Cyber Kill Chain

SUBMITTED BY
AHALIYA S
CSA JAN 2024

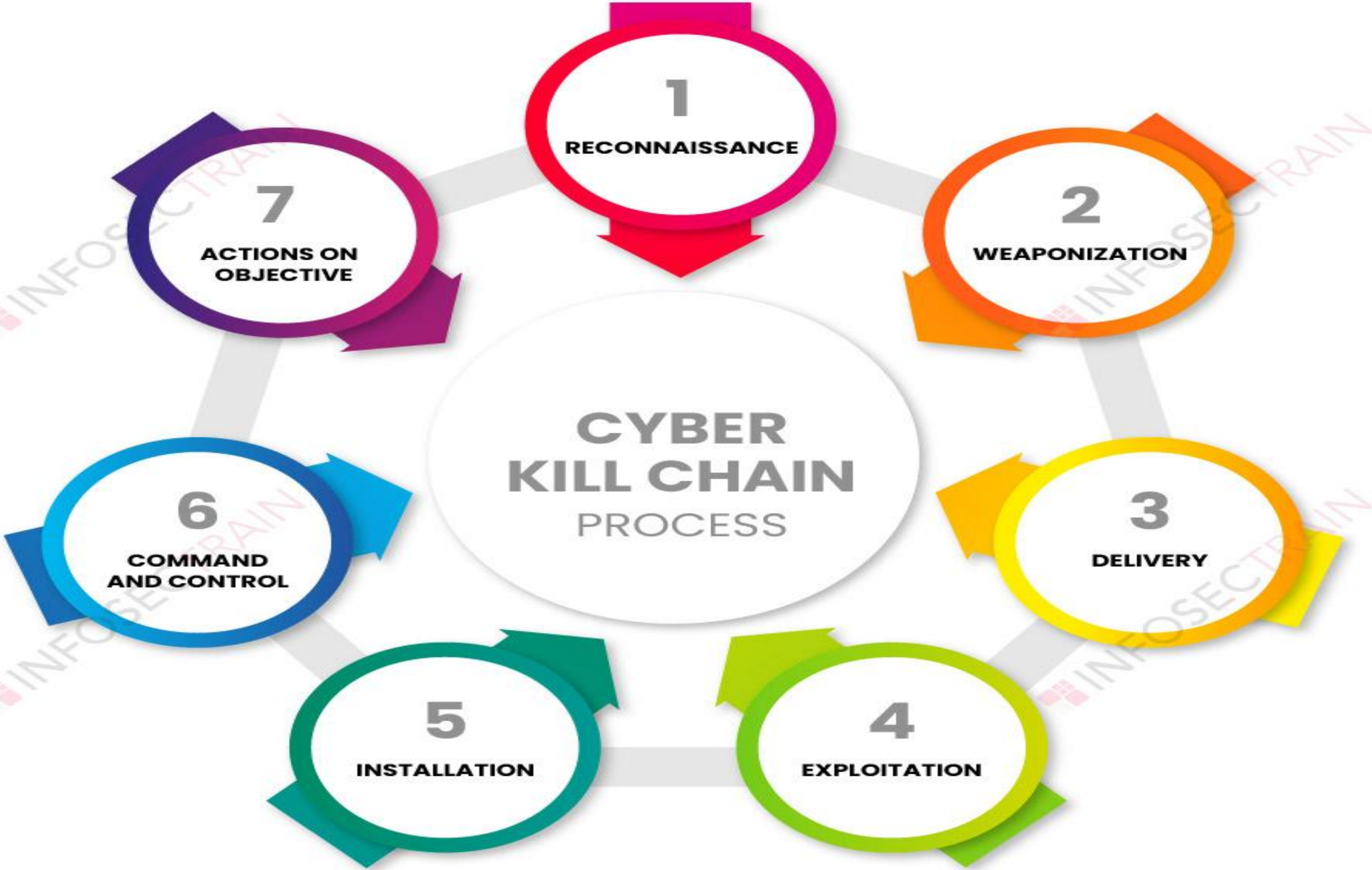
Introduction to the Cyber Kill Chain Concept

Understanding the Anatomy of Cyber Attacks

Cyber Kill Chain

- The Cyber Kill Chain is a concept developed by Lockheed Martin to illustrate the stages of a cyber attack, from initial reconnaissance to achieving the attacker's objectives.
- Importance:
  a. Understanding the Cyber Kill Chain helps organizations comprehend the lifecycle of cyber threats and develop effective defense strategies.
  b. It provides a framework for analyzing and mitigating cyber threats by breaking down attacks into distinct stages.

- Brief Overview:
  - The Cyber Kill Chain consists of seven stages, each representing a crucial step in the progression of a cyber attack.
  - By identifying and disrupting attacks at any stage of the kill chain, organizations can significantly enhance their cybersecurity posture.


1
RECONNAISSANCE
2
WEAPONIZATION
3
DELIVERY
4
EXPLOITATION
5
INSTALLATION
6
COMMAND AND CONTROL
7
ACTIONS ON OBJECTIVE
CYBER KILL CHAIN PROCESS

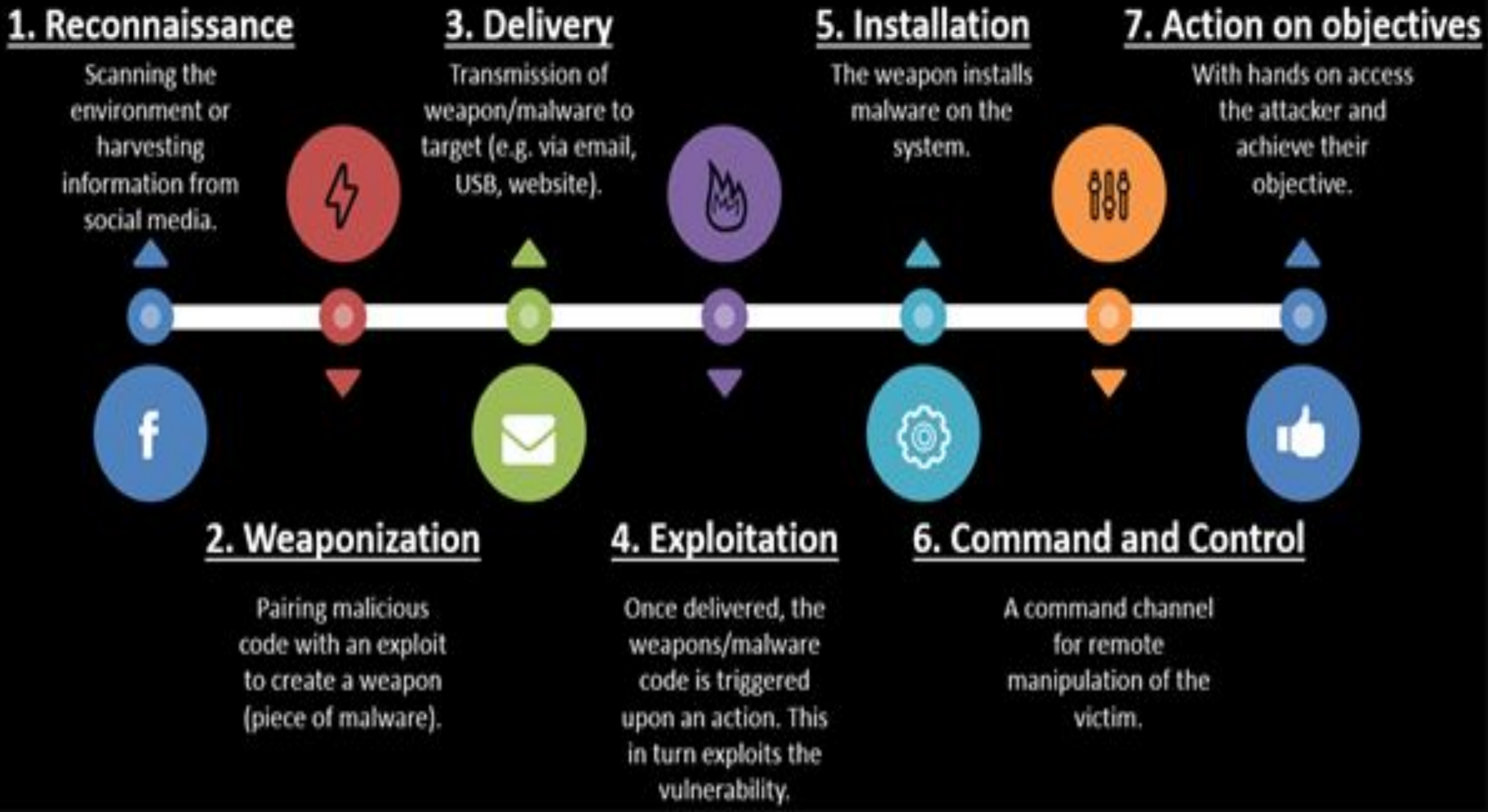
What is the Cyber Kill Chain?

Understanding the Anatomy of Cyber Attacks

What is the Cyber Kill Chain?

- The Cyber Kill Chain is a strategic framework developed by Lockheed Martin to describe the stages of a cyber attack lifecycle. It delineates the steps that adversaries typically follow to infiltrate and exploit a target network or system.
- Origin and Purpose:
    a. Origin: The concept of the Cyber Kill Chain originated from military doctrine, specifically the "kill chain" concept used in military operations.
    b. Purpose: The Cyber Kill Chain was adapted for cybersecurity to provide organizations with a systematic approach to understanding and defending against cyber threats. It aims to break down the complex process of cyber attacks into discrete stages, enabling organizations to identify and disrupt attacks at various points in the kill chain.

Kill Chain: The 7 Stages of a Cyber Attack



1. Reconnaissance

Scanning the environment or harvesting information from social media.

2. Weaponization

Pairing malicious code with an exploit to create a weapon (piece of malware).

3. Delivery

Transmission of weapon/malware to target (e.g. via email, USB, website).

4. Exploitation

Once delivered, the weapons/malware code is triggered upon an action. This in turn exploits the vulnerability.

5. Installation

The weapon installs malware on the system.

6. Command and Control

A command channel for remote manipulation of the victim.

7. Action on objectives

With hands on access the attacker and achieve their objective.

Stages of the Cyber Kill Chain

Understanding the Sequential Progression of Cyber Attacks

Breakdown of the Seven Stages

- The Cyber Kill Chain consists of seven distinct stages, each representing a crucial step in the progression of a cyber attack. These stages are:
    - Reconnaissance
    - Weaponization
    - Delivery
    - Exploitation
    - Installation
    - Command and Control
    - Actions on Objectives
- Explanation of Each Stage:
    - Reconnaissance: Attackers gather information about the target, including identifying vulnerabilities and potential entry points.
    - Weaponization: Malicious tools or payloads are developed or acquired and combined with exploit techniques.
    - Delivery: The weaponized payload is delivered to the target, often through methods like phishing emails or drive-by downloads.
    - Exploitation: Vulnerabilities in the target system are exploited to execute the payload and gain initial access.
    - Installation: The attacker establishes a foothold within the target environment by installing backdoors or malware.
    - Command and Control: The attacker sets up communication channels to control compromised systems and exfiltrate data.
    - Actions on Objectives: The attacker achieves their ultimate goals, which may include data theft, sabotage, or further compromise of systems.

Stage 1 - Reconnaissance

1. Description of the Reconnaissance Stage:
   - The reconnaissance stage is the initial phase of the Cyber Kill Chain where attackers gather intelligence about their target. This involves identifying potential vulnerabilities, discovering system configurations, and mapping out the target's infrastructure.
2. Examples of Reconnaissance Activities:
   - Network Scanning: Scanning the target network to identify active hosts, open ports, and services running on those ports.
   - Social Engineering: Gathering information about employees, organizational structure, and security policies through social media or phishing attacks.
   - OSINT (Open Source Intelligence) Gathering: Collecting publicly available information about the target from sources such as websites, forums, and social media platforms.

Stages 2 and 3 - Weaponization and Delivery

1. Explanation of Weaponization and Delivery Stages:
   - Weaponization: The weaponization stage involves crafting or acquiring malicious payloads, such as malware or exploit kits, and combining them with delivery mechanisms.
   - Delivery: In the delivery stage, the weaponized payloads are transmitted to the target environment, typically through methods like email attachments, malicious links, or compromised websites.
2. Examples and Techniques Used in These Stages:
   - Weaponization Techniques: Exploiting vulnerabilities in software, creating custom malware, or repurposing existing tools for malicious purposes.
   - Delivery Methods: Phishing emails, drive-by downloads, watering hole attacks, and malicious advertisements are commonly used delivery methods.

Stages 4 and 5 - Exploitation and Installation

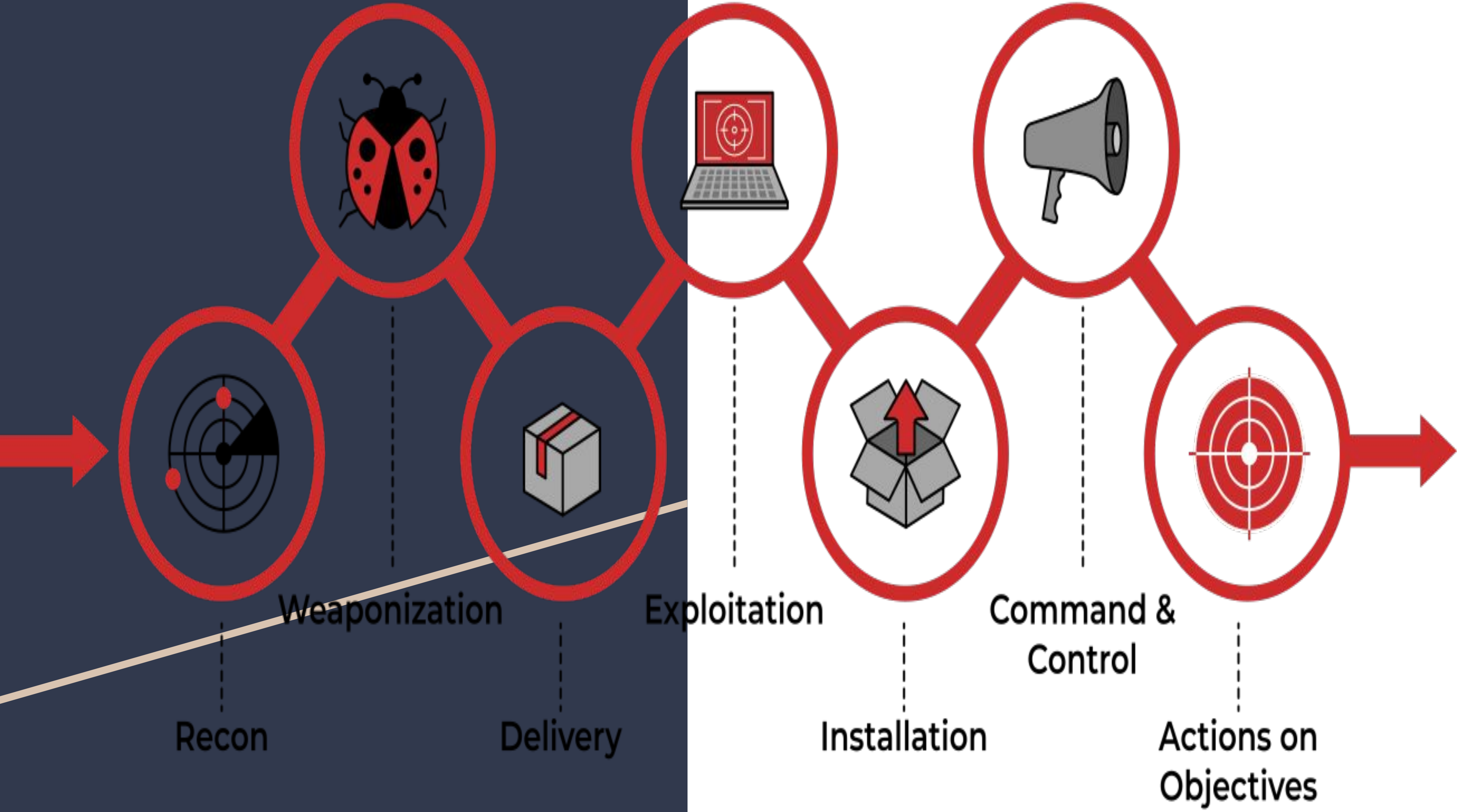
1. Description of Exploitation and Installation Stages:
   - Exploitation: Exploitation involves leveraging vulnerabilities in the target system to gain unauthorized access. This may include exploiting software bugs, misconfigurations, or weak authentication mechanisms.
   - Installation: In the installation stage, attackers establish a persistent presence within the target environment by deploying backdoors, rootkits, or other forms of malware.
2. Examples and Techniques Used in These Stages:
   - Exploitation Techniques: SQL injection, buffer overflow, remote code execution, and privilege escalation are common exploitation techniques.
   - Installation Methods: Dropping and executing malware, creating new user accounts, or modifying system configurations to maintain access.

Stage 6 - Command and Control

1. Explanation of the Command and Control Stage:
    - The command and control (C2) stage involves establishing communication channels between the attacker and compromised systems. This allows attackers to remotely control and manage compromised infrastructure.
2. Examples of Command and Control Infrastructure:
    - Botnets: Networks of compromised devices controlled by a central command server.
    - Remote Access Trojans (RATs): Malicious software that enables remote control and surveillance of compromised systems.
    - Domain Generation Algorithms (DGA): Techniques used to generate dynamic domain names for evading detection.

Stage 7 - Actions on Objectives

1. Description of the Actions on Objectives Stage:
   - In the actions on objectives stage, attackers execute their intended goals, which may include data exfiltration, system manipulation, or disruption of operations.
2. Examples of Objectives Attackers Seek to Achieve:
   - Data Theft: Stealing sensitive information such as financial records, intellectual property, or personal data.
   - System Compromise: Compromising systems to gain persistence, escalate privileges, or sabotage operations.
   - Disruption: Disrupting services, causing downtime, or defacing websites for political or ideological reasons.


Recon
Weaponization
Delivery
Exploitation
Installation
Command & Control
Actions on Objectives

Conclusion

1. Recap of the Cyber Kill Chain Stages:
   - Summarize the seven stages of the Cyber Kill Chain and their significance in understanding and defending against cyber attacks.
2. Importance of Understanding and Defending Against Each Stage:
   - Emphasize the importance of comprehensively analyzing and addressing vulnerabilities and threats at each stage to enhance cybersecurity posture and resilience.
3. Call to Action for Implementing Cybersecurity Measures:
   - Encourage organizations to implement cybersecurity measures based on the Cyber Kill Chain framework, such as threat intelligence, intrusion detection, and incident response capabilities.