Task 13

CYBER KILL CHAIN

Prepared By : S Divya

WHAT IS CYBER KILL CHAIN

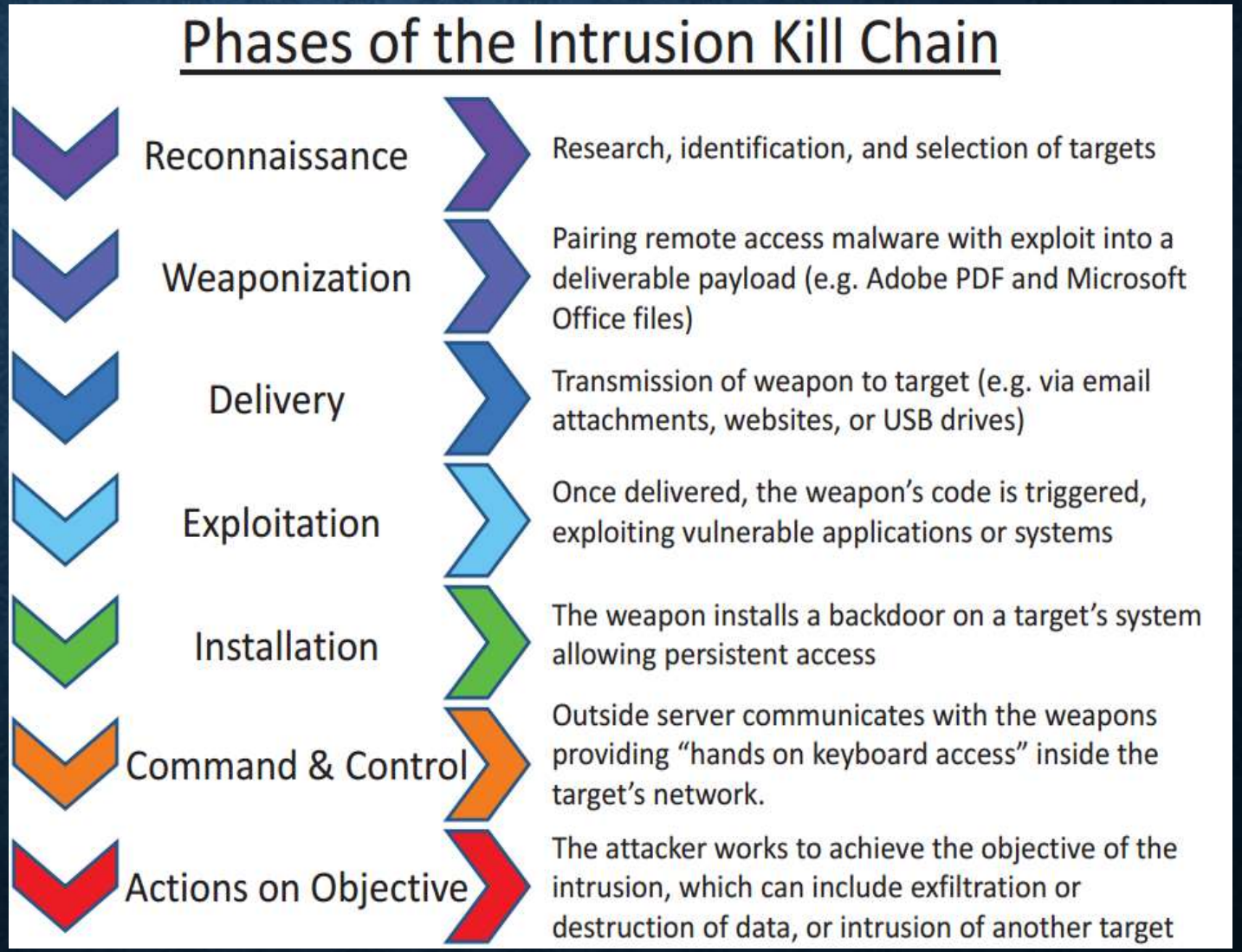
- The cyber kill chain is a model that outlines the stages of a cyberattack, from initial reconnaissance to data exfiltration, helping security teams understand and defend against sophisticated attacks.
- The cyber kill chain is a cybersecurity model that breaks down a typical cyberattack into stages to help security teams identify in-progress cyberattacks and stop them.
- Its purpose is to help organizations understand and defend against cyber threats.
- It is widely used by cybersecurity professionals to understand prevent, and repond to cyber threats.
- It was developed by Lockheed Martin.

Importance of the Cyber Kill Chain

- Proactive Defense: It helps identify attack stages early.
- Mitigation: It allows for focused defensive measures at each phase.
- Incident Response: Improves response to ongoing attacks.

OVERVIEW OF THE SEVEN STAGES

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Action on Objectives



STAGES OF THE CYBER KILL CHAIN

1. Reconnaissance

The cyber kill chain defines a sequence of cyberattack phases with the goal of understanding the mindset of cyber attackers, including their motives, tools, methods, and techniques, how they make decisions, and how they evade detection. Understanding how the cyber kill chain works helps defenders stop cyberattacks in the earliest stages.

2. Weaponization

During the weaponization phase, bad actors use the information uncovered during reconnaissance to create or modify malware to best exploit the targeted organization's weaknesses.

3. Delivery

Once they've built malware, cyber attackers attempt to launch their attack. One of the most common methods is using social engineering techniques such as phishing to trick employees into handing over their sign-in credentials. Bad actors may also gain entry by taking advantage of a public wireless connection that isn't very secure or exploiting a software or hardware vulnerability uncovered during reconnaissance.

4. Exploitation

After cyberthreat actors infiltrate the organization, they use their access to move laterally from system to system. Their goal is to find sensitive data, additional vulnerabilities, administrative accounts, or email servers that they can use to inflict damage on the organization.

5. Installation

In the installation stage, bad actors install malware that gives them control of more systems and accounts.

6. Command and control

After cyberattackers have gained control of a significant number of systems, they create a control center that allows them to operate remotely. During this stage they use obfuscation to cover their tracks and avoid detection. They also use denial-of-service attacks to distract security professionals from their true objective.

7. Actions on objectives

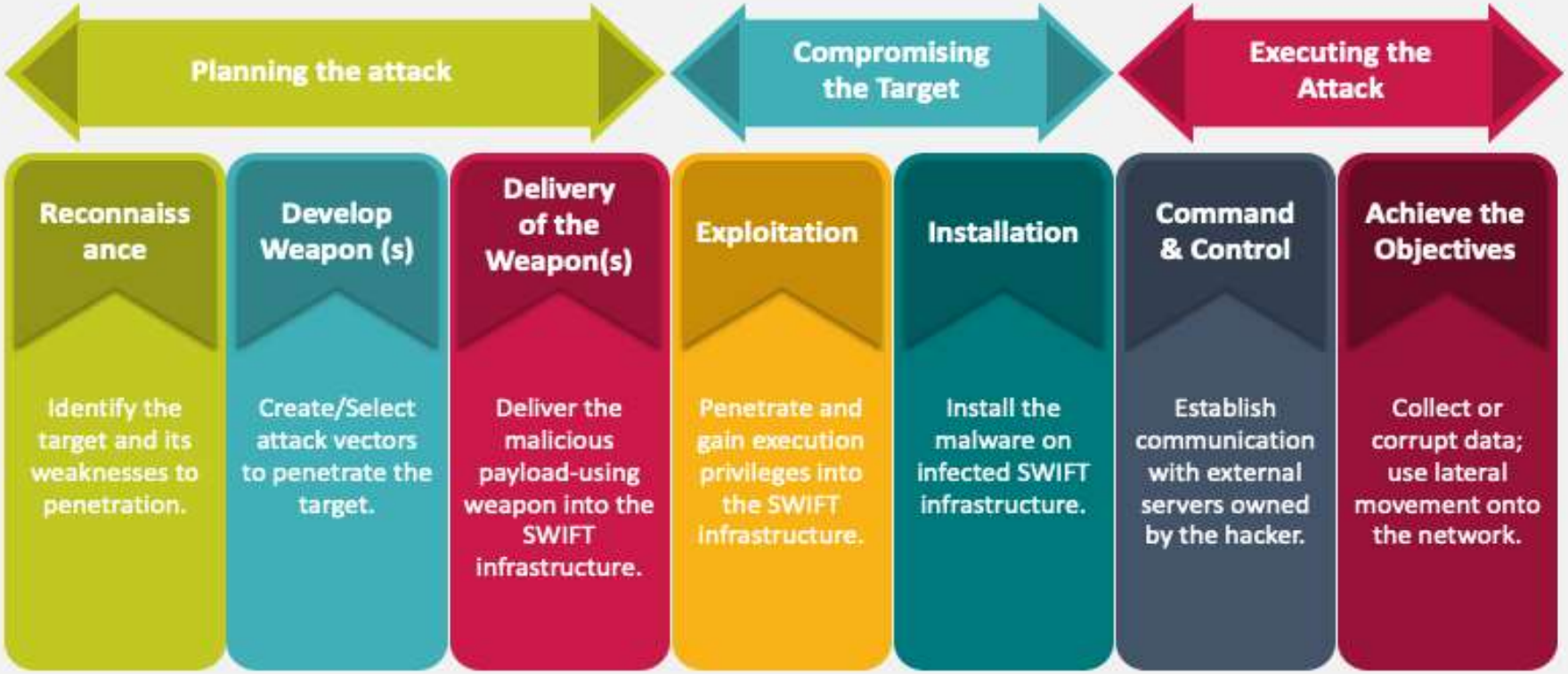
In this stage, cyberattackers take steps to achieve their primary goal, which could include supply chain attacks, data exfiltration, data encryption, or data destruction.

8. Monetization

This include for the activities bad actors take to generate income from the attack, such as using ransomware to extract a payment from their victims or selling sensitive data on the dark web.

CYBER KILL CHAIN

Cyber Kill Chain Activities



ATTACKS BASED ON EACH STEPS OF CYBER KILL CHAIN

- Reconnaissance : In this stage,attackers gather information about the target organization, its systems, and potential vulnerabilities. Examples of attack at this stage include Phishing, Social Engineering.

- Weaponization : In this stage attackers create or obtain a malicious payload such as a virus or Trojan horse and prepare to deliver it to the target designed to exploit identified vulnerabilities. (e.g., Malware, Exploit Kit)

- **Delivery :** In this stage the weaponized payload is delivered to the target, often through phishing emails, compromised websites, or other vectors. Examples of attacks at this stage include Email attacks and Drive by downloads.

- **Exploitation :** In this stage the payload is executed on the target system or network, exploiting vulnerabilities to gain access and establish a foothold in the system. Examples of attacks at this stage include SQL Injection, Remote code execution.

- **Installation** : In this stage attackers install malware or other tools to maintain access and control over the compromised system. Examples of attacks at this stage include Backdoors, Rootkits

- **Command and Control (C2)** : In this stage attackers establish a Command-and-Control (C&C) channel to communicate with the compromised system and issue commands. Examples of attacks at this stage include Botnets, Remote access trojans (RATs).

- **Action on Objectives** : In this stage attackers achieve their ultimate goal such as stealing data, disrupting operations, or causing damage to the system. Examples of attacks at this stage include Data theft and Ransomware.

IMPACT OF THE CYBER KILL CHAIN ON CYBERSECURITY

- Understanding how cyberthreat actors plan and conduct their attacks helps cybersecurity professionals find and mitigate vulnerabilities across the organization.
- It also helps them identify indicators of compromise during the early stages of a cyberattack.
- Many organizations use the cyber kill chain model to proactively put security measures in place and to guide incident response.

Benefits of the cyber kill chain model

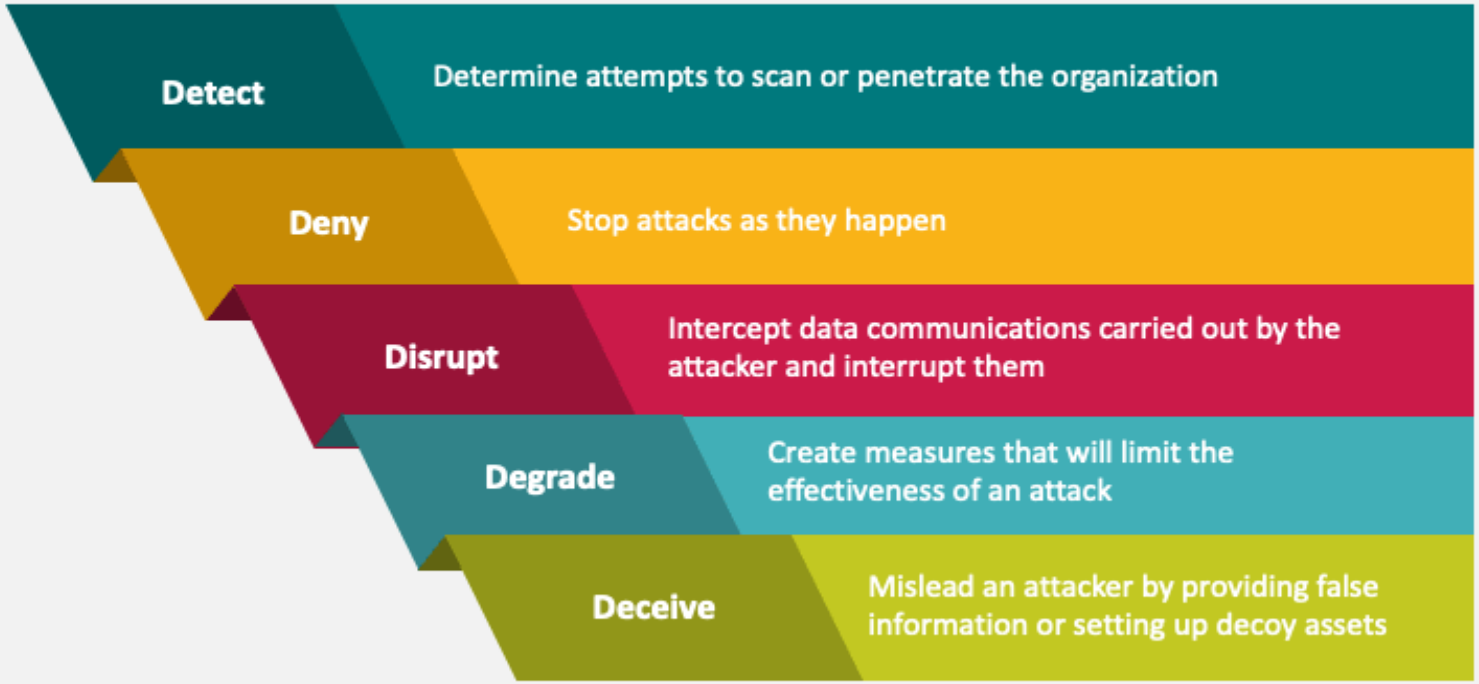
- Identify threats at every stage of the cyber kill chain.
- Make it harder for unauthorized users to gain access.
- Harden privileged accounts, data, and systems.
- Uncover and respond quickly to lateral movement.
- Stop in-progress cyberattacks.

HOW TO IMPLEMENT CYBER KILL CHAIN MODEL

- Implementing the cyber kill chain model starts with analyzing each stage of the model as it relates to the affected organization. This will help security teams identify vulnerabilities and areas of greatest risk.
- Once an organization knows what to prioritize, the following strategies and tools can help security teams detect and respond to sophisticated cyberthreats :-
- Develop an end-to-end threat intelligence program.
- Implement a SIEM solution.
- Deploy an XDR solution.
- Use a unified SecOps platform that includes an XDR solution and a SIEM solution in one platform.
- Put in place comprehensive identity and access management.
- Run regular security training for all employees.
- Develop incident response playbooks.

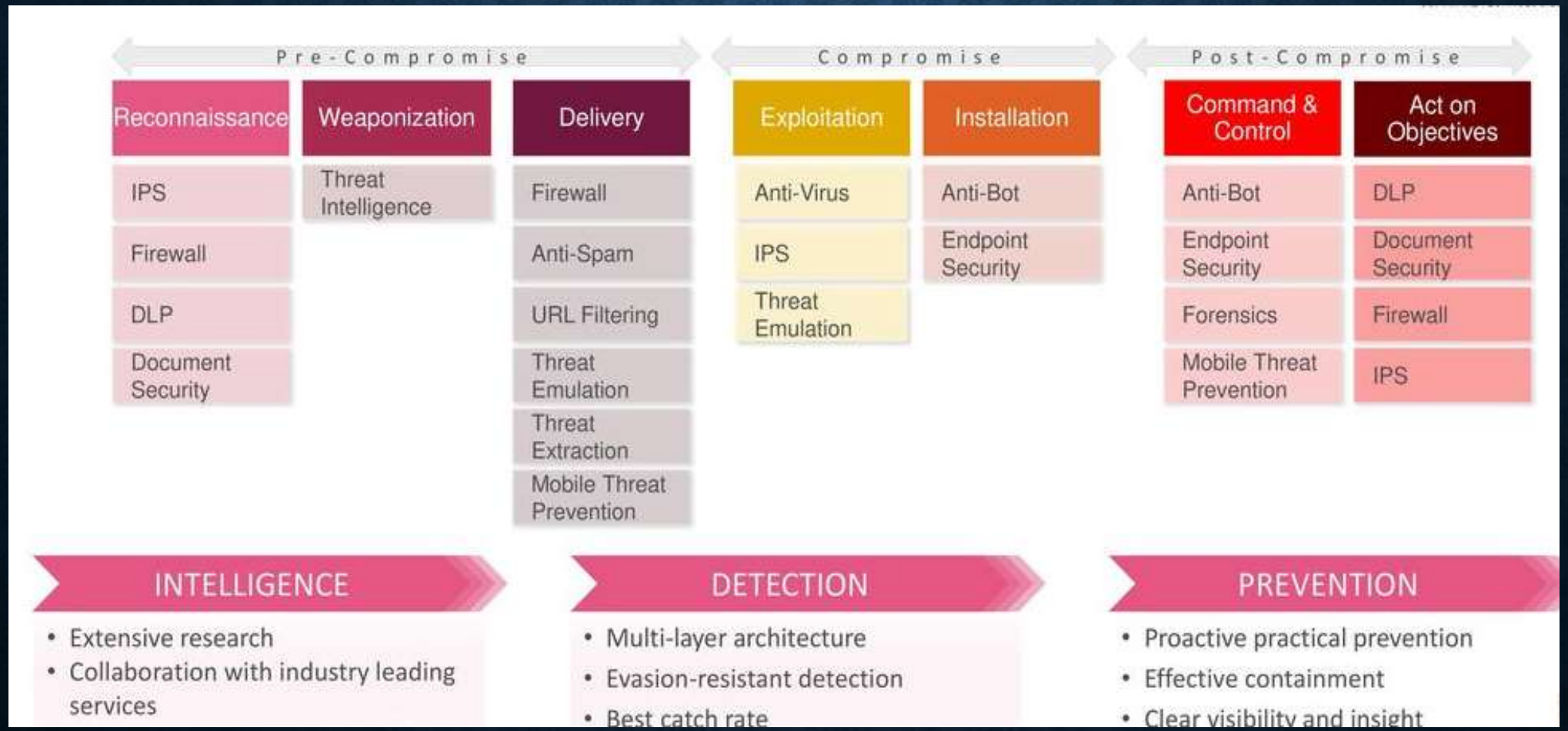
CYBER KILL CHAIN

Security Controls you can Use to Stop the Kill Chain



HOW TO BREAK THE CHAIN

- Apply protection for each of the stages.
- Take strong preventive defense before infection. Successful Defense with Checkpoint



CYBER KILL CHAIN

Breaking the Kill Chain with Advanced Network Security Lines of Defense

THANKYOU