(Cyber) Security Overview

Incident Response LIfecycle (NIST Framework)

The **NIST (National Institute of Standards and Technology)** defines a **6-phase** approach:

1. **Preparation**
   - Develop an incident response plan (IRP).
   - Train teams, conduct security awareness programs.
   - Implement security controls like firewalls, IDS/IPS.
2. **Identification**
   - Detect anomalies through logs, SIEM tools, and alerts.
   - Confirm if an incident has occurred (malware, data breach, DDoS).
   - Classify the severity and type of attack.
3. **Containment**
   - Stop the attack from spreading (isolate infected systems).
   - Implement temporary patches, disable compromised accounts.
   - Ensure forensic evidence is preserved.
4. **Eradication**
   - Remove the root cause of the incident (malware, vulnerabilities).
   - Apply permanent fixes, patch vulnerabilities.
   - Strengthen security measures.
5. **Recovery**
   - Restore affected systems from clean backups.
   - Monitor for lingering threats, ensure full functionality.
   - Reintegrate systems into production.
6. **Lessons Learned**
   - Conduct a post-mortem analysis of the incident.

- Document findings, update response plans.
- Improve security policies and employee training.

Threat Intelligence

(from incident to problem)

- reporting
- monitor new trends and techniques
- operational response: up-to-date (virus) protection
- research into new techniques.

Example Use Case

- A **financial institution** uses threat intelligence to monitor **new phishing campaigns** targeting its customers.
- The security team blocks malicious domains and updates email filtering rules.
- They prevent thousands of phishing attempts **before customers are impacted**.

Cryptography

Cryptography is the practice of securing information by **converting it into an unreadable format** to prevent unauthorized access. It ensures **confidentiality, integrity, authenticity, and non-repudiation** of data.

Key Concepts:

- **Encryption** – Converting plaintext into ciphertext (e.g., AES, RSA).
- **Decryption** – Reversing encryption to retrieve the original data.
- **Hashing** – Generating a fixed-length fingerprint of data (e.g., SHA-256).
- **Digital Signatures** – Verifying authenticity using cryptographic keys.
- **Key Exchange** – Securely sharing encryption keys (e.g., Diffie-Hellman).

Types of Cryptography:

1. **Symmetric Encryption** – Uses one key for both encryption and decryption (e.g., AES).

2. **Asymmetric Encryption** – Uses a public and a private key (e.g., RSA, ECC).

Uses in Cybersecurity:

- **Protects data in transit and at rest** (e.g., SSL/TLS for web security).
- **Secures passwords** (e.g., storing hashes instead of plaintext).
- **Enables secure authentication** (e.g., digital signatures).
- **Prevents data tampering** (e.g., message integrity checks).

Example: HTTPS encrypts web traffic using SSL/TLS, keeping user data safe from eavesdroppers.

Cryptography is essential for **privacy, secure communication, and data protection** in modern cybersecurity.

Network

OSI Model

The **OSI (Open Systems Interconnection) model** is a **7-layer framework** that standardizes communication in a network:

1. **Physical Layer** – Hardware, cables, and wireless signals.
2. **Data Link Layer** – MAC addresses, switches, and error detection.
3. **Network Layer** – IP addressing and routing.
4. **Transport Layer** – Reliable data transmission (TCP, UDP).
5. **Session Layer** – Managing communication sessions.
6. **Presentation Layer** – Encryption, compression, data formats.
7. **Application Layer** – User interactions (HTTP, FTP, DNS).

Relation to Cybersecurity:

- **Physical Layer** – Preventing physical tampering with devices.
- **Data Link Layer** – Protecting against MAC spoofing and ARP poisoning.
- **Network Layer** – Firewalls, IP filtering, and VPNs.
- **Transport Layer** – Preventing DDoS attacks, ensuring encryption (TLS).
- **Session Layer** – Secure authentication and session hijacking protection.
- **Presentation Layer** – Implementing SSL/TLS encryption.

- **Application Layer** – Web security (XSS, SQL injection, authentication).

Revision #1
Created 2025-02-19 09:06:53 UTC by Max
Updated 2025-02-19 09:30:21 UTC by Max