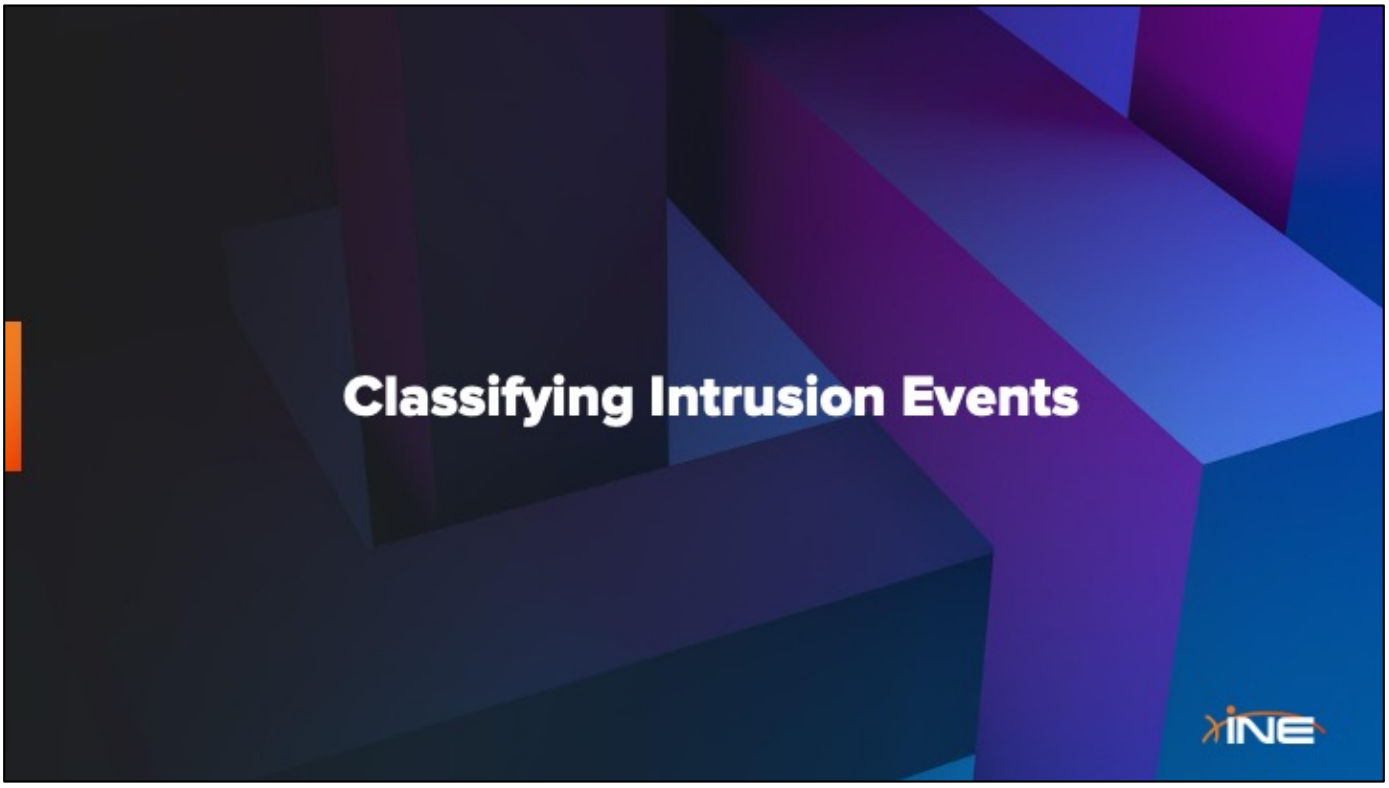


Learning Objectives:

- Understand three frameworks/models used for Intrusion classification
- Gain exposure to the Mitre ATT&CK framework
- Understand the phases of the Cyber Kill Chain
- Explore the benefits of the Diamond Model of Intrusion Analysis

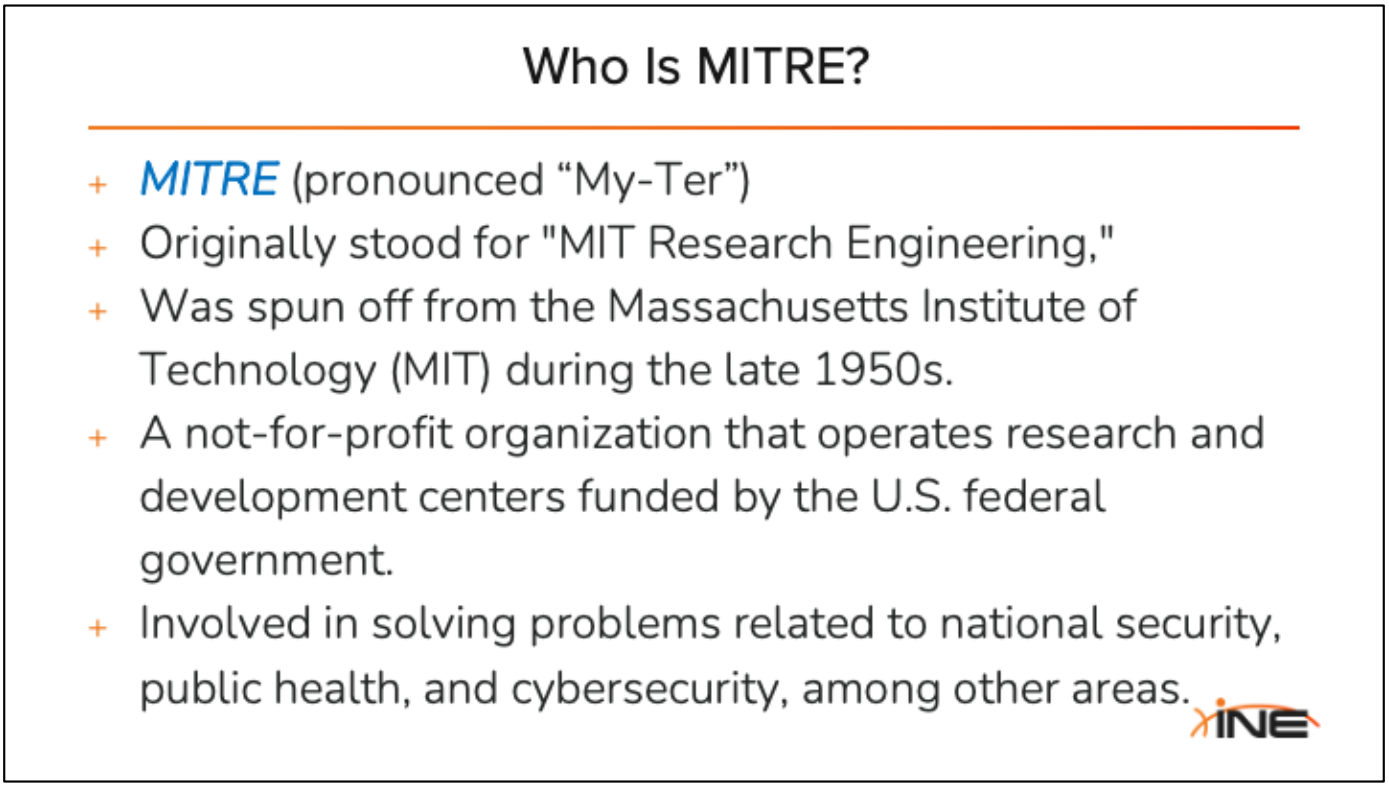
xxxx

Course Prerequisites

- Rudimentary understanding of basic Cyber Security terminology

xxxx

Let's Get Started!



- MITRE runs several federally funded research and development centers (FFRDCs), partnering with government agencies to address complex challenges in various sectors, including defense, aviation, healthcare, and cybersecurity.

What is MITRE ATT&CK

https://attack.mitre.org

- Open source, non-profit, global threat intelligence
- Looks at attacks from perspective of the adversary. Namely;
  - What goals they are trying to achieve
  - What specific methods they use

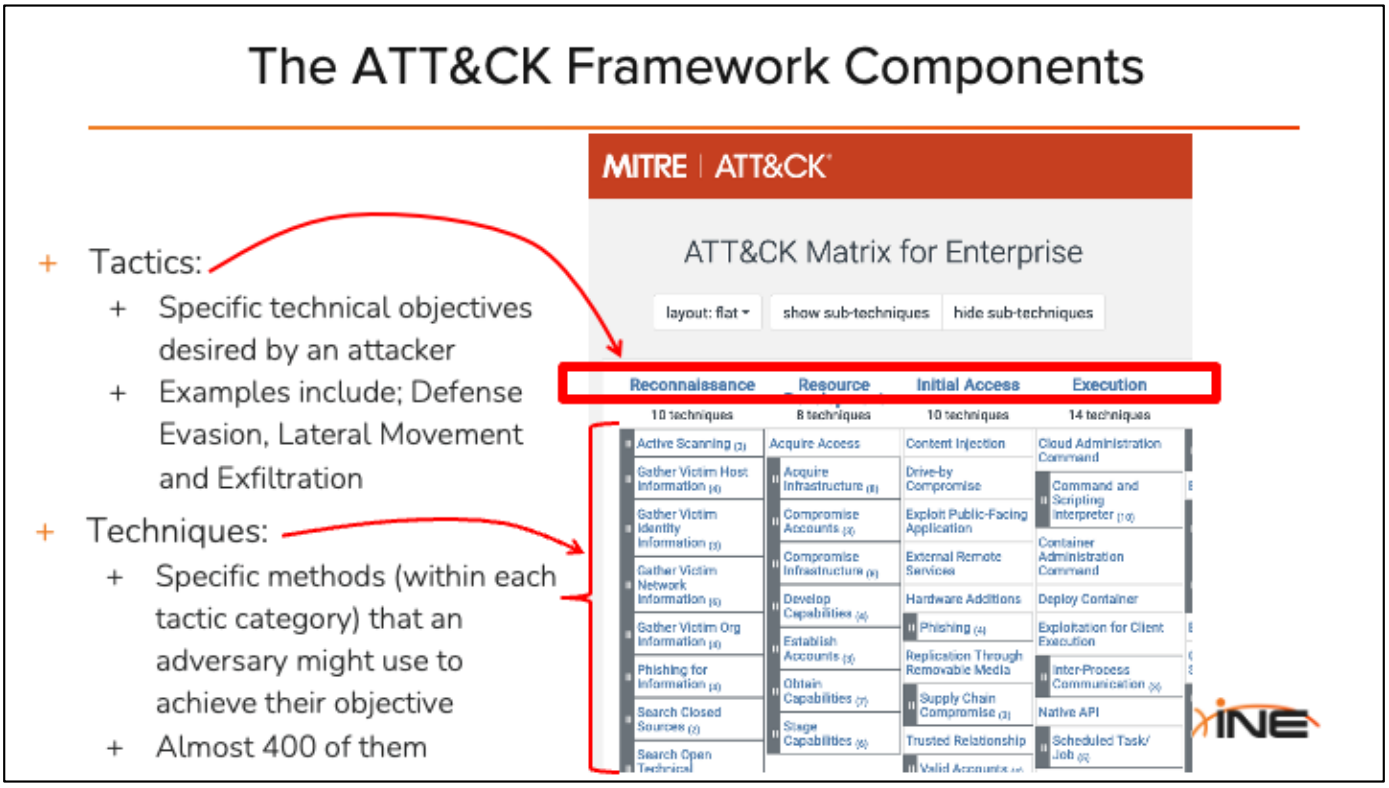
What Problem Did It Solve?

- Adversarial tactics and techniques continue to grow and evolve
  - A good defensive strategy involves continual learning of these TTPs
  - Vulnerability assessments require knowledge of these TTPs
- The need existed for a *centralized and globally-accessible knowledge base of historical and current TTPs*

- When an intrusion event occurs, it is useful to log the TTPs in a central location so other, global defensive organizations can learn from your experiences

Technology Domains

- The MITRE ATT&CK knowledge base divides Tactics and Techniques into three categories:
  - Enterprise networks (Windows and Linux Operating Systems, as well as some Mac and Unix vulnerabilities)
  - Mobile Devices
  - Industrial Control Systems (ICS)



- MITRE ATT&CK is primarily a knowledge based concerned with Advanced Persistent Threats (APTs) rather than simpler attacks such as DoS and Drive-By attacks.
- Tactics represent the “why” of an ATT&CK technique. The tactic is the adversary’s tactical objective for performing an action.
- Techniques represent “how” an adversary achieves a tactical objective by performing an action. For example, an adversary may dump credentials to gain access to useful credentials within a network that can be used later for lateral movement.
- Techniques may also represent “what” an adversary gains by performing an action.
- Each technique includes data related to:
    - Description of the method used
    - Systems or platforms it applies to
    - Specific adversary groups known to use this technique
    - Ways to detect and possibly mitigate the behavior

Using ATT&CK For Intrusion Classification

- When an intrusion is detected, it must be logged and categorized in such a way that:
  - It can be compared and related to past intrusions
  - It can be compared and related to future intrusions
  - The data about the intrusion can be posted in a way that is useful to others.
- ATT&CK maps tactics and techniques to common and well-known categories.
- Mapping data about your own intrusion events to those listed in ATT&CK meets the objectives listed above.

- In other words, we need to classify and categorize the tactics and techniques used in the intrusion event we discovered in a repeatable, and recognizable way.
- If John is allowed to describe Intrusion Event-1 in whatever way he sees fit and include (or omit) whatever data about that intrusion he deems relevant and…
- Sally follows the same random process about Intrusion Event-2 then…
- It's possible both intrusion events came from the same campaign, but there would be no way to form a correlation between the two events.

- By categorizing events according to the framework, organizations can identify gaps in their detection or defense strategies. Understanding how different techniques are used across various stages of an attack allows defenders to strengthen their security controls for each category.

Thanks for Watching!

What is a Defensive Framework

- Blue Teams have two primary defensive goals:
  - Ideally, discourage adversaries from attempting an attack
  - Defend against attacks to prevent adversaries from meeting their objectives
- Defensive frameworks provide *structured approaches* to protecting networks and systems from cyber threats.

- Think about two banks. If one bank always keeps their front doors open with no visible guards, but another bank has armed guards always posted outside of their closed doors, which bank is most likely to encourage an attack? The second bank has taken steps to discourage adversaries from even considering robbing it.

Frameworks Prior to 2011

- Several security frameworks and models existed prior to 2011 such as;
  - Perimeter Defense Models
  - Intrusion Detection Systems
  - Defense in Depth
  - Incident Response Frameworks
- The models and frameworks were either;
  - Primarily reactive
  - Inwardly focused

- In this context, “inwardly focused” means the concentration was on asking yourself “what do I have” (hardware and software) and “how can I protect it”.

What Was The Problem?

- Early security frameworks and models did not solve the problem of;
  - How to systematically track cyberattacks
  - Representing the phases of Advanced Persistent Threats
  - Defending against APTs
- Many earlier frameworks assumed attacks came from outside the network
- Did not account for lateral movement
- Were myopic in scope and vision

- Unlike attacks which would be considered “opportunistic”, APTs are categorized by the fact that they typically occur over multiple stages and for a long period of time. They also often have a goal of remaining undiscovered.
- “Myopic” meaning that their focus was purely on “what do I have and how do I technically protect it”. They didn’t view things from the perspective of an adversary or take non-technical tactics (such as Social Engineering and certain forms of Reconnaissance) into consideration.

The Military “Kill Chain”

- The military "kill chain" is a concept used in military operations to describe the *structured sequence of steps an adversary follows* to identify, engage, and neutralize a target.
- It also refers to the stages that military forces go through to detect, track, and eliminate an enemy target.

- Find: Identifying the target through intelligence gathering, surveillance, or reconnaissance.
- Fix: Pinpointing the target's exact location and tracking it to maintain awareness of its movements.
- Track: Continuously monitoring the target to ensure its location is known and that it can be engaged when necessary.
- Target: Identifying the most appropriate means of engaging and neutralizing the target, which could involve selecting weapons, platforms, or tactics.
- Engage: Deploying or launching the chosen weapon system to strike the target.
- Assess: Evaluating the results of the engagement to determine if the target was successfully neutralized or if further action is required.

- While some describe the military's "Kill Chain" as focusing on identifying and interrupting enemy attacks, notice that all these steps are from the ATTACKER's point of view. This chain is not about defending against an incoming attack (by implementing walls or missile defense systems) but rather going on the offensive to prevent such an attack from even starting. This is not a defensive but an offensive strategy.

Introduction to the Cyber Kill Chain

- Developed by Lockheed Martin in 2011
- Designed to provide a structured approach to understanding and defending against cyberattacks.
- Created in response to the growing complexity of cyber threats, particularly Advanced Persistent Threats (APTs)
- Inspired by the military concepts of “Kill Chain”

Creating the Cyber Kill Chain

- Analyze attacks (especially APTs) from the adversary's point of view.
- Recognize that *most intrusions follow a predictable set of stages*, regardless of the specific tools or techniques used.
- Create a clear map of how an attack progresses from beginning to end by *breaking down the attack process into distinct steps.*

The Goals of the Cyber Kill Chain

- Shift focus away from your own, internal structure to how an adversary might view your assets.
- Identify each stage an adversary might take in the Kill Chain and preemptively mitigate those steps with defensive controls.
- Disrupt the attack before it succeeds!

Thanks for Watching!

Overview of the Cyber Kill Chain

- The purpose:
  - Help defenders take a proactive approach to cybersecurity.
  - Understand and disrupt attacks by understanding the phases of an attack (the “kill chain”)
- Consists of seven distinct phases

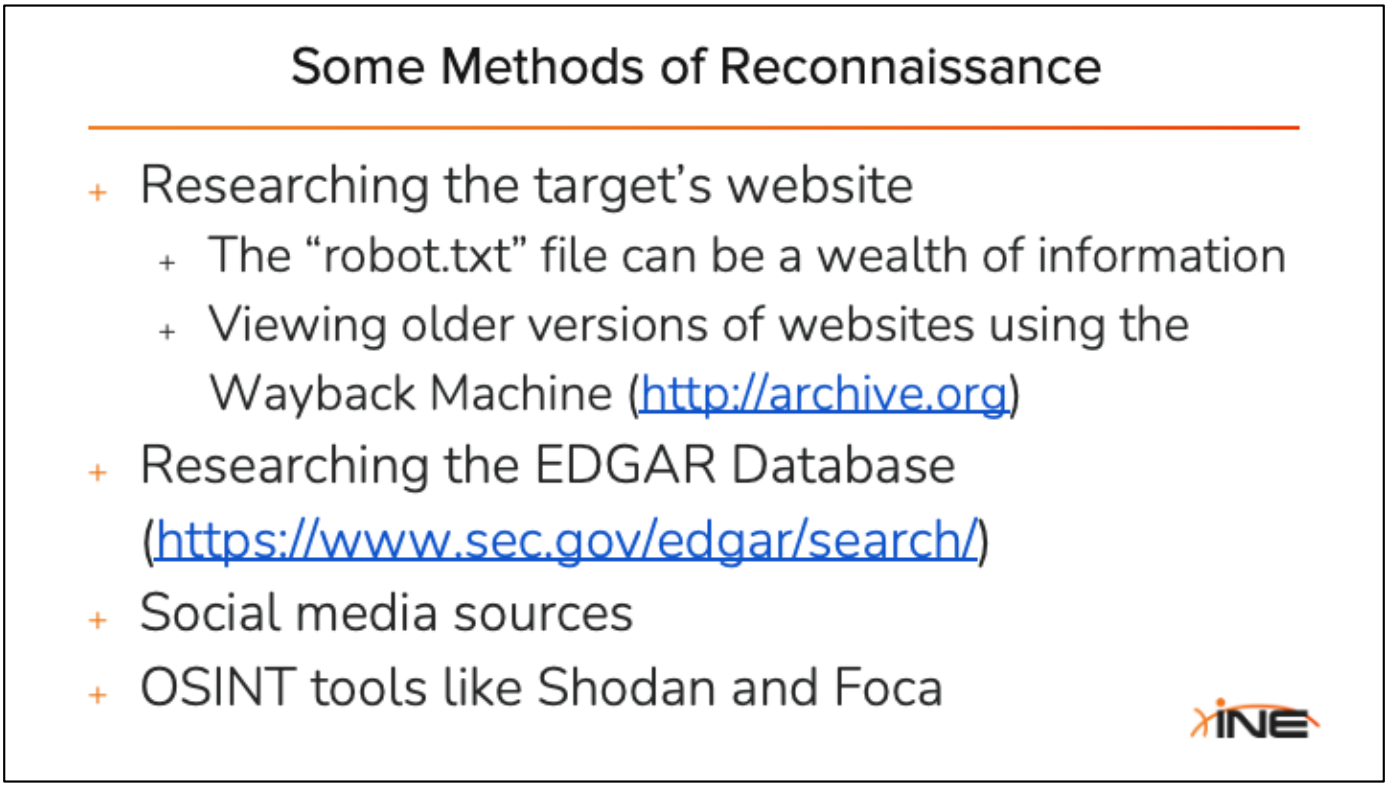
Introducing the Phases

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

Reconnaissance

- Attacker gathers information about the target organization.
- This could involve scanning the network for vulnerabilities, identifying key personnel, or gathering data from public sources.

- For an attacker, this is the most time-consuming of all the phases.



- For publicly-traded companies, any documents they must file with the SEC (U.S. Securities and Exchange Commission) can be found within this searchable database
- OSINT (Open Source Intelligence) tools are cybersecurity tools designed to collect and analyze publicly available information from various sources on the internet. These tools allow attackers (or security professionals) to gather intelligence without engaging directly with the target. Tools like Shodan and Foca perform Internet searches for things like IoT devices and open ports on webservers.

Weaponization

- Determining and crafting the malicious payload
- Pairing the malware with an exploit
  - Creating a delivery mechanism
- Developing and testing the attack
- No direct engagement with the target yet

- Combining a malicious payload with an exploit: In this phase, the attacker creates a weapon by bundling a malicious payload (e.g., malware, ransomware, or spyware) with an exploit targeting a specific vulnerability.
- Creating a delivery mechanism: The attacker packages the weaponized exploit in a form that can be delivered to the victim, such as through email attachments (like malicious PDFs), Office macros, or compromised websites (watering hole attacks).
- No direct engagement with the target yet: During weaponization, the attacker prepares the malicious software but does not yet engage with the intended victim. The goal is to ensure that the payload can be effectively delivered when the opportunity arises.

Weaponization Tools: Metasploit

- An open-source robust penetration testing framework
- Can automate almost all of the pentesting cycle
- Contains extensive database of known vulnerabilities with associated exploits
- Primarily command-line driven
- For more information, see INE's;

"*The Metasploit Framework Bootcamp*"

https://my.ine.com/CyberSecurity/courses/7a72985c/the-metasploit-framework-bootcamp

Metasploit Example

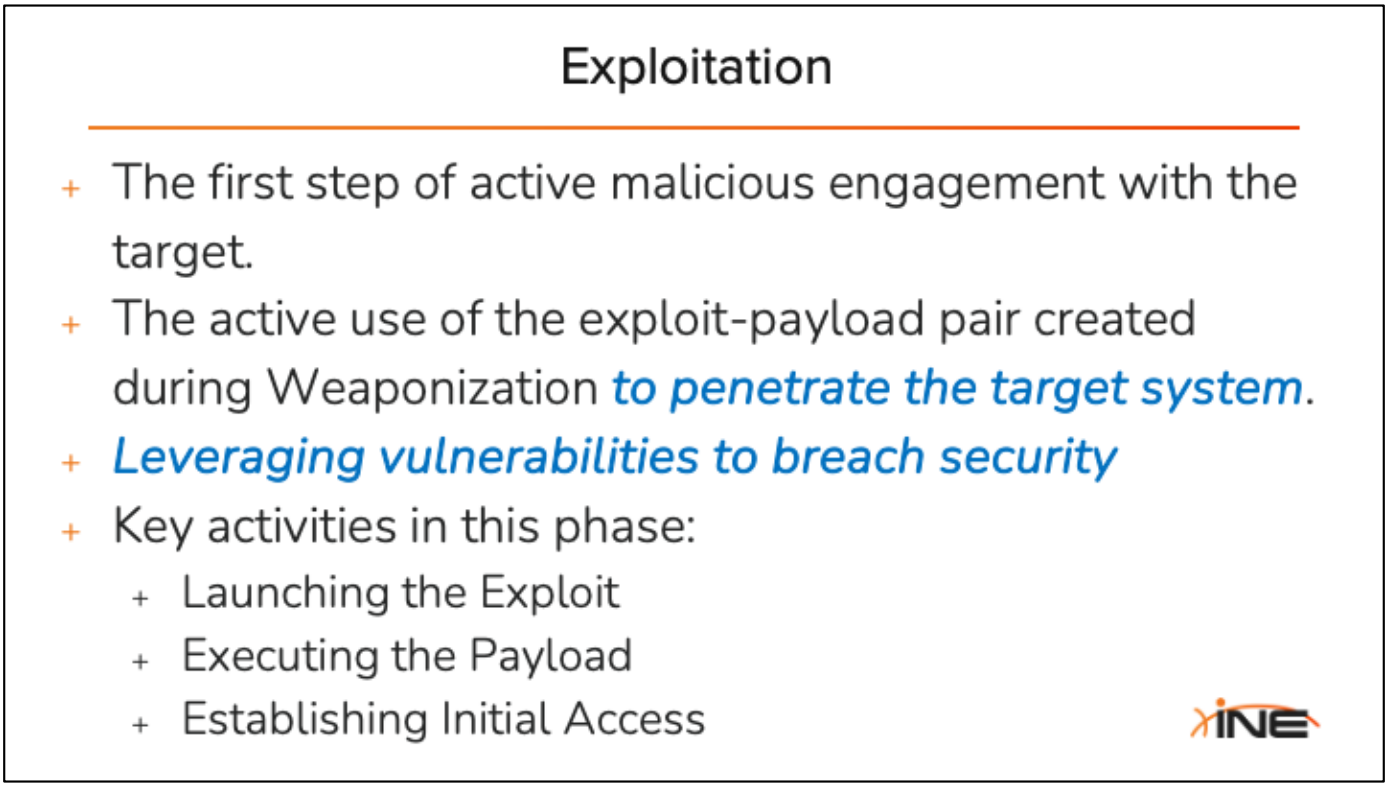
```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf  exploit(ms03_026_dcom) >
msf  exploit(ms03_026_dcom) >
msf  exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  135              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf  exploit(ms03_026_dcom) > set RHOST 192.168.1.150
RHOST => 192.168.1.150
msf  exploit(ms03_026_dcom) > set PAYLOAD windows/shell_bind_tcp
PAYLOAD => windows/shell_bind_tcp
msf  exploit(ms03_026_dcom) >
```

- Here you can see the command-line nature of Metasploit. It is very complicated and requires much training to understand it.
- In this example, some options for a particular Windows exploit called, “ms03_026_dcom” are being set and the Payload that will be executed by this exploit is also being set.
- Metasploit can be used to automate most of the processes in the Cyber Kill Chain including the Reconnaisance phase (which isn’t shown here).

Delivery

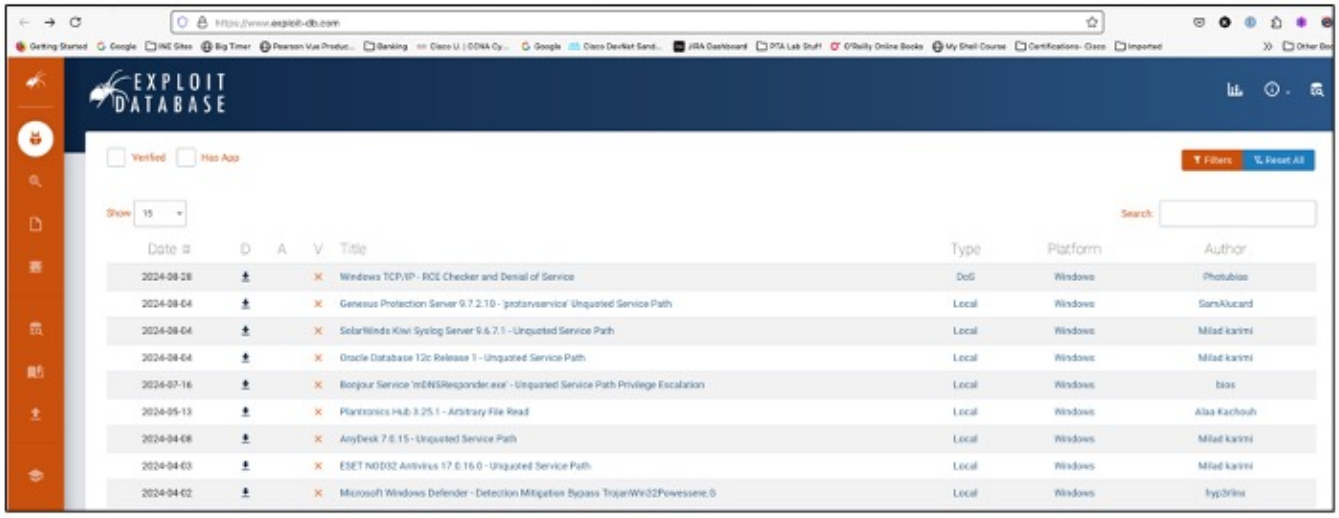
- The method(s) used to transmit the malware and exploit to the target.
- May involve several steps encompassing methods such as;
  - Physical Methods
  - Digital Methods
  - Social Methods

Thanks for Watching!

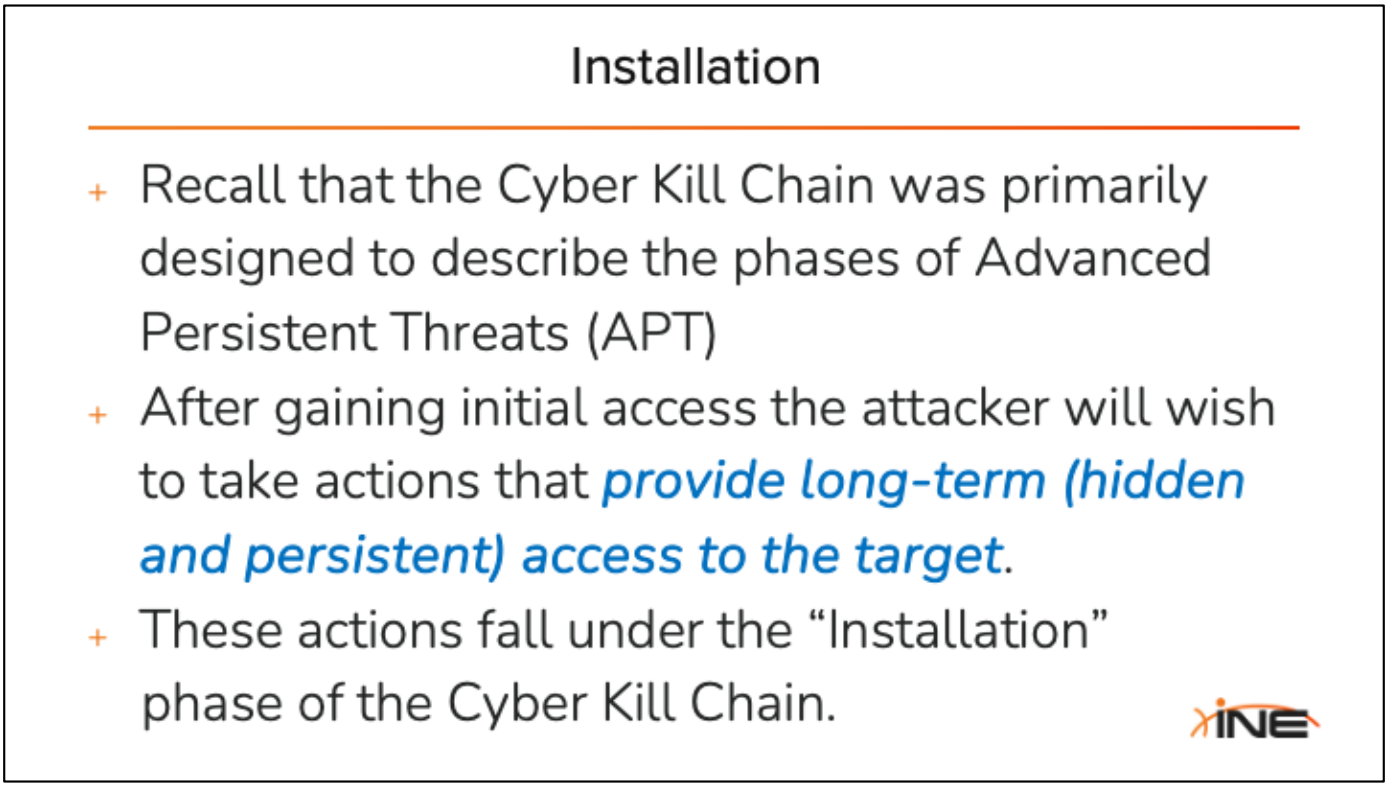


- Purpose: The Exploitation phase focuses on leveraging the identified vulnerability to gain initial access to the target system. The goal here is to exploit the weakness in such a way that the attacker can execute some code or perform some action that compromises the system.
- Scope of Activities:
  - Triggering the Exploit: The attacker uses the vulnerability to run malicious code, like launching a shell or executing a script.
  - Delivering Initial Payloads: Any software or scripts used during this phase are typically designed to open the door for the attacker by either:
    - Establishing a temporary connection (e.g., opening a reverse shell).
    - Running lightweight code (e.g., downloading malware or fetching additional tools).
  - Objective: The attacker's focus is on getting immediate access or control of the system but not necessarily maintaining it over the long term. The code or tools used in this phase may or may not persist on the target system.

Searching for Exploits

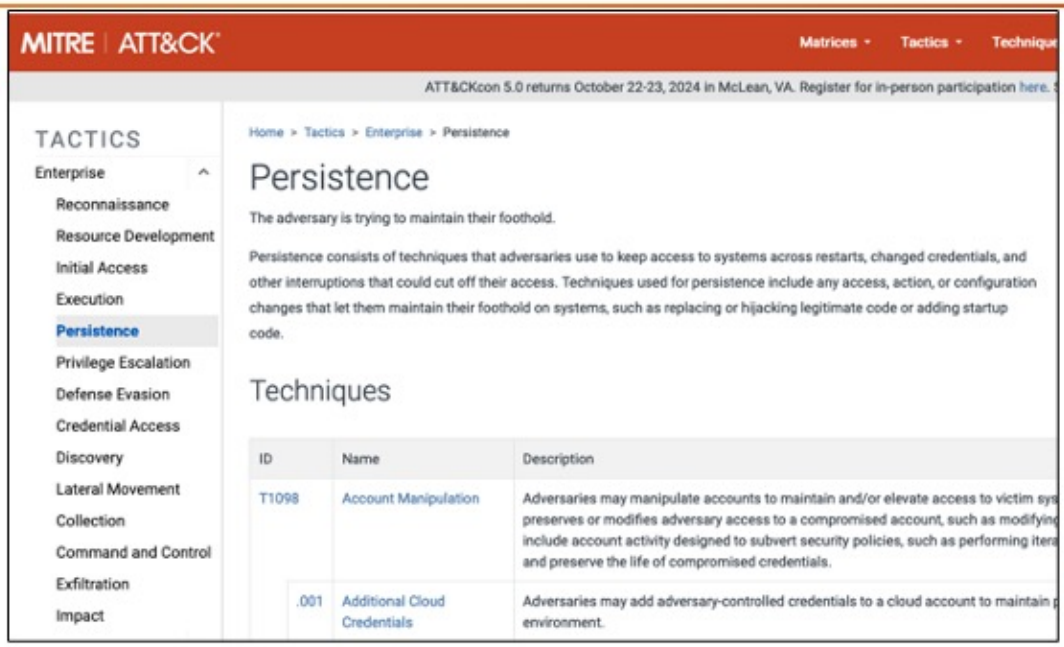


- Many online Knowledge Bases exist for viewing and searching common/known Exploits.
- The graphic here is from https://www.exploit-db.com/
- Another very popular site is Mitre's ATT&CK platform: https://attack.mitre.org/. For discovering exploits one should concentrate of the "tactic" of "Intial Access" within the MITRE framework.

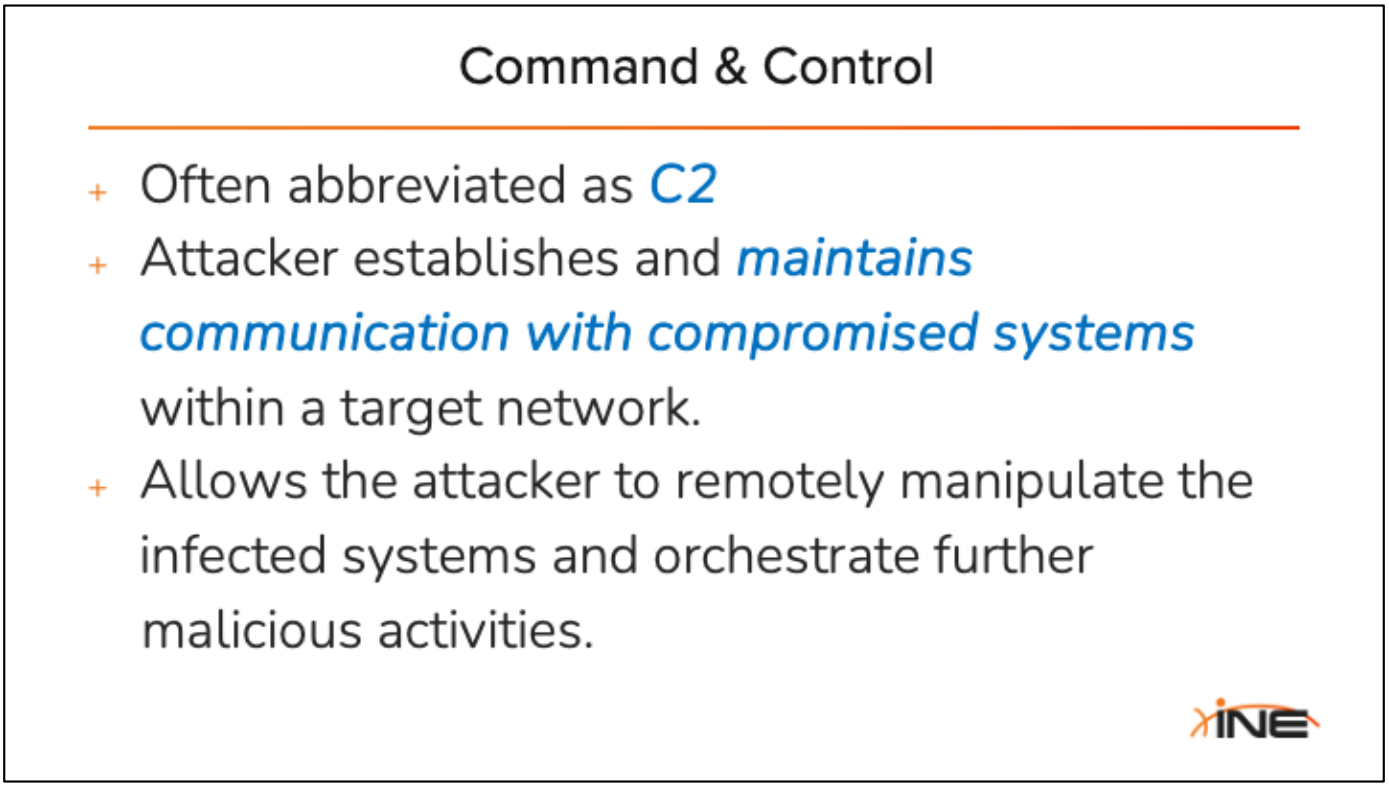


- In the industry, the average stands at between 100-200 days for organizations to detect a cybersecurity breach leaving plenty of time for the "Installation" and subsequent phases in the Kill Chain to occur.
- Most organizations spend most of their time concentrating on how to prevent breaches and exploits, giving little thought to protecting their data after an exploit occurs.
- In this step, the key is "persistence". The attacker is trying to install something that will give them long-term and persistent access.
- Examples of tactics in this phase include:
  - Installing Remote Access Tools (RATs)
  - Hidden and secret VPN sessions
  - Stealing remote login credentials
- RATs are often installed with mechanisms that ensure they remain active and start automatically, surviving reboots and user logouts. This may involve adding registry keys, creating scheduled tasks, or modifying system files to ensure the tool is reactivated regularly.
- Once installed, RATs provide attackers with remote control capabilities, allowing them to execute commands, deploy additional malware, exfiltrate data, or manipulate the system for other purposes.

Finding Examples of Installation



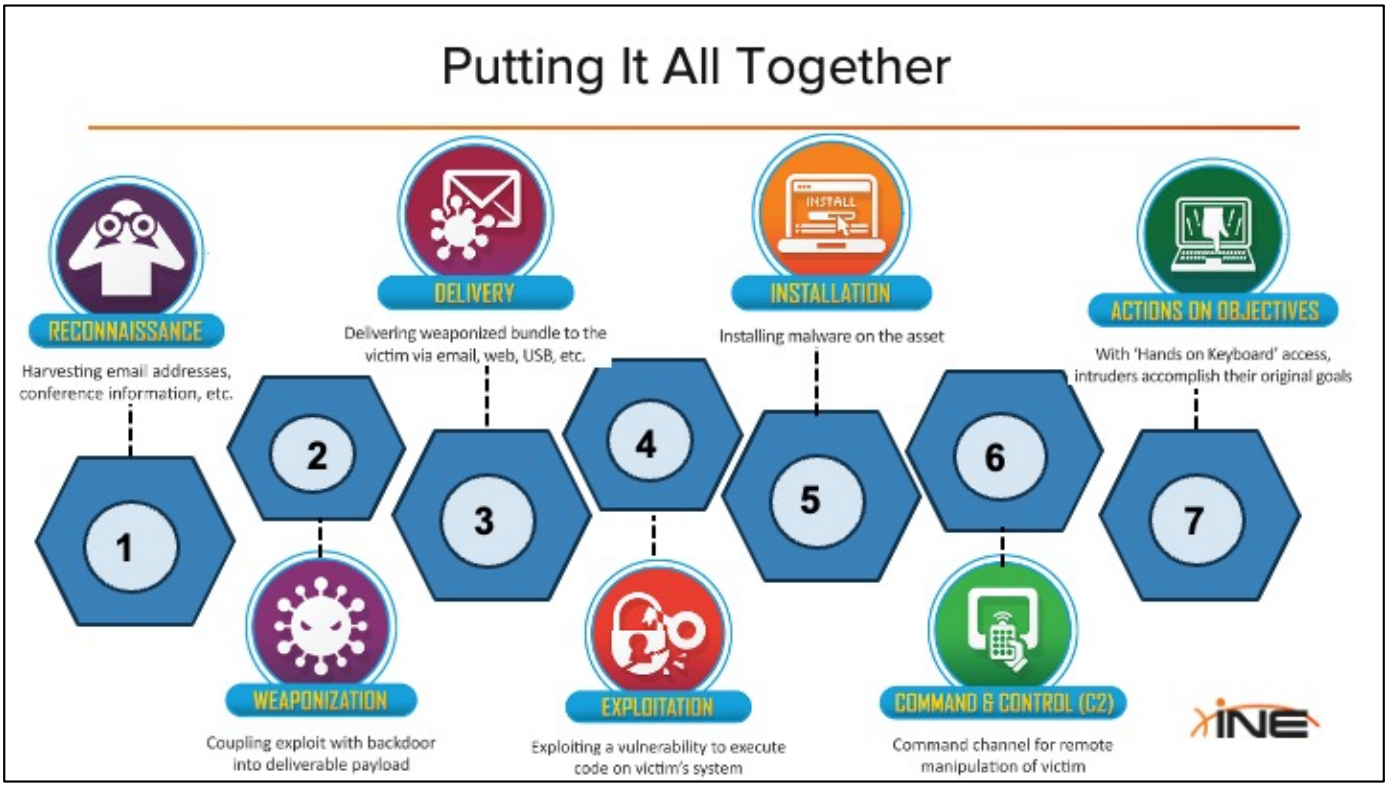
- For insights specifically about the **"Installation" phase** of the Cyber Kill Chain, you'd be looking for resources that discuss how malware establishes persistence, configures itself to avoid detection, or ensures it remains active after a system reboot.
- In the MITRE ATT&CK database the "Persistence" and "Privilege Escalation" tactics within MITRE ATT&CK detail various techniques used during the Installation phase, such as Registry Run Keys / Startup Folder (T1547.001) or Scheduled Task/Job (T1053).



- Purpose
  - Remote Interaction: Once the malware is installed, the C2 phase enables the attacker to communicate with and control the compromised system from a remote location.
  - Directive Execution: Attackers send commands to the compromised systems to execute specific tasks—such as data exfiltration, spreading within the network, or deploying additional payloads.
- Mechanisms
  - Communication Channels: Malware typically establishes a communication channel back to a server controlled by the attacker. These channels can include:
    - HTTP/HTTPS: Commonly used due to the ubiquity and non-suspicious nature of web traffic.
    - DNS: Utilized for covert communications as it's less likely to be blocked and can be harder to detect.
    - SMTP, FTP, or custom protocols designed to blend in with normal network traffic or to use unconventional ports and protocols to evade detection.

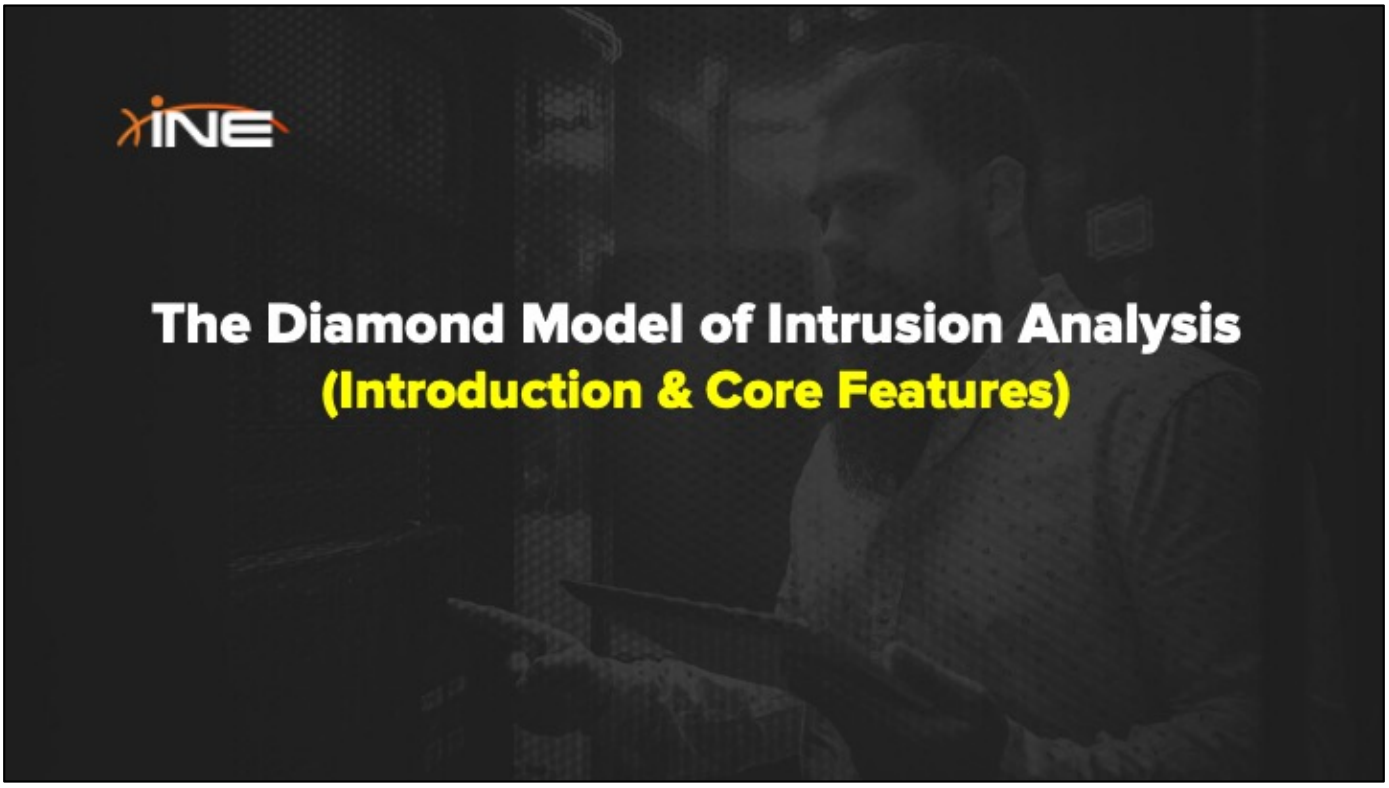
Action on Objectives

- At this phase, the attacker now accomplishes their long-term malicious objectives.
- Actions taken by attackers may include:
  - Collect user credentials
  - Privilege Escalation
  - Lateral Movement
  - Collect and Exfiltrate Data
  - Destroy Systems
  - ...and much more



- Many of the graphics on this slide are thanks to the following page from Lockheed Martin:
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Thanks for Watching!



What Problem Existed?

- When intrusion events are detected, emotions can run hot, leading to;
  - Analysis paralysis
  - Lack of structure in documentation of the event
- The developers of the Diamond Model recognized from their years of combined experience that there was a *scientific process used during intrusion event analysis.*
- The Diamond Model provides that structured, scientific process to apply to event analysis and documentation

- There is a need for “a formal method applying scientific principles to intrusion analysis…providing a comprehensive method of activity documentation, synthesis, and correlation.”
  - From 2013 US D.O.D. report, “The Diamond Model of Intrusion Analysis”
  - https://apps.dtic.mil/sti/pdfs/ADA586960.pdf

Documenting & Analyzing Events

- Without a formal, structured documentation process, each documented intrusion event;
  - Is isolated, lacking context from any other previous event
  - Not useful in identifying ongoing or future adversarial campaigns
  - Provides no context that can help mitigate or defend against future attacks
- A model needs to be developed that provides a guided approach to;
  - Threat hunting strategies
  - Correlating forensic data
  - Forecasting future activity and planning

The Diamond Model

- A model that *visualizes the scientific process used during intrusion event analysis*
- Establishes the basic "atomic elements" of any intrusion event into four core "features":
  - *Adversary*
  - *Infrastructure*
  - *Capability*
  - *Victim*

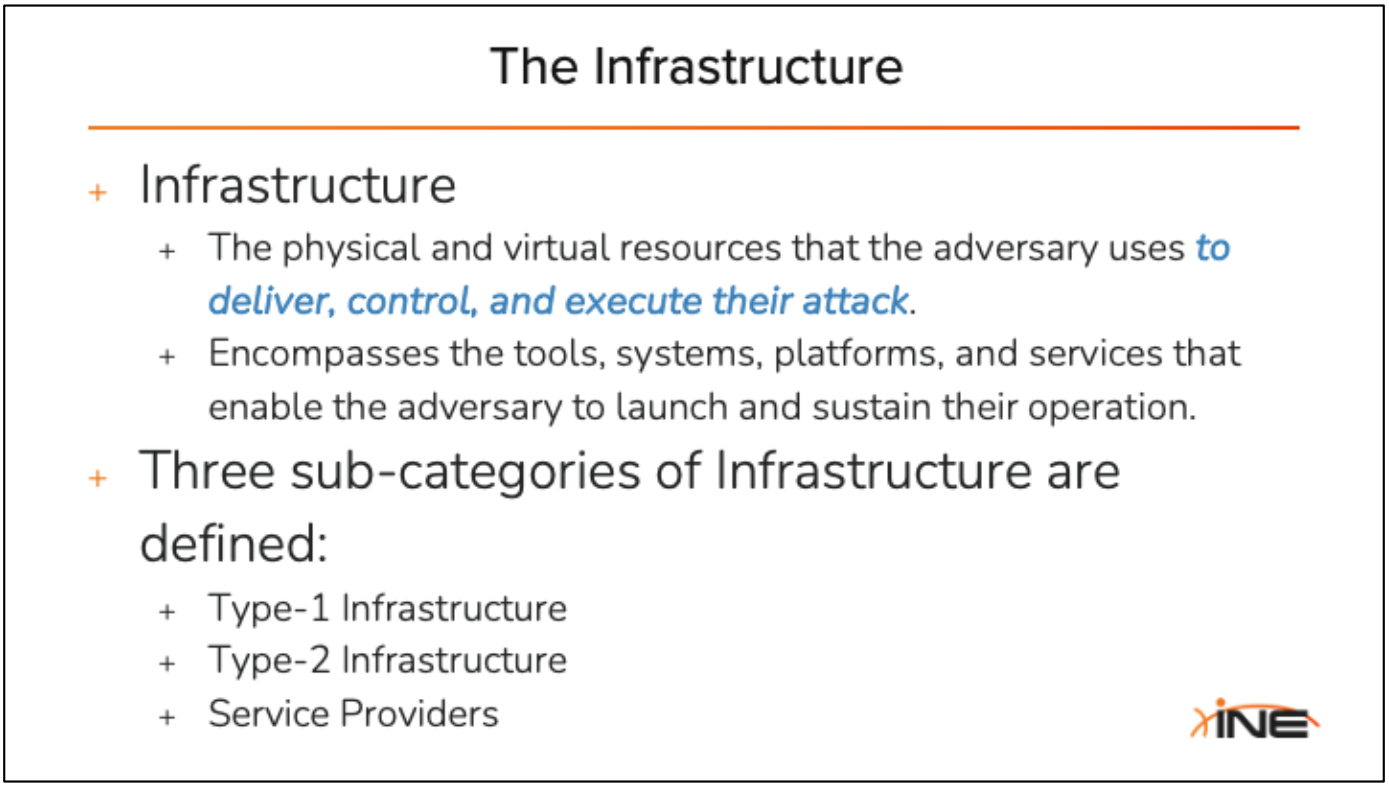
- Initially formulated in 2006 by Chris Betz, and Andy Pendergast (and others) & then published in 2013 by the DoD

The Adversary

- Adversary
  - The actor/organization responsible for utilizing a capability against the victim to achieve their intent.
  - Adversary knowledge is generally elusive, and this feature is likely to be empty for most events
- Adversary can be divided into two subcategories
  - Adversary Operator
  - Adversary Customer

- Adversary Operator (the actual “hacker” or person conducting the intrusion activity)
- Adversary Customer (entity stands to benefit from the activity conducted in the intrusion.)

- Adversary Customer may be the same as the adversary operator, or it may be a separate person or group.



- Examples:
  - Servers or domains used for command and control (C2) communication.
  - Compromised websites that host malicious payloads (malware, phishing pages, etc.).
  - IP addresses, DNS entries, or cloud services leveraged for launching attacks.
  - Botnets or other distributed systems that adversaries use to increase their reach and resilience.
  - Email servers used for phishing campaigns.

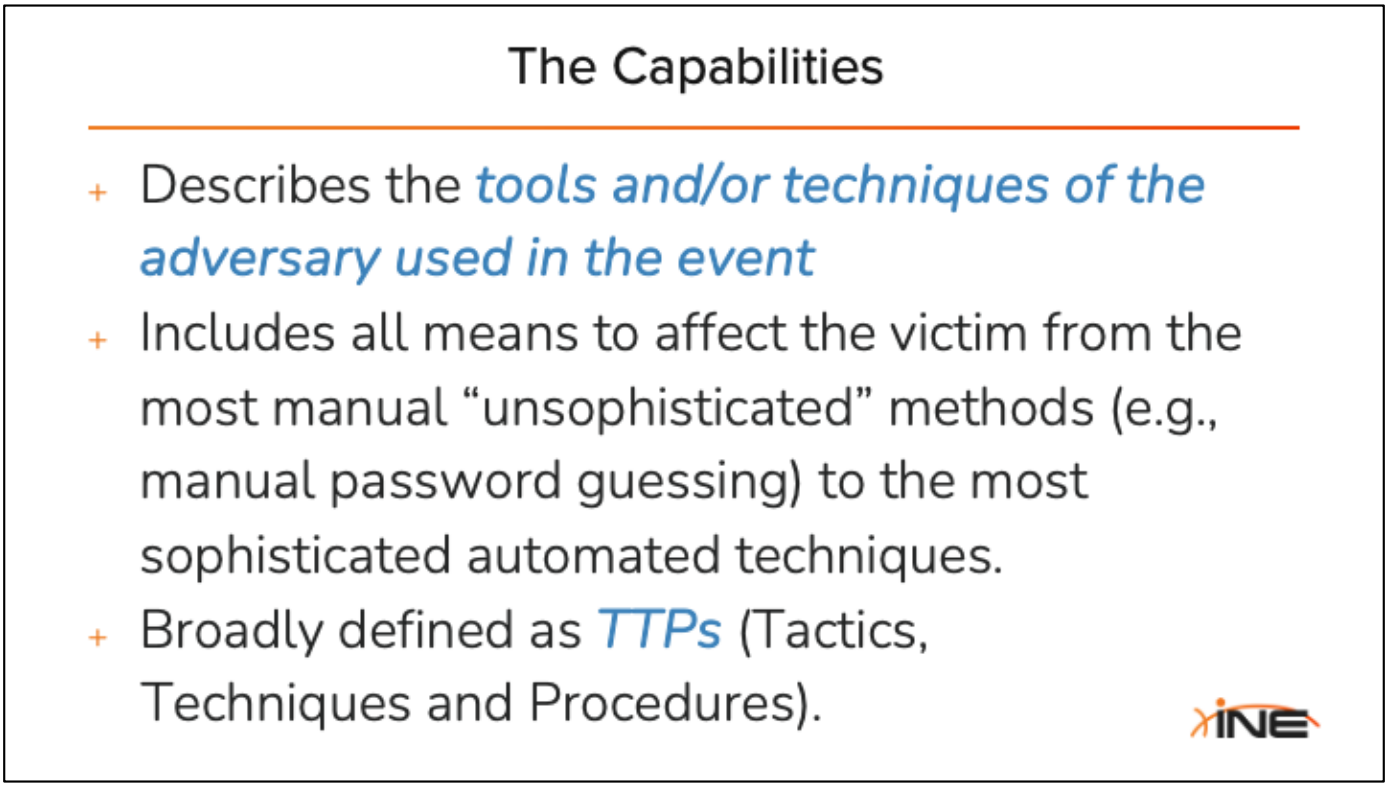
- Key Idea: Infrastructure is the set of resources that the adversary controls (or compromises) to make their attack possible. Think of it as the adversary's operational platform.

- Type 1 Infrastructure
  - Infrastructure which is fully controlled or owned by the adversary or which they may be in physical proximity.
  - Examples include C2 Servers, Phishing Websites (trying to steal login credentials), the Attacker's cloud-based storage

- Type 2 Infrastructure
  - Infrastructure which is controlled by an (witting or unwitting)

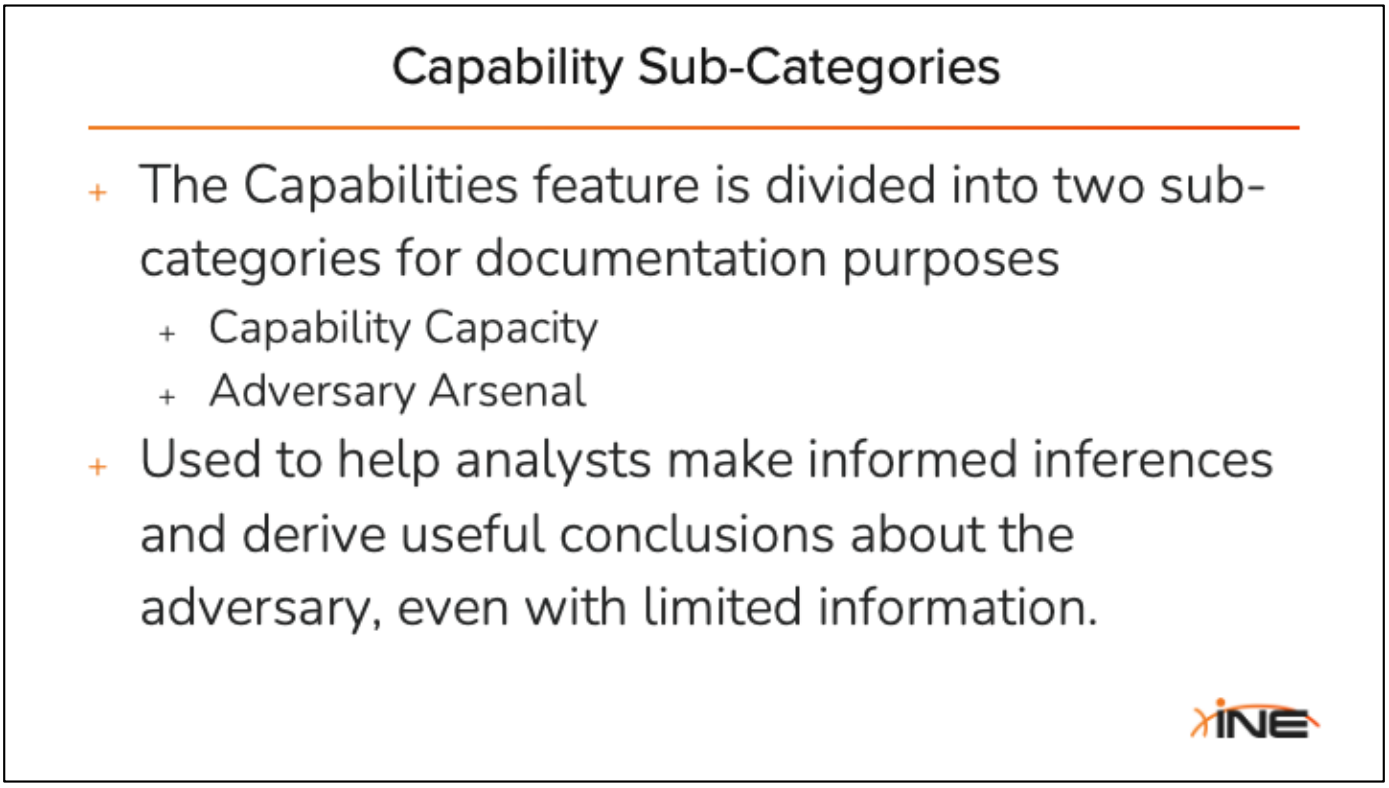
intermediary.
    - Typically, this is the infrastructure that a victim will see as the adversary.
    - It serves to obfuscate the origin and attribution of the activity
    - Examples include zombie hosts, hop-through points, compromised email accounts

- Service Providers
    - Organizations which (wittingly or unwittingly) provide services critical for availability of adversary Type 1 and Type 2 infrastructure
    - Examples include ISPs, Domain Registrars, Web-Mail providers



- Examples:
  - Exploits for vulnerabilities (e.g., zero-day exploits).
  - Malware (such as ransomware, keyloggers, or Trojans).
  - Scripts used to automate tasks or execute commands.
  - Brute-force tools for cracking passwords.
  - Techniques such as social engineering or spear-phishing emails.

- Key Idea: Capabilities are the means by which the adversary enacts their attack. They represent what the adversary can do (their technical prowess), as opposed to how they get their actions delivered (which is the role of infrastructure).



- Capability Capacity
  - Refers to the breadth and depth of the adversary's technical abilities or skills.
  - It focuses on the potential or extent of what the adversary can accomplish using their resources.
  - Essentially, it's a measure of

their operational capability in terms of the range of attacks they can successfully execute.

- Key Aspects:
  - Technical expertise: How skilled is the adversary in executing complex attacks?
  - Knowledge and skillset: The proficiency they have in using various exploits, tools, or vulnerabilities.
  - Flexibility: How adaptable they are in executing different types of attacks or overcoming obstacles (e.g., finding workarounds for security measures).

        - Innovation: How capable they are of creating new methods of attack, such as developing custom malware or zero-day exploits.
        - Resourcefulness: The ability to repurpose tools or innovate new ways of attacking.

- Adversary Arsenal
    - Refers to the specific tools, software, and techniques that the adversary possesses and uses during an attack.
    - It’s the collection of

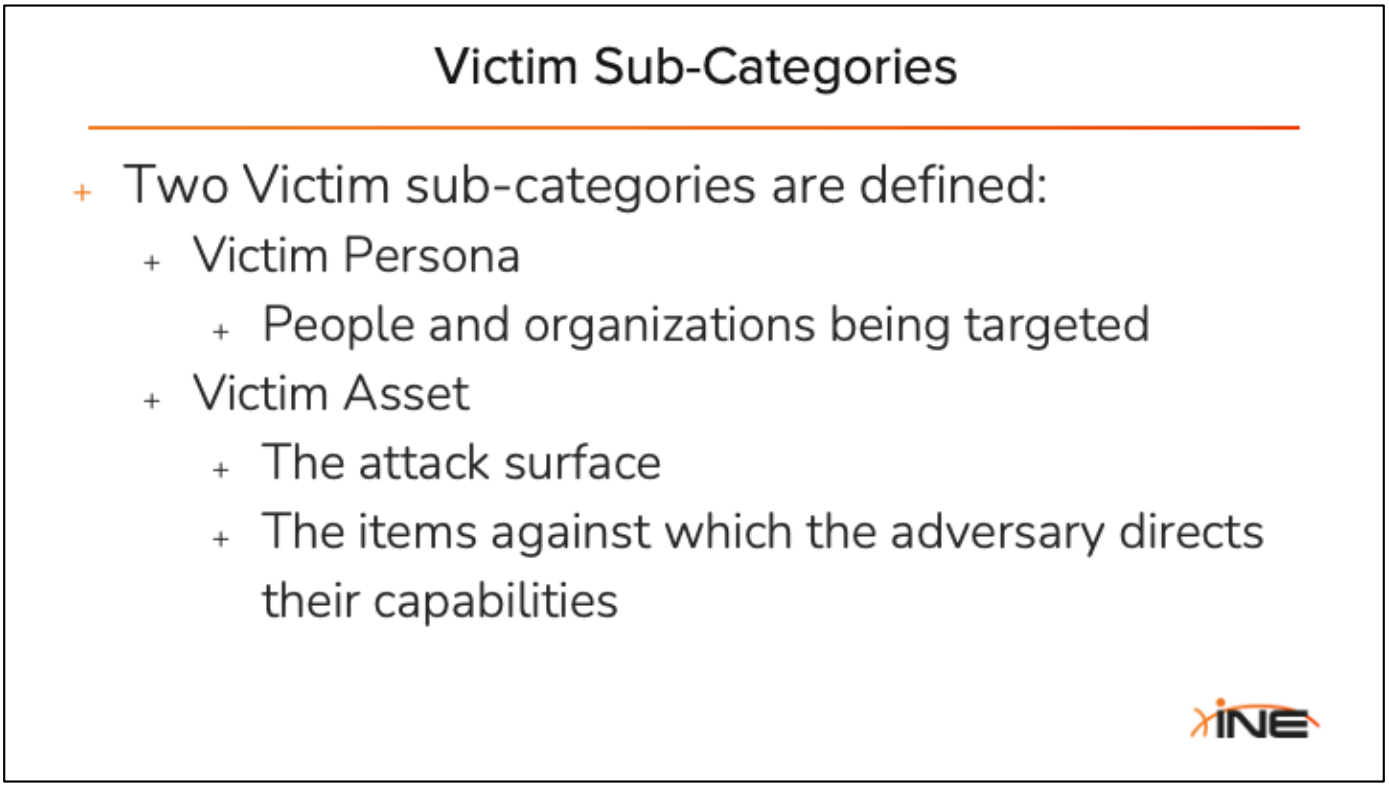
resources they have at their disposal to carry out their operations.

- These can include everything from malware to hacking utilities, exploits, and other digital weapons.
- Populated with data over time as the adversary's attacks are documented

- Even though you might not know the full extent of an adversary's tools, the ones **already identified** in an attack give **insight into their Arsenal**.
- By analyzing the tools, scripts, malware, and techniques used, you can:
  - **Categorize the sophistication** of the observed tools. For example, if the adversary used highly customized malware, this suggests they have access to more than just commodity malware kits.
  - **Investigate correlations** with known threat groups. Many adversaries leave behind distinct indicators (e.g., malware signatures or specific tool usage), which can link them to previously analyzed campaigns. These correlations allow analysts to build a **profile** of likely tools that the adversary possesses.
  - **Assume evolution**: If an adversary has access to a certain class of tools or techniques, it is reasonable to infer that they might have access to or can obtain **related or more advanced capabilities** in the future.

The Victim

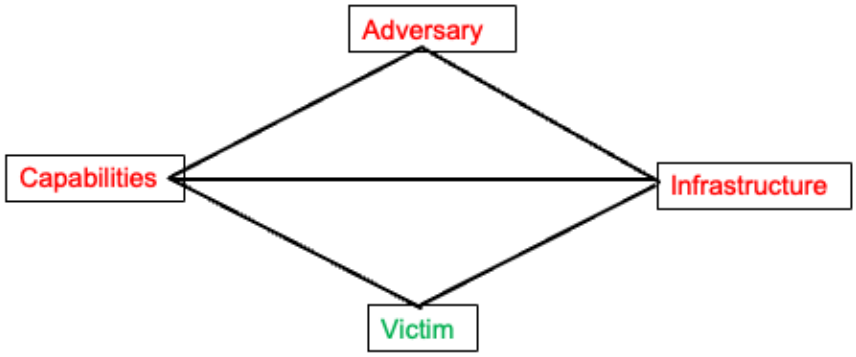
- The *target of the adversary* and against whom vulnerabilities and exposures are exploited and capabilities used
- This entity can take many forms such as:
  - An organization
  - A person
  - An email address
  - A domain



- The “Victim Asset” sub-category includes things like:
  - sets of networks
  - systems
  - hosts
  - email addresses
  - social networking accounts

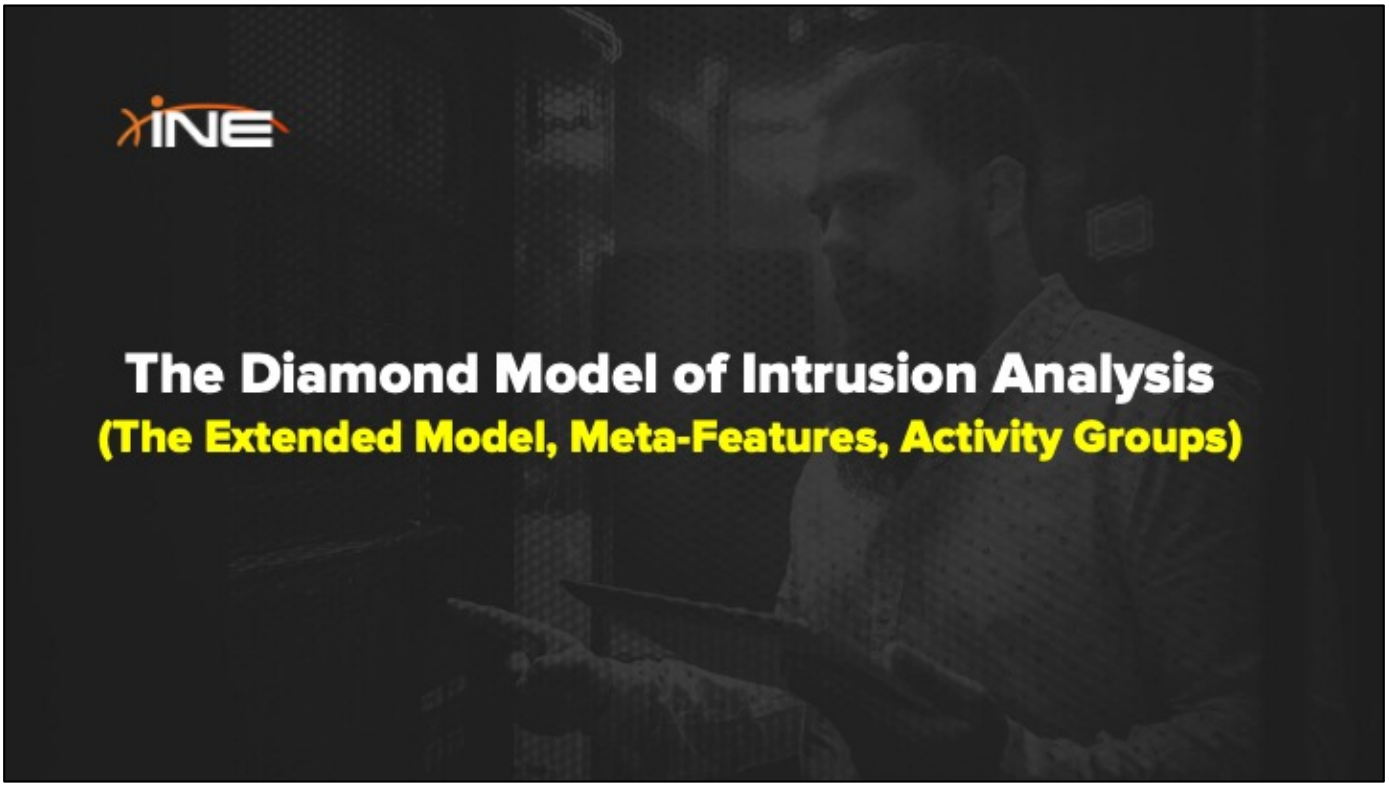
Core Feature Relationships

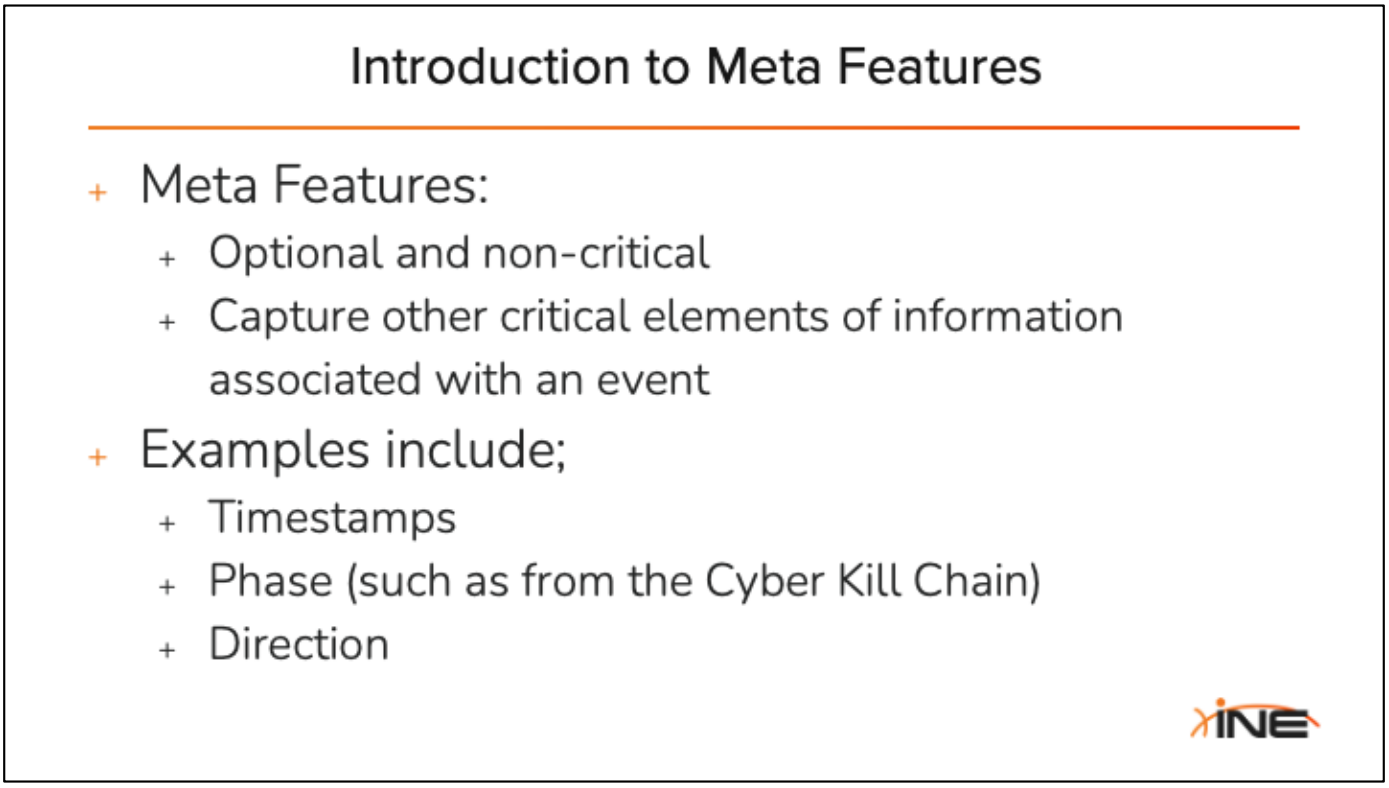
- Core features are “edge connected” displaying their relationships
- Arranged in the shape of a diamond



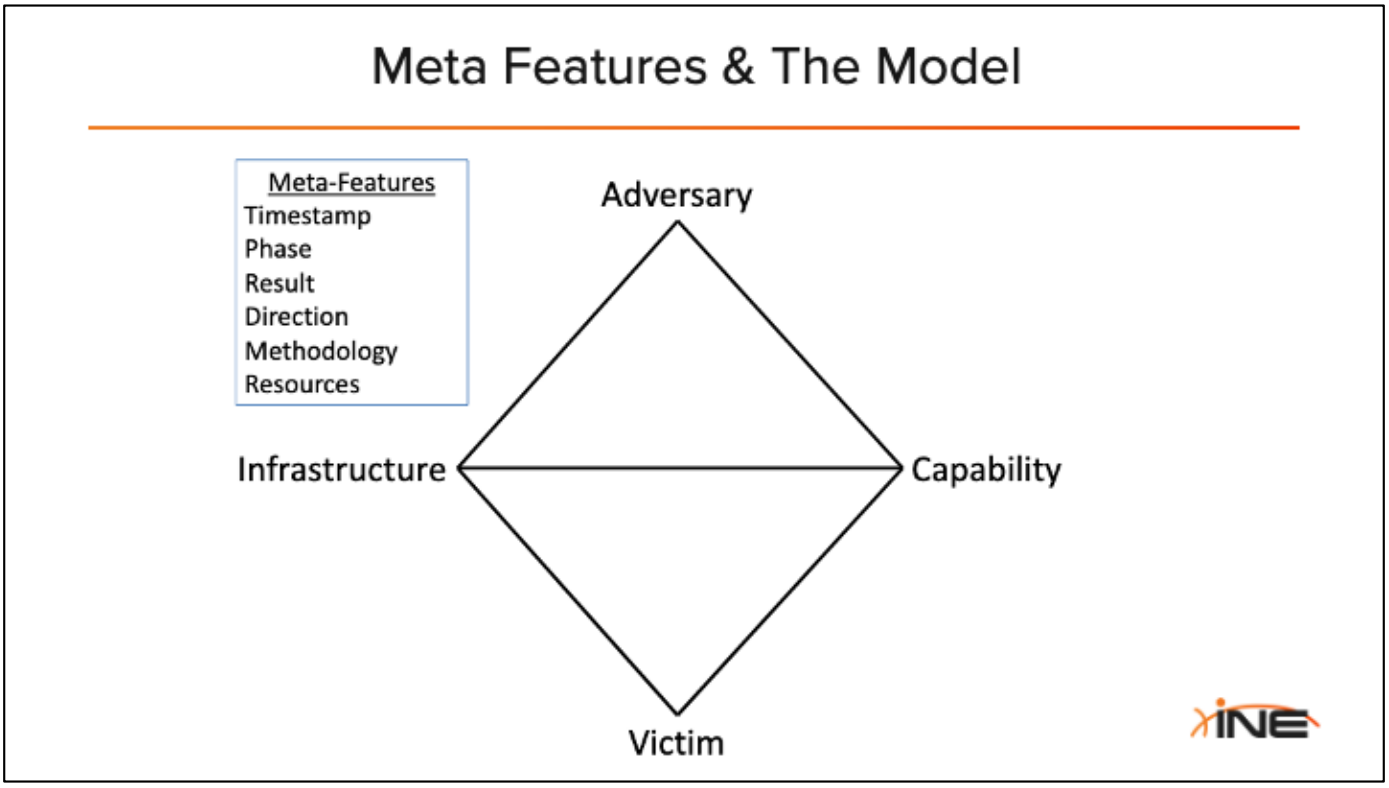
- The edges of the diamond is how you associate the relationship between one core Feature to another core Feature. They are also used to help train your mind about how (in what direction) you should “pivot” when investigating your incident. For example:
  - You discover that your server has been the victim on an incident.
  - As you collect forensic data from your server you should be eyeing that data from the perspective of:
    - How does this data point me back to the Capabilities of the adversary?
    - How does this data point me back to the Infrastructure that was used by the Adversary?

Thanks for Watching!





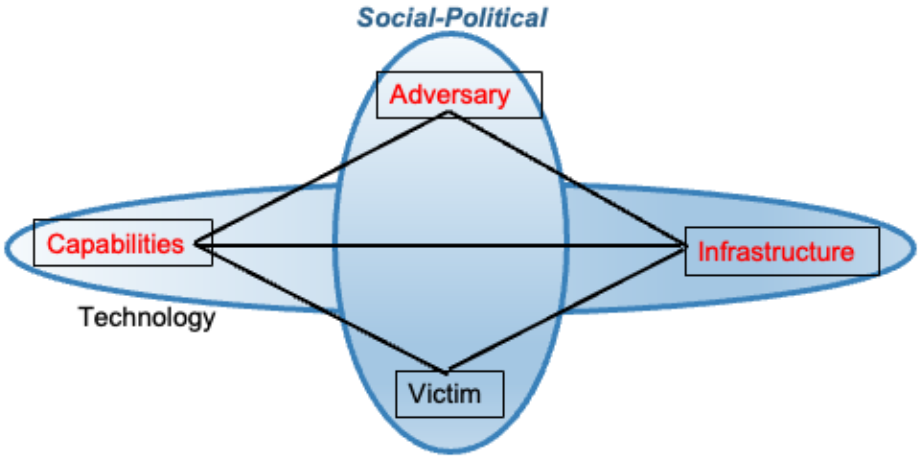
- Just as “meta data” is “data about data” (i.e. data that provides descriptive characteristics about other data) the Diamond Model supports Meta Features



- This is just a visual representation of the Diamond Model and how Meta-Features are typically represented next to it. In practice, all of this data would be stored on a spreadsheet or database and organized in a way that aligns with this model.

The Extended Diamond Model

+ Two common meta-features exist which are often incorporated into an extended Diamond Model



- Social-Political: Defines the relationship between the Adversary and the Victim
- Technology, as a meta-feature, describes the underlying protocols or systems that enable communication and interaction between the Infrastructure and Capabilities. It's the technical means by which tools (Capabilities) interact with resources (Infrastructure).

- For example, if installed malware (CAPABILITY) resolves domains and communicates over HTTP (via an adversary-owned HTTP server) (INFRASTRUCTURE), the technology Meta-Features used are: Internet Protocol (IP), Transport Control Protocol (TCP), Hypertext Transport Protocol (HTTP), and the Domain Name System (DNS).

- By analyzing technology and its potential anomalies/misuse, an analyst discovers new malicious activity regardless of the underlying infrastructure and capability

Diamond "Events"

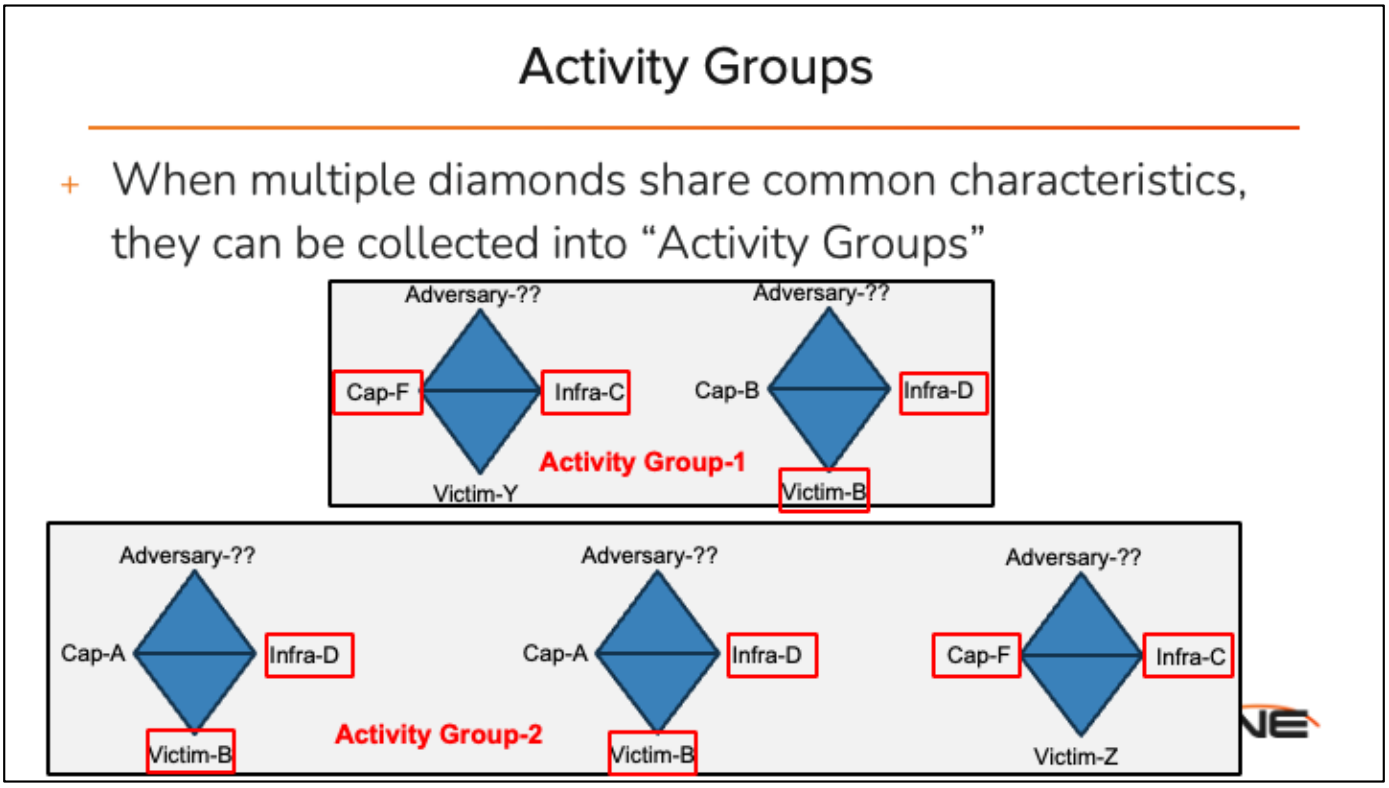
- Each "event" should be analyzed and documented as a single diamond.
- So what constitutes an event?

4 Diamond Event

Axiom 1 *For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result.*

An **event** defines discrete time-bound activity restricted to a specific *phase* where an *adversary*, requiring external *resources*, uses a *capability* and *methodology* over some *infrastructure* against a *victim* with a given *result*. Of course, not all of the features need to be known to create an event. In almost all cases, most features are expected to be unknown and completed only after the initial discovery as new facts are revealed and more data is gathered.

- The quote above is taken directly from the Diamond Model original paper located at:
- https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf



- An **Activity Group** is a **collection of related intrusion events** (diamonds) that share common characteristics, indicating they are likely conducted by the same adversary or set of adversaries.
- Typically, two or more “Core Features” of diamonds need to be in common for those diamonds to be placed into the same Activity Group however, if multiple diamonds occur (against the same victim) within a short span of time, even though each diamond might contain different Capabilities and Infrastructure (with the Adversary initially being unknown) with the only commonality being the Victim…if they all happened within a few seconds or minutes of each other they could logically be assumed to be a part of the same Activity Group because it is safe to say they are all related.

Thanks for Watching!