goal during this post-incident review?

A. To preserve forensic evidence

B. To improve the response process

C. To ensure the incident is properly documented

D. To train the incident response team

Overview of Problem Management

Problem Management

It is a systematic approach to identifying and resolving the root causes of IT service disruptions, focusing on:

- Minimizing the impact
- Enhancing service quality
- Reducing costs

Problem Management Process

Problem identification
Identifies potential problems through recurring incidents, trends in reports, and user complaints

Problem analysis
Investigates the root cause by gathering data, interviewing users, and analyzing logs

Problem resolution
Develops and implements a solution, which may include changes to IT systems and processes

Problem closure
Documents the problem, solution, and lessons learned to prevent similar issues

Continuous improvement
Reviews the problem management process regularly to implement necessary improvements

Configuration Automation and Baseline

Baseline

It is a predefined set of configurations and best practices meticulously designed to create a resilient and secure foundation for computing resources.

It provides a reliable starting point to harden systems against potential vulnerabilities.

It serves as a defined standard for an approved configuration or state, acting as a benchmark for comparing the current system state.

Baseline

Key benefits of implementing security baseline include:

Maintained consistency

Controlled costs

Improved security

Compliance

Types of Baselines

Infrastructure baseline

Represents a snapshot of infrastructure configuration, including virtual machines, storage buckets, networking settings, and security policies

Security baseline

Outlines minimum security requirements for resources, aiding in the identification and mitigation of security risks while ensuring compliance with regulations

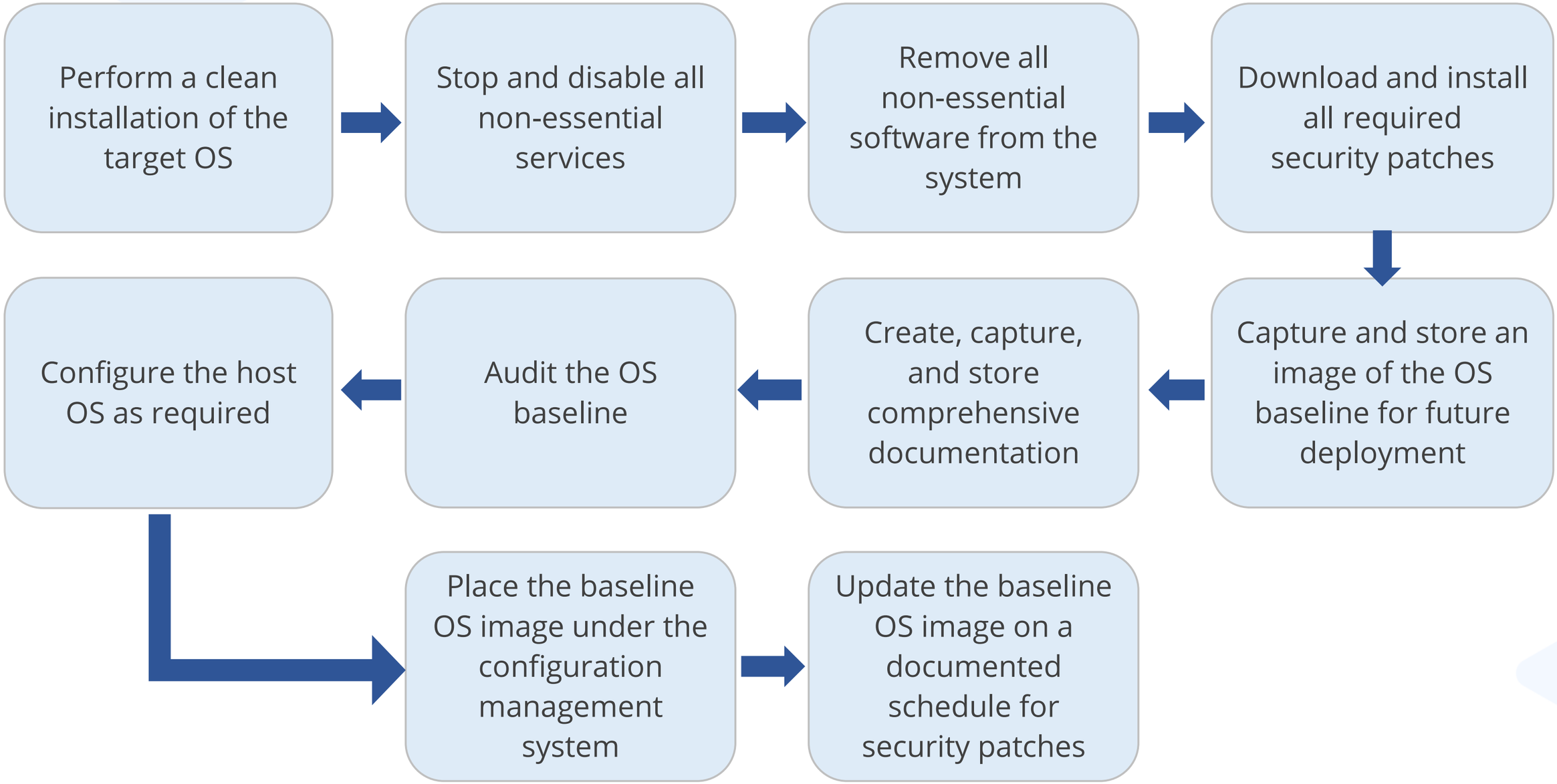
Performance baseline

Assesses typical performance levels of applications and infrastructure, identifying performance bottlenecks, tracking trends, and measuring the impact of changes

Network baseline

Provides a snapshot of normal network operating conditions, including configuration, performance metrics, and traffic patterns

Baseline Process



Infrastructure as a Code (IaC)

It is a method of managing and provisioning IT infrastructure through machine-readable code files, instead of manual configuration or graphical interfaces.

- It utilizes code to define and automate the creation, configuration, and management of infrastructure resources.
- It eliminates the need for manual configuration of servers and network devices.

Infrastructure as a Code (IaC)

The following are its benefits:

- Eliminates manual tasks, improving efficiency
- Ensures consistent provisioning across environments
- Integrates with version control systems for tracking changes and collaboration
- Allows easy scaling based on demand
- Enables the creation of identical environments for testing and development

Infrastructure as a Code: Components

Code files:
They are written in languages such as Terraform, Ansible, or Chef.

Version control system:
It tracks changes and manages different versions of configurations.

Provisioning tools:
They interpret the code and interact with cloud providers or on-premises infrastructure.

Infrastructure as a Code: Use Cases

Cloud deployments:

Spin-up resources on cloud platforms like AWS, Azure, or GCP

DevOps pipelines:

Automate infrastructure provisioning and management within CI/CD pipelines

Bare-metal deployments:

Manage on-premises servers and network devices

Disaster recovery:

Rapidly rebuild infrastructure in case of outages

Configuration Automation

It involves automating the deployment and configuration of applications, servers, middleware, databases, and other IT infrastructure for both on-premises and cloud data center environments.

Benefits:

- Increases operational efficiency
- Enforces compliance policies and reduces risks
- Prevents data center outages caused by configuration drifts
- Establishes best practices to change life cycle management

Automation and Scripting

Automation

- Refers to the use of technology to perform tasks with minimal human intervention
- Encompasses a range of technologies, from simple scripts to complex software programs and robotic systems

Scripting

- Represents a specific type of automation that utilizes programming languages
- Enables the automation of tasks within a computer operating system or application
- Consists of sets of instructions executed step-by-step by the computer

Automation: Use Cases

User provisioning

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

Resource provisioning

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

Establishing guard rails

Ensures systems and resources operate within specified parameters to reduce misconfigurations

Security groups management

Defines who can access specific resources or services

Automation: Use Cases

Ticket creation

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

Service and access management

Automates the enabling or disabling of services and access within systems

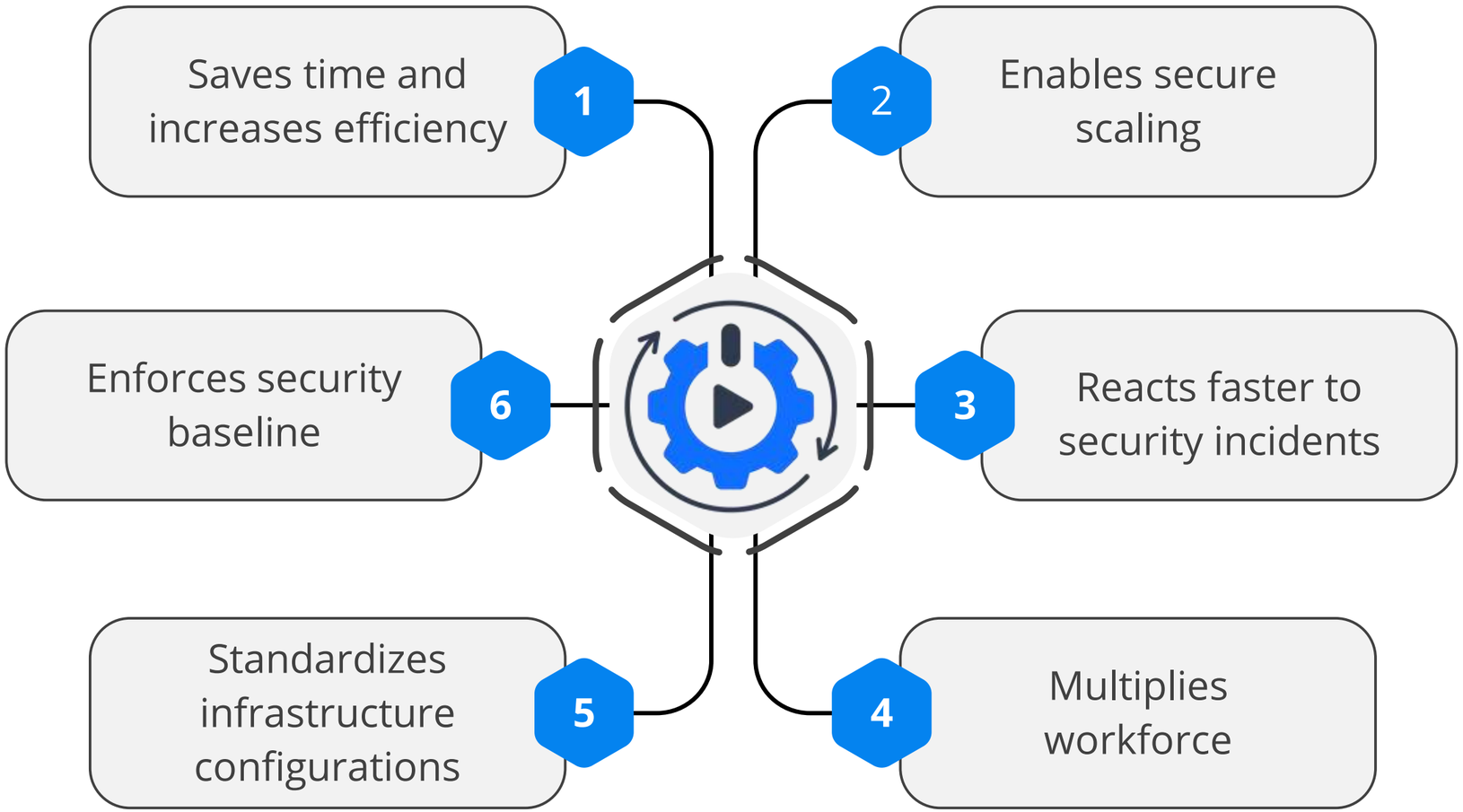
Escalation

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

Integration

APIs link together tools and systems for streamlined automation and complex process management

Automation: Benefits



Applying Foundational Security Operation Concepts

Controls for Protecting Assets: Administrative Controls

These controls help safeguard an organization’s assets and ensure they are compliant.

The controls include:

Personnel security

Ensures quality levels of the personnel by performing employment screening or background checks

Mandatory verification

Detects evidence of fraud

Separation of duties and responsibilities

Divides the security-sensitive tasks into various parts and assigns them to several individuals

Controls for Protecting Assets: Administrative Controls

Least privilege	Need to know	Change control	Record retention and documentation control
Restricts the set of privileges	Provides minimum information to perform an assigned task	Protects a system from unauthorized changes	Administers security controls on documentation and procedures

Identity and Access Management

Identity management

It controls the life cycle of every account in a system, from the provisioning of the account to its eventual removal from the system.

Access management

It refers to the assignment of rights or privileges to accounts, which will allow them to perform the intended function.

Identity and access management (IAM) solutions focus on harmonizing the user provisions and access management across multiple systems with different native access control systems.

Types of User Accounts

A user account grants permission to access computer systems and applications based on the assigned role.

Privileged account

- Possesses extensive powers on a given system
- Includes four types of accounts with different levels of privilege: root or built-in administrator accounts, service accounts, administrator accounts, and power user accounts

Ordinary user account

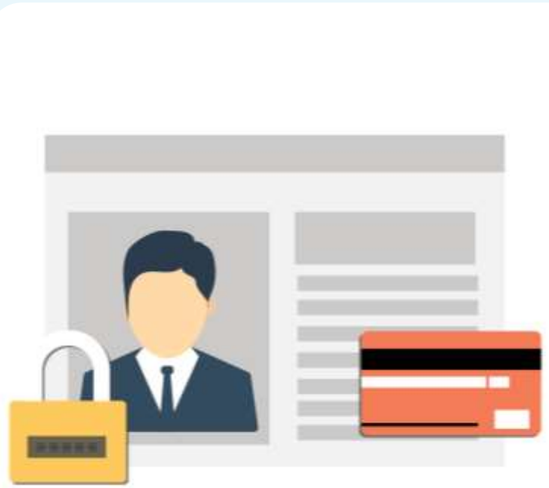
Assigns most users with access limited by following the principles of least privilege and need-to-know

Need for Controlling Privileged Accounts

Accounts with greater privileges are distinct from less privileged user accounts.

Some features of privileged accounts are:

- Have extensive powers on a given system
- If compromised, the attacker could damage the system
- Need regular monitoring as they can be misused
- Are controlled by security operations
- Require a defined procedure for handling privilege account



Monitoring Special Privileges

A security practitioner must validate and review the privileges granted to accounts to ensure:

- Only authorized users are granted access for a required period of time
- Access must only be granted based on user's clearances, thorough background checks, and the user's suitability for the role
- Inactive accounts are removed from the system based on the organization's policy

Quick Check

While reviewing the security system of your company, you identify several potential risks. Which of the following best defines a threat in the context of operations security?

A. It is a loophole that could be exploited in the system.

B. It is a company resource that could be lost due to an incident.

C. It is a likely incident that could cause damage.

D. It is the reduction of loss related to an incident.

Applying Resource Protection

Protecting Valuable Assets

Security operations should:

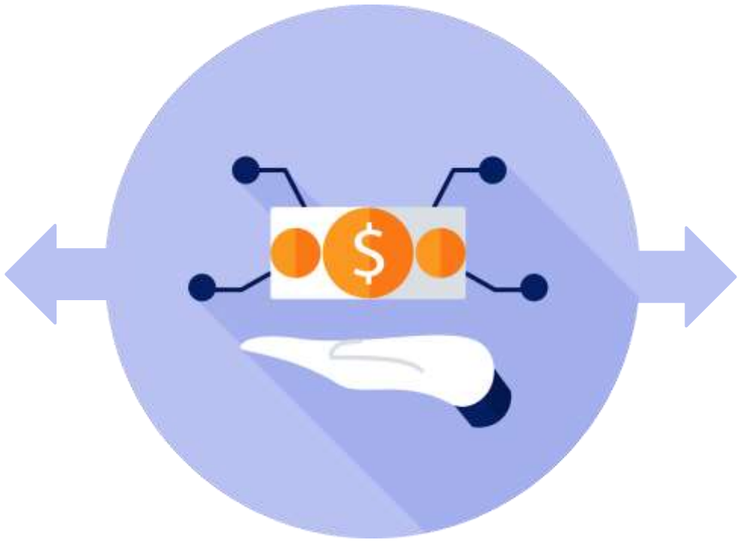
- Provide regular protection to human and material assets
- Maintain the security controls to protect sensitive or critical resources from being compromised

Assets can be:

Tangible	Intangible

Protecting Physical Assets

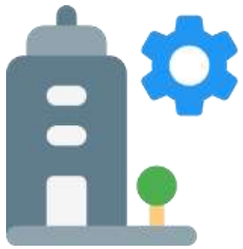
Security professional confirms asset ownership and security operations ensure the protection of physical assets.



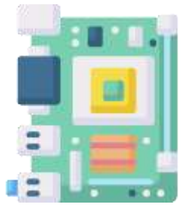
IT department plays the role of the owner as well as custodian of physical assets.

Protecting Physical Assets

The various types of physical assets are:



Facilities



Hardware

Software

Media

Protecting Information Assets

Information assets include all forms of information and types of intellectual properties and are hard to evaluate and delineate.

The important factors in protecting information assets are:

Information classification

Information labeling and handling

Access control

Accountability

Protecting Resources

It is the concept of protecting an organization’s computing resources and assets from loss.

Computing resources of an organization include any:

- Software
- Hardware
- Data owned

Protecting Resources

The resources that need protection are:

- **Hardware resources**: Routers, firewalls, switches, removable drives, file servers, workstations, disks, gateways, and printers
- **Software resources**: Program libraries, source code, vendor software, proprietary software, and operating system software
- **Data resources**: Backup data, user data files, password files, operating data directories, system logs, and audit trails

Hardware Controls for Protecting Assets

The hardware controls include:

Hardware maintenance

Investigating and escorting maintenance and service personnel as they have logical and physical access to the system

Account maintenance

Changing the default passwords and disabling accounts

Diagnostic port controls

Monitoring port usage by authorized personnel and blocking internal or external unauthorized access

Hardware physical controls

Securing the server room, data center, and media storage with locks and alarms

Software Controls for Protecting Assets

Some of the elements of controls on software are antivirus management, software testing, powerful system utilities, and safe software storage.

The software controls include:

Transaction controls

Controls all phases of a transaction

Change controls

Preserves data integrity in a system while changes are being made to the configuration

Test controls

Prevents confidentiality violation and ensures the integrity of a transaction

Backup controls

Allows users to back up their own data in a distributed environment

Media Controls for Protecting Assets

Record retention

- Refers to the duration for which transactions and other types of records, such as legal documents, audit trails, and emails, should be retained
- Done according to management, legal, and audit or tax compliance requirements

Data remanence

- Pertains to the data left on the media after the data has been erased

Object reuse or data remanence

- Refers to a security vulnerability that occurs when sensitive data persists on a storage device even after it has been deleted or overwritten
- Must be securely reassigned so that no residual data is available to the new subject through standard system mechanisms

Quick Check

You are responsible for securing a sensitive system within your organization. To reduce the risk of a single person compromising the system, which of the following best represents the principle of separation of duties?

A. Two operators are required to perform a task.

B. An operator only has the minimum required information about the system to do a job.

C. The operators perform different duties to prevent one person from compromising the system.

D. The duties of the operators are frequently rotated.

Operating Detective and Preventive Measures

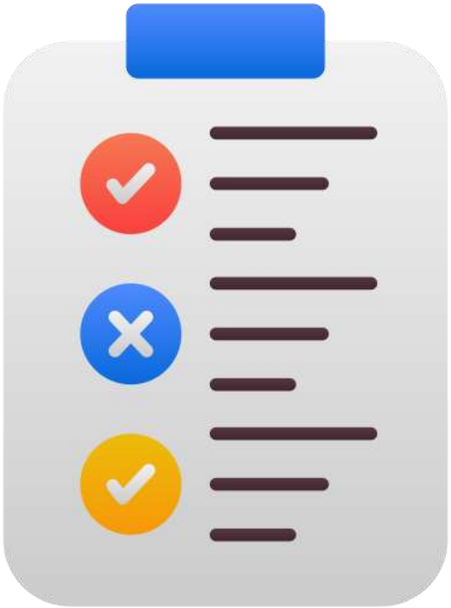
Firewalls

It monitors incoming and outgoing network traffic based on predefined security rules.

Network firewall	Purpose-built appliances for securing enterprise corporate networks
Web application firewall (WAF)	For protecting web applications and APIs from a variety of attacks, including automated (bots), injection, and application-layer denial of service (DoS)
Next generation firewall (NGFW)	Deep-packet inspection firewall that moves beyond port or protocol inspection and blocking, adding application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall

Application Allowlist

- It is a security measure used to restrict what software can run on a device or network.
- It allows only authorized applications to execute, blocking any not on the list.



Application allowlisting is also known as application control or **whitelisting**.

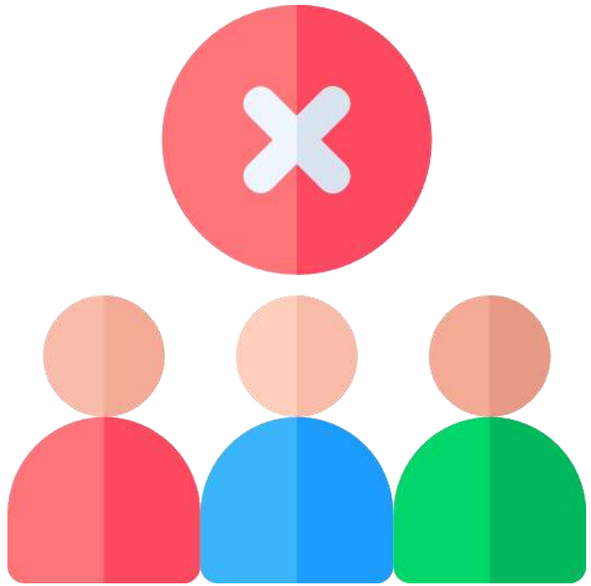
Allowlist: Attributes

- **Security**: Allows only trusted applications to run, preventing malware and other malicious software
- **Improved management**: Ensures only necessary software is installed and running, improving IT oversight
- **Implementation**: Utilizes security software or operating system settings to enforce application allowlisting

Application Blacklist

- It is a list of software programs that are prohibited from running on a computer system or network.
- It is a cybersecurity measure to block potentially harmful or unwanted applications.

Blacklist Attribute



- **Security focus**: Blocks known malware, including viruses, worms, and ransomware
- **Productivity boost**: Improves user productivity by limiting access to non-work-related programs
- **Management control**: Ensures compliance with security policies and software licenses

Third-Party Provided Security Services

Threat intelligence

Vulnerability assessment and penetration testing

Physical security

Network management

Audits and forensics

Sandboxing

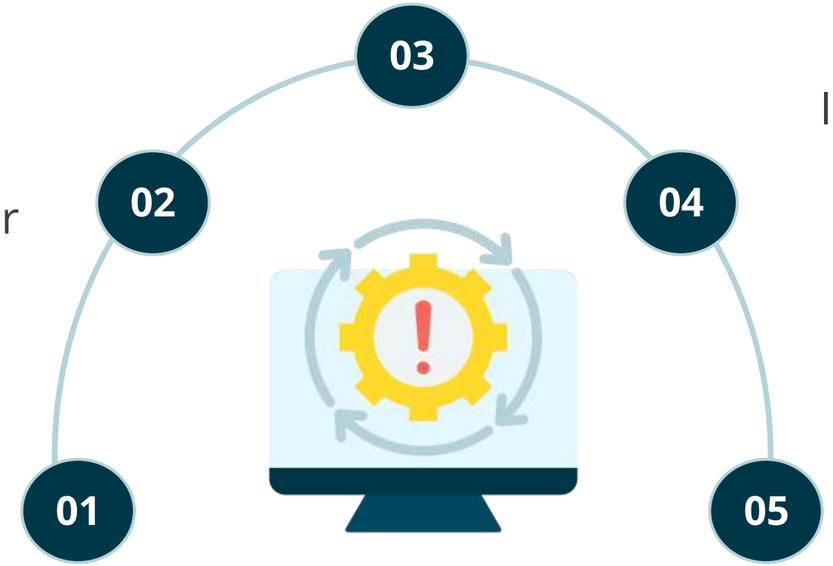
It is a technique used to safely evaluate the threat in an isolated test environment (sandbox).

- 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.
- It sends suspicious email attachments to a virtual sandbox for deep analysis of malicious activity.

Sandboxing: Flow

Analysis:
Analyzes the activity of the code inside the sandbox

Detonation:
Runs the suspicious code within the sandbox and closely monitors its behavior



Threat detection:
Identifies malicious activities such as attempts to steal data, install malware, or damage the system

Isolation:
Allows suspicious programs to execute without affecting the actual system or network

Protection:
Prevents any malicious code from entering the real system

Benefits of Sandboxing

Proactive defense

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

Safe analysis

Examines potentially risky code without putting the actual system or network at risk

Improved detection rates

Uncovers sophisticated malware that might bypass traditional security measures

Honeypot

It is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect, and study hacking attempts aimed at gaining unauthorized access to information systems.

Features of Honeypot

It is a decoy system intended to mimic likely targets for cyberattacks.

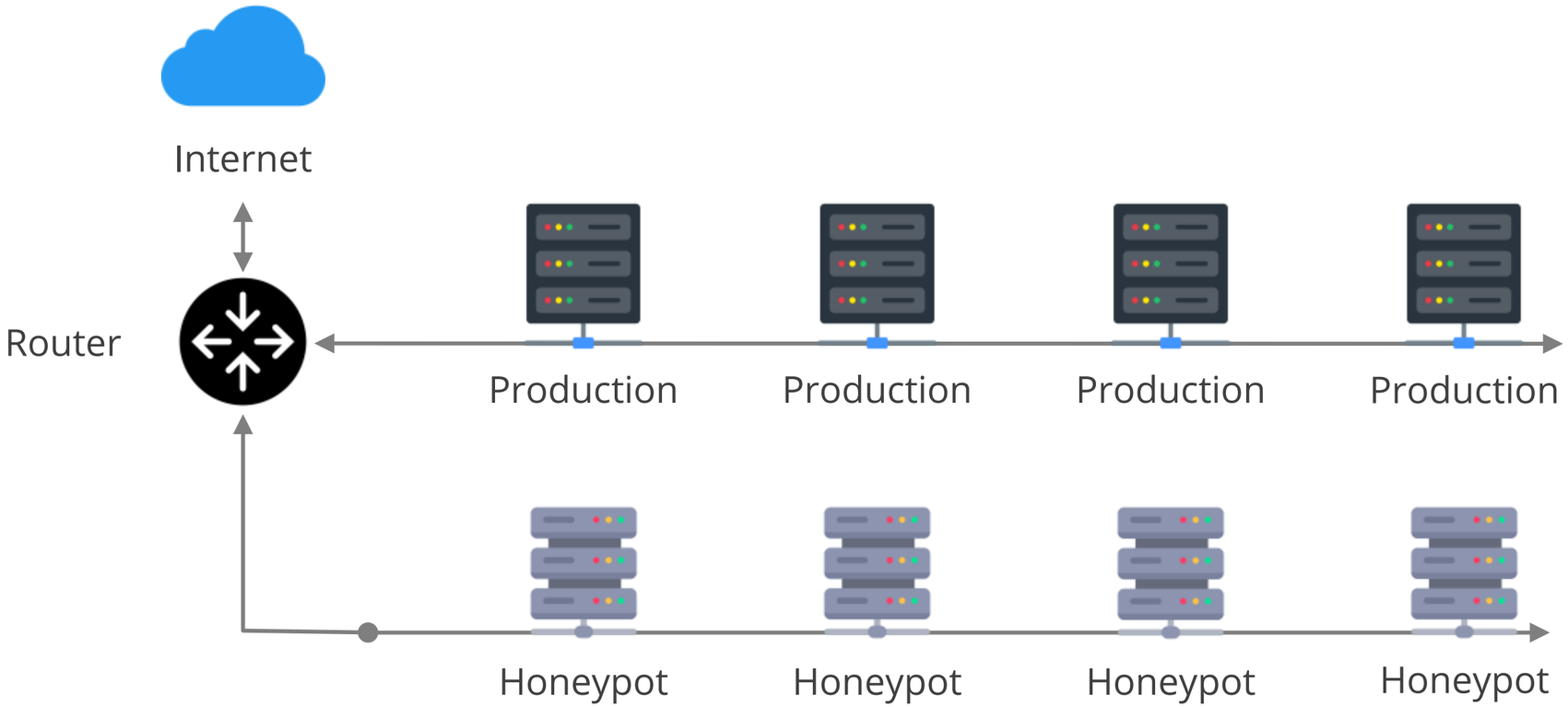
It is not hardened or locked down with enabled services and open ports.

It is designed to confuse attackers into believing it is a production server.

It does not contain any sensitive or valuable data.

Honeynet

It is a set of multiple honeypots linked together as a network or subnet that simulates a larger network installation.



Honeytokens

They are fictitious words or records added to legitimate databases to detect unauthorized attempts to access information.

Their characteristics make them appear as genuine data items.

Honey File

- They are not software applications or services, but decoy files used for security purposes.
- They are intentionally placed on a network file share to lure attackers trying to steal data.

Anti-Malware Systems

Malware has the capacity to disrupt the operation of user workstations as well as servers, which could result in:

- Loss of business information
- Disclosure or compromise of business information
- Corruption of business information
- Disruption of business information processing
- Inability to access business information
- Loss of productivity

Protection against malware can be achieved by applying defense-in-depth and installing central anti-malware management.

Anti-Malware Systems

- Assess the risk of exposure to malicious code or malware (viruses, worms, Trojan horses, and spyware)
- Respond by implementing anti-virus and anti-spyware controls

ML and AI for Cybersecurity

Artificial Intelligence (AI):

Engineering of computers to mimic human behavior

Machine Learning (ML):

Ability to learn without being explicitly programmed

Deep Learning:

Learning based on deep neural network that can learn and make intelligent decisions on its own

ML and AI for Cybersecurity

Automate tasks	Use machine learning to automate repetitive security tasks for higher levels of accuracy and in a fraction of the time
Threat hunting	Search for recurrent patterns, anomalous behavior, and other outliers
Application security	Automate code reviews with AI to help eliminate false negatives and false positives
Incident investigation	Investigate indicators of compromise and gain critical insights to accelerate threat response times
Incident response	Orchestrate and automate hundreds of time-consuming, repetitive, and complicated response actions that previously required significant human intervention

Real-World Scenario

Google tackles Gmail spam with machine learning:

Since its launch in 2004, Gmail has used ML techniques like neural networks to filter emails in its spam filters. Unlike rule-based filters, ML models adapt to changing conditions and identify patterns in unwanted emails that may elude human detection. Google's ML model reportedly achieves 99.9% accuracy in detecting and filtering spam, phishing emails, and malware.

In 2019, Google integrated TensorFlow in Gmail to try to block the last 0.1% of spam emails from getting through. TensorFlow is an open-source ML framework developed at Google in 2015.

TensorFlow's advantage is that it allows Gmail's team to refine its existing machine-learning algorithms to detect spam more accurately. With TensorFlow, Google can also better personalize its spam protection for each user. The same email could be considered spam to one person but important information to another.

Gmail has announced that with TensorFlow it can now detect 100 million more spam emails daily.

Quick Check

A security team when reviewing its intrusion detection system (IDS) after a recent cyberattack, realized that their IDS failed to detect the intrusion. What is this phenomenon called?

A. False positive

B. False negative

C. True positive

D. True negative

Implementing Recovery Strategies

Backup Methods

They ensure data integrity and network availability by protecting and restoring deleted, corrupted, or lost information.

Types of Backup

	Full backup	Differential backup	Incremental backup
Methodology	• Acts as the starting point for all other types of backups • Contains all data in backed up folders and files • Provides the ability to completely restore all backed-up files from a single full backup	• Contains all files that have changed since the last full backup, the latest full backup, and the latest differential backup	• Stores all files that have changed since the last full, differential, or incremental backup • Needs recent full backup as well as every incremental backup made since last full backup when restoring from an incremental backup
Backup speed	Slow	Medium	Fast
Restoration speed	Fast	Medium	Slow
Storage space required	High	Medium	Low

Develop a Recovery Strategy

A recovery strategy is a comprehensive plan for an organization to restore critical business operations after disruptions like cyberattacks, natural disasters, or system failures.

Below are the key components of a robust organizational recovery strategy:

Continuity planning	Predefined actions	Recovery time objective
Develop specific actions to minimize downtime	Enable quick and organized responses	Help minimize economic impact and operational disruption

Develop a Recovery Strategy

The key steps in the recovery strategy phase include:

Assessment of business impact	Identification of recovery options	Implementation planning
Understanding which business functions are critical and the potential impact of their loss	Evaluating various strategies such as data backup solutions, alternative site arrangements, and resource allocation	Developing detailed procedures and checklists to guide the recovery process

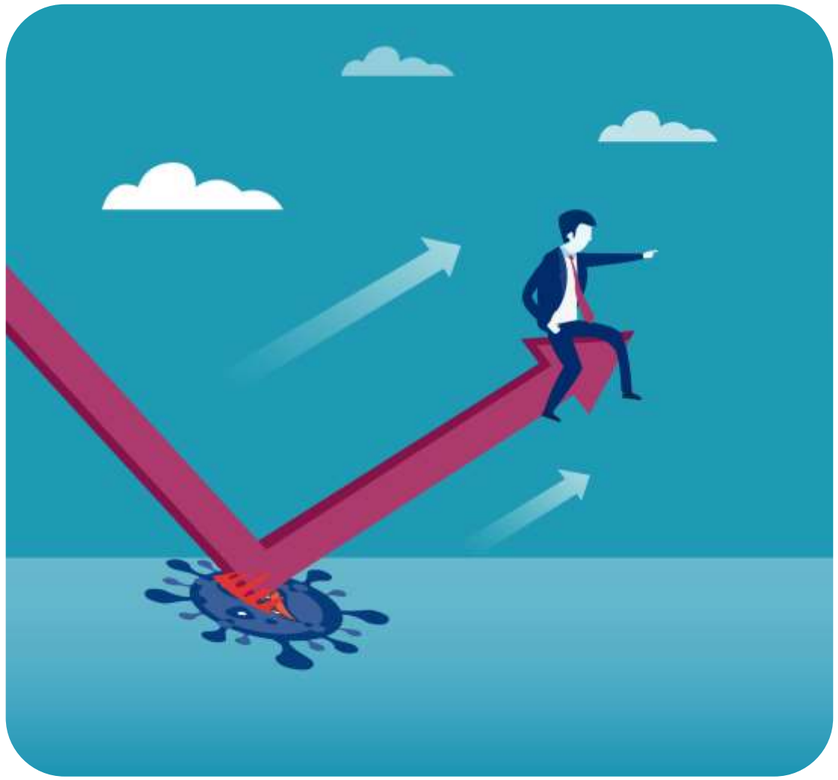
Develop a Recovery Strategy

The focus of the process should be on:

- Responding to the disaster
- Recovering critical functions
- Redeeming noncritical functions
- Salvaging and repairing hardware and software
- Returning to the primary site for operations

Types of Recoveries: Business Recovery

The identification of critical systems, data, equipment, materials, office space, and key business support personnel.



In the event of a disaster, major corporate applications and the related components would be restored first.

Types of Recoveries: Facility and Supply Recovery

It focuses on the main facility, remote sites, and needed equipment (networks, servers, telecommunication, HVAC systems, technical documents, required supplies, and the transportation of equipment and staff).

Types of Recoveries: User Recovery

It is the documentation of procedures for employees to follow during emergency situations. It includes:

Types of Recoveries: Operational Recovery

It determines alternative recovery locations based on MTD and acceptable costs.

It focuses on recovering the following data communication equipment:

- Mainframes
- Systems
- Servers
- LANs
- Peripherals
- Switches
- Routers

Types of Recoveries: Operational Recovery

Additional location options for recovery include:

- Reciprocal or mutual aid agreements
- Mobile sites
- Multiple processing centers
- Service bureaus
- Self-service
- Surviving sites
- Internal arrangements
- Work from home

Recovery Partner Strategies

Reciprocal agreements	• Mutual or bidirectional arrangements between two organizations where one organization can move its operations to the other during disasters • Also known as mutual aid agreements (MAAs)
Multiple processing centers	• Processing centers spread across different geographical locations • Handle the business's operational requirements during recovery
Service bureaus	• Recovery contracts with an offsite service bureau to have the site ready and available for organizations during emergencies • Offer expertise in processes, technology, and business-domains to customers

Backup Sites

They are the locations where businesses can be recovered in the event of a disaster at the primary site.

The different types available are:

- Mirror or redundant site
- Hot site
- Warm site
- Cold site
- Mobile site

Backup Sites: Mirror Site

It is a duplicate production of a system capable of seamlessly conducting IT operations without loss of services to the system’s end user. It is also called redundant site.

It is configured like the primary site and is the most expensive recovery option.

Example

Regulatory bodies have made it mandatory for commercial banks to have redundant sites.

Backup Sites: Hot Site

It is where an organization relocates its data center following a major disruption or disaster.

- It consists of servers, raised floors, power, utilities, fully configured computers, hardware, and critical applications' data mirrored in real time.
- It helps resume critical operations within a very short period.
- It can be internal (owned) or external (outsourced).

Backup Sites: Warm Site

It has hardware and connectivity but lacks the real-time data.

- It relies on backup data to rebuild a system after a disruption.
- It consists of raised floors, power, utilities, computer peripherals, and fully configured computers.
- It is less expensive, more flexible, and requires fewer resources for maintenance.
- It requires more time and resources to activate the site.

Backup Sites: Cold Site

It does not have data backups and immediately available hardware.

- Its configuration and restoration of critical IT services take more time.
- It has a raised floor, power, utilities, and physical security.
- It has no resources or geographic constraints.

Backup Sites: Mobile Site

It keeps the facility intact despite the data center being damaged.

- It is also called data centers on wheels.
- It has towable trailers that contain computer equipment as well as HVAC, fire suppression equipment, and physical security.

Importance of Maintaining Resilient Systems

Resilient systems ensure stability and continuity of operations in case of any service disruptions.

The mechanisms used for controlling the behavior of a system when it fails are:

- **Fail-safe mechanisms** that focus on failing with minimum harm to personnel
- **Fail-secure mechanisms** that focus on failing in a controlled manner to block access while the systems are in an inconsistent state

Fault Tolerance

It is the ability of a system to continue operating in the event of a failure and is provided by redundant items within a system.

In the event of component failure, the fault tolerant system can continue to operate through redundant power supplies.

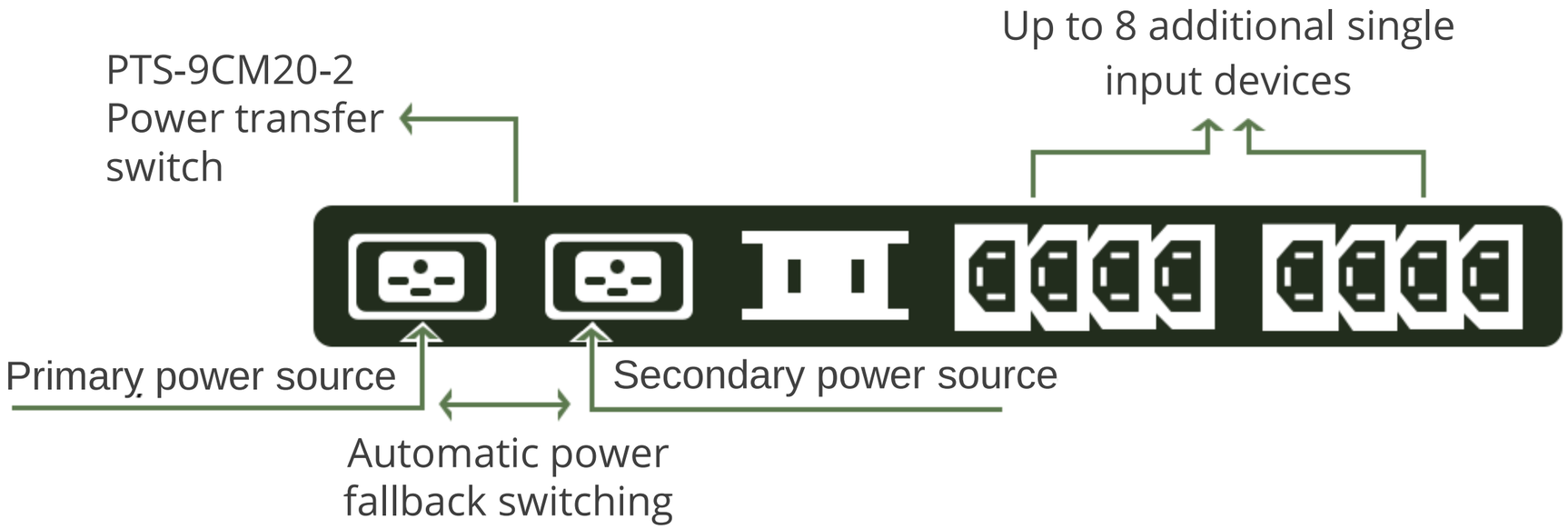
The usage of the spare components determines if it is a cold, warm, or hot spare.

Redundant Power Supplies

Also known as dual power supplies, these are common in systems where failures cannot be tolerated.

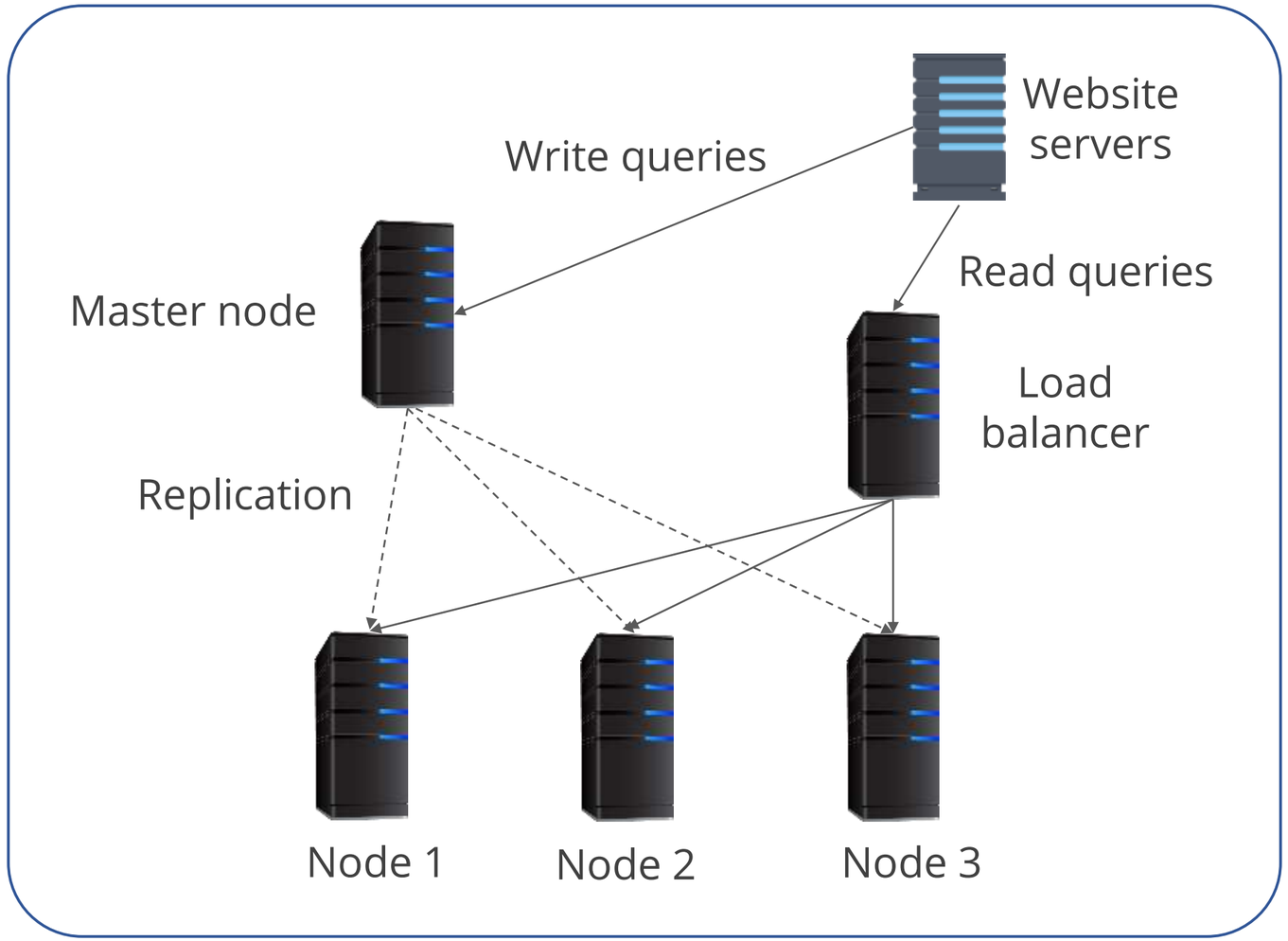
Example

Core network switches



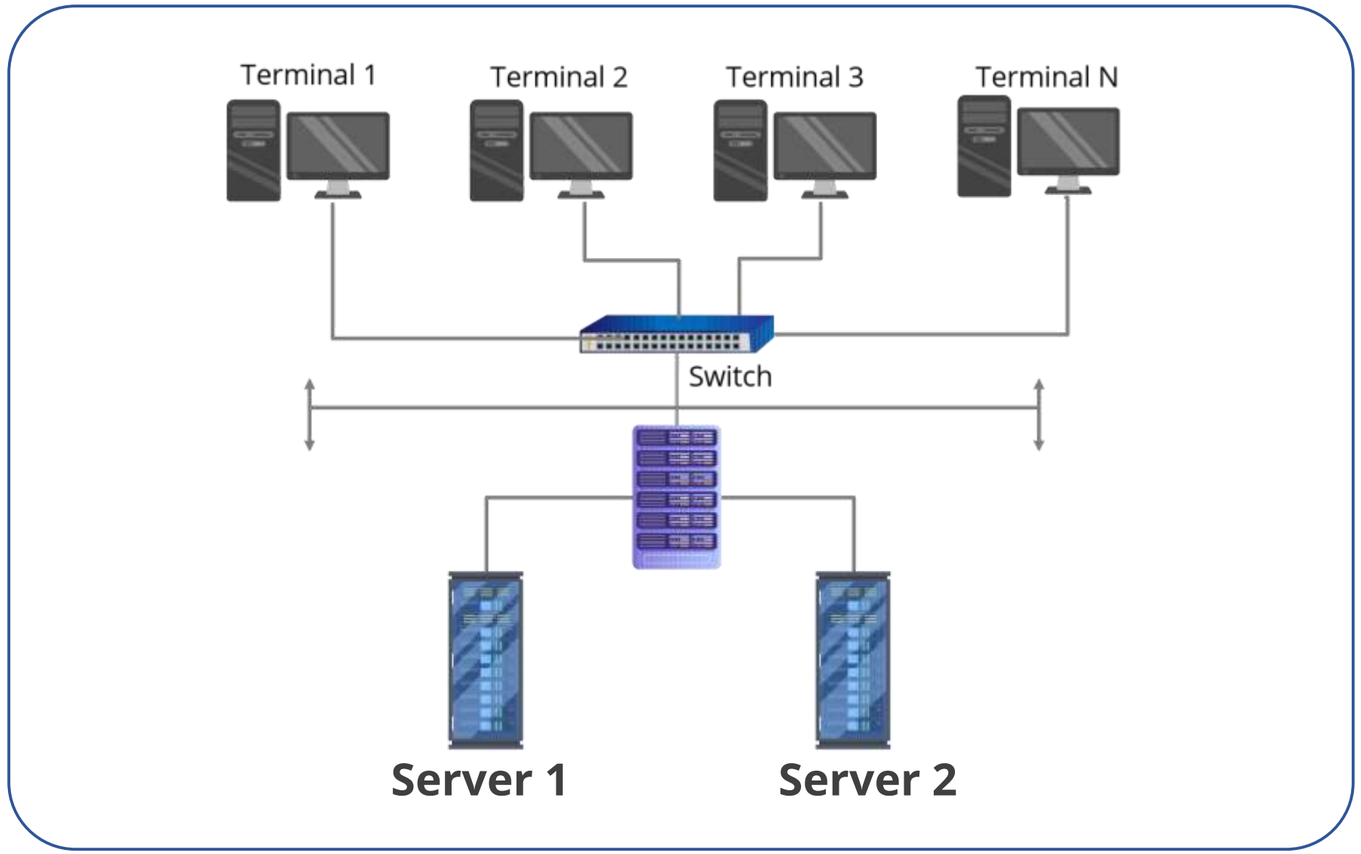
Replication

Data changes are transmitted to a counterpart storage system which is an adjunct to clustering and makes current data available to all cluster nodes.



Redundancy and Fault Tolerance Methods: Cluster

It refers to a group of two or more servers that function as a single logical server.



Cluster Modes

Clusters generally operate in active-active mode or active-passive mode.

Active-active mode

Both servers actively operate and service incoming requests.

Active-passive mode

- One (or more) server actively services requests and one (or more) server remains in a standby state to be able to switch immediately to active mode when the active server fails.
- A failover is an event in a server cluster running in active-passive mode.

A geographical cluster or geo-cluster system is a cluster that can be located anywhere.

Redundant Arrays of Inexpensive or Independent Disks (RAIDs)

It is a data storage technology that combines multiple hard drives into a single logical unit to improve performance and redundancy.

RAID 0: Striping

- Stripes data over many drives
- Does not provide redundancy or parity
- Renders all volumes unusable if one volume fails

RAID 1: Mirroring

- Writes data simultaneously on two drives
- Holds data in the other drive should one drive fail

RAID 3: Byte-level parity

- Holds parity data on one drive while stripes data over all drives
- Reconstructs failed drive from the parity drive

Redundant Arrays of Inexpensive or Independent Disks (RAIDs)

RAID 4: Striped set

- Stripes data at the block level and has dedicated parity or block level

RAID 5: Interleave parity

- Ensures that there is no single point of failure
- Writes data along with parity on all drives

RAID 6: Second or double-parity data

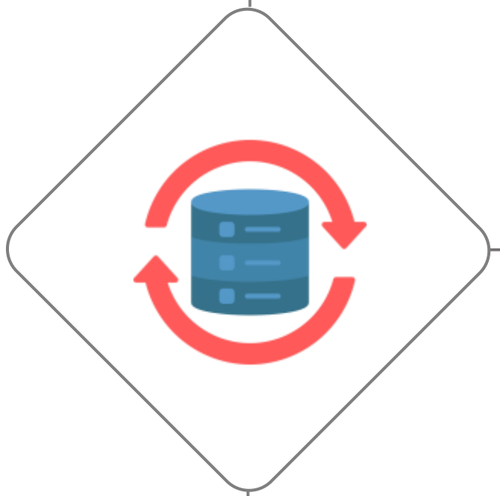
- Has more fault tolerance than level 5 with a second set of parity data written on all drives

RAID 10: Striping and mirroring

- Supports multiple disk failures by simultaneously mirroring and striping data across several drives

Backup and Recovery Concepts

In software and data recovery, data recovery is the prime focus. To create a level of fault tolerance and redundancy, the following concepts are used:



Database shadowing

Writes or duplicates database information simultaneously to another server

Electronic vaulting

Copies the backup data in a batch process to an offsite location

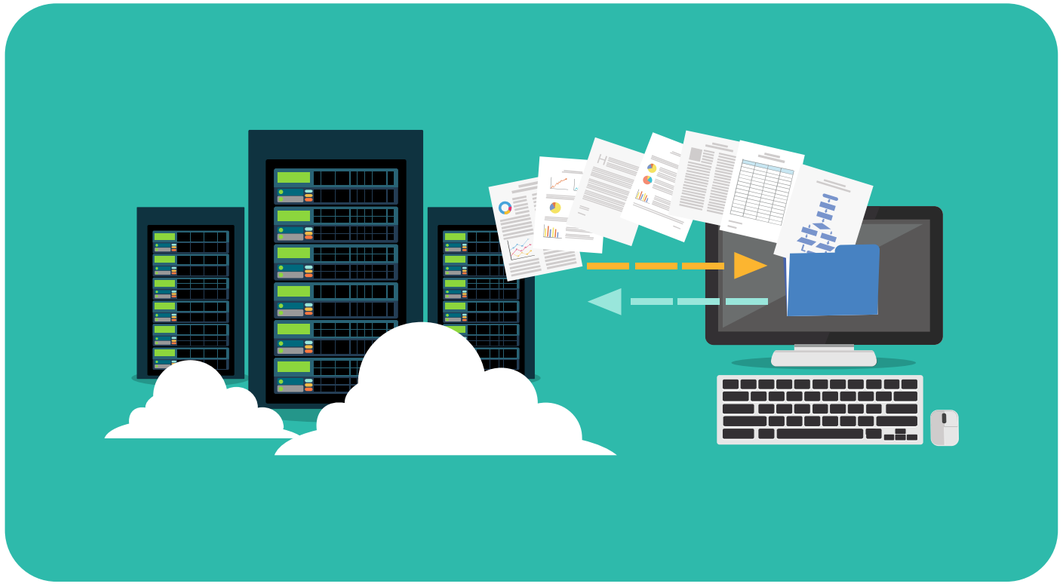
Remote journaling

Allows full synchronization of sites by transferring live data to offsite locations

Best Practices for Backup and Recovery

Backups and offsite storage

- Ensure the frequency of backups as required by the business for optimum recovery
- Store the backup tapes at an offsite location, as a security measure



Quick Check

A company is evaluating disaster recovery options and is considering a cold site solution. What is the main advantage of a cold site recovery solution?

A. Less downtime

B. Less expensive

C. Highly available

D. Zero maintenance

Implementing Disaster Recovery (DR) Processes

Disaster Recovery Processes

The main components of a disaster recovery include:

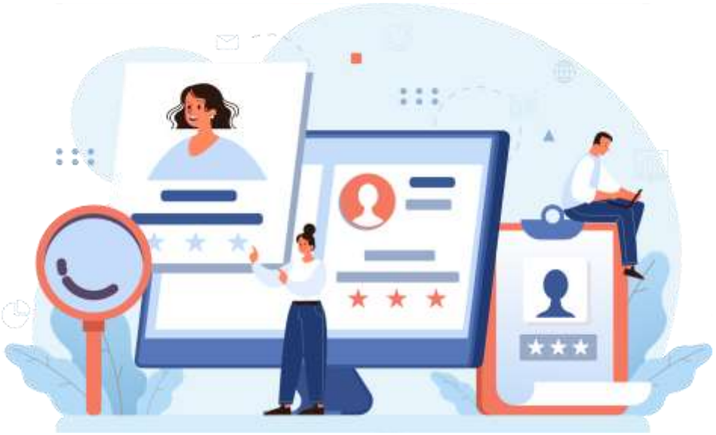
Response

It is the immediate action taken to manage a disaster.

- The BCDR plan must provide for both major and minor disasters.
- It must make personnel health and safety the top-most priority.
- It should also define, in terms of business interruption, what constitutes a disaster, thus, authorizing the activation of the disaster recovery plan.
- It must address individual and organization-wide natural disasters, fire, and physical damage.

Personnel

It involves creating a prioritized contact list of people who should be notified if a disaster occurs.



Appoint a disaster recovery team who will be responsible for acting when a disaster strikes.

Personnel

BCDR team includes:

- Incident response team
- Emergency action team
- Information security team
- Human resources (HR) team
- Damage assessment team
- Administrative support team
- Legal affairs team
- Public relations and communication team

Communications

- After BCP and DRP have been written, they must be communicated to the entire staff of the organization.
- The information should be tailored to individuals and groups.
- The conveyed information should be relevant, clear, and easily understandable for the target audience.

Crisis communication plan provides procedures for disseminating internal and external communications.

Assessment

It is the process of determining the nature, source, and impact of a disaster.

- This is carried out by the disaster response team with input from subject matter experts.
- This facilitates the recovery process by estimating the extent of damage, what can be replaced, restored, or salvaged.
- This also helps to estimate the time required for repair, replacement, and recovery.

Restoration and Recovery

Restoration means bringing a business facility and environment back to its original capabilities.

Recovery means bringing business operations and processes back to the normal working condition.

Restoration

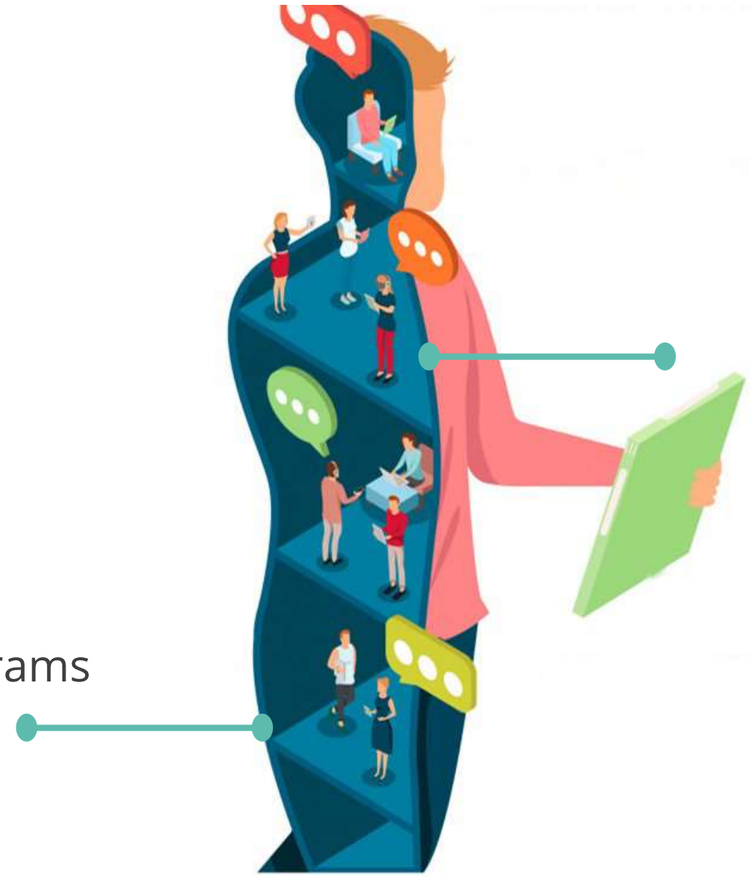
- The goal of BCDR is to resume full normal operations.
- An alternate recovery site will function as the primary site if the primary site is destroyed or severely damaged.
- The recovery site should be safe for people before the restoration process begins.
- The order of restoration of critical business functions is determined during the Business Impact Analysis (BIA).
- The disaster is officially over when all business operations and processes return to normal at the primary site.

Training

The effective execution of these plans will depend on the employees knowing what they must do and under which circumstances.

Training includes:

- Professional seminars
- Special in-house educational programs
- Use of consultants and vendors



Trainings can be in the form of:

- Refresher trainings at regular intervals
- Formal training at the time of hiring

Training

It should be designed and developed by the organizations for all the BCP or DR activities.

Trainings ensure employees:

Know the course of action in the event of an emergency

Are provided basic first aid and CPR training

Are interested in business continuity activities through periodic awareness programs

Training

The various types of training carried out are:

Starting emergency power

- Specifically for operating emergency power supplies
- Regularly testing operations

Call tree training or testing

- Answering the call and taking necessary steps
- Ensuring the calling tree process is successful

Awareness

- It is less formal than training and is generally targeted at all employees in the organization.
- It includes frequent distribution of information (newsletter, email, posters, and flyers).

Lessons Learned

Takeaways and gaps identified in the plan when either recovering at the disaster recovery site or restoring the primary site should be recorded.

Recommendations from DR testing should be implemented to continuously improve the effectiveness of the disaster recovery plan.

Quick Check

Imagine that your team has successfully addressed and contained a security incident. What should be the final phase of the incident response procedure?

A. Recovery phase

B. Lessons learnt phase

C. Remediation phase

D. Mitigation phase

Business Continuity (BC) Planning

Disaster Recovery: Planning Design and Development

According to NIST 800-34, it is the fifth phase to achieve a comprehensive BCP or DRP.

- For the recovery of critical business systems, a detailed plan is prepared and documented by the BCP team.
- The plan includes long-term and short-term goals, such as recovery plans, employee training, maintenance plan, and testing procedures.

Steps for Planning Design and Development

Step 1: Define the scope of the plan

Step 2: Identify potential disasters

Step 3: Define the BCP strategy

Step 4: Calculate funding

- Identify critical sites, systems, and business processes
- Set priorities for restoration

Steps for Planning Design and Development

Step 1: Define the scope of the plan

Step 2: Identify potential disasters

Step 3: Define the BCP strategy

Step 4: Calculate funding

- Identify the potential disasters which may impact the site
- Identify the resources needed to recover
- Identify actions that might eliminate risks in advance

Steps for Planning Design and Development

Step 1: Define the scope of the plan

Step 2: Identify potential disasters

Step 3: Define the BCP strategy

Step 4: Calculate funding

- Select the recovery strategies
- Identify important personnel, systems, and equipment that are required for recovery
- Define the roles and responsibilities of the team members
- Document the continuity strategy, which includes guidance on declaring a disaster

Steps for Planning Design and Development

Step 1: Define the scope of the plan

Step 2: Identify potential disasters

Step 3: Define the BCP strategy

Step 4: Calculate funding

- Identify the long-term and short-term goals to calculate the funding needs

Testing Disaster Recovery Plans (DRP)

Importance of Testing

Testing is the sixth phase of a business continuity and disaster recovery plan.

Testing a disaster recovery plan is important because it:

- Helps to keep the plans updated
- Identifies the shortcomings of the plans
- Tests the readiness of the organization to face disasters
- Refines the existing controls
- Satisfies the requirements of regulatory bodies

Types of Tests: Review

It is the initial and most basic DRP test that:

- Ensures the complete coverage of the plan
- Is performed by the team that had developed the plan
- Helps discover any flaws in DRP
- Ensures that there are no obvious shortcomings and omissions in the plan

Types of Tests: Checklist Testing

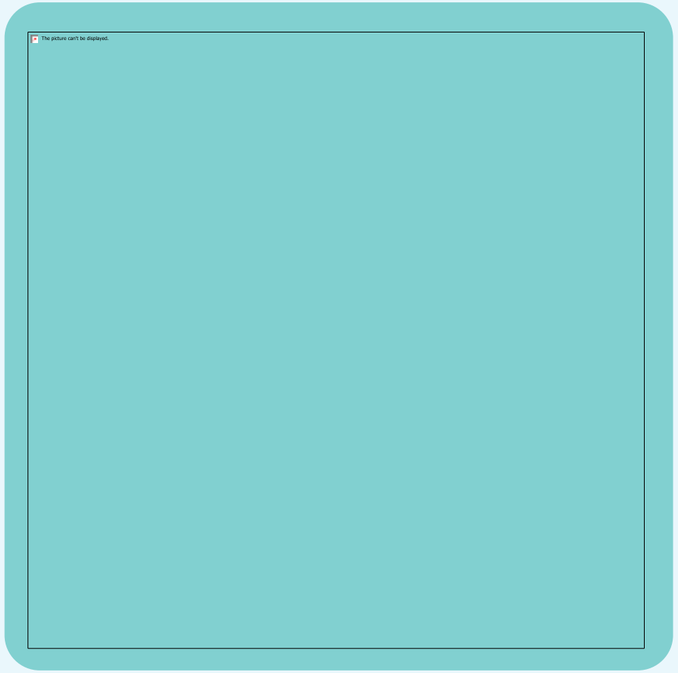
It is also known as consistency testing.

- It is a list of important and necessary components required in the process of recovery.
- It ensures that necessary components are and will be available in the event of a disaster.
- It is an easy and cost-effective method of testing the plan.

Types of Tests: Structured Walkthrough (Tabletop)

It is usually performed prior to in-depth testing and is used to:

- Review the overall approach of targeted recovery of systems and services
- Help the group discuss and perform the proposed recovery procedures in a structured manner
- Identify gaps, omissions, technical missteps, or erroneous assumptions in the process



Types of Tests: Simulation Test

It is also known as walkthrough drill.

- It helps team members to carry out a recovery process.
- It simulates a disaster, and the teams respond according to the directives outlined in the DRP.

Types of Tests: Parallel Processing

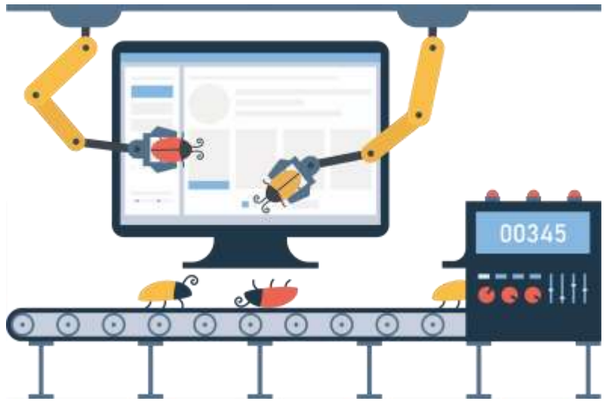
It is used in a business where critical processes involve transactional data.

- It involves the usage of alternate computing sites to recover crucial processing components and restore data from the latest backup.
- It does not interrupt the regular production systems.

Types of Tests: Partial and Complete Business Interruption Test

It has the highest fidelity of all DRP tests.

- It should be exercised with extreme caution as it can actually cause a disaster.
- It makes the organization use the alternate computing facilities and stops normal business processing at the primary location.
- It can only be conducted in organizations with fully redundant and load-balanced operations.



Quick Check

Imagine your organization recently completed a disaster recovery plan (DRP) testing. Which of the following is the best indication that the testing was successful?

A. The recovery time objective was maintained during testing.

B. The test report was shared with the senior management.

C. The business process owners were active participants during testing.

D. Systems were restored in the order of priority during testing.

Maintenance of Disaster Recovery Plans (DRP)

Disaster Recovery Phases: Maintenance

According to NIST 800-34, BCP (or DRP) maintenance is the seventh phase to achieve a comprehensive BCP (or DRP).

- The BCP (or DRP) must be updated once it is completed, tested, trained, and implemented.
- The plan must incorporate all business and IT system changes as they become obsolete quickly.

Disaster Recovery Phases: Maintenance

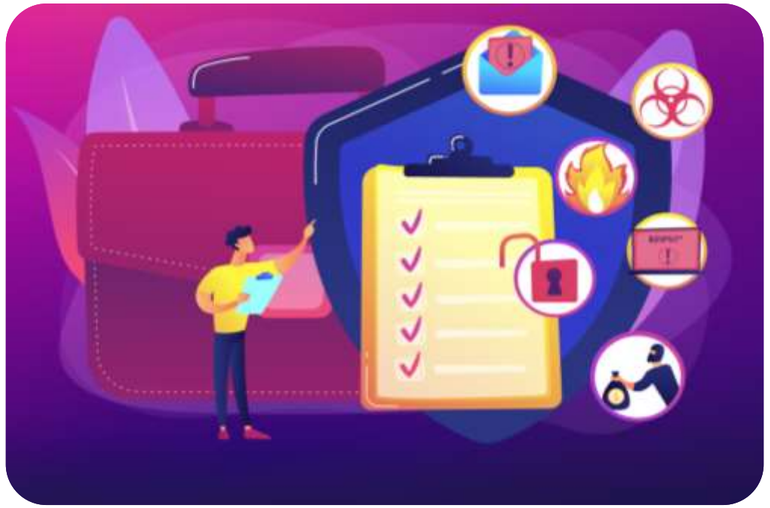
Change management ensures that:

- Security is not adversely affected when new systems are introduced, modified, and updated
- All planned changes are documented and tracked
- Substantial changes are formally approved and documented

Disaster Recovery Phases: Maintenance

The strategies to maintain the plan and ensure it is valid are:

- Make BCP a part of every business decision
- Insert BCP maintenance responsibilities into job descriptions
- Include maintenance in personnel evaluations
- Perform internal audits that include disaster recovery and BCP procedures
- Test the plan annually

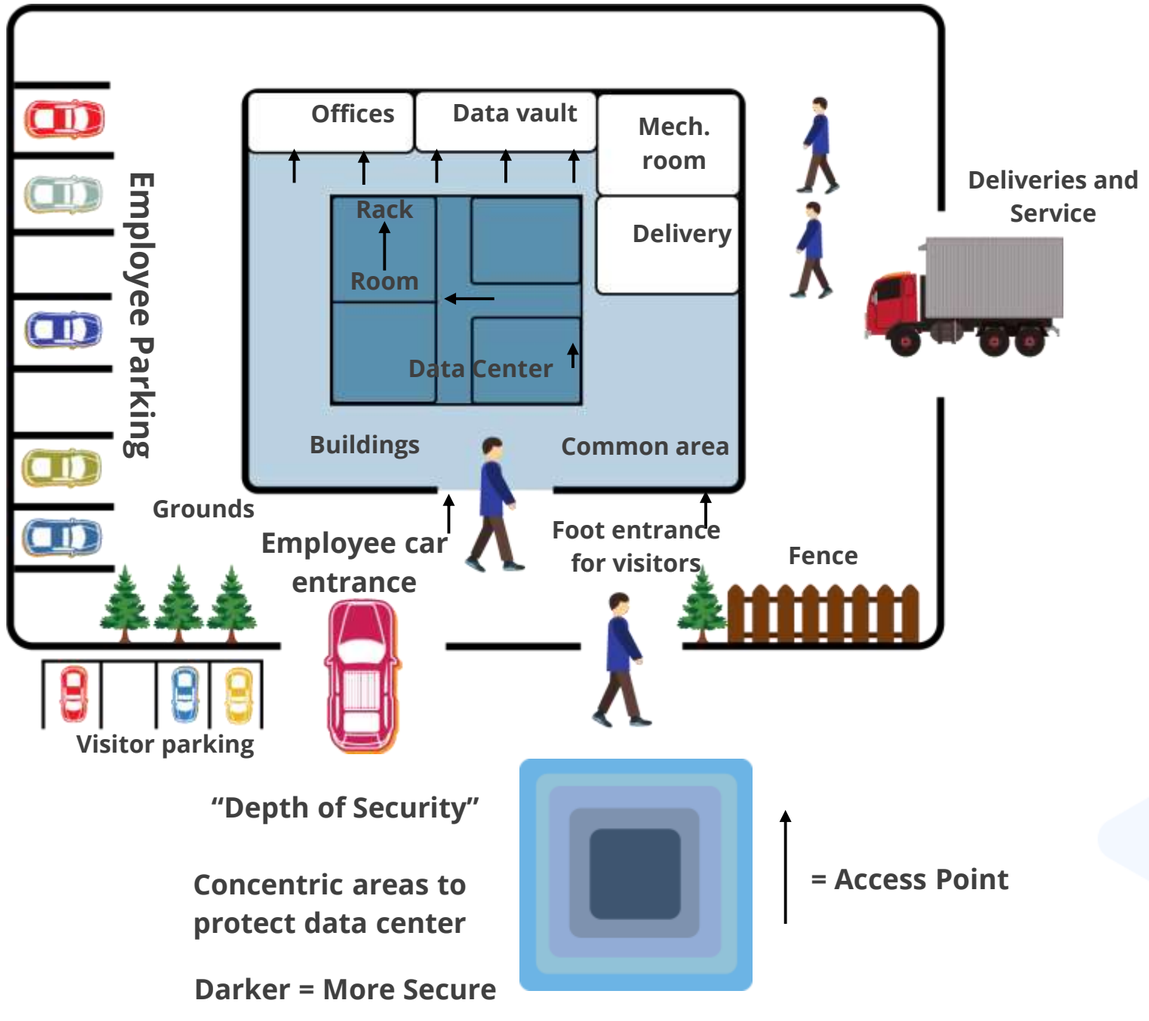


Implementing and Managing Physical Security

Perimeter Security Controls

They help to prevent, detect, and correct unauthorized physical and control access into the facility.

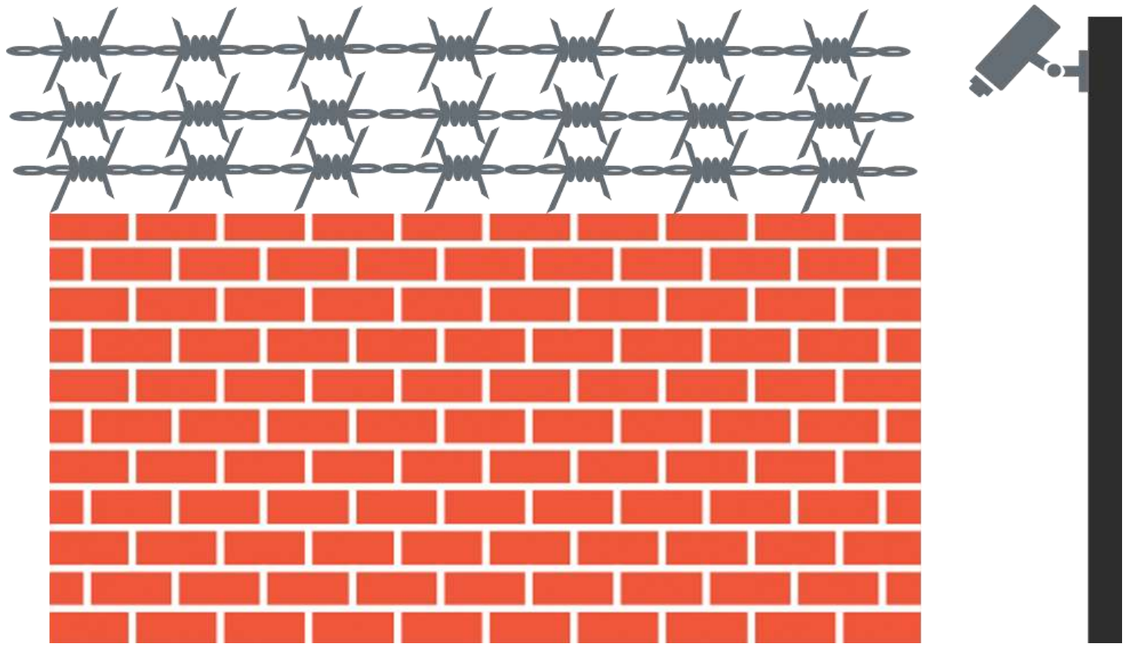
- It employs the defense-in-depth concept.
- It uses layered architecture for barriers, providing the center or the most protected area the highest level of security.
- It is designed by utilizing multiple barriers called rings of protection.
- It reduces the likelihood of a successful attack with the help of a layered design.



Barriers

They define how an area should be designed to obstruct or deny access.

- It keeps the intruders out.
- It helps create delays in intrusion.



Fences

They are perimeter identifiers that are designed and installed to keep intruders out.

The various types of fences include:

Chain link

Barbed wire

Barbed tape

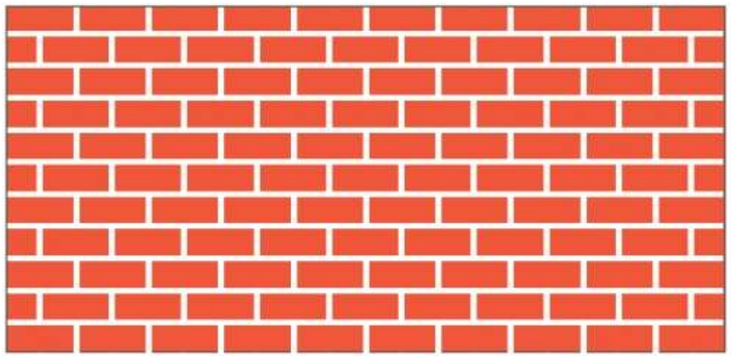
Concertina wire

Height	Effectiveness
3 - 4 ft.	Deters casual trespassers
6 – 8 ft.	Too difficult to climb easily
8 ft. plus 3 strands of barbed or razor wire	Deters determined trespassers

Walls and Bollards

Walls are man-made barriers but are usually more expensive to install than fences.

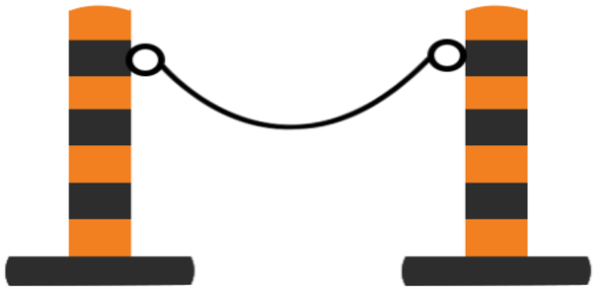
- Common types of walls are:
  - Cinder block
  - Masonry
  - Brick
  - Stone



Bollards are small concrete pillars outside a building.

Example

Traffic bollard

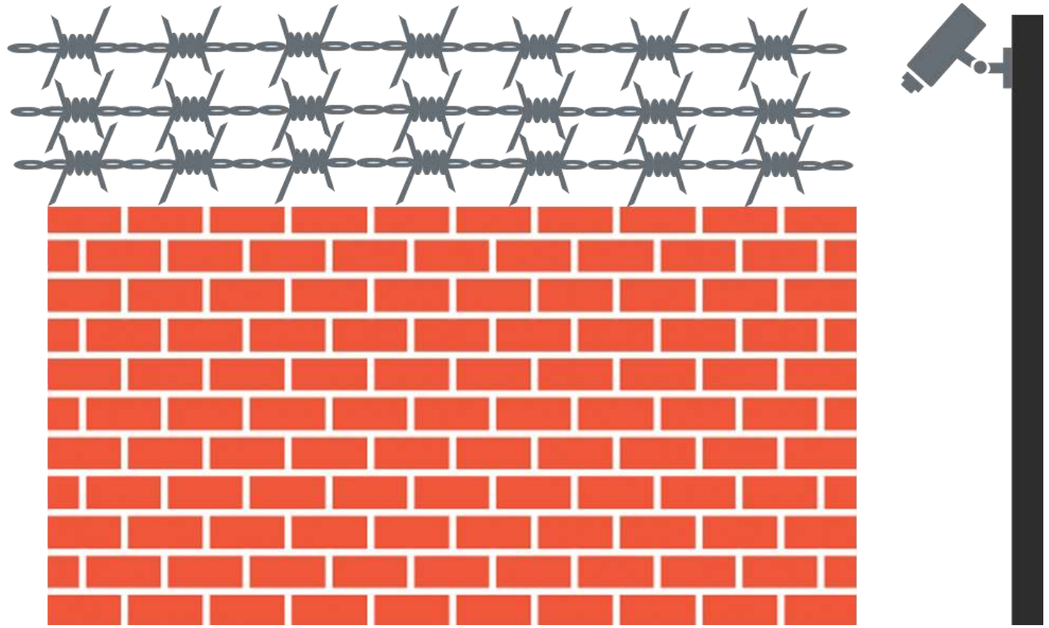


Perimeter Intrusion Detection

They are perimeter sensors that alert security when any intruder attempts to gain access across the open space or breaches the fence line.

Open-terrain sensors include:

- Infrared
- Microwave systems
- Time-domain reflectometry (TDR) systems
- Video content and motion path analysis



Importance of Lighting

- Provides security personnel the ability to visually assess their surroundings at night
- Helps notice and identify individuals at night
- Increases the effectiveness of guard forces and CCTV
- Reduces the need for security personnel
- Provides real and psychological deterrents against intruders
- Provides illumination where natural light is insufficient
- Is inexpensive to maintain

Types of Lighting Systems

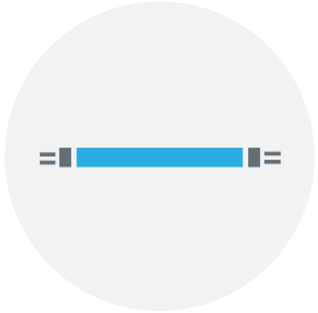
Continuous light

Standby light

Movable light

Emergency light

Types of Lights



Fluorescent lights

Quartz lamps

Mercury vapor lights

Infrared illuminators

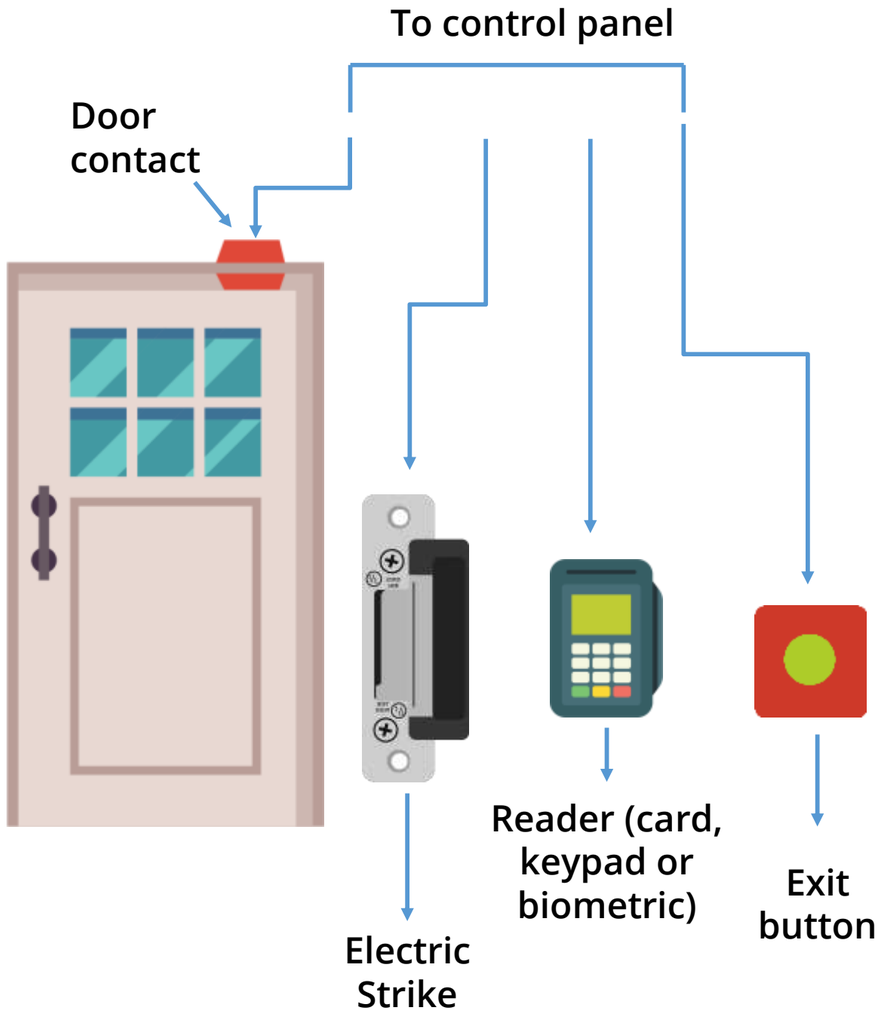
Sodium vapor lights

Access Control

The primary function of an access control system (ACS) is to allow only authorized personnel inside a controlled area and limit the opportunity for a crime to be committed.

Key components of an ACS include:

- Card readers for authentication
- Electric locks for securing entry points
- Alarms to alert against unauthorized access
- Computer systems to manage and monitor access operations



Types of Access Control Systems

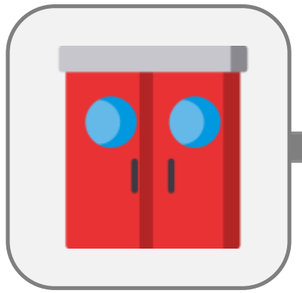
Access cards	Include magnetic stripe, proximity card, and smart card
Biometrics	Include fingerprint, facial image, hand geometry, voice recognition, iris patterns, retina scanning, signature dynamics, and keystroke dynamics
Closed circuit television	Allows one to view and record security events with the help of a collection of cameras, recorders, switches, keyboards, and monitors
CCTV color cameras	Offer additional information, such as the color of a vehicle or a subject's clothing

Types of Access Control Systems

Digital video recorder (DVR) and monitor displays	Help to download a hard drive for storage of historical information
Guards	Protect against fire, theft, vandalism, terrorism, and illegal activity
Guard dogs	Serve as detective, preventive, and deterrent controls

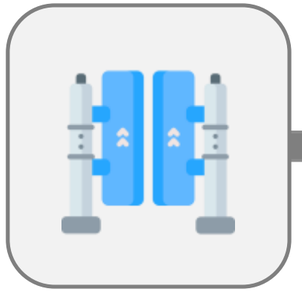
Securing a Building

These are the various means to secure a building:



Solid core, hollow core, and glass doors

Rim, mortise, and cipher locks



Mantrap and turnstile

Bulletproof and laminated windows

Infrared and ultrasound interior intrusion detection systems

Escort and visitor controls

Quick Check

A company is choosing between human guards and automated controls for security. Which of the following highlights the main advantage of using guards?

A. One does not need to screen guards before hiring them.

B. Automated control cannot make discriminating judgments like guards.

C. Guards do not need training.

D. Guards are cheaper than automated controls.

Address Personnel Safety and Security Concerns

Security Advisory

It is a formal communication that provides crucial information on potential risks, threats, and safety precautions for travelers and organizations, ensuring personal safety and asset protection.

Ensuring Travel Safety

Information about technical controls along with personnel training will ensure the safety of employees when they travel.

Employees must understand the dos and don'ts about using IT systems when they go abroad.

Employees must encrypt the devices, use strong passwords, and follow other due care processes when traveling.

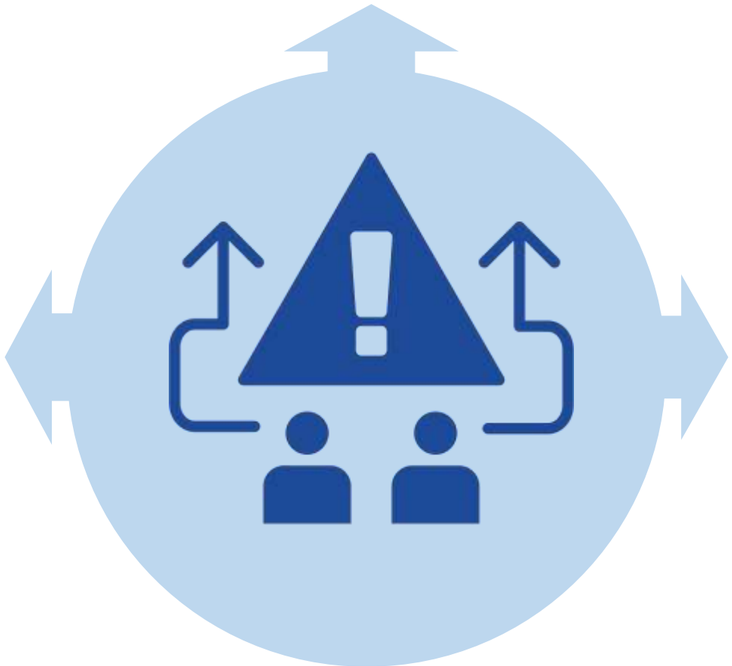
Security Training and Awareness

It equips the learner with the knowledge, skill, and competence to recognize security threats and maintain safety practices.

It educates the learners regarding:

Incident reporting procedures

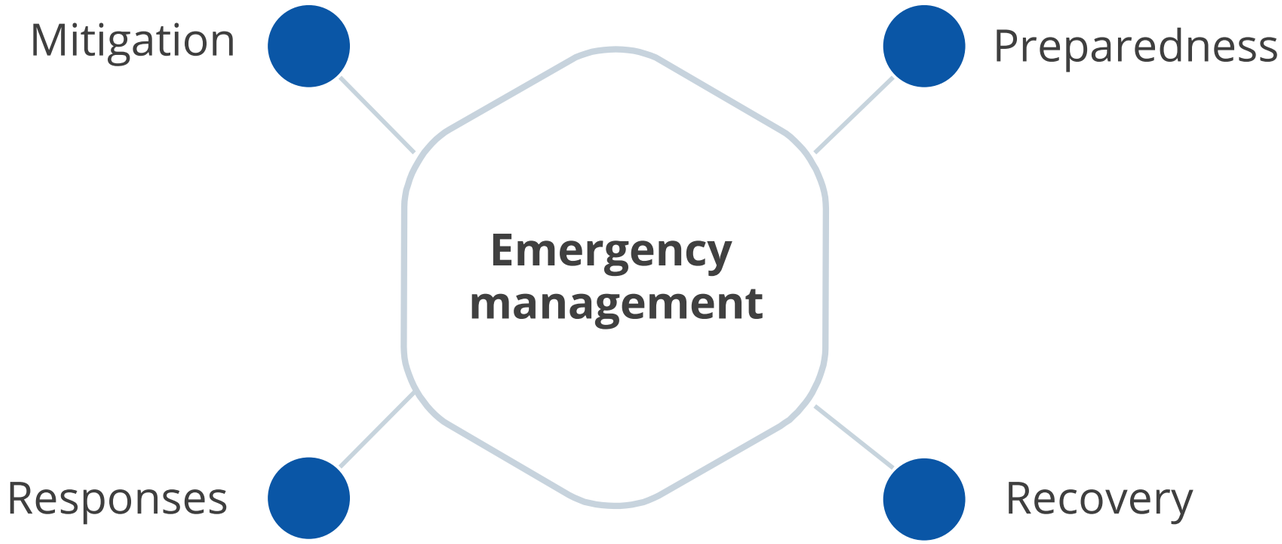
Risks, hazards, and controls associated with the workplace



Emergency procedures

Emergency Management

It is the organization and management of the resources and responsibilities needed to withstand, respond to, and recover from all types of emergencies and disasters.



Human safety should be the top priority in the event of an emergency.

Duress

It is defined as any unlawful threat or coercion used to induce another person to act (or not act) in a manner they otherwise would not (or would).

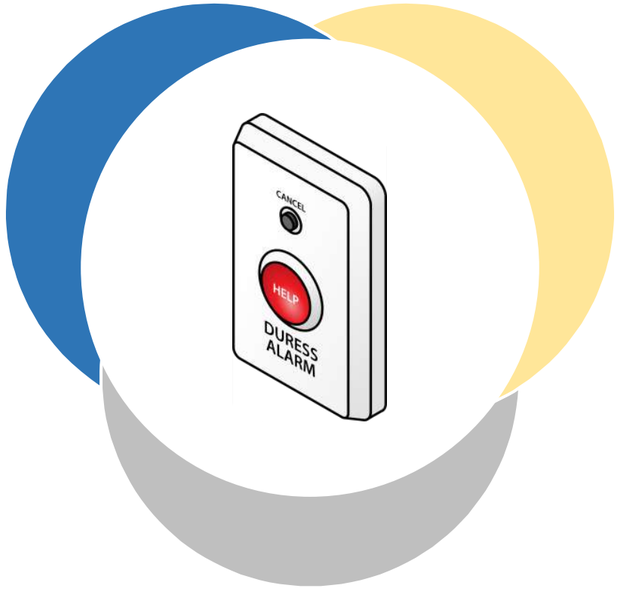
These situations can be life-threatening or deadly.

Employees should undergo training on how to handle a stressful situation and what to do when under duress.

Duress

The following measures can be helpful in handling duress:

A duress code (covert signal) should be used by an individual that is under duress to convey their state.



Lone workers, security guards, or healthcare providers may also use duress or panic alarms if urgent assistance is needed.

When designing duress mitigation controls or training, it's wise to consult law enforcement or security experts.

Key Takeaways

- Intrusion detection and prevention, security information, event management, continuous monitoring, and egress monitoring can be used to log and monitor activities.
- The three important concepts of the security operations domain are threats, vulnerabilities, and assets.
- Incident response is the practice of detecting, determining, minimizing, and resolving a problem.
- A recovery process must focus on responding to the disaster, recovering critical and noncritical functions, salvaging and repairing hardware and software, and returning to the primary site of operations.
- Perimeter security controls are used to prevent, detect, and respond to unauthorized physical access and control breaches at the facility.

Thank You