C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

CS 668:
Module 4
The Unified Kill Chain

Raising Resilience Against
Advanced Cyber Attacks

Why another Kill Chain?

#	Unified Kill Chain
1	Reconnaissance
2	Weaponization
3	Delivery
4	Social Engineering
5	Exploitation
6	Persistence
7	Defense Evasion
8	Command & Control
9	Pivoting
10	Discovery
11	Privilege Escalation
12	Execution
13	Credential Access
14	Lateral Movement
15	Collection
16	Exfiltration
17	Impact
18	Objectives

- Research shows that the traditional Cyber Kill Chain® (CKC), as presented by researchers of Lockheed Martin, is perimeter- and malware-focused.
- As such, the traditional model fails to cover other attack vectors and attacks that occur behind the organizational perimeter.
- The Unified Kill Chain offers significant improvements over these scope limitations of the CKC
- The time-agnostic nature of the tactics in MITRE's ATT&CK™ model (ATT&CK) fails to capture the progression of an attack.

Basic Assumption in LM CKC

- CKC assumes that attackers must progress successfully through each phase of a deterministic sequence.
- However, attack phases may be bypassed which affects defensive strategies fundamentally
  - as an attacker may also bypass the security controls that apply to these phases.
- Instead of focusing on thwarting attacks at the earliest point in time, layered defense strategies that focus on attack phases that occur with a higher frequency or that are vital for the formation of an attack path are thus expected to be more successful.
- Development (or realignment) of layered defense strategies that adopt the *assume breach* and *defense in depth* principles and to optimize the return on investment (ROI) of their security measures

G. Engel, "Deconstructing The Cyber Kill Chain," *Dark Reading*. [Online]. Available: Deconstructing The Cyber Kill Chain (darkreading.com)

What is a Kill Chain?

- To properly defend oneself against advanced cyber attacks, one must first understand how these attacks are typically performed.
- For this purpose, threat modeling is required.
    - The Cyber Kill Chain® by Lockheed Martin (CKC) was traditionally regarded as the industry standard threat model for defending against advanced cyber attacks
- The term “kill chain” describes an *end-to-end* process, or the entire chain of events, that is required to perform a successful attack.
    - Once an attack is understood and deconstructed into discrete phases, it allows defenders to map potential countermeasures against each one of these phases.
- Advanced cyber attacks typically extend beyond exploiting one vulnerability in an internet-connected system.
- Depending on the security posture of the target, attacks may require attackers to forge an attack path through the internal network of the victim, in which multiple correlated vulnerabilities are exploited before critical assets can be targeted and objectives can be achieved.

What is Unified Kill Chain?

- Based on Masters thesis of Paul Pols (2017)
  - Serves to model and defend against cyber attacks, from the attacker's first steps to the achievement of an adversarial objective.
  - The model was designed to defend against end-to-end cyber attacks from a variety of advanced attackers, including Advanced Persistent Threats (APTs).
  - The model has also successfully been applied to defend against ransomware worms, that implement tactics that were previously primarily seen in targeted attacks.
  - The Unified Kill Chain has a proven track recording in raising the resilience of targeted organizations against a range of targeted and (initially) untargeted attacks.

What is Unified Kill Chain Good for?

- The Unified Kill Chain offers a substantiated basis for strategically realigning defensive capabilities and cyber security investments within organizations, in the areas of prevention, detection, response and intelligence
- Unified Kill Chain allows for a structured analysis and comparison of threat intelligence regarding the tactical modus operandi of attackers.
- For prevention, the Unified Kill Chain can be used to map countermeasures to the discrete phases of an attack.
- Detection can be prioritized based on the insights into the ordered arrangement of the attack phases.
- In emergency response situations, the Unified Kill Chain aids investigators in triage and modeling likely attacks paths.
- The model also specifically allows for the improvement of the predictive value of Red Team threat emulations, which aim to test the security posture of organizations in these areas.

Design of Unified Cyber Kill Chain

- The model was first published in the Executive Master's thesis of Paul Pols entitled "*The Unified Kill Chain: modeling Fancy Bear attacks*" at the Cyber Security Academy.
- The Unified Kill Chain extends and combines existing models, such as Lockheed Martins' Cyber Kill Chain® and MITRE's ATT&CK™ for Enterprise.
- The strengths and weaknesses of traditional kill chain models were studied through literature review
- Potential amendments to remedy tactical shortcomings were identified and a first hypothesis for a unified kill chain was designed.
- The first hypothesis for a unified kill chain was iteratively evaluated and improved through real world case studies
- The model was evaluated and refined by modeling the attacks of APT28 alias Fancy Bear.
    - The (intermediate) results were validated through semi-structured interviews

The Unified Kill Chain		
1	**Reconnaissance**	*Researching, identifying and selecting targets using active or passive reconnaissance.*
2	**Weaponization**	*Preparatory activities aimed at setting up the infrastructure required for the attack.*
3	**Delivery**	*Techniques resulting in the transmission of a weaponized object to the targeted environment.*
4	**Social Engineering**	*Techniques aimed at the manipulation of people to perform unsafe actions.*
5	**Exploitation**	*Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.*
6	**Persistence**	*Any access, action or change to a system that gives an attacker persistent presence on the system.*
7	**Defense Evasion**	*Techniques an attacker may specifically use for evading detection or avoiding other defenses.*
8	**Command & Control**	*Techniques that allow attackers to communicate with controlled systems within a target network.*
9	**Pivoting**	*Tunneling traffic through a controlled system to other systems that are not directly accessible.*
10	**Discovery**	*Techniques that allow an attacker to gain knowledge about a system and its network environment.*
11	**Privilege Escalation**	*The result of techniques that provide an attacker with higher permissions on a system or network.*
12	**Execution**	*Techniques that result in execution of attacker-controlled code on a local or remote system.*
13	**Credential Access**	*Techniques resulting in the access of, or control over, system, service or domain credentials.*
14	**Lateral Movement**	*Techniques that enable an adversary to horizontally access and control other remote systems.*
15	**Collection**	*Techniques used to identify and gather data from a target network prior to exfiltration.*
16	**Exfiltration**	*Techniques that result or aid in an attacker removing data from a target network.*
17	**Impact**	*Techniques aimed at manipulating, interrupting or destroying the target system or data.*
18	**Objectives**	*Socio-technical objectives of an attack that are intended to achieve a strategic goal.*

Intermediate Goals

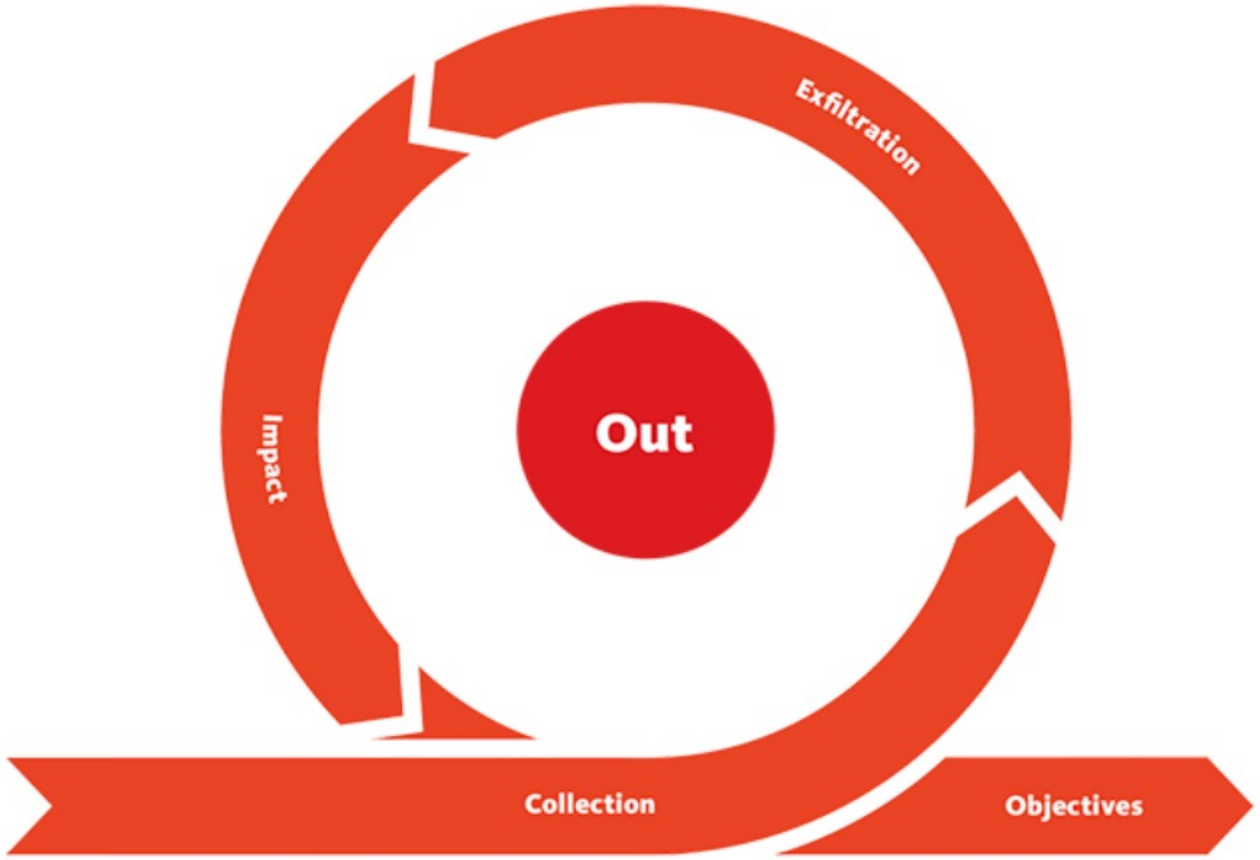
- Multiple tactical phases of an attack can be combined to achieve intermediate goals, such as gaining
  - an initial foothold in a targeted network,
  - propagating through the network to expand the level of access
  - performing actions on critical assets.
- The individual Phases of the Unified Kill Chain are typically combined by attackers to achieve intermediate goals in the phased progression towards achieving their final objectives.

- The objectives of an attack may require an attacker to gain access to systems or data that are only accessible within a trusted environment, typically within the internal network of a targeted organization.
- To gain access to these systems or data, an attacker can employ the first phases of the Unified Kill Chain to breach the organizational perimeter and gain an initial foothold in the network.

Initial Foothold

- Once an attacker has acquired access to a targeted network, additional privileges may be required to gain access to assets that allow the attacker to perform actions on the objectives of the attack.
- Network propagation refers to the activities that attackers typically perform to gain additional access to systems and data in furtherance of their objectives.
- These activities may be performed by an external attacker that has acquired digital or physical access behind the organizational perimeter, typically by compromising one system, through attack vectors such as (spear) phishing, a watering hole attack, a supply chain attack or through an insider threat

Network Propagation



- By gaining an initial foothold in a targeted network, and propagating through the network as required, an attacker can acquire the privileges that are necessary to eventually perform actions on the objectives of the attack.
- When the objective of an attack involves compromising the availability or integrity of an asset, it may suffice to use the acquired privileges to manipulate, interrupt or destroy the target (*Impact*).
- If the objective involves compromising the confidentiality of an asset, additional techniques may be employed to collect the data that the attacker is after (*Collection*). Collected data may be exfiltrated to an attacker-controlled system (*Exfiltration*), until the objectives are achieved.

Action on Objectives

Using the Unified Kill Chain to Model Specific Cyber Attacks and Threat Actor Behavior

- The Unified Kill Chain offers insights into the tactics that attackers employ in advanced cyber attacks and the order in which they typically, but not necessarily, occur.
- The phases of the Unified Kill Chain can be used as building blocks to describe the behavior of attackers in individual cyber attacks (an *attack specific* kill chain), or to describe the tactical modus operandi of an attacker (an *actor specific* kill chain), by putting them in the right order as observed in a specific attack or in the typical modus operandi of an attacker
- The length of a kill chain that describes an individual attack depends on the amount of different tactics that an attacker needs to use to reach their objective.
- The length of the attack specific kill chains is determined in large part by the combination of the modus operandi of an attacker and the defensive posture of targeted organizations.
    - The stronger the security posture, the longer the kill chain is expected to be.

Using UKC to Realign Defensive strategies

- The fact that attack phases may be bypassed affects defensive strategies fundamentally.
    - In bypassing an attack phase, an attacker may also bypass the security controls that apply specifically to that phase.
- Instead of focusing on thwarting attacks at the earliest point in time, defensive strategies that focus on phases that either occur with a higher frequently or that are vital for the formation of an attack path towards an asset are expected to be more successful.
- This notably includes creating, securing and monitoring choke points that force attackers to pivot and start anew before they can act on their objectives.
    - These choke points can be created through measures such as network segmentation in combination with the isolation of identity and access management zones.

Defensive Strategies (2)

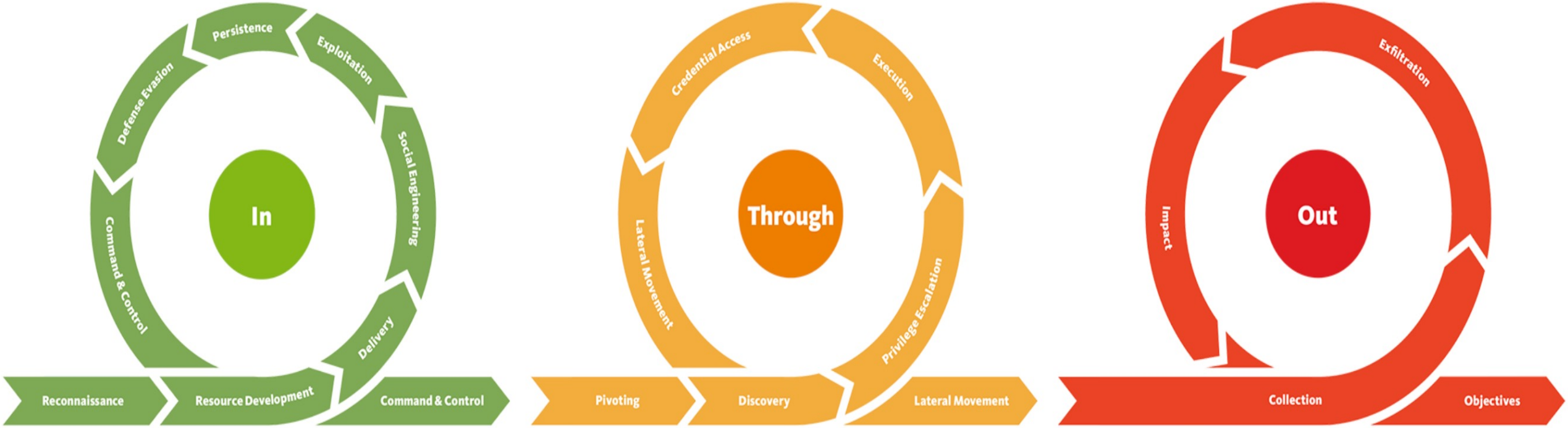
- It is challenging to prevent the compromise of every single internet connected system in a large network, while the number of critical supporting assets is typically far more limited.
- Strategies that aim to defend a limited amount of critical supporting assets may thus be more likely to succeed than strategies that aim to defend all internet connected systems.
- Furthermore, the objectives of an attacker may force them to find an attack path within the confines of the internal network of the targeted organization, which takes place within the locus of control of defenders.
- Organizations can therefore potentially significantly increase their resilience, by focusing their efforts on the attack phases that occur within the confines of their internal network that pave the way to act on the objectives.

C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

Scope of Unified Kill Chain

	Cyber Kill Chain®	MITRE ATT&CK™	Unified Kill Chain
Reconnaissance	√	√	√
Resource Development	√	√	√
Delivery	√	√	√
Social Engineering	✖	✖	√
Exploitation	√	✖	√
Persistence	√	√	√
Defense Evasion	✖	√	√
Command & Control	√	√	√
Pivoting	✖	✖	√
Discovery	✖	√	√
Privilege Escalation	✖	√	√
Execution	✖	√	√
Credential Access	✖	√	√
Lateral Movement	✖	√	√
Collection	✖	√	√
Exfiltration	✖	√	√
Impact	✖	√	√
Objectives	√	✖	√

Conclusion


In
Persistence
Exploitation
Social Engineering
Delivery
Command & Control
Reconnaissance
Resource Development
Command & Control
Defense Evasion
Through
Credential Access
Execution
Privilege Escalation
Lateral Movement
Pivoting
Discovery
Lateral Movement
Out
Exfiltration
Impact
Collection
Objectives

Conclusion (Cont.)

- A conventional belief within cyber security is that attackers have the upper hand, because they only need to exploit one defensive flaw (the defeatist adage).
- Lockheed Martin's Cyber Kill Chain® promised a fundamentally reversed balance, by claiming that defenders could prevail by disrupting attackers at any point in their deterministically phased progression.
- The balance between attackers and defenders that is suggested by the Unified Kill Chain is much more delicate.
- Advanced attacks can be regarded as phased progressions, but individual attack phases may be bypassed, occur more than once or occur out of sequence.
- Raising resilience against the phased progressions of advanced attackers is possible by developing a layered defense strategy that aligns with an organization's threat model by adopting the assume breach and defense in depth principles.