**Security protection usually adopts Defense in Depth, which mainly includes the following layers:**

**1. Physical security: access control, biometrics, surveillance cameras, etc.2. Network security: firewalls, VPNs, intrusion detection systems (IDS/IPS).3. Terminal security: antivirus software, patch management, EDR.4. Application security: secure coding, WAF, penetration testing.**

**5. Data security: encryption, access control, data loss prevention (DLP).6. Identity and access management (IAM): multi-factor authentication (MFA), zero trust.**

**7. Security monitoring and response: log analysis, incident response, SOC monitoring.**

**Multi-layer protection ensures that even if one layer is breached, other layers can still provide protection.**

**There are several types of cyberattacks, including:**

**1.Malware – Viruses, worms, ransomware, and spyware that infect systems.**

**2.Phishing – Deceptive emails or messages trick users into revealing credentials.**

**3.Denial of Service (DoS/DDoS) – Overloading a system to make it unavailable.**

**Man-in-the-Middle (MitM) – Intercepting communication between two parties.**

**4.SQL Injection – Exploiting database vulnerabilities to gain unauthorized access.**

**5.Zero-Day Exploits – Attacks targeting unknown software vulnerabilities.**

**6.Brute Force Attacks – Repeatedly guessing passwords to gain access.**

**The CIA Triad is a fundamental model in cybersecurity, representing three key principles:**

**1.Confidentiality – Ensures that data is accessible only to authorized individuals (e.g., encryption, access controls).**

**2.Integrity – Ensures data is accurate, complete, and unaltered (e.g., hashing, checksums).**

**3.Availability – Ensures data and services are accessible when needed (e.g., redundancy, DDoS protection).**

**Risk Mitigation**

**Risk mitigation involves implementing strategies to reduce security risks. 1.Avoidance – Eliminating risky activities.**

**2.Reduction – Implementing security controls (e.g., firewalls, MFA).**

**3.Transfer – Shifting risk to a third party (e.g., cybersecurity insurance).**

**4.Acceptance – Acknowledging and managing low-risk scenarios.**

**Risk Assessment Activities**

**Risk assessment identifies, analyzes, and prioritizes risks.**

**1.Identify Assets & Threats – Determine valuable data and potential risks.2.Analyze Vulnerabilities – Assess weak points in systems.**

**3.Evaluate Impact & Likelihood – Determine potential consequences and chances of occurrence.**

**4.Implement Controls – Apply security measures to reduce risk.**

**5.Monitor & Review – Continuously assess and update security strategies.**

**Effective risk management enhances cybersecurity resilience.**

**A cryptographic system is a set of methods and protocols used to secure data through encryption and decryption. It ensures Confidentiality, Integrity, and Authentication (CIA Triad). Key components include:**

**1. Encryption Types**

**Symmetric Encryption – Uses the same key for encryption and decryption (e.g., AES, DES).**

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

**2. Cryptographic Functions**

**Hashing – Converts data into a fixed-length hash (e.g., SHA-256, MD5).**

**Digital Signatures – Ensures authenticity and integrity (e.g., RSA, DSA).**

**Key Exchange – Securely shares encryption keys (e.g., Diffie-Hellman).**

**Cryptographic systems protect sensitive data in communication, storage, and authentication processes.**

**A Network Intrusion Detection System (NIDS) monitors network traffic for malicious activity or security policy violations.**

**How NIDS Works**

**1.Traffic Monitoring – Analyzes packets in real time.**

**2.Signature-Based Detection – Matches known attack patterns.**

**3.Anomaly-Based Detection – Identifies deviations from normal behavior.**

**Common NIDS Tools**

**Snort – Open-source, widely used.**

**Suricata – High-performance alternative.**

**Zeek (Bro) – Focuses on deep packet analysis.**

**Intrusion Detection Systems (IDS) use different detection methods to identify threats:**

**1. Signature-Based Detection**

**Compares network traffic to known attack patterns (signatures).**

**Pros: Accurate for known threats.**

**Cons: Ineffective against new or unknown attacks (zero-days).**

**Example: Snort, Suricata.**

**2. Anomaly-Based Detection**

**Establishes a baseline of normal behavior and flags deviations.**

**Pros: Can detect unknown or zero-day attacks.**

**Cons: High false positive rates.**

**Example: Machine learning-based IDS.**

**3. Hybrid Detection**

**Combines signature and anomaly-based methods for better accuracy.**

**Pros: Balances detection capabilities and reduces false positives.**

**Cons: More complex to implement.**

**A honeypot is a decoy system designed to attract cyber attackers and study their behavior. It helps improve security by detecting threats and gathering intelligence.**

**Types of Honeypots**

**1.Low-Interaction Honeypots – Simulate basic services with minimal risk (e.g., Honeyd).**

**2.High-Interaction Honeypots – Mimic real systems, allowing deeper attack analysis (e.g., Honeynet).**

**Benefits of Honeypots**

**1.Detects new attack techniques.**

**2.Diverts attackers from real systems.**

**3.Helps in cybersecurity research and threat intelligence.**

**1) Difference Between HIDS and NIDS**

**HIDS (Host-based IDS): Monitors activities on a specific host, like file changes and system logs. It's installed directly on devices and focuses on internal threats or attacks targeting the host.**

**NIDS (Network-based IDS): Monitors network traffic across multiple devices to detect suspicious patterns. It's deployed at network points and identifies external threats affecting the entire network.**

**2) How IDS Enhances Security Management**

**An IDS improves security by detecting threats in real-time, analyzing traffic for anomalies, and alerting administrators to take action. It also logs events for analysis, helping organizations respond to and prevent future attacks.**

**Difference Between DoS and DDoS**

**Definition:**

**DoS (Denial of Service): An attack that makes a computer resource or network service unavailable by overwhelming it with traffic or requests from a single source.**

**DDoS (Distributed Denial of Service): An attack that uses multiple systems (often a botnet) to flood a target with traffic from different locations, increasing the attack's impact and making it harder to trace.**

**Method:**

**DoS: Usually originates from a single machine or a few machines.**

**DDoS: Involves many devices to create a larger and more sustained impact.**

**Impact:**

**DoS: Less damaging due to fewer resources.**

**DDoS: More impactful due to the combined power of many devices, making it harder to mitigate.**