Introduction to CyberSecurity

MNU-2025

Dr. Ahmed Samy

Course Description

- This course provides a comprehensive introduction to the fundamental concepts of cybersecurity.
- The course covers essential topics to help you understand the importance of cybersecurity, recognize common threats, and learn basic practices to protect digital assets.
- Through a combination of lectures, hands-on activities, and real-world examples, you will gain the knowledge and skills needed to navigate the digital world safely and confidently.

About Me

Dr. Ahmed Samy

Ph.D. in Computer Science and Technology from HIT.

10+ years of teaching experience.
6+ years of technical experience.
Specialized in Networks and Security.

Email: ahmed.samy20@gmail.com

Course Major Contents

In this course, we will cover the below topics:

Introduction to CyberSecurity

Cybersecurity definition, CIA triad, cybersecurity teams, threat actors, skills of cyberSecurity expert.

Network Basics for CyberSecurity

Network Infrastructure, TCP/IP protocols, Common TCP/IP attacks

CyberSecurity Fundamentals

Threats, vulnerabititities, risk, attack vector, malware types

Securing Networks

Firewalls, IDS

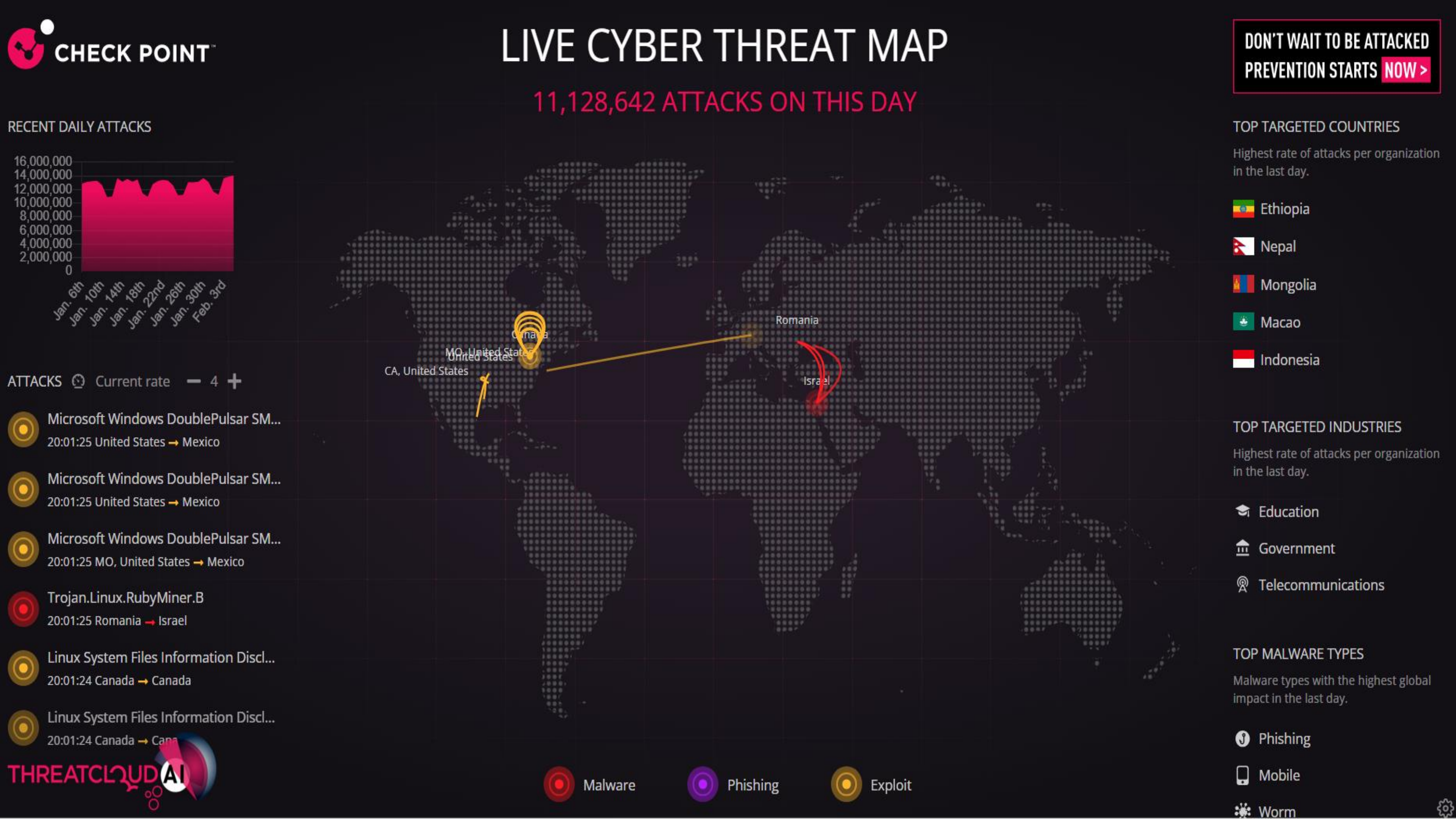
Web Security

Web vulnerabilities, attacks, WAF

Security Operation Center (SOC)

SOC definition, tools

Lec_1: Introduction to Cyber Security



LIVE CYBER THREAT MAP

11,128,642 ATTACKS ON THIS DAY

RECENT DAILY ATTACKS

ATTACKS Current rate — 4 +

Microsoft Windows DoublePulsar SM...
20:01:25 United States → Mexico

Microsoft Windows DoublePulsar SM...
20:01:25 United States → Mexico

Microsoft Windows DoublePulsar SM...
20:01:25 MO, United States → Mexico

Trojan.Linux.RubyMiner.B
20:01:25 Romania → Israel

Linux System Files Information Discl...
20:01:24 Canada → Canada

Linux System Files Information Discl...
20:01:24 Canada → Cana

Malware Phishing Exploit

TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Ethiopia
- Nepal
- Mongolia
- Macao
- Indonesia

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Government
- Telecommunications

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Phishing
- Mobile
- Worm

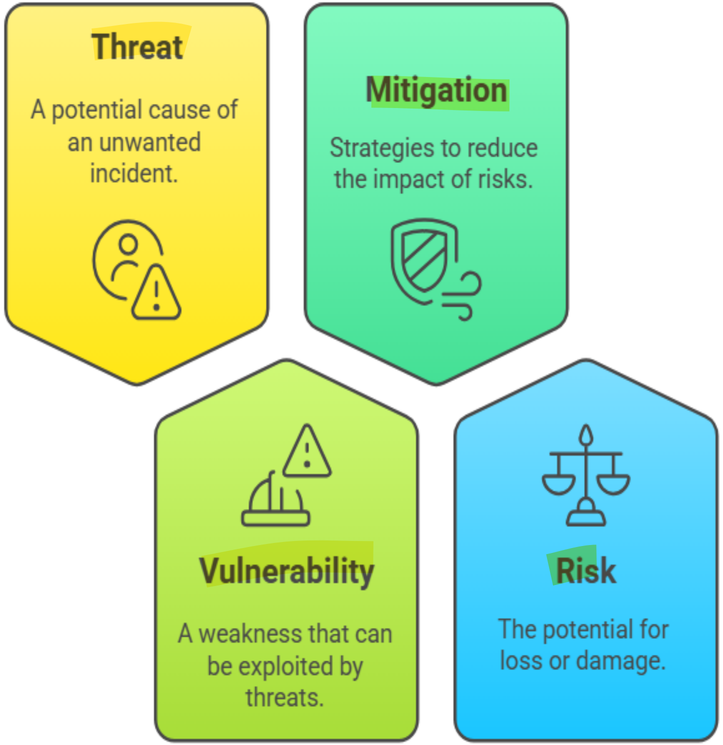
What is Cybersecurity?

- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

- How much of your daily life relies on technology?

- How much of your personal information is stored either on your own computer, smartphone, tablet or on someone else's system?

Common Cybersecurity Terms



Threat

A potential cause of an unwanted incident.

Mitigation

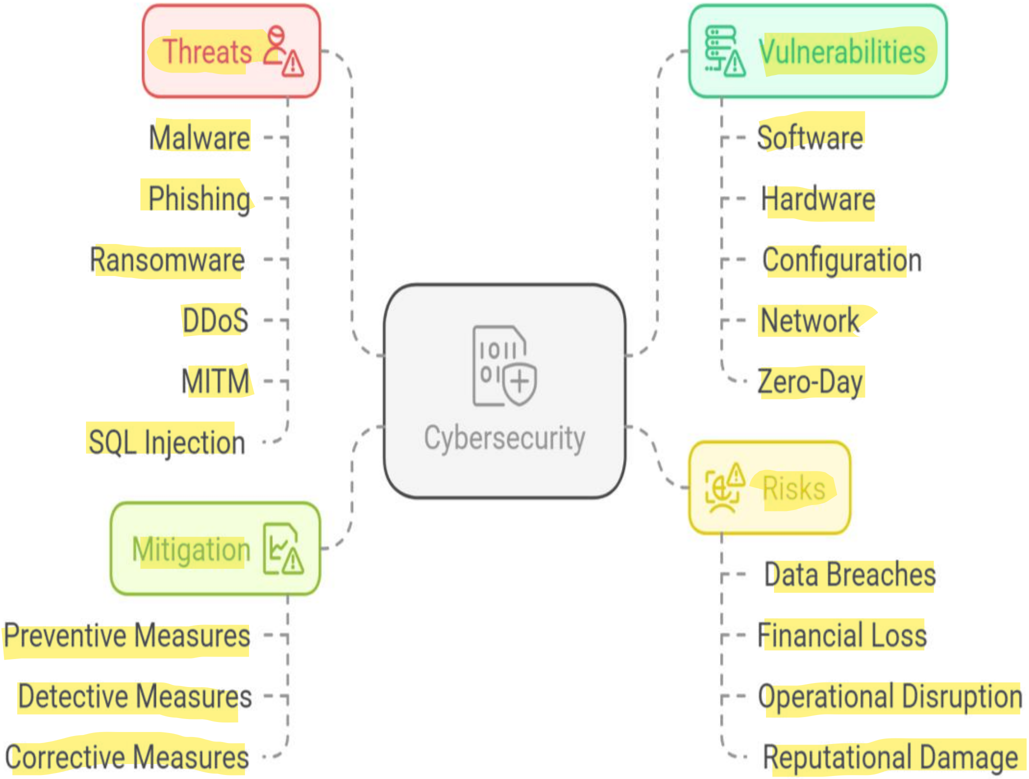
Strategies to reduce the impact of risks.

Vulnerability

A weakness that can be exploited by threats.

Risk

The potential for loss or damage.



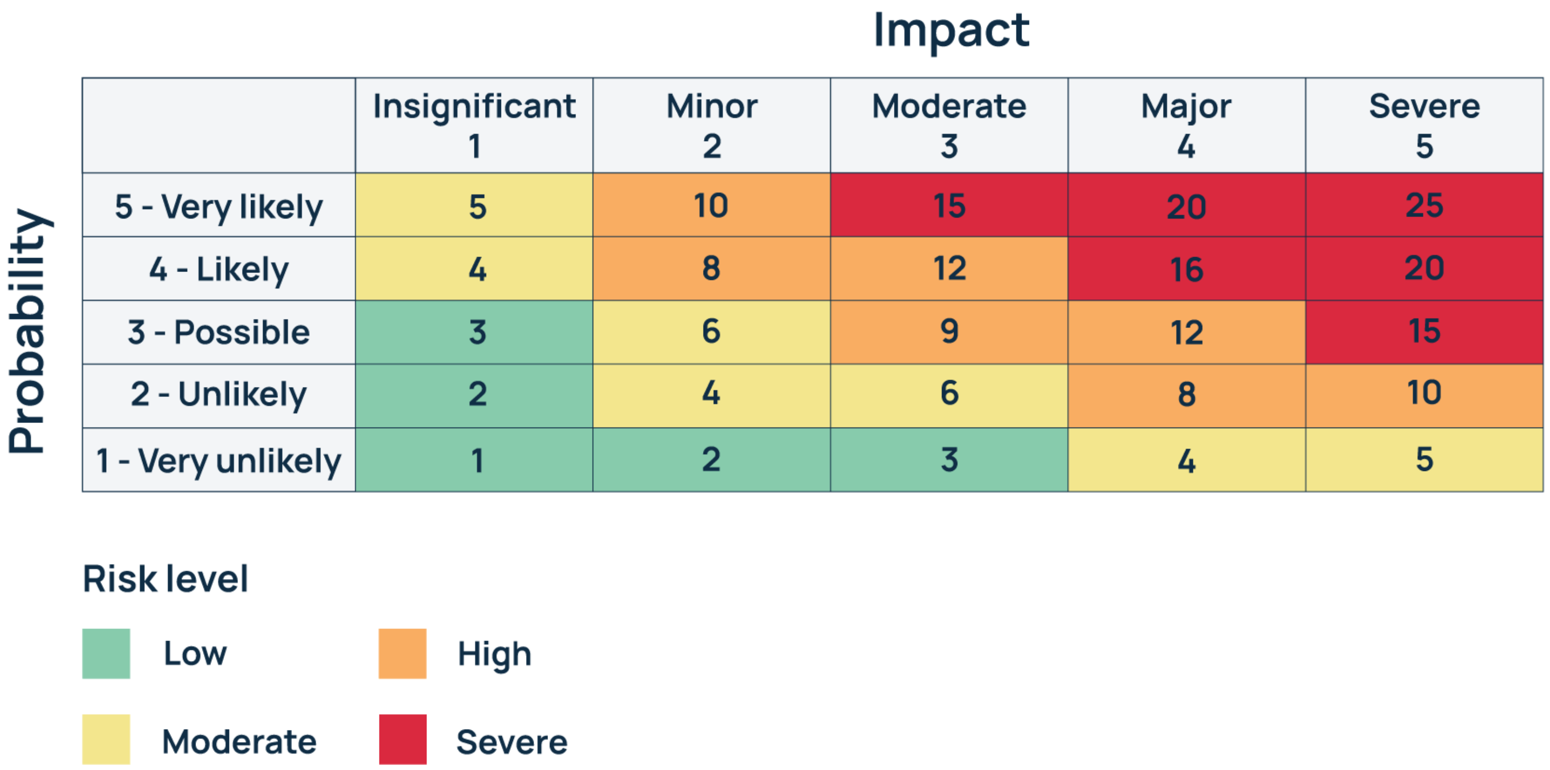
Cybersecurity

Threats
- Malware
- Phishing
- Ransomware
- DDoS
- MITM
- SQL Injection

Vulnerabilities
- Software
- Hardware
- Configuration
- Network
- Zero-Day

Mitigation
- Preventive Measures
- Detective Measures
- Corrective Measures

Risks
- Data Breaches
- Financial Loss
- Operational Disruption
- Reputational Damage



Impact

Probability

	Insignificant 1	Minor 2	Moderate 3	Major 4	Severe 5
5 - Very likely	🟨 5	🟧 10	🟥 15	🟥 20	🟥 25
4 - Likely	🟨 4	🟧 8	🟧 12	🟥 16	🟥 20
3 - Possible	🟩 3	🟨 6	🟧 9	🟧 12	🟥 15
2 - Unlikely	🟩 2	🟨 4	🟨 6	🟧 8	🟧 10
1 - Very unlikely	🟩 1	🟩 2	🟩 3	🟨 4	🟨 5

Risk level

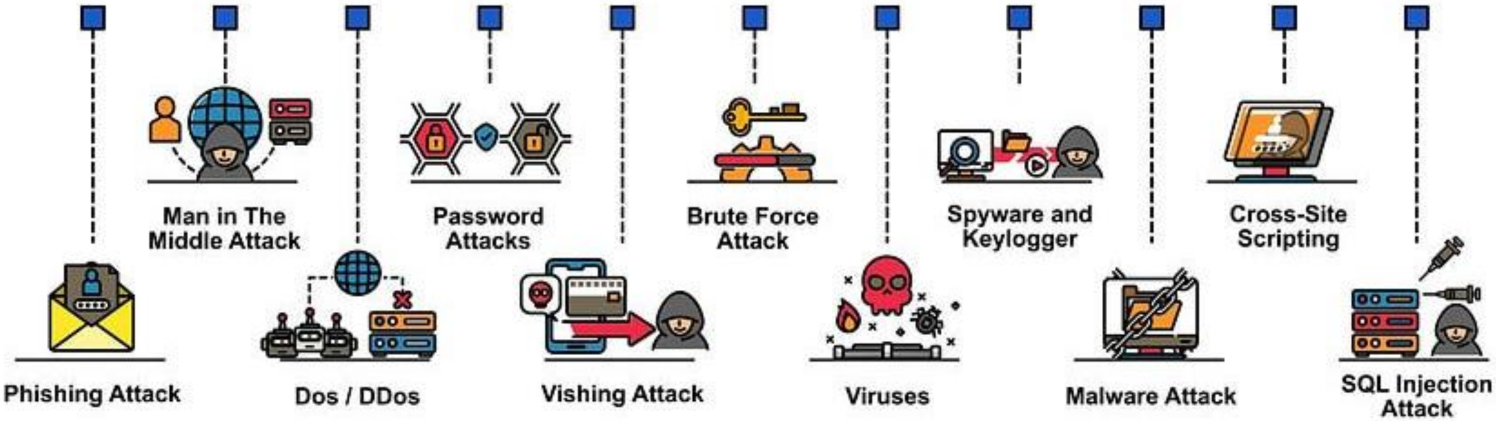
🟩 Low

🟨 Moderate

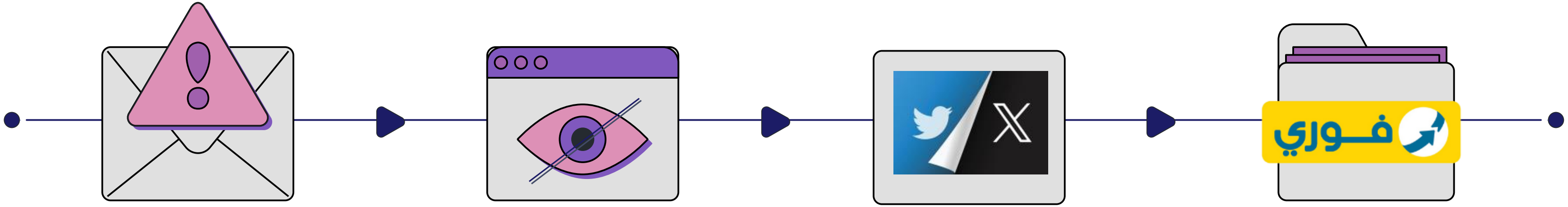
🟧 High

🟥 Severe

Cybersecurity Attacks



Popular Cybersecurity Breaches



Yahoo! (2013)

Over 3 billion user accounts were compromised.

hackers stole names, email addresses, phone numbers, birthdates, hashed passwords, and security questions.

Wannacry Ransomware Attack (2017)

Affected 200,000 computers across 150 countries

exploited a Windows vulnerability to encrypt files and demand ransom payments in Bitcoin.

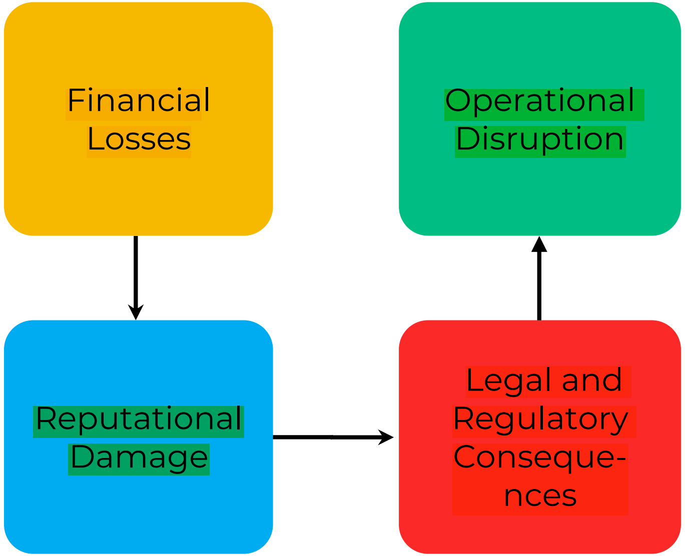
Twitter (2020)

Hackers gained access to Twitter's internal systems and took over accounts of prominent figures like Barack Obama, Elon Musk, and Bill Gates to promote a Bitcoin scam.

Fawry (2023)

the hacker has gained access to all data stored in the Fawry database, including names, credit and debit card numbers, national IDs, and other personal information.

The Impact of Cyber Attacks



Financial Losses

Ransom payments, costs of IT services and cybersecurity consultants, legal fees, system downtime, and revenue loss.

Reputational Damage

Loss of customer trust and brand damage, and loss of competition with other companies.

Legal and Regulatory Consequences

Organizations may face legal action from customers, partners, and other affected parties.

Operational Disruption

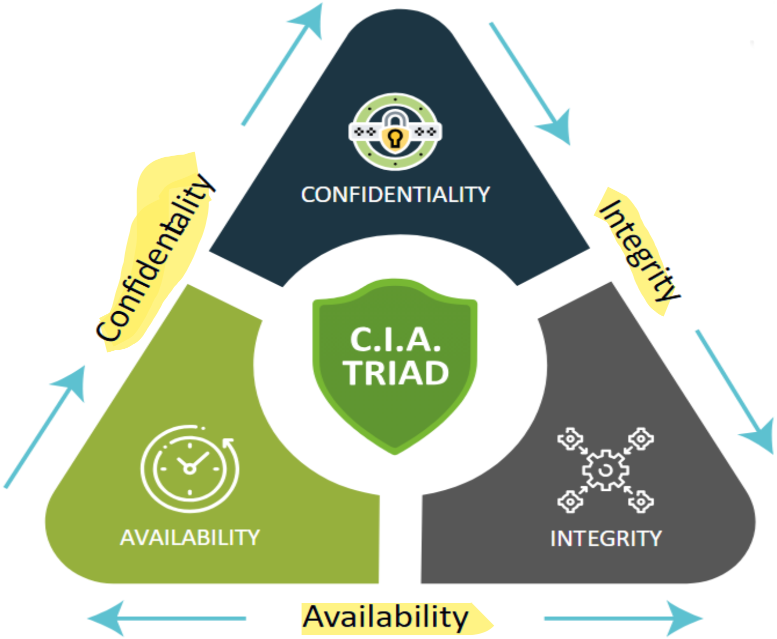
Disrupt critical systems, halting operations and impacting productivity. Affect suppliers and causing delay.

Three Pillars of Cybersecurity

- We can think of the CIA triad as the foundation of cybersecurity.

- Confidentiality, Integrity, and Availability (CIA) are the three pillars of cybersecurity.

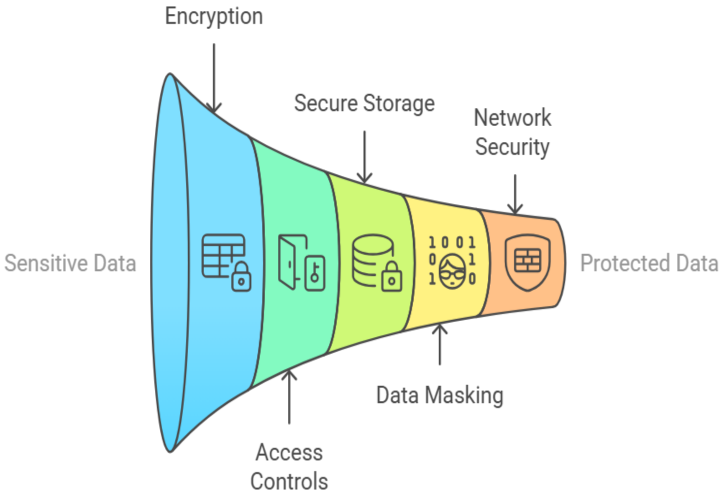
- We can be certain that one or more principles of the CIA triad have been violated – leaving the data owner at risk.



Confidentiality

- Confidentiality is the process of keeping an organization or individual's data private and ensuring only authorized people can access it.
- Example: When a customer logs in to their online banking portal, their username and password are encrypted before being sent to the bank's servers.
- **How Data Confidentiality is Ensured?**
    - Encryption: using complex encryption techniques.
    - Access Controls : passwords and Multi Factor Authentication.
    - Secure Storage: store data in secure domain.
    - Data masking: mask sensitive information.
    - Network Security: firewalls, IPS, IDS.

Ensuring Data Confidentiality

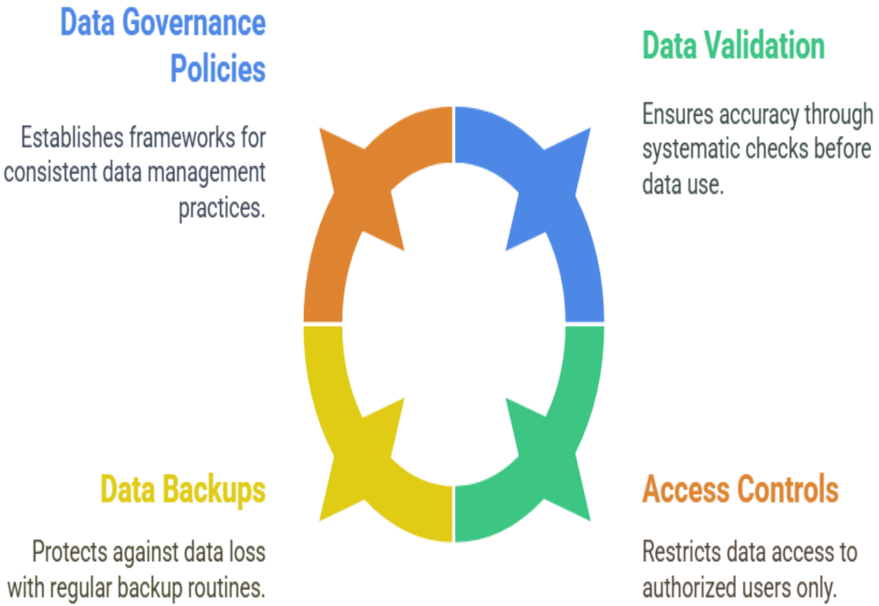


Integrity

- Integrity refers to data that hasn't been tampered with. It ensures that data remains unaltered and trustworthy from the moment it is created, stored, processed, or transmitted until it is deleted.

- Example: e-commerce customers expect the information and pricing of products listed in a store to be accurate and unaltered.

- **How Data Integrity is Ensured?**
  - Data validation
  - Access controls
  - Data backups
  - Data governance policies



Data Governance Policies

Establishes frameworks for consistent data management practices.

Data Validation

Ensures accuracy through systematic checks before data use.

Data Backups

Protects against data loss with regular backup routines.

Access Controls

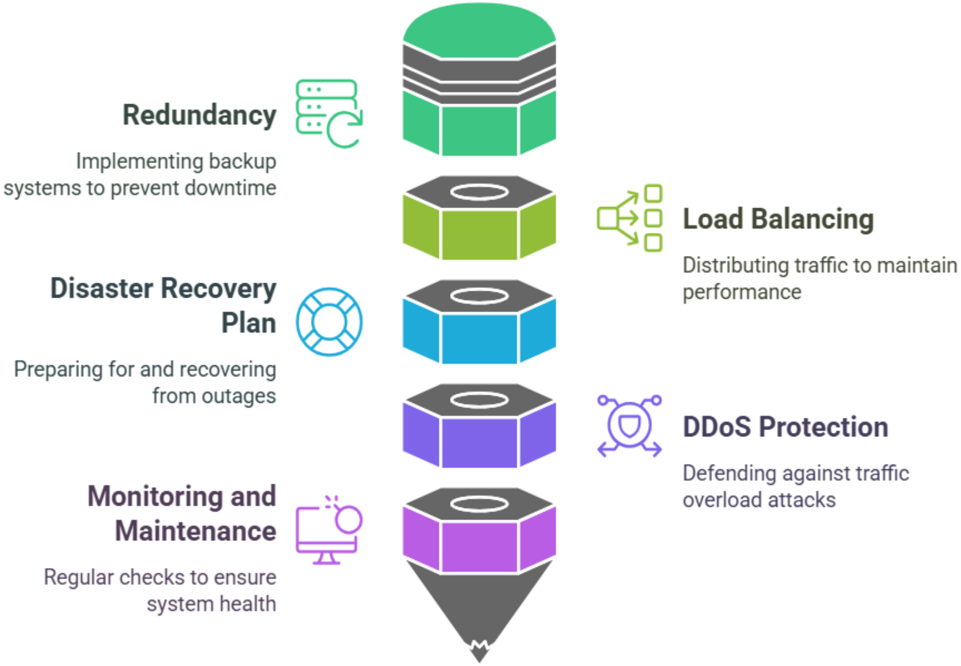
Restricts data access to authorized users only.

Availability

- Availability refers to ensuring that data, systems, and resources are accessible and operational when needed by authorized users.

- An e-commerce website must ensure that its platform is available to customers 24/7, especially during peak shopping periods like Black Friday or holiday sales.

- **How availability is Ensured?**
    - Redundancy
    - Load balancing
    - Disaster recovery plan
    - DDoS protection
    - Monitoring and Maintenance



Redundancy
Implementing backup systems to prevent downtime

Load Balancing
Distributing traffic to maintain performance

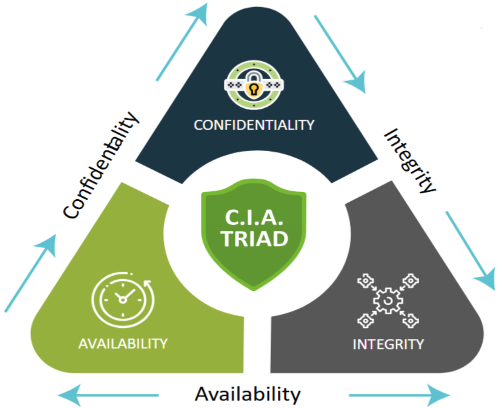
Disaster Recovery Plan
Preparing for and recovering from outages

DDoS Protection
Defending against traffic overload attacks

Monitoring and Maintenance
Regular checks to ensure system health

How to Apply the CIA Triad Principles

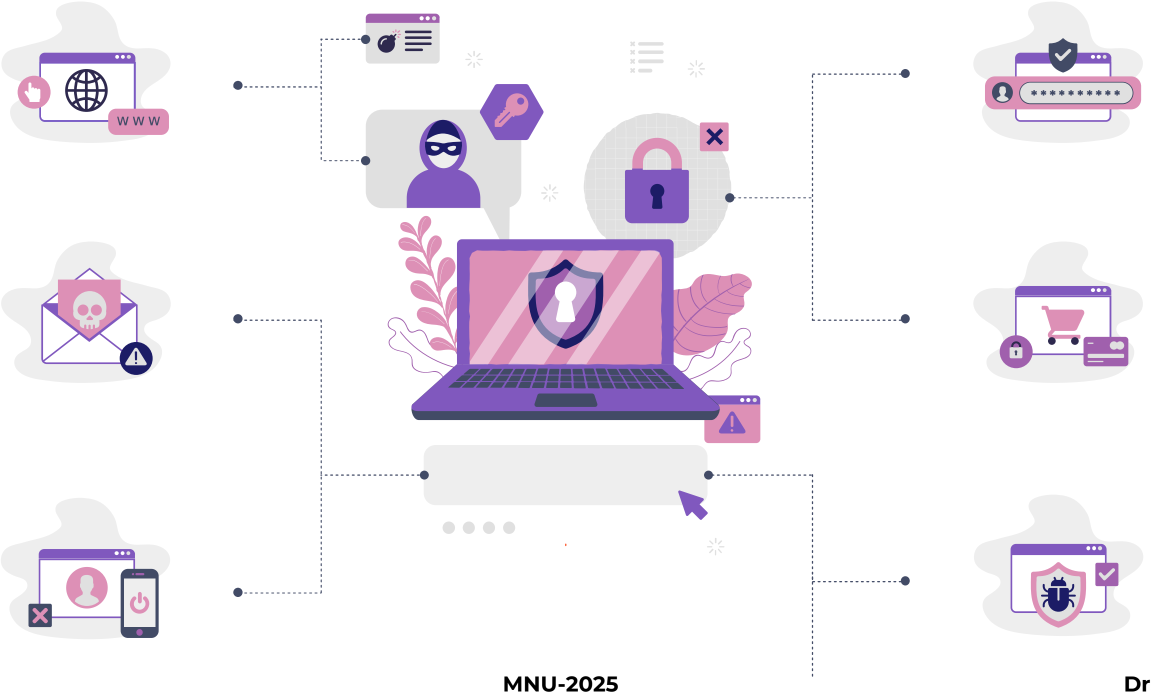
- Confidentiality is critical when it comes to governmental sectors like intelligence services.
- Integrity is more important when it comes to the financial industry – imagine what would happen if someone changed your $5,000,000 to $5!.
- Availability is vital when it comes to healthcare sector – if their systems become unavailable, then the life of patients could be in danger.



How Cybersecurity Works?

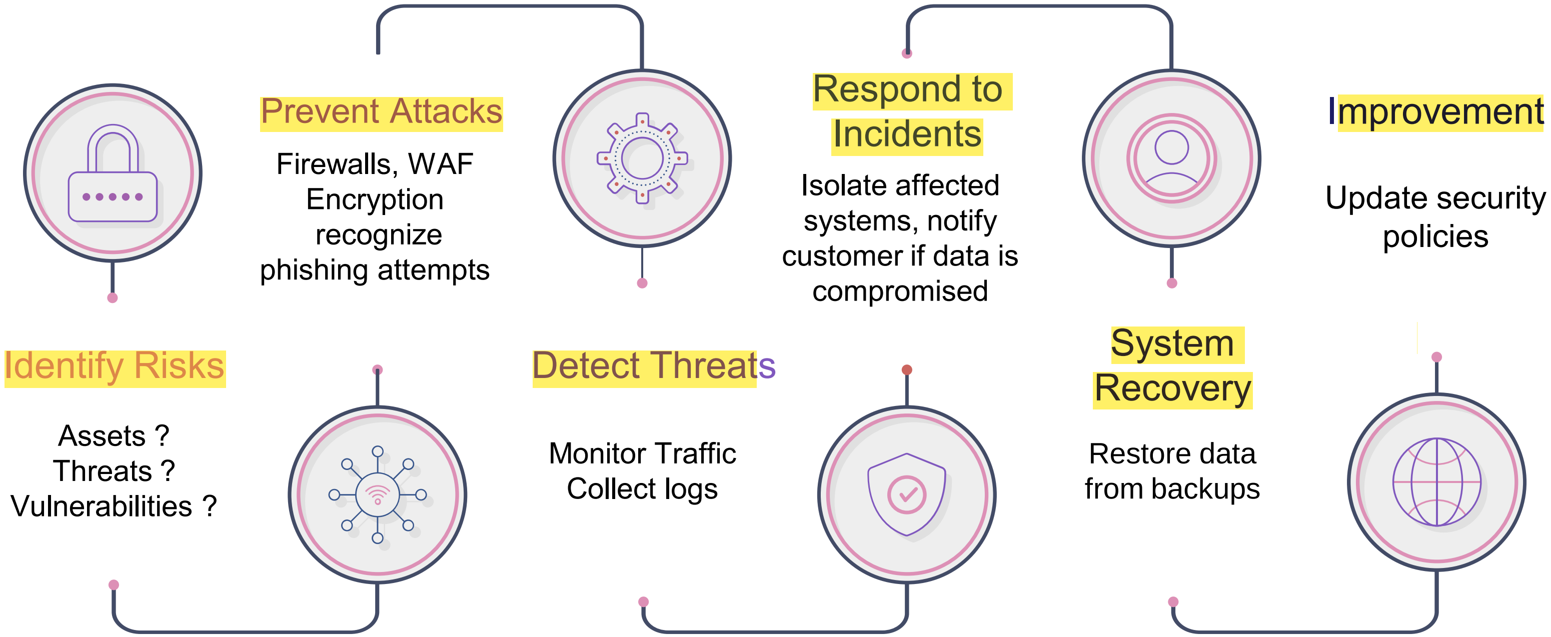
Cybersecurity works by implementing a combination of technologies, processes, and practices designed to protect systems, networks, devices, and data from cyber threats.

1. Identify and Assess Risks
2. Implement Preventive Measures
3. Detect Threats and Anomalies



4. Respond to Incidents
5. Recover and Restore
6. Monitor and Adapt

E-Commerce Practical Example



Identify Risks

Assets ?
Threats ?
Vulnerabilities ?

Prevent Attacks

Firewalls, WAF
Encryption
recognize
phishing attempts

Detect Threats

Monitor Traffic
Collect logs

Respond to Incidents

Isolate affected systems, notify customer if data is compromised

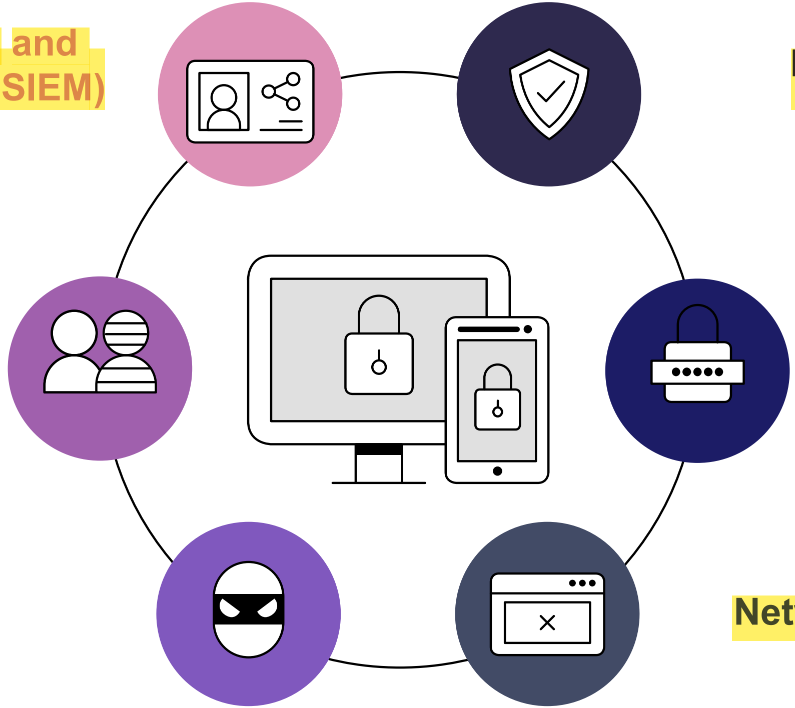
System Recovery

Restore data from backups

Improvement

Update security policies

Security Services



Security Information and Event Management (SIEM)

PAM , IAM

Endpoint Security

Cloud Security

Data loss Prevention

Network Security

Cybersecurity Threat Actors

- **Cybercriminals**: Individuals or groups motivated by financial gain, often using malware, phishing, or ransomware.
- **Hacktivists**: Attackers motivated by political or social causes, often targeting organizations they oppose.
- **Nation-States**: Governments conducting cyber espionage or cyber warfare to steal information or disrupt critical infrastructure.
- **Insiders**: Employees, contractors, or partners who intentionally or accidentally cause harm.
- **Script Kiddies**: Inexperienced attackers using pre-made tools to exploit vulnerabilities.
- **Natural Events**: Environmental factors like storms, floods, or power outages.

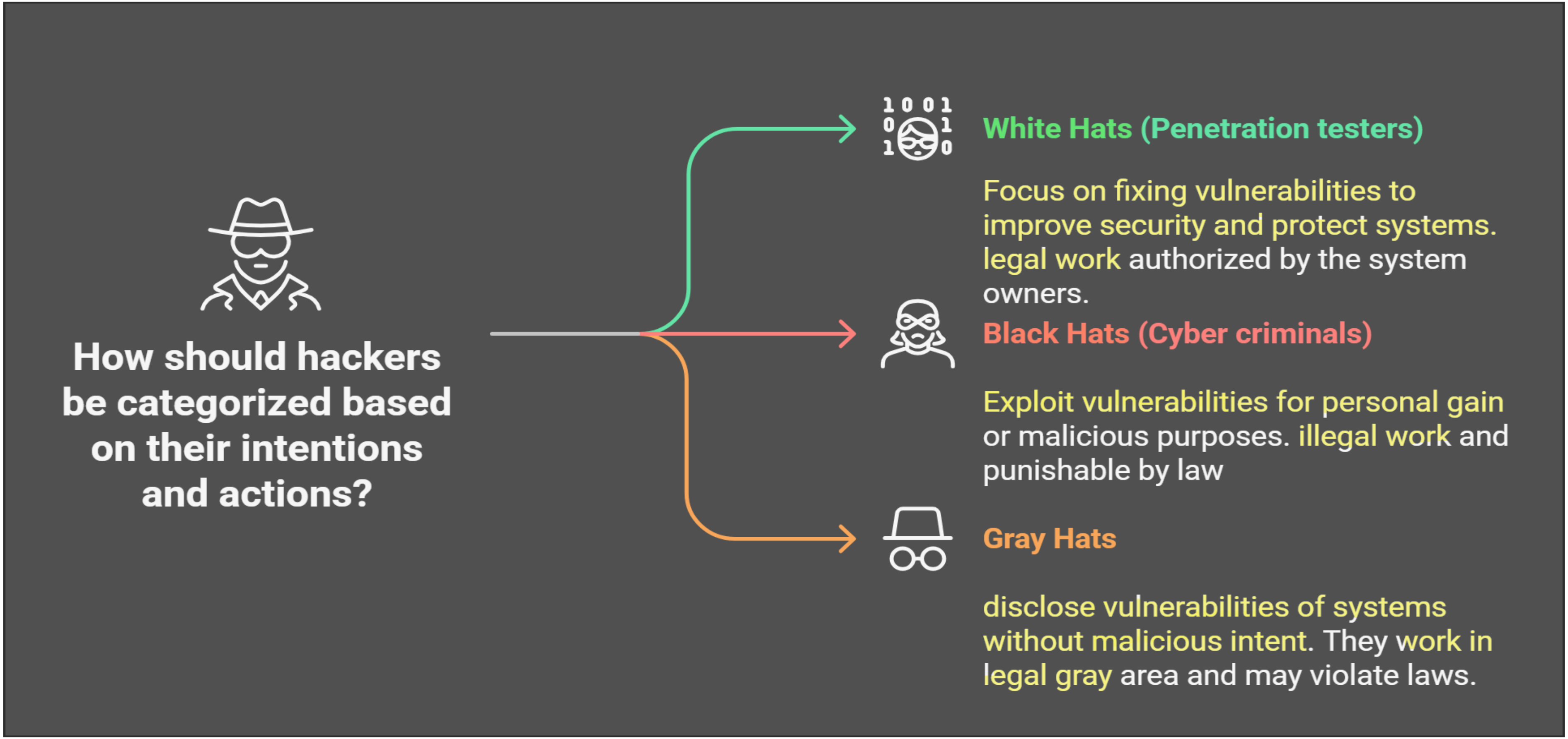
Cybercriminals

- Cybercriminals are threat actors who are motivated to make money using any means necessary.

- While some cybercriminals work independently, they are more often financed and sponsored by criminal organizations.

- It is estimated that globally, cybercriminals steal billions of dollars from consumers and businesses every year.

Types of Hackers



How should hackers be categorized based on their intentions and actions?

White Hats (Penetration testers)

Focus on fixing vulnerabilities to improve security and protect systems. legal work authorized by the system owners.

Black Hats (Cyber criminals)

Exploit vulnerabilities for personal gain or malicious purposes. illegal work and punishable by law

Gray Hats

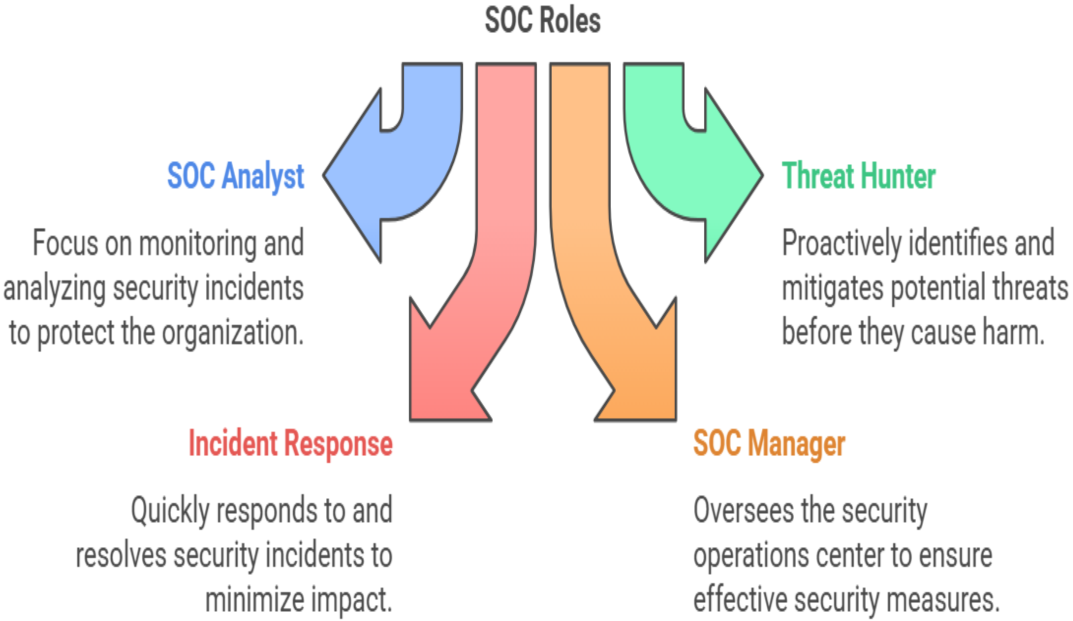
disclose vulnerabilities of systems without malicious intent. They work in legal gray area and may violate laws.

Cybersecurity Teams

- Security Operations Center (SOC) Team.
- Governance, Risk, and Compliance (GRC) Team.
- Incident Response (IR) Team.
- Red Team.
- Blue Team.
- Network Security Team.
- Cloud Security Team.

SOC Team

SOC team is responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents in real time.



SOC Roles

SOC Analyst

Focus on monitoring and analyzing security incidents to protect the organization.

Threat Hunter

Proactively identifies and mitigates potential threats before they cause harm.

Incident Response

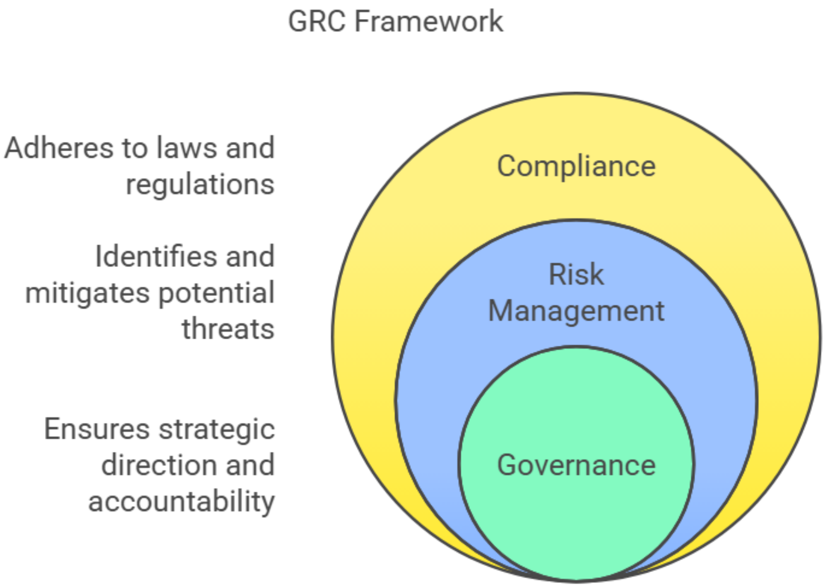
Quickly responds to and resolves security incidents to minimize impact.

SOC Manager

Oversees the security operations center to ensure effective security measures.

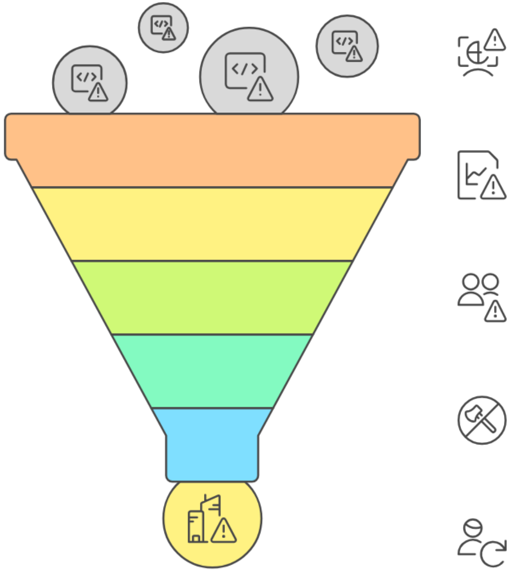
GRC Team

A GRC (Governance, Risk, and Compliance) team is responsible for ensuring that an organization operates in a controlled, compliant, and risk-aware manner.


GRC Framework
Adheres to laws and regulations
Identifies and mitigates potential threats
Ensures strategic direction and accountability
Compliance
Risk Management
Governance

Incident Response (IR) Team

IR minimize the impact of an attack and restore normal operations as quickly and efficiently as possible. A well-defined IRT is crucial for any organization, regardless of size.



Incident Response Team

Incident Detection
Identifying and acknowledging the cybersecurity threat

Assessment and Analysis
Evaluating the incident's scope and impact

Containment
Implementing measures to limit the incident's spread

Eradication
Removing the root cause of the incident

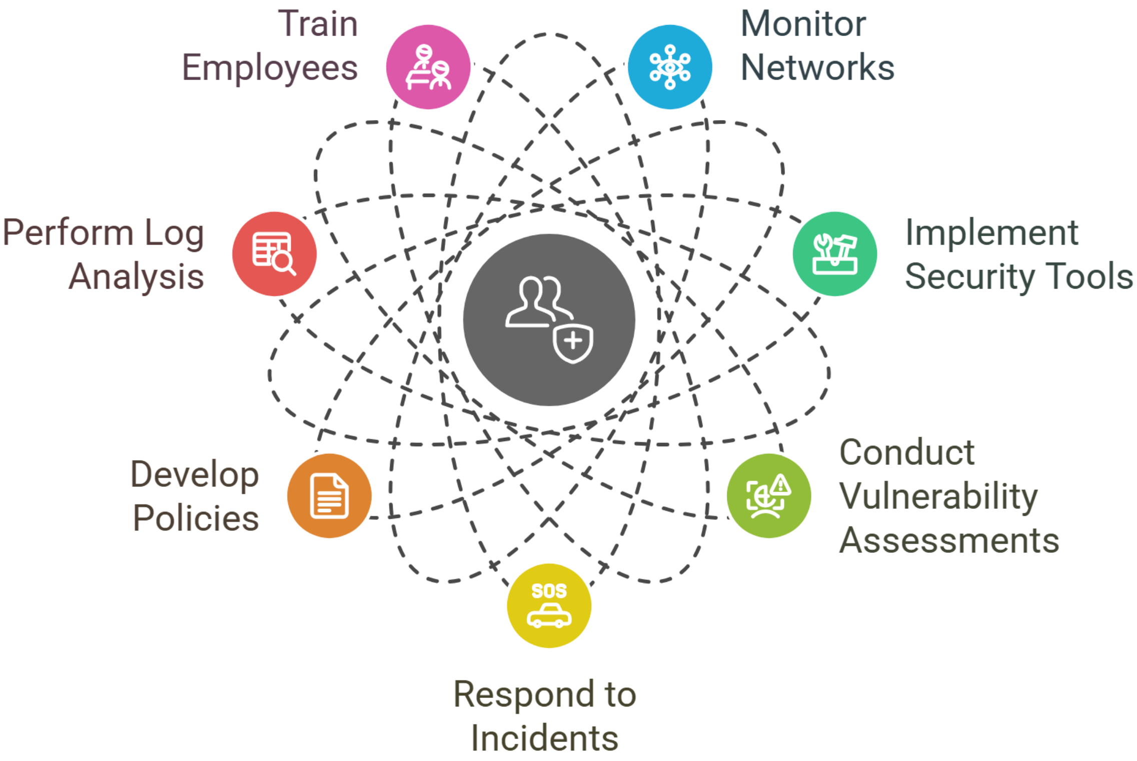
Recovery
Restoring systems to normal operations

Blue Team Vs Red Team

- **Role**: Defenders of the organization's systems, networks, and data.

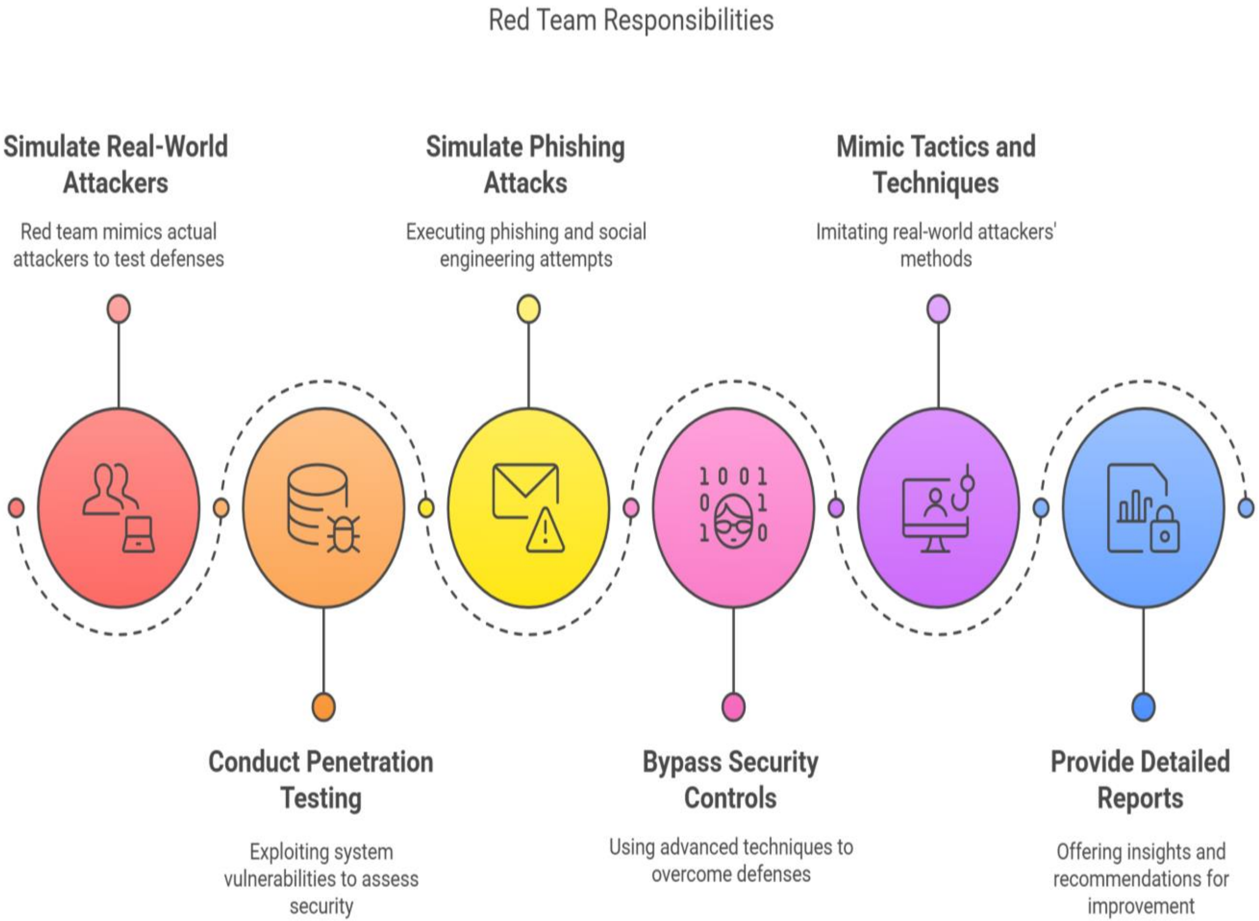
- **Objective**: Protect the organization from cyber threats and respond to incidents.

Blue Team Responsibilities



Blue Team Vs Red Team

- **Role**: Simulate real-world attackers to test the organization's defenses.
- **Objective**: Identify weaknesses in the organization's security by attempting to breach systems.



Red Team Responsibilities

Simulate Real-World Attackers
Red team mimics actual attackers to test defenses

Conduct Penetration Testing
Exploiting system vulnerabilities to assess security

Simulate Phishing Attacks
Executing phishing and social engineering attempts

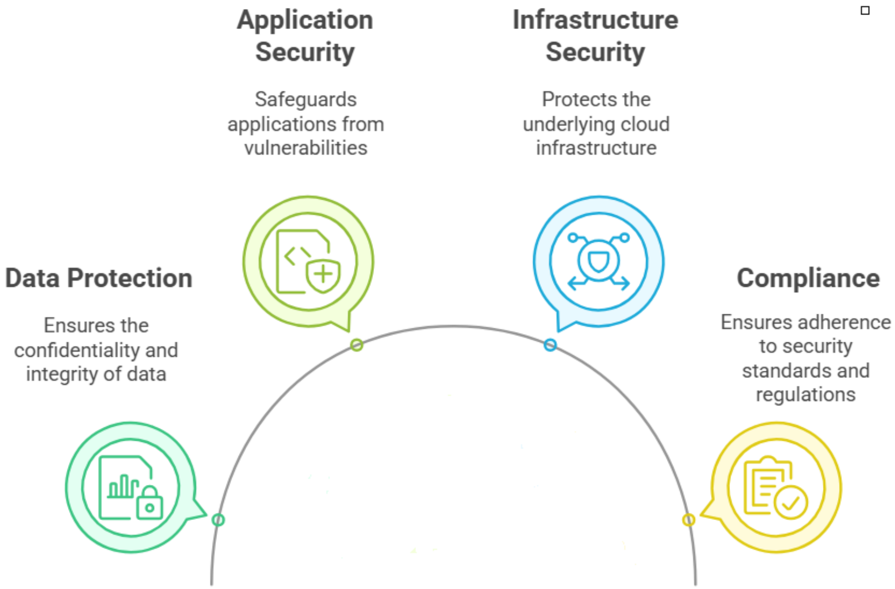
Bypass Security Controls
Using advanced techniques to overcome defenses

Mimic Tactics and Techniques
Imitating real-world attackers' methods

Provide Detailed Reports
Offering insights and recommendations for improvement

Cloud Security Team

- Cloud security team is responsible for protecting its data, applications, and infrastructure residing in cloud environments systems.



Application Security

Safeguards applications from vulnerabilities

Infrastructure Security

Protects the underlying cloud infrastructure

Data Protection

Ensures the confidentiality and integrity of data

Compliance

Ensures adherence to security standards and regulations

Common Cybersecurity tools

- **Red Team tools**
  - Metasploit and Cobalt Strike for penetration testing
  - Nessus and Nmap for Vulnerability Scanning
  - Burp Suite for Web application testing
  - John the Ripper for Passwork cracking
  - Aircrack-ng for cracking WiFi passwords

- **Blue Team Tools:**
  - Splunk, IBM Qradar for SIEM platforms
  - CrowdStrike Falcon and Carbon Black for EDR
  - Wireshark and TCPdump for packet analysis
  - VirusTotal for malware analysis

Thanks!

Do you have any questions?