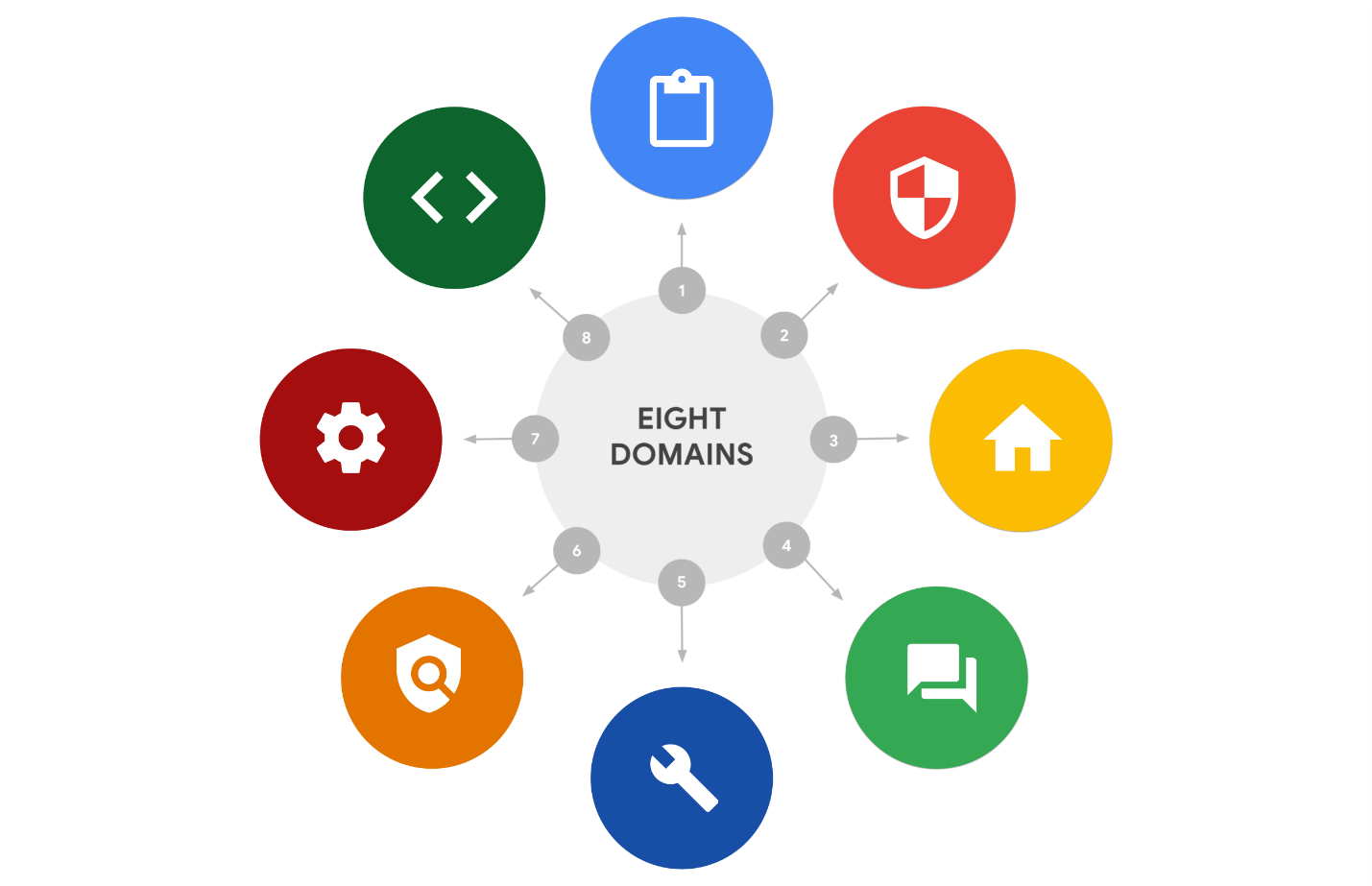
**Determining the Type of Attack**



**Common Types of Cyber Attacks**

1. **Malware**
   * **Definition**: Malicious software designed to harm or exploit any programmable device, service, or network.
   * **Examples**:
     + **Ransomware**: Encrypts data and demands payment for decryption.
     + **Fileless Malware**: Uses legitimate tools built into a system to execute attacks without installing code.
     + **Spyware**: Collects information about a user’s activities without their knowledge.
     + **Adware**: Displays unwanted ads and can degrade device performance.
     + **Trojans**: Disguised as legitimate software to gain access to systems.
     + [**Worms**: Self-replicating malware that spreads without user initiation](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/)[1](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
2. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks**
   * **Definition**: Overwhelm a system’s resources, making it unable to respond to legitimate requests.
   * **Examples**:
     + **DoS Attack**: Floods a target with illegitimate requests.
     + [**DDoS Attack**: Uses multiple compromised systems to launch the attack](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/)[2](https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks).
3. **Phishing**
   * **Definition**: Use of digital communications to trick individuals into revealing sensitive information.
   * **Examples**:
     + **Business Email Compromise (BEC)**: Emails from known sources requesting information for financial gain.
     + **Spear Phishing**: Targets specific individuals or groups.
     + **Whaling**: Targets high-profile individuals like executives.
     + **Vishing**: Uses voice communication to obtain sensitive information.
     + [**Smishing**: Uses text messages to trick users](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/)[1](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
4. **Man-in-the-Middle (MITM) Attacks**
   * **Definition**: Attacker intercepts and alters communication between two parties.
   * **Examples**:
     + **Eavesdropping**: Attacker listens to private conversations.
     + [**Session Hijacking**: Attacker takes control of a user’s session](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/)[2](https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks).
5. **Social Engineering**
   * **Definition**: Manipulation technique exploiting human error to gain private information or access.
   * **Examples**:
     + **Social Media Phishing**: Collects information from social media to initiate attacks.
     + **Watering Hole Attack**: Targets websites frequently visited by specific groups.
     + **USB Baiting**: Leaves malware-infected USB sticks for employees to find.
     + [**Physical Social Engineering**: Impersonates employees or vendors to gain access](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/)[1](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
6. **Code Injection Attacks**

* **Definition**: Inserting malicious code into a program to alter its execution.
* **Examples**:
  + - **SQL Injection**: Injects malicious SQL code to manipulate databases.
    - [**Cross-Site Scripting (XSS)**: Injects malicious scripts into web pages](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/)[1](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).

1. **Identity-Based Attacks**
   * **Definition**: Exploiting user identities to gain unauthorized access.
   * **Examples**:
     + **Credential Stuffing**: Using stolen credentials to access accounts.
     + [**Brute Force Attack**: Trying multiple passwords to gain access](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/)[1](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
2. **Supply Chain Attacks**
   * **Definition**: Targeting less secure elements in the supply chain to compromise a system.
   * **Examples**:
     + **Third-Party Software**: Compromising software from third-party vendors.
     + [**Hardware Attacks**: Inserting malicious hardware components](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/)[1](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).

**Analyzing Potential Indicators to Determine the Type of Attack**

1. **Unusual Network Traffic**: Sudden spikes in network traffic can indicate DoS or DDoS attacks.
2. **Unauthorized Access Attempts**: Multiple failed login attempts may suggest brute force attacks.
3. **Unexpected System Behavior**: Slow performance or frequent crashes can be signs of malware.
4. **Phishing Emails**: Suspicious emails requesting sensitive information can indicate phishing attacks.
5. **Altered Communication**: Intercepted or altered communication can point to MITM attacks.
6. **Unusual File Changes**: Unexpected changes in files or configurations may indicate code injection attacks.

By understanding these indicators and attack types, you can better protect systems and respond to potential threats effectively.