Benchmark – Attack Vectors Models

Ryan Coon

CYB-630

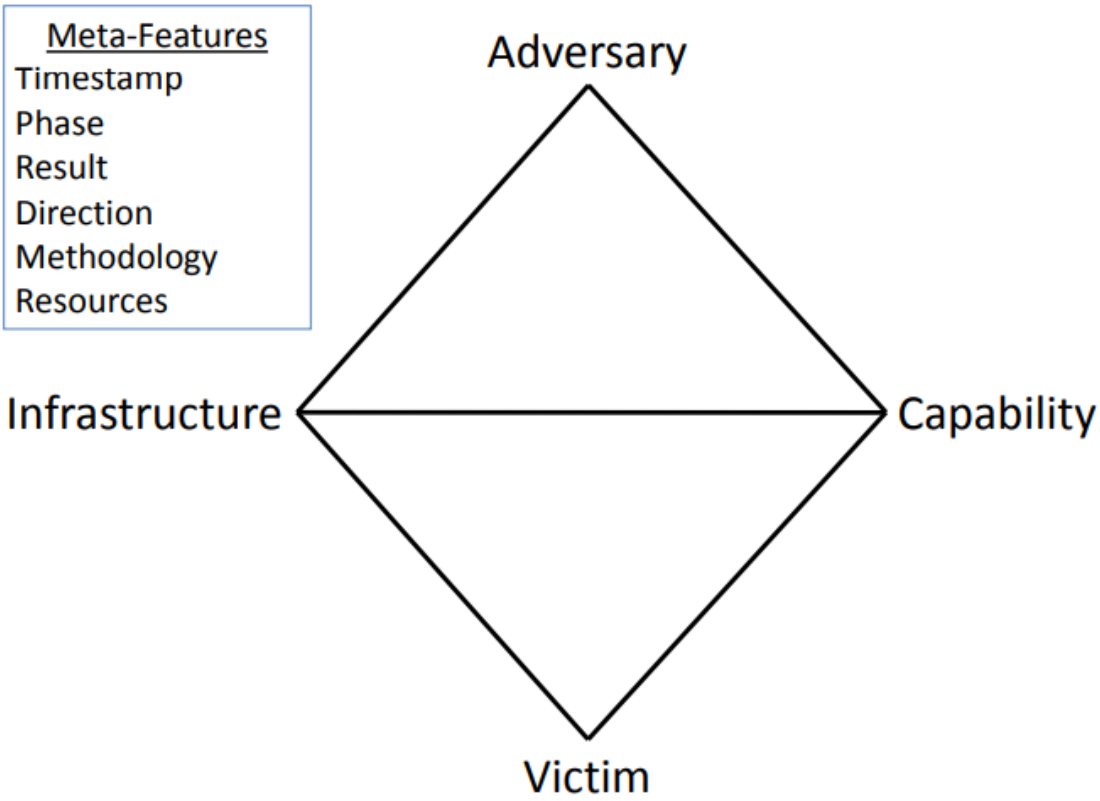
Dr. Hermano Jorge De Queiroz

May 28, 2025

Attack Vectors Model:

Diamond Model of Intrusion Analysis

The main objectives of the Diamond Model of Intrusion Analysis is to identify specific attackers, understand their tactics and procedures they use, and more effectively respond to cyber incidents as they occur.



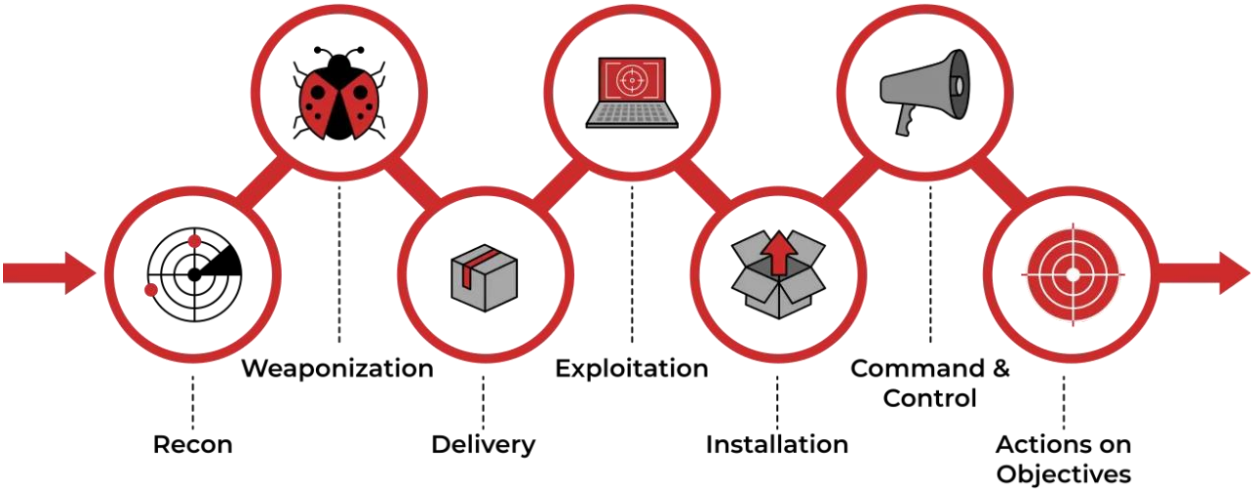
This model uses four vertices to represent the core components of an attack:

- Adversary – The attacker and their tools.
- Infrastructure – The physical and logical communication channels used to deliver, deploy, and control the adversary's capability.
- Capability – The capabilities of the adversary.

- Victim – The organizations, people, or other assets that the adversary is targeting to exploit through their vulnerabilities.

Cyber Kill Chain Model

The Cyber Kill Chain model is a strategic framework developed to understand and combat cyberattacks by breaking them down into distinct stages. This model helps security teams identify, prevent, and respond to attacks more effectively.



This model uses 7 phases that include:

- Reconnaissance - In this initial phase, attackers gather information about their target. This can include identifying network structures, employee details, and potential vulnerabilities. Techniques may involve social engineering, scanning, and researching publicly available information.
- Weaponization - After gathering intelligence, attackers create a weaponized payload. This often involves combining malware with a delivery mechanism, such as a phishing email or a malicious link. The goal is to prepare a tool that can exploit the target's vulnerabilities.
- Delivery - This stage involves transmitting the weaponized payload to the target. Common delivery methods include email attachments, malicious websites, or USB drives. The effectiveness of this stage relies on the success of the previous reconnaissance phase.

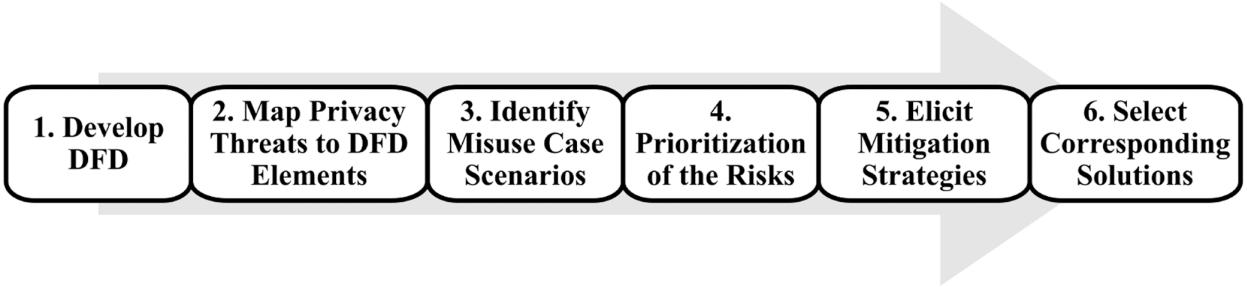
- Exploitation - Once the payload is delivered, the attacker exploits a vulnerability in the target's system. This could involve executing malicious code or taking advantage of software flaws to gain unauthorized access.
- Installation - After exploitation, the attacker installs malware on the target system. This malware can create a backdoor for future access, allowing the attacker to maintain control over the compromised system.
- Command and Control (C2) - In this phase, the attacker establishes a command and control channel to communicate with the compromised system. This allows them to send commands, exfiltrate data, or deploy additional malicious payloads.
- Actions on Objectives - Finally, the attacker achieves their goals, which may include data theft, system disruption, or espionage. This stage represents the culmination of the attack, where the attacker executes their intended actions.

How these two models differ

Feature	Diamond Model of Intrusion Analysis	Cyber Kill Chain Model
Focus	Relationships between adversary, capability, infrastructure, and victim	Stages of a cyberattack
Application	Post-incident analysis	Proactive defense
Nature of Analysis	Cyclical	Linear
Use of Information	Interactions and motivations	Tactics, techniques, and procedures

Privacy Protection Approaces

The LINDDUN threat model is a structured approach to identifying and mitigating privacy threats in systems and applications. It is particularly useful during the early stages of development, allowing teams to proactively address privacy concerns before they become significant issues. The model focuses on various aspects of privacy and provides a systematic way to analyze potential threats.



LINDDUN is an acronym that stands for the following privacy threats:

- Linkability - This threat concerns the ability to link different pieces of data to the same individual. For example, if a user interacts with multiple services, their activities could be linked back to their identity.
- Identifiability - This refers to the risk of identifying individuals from data that is supposed to be anonymous. If data can be re-identified, it poses a significant privacy risk.
- Non-repudiation - This aspect deals with the ability of users to deny their actions. If users can deny their actions, it can lead to accountability issues, especially in sensitive transactions.
- Detectability - This threat involves the ability of third parties to detect user activities. If user actions can be easily monitored, it compromises their privacy.
- Disclosure of information - This refers to the risk of unauthorized access to personal data. If sensitive information is disclosed, it can lead to privacy violations.
- Unawareness - This aspect addresses the lack of user awareness regarding how their data is being used. Users may not be informed about data collection practices, leading to privacy concerns.

- Non-compliance - This threat involves failing to comply with privacy regulations and standards. Non-compliance can result in legal repercussions and loss of user trust.

How LINDDUN Works

The LINDDUN model operates through a systematic process that includes:

- Identifying Assets - Determine what personal data is being collected and processed.
- Analyzing Threats - Use the LINDDUN categories to identify potential privacy threats associated with the data.
- Assessing Risks - Evaluate the likelihood and impact of each identified threat.
- Implementing Countermeasures - Develop strategies to mitigate the identified threats, such as data anonymization, encryption, and user consent mechanisms.

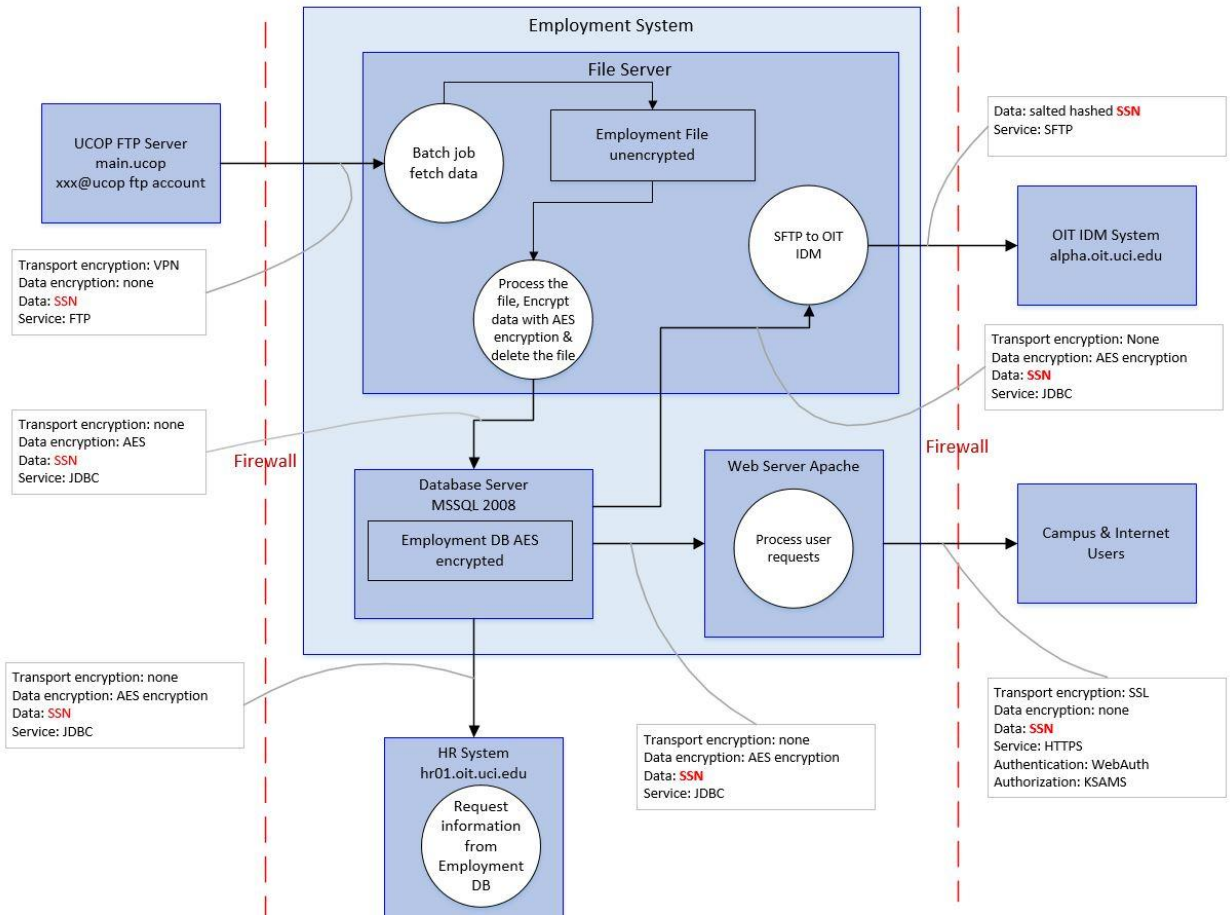
Benefits of Using LINDDUN

- Proactive Privacy Management - By identifying threats early in the development process, organizations can integrate privacy considerations into their design and architecture.
- Structured Approach - The model provides a clear framework for analyzing privacy threats, making it easier for teams to communicate and collaborate on privacy issues.
- Compliance Support - LINDDUN helps organizations align their practices with privacy regulations, reducing the risk of non-compliance.

Privacy Theat Modeling, is a proactive process that helps identify and address potential privacy risk in individuals, systems, and applications. Which is a great approach for individuals, organizations, and government levels to address privacy threats. This process includes analyzing the collection, storage, processing, and sharing of personal data to foresee and mitigate potential privacy risks and breaches. Yet, it is imperative to note, that using several privacy threat models is recommended, as an approach to privacy protection that can include:

- STRIDE
- Central Differential Privacy
- DREAD
- LINDDUN

Cyber Threat Models



Data Flow Diagrams

Data Flow Diagrams (DFDs) are powerful tools in cybersecurity that help visualize the flow of data within a system. They play a crucial role in identifying and protecting against cybercrime threat vectors, motivations, and ideologies. DFDs provide a graphical representation of how data moves through a system, highlighting the processes, data stores, and external entities involved. This visualization helps security professionals understand the architecture of a system and identify potential vulnerabilities.

Understanding Adversary Behavior - DFDs can help security teams analyze how attackers might exploit vulnerabilities in data flows. By understanding

the motivations behind cybercrime—such as financial gain, political activism, or personal vendettas—organizations can better anticipate potential attack strategies.

Identifying Targeted Data - Different attackers have different motivations. For example, a hacker motivated by financial gain may target credit card information, while a hacktivist may seek to expose sensitive government data. DFDs help identify which data is most likely to be targeted based on the motivations of potential adversaries.

Assessing Ideological Threats - By visualizing data flows, organizations can also consider the ideologies behind certain cyber threats. For instance, understanding that a group may target specific data due to ideological beliefs (e.g., political or social causes) can inform the development of tailored security measures.

PASTA Threat Modeling

The PASTA (Process for Attack Simulation and Threat Analysis) threat modeling methodology is a structured approach designed to identify and mitigate potential cyber threats by simulating attacks and analyzing the associated risks. This framework is particularly effective in understanding cybercrime threat vectors, motivations, and ideologies. PASTA is a risk-centric threat modeling methodology that emphasizes the business objectives and the potential impact of threats on those objectives. It consists of several phases that guide teams through the process of identifying vulnerabilities and assessing risks.

Phases of PASTA

Definition of Objectives - This initial phase involves understanding the business objectives and the critical assets that need protection. By identifying what is most valuable, organizations can prioritize their security efforts.

Definition of the Technical Scope - In this phase, the technical environment is defined, including the architecture, technologies, and data flows. This helps in understanding how data moves through the system and where vulnerabilities may exist.

Application Decomposition - The application or system is broken down into its components, allowing for a detailed analysis of each part. This decomposition helps identify potential attack surfaces and entry points for cybercriminals.

Threat Analysis - This phase involves identifying potential threat vectors and the motivations behind them. By analyzing various attack scenarios, organizations can understand how attackers might exploit vulnerabilities.

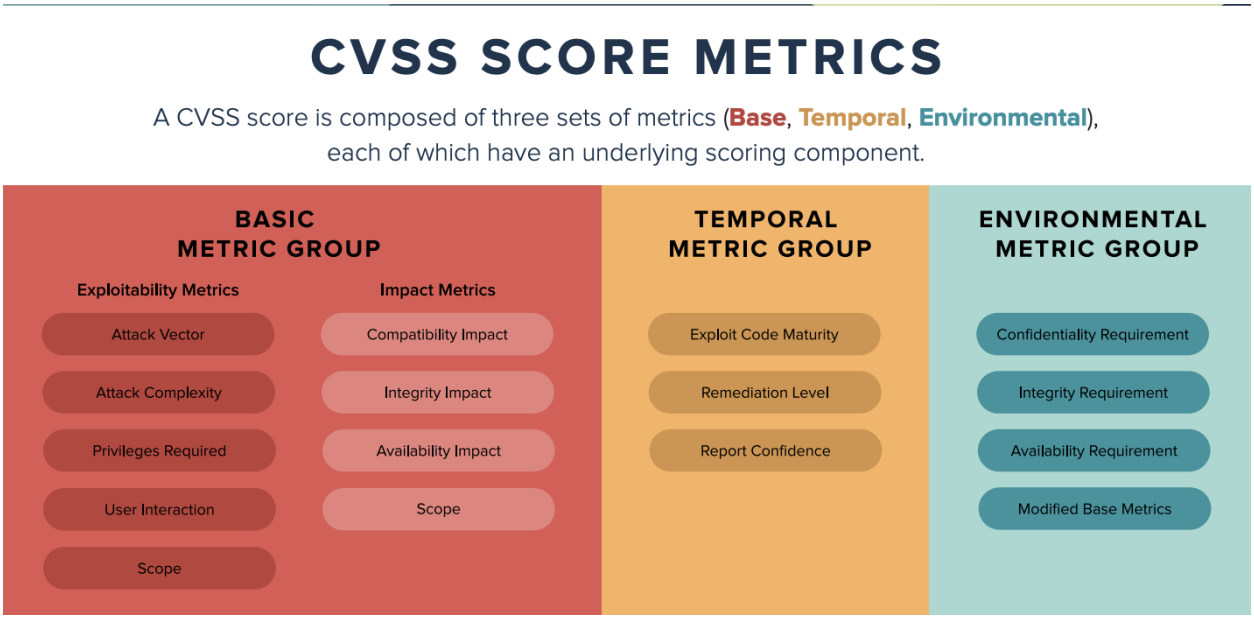
Vulnerability Analysis - Here, the identified threats are matched against known vulnerabilities in the system. This helps in assessing the likelihood of an attack and the potential impact on the organization.

Attack Simulation - In this phase, simulated attacks are conducted based on the identified threats and vulnerabilities. This practical approach allows teams to see how an attack might unfold and the effectiveness of existing security measures.

Risk Analysis and Management - Finally, the risks associated with the identified threats are analyzed, and mitigation strategies are developed. This phase focuses on prioritizing risks and implementing controls to protect against them.

Motivations - PASTA emphasizes understanding the motivations behind cyberattacks, which can include financial gain, political activism, or personal vendettas. By analyzing these motivations, organizations can anticipate potential attack strategies and tailor their defenses accordingly.

Ideologies - The methodology also considers the ideological aspects of cyber threats. For instance, understanding that certain groups may target specific data due to ideological beliefs (e.g., hacktivism) can inform the development of targeted security measures.



CVSS

The Common Vulnerability Scoring System (CVSS) is a standardized framework used to assess the severity of security vulnerabilities in software and systems. It plays a crucial role in identifying and protecting against cybercrime threat vectors, motivations, and ideologies.

CVSS provides a numerical score (ranging from 0 to 10) that reflects the severity of a vulnerability, along with a set of metrics that help organizations understand the potential impact of that vulnerability. The scoring is based on three main metric groups:

Base Metrics - Reflects the intrinsic characteristics of a vulnerability that are constant over time and across environments.

Temporal Metrics - Reflects the characteristics of a vulnerability that change over time, such as the availability of a fix.

Environmental Metrics - Reflects the characteristics of a vulnerability that are specific to a particular environment, such as the importance of the affected system.

Motivations of Cybercriminals

Cybercriminals are often motivated by various factors, including financial gain, ideological beliefs, or personal vendettas. By understanding the CVSS scores of vulnerabilities,

organizations can infer which vulnerabilities might attract specific types of attackers. For instance, vulnerabilities that expose sensitive financial data may attract financially motivated attackers.

Ideological Threats

Certain groups may target vulnerabilities based on ideological beliefs (e.g., hacktivism). CVSS can help identify vulnerabilities in systems that are critical to organizations with political or social significance, allowing for tailored security measures to protect against ideologically motivated attacks.

References:

Azam, N., Michala, L., Ansari, S., & Truong, N. B. (2022). Data Privacy Threat Modelling for Autonomous Systems: A Survey from the GDPR's Perspective. IEEE Transactions on Big Data, 9(2), 1–27. https://doi.org/10.1109/tbdata.2022.3227336

DRATA. (2024). PASTA Threat Modeling: Tutorial + Best Practices. Drata.com. https://drata.com/grc-central/risk/pasta-threat-modeling

Flare. (2023, March 21). Diamond Model of Intrusion Analysis: A Quick Guide - Flare. Flare | Cyber Threat Intel | Digital Risk Protection. https://flare.io/learn/resources/blog/diamond-model/

Neetrox. (2024, June 8). The Cyber Kill Chain | Incident Response Process | InfoSec Write-ups. Medium; InfoSec Write-ups. https://infosecwriteups.com/the-crucial-link-between-the-cyber-kill-chain-and-incident-handling-process-8c3288b8392f

Olaes, T. (2020, April 8). Temporal CVSS Scores. Balbix. https://www.balbix.com/insights/temporal-cvss-scores/

University of California Irvine. (n.d.). Data Flow Diagram | UCI Information Security. Data Flow Diagram. https://www.security.uci.edu/program/risk-assessment/data-flow-diagram/