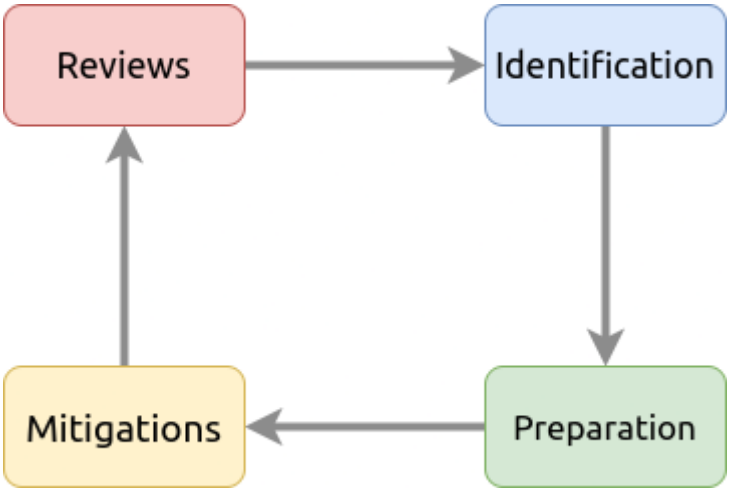
Threat Modelling & Incident Response

Threat modelling is the process of reviewing, improving, and testing the security protocols in place in an organisation's information technology infrastructure and services.

A critical stage of the threat modelling process is identifying likely threats that an application or system may face, the vulnerabilities a system or application may be vulnerable to.



The threat modelling process is very similar to a risk assessment made in workplaces for employees and customers. The principles all return to:

- Preparation
- Identification
- Mitigations
- Review

It is, however, a complex process that needs constant review and discussion with a dedicated team. An effective threat model includes:

- Threat intelligence
- Asset identification
- Mitigation capabilities
- Risk assessment

To help with this, there are frameworks such as **STRIDE** (**S**poofing identity, **T**ampering with data, **R** epudiation threats, **I**nformation disclosure, **D**enial of Service and **E**levation of privileges) and **PASTA** (**P**rocess for **A**ttack **S**imulation and **T**hreat **A**nalysis) infosec never tasted so good!. Let's

detail STRIDE below. STRIDE, authored by two Microsoft security researchers in 1999 is still very relevant today. STRIDE includes six main principles, which I have detailed in the table below:

Principle	**Description**
Spoofing	This principle requires you to authenticate requests and users accessing a system. Spoofing involves a malicious party falsely identifying itself as another. Access keys (such as API keys) or signatures via encryption helps remediate this threat.
Tampering	By providing anti-tampering measures to a system or application, you help provide integrity to the data. Data that is accessed must be kept integral and accurate. For example, shops use seals on food products.
Repudiation	This principle dictates the use of services such as logging of activity for a system or application to track.
Information Disclosure	Applications or services that handle information of multiple users need to be appropriately configured to only show information relevant to the owner is shown.
Denial of Service	Applications and services use up system resources, these two things should have measures in place so that abuse of the application/service won't result in bringing the whole system down.
Elevation of Privilege	This is the worst-case scenario for an application or service. It means that a user was able to escalate their authorization to that of a higher level i.e. an administrator. This scenario often leads to further exploitation or information disclosure.

A breach of security is known as an incident. And despite all rigorous threat models and secure system designs, incidents do happen. Actions taken to resolve and remediate the threat are known as Incident Response (IR) and are a whole career path in cybersecurity.

Incidents are classified using a rating of urgency and impact. Urgency will be determined by the type of attack faced, where the impact will be determined by the affected system and what impact that has on business operations.

Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

An incident is responded to by a **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam (**CSIRT**) which is prearranged group of employees with technical knowledge about the systems and/or current

incident. To successfully solve an incident, these steps are often referred to as the six phases of Incident Response that takes place, listed in the table below:

Action	Description
Preparation	Do we have the resources and plans in place to deal with the security incident?
Identification	Has the threat and the threat actor been correctly identified in order for us to respond to?
Containment	Can the threat/security incident be contained to prevent other systems or users from being impacted?
Eradication	Remove the active threat.
Recovery	Perform a full review of the impacted systems to return to business as usual operations.
	What can be learnt from the incident? I.e. if it was due to a phishing email, employees should be trained better to detect phishing emails.

Revision #2
Created 2023-02-11 21:04:17 UTC by Fettlaus
Updated 2023-02-11 21:16:51 UTC by Fettlaus