**Cybersecurity Threats & Attacks Cheatsheet**

**1. Attack Categories & Methods**

**A. Data Exfiltration (Data Theft)**

* **Definition**: Unauthorized transfer of sensitive data from a system.
* **Common Methods**:
  + **Malware-based Exfiltration** (Trojan, Keyloggers)
  + **Insider Threats** (Employees stealing data)
  + **Command & Control (C2) Channels** (Hidden data transmission via DNS, HTTP, FTP)
  + **Cloud Storage Abuse** (Unauthorized upload of sensitive files)
  + **Steganography** (Hiding data in images, audio, or video)
  + **Encrypted Tunnels** (Using VPNs or TOR for stealthy data transfer)
* **Mitigation Strategies**:
  + Implement **Data Loss Prevention (DLP)** tools.
  + Restrict **USB, clipboard, and email** data transfers.
  + Monitor **network traffic anomalies** (unusual outbound data spikes).
  + Enforce **least privilege access** (zero-trust policies).
  + Use **encryption** and **endpoint detection & response (EDR)** solutions.

**B. Malware Attacks**

* **Ransomware**: Encrypts files, demands ransom (e.g., WannaCry, LockBit).
* **Trojans**: Disguised as legitimate software to execute malicious actions.
* **Spyware/Keyloggers**: Captures keystrokes and user activity.
* **Mitigation**: Use **endpoint protection, sandboxing, and behavioral monitoring**.

**C. Phishing & Social Engineering**

* **Spear Phishing**: Targeted attacks impersonating trusted entities.
* **Whaling**: High-value targets (e.g., executives).
* **Business Email Compromise (BEC)**: CEO fraud, fake invoice scams.
* **Mitigation**: Implement **email filtering, multi-factor authentication (MFA), and user training**.

**D. Denial-of-Service (DoS) & Distributed DoS (DDoS)**

* **Volumetric Attacks**: Overloading bandwidth (e.g., UDP Flood, SYN Flood).
* **Application Layer Attacks**: Targeting web services (e.g., HTTP Flood).
* **Mitigation**: Deploy **WAF, rate-limiting, CDN, and anomaly-based detection**.

**E. Network Attacks**

* **Man-in-the-Middle (MITM)**: Intercepting communications (e.g., ARP spoofing).
* **DNS Spoofing**: Redirecting users to malicious websites.
* **Mitigation**: Use **TLS encryption, DNSSEC, and VPNs**.

**F. Cloud Security Threats**

* **Misconfigurations**: Publicly exposed storage (e.g., open S3 buckets).
* **Insider Threats**: Unauthorized cloud data access.
* **Mitigation**: Enable **cloud monitoring, identity & access management (IAM), and compliance checks**.

**2. Cybersecurity Detection & Prevention Strategies**

| **Attack Type** | **Detection Methods** | **Prevention Strategies** |
| --- | --- | --- |
| **Data Exfiltration** | Traffic analysis, anomaly detection, endpoint monitoring | DLP, EDR, behavior analytics |
| **Ransomware** | File integrity checks, heuristic analysis | Backup strategy, zero-trust security |
| **Phishing** | Email filtering, domain monitoring | MFA, security awareness training |
| **DDoS** | Anomaly-based detection, rate-limiting | WAF, CDN, geo-blocking |
| **MITM** | Packet inspection, SSL stripping detection | TLS 1.3, VPN, HSTS |