Samuel A. Ntombwen

College of Science, Engineering and Technology, Grand Canyon University

CYB-630-O500 ENTERPRISE CYBER LAW AND COMPLIANCE STRATEGIES

Instructor: Dr. JEAN PIERRE NZIGA

Date: September 25, 2024

Diamond Model of Intrusion Analysis and Cyber Kill Chain Model

There are several approaches, frameworks, and techniques used to track and analyze the various characteristics of cyber intrusions by threat actors when it comes to cybersecurity. In this paper, we will review two well-known approaches; the diamond model of intrusion analysis and the cyber kill chain model.

Diamond Model of Intrusion Analysis

The Diamond Model of Intrusion Analysis is a cybersecurity framework that helps organizations analyze cyber intrusions. It was first proposed in a 2013 U.S. Department of Defense technical report titled “The Diamond Model of Intrusion Analysis” by Sergio Caltigirone, Andrew Pendergast, and Christopher Bets (Caltagirone et al., 2013).

The main objectives of this model are to identify specific attackers, understand the tactics, threats, and procedures they use, and be able to respond more effectively to cyber incidents as they occur. This framework has four major components: adversaries, infrastructure, capabilities, and targets. Furthermore, these components have several links such as adversary-victim, adversary-infrastructure, and victim-capability. The Diamond Model primarily focuses on the task of attribution: identifying those responsible for a cyber incident. It is a highly flexible schema and can be applied to any threat vectors such as advanced persistent threat (APT) or insider threats.

BENCHMARK - ATTACK VECTORS MODELS

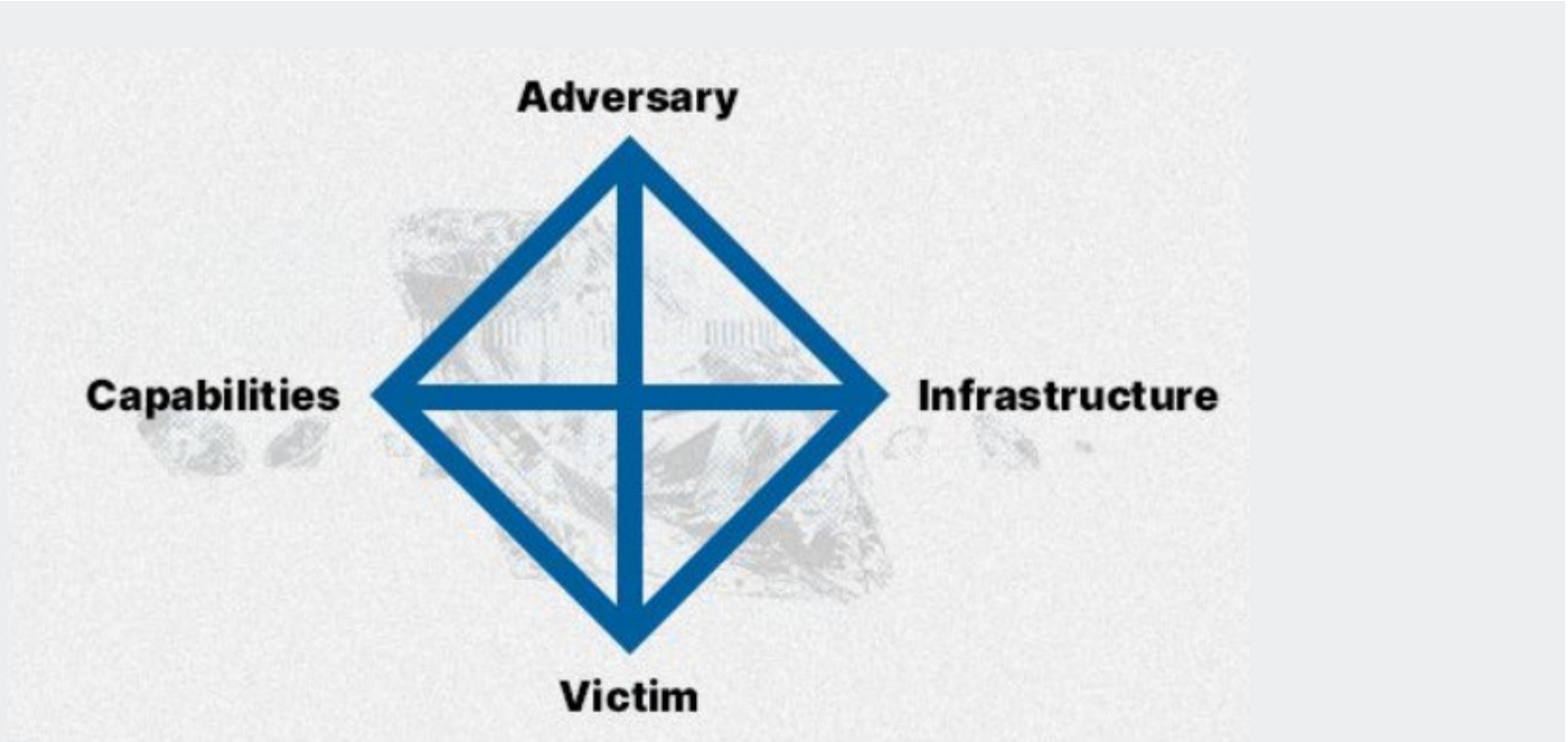

Fig 1. The Diamond Model of Intrusion Analysis

How the Diamond Model Works

The four main components mentioned above are explained as:

- **Adversary**: The attacker or group responsible for an attack.
- **Infrastructure**: The resources or assets the adversary (attacker) uses during the attack. These can be laptops, servers, networks, or IP addresses.
- **Capability**: A method, tool, or technique used by the attacker during the attack. Examples are SQL injection, or email phishing.
- **Victim**: The individual or organization the adversary targets during the attack.

The relationships or links mentioned above are:

- **Adversary-victim**: The interaction between the adversary (attacker) and the victim (target). This relationship concerns questions such as why the attacker selected this target and the attacker's motivations and objectives.
- **Adversary-infrastructure**: This is about the type of technical resources the attacker uses during the attack. This relationship concerns how the attacker establishes and maintains its cyber operations.
- **Victim-infrastructure**: This relationship concerns the attacker's use of various channels, methods, and vectors against the target.
- **Victim-capability**: This relationship concerns specific tactics and attack signatures used against the target or victim.

Benefits of Using the Diamond Model

Holistic Understanding

The Diamond Model examines and analyzes the technical, human, and organizational aspects of a cyberattack. This is done in the form of the attacker and target.

Structured Analysis

This model provides a clear, organized way for cybersecurity professionals to structure and process data relating to cyber threats and attacks. This makes it easier to collaborate and share information.

Incident Response and Threat Intelligence

The Diamond Model of Intrusion Analysis offers benefits both for threat intelligence (prior to an attack) and incident response (after an attack), helping analysis collect and analyze data.

By modeling the relationships between adversaries, victims, infrastructure, and capabilities, the Diamond Model helps cybersecurity professionals see how the different elements of a cyberattack interact with and influence one another.

Key Attributes of Each Element of the Diamond Model

The elements of the Diamond Model listed above have different attributes that include valuable additional information. For example some key attributes of the adversary element are identity, name, motivations and objectives, technical capabilities, skills and knowledge.

Cyber Kill Chain Model

Lockhead Martin derived the kill chain framework based on a military model that was originally established to identify, prepare for attack, engage, and destroy the target. The framework has since evolved to better anticipate and recognize insider threats, social engineering, advanced ransomware and innovative attacks.

It is a series of steps that trace stages of a cyberattack from the first stage of reconnaissance to the exfiltration of data. The kill chain framework helps cybersecurity professionals understand and combat ransomeware, security breaches, and APTs.

BENCHMARK - ATTACK VECTORS MODELS

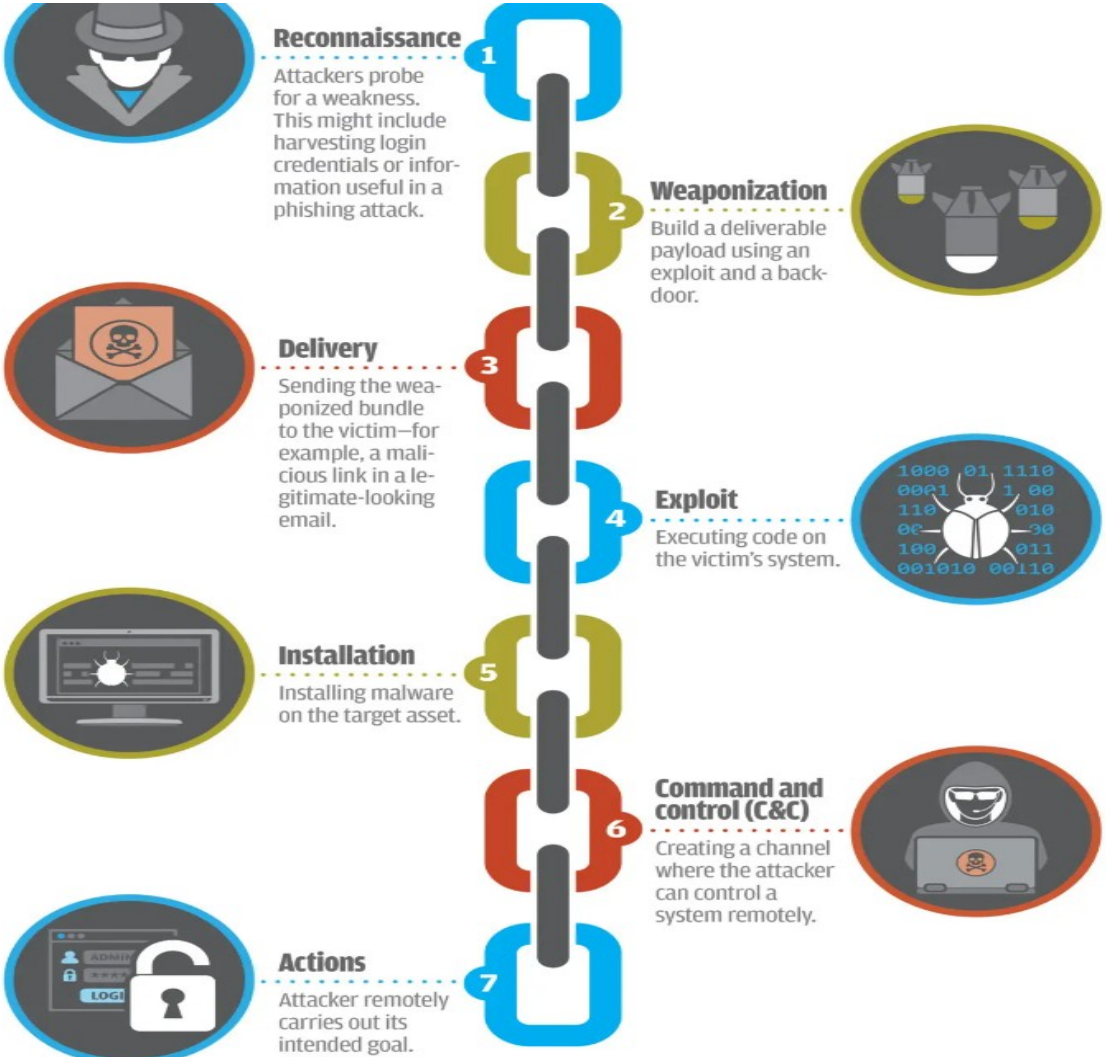

Fig 2. The Cyber Kill Chain Model

How the Cyber Kill Chain Works

There are several major stages of the cyber kill chain model that range from reconnaissance to lateral movements, to data exfiltration. All common attack vectors trigger some activity on the cyber kill chain. There seven stages of the kill chain: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.

Reconnaissance: This is the observation stage (it can be passive or active reconnaissance) where the attacker assesses the situation in order to identify the target and tactics for the attack.

Weaponization: In this stage the attacker creates or selects malware or exploits to target vulnerabilities that were found in the reconnaissance phase.

Delivery: The malware or exploit is being deployed to the target system

Exploitation: Here the attacker gains initial access and establish a foothold.

Installation: Once and attacker gets a foothold of a system, they begin executing the malware and establishing persistence.

Command and Control: In this stage the attacker communicates with the compromised system to control it remotely.

Actions on Objectives: This is where the attacker achieves his goals such as data exfiltration, disruption, or extortion.

Differences

While both the Diamond Model, and Cyber Kill Chain are valuable tools for understanding and defending against cyberattacks. Though they both aim at securing assets, they have their differences in areas such as focus, granularity, and application.

Focus

The Cyber Kill Chain emphasizes on the attack stages, giving the cyber professional a picture of what an attacker would do next if there is an ongoing attack. The Diamond Model focuses on the attacker's motivations and capabilities. This helps the cyber professional to know what type of attack would be carried out based on the reason and the capability of the attacker.

Granularity

The Cyber Kill Chain is more specific. It gives you the seven stages of an attack and exactly what to expect during those stages. The Diamond Model of Intrusion Analysis offers a broader perspective.

Application

The Cyber Kill Chain is more focused on incident response, while the Diamond Model of Intrusion Analysis is useful for threat intelligence and threat hunting.

Approaches to Protect Privacy

These are several approaches individuals, organizations, and governments use to protect privacy. Some of them are;

Encryption

This involves converting sensitive information into a coded form, making it unreadable to anyone without the proper decryption key. This is utilized by mostly governments and organizations for storing sensitive data to preserve integrity.

Network Security

This refers to the measures used to protect the information and assets stored on computer networks from unauthorized access, theft, or damage. Tools such as firewalls, intrusion detection and prevention systems are used to achieve network security.

BENCHMARK - ATTACK VECTORS MODELS

Access Control

Access control is a method of restricting access to sensitive information to only authorized persons. This can be achieved through the use of passwords, multi-factor authentication, and role-based access control. These methods ensure that only those with the proper authorization can access sensitive data, thereby reducing the risk of data breaches and unauthorized access. This is used by individuals, organizations, and governments.

Backups

It is almost impossible to completely prevent a cyber attack. That is why it is important to back up data regularly to ensure that data is preserved in the event of a successful breach. Organizations, governments, and individuals use backup technologies such as detachable drives, cloud storage, and hybrid storage.

Physical Security

This might sound out of place when talking about cybersecurity but physical security is very important. It involves measures used to ensure physical devices and facilities that store sensitive information are secured. This can include locking devices in a secure storage cabinet or vault, implementing access control systems with biometric authentication or key cards, and installing security cameras and alarms in sensitive areas.

Identification and Protection

The Cyber Chain Kill Model and the Diamond Model of Intrusion Analysis help to identify and protect against cybercrime threat vectors, motivations, and ideologies by giving the cyber professionals a clear picture of the path an attacker would take to accomplish his objective. When these cyber professionals are equipped with such information, they can use counter tools and techniques to prevent these attacks from happening.

Cyber Kill Chain Model

These are some tools and techniques that can be used to counter cyber threats or attacks based on the Cyber Kill chain model.

- **Reconnaissance**: Vulnerability scanners, network traffic analysis tools, threat intelligence feeds.
- **Weaponization**: Sandboxes, endpoint protection and response (EDR) solutions to detect malicious code generation.
- **Delivery**: Advanced firewalls with web filtering and email security features, intrusion detection and prevention systems (IDS/IPS).
- **Exploitation**: Patch management, code hardening techniques, application whitelisting.
- **Installation** : EDR solutions for detecting suspicious file execution and persistence mechanisms, endpoint sandboxes.
- **Command and Control**: Network traffic analysis tools such as WireShark to identify suspicious communication patterns, DNS filtering, advanced firewalls blocking C2 server connection.

- **Actions on Objectives**: Data leak prevention (DLP) tools, file integrity monitoring, application control solutions to prevent unauthorized data access or exfiltration.

Diamond Model of Intrusion Analysis

- **Motivations**: Threat intelligence feeds to identify active threat groups and their goals. Incident analysis to understand attacker's objectives.
- **Capabilities**: Vulnerability scanners to assess potential attacker targets, security assessments to identify weaknesses exploitable by attackers with specific skill sets.
- **Infrastructure**: Network traffic analysis tools to detect C2 server connections. Network segmentation to limit attacker movement. Endpoint security solutions to isolate compromised systems.
- **Tactics and Techniques**: EDR solutions with deep behavioral analysis to detect TTPs, deception tools to mislead attackers and gather intelligence on their methods.

References

Buckbee, M. (June 2, 2023). What is The Cyber Kill Chain and How to Use it Effectively. Retrieved from https://www.varonis.com/blog/cyber-kill-chain

Tidmarsh, D. (November 7, 2023). Diamond Model of Intrusion Analysis: What, Why, And how to Learn. Retrieved from https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/diamond-model-intrusion-analysis/