Threat Modelling

Information Security Branch
Office of the Chief Information Officer

Welcome to the BC Provincial Government's training course on:

Threat Modelling

Here are a few tips to allow you to make the most of your learning experience:

Course navigation is through the arrow keys on your keyboard or using your mouse to click the icons at the bottom of the screen. This course is accessible as a spoken word option. During the course, the Menu above will provide the option of moving around the course. The Transcript provides the spoken word text for reading.

If you are unsure of the terms used in this course, you can look using the Glossary which is linked at the top of the window and can be accessed throughout the course.

Learning Objectives

This training course is just one part of the Office of the Chief Information Officer (OCIO) Information Security Branch (ISB) education series.

The goal of this course is to inform staff of what threat modelling is, why it is important, and how it fits into the Security Threat Risk Assessment, and Statement of Acceptable Risk, processes.

Although this course assumes some knowledge of information technology and security, it covers these topics at a high level for non-specialist audience as well.

If further help is needed understanding, accessing or completing this course, please email:

VulnerabilityandRiskManagement@gov.bc.ca

First Nations Acknowledgment and Respect

This course was created by those working within the communities of southern Vancouver Island and the south Gulf Islands that are located in the traditional territories of the Lkwungen (Esquimalt and Songhees), Malahat, Pacheedaht, Scia'new, T'Sou-ke and W̱SÁNEĆ (Pauquachin, Tsartlip, Tsawout, Tseycum) peoples.

We acknowledge and respect our traditional hosts.

Jennifer Adomeit

BC Provincial Government Information Security Branch

Information management and technology play a crucial role in government service delivery. As such, the BC Provincial Government takes an approach that balances the protection of sensitive information with the need to share that information across government programs, the broader public sector, and to residents.

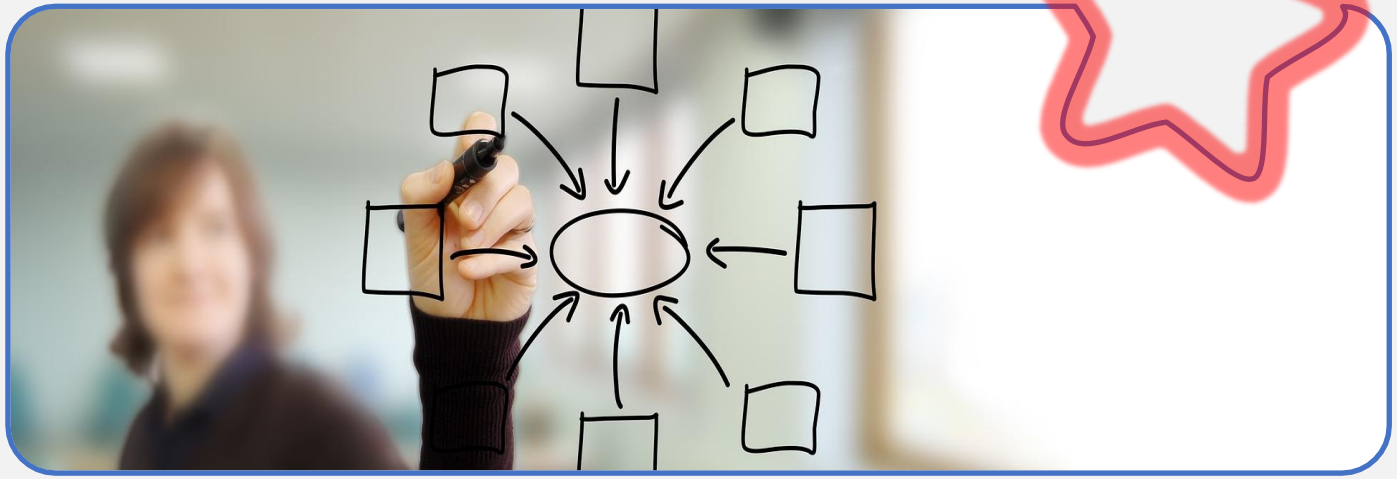
Through the Information Security program, the Province promotes a risk-based approach to information security and ensures programs, plans and processes are in place that appropriately manage the risks to the confidentiality, integrity and availability of Government information.

The BC Provincial Government has subject matter experts (SME) supporting information security awareness, vulnerability and risk management, advisory services, security operations, and investigations and forensics.

For more information on the ISB you can visit our website at: http://www.gov.bc.ca/informationsecurity

Course Sections

1. What is Threat Modelling
2. How Threat Modelling helps information security
3. Threat Modelling basics
4. Threat Modelling Frameworks
5. Provincial Government OCIO and Threat Modelling
6. Common Mistakes When Threat Modelling
7. Acme Docs Threat Model Example
8. Completing Your Threat Model
9. Course Goal



What is Threat Modelling

"Threat modelling is the use of abstractions to aid in thinking about risks."

Adam Shostack, from 'Threat Modeling: Designing for Security'

Threat modelling is in all of our lives, something that we incorporate in our day-to-day living without even realising. For example, a child determining the best way to school whilst avoiding walking across busy roads; that is threat modelling.

Information security threat modelling is a structured approach and process to analysing security of something within information security's remit; a network, software, hardware and so on. The process starts with the identification of all the possible entry points and follows with the enumeration and prioritisation of the associated potential threats.

The goal is to mitigate these threats and prevent any future attacks.

Threat Model Conceptual Overview

Threat modelling is a process for optimising information security by identifying objectives and vulnerabilities and then defining countermeasures to those risks. A threat is a potential or actual adverse event that may be malicious (such as a man in the middle attack) or incidental (such as the failure of a storage device), or accidental (such as software misconfiguration), and that can compromise the data of the BC Government.

The goal of threat modelling is to understand where the most effort should be applied in order to keep a system secure; identifying threats to a system and understanding what it is we want to protect from those threats. By threat modelling applications, we can better protect data while educating and building a culture of security throughout the BC Government.

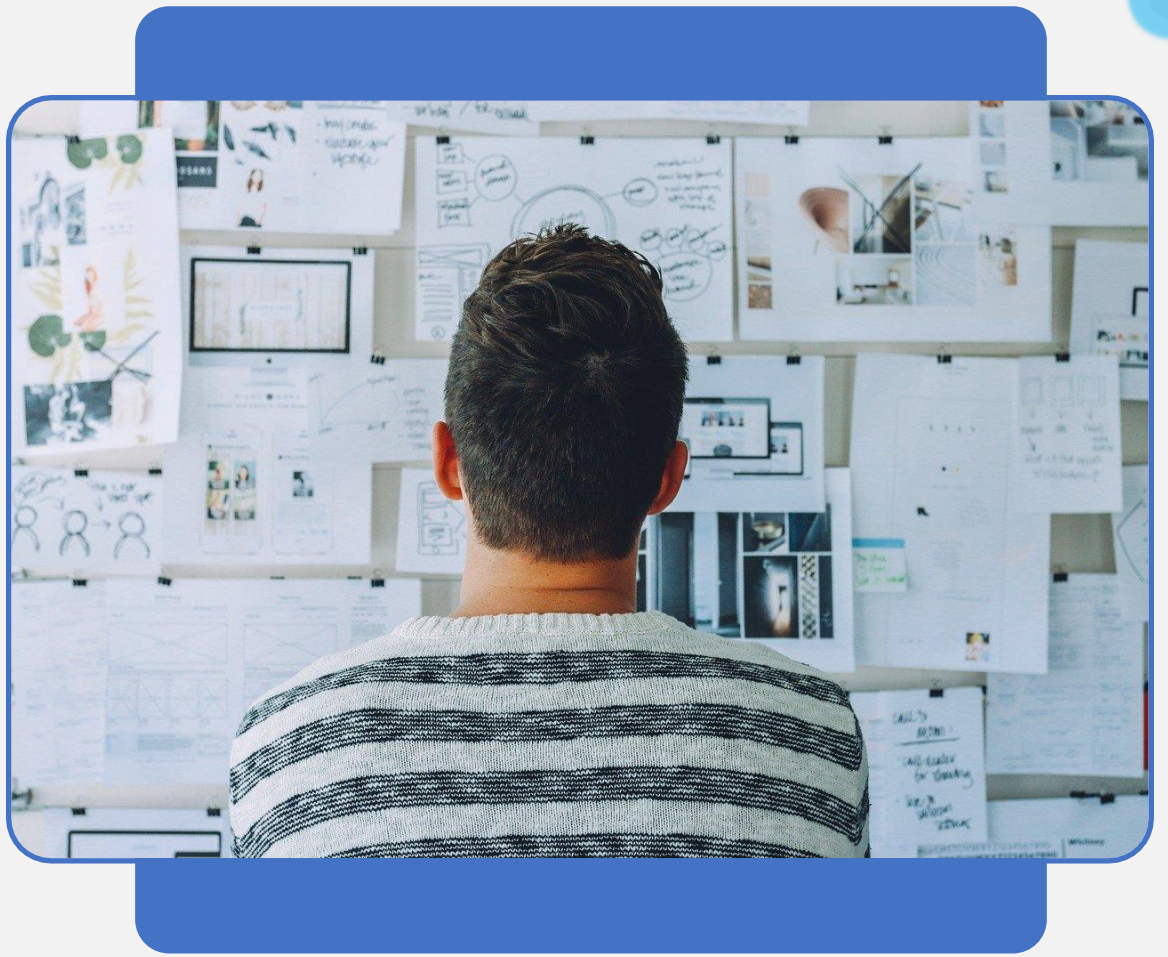
Threat Model Conceptual Overview

When you are threat modelling, you bring the security specialist, architect, the operations or infrastructure team and lead developers together with the business area. The living process which is known as threat model includes inputs from the whole team. Threat modeling fosters a culture of communication and collaboration, it helps the team members build an understanding of each other's roles, business objectives and pain points.

Threat modelling is not a single process, or even a single document necessarily; it is a collection of activities that make up the creation of a 'threat model'. Because there are many activities, multiple frameworks have been developed that help to organise threat modeling. These models also make sure that nothing is missed and that best practice is followed.

Once a threat model framework is understood you can either follow that framework, create your own, or pull from different frameworks to address the issues you are facing. Threat modelling is very flexible and can apply to different types of activities, from information security, aviation, hardware design, road layouts to street lighting.

Threat modelling is an open framework of related activities, which the more you put into, the more value you get out of.



How Threat Modelling helps with information security

Understanding and managing threats is a central concern for every organisation, including the BC Government. Risks can take different forms and originate from either inside or outside the organisation. Information security is amongst one of the concerns that drive strategy at large organisations, including the risk of non-compliance, data breaches, infrastructure outages, legal and financial penalties and more.

Information security regulations are stricter now than ever before. They are heavily focused on risk management and putting controls in place to prevent potential threats. The General Data Protection Regulation (GDPR), for example, was approved by the European parliament to strengthen data protection regulations, and here in British Columbia we have the *Freedom of Information and Protection of Privacy Act* (FOIPPA) that legislates how privacy data is handled.

This is where threat modelling comes into play as it addresses all the underlying sub-threats and root causes of higher-level threats. The process of threat modelling breaks down a system's architecture. It identifies key structural elements and system assets in order to highlight risks and potential associated attacks against the system, and allows for educated mitigation or acceptance of those risks.

Threat modelling, when combined with risk management, can help provide answers to the question of who will attack your systems, and how or where the attack will originate from.

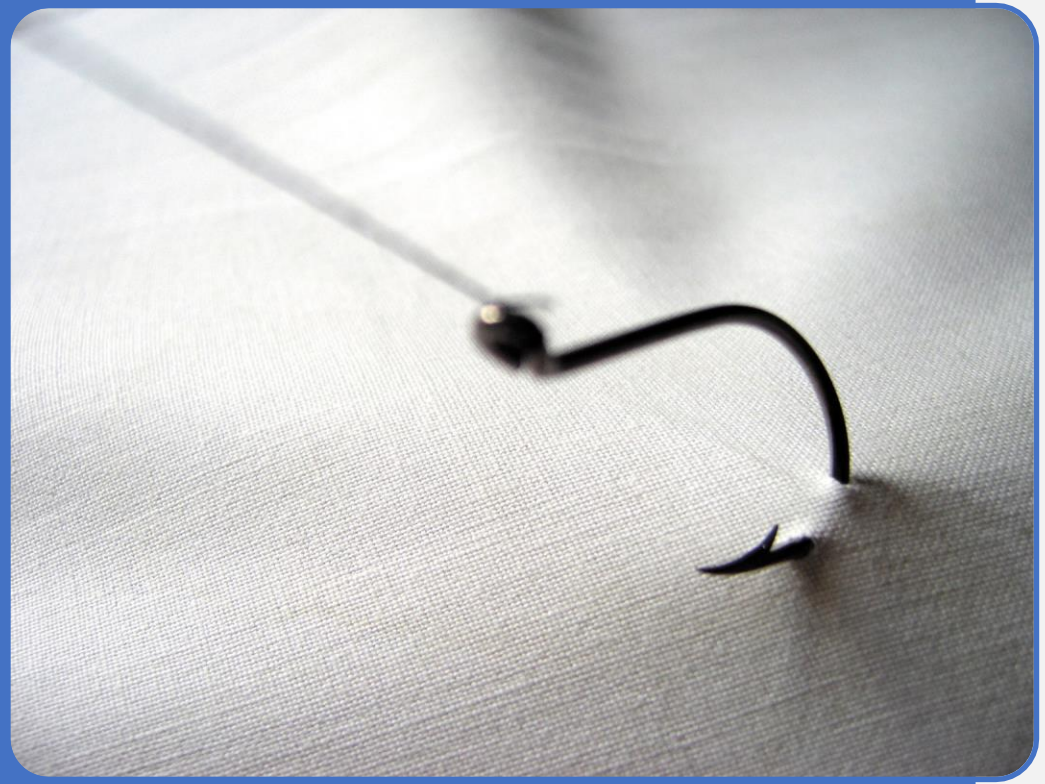
It provides valuable insights on the IT risks facing organisations, and can then help outline necessary measures and sufficient controls to stop the threat before it impacts them.

Common Threats Addressed by Threat Modelling

Cybersecurity threats are abundant and ever-changing. That's why threat modelling, diagramming various threats and impacts, is a critical and necessary practice to prepare for whatever threats come your way. Threat modelling, like SWOT analysis, helps companies build a well-rounded, continuously evolving threat defense scheme. When planned and implemented properly, cybersecurity threat models will ensure that each nook and cranny of your networks and applications remains protected now and as new threats emerge.

There is sometimes confusion around the definition of *threat*, which can be defined in one of two ways:

1. **A potential event that will have an unwelcome consequence.**
2. **An individual, organisation, or system from which an attack can originate.**



DDoS attacks

DDoS (distributed denial of service) attacks are a method of bombarding websites and web applications with enormous traffic requests that overload the servers they are hosted on. These attacks are powered by thousands of bots and are indistinguishable from legitimate users attempting to access the site.

Companies can model their defense and response plans to prevent this from happening. Businesses can use DDoS protection software, load balancing software and network monitoring software to improve their ability to discover DDoS attacks early, balance workloads properly and restrict traffic access by malicious visitors.

Phishing

Phishing is a method of obtaining user information through fraudulent communications targeted directly at people. It's often accomplished through emails disguised as coming from a legitimate source, but delivers the target's information back to the hacker's actual source.

Phishing can enable hackers to gain access to sensitive information or privileged applications. Businesses can prevent this through the use of email security software for filtering and identification, along with security awareness training to ensure employees can identify fraudulent communications.

Malware

Malicious software is a category of cybersecurity threats that includes threats such as computer **viruses, spyware and adware**. It's one of the most common threats to target both businesses and individuals.

Companies can use threat modeling to ensure that their firewalls are adequately prepared, that zero-day vulnerabilities are minimised and that new exploits or malware signatures are documented. Proper planning, along with antivirus and other security software, will ensure networks are not compromised by malware.

Pharming

Its objective is to convince you to visit a malicious and illegitimate website by redirecting the legitimate URL. You may then give your personal information to this malicious person.

Ransomware

Ransomware went became well known due to *Wannacry* and *Petya* and its variants. The malicious program restricts the access to your system and files, often through encryption. Then they demand payment for regaining access to your data.

Threat Modelling Basics

The Four Step Threat Model

A threat model helps to drive the vulnerability mitigation process and is one of the best methods of improving system security. It will determine the attack surface for the application or system and allow for more accurate assigning of risk to various threats.

Threat modelling, at its most simple, breaks down into a four-step process:

1. **What are we deploying or building?**
2. **What can go wrong?**
3. **What are you going to do about it?**
4. **Review the work done at steps 1-3 and repeat as necessary.**

The Four-Step Threat Model:

1

What are we deploying or building?

This is an information gathering and understanding step. You need to define the scope of the Threat Model. To do that, you need to understand the application or system that you are building, examples of helpful techniques are:

- Architecture diagrams
- Dataflow transitions
- Data classifications

You will also need to gather people from different roles with sufficient technical and risk awareness to provide information for the framework to be used during the threat modelling exercise.

2

What can go wrong?

This is a **research** activity in which you want to find the main threats that apply to your application or system. There are many ways to approach the question, including brainstorming or using a structure to help think it through. Structures that can help include Microsoft STRIDE, Kill Chains, Common Attack Pattern Enumeration and Classification (CAPEC) and others. Shortly, this course will discuss options for modelling frameworks.

3 **What are we going to do about that?**

In this phase you turn your findings into specific actions. Examples of this are:

- Take the issue out of threat modelling and consider what needs to happen next, weighting the risk vs value for the issue and the attention it receives as part of threat prioritisation.
- Allow whoever creates priorities during threat modelling to contextualise the risk, then decide on what should be immediately prioritised, what should be put aside, and what research is necessary for further focus later on.

Threats that impact life and limb would be the highest priority, followed by those that impact the functioning or ability of the business. Other priorities are likely to be business area specific.

4 **Review the work done at Steps 1-3 and repeat as necessary**

Finally, carry out a retrospective activity over the work you have done to check quality, feasibility, progress, and or planning. If any issues still exist that need to be addressed in the threat model then return to step one and repeat.

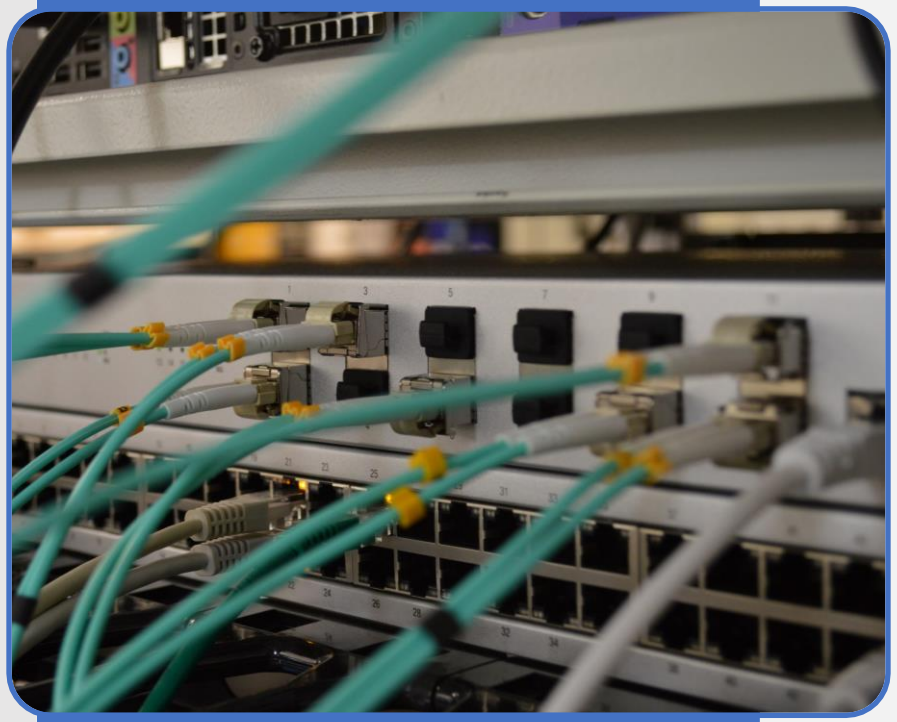
Common Components of Threat Modelling

These are a few components of threat modeling that can improve security:

Secure design

This is necessary during the application development phase to ensure the identification and prevention of vulnerabilities. Code analysis and security testing during all stages of development can help to ensure bugs, flaws, and other vulnerabilities are minimised.

Companies can analyse their code for known flaws during development or dynamically as an application runs and perform penetration tests after development. The resulting data is used to plan for future attack mitigation and to implement updates related to new threats.



Threat intelligence

It is important to keep an up-to-date database of threats and vulnerabilities to ensure applications, endpoints and networks are prepared to defend against emerging threats. These databases may comprise of public information, reside in proprietary threat intelligence software, or be built in-house.

Asset identification

Assets need to be properly documented at all times. Without proper tracking and documentation, these assets may possess known flaws that are not be identified. New assets, even potentially dangerous third-party assets, may access networks without the security team’s knowledge.

Mitigation capabilities

These refer to a security team's ability to detect and resolve attacks as they emerge. This may mean the identification of malicious traffic and removal of malware, or it could refer to contacting your managed security services provider. Either way, mitigation is essential to effective planning so that teams are aware of their ability to combat threats with their existing resources.

Risk assessment

After the application code is determined to be safe and endpoints are properly implemented, companies can assess the overall risk of their various IT components. Components may be scored and ranked or identified as *at risk*. Either way, they will be identified and secured in order of importance.

Threat intelligence

It is important to keep an up-to-date database of threats and vulnerabilities to ensure applications, endpoints and networks are prepared to defend against emerging threats. These databases may comprise of public information, reside in proprietary threat intelligence software, or be built in-house.

Asset identification

Assets need to be properly documented at all times. Without proper tracking and documentation, these assets may possess known flaws that are not be identified. New assets, even potentially dangerous third-party assets, may access networks without the security team’s knowledge.

Threat Modelling Frameworks

Threat Modelling Frameworks

A threat modelling practice flows from a methodology or **framework**. There are many threat modelling frameworks available for use. Some of these are specialised models designed for a specific task, for example, some focus specifically on risk or on privacy concerns. They can be optionally combined to create a more robust and well-rounded view of potential threats.

Threat modelling should be performed early in the development cycle because if potential issues arise, they can be caught early and remedied. This can prevent a much costlier fix down the line.

Using threat modelling to think about security requirements can lead to proactive architectural decisions that help reduce threats right from the start.

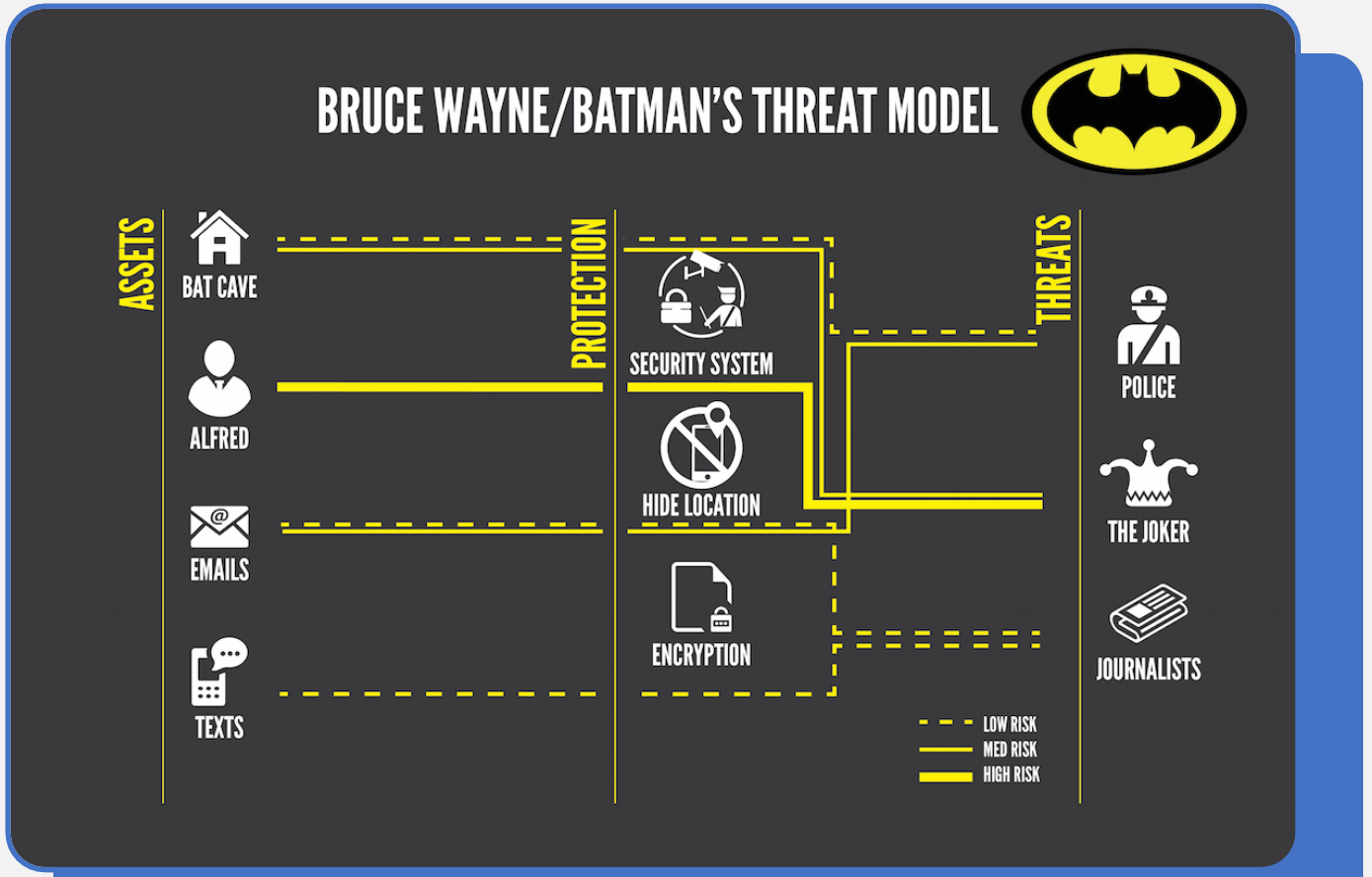


Image from Tiffany Liu, MIT

Threat modelling frameworks are tools that help us provide a means to understand threat, they do not solve threat directly or take into account security policy or the Provincial Government's risk appetite. Information security policy serves as a tool to provide *guidance* on how to manage and secure all business operations, including critical assets, infrastructure and people in the organisation.

This guidance (e.g. usage and controls) facilitates the provisions for threat assessment and compliance based on local context. The lack of effective threat assessment frameworks at local context have promoted the exposure of critical assets such as database servers, email servers, web servers and user smart-devices at the hand of attackers and thus increase risks and probability to compromise the assets.

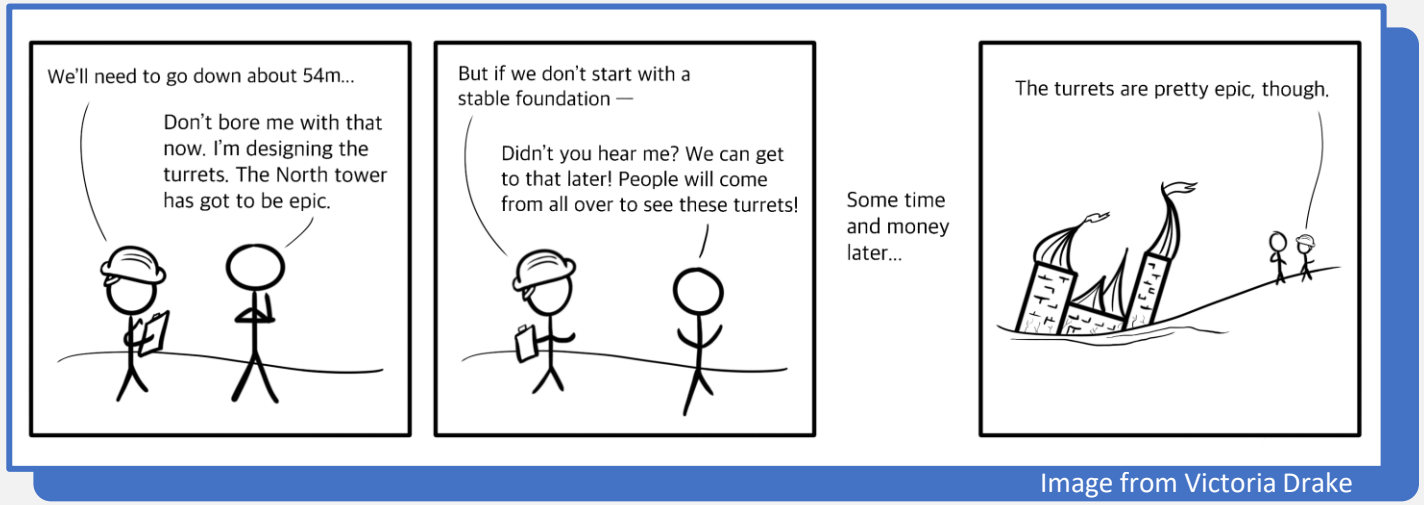


Image from Victoria Drake

Common Threat Modelling Frameworks

Threat Models

There are a large number of threat models in existence, each Government or company could theoretically use a model tailored to their specific needs, and branches within those could use different models again. The most *beneficial* threat model is one that suites your needs.

At the end of this section are links to a number of threat modelling tools.

1

Microsoft STRIDE Threat Modelling Tool (Developer Focused):

STRIDE is an initialism that stands for **S**poofing **T**ampering **R**epudiation **I**nformation Message **D**isclosure Denial of Service and **E**levation of Privilege. The STRIDE threat modelling goal is to get an application to meet the security properties of Confidentiality, Integrity, and Availability (CIA), along with Authorisation, Authentication, and Non-Repudiation. Once the security subject matter experts construct the data flow diagram-based threat model, subject matter experts check the application against the STRIDE threat model classification scheme.

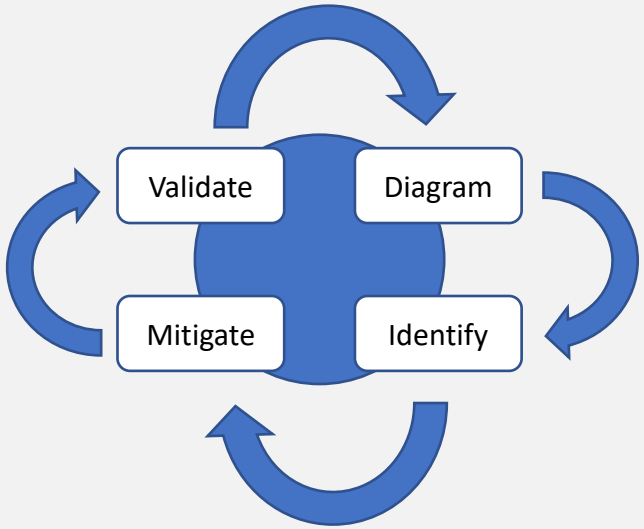
The free Microsoft threat modelling tool allows for easier threat modelling by using a standard notation for visualising system components, data flows, and security boundaries. It also helps threat modelers identify classes of threats they should consider based on the structure of their software design. The tool is designed with non-security experts in mind, making threat modelling easier for all developers by providing clear guidance on creating and analysing threat models. It should be noted that STRIDE and the threat model tool is no longer developed by Microsoft but is still available.

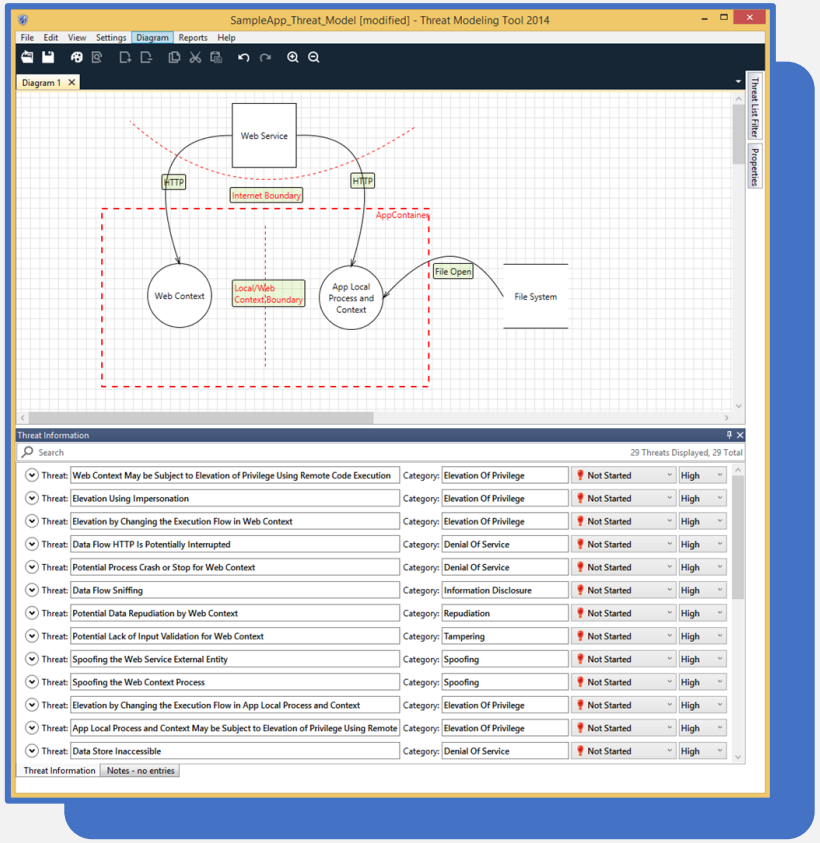
https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Microsoft STRIDE diagrams

The STRIDE approach involves creating a diagram, identifying threats, mitigating them and validating each mitigation.

Below is a diagram that highlights this process:





Here are the high level Microsoft STRIDE processes in a step by step diagram:

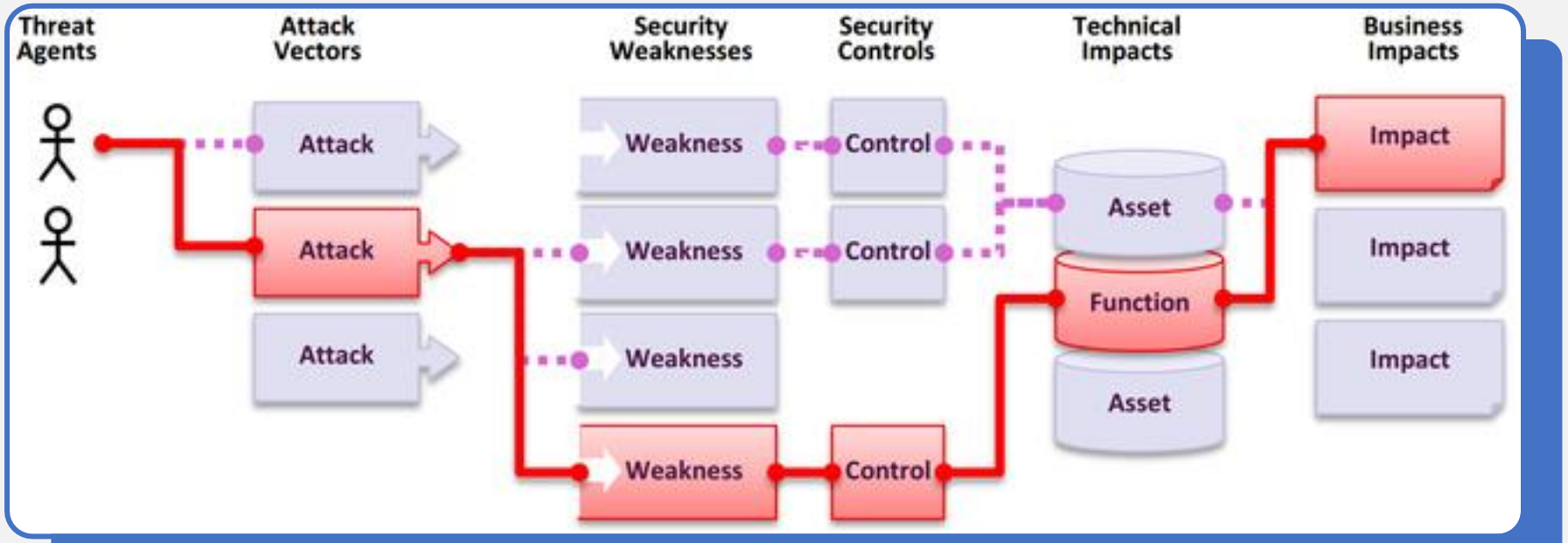
- Identify assets
- Create an architecture view
- Decompose the application
- Identify the threats
- Document the threats
- Rate the threats

2

OWASP Application Threat modelling (Software Focused):

The Open Web Application Security Project® (OWASP) is a non-profit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

https://owasp.org/, https://owasp.org/www-community/Application_Threat_Modeling



The OWASP threat model, image from OWASP

3 OCTAVE (Practice Focused):

The **O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation methodology was one of the first created specifically for information security threat modelling. Developed at Carnegie Mellon University's Software Engineering Institute (SEI) in collaboration with CERT, OCTAVE threat modelling methodology is heavy-weighted and focused on assessing organisational (non-technical) risks that may result from breached data assets.

Using this threat modelling methodology, an organisation's information assets are identified and the datasets they contain receive attributes based on the data stored. The intent is to eliminate confusion about the scope of a threat model and reduce excessive documentation for assets that are poorly defined or are outside the purview of the project.

OCTAVE threat modelling provides a robust, asset-centric view, and organisational risk awareness, but the documentation can become voluminous. OCTAVE is most useful when creating a risk-aware corporate culture. The method is highly customisable to an organisation's specific security objectives and risk environment.

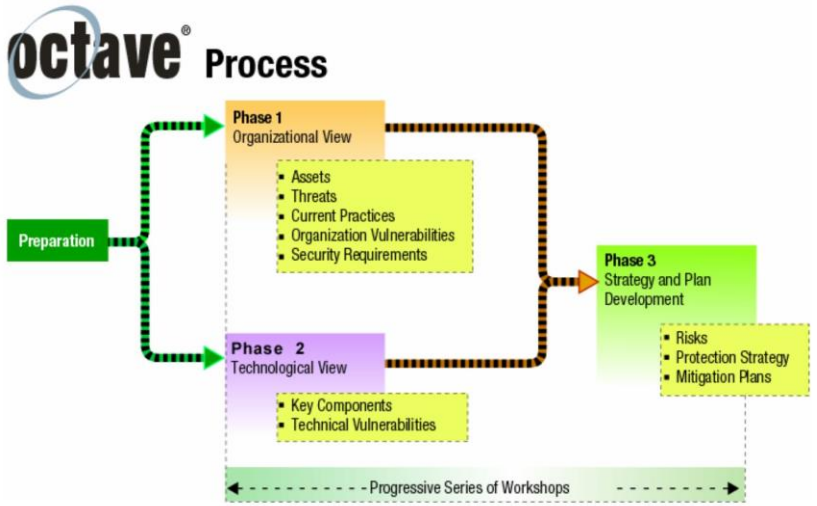


Diagram of the Octave process, image from Octave

https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html

4 Trike Threat modelling (Acceptable Risk Focused)

Trike is a free and open source threat modelling methodology. The project began in 2006 as an attempt to improve the efficiency and effectiveness of existing threat modelling methodologies, and is still being actively used and developed. Trike also contains threat modelling tools: http://www.octotrike.org/tools.

Trike threat modelling is a unique threat modelling process focused on satisfying the security auditing process from an information risk management perspective. It provides a risk-based approach with unique implementation, and risk modelling process. The foundation of the Trike threat modelling methodology is a *requirements model*. The requirements model ensures the assigned level of risk for each asset is acceptable to the various stakeholders.

With the requirements model in place, the next step in Trike threat modelling is to create a data flow diagram (DFD). A DFD maps out the flow of information for any process or system. Trust boundaries were added in the early 2000s to adopt data flow diagrams to threat modelling.

In the Trike threat modelling methodology, DFDs are used to illustrate data flow in an implementation model and the actions users can perform in within a system state. The implementation model is then analysed to produce a Trike threat model. As threats are enumerated, appropriate risk values are assigned to them from which the user then creates attack graphs. Users then assign mitigating controls as required to address prioritised threats and the associated risks. Finally, users develop a risk model from the completed threat model based on assets, roles, actions and threat exposure.

http://www.octotrike.org/

5

P.A.S.T.A. Threat modelling (Attacker Focused)

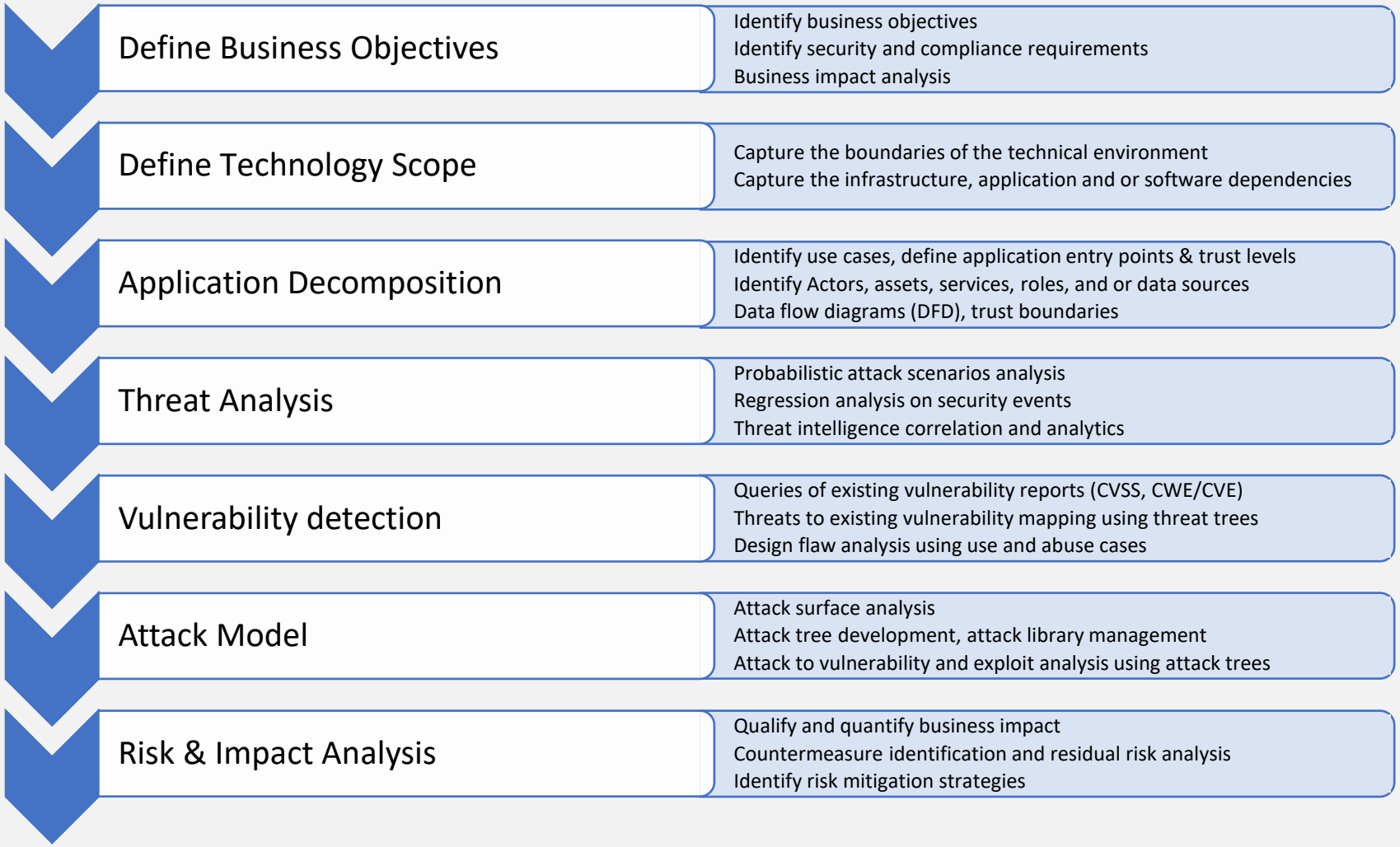
The Process for Attack Simulation and Threat Analysis (PASTA) is a relatively new application threat modelling methodology. PASTA threat modelling provides a seven-step process for risk analysis, which is platform insensitive. The goal of the PASTA methodology is to align business objectives with technical requirements while taking into account business impact analysis and compliance requirements. The output provides threat management, enumeration, and scoring.

PASTA is a risk-centric methodology aligns business objectives with technical requirements to provide organisations asset-centric mitigation strategy. PASTA allows security experts to understand the attacker's perspective on applications and infrastructure better, and then develop threat management, enumeration, and scoring processes. The risk and business impact analysis aspect of PASTA threat modelling can elevate into a strategic business exercise for key decision makers rather than just a software development practice for IT teams.

The PASTA methodology combines an attacker-centric perspective on potential threats with risk and impact analysis. The outputs are asset-centric. Also, the risk and business impact analysis of the method elevates threat modelling from a "software development only" exercise to a strategic business exercise by involving key decision makers. PASTA works best for organisations that wish to align threat modelling with strategic objectives because it incorporates business impact analysis as an integral part of the process and expands cybersecurity responsibilities beyond the IT department. This alignment can sometimes be a weakness of the PASTA threat modelling methodologies. Depending on the technological literacy of key stakeholders throughout the organisation, adopting the PASTA methodology can require many additional hours of training and education.

From **Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis,** Tony UcedaVelez, Marco M. Morana

Process diagram for Attack Simulation & Threat Analysis Methodology (PASTA)



6 VAST Threat modelling (Enterprise Focused)

The Visual, Agile, and Simple Threat modelling (VAST) scales across the infrastructure and includes DevOps. VAST can integrate seamlessly into an agile environment and provide actionable, accurate, and consistent outputs for developers, security teams, and senior executives alike. VAST is based on the commercial threat modelling platform, ThreatModeler, which relies heavily on automation, VAST aims to be highly scalable and usable and relies on integration and collaboration.

Application threat models for development teams are created with process flow diagrams (PFD). Process flow diagrams map the features and communications of an application in much the same way as developers and architects think about the application during an SDLC design session.

Operational threat models are designed for the infrastructure teams. Though more similar to traditional DFDs than application threat models, the data flow information is presented from an attacker – not a data packet – perspective. By relying on PFDs rather than DFDs, VAST threat models do not require extensive systems expertise.

Uniquely addressing both developer and infrastructure team concerns allows organisations to incorporate threat modelling as a part of their DevOps lifecycle with different outputs for various key stakeholders.

The most significant difference of the VAST threat modelling methodology, however, is its ability to allow organisations to scale across thousands of threat models. The pillars of a scalable threat modelling practice – automation, integration, and collaboration – are foundational to VAST threat modelling. As the organisation matures and new threats arise, these pillars help to develop a sustainable self-service threat modelling practice driven by the DevOps teams rather than the security team.

VAST requires two types of models to be created: threat models for applications and operational threat models. Former use process flow diagrams that represent the architectural point of view, while the latter focuses on attackers' point of view based on the diagrams.

https://threatmodeler.com/threat-modeling-methodologies-vast/

Threat Modelling Tools

These are selection of a few of the software tools available to help threat modeling. No tool recommendation is made as each has strengths and weaknesses that depend on what the tool is being used to assess. It is better to understand a little about each tool and then choose what will work best for your situation:

IriusRisk

Offers both a community and a commercial version of the tool. This tool focuses on the creation and maintenance of a live Threat Model for the entire software development life cycle (SDLC).

PyTM

An open-source Pythonic framework for threat modeling. It encodes threat information in python code and processes that code into a variety of forms.

SecuriCAD

Conducts automated attack simulations to current and future IT architectures, identifies and quantifies risks holistically, including structural vulnerabilities, and provides decision support based on the findings. securiCAD is offered in both commercial and community editions.

ThreatModeler

It is an Amazon web services (AWS) software as a service (SaaS) that allows users to create their system diagrams using a library of known components, identify software used, make connections, and insert mitigation components and processes. This tool is kept up-to-date with Common Vulnerabilities and Exposures (CVEs) for many hardware and software products that could cause compromise if not updated, or mitigations put in place. This is a paid service.

SD Elements

Security Compass is a software security requirements management platform that includes automated threat modeling capabilities. A set of threats is generated by completing a short questionnaire about the technical details and compliance drivers of the application. Countermeasures are included in the form of actionable tasks for developers that can be tracked and managed throughout the entire SDLC.

Tutamantic

"Automated Design Analysis" is an interesting tool which provides microservices for threat modeling. In contrast to integrated tools, users upload a Visio file, and receive a spreadsheet of threats.

OWASP Threat Dragon Project

A free, open source, online threat modeling web application including system diagramming and a rule engine to auto-generate threats/mitigations.

Mozilla SeaSponge

A free, open source, accessible threat modeling tool from Mozilla. (Last updated in 2015).

OVVL

The "Open Weakness and Vulnerability Modeller". A free, open source threat modelling tool based on STRIDE focusing particularly on providing support for the later stages of the secure development lifecycle.

OWASP Threat Dragon Project

Provincial Government OCIO and Threat Modelling

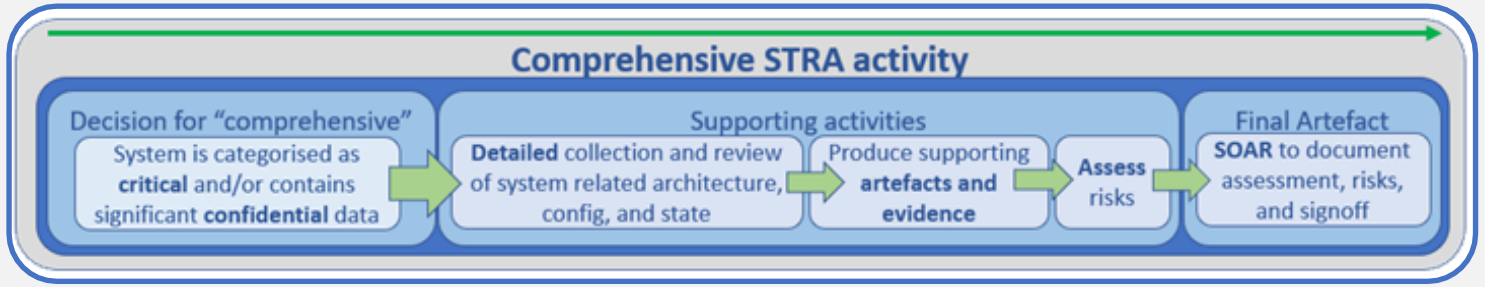
The BC Provincial Government OCIO and Threat Modelling: SOAR & STRA

What is a Security Threat and Risk Assessment (STRA)?

STRAs are an assessment used by the BC public service to assess digital risks. This is a key supporting enabler for responsible digital government. STRAs are a snap-shot in time and raise the awareness of system security risks in an organisation to the level at which risk-based decisions can occur effectively. STRAs are key to empowering management to make informed risk-based decisions about information assets that are directly or indirectly under their control as part of their responsibilities and accountabilities. An STRA also documents risk ratings and planned treatments, a threat model should be a part of that documentation.

STRAs are accomplished by identifying how likely threats are to act on vulnerabilities (weaknesses) and what the potential impacts could mean to the business. An STRA should be completed for each new system, or significant change to a system.

In the BC Government process, the risk assessment is broken down into STRA and SOAR (Statements of Acceptable Risk). The STRA is considered the more comprehensive assessment, as it has extra requirements above the SOAR, whilst also requiring the SOAR to be completed.

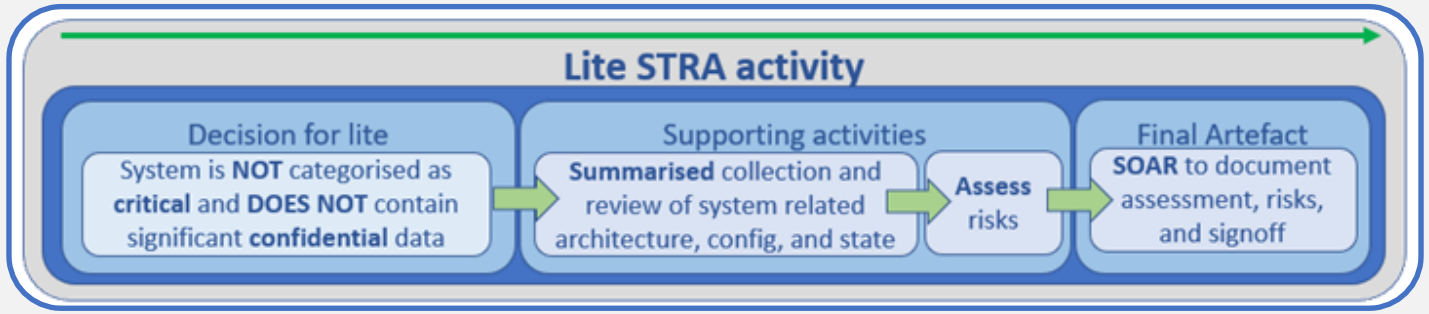


What are Statements of Acceptable Risk?

A SOAR is needed to complete the comprehensive STRA process and is the final document of that process. A comprehensive STRA with its additional detail, evidence, and artefacts, is not always required. A lite-STRA is much faster to work through it only requires the SOAR. Depending on the system to be assessed, the Primary Risk Evaluator will decide if a lite or comprehensive STRA is the right choice.

An STRA and SOAR are always needed when a system uses provincial government data with information technology. This is true even if provincial government data is transmitted, handled, or stored by a third party. *The Province of BC is still accountable for its data.*

Security risks need to be considered at every stage of a system's lifecycle. The Information Security Policy, Information Security Standard, and Security Threat and Risk Assessment Standard define specific triggers and situations for when an STRA should be conducted.



For further information on the STRA or SOAR process see the Information Security Branch website at:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-threat-and-risk-assessment

Why use a Threat Model with a SOAR or STRA

As a threat model is a process in which potential threats, such as a lack of safeguards, can be identified and mitigations can be prioritised.
The purpose of threat modeling is to provide a systematic analysis of what controls or defenses need to be included, given the type of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker. Threat modeling answers questions like:
Where am I most vulnerable to attack?
What are the most relevant threats?
What do I need to do to safeguard against these threats?
Undertaking a threat model will help inform what level of protection an information system will need; if the STRA-lite (SOAR only) process or the comprehensive STRA process is required for a particular project.

Common Mistakes When Threat Modelling

Threat Modelling: Common Mistakes

When threat modelling it is easy to fall into some common pitfalls. Here are a few of the mistakes that you can learn to avoid:

Structure comes first

Thinking like an attacker might seem like good advice at first, but it is role play. You are not an attacker, and you are making guesses at how they might think about getting into your systems. Although this is not the worst thing you can do as part of your threat modelling, cover the cybersecurity basics *before* you search your feelings.

Keep yourself grounded

Don't get too esoteric, you can do this by keeping your threats realistic. ET's will not corrupt your data with their advanced mind-UI controls. And if they could, what are you going to do about it? No, wrapping a server in tin-foil is not a solution.

Focus on the risks that are both **real** and **manageable**.

Concentrate on the threats
Now that our threats are realistic and servers are tin-foil free, threats are where our focus should be. Although it is important to look at your data flow and control flow and know what vulnerabilities might exist, you need to look at threats more explicitly. Identify the opportunities an attacker might have to thwart your controls to affect the confidentiality, integrity, availability, productivity, and the proprietary nature of your data. Threats are not the end though, understanding a threat is just one step towards resolving a threat and that is the end goal.

Apply policy and guidelines
Everything done in threat modelling must follow BC Government policy and guidelines, when applicable.

Team diversity matters

Gather a diverse team and include the stakeholders and customer voices, if applicable. Information security people are important but don't exclude other people, you need to understand what you are doing makes sense. It's not a puzzle to solve but a solution to build; for that you need many viewpoints, not just one.

Do include old systems

Many breaches happen through not including old systems, the overall cost of a government breach is in millions of dollars.

My threat model is complete or never complete enough

This is a two-edged sword. Never assume that the threat modelling team can imagine every potential threat, and don't hold off deployment of a new system because there is a miniscule amount of risk either. So when the boss asks if the threat model is complete? Give them a realistic risk assessment and tell them that when the risk profile changes, there's a plan to update the threat models. Let others have input into the threat model so you don't get lost in the weeds.

You need not be an expert in threat modelling to use threat models

Think of threat models like muscle memory, you get better with practice. It doesn't have to be perfect as long as guidance and policy requirements are met.

Starting threat modelling early

Understanding threats and resolving them will be most beneficial before launch, when threats can be fixed without downtime and taking undue risks. The earlier in the process, the better.

Think about the long game, not just the threat of the day

Do not rush after the latest threats or pay too much attention to specific threat actors when building threat models. It is possible that ransomware and crypto-mining software might present the biggest current threats to your security. Rather than modelling specifically against these threats, focus instead on controls for mitigating any threat to the confidentiality, integrity and availability of your systems. Your focus should be on building repeatable processes so every time something changes you are prepared for it. The key is having a standard process or methodology that is done the same way each way time, regardless of the newness of a threat. You need to know what it is you are trying to protect and begin from there.

Acme Docs: A Threat Model Example

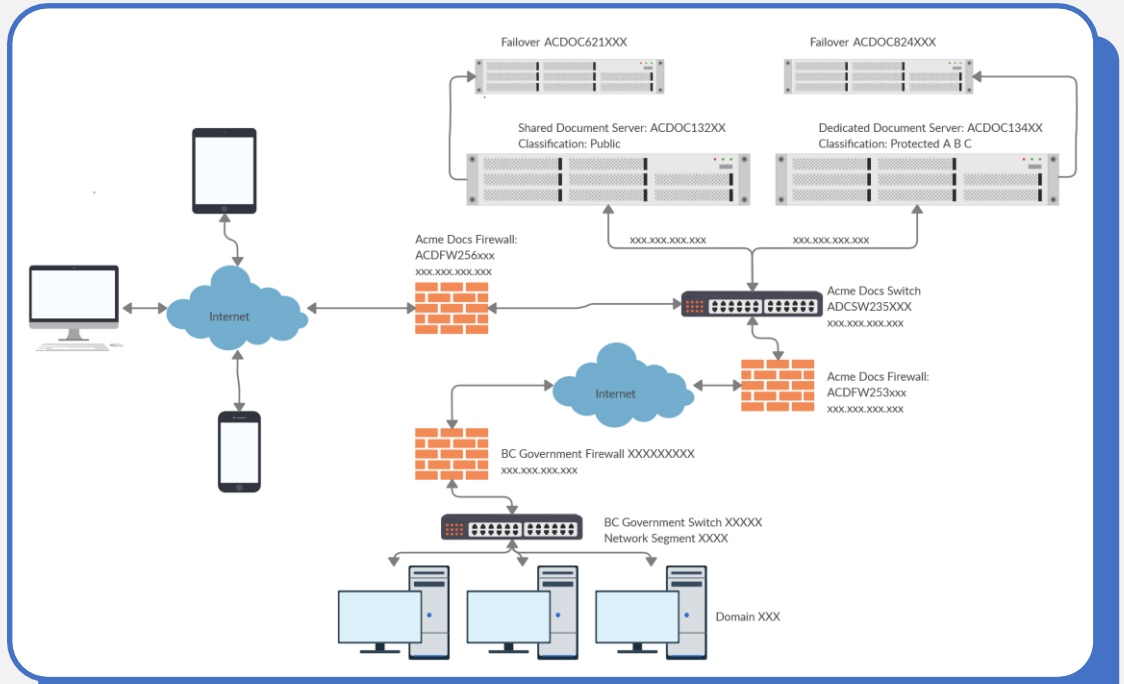
Example Threat Model: ACME Docs

This is a fictional high-level threat model example, to address the risk we will follow the four-step model from section 3.

The company '**Acme Docs**', a cloud service that securely handles documents to provide a cloud service, it is proposed to use this company to provide a document storage solution for a particular ministry. The ministry would upload and download documents of various classifications from Acme Docs cloud service, as do Acme Docs other customers. Acme Docs accesses this cloud too, for software updates, version maintenance and monitoring. Each customer is stored in separate databases within the same application servers, though a more expensive separate store option is available.

Step one of the four-step threat model plan is understanding ***What are we building***.
The implementation team get together with the business area to discuss their specific needs. After understanding the business need the implementation team meets with Acme Docs to see if the business requirements are consistent with their understanding. The team then works out the legal, policy, guidelines and best practices that need to be followed.

Once the basics are understood it is time to gather details so that the full picture can be understood. In this example we are not following a specific threat model, as described earlier, but are taking what we need from various models to achieve our goal. Through meetings with the business area, service provider (Acme Docs), documenting the technical architecture, network diagrams, understanding the data classification, business context and information like the data flow diagrams, we can gather facts and understand the solution.

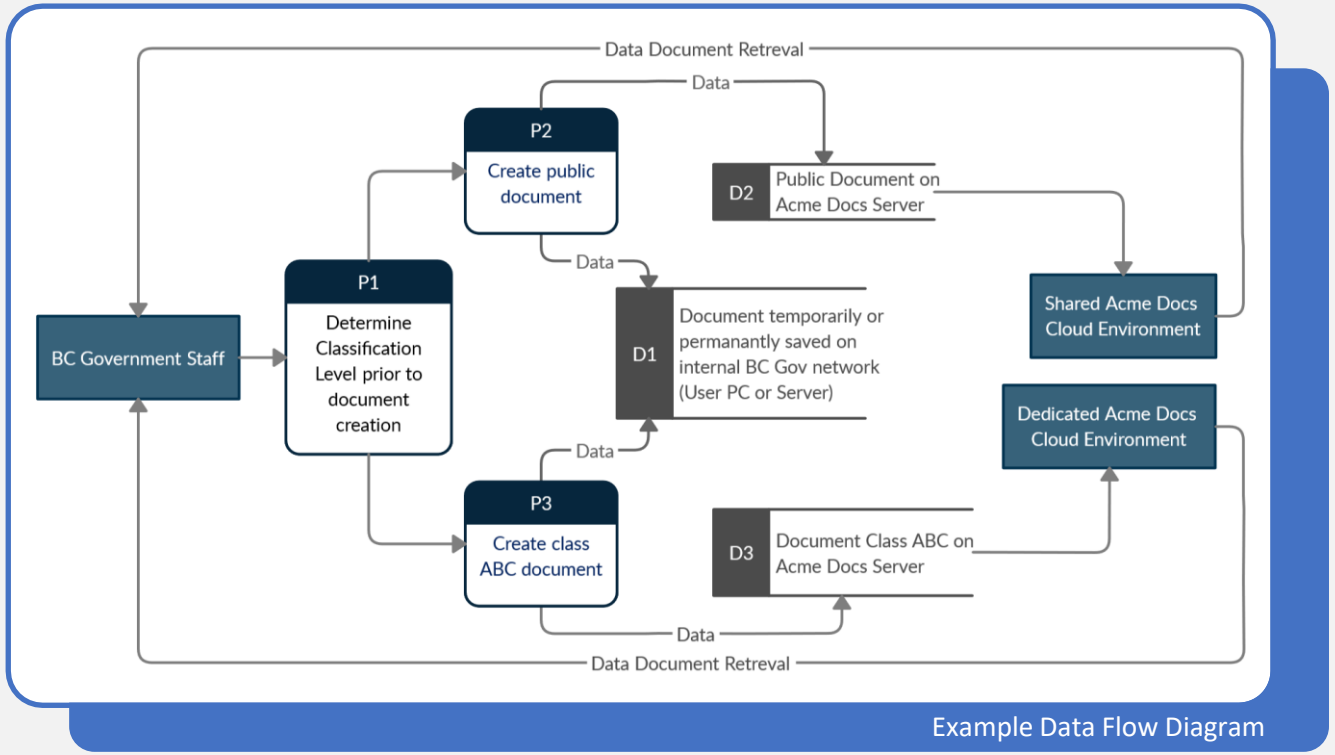


Example Network Diagram

Example Documents:

- Use internal Policy & Guidelines
- Use external best practice
- Project Planning document
- Technical Architecture Diagram
- Network Diagram
- Asset Inventory
- Threat Inventory
- Threat Model Document
- Threat &/Or Attack Tree
- Statement of Acceptable Risk (SOAR)
- Security Threat Risk Assessment (STRA)

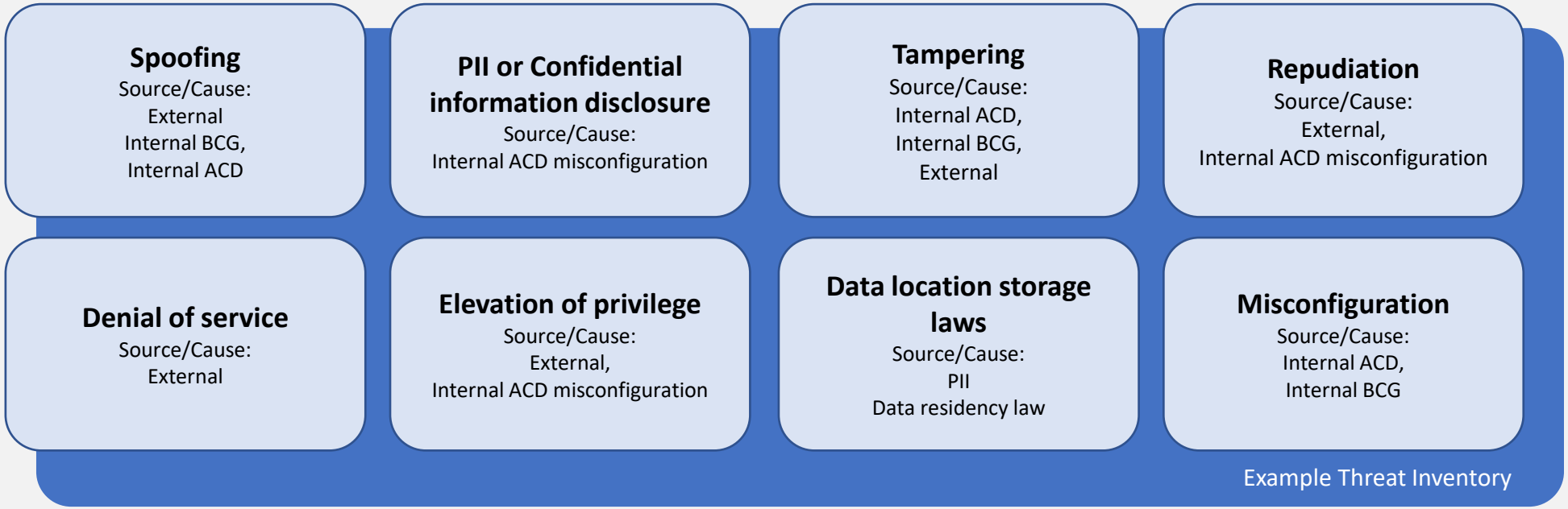
The team determines that the service needs to be hosted in Canada, as it involves non-public data, and after creating a data flow diagram they determine that the public data can be stored on the less expensive shared storage while the none-public data must be stored on more expensive dedicated encrypted servers. This proposal meets both the legal and policy requirements for this system. Privacy and information security are included from the start as it makes the solution easier to manage, and cheaper, as the project progresses.



Example Data Flow Diagram

After creating the documentation to understand the requirements of the project, and confirming the data flow with security experts and the business, the team moves on to **step 2.** This is where it is determined: ***What can go wrong.***

This is when the security threats can be understood, in this case the team writes out the potential high-level threats using threat intelligence and determines the high-level threats, and sources of those threats, faced by the project:



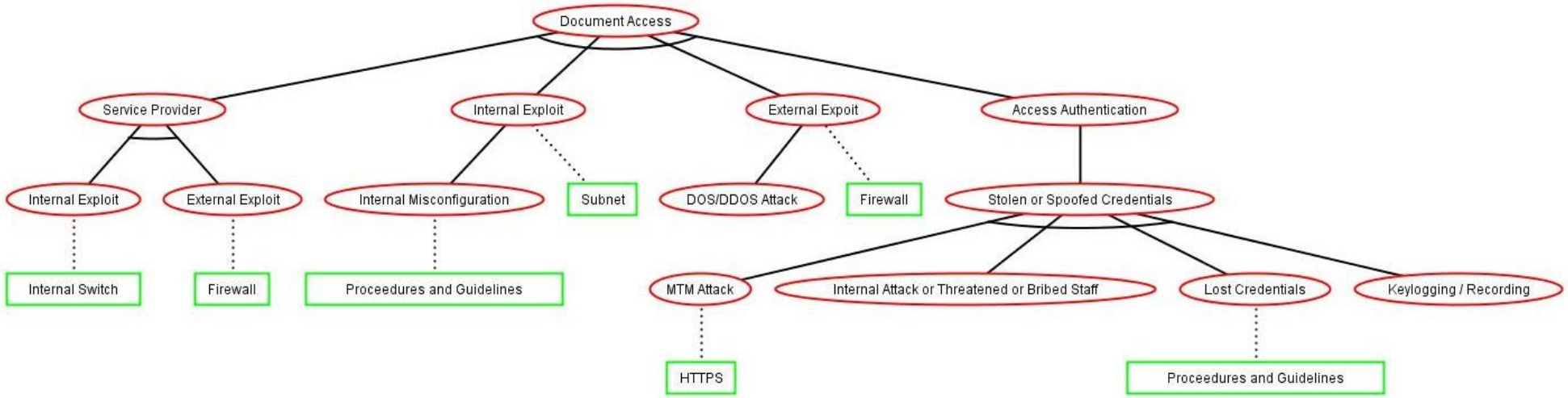
Example Threat Inventory

The threat inventory can be as detailed as needed, it can help to focus the team on the threats that are considered to be the most important.

Attack Tree Example

After the threat inventory the team create an attack tree, attack trees are conceptual diagrams showing how an asset, or target, might be attacked. See: https://en.wikipedia.org/wiki/Attack_tree.

Threat and attack trees are almost identical and are often used to mean the same thing. However, a threat tree is seen from the defenders' viewpoint and can provide some additional details such as threat ranking (prioritising), while an attack tree is from the attacker's viewpoint and can show defences, such as a firewall. Use which suits your situation the best.



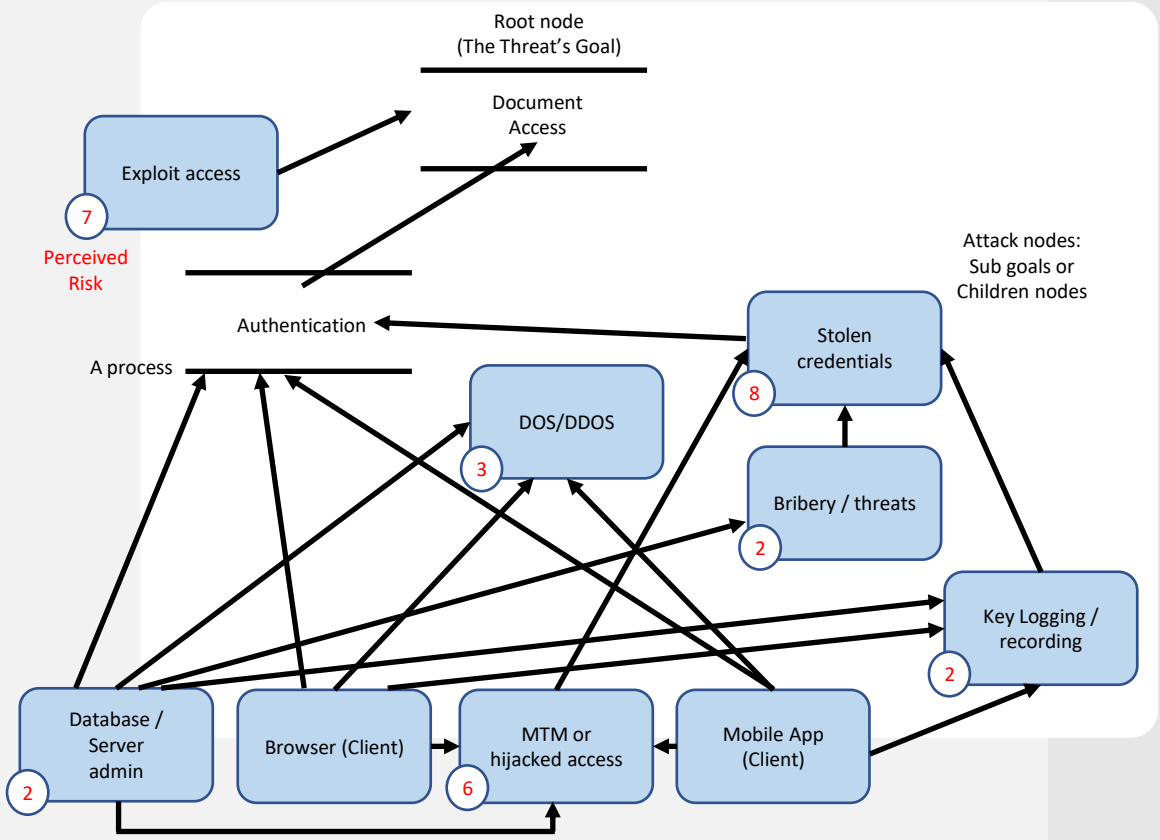
This attack tree was created using the open source ADTool, https://satoss.uni.lu/members/piotr/adtool/

Threat Tree Ranking Example

The attack tree showed the risks, the team decide that they want to go deeper and prioritise the threats. In this example, the team decides to create a threat model using a *threat tree,* with threat ranking, a process where threat levels can be assigned to each of the potential threats. These levels can dynamically change depending on the information available and the perceived risk.

The ranking key here is: 1 is lowest threat and 10 is highest threat. In this example we can see the highest threats, at this snapshot in time, are a man in the middle attack, leading to stolen credentials and exploit gaining access. These would become the priorities to be addressed by the team.

The threat ranking is formed from other activities, such as the STRA, threat inventory, data flow diagram, network diagram, and so on. Therefore the ranks are dynamic, they can change as more information is gathered and understood during the threat modeling process. The rankings are also formed jointly with other teams to ensure the right value is placed on the business needs, for example, something may be a technical risk but if the data to be protected is public, and presents no danger if released, then the risk associated with it is likely to be low.

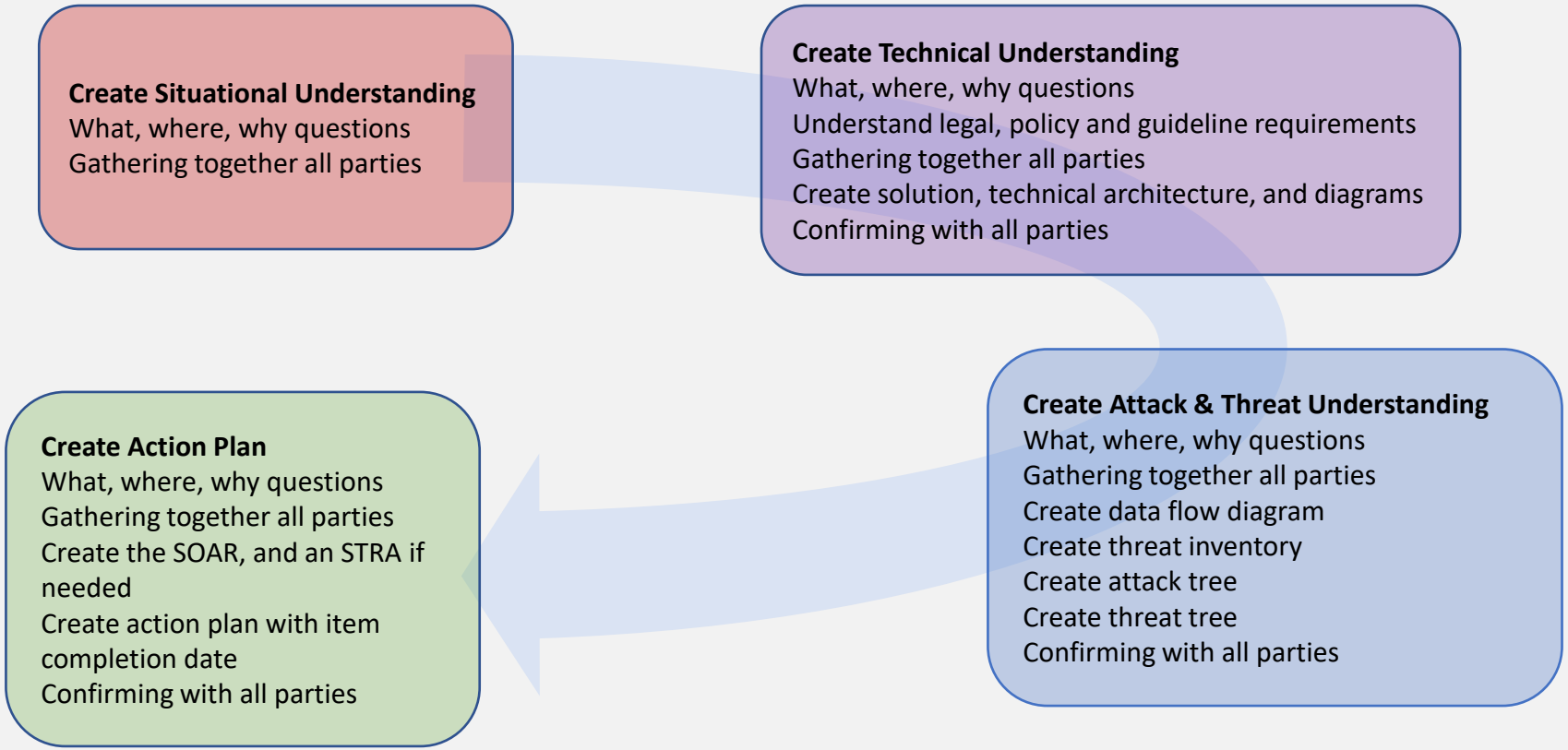


The team then completes a comprehensive STRA, which includes the SOAR. Doing this brings them from step two into step three: **What are you going to do about it?**

The STRA process includes taking each identified risk and addressing them, risks can be accepted, mitigated, resolved or become action items. An accepted risk is deemed to be **low risk** and or **low likelihood**. Low risks are not critical to the operation of the system or process.

Risks that are mitigated are those addressed by a different protection, such as a firewall. Resolved risks are those that have been addressed during the risk assessment process, and action items are those risks yet to be addressed. Action items must contain a plan of how to address the outstanding risk, and a date of when that will occur.

The threat model process for the Acme Docs example went as follows:



Completing Your Threat Model

Can a Threat Model Be Considered Complete?

No, not really. A threat model is a living document, or documents. It is likely to be revised many times, including being: questioned, revisited, updated and revised. A threat model can be considered '*complete*' when you:

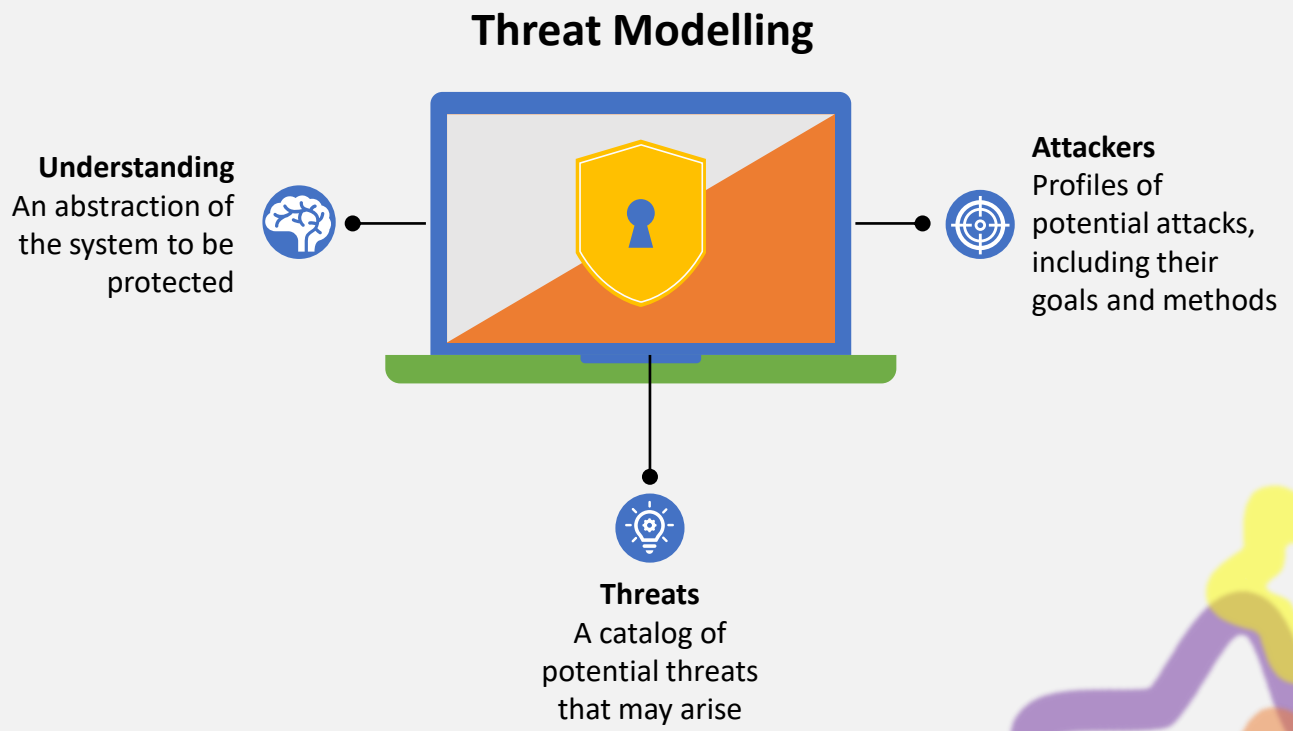
- Understand what it is you want to protect
- Understand how what you want to protect is likely to be attacked; the how and why
- Understand the threats facing what you want to protect

Remember that nothing in information security is ever really complete. With environment revisions, software updates and changes, new cracking tools or vulnerabilities; what is considered complete now may be open again tomorrow. Threat modelling is a four-step process, and although people do not prioritise step four it is vital that revising and revisiting your security is included in your plans.

1. What are we deploying or building?
2. What can go wrong?
3. What are you going to do about it?
4. **Review the work done at steps 1-3 and repeat as necessary.**

Remember that many threat modeling frameworks exist, and they can be combined to create a more robust and well-rounded view of potential threats. Use the framework right for the situation you face, or mix frameworks. Not all of them are comprehensive; some are abstract and others are people-centric. Some methods focus specifically on risk or privacy concerns.

As long as your threat model has been performed early enough in the development cycle, when potential issues can be caught early and remedied, you will have prevented a much costlier fix down the line. Using threat modeling to think about security requirements can lead to proactive architectural decisions that help reduce threats from the start.



Course Goal

Now that this course is complete you should be able to understand what Threat Modelling is, why it is important, and the basics of how to go about using threat modelling within the BC Provincial Government.

Thank you for your time and energy in taking this course.

Together we make our residents data more secure.

Glossary

AWS: Amazon Web Services

CIA: Confidentiality, Integrity, and Availability

CISO: Chief Information Security Officer

CVE: Common Vulnerabilities and Exposures

CVSS: Common Vulnerability Scoring System

DFD: Data Flow Diagram

IM: Information Management

IT: Information Technology

ISB: Information Security Branch

ISP: Information Security Policy

ISRM: Information Security Risk Management

OCIO: Office of the Chief Information Officer

OIPC: Office of the Information and Privacy Commissioner

MCIO: Ministry Chief Information Officer

MISO: Ministry Information Security Officer

NIST: National Institute of Standards and Technology

SaaS: Software as a Service

STRA: Security Threat Risk Assessment

SME: Subject Matter Experts

VM: Vulnerability Management

VRM: Vulnerability Risk Management