6
Cyber Threat Modeling and Adversary Analysis

To implement a sound defense system, it is essential to understand *what* needs protection and from *who*. With the increase in security breaches, organizations must measure and project the potential threats that can impact the system and develop proper mitigation plans. Such is the purpose of threat modeling. **Threat modeling** is used to better understand yourself, understand the adversary, and map the two to create a better defense (remediation plan and resource protection). When an organization initiates threat modeling, two main components need to be highlighted: *organization resources* and *adversary knowledge*.

This chapter focuses on strategically modeling threats and analyzing the adversary's behavior. This chapter aims to equip you with the methodologies necessary for proactive cyber threat analysis and defense. We will look at adversary modeling as it is a critical concept in identifying the behaviors and characteristics of adversaries.

By the end of this chapter, you should be able to do the following:

- Understand the threat modeling process.
- Understand the different threat modeling methodologies and their optimal application.
- Understand SIEM and its importance in threat intelligence and modeling.
- Understand and perform advanced analytics to identify abnormal user behavior.
- Understand and discuss automatic and manual techniques for adversary analysis.

In this chapter, we are going to cover the following main topics:

- The strategic threat modeling process
- Threat modeling methodologies
- Advanced threat modeling with SIEM
- User behavior logic
- Adversary analysis techniques

Technical requirements

For this chapter, no special technical requirements have been highlighted. Most of the use cases will make use of web applications if necessary.

The strategic threat modeling process

The threat modeling process is a *systematic* and *structured* set of steps that facilitate the planning, provisioning, and optimization of security operations. It consists of breaking down the necessary elements that can be used to ensure and enforce protection. Those elements include the following:

- **Identifying assets**: Any resource that can be compromised or wanted by an adversary.
- **Risk and vulnerability assessment**: The ability to highlight system flows that, if exploited, can compromise an organization's assets.
- **Adversaries and threats**: The different adversary groups that have targeted or are targeting assets in the organization's profile, their **Tactics, Techniques, and Procedures** (**TTPs**), and all existing threat vectors that they can use to exploit the system flows.

The security or threat intelligence analyst must then map these three elements to create a basic threat model that can help implement a solid and effective security defense. A threat model is not standard. Hence, each organization may have different models, depending on the objectives and business profile. Therefore, we can deduce the main questions that can drive the development of a threat model process: *What do we have that might be of interest to attackers? Who can attack or target our system? How can they attack our system? What can we do to stop the attack or at least reduce its impact? Is the system safe now?*

Using these questions, we can build a threat modeling process skeleton to serve as the basis of our security operations, as shown in the following diagram:

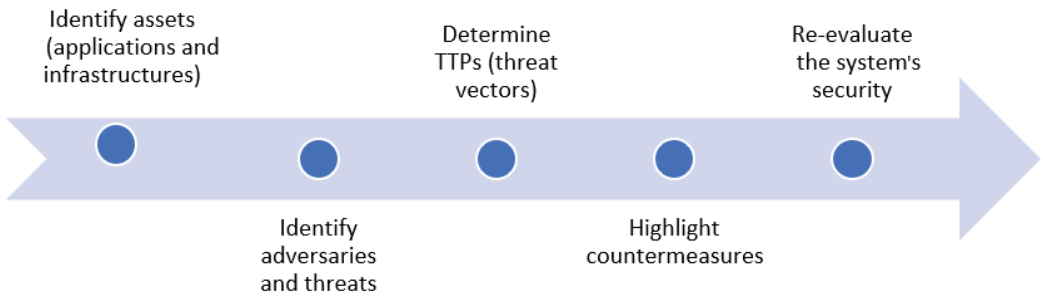

Figure 6.1 – Basic threat modeling process

Each step involves a set of techniques to simplify the modeling process. In the following subsections, we look at each step in detail and summarize the techniques that are mainly used.

Identifying and decomposing assets

The first step involves highlighting the resources that adversaries can attack – knowing the organization. Assets are classified based on the business units they belong to. For example, you can group assets into four categories: financial and personal data, network data, intellectual property, and system availability. **System availability** applies to those resources that, if compromised, can stop the business' operations. This includes software applications, network traffic, and so on. During the identification and decomposition phase, the threat intelligence analyst, along with the internal security members, must understand how assets interact with each other and the external world. They must explicitly create use cases around each asset to highlight its utility (how it is used and manipulated). By understanding the use case for each asset, the analyst must identify access points (points that can allow a hacker to gain access to the system and compromise that specific asset) and highlight the asset's trust levels (how access to the asset is controlled internally and externally).

Asset identification includes resources such as servers, endpoints, laptops, applications, intellectual property, databases, sensitive files, network resources (bandwidth utilization), and server rooms (any physical and digital resource that is of utmost importance to the organization). The internal team and the intelligence analyst must document all assets, their use, and location.

Another critical aspect of the first step is asset decomposition. **Decomposition** involves breaking down asset utilities, highlighting entry points, and access right management to effectively evaluate its security. By decomposing assets, we look at how all the assets come together and identify at which point the asset can be targeted. We can use a **data flow diagram** or a **process flow diagram** to decompose organization assets. Although not designed originally for security modeling (system development and engineering), a data flow diagram displays all the primary building blocks of applications and how they work. This shows how interactions between components are done, and the protocols and third-party applications used to make the applications work. A process flow diagram decomposes assets in a way to highlight how attackers can target them. A process flow diagram uses the concept that attackers focus on the processes between the different use cases of the assets rather than the data flow. In this part, we use a bit of both as an attacker can also leverage vulnerabilities at the application level (such as web servers, JDBCs, database servers) and the physical level (lack of security in the data center where physical servers are installed). Resource decomposition for a typical health organization is shown in the following diagram (the assets are not exhaustive but comprehensive).

From the following diagram, we can identify the list of assets (an **Apache web server** containing the **medical application** for users situated in **Data Center B**, which is also a DMZ, as well as three database servers containing users' **financial**, **personal**, and **medical information**, which is located in **Data Center A**):

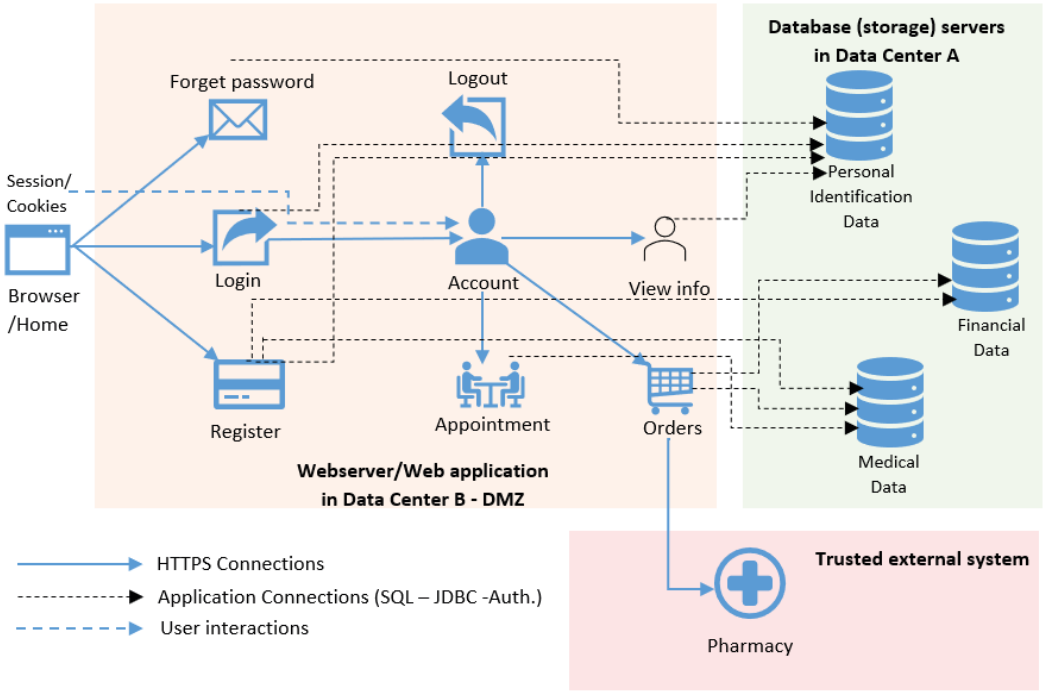

Figure 6.2 – Basic asset decomposition for the threat modeling process

The preceding diagram also displays the different use case applications for asset interactions. For example, a patient can register, log in, or use the forgot password application to interact with the system's backend. Those are some of the most targeted points of entry in a system. If they're not secured appropriately, an attacker can inject malicious codes to compromise the system. The preceding diagram also shows the different resources that can be impacted during a cyber attack. Thus, it is a good visualization and first hint at countermeasure implementation.

Asset decomposition is not a standard process. It depends on the organization's business and sensitive resources. It can be simple or complex, depending on the organization's size. The process of decomposing assets using a process flow diagram includes the following:

- **Determining the asset's use cases**: Web or desktop applications (login, search forms, contact forms, password recovery, session data). It also includes highlighting storage and repositories, their content, and location.
- **Outlining communication protocols**: This describes how assets communicate internally and how they interact with external systems (trusted or public, such as the internet).

- **Outline other resources that can be used to control the assets**: This can be digital technical controls or physical server rooms.

By listing and decomposing assets (applications and infrastructures), an organization should be able to visualize what could be of interest to the adversaries and what could be potential doors to those resources (also known as **attack surfaces**). This step is very crucial when performing threat modeling.

Adversaries and threat analysis

Adversary is a cybersecurity term that has is primarily attributed to an attacker or a threat actor with malicious intent. As traditionally known, the primary objective of an adversary is to compromise one or all of the **Confidentiality, Integrity, Availability** (**CIA**) triad parameters. However, in the scope of modeling threats, we refer to an adversary as every person, robot, tool, and system that can voluntarily or involuntarily attack the system or initiate unauthorized access to the organization's assets. We go a little bit above the traditional definition of an adversary as some adversaries do not need to have malicious intents to be categorized as threats.

This step involves outlining the adversary and their spectrum of applications (abilities, capabilities, and objectives). An organization can choose to model adversaries in groups or individually. This step answers the question, *"Who is targeting our system?"*. The following is a non-exhaustive list of adversaries, along with their spectrum of operation. However, it is advised for each organization to have an exhaustive list of adversaries or groups, including untrusted journalists. It is also essential to determine the adversary, the threat they pose, their motivation, and their likelihood to compromise your organization (which varies depending on the industry, business size, political climate, country of operations, and so on), as shown here:

- **Black Hat Hackers**: They are known for accessing complex systems, bypassing complex security infrastructures (threats include system hacking, spoofing, man-in-the-middle attacks, social engineering attacks, impersonation, system intrusion, and so on). These people should be a concern to any organization. This category includes structured black hat hackers (*professionals with solid skills* in compromising systems) and unstructured black hat hackers (also known as *script kiddies*). Their motivations include curiosity, ego (fame), financial gain, data alteration, theft, and more. They target enterprises and individuals, depending on their motives.

- **Organized Crime**: Organized crime is another category of adversaries that organizations and analysts must consider. However, depending on the type of business and its objectives, it is essential to determine if organized crime can be a threat to you. *Do you have something that the group can target?* This category of adversaries possesses resources and might be led and controlled by influential criminal organizations (threats include phishing, credit card fraud, backdoors, advanced malware, rootkits, zero-day attacks, crypto cracking, C2 systems, and more). Their motivations may include profit, sensitive data theft, and unauthorized data modification. Organized crime usually targets enterprises, credit card companies (point of sales), and any organization with valuable data for them.
- **Industrial Espionage**: In the world of competition, businesses can do whatever it takes to stay ahead of the game. Industrial espionage targets an organization's trade secrets, which can be detrimental to a business and its integrity. Therefore, it is essential to evaluate the possibility of industrial espionage. The first step should have identified company files, IPRs, and any property information that needs protection. Industrial espionage threats include high-level attacks with long-term objectives. Its scope is broad and sophisticated. Their motivations include technology and knowledge compromise and critical corporate data theft. The likelihood of espionage attacks occurring depends on the organization's business domain, objectives, and assets to protect.
- **Insiders**: Insiders can be challenging to detect or fight against because they form part of the business. It is not straightforward to detect the moment where their loyalty or intention changes. Insiders can be disgruntled staff members (probably with administration access rights) or ordinary employees who inadvertently compromise the system with malpractices. Their threats span fraud, mediocre performance to malicious code, and unsafe security practices. Depending on their class (a malicious internal hacker or poorly trained staff), their motivations can be financial gain, dissatisfaction, or simply unintentional mistakes. Hence, having an insider group of actors is of utmost importance when performing threat modeling.
- **Hacktivists**: This category of adversaries compromises systems for supporting or not supporting certain ideologies. As a business, it is essential to evaluate if hacktivist groups can be a threat to the organization. For example, for companies or individuals who work on social policies and political matters (attorneys, contractors, and state organizations), it is crucial to insert hacktivists into the adversary definition matrix, as explained in the *Adversary analysis techniques* section later. Their motivation includes ideology support and, to some extent, profit. Some threats in this category include ransomware, phishing, **Distribution Denial of Service** (**DDoS**), rootkits, and zero-day exploits. This category's attack probability depends on an organization's business and social or political stand.

- **Nation-State Hackers**: Competition is not only economic. It is also political. With the recent increase in inter-state espionage, countries have taken different stands on cyberspace matters. Governments are sponsoring hackers to attack other governments for intelligence and other motivations. State hackers are also known for targeting individuals and businesses to gain economic and technological benefits on behalf of the state. The state's backup (licensed hacking) makes them almost untouchable and challenging to detect – they are provided all sorts of resources and new technologies to conduct their malicious activities. Their threats include **Advanced Persistent Threats** (**APTs**), **sophisticated multi-vector attacks**, and **critical infrastructure compromise**. The motivation behind this adversary category includes political and economic advantage, social or military power, and revenge. Geopolitical cyber crimes need to be considered by any organization that wishes to provide reliable system protection. The likelihood of a state-sponsored hack occurring depends on the country of operation and the line of business. ID agent presents some helpful information about nation-state hacking at the following link: `https://bit.ly/3sKN6XT`.
- **Cyber Terrorists**: Terrorist groups present a significant threat to organizations. They rely less and less on military strategies and adopt cyber techniques to fulfill their objectives. Although in most cases, they target governments, organizations need to include them in their adversary matrix. The likelihood of such attacks depends on the organization's line of business and its affiliation with specific social or political ideologies. An online shop organization is unlikely to experience a cyber-terrorist attack compared to a government contracting law firm that supports a movement. Their threats include APTs, ransomware, phishing, DDoS, and supply chain attacks. Cyber terrorist actors' motivation is ideological through violence. Thus, an organization must rank cyber-terrorist groups and their impact in the adversary matrix.
- **Other Non-Malicious Groups**: An attack does not have to be malicious to fall into the threat category. Search engines, for example, can make your information available to competitors if there is no restriction on the amount of information that's shared on the internet. Journalists may try to access an organization's sensitive information – not to harm or compromise but to publish their stories and *prove a point*. An employee who's not appropriately trained can leave windows of vulnerabilities in the system unintentionally. The organization must consider this category of attack when modeling threats.

There are several adversary groups. The threat intelligence analyst needs to work with the internal security stakeholders to identify all the potential threat actors and create a threat map to visualize the threat model.

Threat analysis

Each of the adversaries mentioned previously has a motivation for their actions. What makes them threats are their *intents*, *capabilities*, and *opportunities*. Threat analysts must map these assets to the adversaries, taking into consideration the three characteristics of a threat. A framework such as the **MITRE ATT&CK** framework is an efficient way to map adversary groups with assets that they are after. At this stage of the modeling process, the analyst does not have to detail the techniques that are used by the groups. We have provided an adversary asset map, as shown in the following diagram, to illustrate this concept. This map's needs must be extended based on the assets identified and adversaries defined:

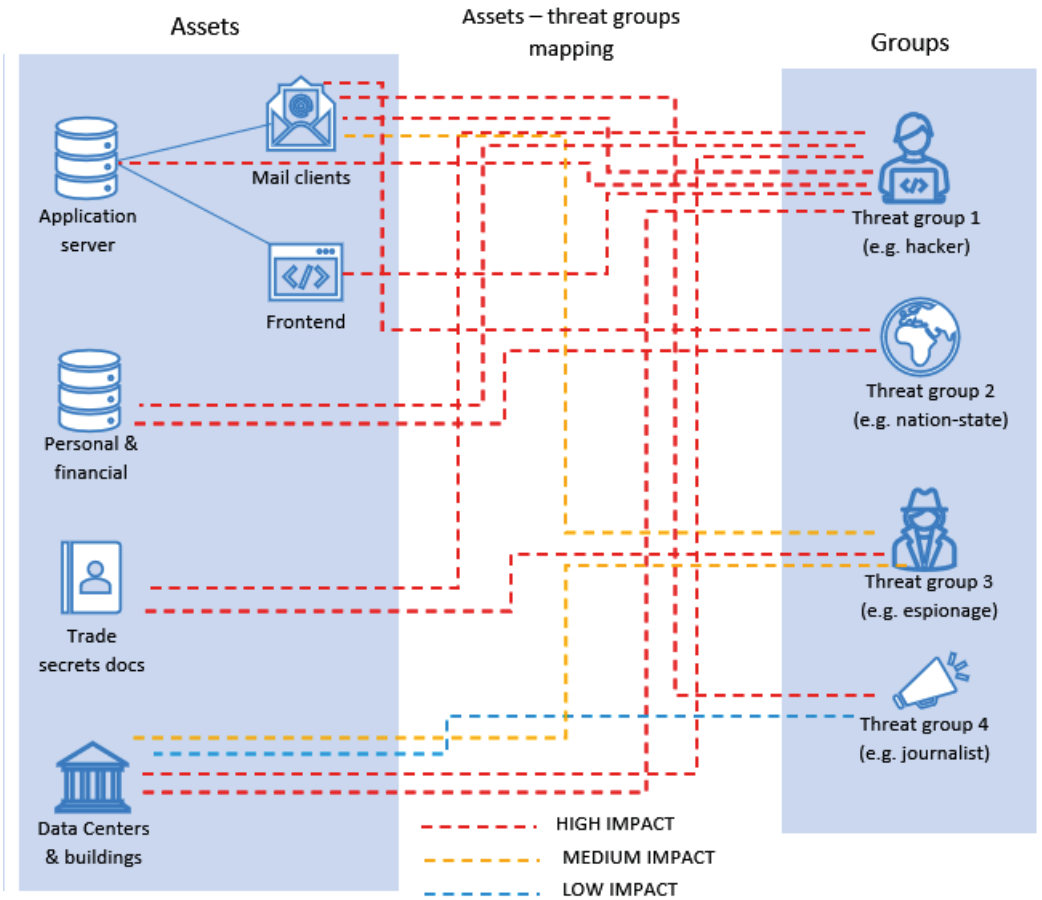

Figure 6.3 – Simplified assets to threat groups (adversaries) mapping

The preceding diagram illustrates a simple model for mapping assets to threat groups. For example, malicious hackers are known for targeting any or all resources in the organization that are valuable to them. They can target servers, encrypt data, and exfiltrate sensitive information depending on their objectives. If a hacker group gains access to financial and personal information, the impact is *high*. Suppose the same group gains physical access to a data center (through an insider actor). In that case, the impact is also high because they can physically plug devices to implant malware. State-sponsored hackers might be after personal information for national security. They become high risk when they get access to the personal information database. They can also be considered high risk if they access the organization's email server (or messages).

A standard journalist who wants to publish a story can be a risk to an organization. They are at high risk when he/she has access to corporate emails (can use that as proof for the story). They are low risk when there is physical access to the company building (information will not just be given to them).

This mapping can be done using colors where *red* means *high impact* to the organization and *blue* means *low impact*. Alternatively, it can be done using weighted lines with high-weighted lines representing asset-to-adversary high impact or high-risk links. The threat intelligence team must map the adversaries to assets to understand the threat level that each adversary poses. Next, we will look at step three: attack surfaces and threat vectors.

Attack surfaces and threat vectors

An adversary must identify an entry point (or entry points) into the target system for cyber attacks to occur. All the entry points to a particular system create an *attack surface*. Protecting a network means reducing the attack surfaces – the fewer attack surfaces there are, the lower the chance of experiencing cyber attacks. The first task in step three is to define all the organization attack surfaces. Once an attack surface has been identified, the adversary selects the best and most reliable methods to conduct the attack. These are known as *threat vectors*. The second task of step three is to highlight all, if not most, threat vectors that adversaries use. The last task is to map the attack surfaces to threat vectors to create a surface-vector matrix.

Attack surfaces

There are two fundamental attack surfaces in cyberspace: *people* and *devices*. While organizations invest a lot in device security, people remain the weakest link in the security chain and the most targeted entry points to networks and systems. Although they have improved in the past years (from 25% to 3.4% for phishing attacks), human errors still account for 22% of security breaches, according to the *2020 Verizon report* (`https://duo.sc/3vam3Hd`). And 95% of cloud breaches are attributed to human errors (mostly misconfigurations), as reported by *Gartner* (`https://on.wsj.com/3vchI6A`). Techniques such as social engineering, which is entirely based on manipulating people, account for 70-90% of data breaches (`https://bit.ly/3naESHy`). All these statistics show that when modeling threats, the likelihood of cyberattacks occurring through people should be set to *high*.

Devices, on the other hand, play a crucial role in networks and systems. Physical or virtual, they are used as endpoints, storage components, network elements, security components, servers, and so on. The threat analysis team must list the devices and applications in the network. The team must classify devices in such a way as to identify them. For example, we can have six device categories:

- **Infrastructure**: This refers to devices or resources that facilitate communication, business operations, and accessibility to other resources. This includes servers, switches, routers, firewalls, IDSes, IPSes, wireless **access points** (**APs**), proxy servers, VPN gateways, **Network Attached Storage** (**NAS**) devices, and any other node used to facilitate communication and accessibility. These devices provide different services to the system.
- **Applications**: This refers to services that network elements or vendors provide. The analyst must list the different services used, such as DNS services, SMTP services, DHCP services, share directories, NTP services, web applications, authentication services such as LDAP, and others. They must also list regular applications that can be used for daily operational tasks (Office 365, Adobe programs, and so on).
- **Endpoints**: This includes end-station devices such as workstations, laptops, mobile phones, printers, point of sale devices, and industrial machines. The analyst must list all the endpoints that are available in the system for reliable protection.
- **IoT devices**: With the number of connected devices projected to grow in the future, several organizations are already adopting IoT technologies. If applicable, these devices need to be added to the list of potential attack surfaces. Such devices include biometric scanners, smart surveillance cameras, **voice over IP** (**VoIP**) devices, and intelligent equipment. Companies that build self-driving cars must also add them to the list because they are an attack surface.

- **Cloud resources**: This refers to the organization or individual cloud-based infrastructure and applications such as cloud storage, cloud networks (virtual private cloud), and cloud web servers. The analyst must be aware of all the cloud services that the organization runs.
- **Supply chain**: The supply chain includes any additional resources such as third-party licenses, software, applications, and certificates. All of these need to be included in the attack surface list.

Devices and people constitute a potential risk to a system and present an excellent attack surface for adversaries. Hence, to protect the system, it is essential to enumerate all existing attack surfaces accurately. It is challenging to list all the endpoint devices for a large enterprise. Hence, it is necessary to focus on the types of endpoints and their known vulnerabilities. It serves as a policy and reference when it comes to resource management – for example, denying access to all workstations that do not have the latest operating system could be an effective endpoint management rule to reduce the chances of attacks occurring.

Threat vectors

Adversaries use several methods and techniques to attack networks and systems. The MITRE ATT&CK framework provides most of the global TTPs that are used by attackers to carry out different tasks. The threat intelligence team's task is to list attack methods that can be used to compromise the organization and its resources. However, the following are some of the standard methods used by threat actors to perpetrate attacks:

- **Phishing**: A standard and widespread method of perpetrating cyber attacks. Phishing, in general, can be challenging to mitigate because, most of the time, employees or individuals are not careful or trained enough to analyze the structure of phishing content. Almost 25% of data breaches involve phishing, as per *Verizon report 2020*. Phishing is one of the biggest carriers of malware, ransomware, data theft or alteration, and sensible data compromise (email, identity, and so on). The intelligence team must be aware that the likelihood of phishing attempts against the organization or an individual is *high*.
- **Malware**: Malicious software is the heartbeat of many data breaches. In almost every data breach, malicious software is involved. **Worms**, **viruses**, **spyware**, and **trojans** are all used to carry out malicious activities. Although its impact can be overlooked by individual and home users, malware infections can completely break down a system and affect the integrity and availability of the entire network. Hence, the intelligence team needs to consider a high probability of potential malware infection.

- **Ransomware**: The ransomware trend has been increasing recently and, according to the same Verizon report, it makes up 27% of malware attacks. *Statista* has shown that more than 300 million ransomware attacks were registered in 2020 (`https://bit.ly/3sN26Vg`). As the name suggests, the objective of the attack is to lock an organization's or individual's resources and demand a ransom to unlock them. Ransomware, like most malware, requires a vessel or another threat vector to enter the target system. It leverages vectors such as phishing, software vulnerabilities, malicious links, or remote control protocols to compromise the target. The intelligence team must be aware that the probability of a ransomware attack is *high* and growing at a fast pace. The three most common infection methods for ransomware involve **phishing**, **Remote Desktop Protocol** (**RDP**), and **unpatched vulnerabilities**.
- **Weak, stolen, and compromised credentials**: Usernames and passwords are still the most popular authentication method. When they're not protected appropriately, credentials can be exposed to unauthorized people, leading to unwanted access to accounts or resources. Weak passwords can be brute-forced and used maliciously. Admin users pose a high risk of credential attacks as their access privilege level allows them to control sensitive assets. Stolen or weak credentials make up 37% of credential theft breaches (as per the Verizon report). Harvested credentials and other **personally identifiable information (PII**) is often sold to criminal groups and brokers (mostly on the dark web) for financial gain through targeted attacks.
- **Poor or non-existent encryption**: Handling sensitive information is crucial. Non-existent encryption gives the attacker opportunities to access plain text information. Encryption plays an important role in the confidentiality aspect of the CIA triad. Encryption is applied to data in transit or at rest. If not correctly handled, adversaries can crack the ciphered traffic to access plaintext information. And if non-existent, then Christmas is brought to the attacker. **Man-in-the-middle** attacks are a threat vector that also leverages poor and non-existing encryption to eavesdrop on network traffic. Poor and missing encryption is a vector that can be attributed to human errors. Hence, it is essential to evaluate encryption flows.

- **Misconfiguration**: Misconfiguration is a human error risk and, as shown by the Verizon report, accounts for 22% of breaches as of 2020. Service misconfiguration is also the center of most web applications' attacks nowadays. Examples of misconfiguration include unvalidated or poorly validated form inputs and incorrectly configured SSL certificates. This category of threat vectors allows an adversary to inject malicious codes into the system. Some other vectors that make use of misconfiguration include **SQL injection**, **cross-site scripting** (**XSS**), **code injection, sensitive data exposure**, and **broken authentication**, just to name a few. The OWASP top 10 mainly describes vulnerabilities that result from misconfiguration. The intelligence team must consider misconfiguration risks. *Chapter 11*, *Usable Security:Threat Intelligence as Part of the Process*, provides good practices to facilitate the secure development of applications and products.
- **Unpatched vulnerabilities**: An organization or individual must always ensure that they use the latest patched software in the product or service stack. Adversaries can use unpatched vulnerabilities as attack vectors to compromise targets if the latter have not patched their software in the application stack. Fewer breaches, however, are linked to unpatched vulnerabilities, but their consequences can be fatal. One of the most popular unpatched vulnerability attacks is the *2017 Equifax breach*, which cost more than $500 million in loss and more than $1 billion in security upgrades (`https://www.gao.gov/assets/gao-18-559.pdf`). Hence, unpatched vulnerabilities should not be taken lightly by the intelligence or the internal security team.

It is essential for the intelligence team to properly enumerate the potential threat vectors that adversaries can use against the organization or the individual that needs security. The more details included in the threat vector list and the more efficient the threat vector to attack surface map, the better the mitigation steps and recommendations will be.

Threat vectors to attack surface mapping

In the previous two subsections, we listed the attack surfaces and threat vectors that can facilitate cyber-attacks in our system. The next important task is to build a **vector-surface matrix** and an **attack tree** to link all the potential system entry points to the methods that can be used to exploit them. The vector-surface matrix is shown in the following diagram:

Attack surfaces	Category	attack surfaces vs threat vectors	phishing	malware	ransomware	malicious intruder	MITM	social engineering	weak passwords	brute-force	poor encryption	misconfiguration	unpatched vulnerabilities	credential theft	physical break-in	Spoofing & Poisoning	...
			Threat vectors														
	Infrastructure	servers		X	X	X			X	X	X	X	X	X			
		storage			X	X			X	X	X	X		X			
		routers			X	X			X	X		X	X			X	
		switches			X	X			X	X		X	X			X	
		firewalls, IDS, IPS				X			X			X					
		Wi-Fi AP				X			X	X		X	X				
		⋮															
	Applications	DNS services				X	X					X				X	
		DHCP services				X	X					X				X	
		LDAP Auth.				X				X		X		X			
		SMTP service				X	X					X					
		⋮				X						X					
	Endpoints	laptops			X	X			X			X	X	X	X		
		point of sales				X			X			X	X	X	X		
		smartphones			X	X			X			X	X	X	X		
		⋮															
	IoT Devices	biometric scanners				X						X	X		X		
		VoIP devices				X			X			X	X		X		
		CCTV cameras				X						X	X		X		
		⋮															
	Cloud	VPC				X						X					
		cloud webserver				X			X	X	X	X		X			
		cloud storage			X	X			X	X	X	X		X			
		⋮															
	3rd party	applications (apache, Java, etc)			X	X						X	X				
		libraries				X						X	X				
		SSL certificates				X					X	X	X				
		⋮															
	people	people, employees	X					X									

Figure 6.4 – Simplified attack surface – threat vectors matrix

The construction of the matrix, as shown in the preceding diagram, is simple. We put the attack surfaces on one axis and the threat vectors on the other. Then, we fill each block of the matrix with a sign if applicable. For example, although social engineering can affect the entire system, the point of entry is people. However, misconfiguration can be an entry point to each of the attack surfaces except people (for example a misconfigured server is a valid entry point, and so is a misconfigured DNS service).

The threat intelligence team must fill this matrix to understand how mitigation plans can be put in motion. For example, suppose we know that brute-force attacks can affect Wi-Fi access points. In that case, we can implement mitigation strategies to avoid brute-forcing Wi-Fi access points, such as account locking after a consecutive number of failed attempts.

Attack tree concept

Attack trees are diagrams that intelligence and security analysts can use to illustrate how an asset can be attacked. They are hierarchical maps of **asset-vector mappings**. The objective of the tree is to highlight potential paths that lead to the asset attack. We can use the attack tree to represent assets' attack vectors graphically and facilitate the development of countermeasures and mitigation steps. We select a **root node** to build an attack tree (representing the attack goal), **leaf nodes** (representing a specific vector), and **OR**/**AND** nodes to describe ways to get to the leaf nodes. The tree can only have one root node but may have several leaf nodes. Leaf nodes can also be split into several sub-nodes or OR/AND nodes:

- **Selecting the root node**: The root node that's selected is based on the goal. The analyst identifies the asset and asks the question, *What can be compromised?* An example of a root node is *stealing personal and credit information*.
- **Identifying leaf nodes**: The leaf nodes are subgoals or vectors to compromise the selected asset in the root node. For the preceding example, we can identify vectors such as *phishing*, *misconfigurations* (or *vulnerabilities*), *physical access* to the server room, and *breaking into the IT admin's PC* as leaf nodes.
- **Selecting the OR/AND nodes**: AND nodes are used when all the attack methods must be achieved. OR nodes are used when one or more procedures must be completed. We can use *phishing emails with attachments* OR *phishing emails with malicious (cloned) links* for a phishing node. We can use *input form attacks* OR *login brute force* for a misconfiguration leaf node.
- **Ranking the non-root node**: The threat intelligence analyst needs to rank all the non-root nodes. This ranking determines the likelihood of each leaf node or method occurring. In a typical attack tree, ranking can be achieved through boolean (1 or 0, yes or no) or assigned values. For example, an analyst can assign a value of *0.1* or *no* for physical access to steal personal and credit information.

Using this concept, we can create a comprehensive attack tree for a medium financial company using a critical asset (personal and credit information database). This tree is shown in the following diagram:

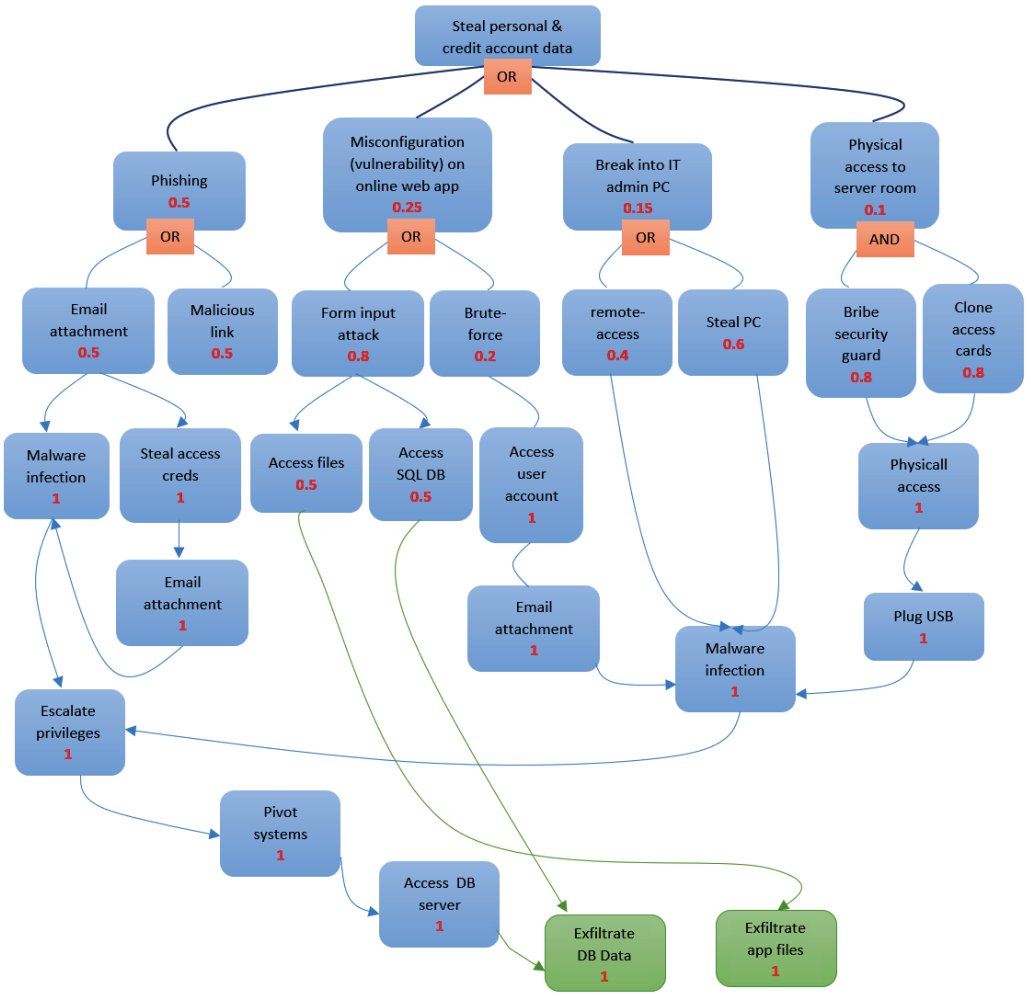

Figure 6.5 – Attack tree

The analysis of the existing infrastructure must support the ranking. The preceding diagram shows that there is a high probability of an attack occurring through phishing. Physical access to the server room is unlikely to happen unless the attacker is assisted by a person with access. A form input attack occurring by an attacker using the organization's online application is an option that is likely to be attempted compared to brute-forcing the authentication application.

The intelligence analyst and the security team should create attack trees for all the assets to facilitate countermeasures and mitigation plans. In the following section, we will look at an adversary and attack analysis use case: the Twisted Spider.

Adversary analysis use case – Twisted Spider

The first case we will look at is the Russian group known as Twisted Spider. The following points provide an analysis of the criminal group, which make up part of a criminal cartel in Eastern Europe:

- **Origin**: Eastern Europe, primarily speaking Russian.
- **Threat vector(s)**: Ransomware with several types, including the Maze and Egregor ransomware.
- **Ransomware technique**: Payload execution protection with a key, making it challenging for malware analysts. The group uses Rclone (`https://rclone.org/`), known as the Swiss-army knife of cloud storage. It also leverages public infrastructure such as FTP servers, C2 servers, and DropBox to exfiltrate data.
- **Attack restriction**: The payload can't be executed on Russian victims. That functionality is achieved by allowing the malware to check the victim's language. Old Soviet Union countries are exempted from the attack.
- **Campaigns and timeline**: Twisted Spider used the Maze ransomware between May 2019 and November 2020 and migrated to the Egregor ransomware after conducting several campaigns and personas with each malware.
- **Consequences**: The group extracted more than $75 million from various organizations, including hospitals, government institutions, and private sector organizations.
- **Anonymity**: Almost non-existent as the group willingly draws media attention, communicating with magazines and cybersecurity news organizations.
- **Some notable attacks and breaches**: The *Canon 2020 ransomware attack*, where almost 10 TB of data was stolen. The group's Maze ransomware was used for the breach. The group encrypted Canon, USA data and pressured the company to pay a ransom to restore the data. There was also the *Cognizant 2020 ransomware attack*, which cost the company more than $50 million in repairs. Finally, there was the *Allied Universal 2019 ransomware attac*k, where approximately 7 GB of data was extorted from demanding ransom. Many such breaches have been published by BleepingComputer (`https://bit.ly/2Ye1ler`).

- **Attach tree**: The group attack tree can be broken into two phases: data exfiltration and system encryption. This is shown in the following diagram:

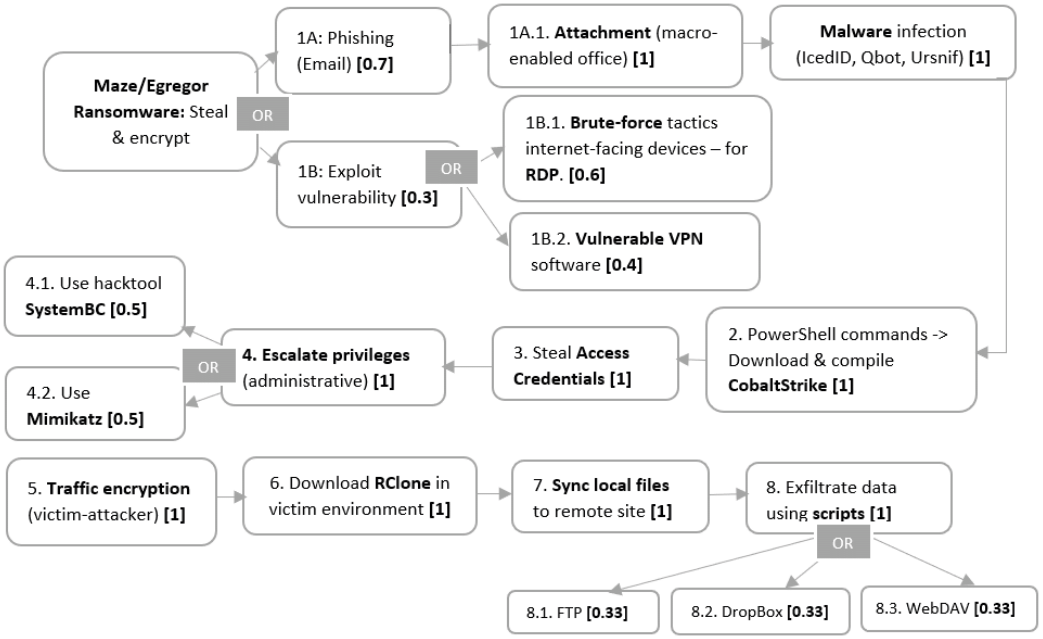

Figure 6.6 – Attack tree for Twisted Spider – part 1

The preceding diagram displays the attack tree before the data exfiltration process. We can see that the group uses phishing and vulnerability exploitation to gain access to the system. They also leverage open tools to communicate with the remote server (C2 server). The following diagram shows the second part of the group attack TTPs:

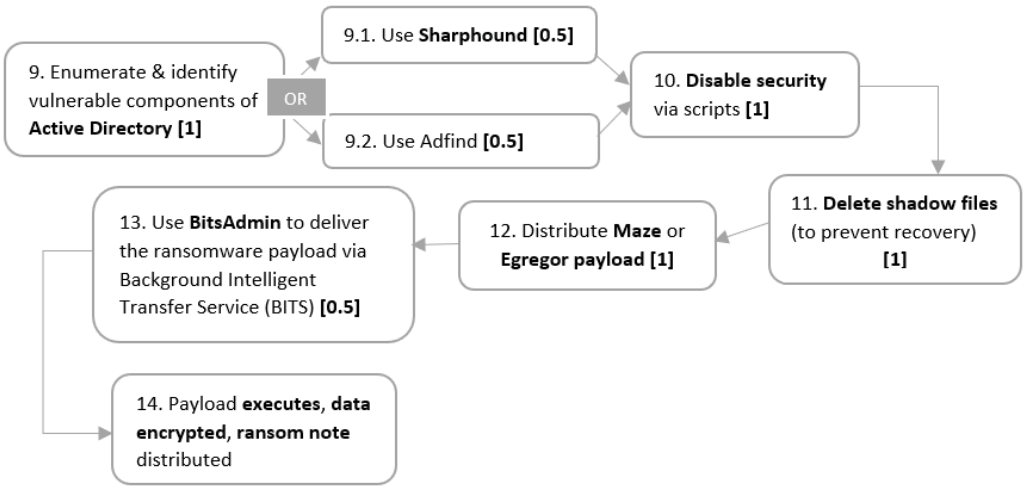

Figure 6.7 – Attack tree for Twisted Spider – part 2

- **Indicators of Compromise** (**IoCs**): Several IoCs are exposed directly linked to the Twister Spider group. Details of these indicators can be found at the following link. However, some infrastructure indicators include the C2 server IPs 91.218.114.30 and 91.218.114.31. IoCs will be covered in more detail in *Chapter 13*, *Effective Threat Intelligence Metrics, Performance Indicators, and the Pyramid of Pain*.

More information on the Twister Spider can be found at `https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf`.

As a cyber threat analyst, it is essential to understand how to profile and analyze adversaries. As an exercise, you can search for any adversary group and analyze them by following the structure provided in this section. In the next section, we will look at ways to identify countermeasures to threats and attacks.

Identifying countermeasures

Countermeasures involve all the steps that can be put in place to prevent attacks from happening or minimizing their impact. This stage aims to answer the following two questions: *How can I prevent the attack?*, in case the attack has already happened, and *How can I control the damage?*, where the analyst creates a table of each attack vector, provides a description, probable mode of infection, and possible countermeasures. Here we will provide an example of a vector and its countermeasures. We will also provide a basic guideline for making a threat model report summary:

- **Threat vector 1**: Malware attack.

  Description: A malware attack occurs when malicious software is implanted in the system and compromises the organization's standard operations. Consequences range from service disruption to remote system control and complete system shutdown. Note that malware can do a lot more damage than what's cited here.

  Mode of infection: Malware infection can happen through known system vulnerabilities, unpatched software applications, phishing, outdated vulnerable software, and many more.

  Countermeasures: Malware attacks can be difficult to avoid, especially in the case of zero-day exploits. However, it is essential to install reliable and up-to-date *antivirus* software. *Firewalls*, *IDSes*, and *IPSes* reduce the likelihood of malware attacks.

- **Threat vector 2**: Weak, stolen, and compromised credentials.

  Description: Credentials are very important for gaining access to the organization's resources. Attackers can compromise weak passwords or authentication processes. The consequences range from sensitive information breaches to identify theft.

  Mode of infection: Authentication credentials theft can happen through **shoulder surfing**, **dumpster diving**, **social engineering**, **man-in-the-middle** attacks, or **brute-force attacks**.

  Countermeasures: Users must use *complex and strong password combinations* (the organization must implement good password policies). *Avoid credential sharing*, especially when accessing network resources. *Implement two-factor authentication*. *Regularly reset the password* without using repetition or similarities to previously used passwords (enforce the policy to change passwords frequently). *Continuously track leaked passwords* through shared intelligence sources and immediately reset passwords if they're publicly compromised. *Limit the number of acceptable failed attempts* to ensure that brute-force or dictionary attacks are not used against the system and *take the appropriate action*.

> **Important Note**
>
> Password authentication needs to be carefully considered when it comes to usability versus security matters. Complex passwords can push users to write them down to avoid the hard effort of memorizing them, which is a security risk. Passwords must be secure and reasonable. Usable security will be tackled in *Chapter 11*, *Usable Security:Threat Intelligence as Part of the Process*.

- **Threat vector 3**: Phishing.

  Description: Phishing is a cyber method where the attacker impersonates a legitimate institution or person to push the target to take some actions that will compromise the security standard.

  Mode of infection: Phishing can happen through *opening email attachments*, *clicking malicious links*, *opening an infected file* (a trojan) from a USB drive, and *giving information over the phone*.

  Countermeasures: *Educate the users/employees* on detecting phishing content. Trace web browsing activities, email links being clicked, and files being opened. Phishing is easy to countermeasure but challenging to detect. Advanced phishing techniques can be difficult to countermeasure, especially when illegitimate traffic uses legitimate channels to expand the phishing campaigns. Because social engineering is its main road, *user awareness* is the best countermeasure. The CTI team (or analyst) must work with the rest of the security awareness team to build solid awareness and assist in protecting and counterattacking phishing campaigns.

Another effective way to represent countermeasures is to include them in the adversary to asset mapping, as illustrated in *Figure 6.3*. This method provides a visual representation of possible countermeasures between an asset and an adversary.

System re-evaluation

The last step of the strategic process for threat modeling involves re-accessing the system security stance after identifying all system threat components. This step introduces the best practices to minimize attack surfaces. The intelligence team or the organization security units must do the following:

- Assess the vulnerabilities after the threat model's output. It is essential to regularly perform **vulnerability assessments** to ensure that the entry points to the system are controlled.

- Perform **penetration testing** once in a while (this depends on the organization's insurance and regulation, but it should occur at least once a year) to simulate real cyberattacks and evaluate the overall security stance of the organization. Also known as **ethical hacking**, it is the most effective method of evaluating system security (it allows you to view security from the adversary's perspective). However, it is essential to plan for the correct penetration testing operations. For more information about the different types of penetration testing, as well as their advantages and disadvantages, please refer to the following link: `https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/`.
- Monitor network traffic to detect anomalies in traffic. Network monitoring tools, packet analyzers, and AI-based tools (for example, using machine learning for traffic pattern analysis) can be used for this purpose. The intelligence team can use a set of **Indicators of Compromise** (**IoCs**) to detect abnormal behavior in the network. IoC blocklists and threat hunting can be used to detect and block malicious traffic. We will discuss IoCs in *Chapter 13*, *Effective Threat Intelligence Metrics, Performance Indicators, and the Pyramid of Pain*.

In this section, we looked at the strategic manual method for threat modeling. In each step, the threat intelligence team needs to create a threat map to visualize the threat and attack flows of different assets (create attack trees for each potential asset threat). Documentation is vital in the threat modeling process. Therefore, the CTI team needs to keep an updated document of all assets and their decomposition, attack surfaces, probable threat vectors, and countermeasures. This document is owned by the CTI team but must be updated by the strategic, tactical, and technical security teams. In the next section, we will look at various threat modeling methodologies.

Threat modeling methodologies

Threat modeling methodologies are processes that are put in place by some expert security organizations to facilitate the threat modeling process. Although organizations can develop threat modeling methodologies, several existing methods are ready to be used. The methodology you choose depends on the threat to be modeled. Several methodologies are used for threat modeling, such as **STRIDE** (`https://bit.ly/3yKJzvP`), **DREAD**, **PASTA**, **TRIKE**, **VAST**, **OCTAVE**, and **CVSS** (**NIST**). In this section, we will look at the STRIDE and NIST methodologies and how they work.

> **Important Note**
>
> As an analyst, it is essential to know about the rest of the methodologies and how they can be applied to your threat modeling exercises. We are not going to cover all these methodologies in detail.

Damage, Reproducibility, Exploitability, Affected users, Discoverability (**DREAD**) is also a threat model methodology or risk assessment framework developed by Microsoft. The methodology uses the mentioned five components to analyze different threats that can affect the organization's resources quantitatively. The CTI analyst assigns values to each element, all of which can be used to prioritize mitigation plans.

Process for Attack Simulation and Threat Analysis (**PASTA**) looks at threat mitigation and countermeasures as a business problem. It adopts seven tactical steps process to counter threats effectively. The model helps threat intelligence analysts analyze attacks that exploit vulnerabilities and map those attacks to threat cases. PASTA goes beyond modeling applications and assets by focusing on business impact (such as revenue losses due to an attack, cost of system repair or restore, and so on). It correlates threat impacts and risks to the business. By using PASTA, the CTI team or analyst can focus on threats that directly impact an organization's operations and environments. The CTI analyst simulates these attacks to identify the exploits that can be used and implement countermeasures.

TRIKE is a threat model and risk assessment framework based mainly on the defensive aspect of threats and attacks. Compared to the other threat models, TRIKE does not focus on the attacker's behavior. It is entirely open source, and it can be installed as a desktop tool for threat modeling or used as a spreadsheet. Every asset or application component is assessed using the **create**, **read**, **update**, **delete** (**CRUD**) concept.

Visual, Agile, Simple Threat (**VAST**) looks at threat modeling in terms of the entire software development cycle. VAST is the core methodology of *ThreatModeler*, a commercial threat modeling tool. VAST uses three main pillars for threat modeling: automation, integration, and collaboration.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (**OCTAVE**) is a threat modeling and strategic risk assessment framework that leverages the knowledge of individuals in an organization to identify the state of security practice. OCTAVE takes an accountability approach where everyone is involved in security practices. The model identifies risks to critical assets and prioritizes improving critical asset areas first. OCTAVE is characterized by two aspects: *operational risk* and *security practices*. The model is built on three phases: asset-based threat profile construction, infrastructure vulnerability identification, and security strategy development.

Threat modeling with STRIDE

Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (**STRIDE**) is a threat modeling methodology used by Microsoft as part of the security development life cycle. It is the oldest threat modeling process. From the acronym, we can see that STRIDE applies threat modeling using a set of defined threat vectors. It allows us to integrate security in the early development stages. Hence, it is important to understand the assets and application requirements to ensure maximum protection against CIA triad violation. Let's describe STRIDE and its application:

- **Threat vector 1**: Spoofing.

  Description: Spoofing is a cyberattack in which an attacker tries to impersonate someone or something else. The objective is to pretend to be a legitimate entity and extract useful information such as credentials, IP addresses, plaintext traffic, or provide remote access.

  Violated component: AUTHENTICATION.

  Examples: Pretending to be an IT admin and pushing the target to install a DLL file on the computer to allow the attacker to control the victim's system remotely, or pretending to be the bank and pushing the user to enter the login credentials from a look-alike sender address.

  Operating mode: Spoofing can be applied at different levels, including files (changing file extensions or creating multiple files), processes (overtaking a legitimate process), networks (ARP, IP, DNS), and users (impersonating a user).

- **Threat vector 2**: Tampering.

  Description: Tampering is an attack that's used to modify system data. An attacker can modify data at rest (on disk or in memory) or in transit (as it moves through the network).

  Violated component: INTEGRITY.

  Examples: Automatically embedding malware in all the downloads in the network traffic or changing signal bits as they are being transmitted through the network.

  Operating mode: Tampering can be applied to files (redirecting to malicious files, modifying server configuration files), code (API modifications, memory data attack), or networks (modifying data moving in the network, redirecting traffic to a malicious destination).

- **Threat vector 3**: Repudiation.

  Description: Repudiation involves denying accountability for something that was done. It makes it challenging to link an action to the owner.

  Violated component: NON-REPUDIATION.

  Examples: Inserting code into the web application files and not claiming to have done it.

  Operating mode: Repudiation can be applied at different levels, including physical devices, applications, services, and users (use another person's credentials to conduct an activity and denying it because all the pieces of evidence point to the original credential owner).

- **Threat vector 4**: Information disclosure.

  Description: Information disclosure is an attack that's used to access information that someone is not supposed to access – unauthorized access.

  Violated component: CONFIDENTIALITY.

  Examples: Extracting personal information using SQL injection or accessing system username and password hashes using **XSS**.

  Operating mode: Information disclosure can happen by leveraging permission issues (misconfigured access control, server access permission), security (accessing hashes and cryptographic keys), and network traffic (eavesdropping network traffic).

- **Threat vector 5**: **Denial of Service** (**DoS**).

  Description: DoS is an attack that's used to interrupt or shut down system operations, so you're partially or fully denied access to network resources.

  Violated component: AVAILABILITY.

  Examples: Sending more request packets to the network that it can handle to disrupt traffic flow or creating too many processes to crash a server or device's memory.

  Operating mode: DoS can be applied to processes (crashing memory and disks), data repositories (databases, servers), and networks (bandwidth utilization consumption).

- **Threat vector 6**: Elevation of privilege.

  Description: Elevation of privilege is an attack that's used to increase permissions and access resources without authorization.

  Violated component: AUTHORIZATION.

Examples: Gaining *write* access to a credit accounts database or increasing access privileges by modifying configuration or server files.

Operating mode: Elevation of privilege leverages poor access control management.

The main problem is understanding how attackers can spoof, tamper with, repudiate, disclose, deny access to, or elevate privileges in any part of the system or assets (infrastructure, applications, supply chain, IoT services, and others). The security team can then implement countermeasures as the system is analyzed or applications are developed. You can insert all the components of STRIDE into the design process and document the flows, countermeasures, and mitigation steps for future assessment and references. STRIDE uses the approach shown in *Figure 6.1*.

Threat modeling with NIST

NIST defines a data-centric threat modeling approach rather than just following best security practices. The NIST approach considers each asset as a whole and deduces security needs based on individual cases. Using NIST, the CTI team focuses on the security stance of each asset instance, such as credit users' personal information stored in a database server inside a data center. The threat modeling of such a case would be different from the one of users' personal information stored in an IT admin's personal computer. The NIST threat model involves four steps: data and system identification and characterization, attack vector selection, security control characterization, and threat model analysis, as follows:

- **Identifying and characterizing the system and data of interest**: The CTI team identifies the system and the data that needs protection. Then, they determine how the system and the data are used in the organization. This includes identifying the following:

  The authorized location of the data of interest: The CTI team must identify the different places where the data resides (storage) within the organization. It must also know the transmission mechanisms (how data of interest moves from one place to another and how it is handled while being transmitted). The analyst must be aware of the data's execution environment (is the data executed in memory or on disk? What processors handle processing such data?). Another critical factor when assessing a data location is to know how data is inserted or written to the system and how it is taken out (through printing or a screen display).

The detailed movement and behavior of the data: The CTI team needs to track the data and how it is handled. It is essential to understand how and what the users use the data for? What are the processes that handle them? What is the technology that supports the data and the system? This allows the CTI team to know where the data is the most vulnerable during its movement. For example, point-of-sale devices have been seen to be susceptible when data is in memory.

The security objectives of the data: How does the CIA triad apply to the data? The CTI team must identify which components of the triad are a priority. For example, in terms of personal information, confidentiality may be the top priority when modeling threats. Even if the data is breached, how can we make it impossible for the adversary to access it?

The authorization to access the data: The CTI must include all the processes and users that have access to the data of interest and their permissions. Identifying and characterizing data and systems is the first step in identifying where data can be vulnerable. Let's look at an example:

Data of interest: Users' credit information.

Summary: Users' credit information is stored in the organization server but accessible through VPN by different business units (tellers, IT admins, data analysts, and so on).

System of interest components: *Users' laptops* (a teller who looks at credit balance on the *screen*, a data analyst who *downloads* a subset of users' data to perform some operations on the local machine, or a developer who updates the system application to write data to the server). *Printers* (the teller or the analyst can print the dataset for different purposes). The authorized locations include the storage for each individual with access. The information is transmitted over *LAN* or *WLAN*. Execution is performed on *server memory* for the teller and *local memory* for the analyst.

Security objectives: Confidentiality is a priority when complying with the POPII Act. However, all the elements of the CIA triad matter. The modeling is, however, based on ensuring the *confidentiality* of the users' credit information.

From this example, we can identify all the users who have access to the data and handles it. Tellers, data analysts, and application developers have access (maybe different and limited).

- **Identifying and selecting attack vectors for the data of interest**: The CTI analyst identifies the threat vectors that can be used to compromise the data of interest. The more attack vectors the CTI identifies, the better for step 3. However, the analyst must assess the likelihood of each threat vector to be used in the scope of the model. When we use the preceding example, step 2 is applied as follows:

  Location 1: Data stored on the local drive of the bank data analyst.

  The attacker forces access to the analyst PC and copies the dataset. He/she gains physical access to the PC and installs malware. The attacker steals the analyst's VPN credentials. He/she downloads sessions and cookies on the PC. The attacker uses social engineering to install malware (keyloggers, spyware, or any malicious software) on the analyst PC.

  Location 2: Data printed by the teller or the analyst.

  Attackers monitor and break into the wireless network and capture all data sent to the printer. An attacker shoulder-surfs the teller to view the information printed on the screen. The attacker breaks into the wireless network and performs a MITM attack.

  Selected potential vectors: Credential theft, session hijacking, implanting physical malware, wireless attacks, and spear phishing.

- **Characterizing the security controls for mitigation processes**: In this step, the CTI analyst identifies countermeasures and mitigation processes for each attack vector. Here, we assume that the organization has a security policy in place. The CTI needs to rank each measure taken to address the exploitation of each threat vector. This ranking depends on the organization. However, the high/medium/low approach works well. Step 3 for this example is as follows:

  Credential theft: *Strong password* using *strong encryption* techniques (effectiveness: low; implementation cost: low; management and control: low; impact on usability: low; impact on performance: low). *Multi-factor authentication* (effectiveness: high; implementation: medium; maintenance: medium; usability impact: medium; performance impact: low).

  Session hijacking: *End-to-end encryption* (effectiveness: high; implementation cost: low; management and control: low; usability impact: low; performance impact: low). *Random long session cookies* (effectiveness: high; implementation cost: low; management and control: low; usability impact: low; performance impact: low).

Malware implant: *Antivirus*, *IDSes*, *IPSes*, *firewalls* (effectiveness: high; implementation: high; maintenance and control: medium; usability impact: medium; performance impact: medium). *Patching vulnerabilities* (effectiveness: high; implementation cost: low; management and control: low; usability impact: medium; performance impact: medium).

Wireless attacks: *Strong encryption*, such as WPA-2 Enterprise and *strong passwords* (effectiveness: medium; implementation cost: low; management and control: low; usability impact: medium; performance impact: low).

Phishing: *User education* (effectiveness: high; implementation cost: low; management and control: low; usability impact: low; performance impact: low). *Phishing detectors* (effectiveness: high; implementation cost: medium; management and control: medium; usability impact: low; performance impact: low).

- **Analyzing the threat model**: In this step, the CTI analyst or team analyzes the results of the previous steps to assess the reliability of the implemented security protocols against their respective threat vectors. The analyst can assign a score to each measure to evaluate its contribution to the overall security stance. Countermeasures with high effectiveness can be given a set of values; the same goes for other countermeasures. In the end, the analyst calculates all the implications for each security control.

With that, we have seen that NIST can be used to model data-centric threats. The CTI team must document everything.

Threat modeling methodologies facilitate the process of analyzing risks to the organization's assets. The choice of methodologies depends solely on the organization, the assets or applications, and the business objectives. In the next section, we will look at how SIEM can be used for threat modeling.

Threat modeling use case

The objective of this use case is to provide a practical threat model approach to scenarios. We will use the Equifax data breach as an executive summary and the base of the modeling process.

Scenario: You are a CTI analyst in ABCompany, a credit record company that works with several partners, including banks, insurance companies, retail, and manufacturing. Your company also deals with credit disputes through an online web portal where users can log credit record issues with any organization. Due to the recent cyberattacks on the financial and insurance industries and the exposure of personal data in the sector, you have been tasked to research the 2017 Equifax data breach and extract valuable information for other security professionals operating in the design, passive defense, and active defense areas. You must also develop a threat model to identify the resources (and assets) that may be the targets, as well as identify possible TTPs that may be linked to threat actors.

Equifax data breach summary

In this section, we will summarize the data breach by providing an executive summary, state the kinds of threat vector(s) used, determine the timeline, map the attack to a threat intelligence framework, summarize the vulnerabilities, identify the consequences of the breach, and look at what was done to strengthen the system.

Executive summary: Between May and July 2017, Equifax, a major credit record company, reported a major data breach that saw nearly 150 million people's personal and financial information being stolen. The attacker leveraged a vulnerability on an unpatched Apache Struts framework (web server) in one of the database servers that's used for online disputes. The attack went undetected for over 2 months.

Threat vectors: Unpatched vulnerabilities, poor or non-existing encryption, and misconfiguration (SQL code execution and easy system pivoting).

Timeline: The Equifax attack timeline is as follows:

1. The attacker ran a vulnerability scanner in March 2017 and discovered a known vulnerability in the web server software, Apache Struts, running on the online portal.
2. The attacker created an exploit, used several techniques to cloak it from Equifax systems, and executed SQL queries on the database (around 9,000 queries).
3. The attacker exfiltrated personal and financial data.
4. The attacker located additional servers, accessed unencrypted login credentials, and issued additional system commands to query and exfiltrate more PIIs from other databases.
5. The attacker went 2 months undetected and exfiltrated data during that period (May 13, 2017 to July 29, 2017).
6. On July 29, 2017, Equifax officially announced the attack. The organization determined the extent of the breach on September 7, 2017.

Now, let's look at the different techniques used by the attacker (adversary) to fulfill their needs.

Identified TTPs: The attacker performed *active reconnaissance by scanning the web* for vulnerabilities. As a result, they identified an internet-facing server housing the online portal dispute, running software with the *CVE2017-5638 vulnerability*. The attacker gained access and could execute commands. The attacker used *existing encrypted communication channels* to blend their activities with regular traffic, achieved *persistence*, and *avoided detection*. The attacker finally *escalated privileges* and *ran system commands* on other databases. You can map this attack to the MITRE ATT&CK framework, as shown in the following diagram:

Reconnaissance	Initial Access	Persistence	Privilege Escalation	Defense Evasion	Collection	Command and Control	Exfiltration
Active Scanning (2)	Exploit Public-Facing Application	Valid Accounts (4)	Valid Accounts (4)	Indicator Removal on Host (6)	Data from Information Repositories (2)	Ingress Tool Transfer	Exfiltration Over Alternative Protocol (3)
	Valid Accounts (4)			Valid Accounts (4)		Proxy (4)	

Figure 6.8 – Mapping the Equifax data breach to the MITRE ATT&CK framework

The preceding diagram only shows the tactics found in the report. Use the tactics and techniques described in the breach report and link them to the MITRE TTPs.

Vulnerability and security gaps: You need to think about and identify the gaps in Equifax security, which is essential in modeling your organization. We can identify four possible security gaps (based on the report, you can identify more). We have the following:

- **Inefficient software patching management**: The vulnerability was known before the attack, and a patch was released, but the organization failed to apply it. The monitoring system failed to inspect encrypted traffic because the SSL certificate expired 10 months prior.
- **Privileged Access Management problem**: Lack of restrictions in resource accesses as the attacker could extend the attacks to 58 more databases.
- **Event monitoring gap**: Equifax had event monitoring systems and logs. However, external system scanning did not alert the security team, which could have helped stop the attack at the first stage of the Cyber Kill Chain.
- **Personal data storage issue**: Equifax had personal data stored in plain text.

This list is not exhaustive. Read the report to identify any relevant information that can help strengthen your organization. Some of the prevention measures are shown here:

Prevention and countermeasures: Following the data breach, Equifax took some actions to strengthen the system. Some of these actions included the following:

- A new management process to identify and patch software and applications.
- New policies for data and application protection.
- New tools with advanced features to continuously monitor network traffic.
- Communication monitoring, which was performed on the external boundaries of the organization.
- Traffic restrictions between internal servers and implementing new security control frameworks.
- New endpoint security tools were implemented to detect misconfigurations.
- A risk awareness program was implemented and shared with the board, with the CISO directly reporting to the CEO.

In this first step, you have summarized the data breach, and you can share the main point with the strategic team and the rest of the group. For more information on the Equifax data breach, please refer to `https://www.gao.gov/products/gao-18-559` and `https://bit.ly/3tkE5XC`.

Threat modeling for ABCompany

Threat modeling is not straightforward. Depending on the organization and industry, some of the components might be different. The objective is to show you how to approach such a case. We will use the logic shown in *Figure 6.1* and the STRIDE mapping. Let's get started:

- **Assets and decomposition**: The assets that belong to the threat model include the *employees' PII* (not internet facing), the *users' PII* (internet-facing with session protection), *credit information* (internet-facing with session protection), *dispute and policy documents* (not internet facing), and *web portal* (SSL, session protected, and the login form). The adversaries could target all the assets.

  Note that you can identify more based on your organization.

- **Adversary analysis**: We can identify potential adversaries based on the Equifax report and the MITRE ATT&CK tactics spotted. Credit card information and PII data can be targeted by *financially motivated actors* (black hat hackers, organized crime, and malicious insiders). *Hacktivists* and *cyber-terrorists* can target web portals and public-facing applications. Dispute and policy documents are sensitive and can be targeted by industrial spies (espionage).
- **Threat identification**: Based on the Equifax breach, we can highlight *unpatched vulnerabilities*, *misconfigurations*, *weak and no encryption*, *unprotected credentials*, and *system lateral movement*. However, based on the types of adversaries ABCompany may face, we can add *phishing*, *malware*, *ransomware*, and *zero-day threats*.
- **Attack surfaces**: ABCompany has two data centers with *physical servers* running Linux. *Employees* have *laptops* that can be used to access the ABCompany's network via *VPN*. Web traffic is proxied using a *proxy server*. Network traffic is encrypted using *SSL certificates*. Customers can also use their *endpoint devices* to log into the customer portal. *Partners* (banks, insurance companies, and so on) can access users' credit information through a secured public network. Use *Figure 6.4* to draw the threat vector to the attack map.
- **Countermeasures identification**: Refer to the *Identifying countermeasures* section to document the countermeasures of all possible threat vectors.

Use this information to draw a simple threat modeling map, as shown in the following diagram:

ABCompany				
Employees PII	**Customers PII**	**Customers credit information**	**Dispute and policy documents**	**Web application (portal)**
Not public-facing Must be encrypted *(must be protected at rest and in transit)*	Public-facing Session protection *(must be protected at rest and in transit)*		Not public-facing Must be protected at rest as well in transit	public facing Login form Session protection *(constant monitoring of activities)*
- Poor or non-existent encryption - Tempering - Spoofing (impersonatte) - Repudiation (hide trace) - Information disclosure			- Ransomware - Tempering - Document theft - Lateral movement	- Brute force - Weak credentials - Poor configuration - Cross-site scripting - Denial of Service - Elevation of Priviledge - unpatched vulnerability
Black hat hackers Organized crime Malicious insider			Industrial Espionage Organized crime	Hacktivists Cyber-terrorists Script kiddies

Figure 6.9 – Simplified ABCompany threat model

Here, we can see the various STRIDE components. Threat modeling can be resource-intensive for large organizations. It is important to automate the process to ensure that all the assets, vectors, and surfaces are profiled reliably. This is why we must have a SIEM system, as described in the next section.

Advanced threat modeling with SIEM

Security Information and Event Management (**SIEM**) is a platform, tool, product, or system that allows security professionals to aggregate multiple data sources, search through security and network events, and produce analytics and reports to support business decisions. SIEM completes threat intelligence platforms by converting raw data into a human-readable and interpretable form. SIEM performs the following tasks:

- **Data collection**: SIEM collects security events in the network. This can be system logs, network device logs, endpoint device logs, application logs, or any other security documentation that can be analyzed.

- **Data normalization**: SIEM processes the data through a reliable mediation layer to have all the collected data in a format that the system can use. By normalizing the data, SIEM manages security by monitoring network *flows* and *events*. It leverages advanced analytics to consolidate data collected from multiple diverse sources and pinpoints events (security incidents) in the network.
- **Data correlation**: To identify security threats, SIEM correlates raw data using analytics methods to find information patterns in the collected data. Correlation is an important task of SIEM as it reveals relationships between data from the same or different sources using rules or statistical methods.
- **Real-time analysis**: SIEM minimizes the time required to detect security events, identifies their sources, and reports for actions. All the network flows and events are processed in real time to facilitate the rapid identification of security threats.
- **Reporting**: Most SIEM systems have a reporting and dashboard module to allow security analysts to view network threats, alarms, events, and the flow of interest in an organized manner.

Because SIEM can perform real-time data analytics on network events and flows, this gives it the upper hand in automated threat modeling. The advantage of using SIEM for threat modeling includes *accurately identifying assets* (because SIEM data logs come from all network points), *real-time threat identification*, and *quick responses*. SIEM reporting and alarming systems can also be used for quickly alerting us to the presence of threats. Some of the advantages of using SIEM for threat modeling include the following:

- **Advanced analytics**: Automatically identify abnormal behavior in the system, indicating the need for investigation and potential threat presence. SIEM correlates with other data sources to also recognize the probable source and types of threats.
- **Complete modeling automation**: When using SIEM, data and all other necessary information is inserted initially. For fully automated SIEM, data collection and feeding are automated through the use of APIs. Hence, less manual work needs to be done and scalability is improved.
- **Integrated forensics analytics**: Since all the data sits in the same place, SIEM lets you collect system events and flows that can be used to investigate threats and attacks. SIEM provides enough evidence to support threat and attack cases.
- **Automated threat and incidence response**: Once a threat or the vulnerability of an asset has been discovered, SIEM automatically creates a set of alarms to get the security team's attention to take action. Advanced SIEM provides references to mitigate and countermeasure known threats.

- **Threat hunting**: Leveraging threat intelligence data, SIEM allows you to identify new threats that could affect the organization. When SIEM is coupled with machine learning capabilities and user behavior analytics, threat modeling is enriched with new threat data patterns. Although outside the scope of this book, threat hunting is essential in SIEM-based modeling because it gives analysts the upper hand on adversaries by streamlining threat detection.

Examples of SIEM tools include *IBM QRadar*, *AT&T AlienVault Unified Security Management*, *Splunk Enterprise Security*, and *SolarWinds Security Event Manager*. While most of these tools are commercial, some are open source SIEMs such as *OSSEC*, the *Open Source HIDS Security System*, *Splunk Community Edition*, *Apache Metron*, and *Elastic Search*. More details on SIEM will be provided in *Chapter 12*, *SIEM Solutions and Intelligence-Driven SOCs*. In the next section, we will look at user behavior logic from the attacker and the organization members' perspectives.

User behavior logic

Analytics and logic have become an integral part of security for many years now. Most analytics, however, is done on the network traffic side, where packets are analyzed by firewalls, IDSes, IPSes, and antivirus software. However, users are the biggest concern in security because single security malpractice is enough to jeopardize the entire system's security. User behavior logic or **user behavior analytics** (**UBA**) focuses on *internal threat modeling* by analyzing what users do regularly: network activities, applications they launch, the files and databases they access, and download patterns.

Using UBA, you can search for and identify abnormal and unusual behavior in the system and report it to the relevant stakeholder in the form of alarms and indicators. UBA analyzes all traffic independently of its origin. Therefore, UBA can model internal threats and, if integrated with SIEM, automatically provide references and countermeasures.

Benefits of UBA

UBA is proving to be essential in IT infrastructure security because it fills the current threat modeling and security methods gap. The security system can easily flag an attacker's failed attempts to log into an organization portal as a potential threat or attack. Let's look at the failed attempts from inside the organization or from a legitimate user. The security system logs the activity but does not flag it because of the trusted origin. This is the reason why a hacker that gains access to a system might stay hidden for a long time before being detected (he/she does everything in the system as a legitimate user). Organizations use *perimeter-based* security to protect the inside from the outside of the system. However, with the latest trends in breaches, attackers have shown that they can access the perimeter and camouflage themselves as ordinary insiders. UBA software provides the following benefits:

- **Automatic detection of internal and external threats**: UBA consolidates data coming from endpoints, networks, the cloud, applications, intelligence, user access, emails, and any other internal source to analyze behaviors, isolate unusual activities (from users' perspectives), and provide complete visibility of events and flows. An attacker who gains access to the system as a legitimate user will be flagged when trying to access resources that he/she has never accessed before. A sudden change in users and system behavior is enough to set off security alarms. UBA identifies threats that go around the security perimeter.
- **User focus rather than event focus**: While most security systems track devices and network events, UBA explicitly dives into human (user) behavior patterns, performs advanced analytics, and detects anomalies in the behavior (potential threats indicators). With other security tools such as SIEM and TIP, UBA provides complete visibility into system threats and attacks.
- **Opex saving**: Because UBA is an automated system, the amount of manual input is minimized. UBA can reduce the number of intelligence or security analysts. However, it does not replace legacy security systems. Instead, it is used to complement the existing infrastructure to improve the organization's security. The strategic team can benefit from UBA by playing with the budget.

By integrating UBA into the CTI project, organizations can move beyond the traditional process of monitoring traffic, enhancing the system's ability to identify abnormal system behavior quickly.

UBA selection guide – how it works

UBA works in two ways: using *defined rules* and using *dynamic analytics models*. A rule-based UBA system allows security and threat intelligence analysts to define formulas and logic that force the system to report behaviors that violate those rules and logic. A typical example of a rule-based UBA is an analyst who creates a rule around sensitive files, such as the following simple logic:

```
If sensitive file access:
   If user is not at work:
      raise a flag  //potential malicious activity
   else if user not admin before:
      raise flag //possible elevation of privilege
   else:
      log the activity
      do not flag   //potential legitimate user
```

Whenever a user accesses a sensitive file, the UBA checks if the user is accessing the file during working hours. If not, it flags this behavior and notifies the relevant stakeholders. If the user accessing the file is not an administrator, the UBA flags the behavior (which could be a potential privilege escalation). Otherwise, the system assumes that it is a legitimate user. Rule-based UBA requires the analyst to have *enough expertise* in the domain and good knowledge of *adversaries operating TTPs*. This is important to facilitate the creation of practical rules.

Dynamic model-based UBA leverages dynamic statistics and machine learning to classify or categorize user behaviors. It automatically analysis users' activities to detect all activities that fall within the suspicious category. The following diagram shows the UBA engine analyzing internal and external traffic to classify whether the behavior is a threat:

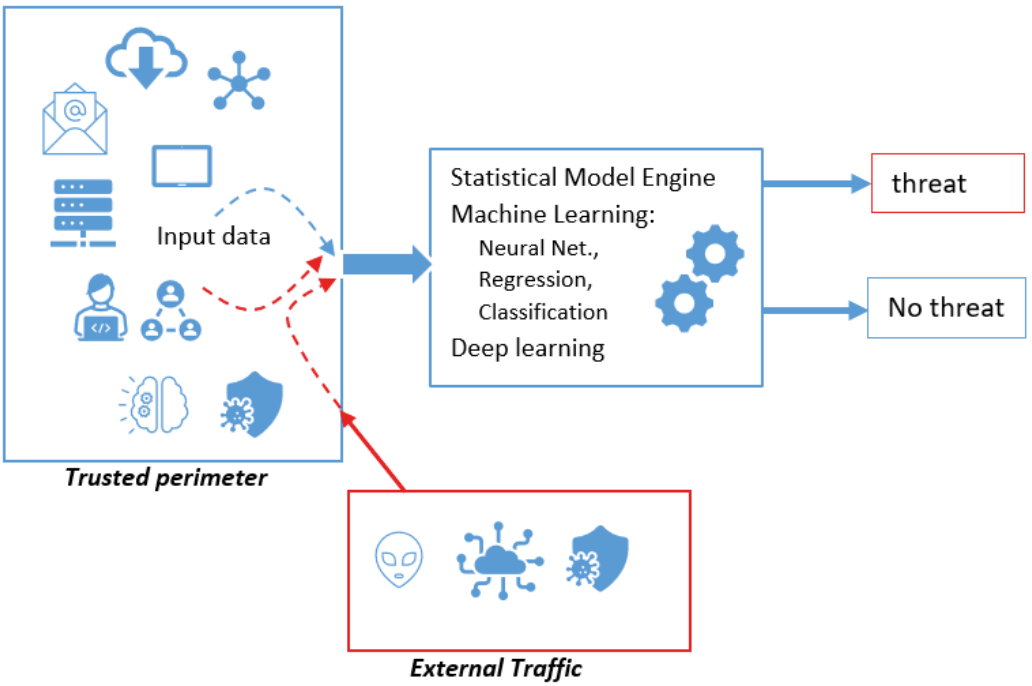

Figure 6.10 – Simplified UBA model

UBA can be deployed as a standalone tool or integrated into SIEM tools. Regardless of the deployment method, there are certain important features that an organization must look at when acquiring a UBA solution:

- **Big data support**: A UBA tool or piece of software must support big data as security data comes in various voluminous formats and at different speeds. Most SIEM systems support big data as well.
- **Multiple data sources support**: Although UBA focuses on user behavior, it must also support events and flows to enhance the analytics processes. It must be able to input historical user activities and all the metadata such as access times, permissions, IP addresses, and email data (recipients and senders, objects, signatures, and embedded links).

- **Real-time notification**: It must support the ability to report potential threats in real time to allow analysts to take action. It is recommended to have reference engines when making decisions in case of threats.

UBA is an important tool for threat modeling, security monitoring, and attack detection. It enlarges the security protection scope of organizations. Depending on the budget, UBA can add costs to the operational security budget. However, its benefits are not to be ignored. In the next section, we will analyze how adversaries work and what organizations can do to secure the system.

Adversary analysis techniques

Cyberattack frameworks are important in analyzing the techniques used by adversaries to compromise IT infrastructures. One of the CTI project objectives is to build an effective threat and attack strategy. However, to build such a strategy, the intelligence analyst must understand the fundamental methods used by attackers. We will look at the IBM Xforce framework model approach as an example (`https://ibm.co/3xGsYdw`). The model provides comprehensive attack knowledge to minimize risk exposure and protect against cyberattacks.

A cyberattack happens in phases that may or may not be sequential, depending on the type of attack, the adversary, and the target system. An adversary attack is divided into two main operations: *attack preparation* and *attack execution*.

Adversary attack preparation

During the preparation phase, the adversary identifies the target, sets the objectives, and launches the initial attack to check if the attack is successful or not. If the attack is successful, the adversary moves to the execution operation. If not, they revise the attack plan, change their techniques, and relaunch the attack. The typical tasks that are performed during the preparation phase include the following:

- **Determining the attack objective(s)**: This is the main requirement of the attack. The adversary might want to steal sensitive data or implement ransomware to make money. This is the beginning of the attack plan's implementation.

- **Conduct effective reconnaissance**: Cyber attackers are known to be patient. Adversaries are likely to research the organization to identify potential access points. The search scope includes, but is not limited to, employees and their roles, customers, vendors, online-facing assets, possible portals, and past data breach history. For example, an adversary who finds an organization's IT manager's email addresses on social platforms such as LinkedIn can use this as a potential attack surface. During the reconnaissance phase, the attacker tries to get the system footprint.
- **Prepare Tactics, Techniques, and Procedures** (**TTPs**): Based on the information collected during the reconnaissance step, adversaries identify the TTPs that are likely to succeed against the target system. An adversary who obtains the IT manager's email address can construct a reliable phishing attack. If online-facing network devices were identified, the adversary could use known vulnerabilities to compromise the internet gateway or perform a brute-force attack. During this step, the attack determines the malware and techniques that can be used to access and expand the access once they're in the target system. All the attack vectors are at the disposition of the attacker at this stage.
- **Prepare the attack infrastructure**: After selecting the appropriate TTPs, the adversary avails the tools (software, applications, and technologies) to conduct the attack. The adversary may construct a **command and control** (**C2**) channel to communicate with the victim. He/she may also use obfuscation techniques to avoid tracing the attack. Hence, some resources that could be availed include a domain (the attacker may buy or use free online domains), servers and proxies (acquire or use free online servers), mail services (purchase or use online free web services), SSL certificates (buy or use free online certificates), and VPN services (purchase or use free VPN services). For phishing attacks, the adversary may mirror legitimate resources (the organization's website, employees, or portals).
- **Prepare the malware and software kit**: Once the tools and resources have been availed, the adversary prepares the malware and software toolkit. He/she chooses which tools will be used to create the malware, the programming language, and how to communicate with the infected system. The adversary either develops the malware to use, reuses an existing one, or outsources the services from skilled hackers. An adversary can also acquire known vulnerabilities or zero-day exploits to conduct the attack. In most cases, attacks are simulated and tested before they are executed in the target system. The attacker tests the behavior of the attack in a local test lab in the presence of firewalls, antiviruses, and other security devices. The goal is to ensure that the attack works as expected.

- **Ensure operational security**: The adversary does not want to be discovered and identified. Hence, he/she uses every possible method to hide any information that can expose them. At this stage, the attacker ensures that every attack trace exposing critical information (IP addresses, domain owner, web service used, and so on) is hidden, obfuscated, or unavailable from public repositories. The adversary is likely to have a contingency plan in case the attack is exposed.
- **Review the feedback cycle**: This is a continuous process. The adversary reviews the preparation steps and ensures that the data that's gathered is used adequately. He/she reviews each step and adjusts the attack plan, should there be any change or update information in the attack preparation cycle. This task is performed at each stage of the attack to ensure its success.
- **Launch the attack**: The adversary is now ready to launch the attack against the target organization or individual. The attack is launched directly or indirectly. A direct attack involves instantaneous contact with the target system, such as using SQL injection on the web application, using stolen credentials on the portal, physically accessing the target system's Wi-Fi network, or sending a phishing email to an employee connected to the target network.
- **Indirect attack**. The indirect attack includes infecting an employee's laptop and waiting to connect to the target network to gain access. An adversary can also mirror the organization's online application and lure the employees to go to the malicious site. The method of attack depends on the adversary landscape of the target organization.
- **Determine the attack outcome**: The adversary evaluates whether the attack has been successful or not. If a complete or partial failure occurs, the adversary is likely to revise the attack plan and reconstruct the preparation phase. Adversaries are patient; hence, they are likely to adjust the plan until it succeeds. In the case of complete success, the adversary moves to the next phase of the attack: *execution*.

This subsection has detailed the steps taken by adversaries to prepare and initiate cyberattacks against organizations and individuals. Cyber attackers are resilient in their operations, and so should the organizations to ensure that the system is not compromised at any point. In the next section, we will provide some defensive tips that an organization can use to detect and protect against an adversary preparation phase.

Attack preparation countermeasures

Attack preparation is not easy to countermeasure until the few last steps (launching the attack). However, organizations and individuals can put some best practices in place to ensure system security.

The CTI team needs to build a *good threat profile* for possible adversaries that can target the organization. Threat intelligence frameworks such as the MITRE ATT&CK framework can be used to identify potential adversary groups that pose threats to the organization. The team must determine if the selected groups have ever targeted the organization or another organization of the same portfolio. It must highlight the possible goals of the adversaries in their interest in the organization. The following are some countermeasures you can perform to prepare for the adversary attack:

- **Protect the most critical assets**: This comes back to asset identification and prioritization. The CTI team must have a list of critical assets and the measures taken to protect them. They must also identify the gap in the current critical asset safeguarding measures and recommend reliable methods such as limiting access, encrypting PII at rest or in transit, and protecting the asset when in employees' local machines.
- **Limit the amount of public information**: The more information an organization puts online, the more data the adversaries have to prepare the attack and identify potential attack surfaces. Internet gateway information, email addresses, domain registration details, and third-party vendors are information that can give an adversary the necessary knowledge to initiate an attack project. Hence, not exposing such information challenges the adversary's preparation.
- **Educate employees and individuals**: In most cyberattacks, human factors are involved. Attacks such as phishing and ransomware still heavily depend on human actions. It is essential to educate employees so that they can identify malicious activities (phishing emails, malicious links, mirrored web applications, and so on). Domains such as `tesla.com` and `teslaa.com` are not the same; `microsoft.com` and `mikrosoft.com` are different as well.
- **Install phishing detection software**: It is essential to have phishing detectors or typo-changed domain detectors (specifically related to the organization's private domain). This measure can prevent domain crafting.

Several best practices can help minimize or make the adversary's life difficult. *The pyramid of pain* can be used as a reference to detect adversaries' activities. It also shows you how painful it gets for an adversary each time the security team denies a pyramid's level of access. The organization must mature the security infrastructure to take advantage of threat intelligence to protect the system effectively. In the following subsection, we will look at the second phase of the attack framework: the execution phase.

Adversary attack execution

This step assumes that the phase step was successful. The adversary takes a series of steps to establish a foothold in the system and reach the objectives. The execution phase can be done automatically or event-based, depending on the techniques used by the adversary. When automatic execution is used, the malware spreads in the system without the attacker's boost and quickly infects the system. In event-based execution, the malware relies on network or user events to extend into the system. Adversaries perform the following steps to ensure that their objectives are met.

Initial compromise and foothold establishment

In this step, the adversary has access to one or more hosts in the system or has been able to get access to the network. Suppose that the attacker has logged into the system as a trusted user. He/she can target individuals of higher privileges in the organization as emails and messages come from the trusted perimeter. Spear phishing is used for such purposes. The attacker ensures that access and control of the hacked host are maintained. At this stage, the adversary can install backdoors on the compromised host to facilitate remote access and control through the C2 channel that was prepared in the first phase.

The adversary ensures that outbound communication is appropriately and securely established for bi-directional communication between the victim and the attacker's server. C2 channels are mostly encrypted, and the adversary's end server information is obfuscated to hide the attacks. Backdoor and account access are two main tactics used by attackers to establish a foothold.

Access expansion

After establishing the foothold, the adversary attempts to gain more insight and expand their foothold in the victim's system. The steps to expand access includes **privilege escalation**, **lateral movement**, **internal reconnaissance**, and **access persistence**, as follows:

- **Privilege escalation**: The attacker attempts to access more resources, even when he/she does not have the intended permission. The attacker can use credential dumping or pass the hash techniques to bypass authentication and gain access to root-level resources.
- **Lateral movement**: The adversary attempts to access other networks, hosts, and repositories in the victim's system. Pivoting is one of the methods that's used to access other corporate networks. However, methods such as **PsExec** and **net** use commands that can give access to other organizational resources. The adversary leverages new and existing techniques to move through the system.
- **Internal reconnaissance**: This is an essential step for the adversary to work toward the objectives and maybe exfiltrate more than planned. The adversaries attempt to gather more information on the victim from an internal view. They can leverage the operating system's commands or use scanners (such as **Nmap**) to enumerate the system.
- **Access persistence**: This is done if the adversary wants to maintain access for future attacks. He/she ensures that the foothold is persistent, even after a system restart or cleaning. Most adversaries use backdoors and web shells (for remote web server control) to maintain persistence in the victim's system.

The execution phase of the adversary operation is dangerous as he/she has access to the system. The detailed steps are not sequential, which means that an adversary can simultaneously conduct privilege escalation and persistence. At this stage, the victim organization can only rely on advanced monitoring methods to detect the attack. This is because adversaries are likely to evade all sorts of defense systems once they're inside. In the next subsection, we will look at some common mitigations techniques for attack execution.

Attack execution mitigation procedures

Once an attack has been successfully conducted, the objective of the security team is to minimize the impact of the attack until the threat is completely removed. It takes time for an organization to detect cyber attacks when the system has been compromised already. That is a fact: most research shows that the average time to detect an attack that has occurred is more than 30 days. Let's look at some of the security best practices that can minimize attack factors:

- **Restrict installation processes in the system**: Adversaries might want to install backdoors or other malware to expand the foothold of the victim. By restricting the installation of software in the system, the privilege to install malware is limited or nullified unless the attacker has higher privilege access.
- **Implement effective access control**: Use the concept of *least privilege*. Do not give more permissions than is required. This measure limits the level of access that an adversary may have and limits their ability to move around the system. Implement and enforce *strong password policies* with the use of **Multi-Factor Authentication** (**MFA**), frequently changing passwords, and prohibiting password sharing.
- **Constantly monitor network traffic**: The CTI team can recommend using SIEM, TIPs, legacy monitoring tools, and UBAs to monitor network traffic effectively and identify anomalies in the network or user traffic patterns. This countermeasure includes monitoring both ingress and egress traffic to prevent outbound communication that the C2 channel can set.
- **Implement a strong system log management**: In well-designed IT infrastructures, all activities are recorded in the form of logs. Attackers are known for compromising system logs (clear, delete, and destroy). Therefore, the organization must restrict access to log files to ensure that malicious and legitimate users do not tamper with them.
- **Monitor system processes**: Hiding malware in legitimate processes is one of the methods used by adversaries to evade defense systems. The security team needs to monitor system processes and report changes in process behaviors.
- **Implement effective patch management**: The security team must ensure that all system software, applications, and services are frequently patched. This countermeasure removes the possibility of exploitation due to unpatched or vulnerable applications in the system. It is essential to automate the patch management process.

- **Establish adequate endpoint protection and management and invest in threat-hunting**: This helps you stay ahead of adversaries in the cyberwar arena. Use encryption when necessary (especially for sensitive assets and data). When strong encryption is used, exfiltrated data can be useless if the attacker does not have the means to decrypt the data.

All these measures are containment measures that are used to defend the system and enhance its security stance in the presence of a breach. Nevertheless, the organization still needs to have reliable **incident response** (**IR**) and *forensics* teams to eradicate the threat and collect pieces of evidence to trace the attack to its source. The CTI team and the internal security team must work together to protect and prepare the system in case of attacks.

Summary

Threat modeling is a vital topic in terms of building intelligence. Understanding the attack surfaces, the threat vectors, and the adversaries (and their motives) facilitates a good security stance. This chapter has covered threat modeling by focusing on the different methods that a CTI team can adopt to build a reliable threat profile. The common denominator for all threat modeling approaches includes knowing the assets, the vectors, and the surfaces as they are points of interest to attackers. The result of threat modeling is used to select data sources that should be used for the intelligence program.

At this point, you should be able to perform threat and adversary modeling. You should also be able to select the appropriate method for a modeling task or customize the approach based on your organization's requirements.

In the next chapter, we will look at threat intelligence data sources.