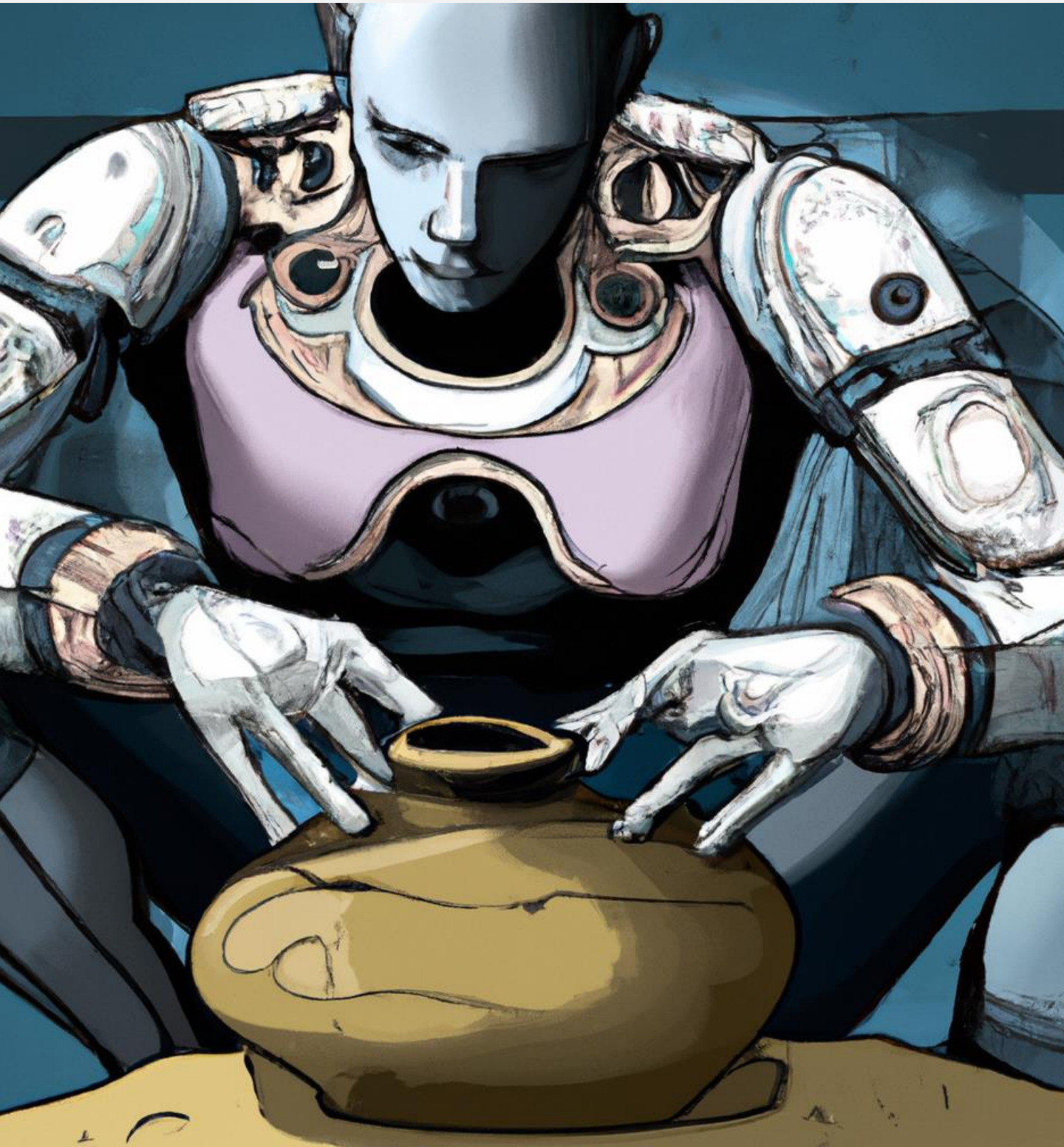
XRATOR
CONQUER YOUR RISK

WHITEPAPER
January 2023

REVAMPING THREAT MODELING

Improving Cyber Risk Management by integrating real-world threat activity into the risk mitigation process.



Foreword

Jean-Loup Richet (PhD)
Associate professor, co-director of the Risk Chair, Sorbonne Business School

This manuscript, "*Revamping Threat Modeling: Improving Cyber Risk Management by integrating real-world threat activity into the risk mitigation process*", provides an invaluable look at the current state of threat modeling and how it can be improved to better manage cyber risks.

This white paper is especially timely considering the current threat landscape. Recent advancement in AI technologies have induced extreme growth and innovation on the threat side, leading to increased cyber attacks, and constantly changing and adapting threats landscape. Organizations need to be able to effectively and efficiently identify, assess, and mitigate risks.

The authors make a compelling case that threat activities are often underestimated in risk management, and offer a comprehensive review of existing threat modeling methodologies. I would rejoin the authors here: threats are also forgotten in research **[1]**.

"I would like to make a call for more academic papers on cyber threat intelligence, as we need more contribution to the field aligned with the needs of cyber security professionals."

Then, the authors provide specific suggestions on aligning threat modeling with threat intelligence, and finally discuss how this knowledge can be incorporated into the risk management process, relying on existing and recognized methodologies such as PASTA and EBIOS RM.

Overall, this manuscript is a must-read for anyone interested in the latest developments in cyber risk management.

Introduction

The Importance of understanding the Attacker.

As the reliance on technology and interconnected systems continues to grow, so too do the potential consequences of cyber attacks.

From disruption of essential services and infrastructure to financial losses and damage to reputation, the stakes of inadequate cyber risk management are high.

When security incidents occur, there is usually little understanding of who the attacker is, why they attack, and how they operate. It is difficult to make informed decisions about countermeasures.

Cybercriminals who are neither identified nor held accountable for their actions will continue their criminal behavior. When we do not understand the attacker, we can only suffer the results of their actions.

"The ability to anticipate and mitigate cyber threats is the difference between proactively managing risk and reacting to disaster."

Improving Risk Assessment through Intelligence on Real-World Cyber Threats

Cyber Risk Management is a preventive activity aiming to reduce an organization vulnerability, reduces harms to the system and increase the risk taken by adversaries in their malicious operation. The problem is that threat assessment in risk management is rarely tied to real-world cyber threat that are effectively accurate in relation with the studied object.

Improving risk assessment requires intelligence on these threats. We therefore see the potential to develop models and tools that enable automatic or semi-automatic classification and discovery of cyber adversaries, attack methods and ultimate motivation. The challenge is that cybersecurity operations require clear terminology to describe threats, attacks and their origins. In addition, cybersecurity tools and technologies need semantic models to automatically identify threats and anticipate attacks opportunities.

In this article, we explore the utility of threat analysis in the context of cyber risk management, conducting a review of various threat modeling methods. Building on this foundation, we then present our contribution to the field: the integration of cyber threat intelligence into the threat modeling and risk management processes.

Key Takeaways

1. **Cyber Consequences**: Cyber attacks have the potential to cause significant consequences for organizations.
2. **Threat Analysis**: Threat analysis is a crucial component of risk management
3. **Threat Integration**: Integrating real-world threat activity into the risk assessment process can improve the accuracy and efficiency of risk management.
4. **Threat Intelligence**: Cyber threat intelligence can be used to enhance both threat modeling and risk management.

By combining the insights of Threat Intelligence and Threat Modeling, we aim to provide a more comprehensive and effective approach to cyber risk management.

White Paper Agenda

1. **The Utility of Threat Analysis in Cyber Risk Management**

   Cybernetics and cyberspace, Cyber Risk Management, Cyber Threat Intelligence and Cyber Threat Modeling

2. **Threat Modeling Methods**

   Threat Agent, Attack Implementation, System Design and Risk driven methods

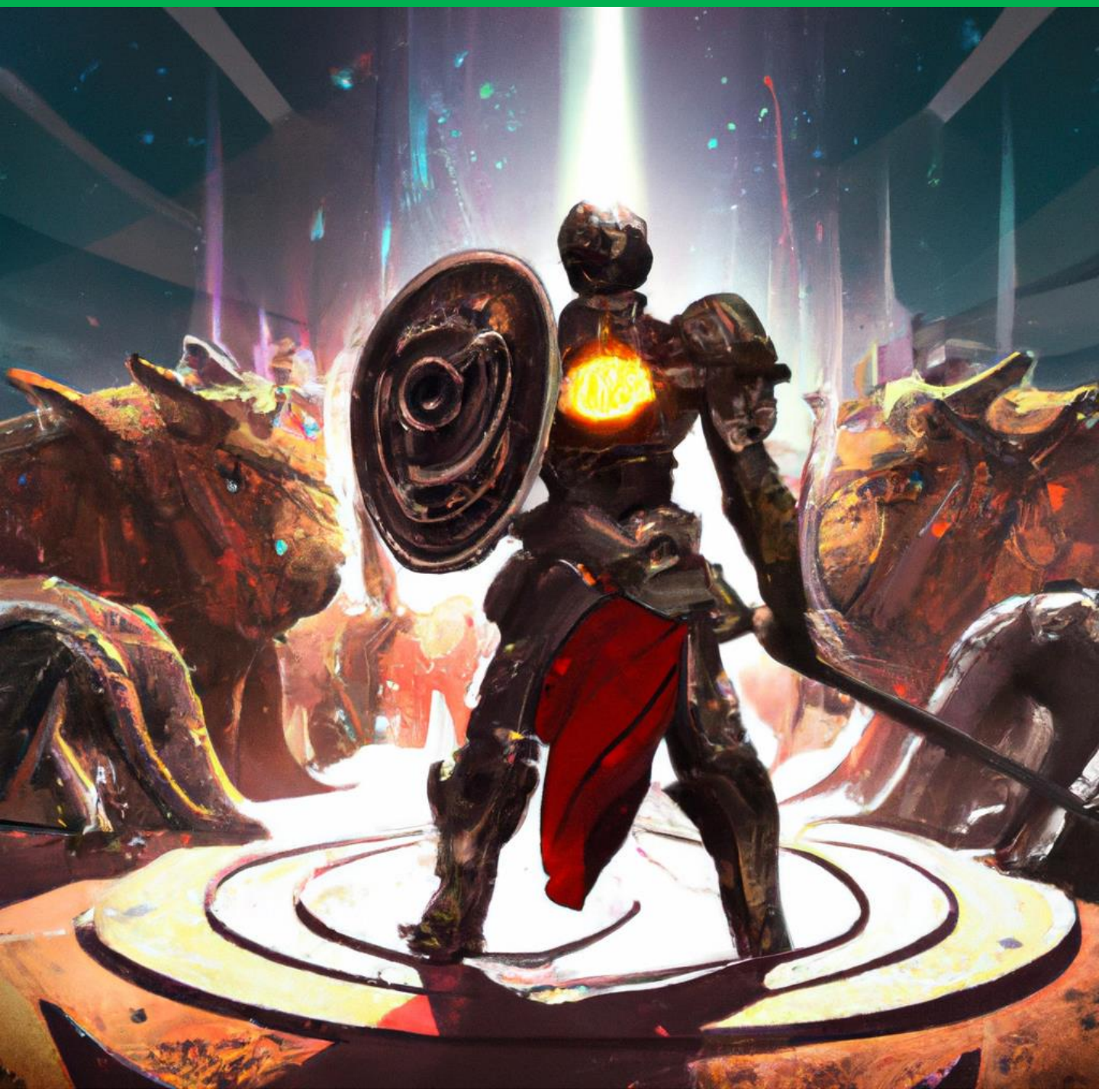
3. **Enhancing Threat Modeling with Cyber Threat Intelligence**

   Persona Non Grata, Attack Trees, CVSS, STRIDE

4. **Integrating Cyber Threat Intelligence into Cyber Risk Management**

   PASTA and EBIOS RM

1. The Utility of Threat Analysis in Cyber Risk Management



Introduction

Risk Management has taken the habits to always considered the threat factor as existing, competent and motivated. It focus on understanding the organization vulnerabilities and evaluating the impact of the realized risk. It is known as conditional risk.

Since the 1980's, researchers for the defense industry developed the threat analysis aspect inspired by intelligence and prospective disciplines. Those threat model gives a methodology and stereotypes to improve risk assessment. Thus, the likelihood risk factor is not anymore, a combination of adversary capabilities and intent, countermeasures and residual vulnerability; the likelihood risk factor became the probability of success of the threat.

But Threat Modeling have not been much used outside Software Security-By-Design Development Lifecycle, leaving the physical, human and business domain aside. In addition, Threat Modeling now relies on stereotypical events and adversaries that may not match the ever-evolving threat landscape. Even more when an organization must protect against Advanced Persistent Threat (APT) and state-sponsored group that do have the capability to adapt their operation regarding any organization defense posture.

This article argue that Cyber Threat Intelligence, the discipline of documenting and normalizing adversaries and threat events, is of great added value for cyber threat modeling and cyber risk management.

Content

1.1 Cybernetics and Cyberspace

Cybernetics is a meta-discipline that evade easy definition. MIT mathematician Norbert Wiener is generally credited for giving birth to this inter-disciplinary field of study in 1948 with his book "*Cybernetics, or Control and Communication in the Animal and the Machine*" **[2]**. We will understand here cybernetics as the scientific study of communications systems and automatic control systems in both machines and living things.

The prefix "*cyber*" is popularly used to describes IT related matter. It is in reality the short form of cyberspace, a wider concept. For example, "*Cyber Risks*" means "*the risks that occur in cyberspace*". Cyberspace is much more that "the space of computers and its related technologies".

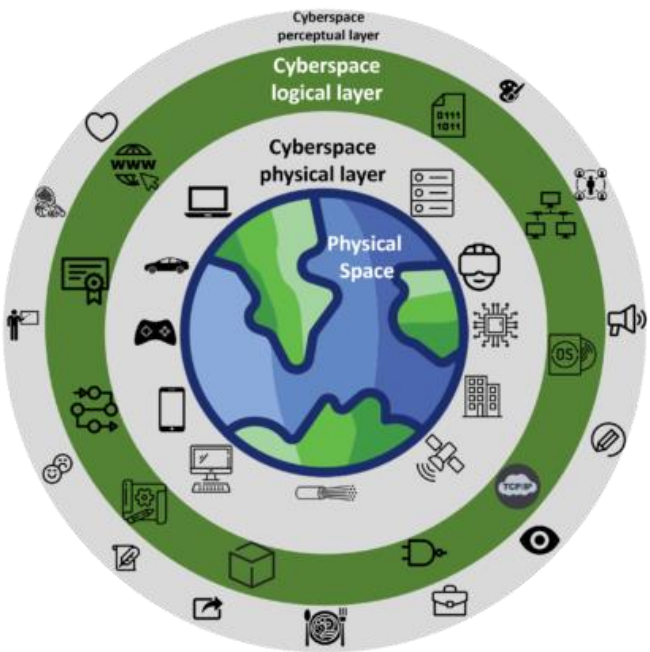
Cyberspace was first coined by the Danish artist duo Susanne Ussing and Carsten Hoff from 1968 to 1970 to express a "*sensory space*", where a physical room can sense and adapt to human being **[3]**. Then, the father of the Cyberpunk Sci-Fi sub-genre, William Gibson, used it in the 1980s as "*a graphic representation of data abstracted from banks of every computer in human system*". Two novels describes Gibson's view: *Neuromancer* (1984) and *Burning Chrome* (1988).

"Cyberspace.
A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts...
A graphic representation of data abstracted from banks of every computer in the human system.
Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..."
Neuromancer, William Gibson, 1984

In the globally admitted meta-definition, cyberspace is a *paraspace* (a "fake" space existing parallel to normal or ordinary space), realized and governed by scientific and philosophical laws, composed of three layers **[3][4][5]**:

- **Physical**: a cyber-enabled physical space existing in the physical space ("*the real world*"). It includes geography, materials, buildings, and any physical object of the real world that exist for or by the cyberspace. This layer exists by ontology and aesthetic.
- **Logical**: a cyber-enabled conceptual social space created by human to interact with computer technology, or to interact with other human thanks to computer technology. It includes communication protocols, operating systems, software and hardware design patterns, software languages. This layer involves the underlying codification of interaction between human and machine through human physical and conceptual meetings points based on data: *dataspaces* or *cyberplaces*.
- **Perceptual**: a cyber-enabled relational thinking space created by human to interact with human cognition or artificial cognition. It includes instinct, attention, awareness, imagination or emotion. This layers involves the existence of human as a projected cognition into a cyberplace (an avatar). A human is defined (*monitored* or *quantified*) by its interaction and relation with the logical layer and with other human or artificial avatars within the cyberplace.

Cyberspace co-exist within the real world. Cyberspace is not *naturally* produces but is the pure product of human cognition and human craft. Human cognition, perception and social interaction (the perceptual space) are the gateway between the physical space (where machines lies) and the logical space (where software and protocols lie).



Our subject of protecting technological systems against technological assault is first a human factor issue, a matter of a human attacking another human. Technology is just a way to achieve it.

1.2 Cyber Risk Management

Cyber risk is a risk that is caused by a cyber threat **[7]**. A computer damaged because of a fire is not a cyber risk, because fire is not a cyber threat. Cyber threat can be malicious or non malicious, or both. A malicious cyber-threat means that the threat has the intention to cause harm, and non-malicious threat otherwise. We will here focus on malicious threat.

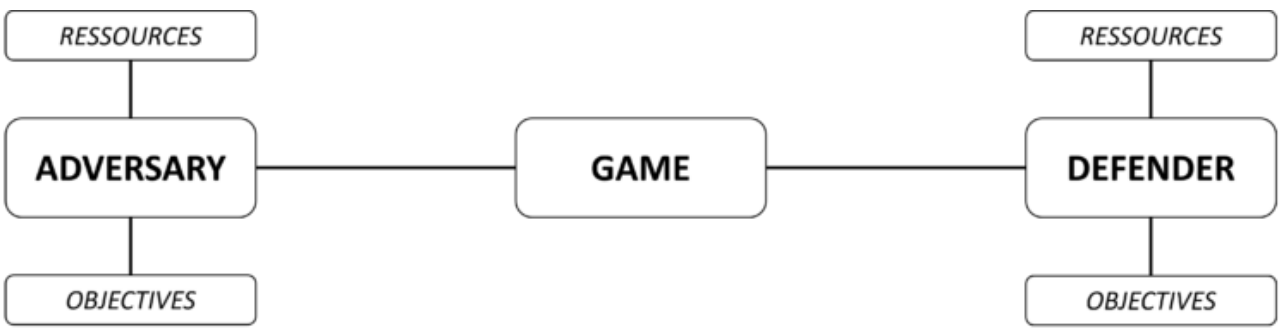
When it comes to Information and Communication Technologies, a risk is generally estimated with the following formula:

Risk = Threat x Vulnerability x Consequence

This approach of risks is based on the Risk Analysis and Management for Critical Asset Protection (RAMCAP) with the following understanding **[7]**:

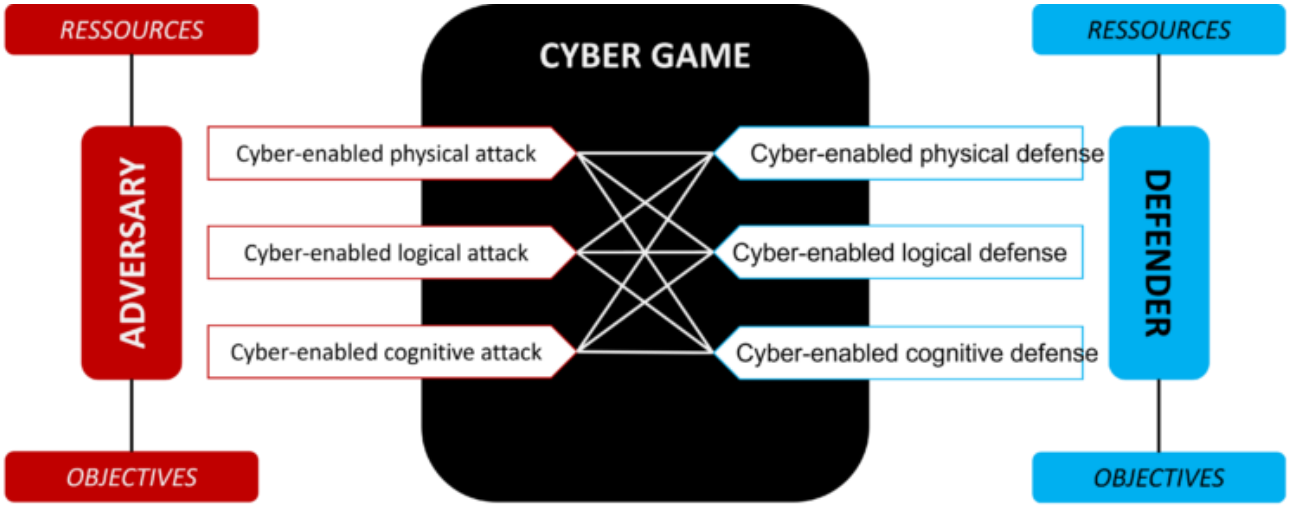
- **Risk**: the potential loss or harm due to the likelihood of an unwanted event caused by a threat.
- **Consequence**: The outcome of an event including short to long term, direct and indirect effects.
- **Vulnerability**: Any weakness in an organization's asset, infrastructure or operation that can be exploited by an adversary.
- **Threat**: Any event caused by an adversary's intention and capability to undertake actions detrimental to an asset or a population.

For a defending organization, the success of the adversary is detrimental to its own good. The defender have the motivation to defend itself and to built a countermeasure capability. It implies the motivation to invest time and resources to defeat the adversary at least up to the level of a realized cyber-risk will have meaningless consequences.



For the adversary, the success of the defender force it either to change its target or to upgrade its capability. In both case it implies the motivation to invest time and resources to defeat the defender.

The adversary and the defender are both involved in a project. A project implies a likelihood to not achieve 100% of the objectives. Both parties have then a risk management and deploys a strategy to overcome the other. This allows to represent the relationship between the attacker and the defender as a game taking place in cyberspace.



To reduce their own risk, each player can reduce their vulnerability, mitigate the consequences of an undesirable event or increase the risk of the other player, in all three layers of cyberspace.

"Cybersecurity increases the adversary's technical risks. The role of cyberdefense is to increase the adversary's operational risks. The whole game of political attribution is to increase the adversary's strategical risk."
Ronan Mouchoux, Cofounder of XRATOR

1.3 Cyber Threat Intelligence

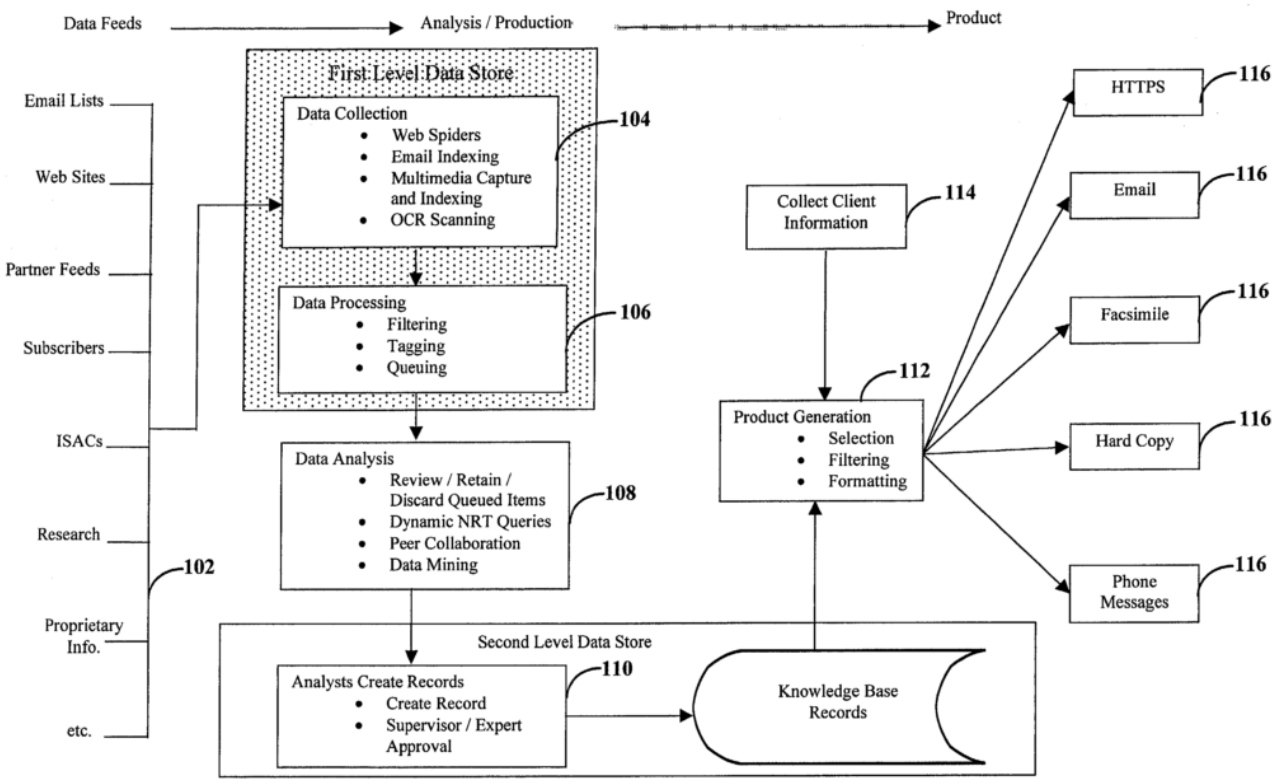
The origin of **Threat Intelligence** seems to comes from 1970s-1980s aircraft electronic countermeasures efforts **[8]**. The idea is that adversarial aircrafts do have electromagnetic signature that can be detected, analyzed, categorized by a Radar Warning Receiver (RWR). Used during combat aircraft, it allows to detect and identify hostile aircraft giving the flying crew the ability to manually or automatically avoid, evade or engage the detected threat.

During the same period, **Dynamic Threat Analysis** is conceptualized as a component of the LAVA (Los Alamos Vulnerability / Risk Assessment System) IT risk management expert system **[9]**. When performing a risk assessment, the intent to attack tend to be assumed and adversary capabilities to match the difficulty posed by the defender (meaning Threat = 1).

It is what RAMCAP calls *conditional risk*, where the measure of the risk depends on consequences and vulnerability. The adversary capabilities and intent, countermeasures and residual vulnerability are combined into a *likelihood* factor of adversary success.

Thanks to Dynamic Threat Analysis, the LAVA system has information about the threat pedigree (static component), and changing factors such as its goals, capabilities and opportunities (dynamic component). Just like the defender, the adversary is able to adapt, learn, equip or have a variable attractiveness toward particular assets or goals.

The concept of Threat Intelligence as we know it today is then applied to cyberspace environment in 2000 as a system and a method for the collection, analysis, and distribution of cyber-threat alerts **[10]**. The idea is to ***extract and analyze features of attack methods*** (Indicators of Compromise (IOC), Modus Operandi (TTP), Threat Actor) to take the appropriate corresponding proactive and reactive defensive decisions.



Functional diagram of a Cyber Threat Intelligence System, US20020038430A1

A common issue raised in the Cyber Threat Intelligence community is that the various standard for qualifying threat related indicators and behavior that is hindering seamless understanding between producers and consumers **[11]**. Efforts of structured expression, such as **STIX** and **MITRE ATT&CK**, do have their limitation in practice **[12]**.

1.4 Cyber Threat Modeling

Threat Modeling is born from the US Departement of Defense in the 1970's as part of Indications and Warning Analysis (I&W). I&W is a discipline used in the military and intelligence community to produce indicators mapped to prospective risks scenarios **[13]**.

Tracking the emergence of those indicators and mapping them to the related scenario help to determine what scenario may be ongoing, at what stage of the scenario we are and when to alert decision-makers. To create a computerized Indications and Warning Analysis Management System (IWAMS), researchers for the Defense Advanced Research Project Agency (DARPA) modeled the work performed by human analyst in three major steps : monitoring, threat recognition and projection.

Threat modeling is a preliminary phase of the threat recognition step. The idea is to define a Threat Model as a structured set of indicators. If monitored indicators to match this **threat identikit** up to a predefined trigger, then the observed situation match the appropriate threat.

Threat Modeling was translated to computer related technologies in the late 1980's. The challenge was to identify potential and actual threat, to integrate this analysis in a structured manner in the risk assessment process to achieve a sound comprehensive computer security posture **[14]**. Developing an effective computer security effort involves four critical steps:

1. Identify the **asset** to be protected (hardware, software, data, communication, people);
2. Determine the **threat** relevant to the identified assets;
3. Select potential **countermeasures**;
4. Perform a risk analysis to evaluate the **likelihood** of the success of the threat, with and without countermeasures.

The second step requires to have one or several methodologies to develop flexible threat model for both technical and managerial decision maker. Those flexible model can also be used to create, maintain and provide a set of stereotypical adversaries or events to perform risk analysis.

A threat is then defined as an agent (natural elements such as flood and human element such as a terrorist), an intention to act (no deliberate action or deliberate action), an implementation method (an event or action: explosion, spoofing) and a categorical impact (example: high impact on integrity).

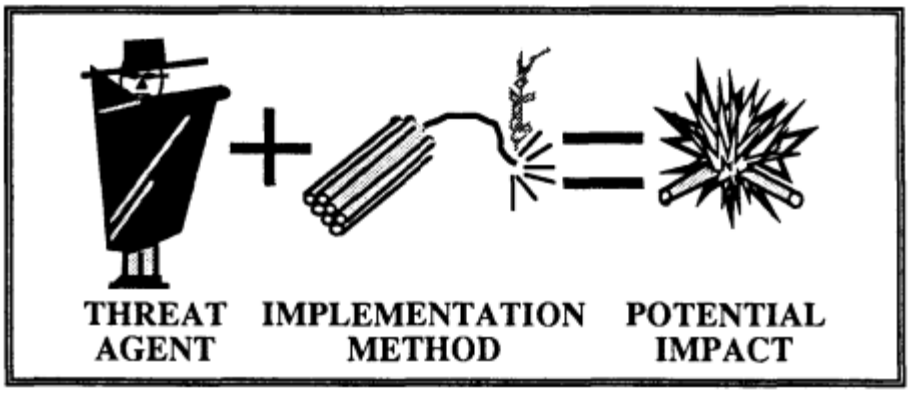


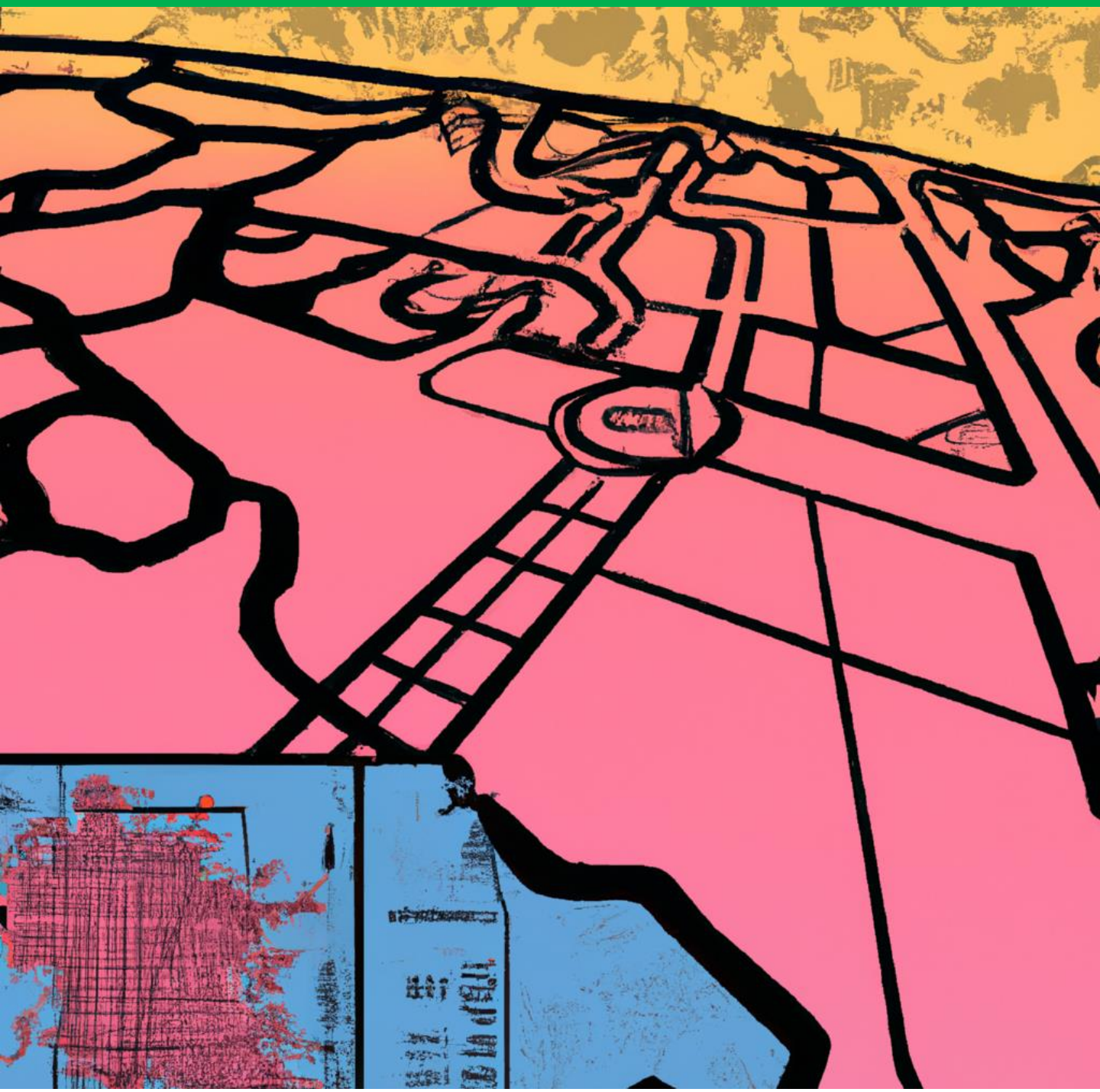
Figure 2
THREAT MODEL ELEMENTS

A major difference between natural threat agent and human threat agent is that the first one are not acting in the cyber paraspace, thus can't be defined as cyber threat. Then, the major difference between a non deliberated threat and a deliberated threat is that the first one can be compute based on frequency, when the second can't **[15]**.

Threat modeling expanded in a private sector during the 1990's, with especially Schneier's **Attack Trees** **[16]** and Kohnfelder & Garg's **STRIDE** **[17]**. Both provide typical events or adversaries, but both are more leaning toward software related threat rather than the full range of cyber assets. More recent research argues that cyber attacks may find their driver in the social, political, economic and cultural (SPEC) dimensions of human conflicts in the physical world **[18]**.

Finally, Threat Modeling and its broad usage suffer from key limitations. It is a very diverse topic that cover cyber attack to terrorist attacks, works either with flexible abstract model or precise taxonomies. Most of the work remains manual, with varying validation methods. Recent academic research calls for more automation and to use more empirical data and less abstraction **[19][20]**.

2. Threat Modeling Methods



Introduction

By essence, Cyber Threat Intelligence collects, documents and normalize in vivo cyber adversaries' data. It is a pool of empirical information that are waiting to be used in risk assessment of cyber-attack simulation. Instead of using Delphi-alike methods, gathering expert opinion, to fill a threat model methodology, we will explore here the compatibility and relevance of Threat Intelligence normalization with existing Threat Modeling methods.

We select nine threat modeling methods that seems to be the most popular and the most use by practitioners **[21]**. From this references, we decided to exclude:

- The Visual, Agile, and Simple Threat (VAST) methods because of the lack of documentation and publication.
- The hTMM / qTMM because of the lack of independent review and documentation.
- The Trike framework because of the lack of documentation and maintenance.

We decided to include the EBIOS RM methodology because of its strong emphasize of “Risk Origin” (a.k.a. Threat Agent).

We divided the nine modeling techniques into four categories:

- **Threat Agent driven method**: Methodology that is driven by the human adversaries and their goals;
- **Attack implementation driven method**: Methodology that is driven by the type of attack you apply to a system;
- **System Design driven methods**: Methodology that is based on a system modeling on which we apply security stress or expectation;
- **Risk driven methods**: Methodology that integrate the threat agent, the security stress, the impact on the system and mitigation measures.

This section objectives is to describe briefly each methods and component. This analysis will help us in the next section to evaluate the compatibility with Cyber Threat Intelligence.

Security Cards – Personae Non Gratae – Attack Trees – CVSS – STRIDE – LINDDUN – PASTA – OCTAVE – EBIOS RM

2.1 Threat Agent driven methods

Threat Agent driven methods are centered around the analysis of the human adversary, their ability and motives.

1. Security Cards

The Security Cards is a brainstorming techniques developed in 2013 by Tamara Denning, Batya Friedman and Tadayoshi Kohno (University of Washington) **[22]**. The toolkit is composed of 42 cards break down in four categories:

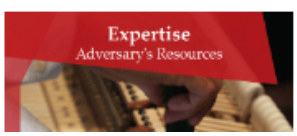
- **Human Impact**: how human can be affected by their lives ?
- **Adversary's motivation**: why does the adversary engage into attacking the system ?
- **Adversary's resources**: what resources does the adversary have ?
- **Adversary methods**: how the adversary can attack the system ?

HUMAN IMPACT
9 CARDS
Human Impact points to the myriad of ways in which human beings can be affected in their lives, from intimate relationships and emotional experience to privacy violations with personal data to widespread societal impacts at the level of the economy, government, and social structure.

ADVERSARY'S MOTIVATIONS
13 CARDS
Adversary's Motivations emphasizes the variety of reasons an individual or group might wish to attack a system, from ideological reasons focused on religion, politics, or diplomacy to more self-oriented motivations such as convenience or self promotion.

ADVERSARY'S RESOURCES
11 CARDS
Adversary's Resources presents an array of different assets that might be at an adversary's disposal, from hardware and software tools to the ability to influence the actions of groups of people, or access to technical or social expertise.

ADVERSARY'S METHODS
9 CARDS
Adversary's Methods explores high-level ways that an adversary might approach attacking a system, from the familiar technological attack to manipulating or coercing people, covering up evidence, or leveraging logistical and bureaucratic processes.

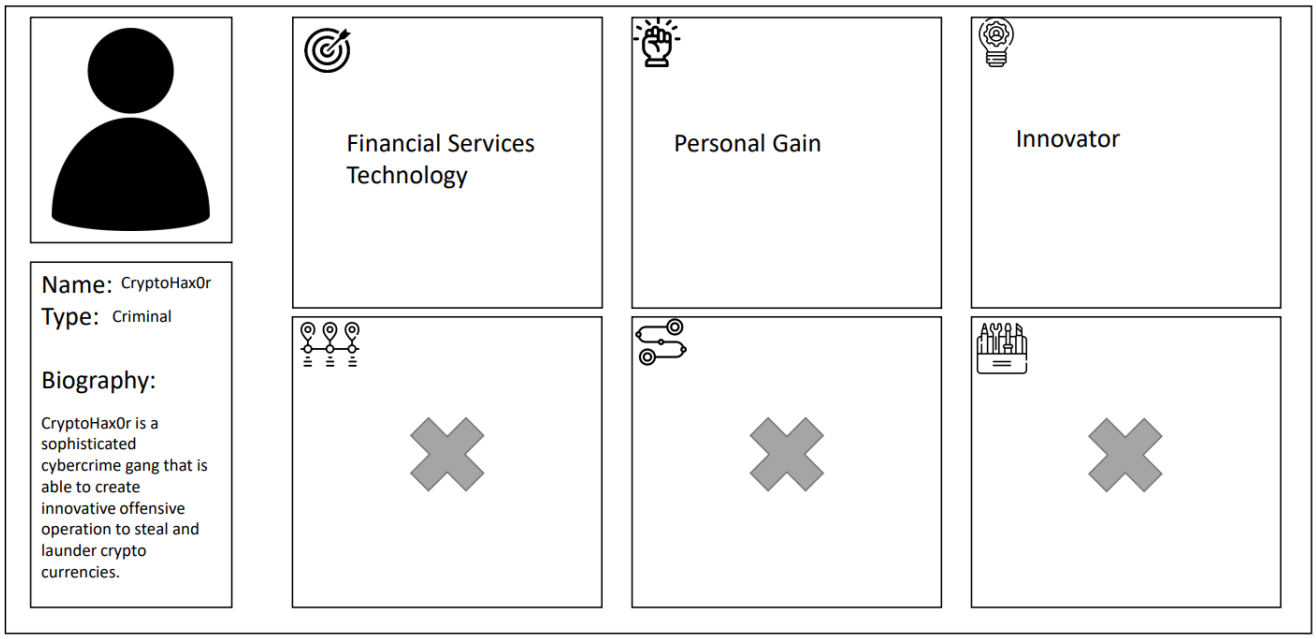


This methods is comprehensive enough to covers nearly all the possibilities, but also does produce a lot of false positive. The method produce little consistency when repeated over time or across panelist. Security Cards can be a good methods to cover nonobvious cases or to provide support to gamified awareness session.

2. Personae non Gratae

The Personae non Gratae, or Persona Non Grata, method focus on the motivation and skills of human adversaries **[23]**. The mindset is to apply the right amount of security to a system regarding a relevant threat agent and impact of the system disruption to the organization.

Protecting Play-2-Earn Development Studio from Bridge Hack



The process is to set the context of the system to protect (a company, a network, an application) and to create an Identikit of the threat agent. To facilitate the role-play dynamics, the identikit may include a biography, a timeline of past malicious action, a stereotypical modus operandi and available resources. It should include the motivation of the action and a level of sophistication.

The methods has very consistent results when repeated on the same system across panel or over time. The problem is that it tends to focus on the subset of the most obvious adversaries. It is a very good method to spot "*Grey Rhino*" (very plausible threat), not so much to uncover "*Black Swan*" (High Impact – Low Probability threat).

2.2 Attack Implementation driven methods

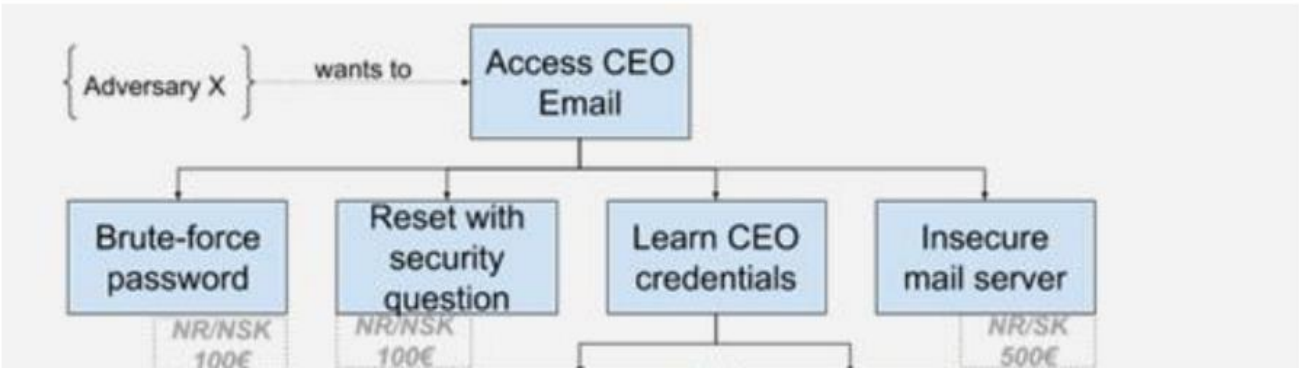
Attack Implementation driven methods are guided by the analysis of methods used by the adversary's operator to produce malicious consequences on a component of the system, producing a higher-level impact on the component's system.

1. Attack Trees

Design as a tree, it is very compatible with data mining, statistics and machine learning. The root of the tree is the operational goal of the attack. It is the "*why*" the threat operator conduct the operation. The leaves of the tree are the atomic way to achieve the goal. It is "*how*" the operator will conduct its ultimate malicious task **[24]**.

The process is to set a goal, and to dig the "how" until reaching a technique that is precise enough to be implemented. Once the tree is created, the analyst will evaluate each leaves to determine:

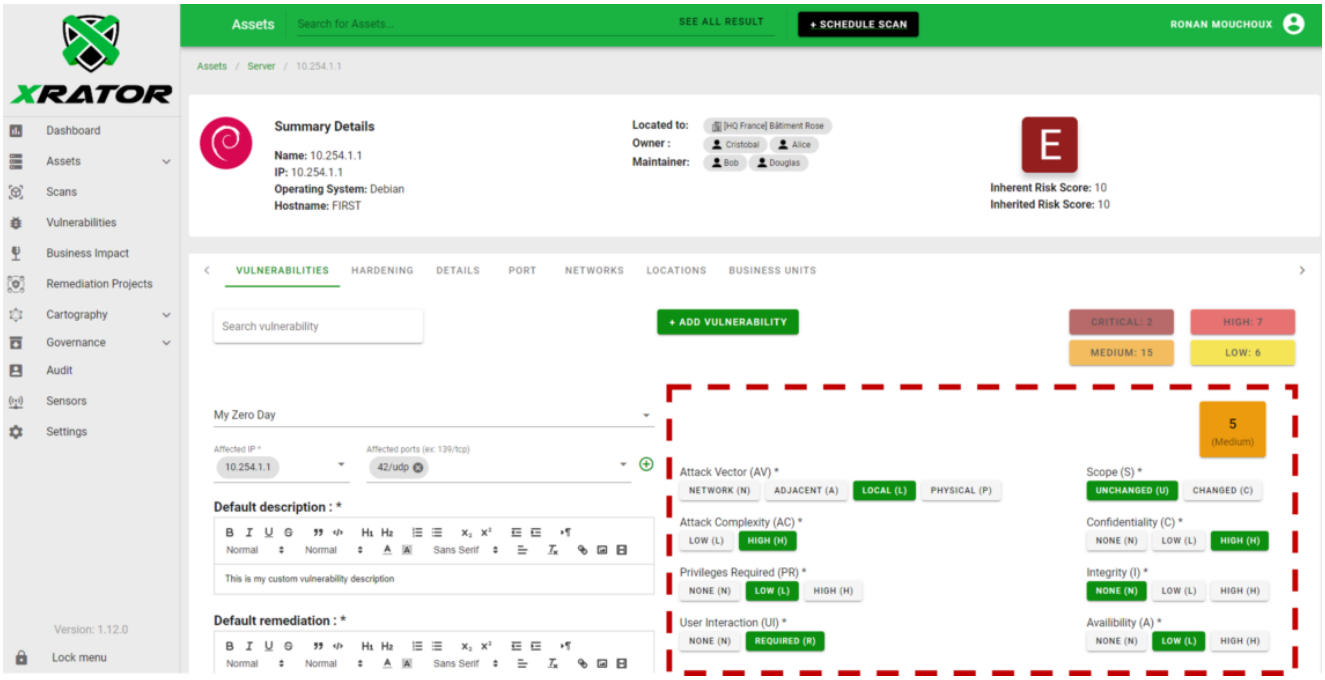
- Does the leave is possible or not ?
- Does the leave require special equipment or special skills ?
- Does the leave is risky or not risky for the attacker ?
- How much does the implementation of the leave cost ?



The attack trees produce very consistent results when repeated on the same system across panel or over time. But attack tree are also quite flexible, with associated downsides. It is not always easy to know if a leave is really one or if you drilled to much, or not enough. The assessment of the riskiness, the special resources or possibility is relative. Also, when creating the branches and leaves, it may sometimes confusing and leads practitioner to start discussing "how" to be in position to perform such ultimate attack, transitioning to intrusion path analysis. Finally, a quite good knowledge about the system seems mandatory to perform a reliable analysis.

2. CVSS

The Common Vulnerability Scoring System (CVSS) is probably the most well-known and used software-based threat modeling method. Developed by the NIST and maintained by the FIRST, it is the de facto standard to communicate the characteristics and the severity of software vulnerabilities **[25]**.



The CVSS method produce very consistent results when repeated on the same system across panel or over time, for a given vulnerability. It has a scoring system, a string-based hash that condense parameters and an open scoring system.

Yet it requires good vulnerability assessment knowledge and thus is not as inclusive to non-technical audience as other methods. It also focus more on the weakness of the system than the threat agent or its ability.

2.3 System Design driven methods

System Design driven methods starts by modeling the in-place or to-be-developed system and then look for attack opportunities.

1. STRIDE

STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This threat modeling framework was developed by Loren Kohnfelder and Praerit Garg from Microsoft in 1999 to help software architect and developers to anticipate the types of attacks their system could suffer from **[26]**.

Type	Description	Security Control
Spoofing	Threat action aimed at accessing and use of another user's credentials, such as username and password.	*Authentication*
Tampering	Threat action intending to maliciously change or modify persistent data, such as records in a database, and the alteration of data in transit between two computers over an open network, such as the Internet.	*Integrity*
Repudiation	Threat action aimed at performing prohibited operations in a system that lacks the ability to trace the operations.	*Non-Repudiation*
Information disclosure	Threat action intending to read a file that one was not granted access to, or to read data in transit.	*Confidentiality*
Denial of service	Threat action attempting to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	*Availability*
Elevation of privilege	Threat action intending to gain privileged access to resources in order to gain unauthorized access to information or to compromise a system.	*Authorization*

STRIDE is probably the most widespread Threat modeling methods of all with accessible tooling such as OWASP Threat Dragon **[27]** or Microsoft Threat Modeling Tool **[28]**. STRIDE heavily relies on building a Data Flow Diagram. It is the first step of the method to build one.

STRIDE is more about knowing its software structure than reflecting about threat. The Data Flow Diagram must be perfect for STRIDE to be relevant. The second downsides is that you can hardly include by design all the security function and equipment that are in place and the security decision for countermeasures.

Each element of the Data Flow Diagram must be auscultated and passed through the STRIDE checklist. It is then very time consuming because the attacks opportunities are exponentially growing with the size of the system.

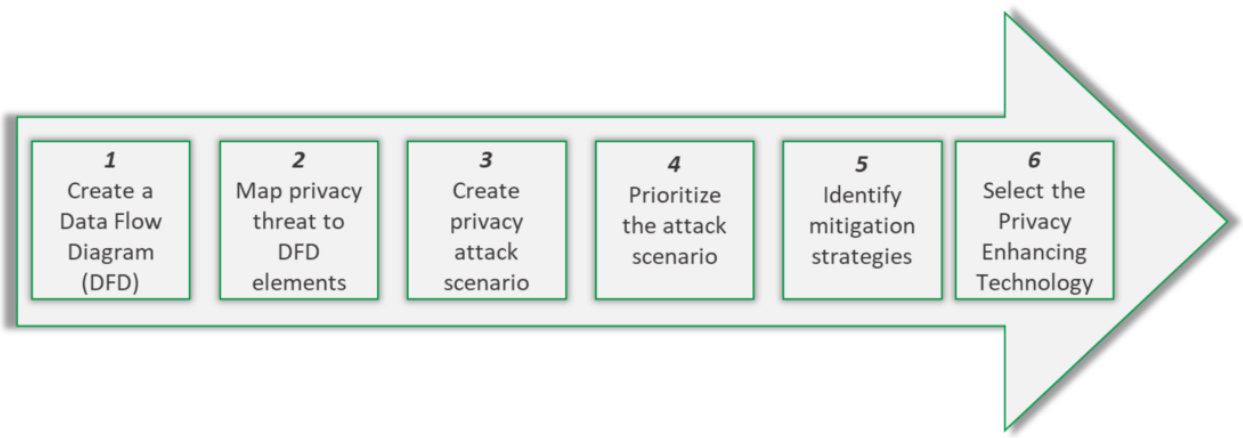
The method is moderately consistent over time and panel, has a moderately low rate of false positives and a moderately high rate of false negatives **[29]**.

2. LINDDUN

LINDDUN stands for (Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance). It is a modeling method focused on privacy and data security.

The framework has been created by noting that STRIDE was not properly covering data privacy threats in software-based system. It provides a systematic methodology to model attacks on data privacy, a catalogue of privacy threat pattern and a way to integrate Privacy Enhancing Technologies (PETs) **[30]**.

The LINDDUN Privacy-centric Threat Modeling Methodology (WUYTS & al, 2014)



Like STRIDE, LINDDUN also rely on Data Flow Diagram. The methodology is time consuming and intensive. The benefits for Data Privacy Officer or Data Security specialist is the extensive privacy knowledge base and documentation.

2.4 Risk-driven methods

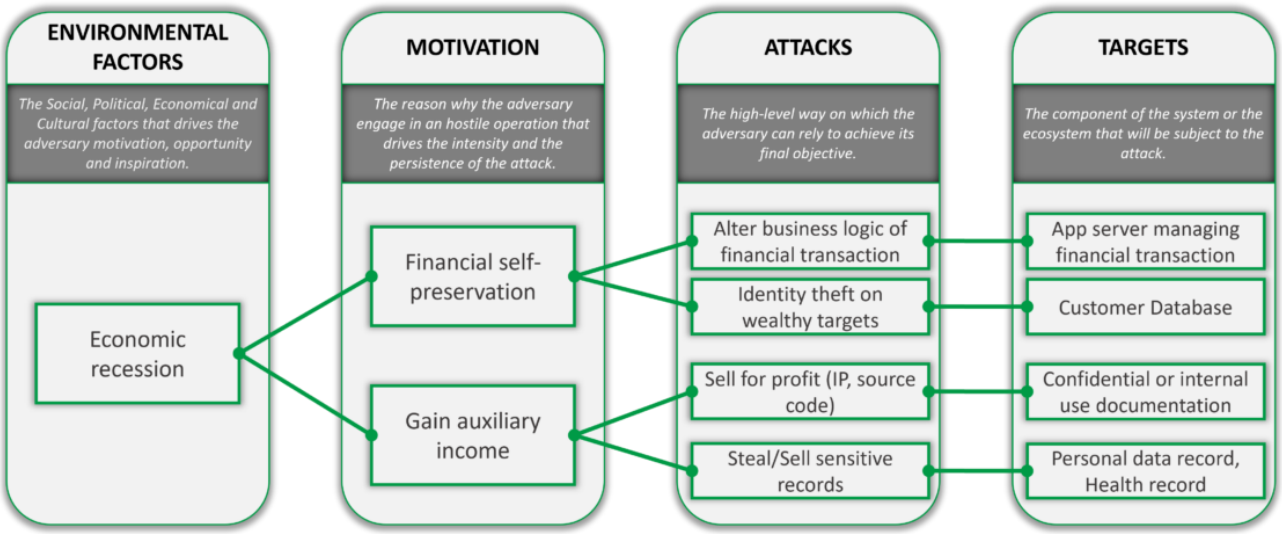
Risk driven threat modeling frameworks are a full set of methods that are fully compatible or following the big picture of ISO/IEC 27005 : identify and assess the risks, mitigation strategies, monitor risks and mitigation, stakeholder information.

1. PASTA

PASTA is the acronym of Process for Attack Simulation and Threat Analysis. Created by Tony Uceda Vélez and Marco Morana in 2014, their contribution to Threat Modeling is a greater inclusion of the business context in which the system to protect evolves **[31]**.

The methodology is based on the thesis that social, cultural, economic and cultural (SPEC) factors serve as key drivers upon software adversaries act. They consider that the "Secure Software Development Life Cycle" (S-SDLC) can't on its own counterattack vectors coming from human component, such as corruption or extreme expertise leading to zero-day attacks. Their ambition is to level up the game of Software Threat Modeling up to the level of Military Threat Modeling (cf *1.4 Cyber Threat Modeling*).

The PASTA SPEC-centric Threat Modeling Methodology (VÉLEZ & al, 2015)



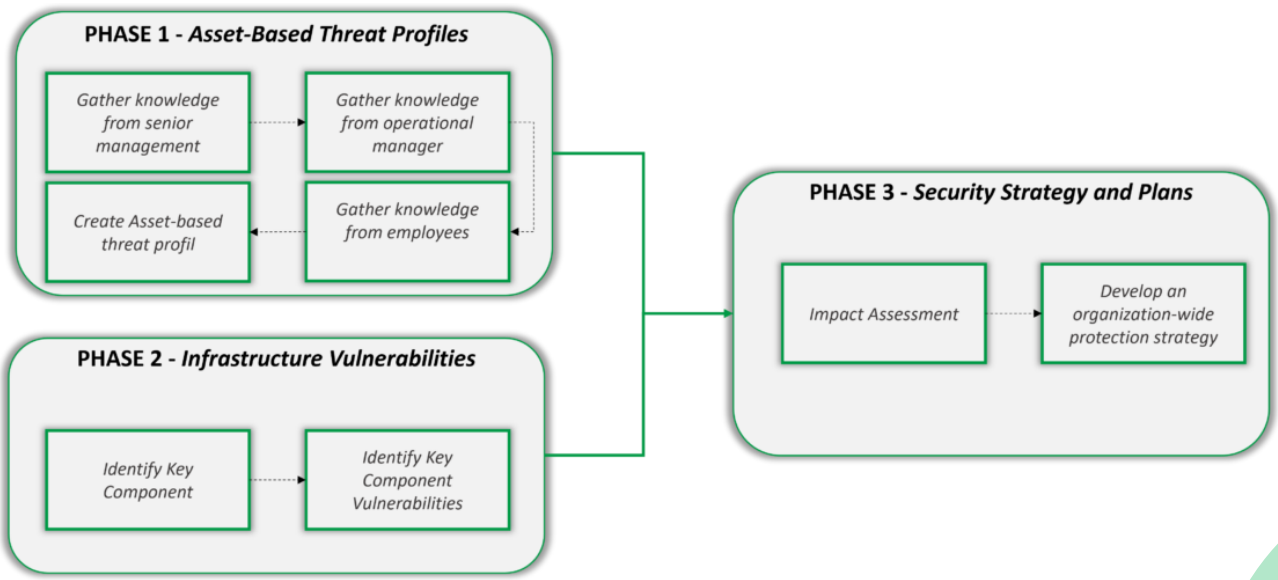
The PASTA methodology contains seven stages from Business Context to the Risk Identification & Countermeasures. It uses other Threat Modeling tools during the process:

1. **Define Objectives**: No outside threat modeling tool;
2. **Define Technical Scope**: High level Application Architecture Diagram;
3. **Application decomposition**: Data Flow Diagram;
4. **Threat Analysis**: Ingesting Cyber Threat Intelligence (no standard) ;
5. **Vulnerability & Weakness Analysis**: Attack Tree, CVSS (MITRE CVE), CWSS (MITRE CWE);
6. **Attack Modeling**: Attack Tree;
7. **Risk & Impact Analysis**: No outside threat modeling tool;

The input are from the strategic and operational level of an organization. The output are asset-centric and includes enumeration and scoring of attack implementation.
The process is highly time consuming and intensive. It combines all the benefits and downsides of the modeling methods they integrates. The benefits of PASTA is to include non-technical people in the definition phases, to be inclusive with strategic management and to integrate the human and social factor in the system security evaluation. The senior management is also aware of the business impact of security requirements or non-action **[32]**.

2. OCTAVE

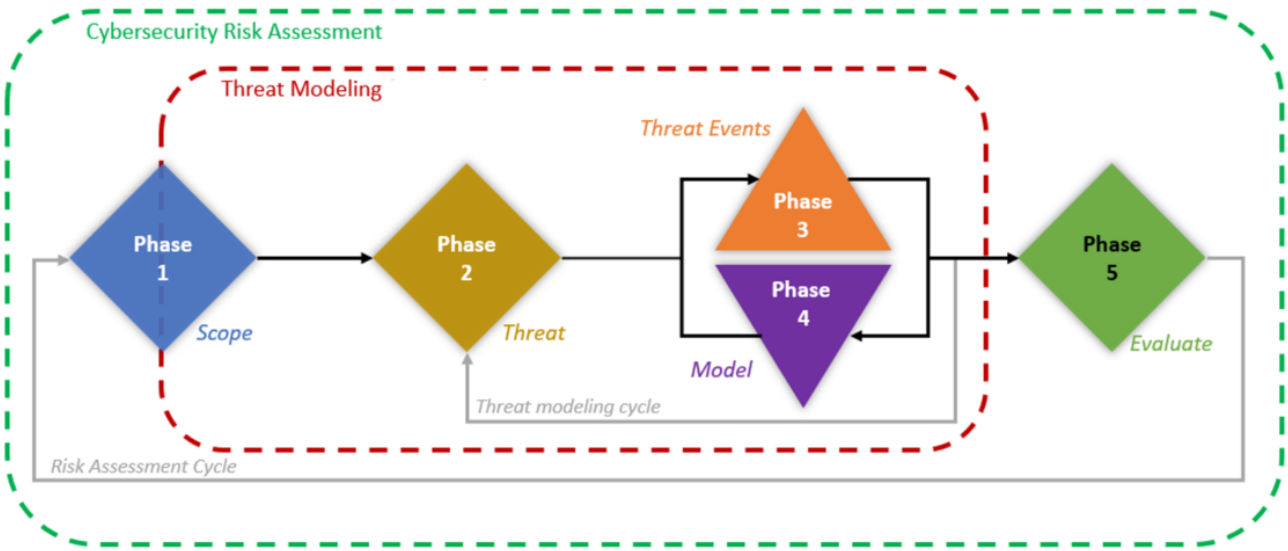
OCTAVE stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation **[33]**. It is a strategic assessment a planning method for cybersecurity. It was created in 2003 by the CERT-SEI of Carnegie Mellon University, and updated in 2006. Unlike other threat modeling approach, OCTAVE was designed to address organizational risk and strategic issues.



OCTAVE is split into three phases regrouping a total of eight processes. It encourages collaboration among stakeholders, is scalable and has consistent result when repeated on the same system across panel or over time. But it is very time consuming, and the documentation is large but vague.

3. EBIOS RM

France's National Cybersecurity Agency (ANSSI) has introduced EBIOS Risk Manager, a procedure for evaluating and handling cyber risks **[34]**. EBIOS RM is a Risk Assessment systematic methodology including threat agent identification, macro attack modeling and cyber kill chain attack modeling. It follows the ISO/EIC 27005 principles. We yet choose to include it in this Threat modeling review as it greatly emphasize threat-based assessment, like PASTA or OCTAVE.

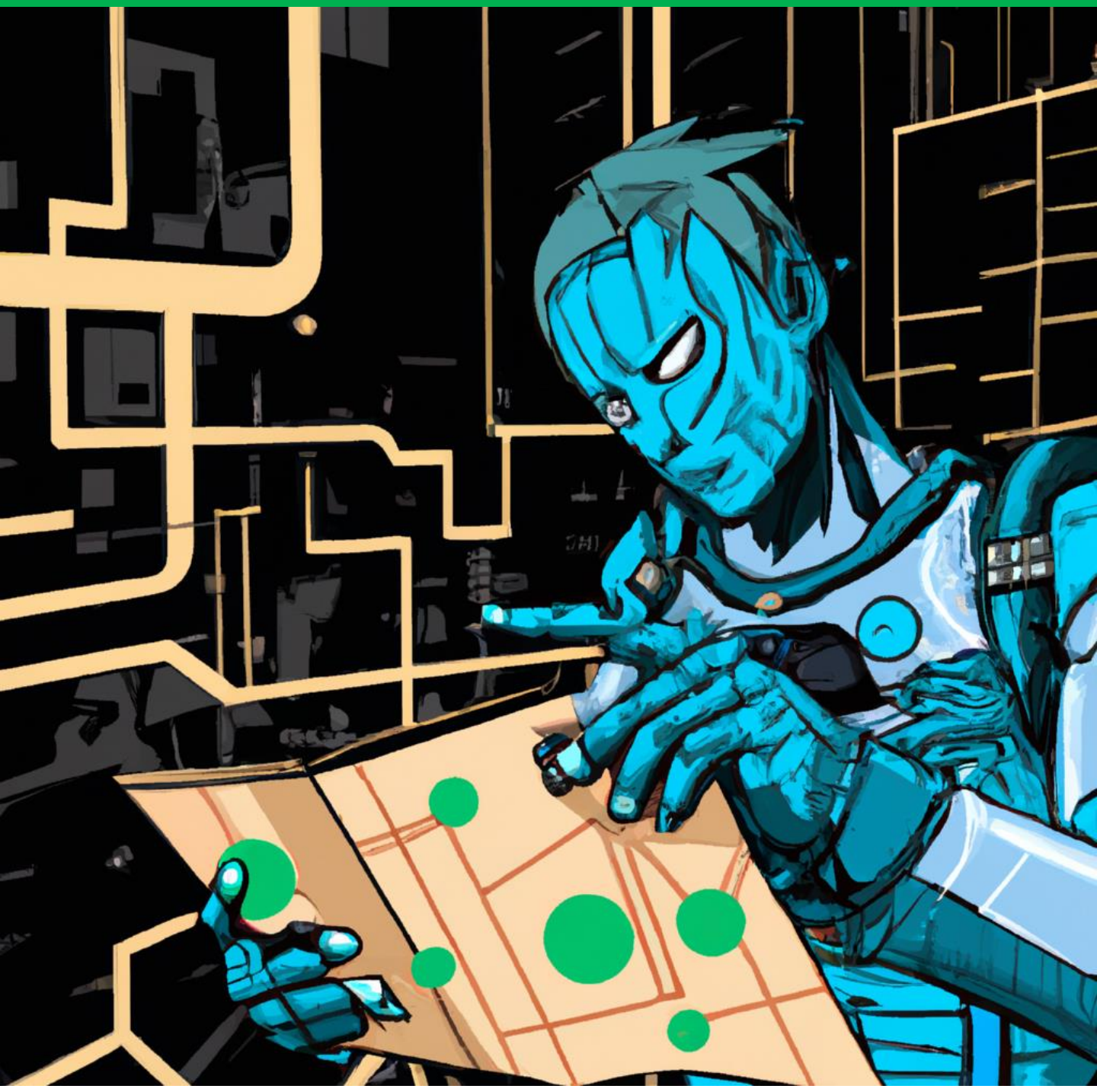


The EBIOS methodology contains 5 steps, starting from the organization's crown jewels and business context:

1. **Scope and security baseline**: Define the perimeter, identify participant in the analysis and the timeframe of the assessment.
2. **Risk origins**: Identify and characterize the risk origin (the Threat Agent)
3. **Strategic scenarios**: Mapping of the business dependencies and threat vectors.
4. **Operational scenarios**: Build technical scenario based on a KNOWING-ENTERING-FINDING-EXPLOITING simplified cyber kill chain.
5. **Risk treatment**: Summarize the risk and define the risk mitigation strategy.

The process is intensive and time consuming. It also lack the leverage of existing threat modeling tools and sometimes reinvent the wheel. The benefits are similar to OCTAVE. Non-technical and strategic contributor are included. Also, EBIOS RM put a strong emphasize on the identification of the threat and its modus operandi.

3. Enhancing Threat Modeling with Cyber Threat Intelligence



Introduction

Threat modeling methods such as EBIOS RM or PASTA explicitly integrate Threat Intelligence in their process. In other method, such as Personae Non Gratae, the integration opportunity is more implicit but quite obvious.

In this section we offer a perspective where we tied classical cyber threat intelligence methods and frameworks with existing Threat Modeling methodologies. The objectives is to improve the normalization of intelligence outputs and to feed threat model with fresh, accurate and real-world threat analysis insight.

Based on XRATOR's real world experience conducting threat modeling workshop and threat intelligence analysis, we offer to the cybersecurity community the following tips and improvement to current methodologies.

Content

1. **Historical Context**: From military to Software Security.
2. **Persona non Grata**: Using STIX Open Vocab to facilitate communication and correlation.
3. **Attack Trees**: Leveraging MITRE CAPEC and MITRE ATT&CK to structure the analysis and the remediation.
4. **CVSS**: Using STIX Open Vocab to prioritize vulnerability mitigation.
5. **STRIDE**: Leveraging MITRE CAPEC and MITRE ATT&CK to structure the analysis and the remediation.

"Threat analysis is the cornerstone of effective risk management.
Without it, organizations are blind to the dangers they face."

3.1 Historical context and military inspiration

The origins of threat modeling can be traced back to the Cold War and **the Indication & Warning (I&W) intelligence** activities, when the US military began to prioritize the protection of its critical assets and infrastructure from potential ballistic threats posed by foreign powers **[12][31]**.

In the early 1960s, the US military developed the LAVA system to identify and prioritize vulnerabilities in its systems and assets **[8]**. This process involved analyzing the potential impacts of various threats, such as sabotage or espionage, and determining the likelihood of those threats occurring.

To develop threat modeling necessary for the Threat recognition step of I&W (cf *1.4 Cyber Threat Modeling*), analysts and designers followed three preliminary steps:

1. **Define the scope of the threat modeling effort**: This involves defining the boundaries of the system or asset that is being analyzed and identifying the stakeholders who will be involved in the threat modeling process.
2. **Collect threat intelligence**: This involves gathering information about potential threats to the system or asset being analyzed. This may involve collecting data from a variety of sources, including human intelligence, signals intelligence, and open-source information.
3. **Analyze threat intelligence**: This involves analyzing the collected threat intelligence to identify potential threats and assess their likelihood and potential impact. This may involve analyzing historical data, assessing the capabilities of potential adversaries, and considering the potential consequences of a threat being realized.

Threat modeling and Threat Intelligence are both a cyclical process. Once you analyzed historical data thanks to threat intelligence, you create a first threat model. Once you have a first threat model, you can improve the structure of the information gathered, processed and analyzed while conducting threat intelligence.

Hands in hands, the combination of a knowledge structure provided by Threat Modeling and historical data on Threat Agents and Threat Events provided by Threat Intelligence creates **Threat Catalogues**. Those threat catalogues are leverage for any threat recognition and scenario projection tasks.

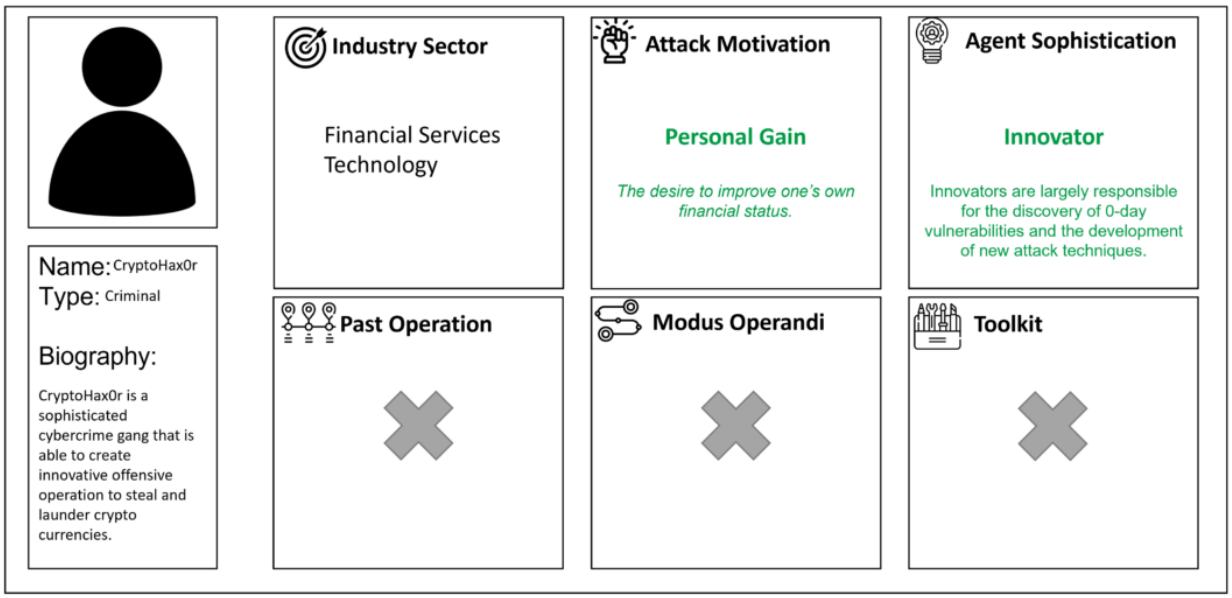
3.2 Personae non gratae and STIX Open Vocab

One advantage of Personae Non Gratae is to gather technical and nontechnical people to create an identikit of the adversary. A first limitation is that when defining the industrial sector target, the level of sophistication or the motivation, people may use different words to express the same meaning, or same words to express different meaning.

The first negative outcome is a low capability to leverage past workshops and to track "*Grey Rhino*" adversaries over time. The second negative outcome is a lower quality in a Persona non Grata workshop.

The solution is to use a well-established structured vocabulary, such as STIX Open Vocab. This naming convention enables a greater compatibility and understandability of analysis.

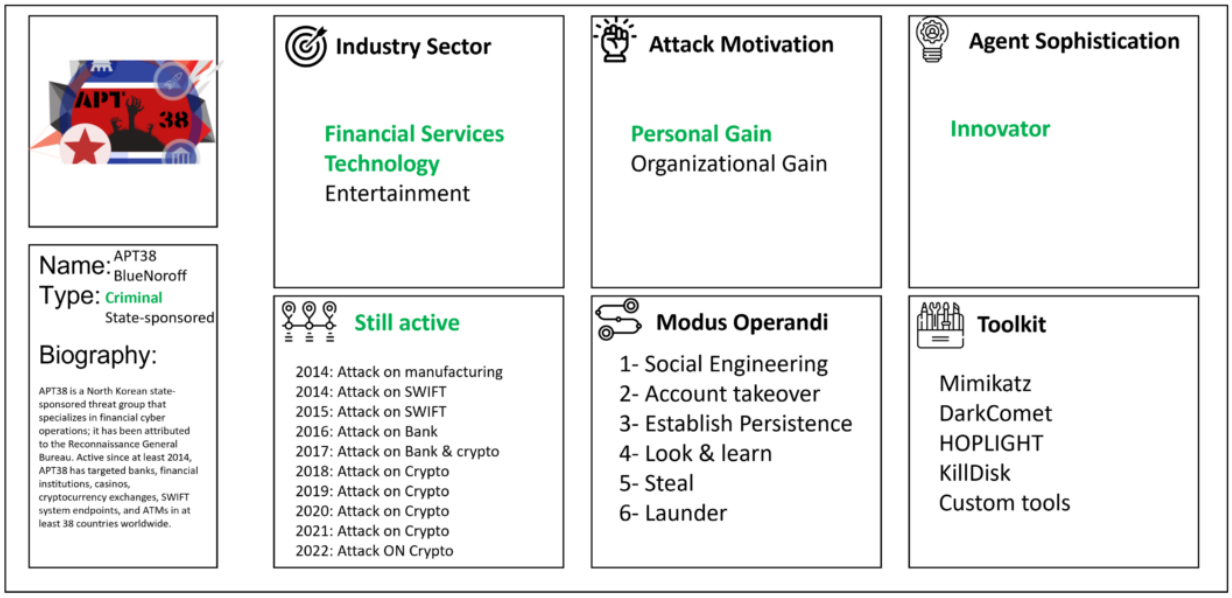
Using STIX Open Vocab with Persona Non Grata



The second limitation of the Persona Non Grata is that the workshop audience may have little to no sense of reality when it comes to defining a Persona malicious pedigree, how it operates and what kind of tool they may use to conduct their operation.

By using a structured vocabulary to store and exchange threat intelligence analysis, it is very easy to query the Threat Historical Database with the Persona Non Grata characteristics, and get the closest Cyber Adversary. Hence, the persona non grata pedigree, modus operandi and arsenal is matching a real adversary.

Feeding Persona Non Grata with Threat Intelligence



The benefits is to create projection based on real-world cyber operation. The drawback is that “Black Swan” events or adversaries are put aside, but this is an inherent limitation of the Personae Non Grate methodology.

3.3 Attack Trees and MITRE CAPEC/ATT&CK

The MITRE Common Attack Pattern Enumeration and Classification (CAPEC) and MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) are publicly available databases that can be used to inform the process of threat modeling. Both CAPEC and ATT&CK are maintained by MITRE, a non-profit organization that provides technical and research support to the US government.

During the attack tree threat modeling method, both CAPEC and ATT&CK can be used to identify and classify the various types of attacks that could potentially be used against a system or asset. Attack trees are graphical representations of the various steps that an attacker might take to compromise a system or asset, and they can be used to identify and prioritize the potential vulnerabilities and risks associated with a system.

To use CAPEC and ATT&CK during the attack tree threat modeling method, you can follow these steps:

1. **Identify the system or asset being analyzed**: This involves defining the boundaries of the system or asset that is being analyzed and identifying the stakeholders who will be involved in the threat modeling process.
2. **Identify potential attack vectors**: This involves identifying the various ways that an attacker could potentially compromise the system or asset being analyzed. This may involve identifying external threats, such as cyber attacks or physical threats, as well as internal threats, such as employee mistakes or malicious insiders.
3. **Search the CAPEC and ATT&CK databases for relevant attack patterns**: This involves searching the CAPEC and ATT&CK databases for attack patterns that could potentially be used against the system or asset being analyzed. This may involve searching for attack patterns based on the types of attacks being considered, the target system or asset, or other relevant criteria.
4. **Use the attack patterns identified in the CAPEC and ATT&CK databases to create an attack tree**: This involves creating an attack tree that represents the various steps that an attacker might take to compromise the system or asset being analyzed. The attack tree should include the attack patterns identified in the CAPEC and ATT&CK databases, as well as any additional steps or considerations that are relevant to the specific system or asset being analyzed.

The benefits of including CAPEC and/or ATT&CK in an Attack Tree process are:

- **Comprehensive coverage**: They contain a large and comprehensive collection of attack patterns and tactics, techniques, and procedures (TTPs) that can be used to inform the threat modeling process. This can help to ensure that the attack tree being developed is comprehensive and covers a wide range of potential threats and vulnerabilities.
- **Industry standard**: CAPEC and ATT&CK are widely recognized as industry standards for threat modeling and are used by a wide range of organizations around the world. This can help to ensure that the attack tree being developed is based on best practices and accepted standards in the field.
- **Structured and standardized**: Both database use a structured and standardized format for representing attack patterns and TTPs, which can help to ensure that the attack tree being developed is understandable and easier to query afterwards.
- **Provide detection measures and remediation**: The MITRE ATT&CK database contains for most of the offensive techniques detection advises and mitigation course of action, that can help in the later stage of the attack tree. MITRE CAPEC do not contain countermeasures, but is linked to other frameworks such as MITRE CWE, OWASP Attacks or the WASC Threat Classification that do.

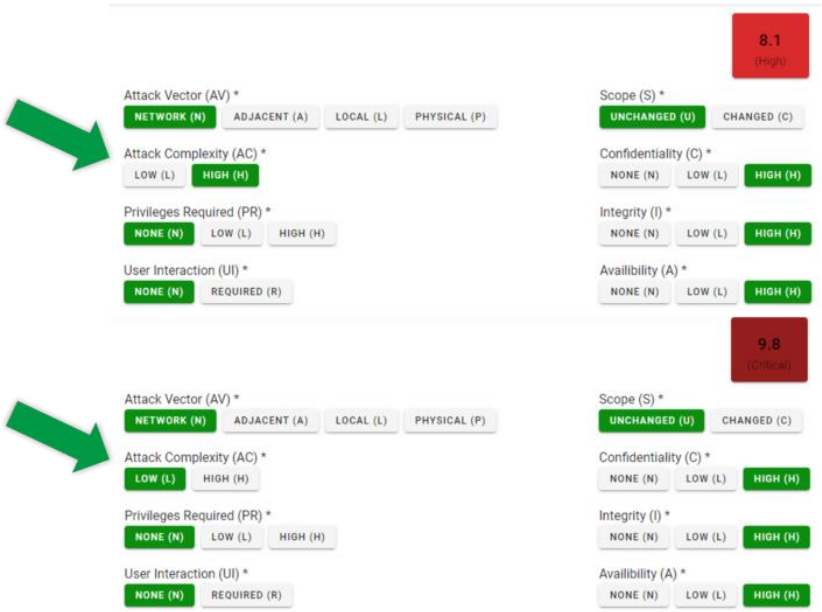
By using those structured database to define the Attack Tree, it is then easier to match the tree with a Threat Intelligence database and pinpoint the past attacks that may be relevant to conduct a test or to define a simulation scenario.

3.3 CVSS and STIX Open Vocab

One of the main limitation of CVSS when it comes to Threat Modeling is that it is too focus on the weakness of the system and left behind the threat agent or its ability.

The immediate problem appears when trying then to prioritize vulnerability remediation. Among the vector contributing to the score of a vulnerability, there is the “Attack Complexity (AC)” with two possible values: Low complexity or High complexity.

“Low” versus “High” Attack Complexity impact on CVSS



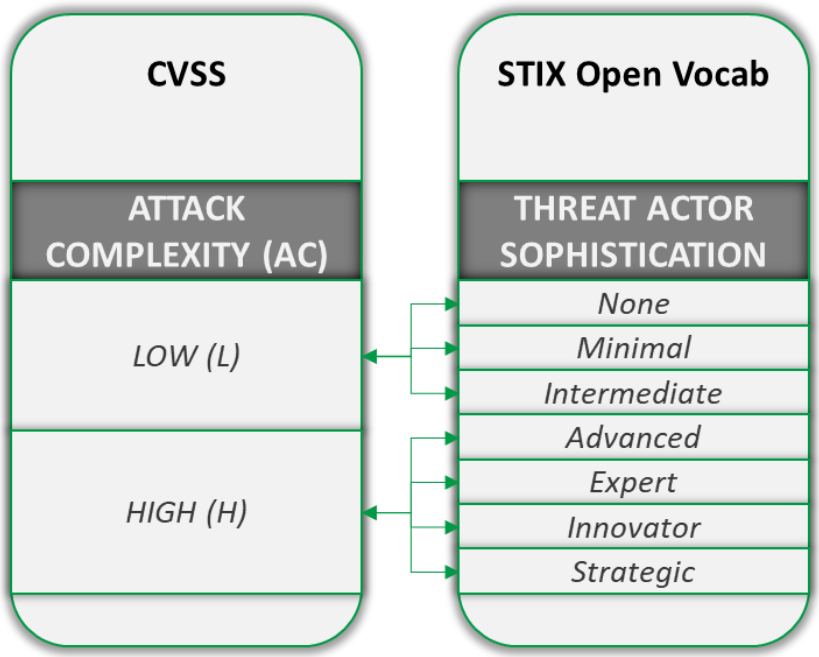
In CVSS the Attack Complexity is an absolute value, but we understand that it is relative to the Threat Agent sophistication. Highly sophisticated adversaries may have little to no trouble to exploit a vulnerability that has been classified as “High complexity”.

In the subjective perspective of such a confrontation, the attacker may perceive it as a “Low complexity”, changing virtually the vulnerability severity for the defender from High to Critical.

By using STIX OpenVocab's "Threat Actor Sophistication" against the CVSS's "Attack Complexity", it helps to prioritize vulnerability remediation based on the organization Threat Landscape.

One organization with sophisticated adversaries will see their risk scoring revised upwards, while organization with no relevant Threat Agent will see their risk scoring revised downwards.

Mapping CVSS Vectors with STIX Open Vocab



3.4 STRIDE and MITRE CAPEC/ATT&CK

Very similarly to use MITRE CAPEC/ATT&CK for Attack Trees, the Threat Event databases can be leverage to refine a STRIDE analysis. STRIDE involves identifying and analyzing six types of threats: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

CAPEC and ATT&CK can provides more detailed information with detailed procedures for each of the sic STRIDE's threats. It may also help to go a step further in the threat analysis by providing information about the motivations and goals of attackers, the tactics and techniques they use, and the systems and assets they target.

4. Integrating Threat Intelligence into Cyber Risk Management

Introduction

Risk Management generally considered the threat factor as real. The outcome is to provide conditional risk assessment that does not fit an organization threat landscape.

For about a decade now, Cyber Threat Intelligence activities emerged as the most mature way to provide information about adversaries and their modus operandi.

This intelligence can be used for risk assessment by helping organizations to understand the potential threats they face, and the likelihood of those threats being realized, with the following main benefits:

- **Improved understanding of the threat landscape**: Gain a better understanding of the types of threats to prioritize their risk assessment efforts and allocate resources appropriately.
- **Enhanced risk assessment accuracy**: Basing risk assessments on up-to-date and accurate to more accurately assess the risks they face and make more informed decisions about how to mitigate those risks.
- **Improved risk management**: Implement risk management measures that are tailored to the specific threats they face to better protect their assets.
- **Enhance your preparedness**: Appropriately respond to a cyber to minimize the damage caused by a cyber attack and recover more quickly.

During our Threat Modeling methods review, we identify two main approach that do integrate Threat Intelligence in their process: PASTA and EBIOS RM.

Based on XRATOR's real world experience conducting tailored risk assessment using threat intelligence, we offer to the cybersecurity community the following tips and improvement to current methodologies.

4.1 PASTA

PASTA uses a structured approach to identify and evaluate potential threats, and it incorporates the use of cyber threat intelligence as a key component of the process. It is deeply rooted in the steps number 4 (“Threat Analysis”), 5 (“Vulnerability & Weakness Analysis”) and 6 (“Attack Modeling”).

During our review, we emphasize that PASTA relied on ingesting Cyber Threat Intelligence during the phase 4 and used no standard. We highly recommend during this phase to use:

- **STIX Open Vocab**: to structure and normalize adversary’s sophistication and motives.
- **MITRE CAPEC/ATT&CK**: to structure and normalize the Threat Events.
- **Cyber Kill Chain**: to structure and normalize the Threat Agent’s Tactics, Techniques and Procedures (TTP).

This improvement will help to create more reproductible threat-based risk assessment, to compare them in time and to facilitate the communication with a shared vocabulary.

PASTA’s Vulnerability & Weakness Analysis phase and PASTA’s Attack Modeling phase are mainly based on Attack Tree and CVSS. The advises we provide previously (cf *3.3 Attack Trees and MITRE CAPEC/ATT&CK* and *3.4 CVSS and STIX Open Vocab*) still applies.

With the structuration of the previous threat intelligence phases, the vulnerability analysis and attack modeling work will be facilitated and more straightforward.

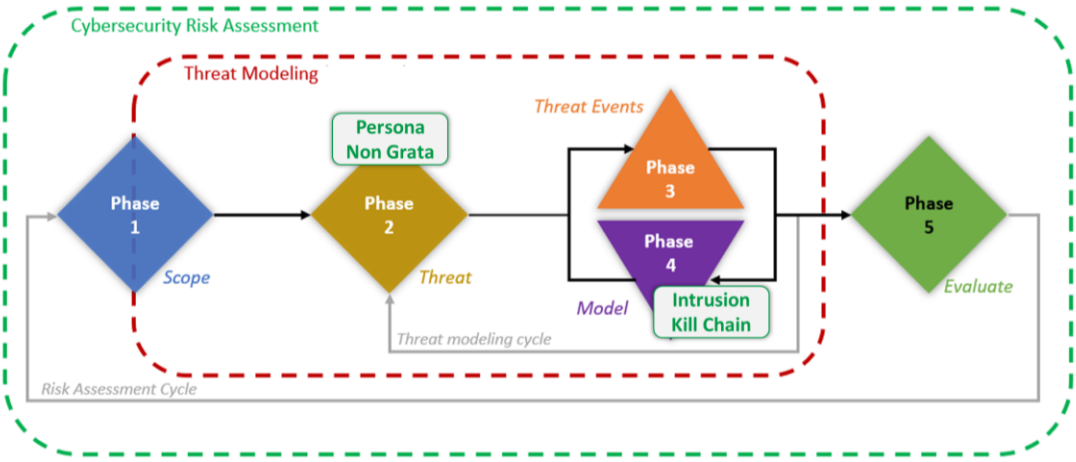
4.2 EBIOS RM

EBIOS RM integrates key activities and tools of cyber threat intelligence as component of its phase n°2 (“Adversary Identification”) and its phase n°4 (“Operational Scenario Modeling”).

A first limitation of EBIOS RM is that they do not recommend any method for the Adversary Identification phase. The approach is left to the discretion of the workshop attendees. We highly recommend during this phase to use the ***Persona Non Grata*** Threat Modeling approach complemented with ***STIX Open Vocabulary***.

A second limitation of EBIOS RM is that they do not encourage the use of a standard Kill Chain during the phase n°4. The goal of this phase is to build technical scenario based on a KNOWING-ENTERING-FINDING-EXPLOITING simplified cyber kill chain, with a free expression of the attack techniques used at each phases.

While this simplified Kill Chain is very handy for a nontechnical audience, it may be difficult to communicate with other stakeholder that will not be familiar with the custom kill chain. Using the traditional ***Lockheed Martin Intrusion Kill Chain***, even with its own limitation, may be more suitable.



But moreover, the lack of normalization and structured vocabulary in the expression of techniques is more concerning. Using by default a shared knowledge database such as ***MITRE ATT&CK*** or ***MITRE CAPEC*** helps to refine the attack techniques, facilitate a coverage review with the Security Operating Center, made more straightforward the operational countermeasures and mitigation and structure the possible intervention of a Red Team on the critical attack paths that have been identified.

Final words

Conclusion

In our increasingly interconnected and technology-dependent world, cyber attacks have the potential to disrupt essential services and infrastructure, put to the ground organization of all sizes, leading to widespread and severe social, political, economical and individual consequences. Ensuring an effective cyber risk management program is essential. To improve the efficiency and accuracy of Risk Management, it is now critical to integrate the ***threat*** component when assessing the situation and prioritizing the mitigation.

During our review of Threat Modeling methodologies, we identified approach suitable for Threat Agent focus situation, Threat Event approach, as well as for vulnerability exploitation. Threat Modeling has been in use since the Cold War by military to deal with critical situation and software threat modeling is a widespread activity since the late 1990's, with notable traction recently to ensure security by design.

Based on XRATOR's expertise in Offensive Security, Risk Assessment and Threat Intelligence, we contribute to improve Cyber Risk Management by providing concrete methods to integrates deeply real-world threat activity into the risk mitigation process. We shows how Threat modeling could improve the risk assessment process, relying on existing and recognized methodologies such as PASTA and EBIOS RM. We also provide advises and tools, from the Cyber Threat Intelligence disciplines, to enhance the precision and the normalization of the overall process.

References

[1] RICHET, Jean-Loup. *How cybercriminal communities grow and change: An investigation of ad-fraud communities*. Technological Forecasting and Social Change, 2022, vol. 174, p. 121282.

[2] WIENER, Norbert. *Cybernetics or Control and Communication in the Animal and the Machine*. MIT press, 2019.

[3] NING, Huansheng, YE, Xiaozhen, BOURAS, Mohammed Amine, et al. *General cyberspace: Cyberspace and cyber-enabled spaces*. IEEE Internet of Things Journal, 2018, vol. 5, no 3, p. 1843-1856.

[4] STRATE, Lance. *The varieties of cyberspace: Problems in definition and delimitation*. Western Journal of Communication (includes Communication Reports), 1999, vol. 63, no 3, p. 382-412

[5] WILLIAMS, Brett T. *Cyberspace operations*. presentation at the Joint Advanced Cyber Warfare Course, 2014, vol. 11.

[6] REFSDAL, Atle, SOLHAUG, Bjørnar, et STØLEN, Ketil. *Cyber-risk management. In : Cyber-risk management*. Springer, Cham, 2015. p. 33-47.

[7] COX, JR, Louis Anthony. *Some limitations of "Risk= Threat× Vulnerability× Consequence" for risk analysis of terrorist attacks*. Risk Analysis: An International Journal, 2008, vol. 28, no 6, p. 1749-1761.

[8] SPENCER, W. Dean. *Software development for AN*. Georgia Institute of Technology, 1979.

[9] SMITH, Suzanne T. *Risk assessment and LAVA's (Los Alamos Vulnerability and Risk Assessment) dynamic threat analysis.* Los Alamos National Lab.(LANL), Los Alamos, NM (United States), 1989.

[10] EDWARDS, Charles, MIGUES, Samuel, NEBEL, Roger, et al. *System and method of data collection, processing, analysis, and annotation for monitoring cyber-threats and the notification thereof to subscribers*. U.S. Patent Application No 09/950,820, 28 mars 2002.

[11] ABU, Md Sahrom, SELAMAT, Siti Rahayu, ARIFFIN, Aswami, et al. *Cyber threat intelligence–issue and challenges*. Indonesian Journal of Electrical Engineering and Computer Science, 2018, vol. 10, no 1, p. 371-379.

References

[12] KWIATKWOSKI, Ivan, MOUCHOUX, Ronan *Automation and Structured Knowledge in Tactical Threat Intelligence*, Botconf, 2018.

[13] CLARKSON, Albert, KRASNO, Laurence, et KIDD, Jerry. *Indications and Warning Analysis Management System IWAMS. A Design Study*. ESL INC SUNNYVALE CA, 1980.

[14] CLEVER, John J. *Computer site threat identification and analysis.* Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 1989.

[15] PARKER, Donn B. *Managers' Guide to Computer Security*. Reston Pub., 1981.

[16] SALTER, Chris, SAYDJARI, O. Sami, SCHNEIER, Bruce, *et al. Toward a secure system engineering methodolgy.* In : *Proceedings of the 1998 workshop on New security paradigms*. 1998. p. 2-10.

[17] SHOSTACK, Adam. *Experiences Threat Modeling at Microsoft.* MODSEC@ MoDELS, 2008, vol. 2008, p. 35.

[18] SHARMA, Anup, GANDHI, Robin, ZHU, Qiuming, *et al. A social dimensional cyber threat model with formal concept analysis and fact-proposition inference*. *International Journal of Information and Computer Security*, 2013, vol. 5, no 4, p. 301-333.

[19] XIONG, Lagerström. Xiong W., Lagerstrm R. *Threat modeling a systematic literature review*, Computers & Security, 2019, vol. 84, p. 53-69.

[20] ENGSTRÖMA, Viktor et LAGERSTRÖMA, Robert. *Two decades of cyberattack simulations: A systematic literature review. Computers & Security*, 2022, p. 102681.

[21] SHEVCHENKO, Nataliya, CHICK, Timothy A., O'RIORDAN, Paige, et al. *Threat modeling: a summary of available methods.* Carnegie Mellon University Software Engineering Institute Pittsburgh United States, 2018.

[22] Denning, T. A.; Friedman, B.; & Kohno, T. Home. *Security Cards: A security threat brainstorming toolkit*. 2013.

[23] Cleland-Huang, Jane. *"How well do you know your personae non gratae?."* IEEE software 31.4 (2014): 28-31.

[24] SCHNEIER, Bruce. *Attack trees.* Dr. Dobb's journal, 1999, vol. 24, no 12, p. 21-29.

References

[25] *Common Vulnerability Scoring System v3.0: Specification Document*. Forum of Incident Response and Security Teams. (accessed on the 2022-11-23).

[26] Kohnfelder, Loren, and Praerit Garg. "*The threats to our products.*" Microsoft Interface, Microsoft Corporation 33 (1999).

[27] *OWASP Threat Dragon*. Open Web Application Security Project (accessed on the 2022-11-24).

[28] *Getting started with the Threat Modeling Tool*. Microsoft (accessed on the 2022-11-24).

[29] SCANDARIATO, Riccardo, WUYTS, Kim, et JOOSEN, Wouter. A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering*, 2015, vol. 20, no 2, p. 163-180.

[30] WUYTS, Kim, SCANDARIATO, R., JOOSEN, W., *et al. LINDDUN: a privacy threat analysis framework*. 2014.

[31] UCEDAVELEZ, Tony et MORANA, Marco M. *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons, 2015.

[32] UCEDAVELEZ, Tony. Real world threat modeling using the pasta methodology. *OWASP App Sec EU*, 2012.

[33] Alberts, C.; Dorofee, A.; Stevens, J; & Woody, C. *Introduction to the OCTAVE Approach.* Software Engineering Institute, Carnegie Mellon University. August 2003. (accessed on the 2022-11-25).

[34] *EBIOS Risk Manager - The Method*. ANSSI (accessed on the 2022-11-25)

Lead the change.