Kaitlin Hoffmann

Office Hours: SH 243 Monday 1:15 - 3:15 PM. Tuesday 2:45 - 4:45 PM.

Email: hoffmank4@newpaltz.edu

CYBER KILL CHAIN

NETWORK SECURITY

OBJECTIVES

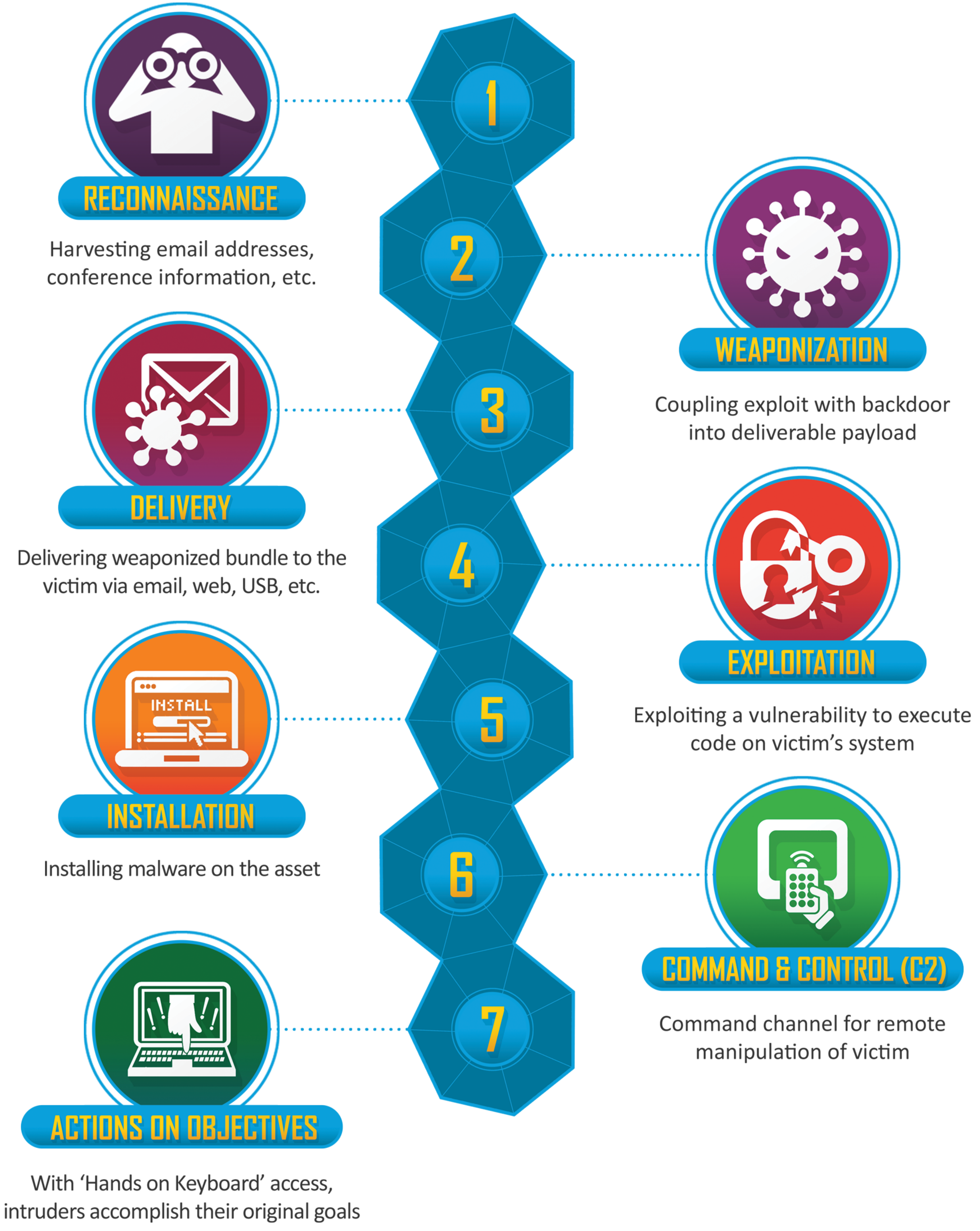
- What is the cyber kill chain
- Understand each step of the cyber kill chain
- Know examples of each

WHAT IS THE CYBER KILL CHAIN?

- Developed by Lockheed Martin, **the Cyber Kill Chain** framework is part of the **Intelligence Driven Defense** model for identification and prevention of cyber intrusions activity.
- The model identifies what the adversaries/bad actors must complete in order to achieve their objective.
- The seven steps of the Cyber Kill Chain enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.

Helps security teams to recognize, intercept, or prevent cyberattacks.

Helps organizations to better understand relevant threats and improve incident management and response.



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

RECONNAISSANCE

- Reconnaissance is discovering and collecting information on the system and the victim. The reconnaissance phase is the **planning phase** for the adversaries.
- Open source intelligence (OSINT) is the act of gathering and analyzing publicly available data for intelligence purposes.
- Next module will go in depth with reconnaissance and some of the tools used.

Harvesting email addresses, conference information, etc.

PASSIVE RECONNAISSANCE

- In **passive reconnaissance**, you rely on publicly available knowledge. It is the knowledge that you can access from publicly available resources **without directly engaging** with the target.
- Think of it like you are looking at target territory from afar without stepping foot on that territory.
- Passive reconnaissance activities include many activities, for instance:
  - Looking up DNS records of a domain from a public DNS server.
  - Checking job ads related to the target website.
  - Reading news articles about the target company.

ACTIVE RECONNAISSANCE

- Active reconnaissance, on the other hand, cannot be achieved so discreetly. It requires **direct engagement** with the target.
- Think of it like you check the locks on the doors and windows, among other potential entry points.
- Examples of active reconnaissance activities include:
  - Connecting to one of the company servers such as HTTP, FTP, and SMTP.
  - Calling the company in an attempt to get information (social engineering).
  - Entering company premises pretending to be a repairman.

IMPORTANT: Due to the invasive nature of active reconnaissance, one can quickly get into legal trouble unless one obtains proper legal authorization.

TARGET RETAILER EXAMPLE

- In 2013, attackers gained access to Target’s computer network, stole the financial and personal information of as many as 110 million Target customers, and then removed this sensitive information from Target’s network to a server in Eastern Europe.
- Reference: *A “Kill Chain” Analysis of the 2013 Target Data Breach* https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

TARGET RETAILER EXAMPLE – RECONNAISSANCE

- HVAC vendor, Fazio Mechanical Services, had access to Target’s network for electronic billing, contract submission, and project management purposes.
- Attackers stole credentials from Fazio through phishing. Emails may have been ladened with malware.
- How did the attacker know about Fazio? Through Reconnaissance!!

TARGET RETAILER EXAMPLE – RECONNAISSANCE

- Attacker may have found information on Target's third-party vendors through ***simple Internet searches***!! Target's supplier portal and facilities management pages used to be available publicly.
- A metadata analysis allowed the attacker to map Target's internal network prior to the breach.
- **To disrupt this step in the kill chain:** Target could have limited the amount of publicly available vendor information. Target could have also shared threat information with its suppliers and vendors and encouraged collaboration on security within the community.

WEAPONIZATION

- During the Weaponization phase, the attacker **creates** an attack vector, such as remote access malware, ransomware, virus or worm that can exploit a known vulnerability.
- During this phase, the attacker may also set up back doors so that they can continue to access to the system if their original point of entry is identified and closed by network administrators.

Coupling exploit with backdoor
into deliverable payload

TARGET RETAILER EXAMPLE – WEAPONIZATION

- While unconfirmed, the attacker likely weaponized its malware targeting Fazio in an email attachment, likely a PDF or Microsoft Office document.
- **To disrupt this step in the kill chain:** Fazio could have used a broadly accepted real-time monitoring and anti-malware software. Instead, Fazio used the free version of Malwarebytes Anti-Malware, which does not provide real-time protection and is intended only for individual consumer use.

DELIVERY

- In the Delivery step, the intruder launches the attack. The specific steps taken will depend on the type of attack they intend to carry out.
- For example, the attacker may send email attachments or a malicious link to spur user activity to advance the plan. This activity may be combined with social engineering techniques to increase the effectiveness of the campaign.

Delivering weaponized bundle to the victim via email, web, USB, etc.

TARGET RETAILER EXAMPLE - DELIVERY

- The attacker sent infected emails to Fazio in a so-called phishing attack.
- **To disrupt this step in the kill chain:** Fazio could have trained its staff to recognize and report phishing emails. Real-time monitoring and anti-malware software could have also potentially detected the infected file(s).

TARGET RETAILER EXAMPLE – DELIVERY

- The malware on Fazio's systems may have recorded passwords and provided the attackers with their key to Target's Ariba external billing system.
- **To disrupt this step in the kill chain:** Target could have required two factor authentication for its vendors. According to a former Target vendor manager, Target rarely required two-factor authentication from its low-level contractors.

EXPLOITATION

- In the Exploitation phase, the malicious code is executed within the victim's system.
- Attackers often move laterally across systems, identifying more potential entry points and weaknesses.

Exploiting a vulnerability to execute code on victim's system

TARGET RETAILER EXAMPLE – EXPLOITATION

- Once delivered, the RAM scraping malware and exfiltration malware began recording millions of card swipes and storing the stolen data for later exfiltration.
- **To disrupt this step in the kill chain:** Target could have potentially blocked the effect of the exfiltration malware on its servers by either allowing its FireEye software to delete any detected malware, or, if not choosing the automatic option, by following up on the several alerts that were triggered at the time of malware delivery.

TARGET RETAILER EXAMPLE – EXPLOITATION

- **Another protective step** could have been paying greater attention to industry and government intelligence analyses. According to an FBI industry notification, RAM scraping malware has been observed since 2011.
- A Reuters report stated that Visa published in April and August of 2013 two warnings about the use of RAM scraping malware in attacks targeting retailers.
- These warnings apparently included recommendations for reducing the risk of a successful attack.

INSTALLATION

- Immediately following the Exploitation phase, the malware or other attack vector will be installed on the victim's system.
- This is a turning point in the attack lifecycle, as the threat actor has entered the system and can now assume control.

Installing malware on the asset

TARGET RETAILER EXAMPLE – INSTALLATION

- The attacker maintained access to Fazio’s systems for some time while attempting to further breach Target’s network.
- Attackers may have exploited a default account name used in a BMC Software information technology management system.
- **To disrupt this step in the kill chain:** The elimination or alteration of unneeded default accounts.

COMMAND AND CONTROL (C2)

- In Command & Control, the attacker is able to use the malware to assume remote control of a device or identity within the target network.
- In this stage, the attacker may also work to move laterally throughout the network, expanding their access and establishing more points of entry for the future.

Command channel for remote manipulation of victim

TARGET RETAILER EXAMPLE – COMMAND AND CONTROL

- The attackers had access to Target’s internal network for over a month and compromised internal servers with exfiltration malware.
- While the exact method by which the attackers maintained command and control is unknown, it is clear the attackers were able to maintain a line of communication between the outside Internet and Target’s cardholder network.

TARGET RETAILER EXAMPLE – COMMAND AND CONTROL

- **To disrupt this step in the kill chain 1:** Analyze the location of credentialed users in the network. For example, if attackers were still using Fazio's credentials, it would have showed his credential was being used in an unrelated area of the Target network.
- **To disrupt this step in the kill chain 2:** The use of strong firewalls between Target's internal systems and the outside Internet to help disrupt the attacker's command and control. Target could also have filtered or blocked certain Internet connections commonly used for command and control.

ACTIONS ON OBJECTIVES

- In this stage, the attacker takes steps to carry out their intended goals, which may include data theft, destruction, encryption or exfiltration.

With 'Hands on Keyboard' access, intruders accomplish their original goals

TARGET RETAILER EXAMPLE – ACTIONS ON OBJECTIVES

- The attackers transmitted the stolen data to outside servers – at least one of which was located in Russia – in plain text via FTP over the course of two weeks.
- **To disrupt this step in the kill chain:** Protective defensive steps could have included white listing approved FTP servers to which Target's network is allowed to upload data.
  - For example, a white list could have dismissed connections between Target's network and Russia-based Internet servers.

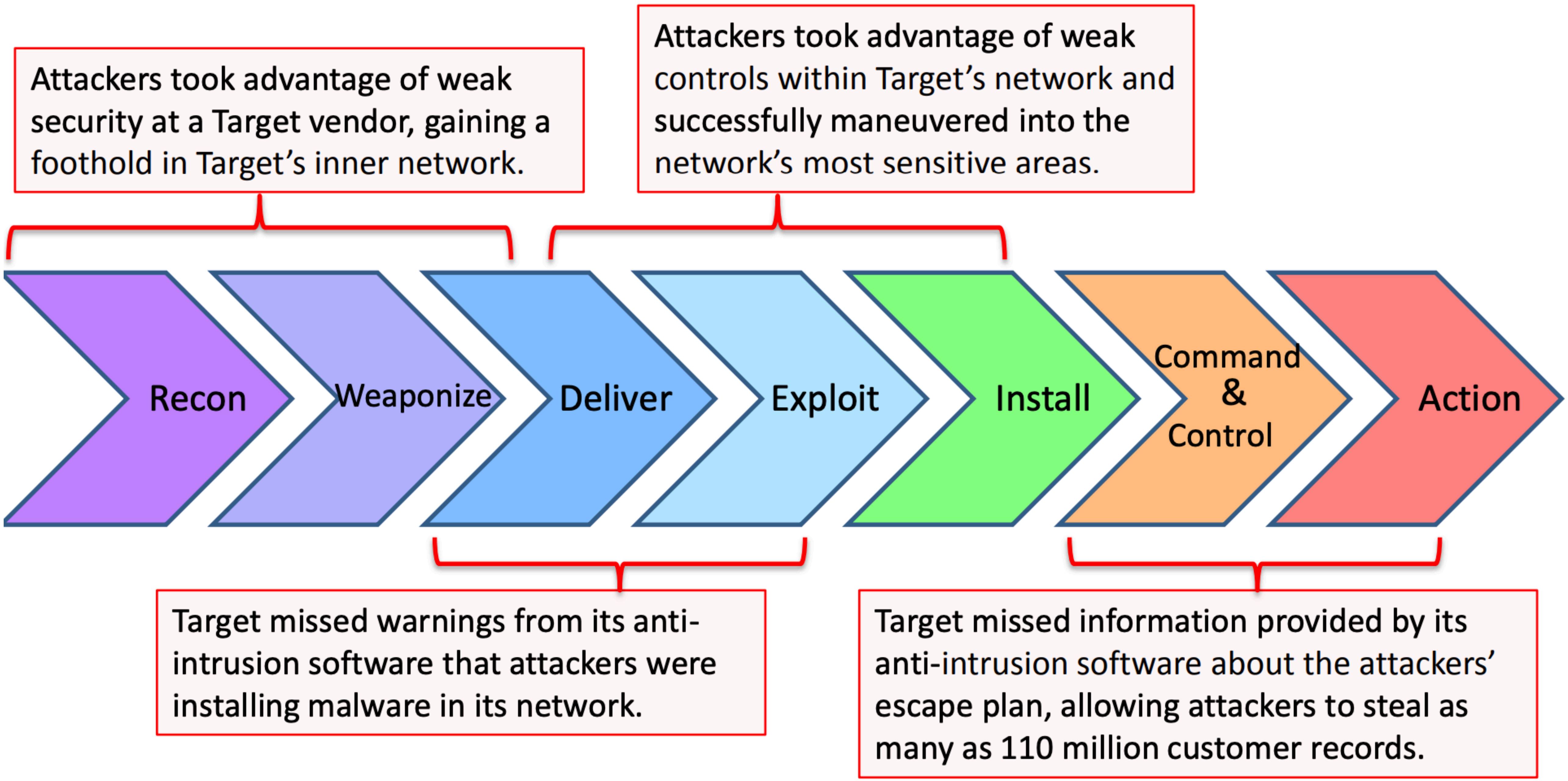
TARGET RETAILER EXAMPLE – ACTIONS ON OBJECTIVES

- Target's FireEye software reportedly did detect the data exfiltration malware and decoded the destination of servers on which data for millions of stolen credit cards were stored for days at a time.
- **To disrupt this step in the kill chain:** Simply acting on this information could have stopped the exfiltration, not only at this last stage, but especially during the "delivery" step on the kill chain.

target

CYBER KILL CHAIN - HTTPS://WWW.COMMERCE.SENATE.GOV/SERVICES/FILES/24D3C229-4F2F-405D-B8DB-A3A67F183883

Target's Possible Missed Opportunities



Attackers took advantage of weak security at a Target vendor, gaining a foothold in Target's inner network.

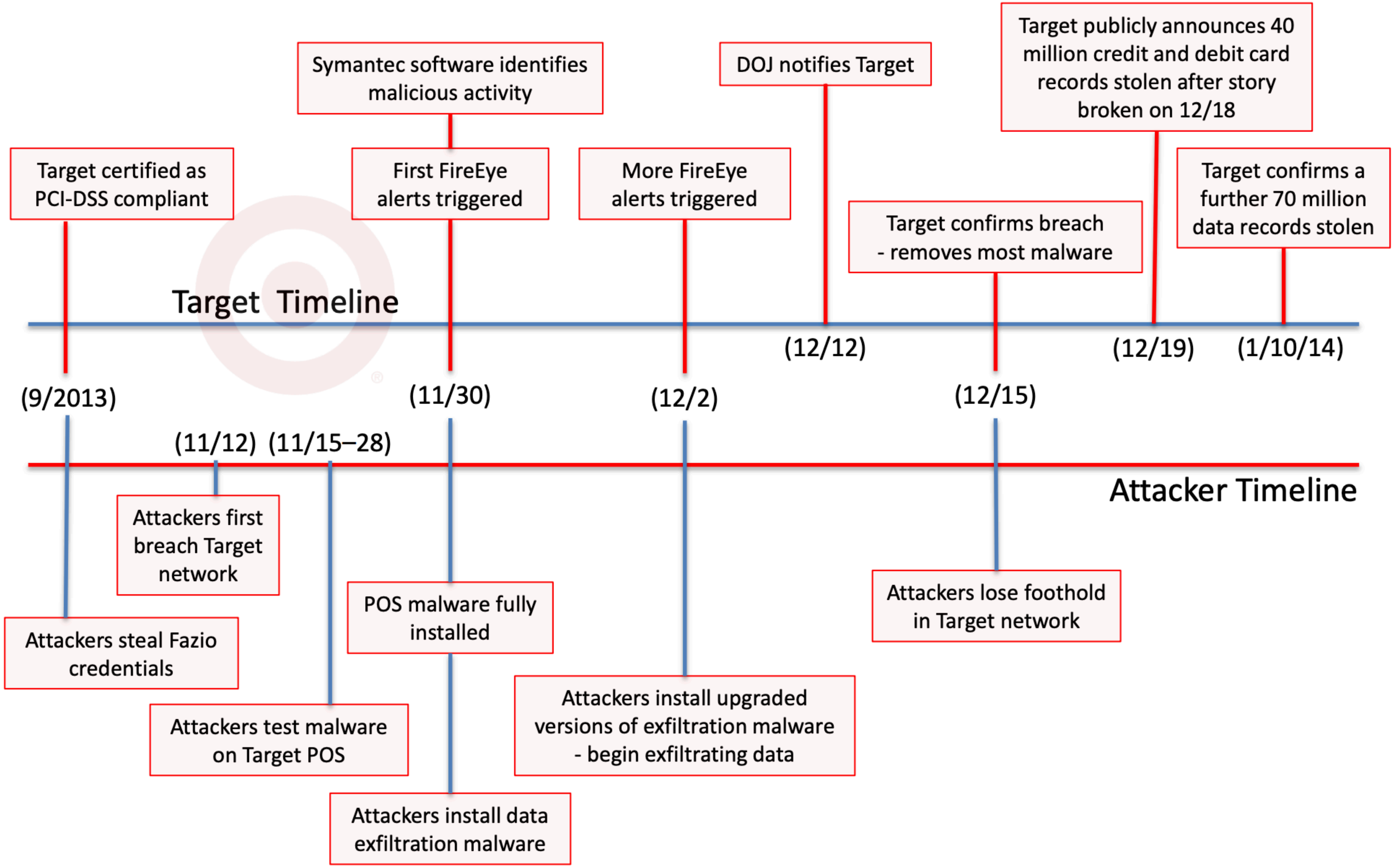
Attackers took advantage of weak controls within Target's network and successfully maneuvered into the network's most sensitive areas.

Target missed warnings from its anti-intrusion software that attackers were installing malware in its network.

Target missed information provided by its anti-intrusion software about the attackers' escape plan, allowing attackers to steal as many as 110 million customer records.

CYBER KILL CHAIN - HTTPS://WWW.COMMERCE.SENATE.GOV/SERVICES/FILES/24D3C229-4F2F-405D-B8DB-A3A67F183883

A Timeline of the Target Data Breach



Target Timeline

(9/2013) Target certified as PCI-DSS compliant

(11/30) Symantec software identifies malicious activity

(11/30) First FireEye alerts triggered

(12/2) More FireEye alerts triggered

(12/12) DOJ notifies Target

(12/15) Target confirms breach - removes most malware

(12/19) Target publicly announces 40 million credit and debit card records stolen after story broken on 12/18

(1/10/14) Target confirms a further 70 million data records stolen

Attacker Timeline

(9/2013) Attackers steal Fazio credentials

(11/12) Attackers first breach Target network

(11/15–28) Attackers test malware on Target POS

(11/30) POS malware fully installed

(11/30) Attackers install data exfiltration malware

(12/2) Attackers install upgraded versions of exfiltration malware - begin exfiltrating data

(12/15) Attackers lose foothold in Target network

WEAKNESSES IN THE CYBER KILL CHAIN

- **Limited attack detection profile** - doesn’t adequately cover web threats such as advanced web-based exploits like SQL injection, cross-site scripting (XSS), and zero-day vulnerabilities.
- **No insider threat detection** - The traditional cyber kill chain does not account for insider threats, which pose a significant risk to organizations.
- **Lack of flexibility** - Not all attackers follow the cyber kill chain linearly. They can skip, combine, or backtrack stages (Spray and Pray attack).

WEAKNESSES IN THE CYBER KILL CHAIN

- **Transformative technologies** - cloud computing, DevOps, IoT, machine learning, and automation have broadened the scope of cyberattacks. These innovations introduce new entry points and new data sources, challenging the traditional kill chain framework to adapt.
- **Emerging threats & techniques** - deepfake phishing, AI-driven attacks, and sophisticated ransomware campaigns require more dynamic and responsive security models.

WEAKNESSES IN THE CYBER KILL CHAIN

- Addressing these weaknesses requires integrating more comprehensive and flexible frameworks, like MITRE ATT&CK and Cyber COBRA, which offer a more detailed and adaptive approach to modern cyber threats.
- Organizations must continuously evolve their security strategies to stay ahead of attackers and protect their digital assets effectively.
- https://attack.mitre.org/tactics/enterprise/

ASSIGNMENT 2

- Read *Gaining the Advantage* entirely: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- Read *Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform*: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf
- Complete the following lab: https://tryhackme.com/r/room/cyberkillchainzmt and submit proof of completion with screenshot.