secarma
CYBERSECURITY EXPERTS

A Advise C Certify T Test

Threat Modelling

What is Threat Modelling?

Threat Modelling is a structured tabletop exercise which is used to identify and mitigate potential threats to a system or application. It is an essential step in the software development process to ensure that security is built into the product from the outset. Threat modelling has become more critical than ever before due to the ever-growing number of cyber-threats.

Threat Modelling is a risk management activity performed by those with a deep technical understanding of the application, module, or business process.

Who Is It For?

Threat Modelling should be utilised by anyone:

- Developing software,
- Utilising third party APIs,
- With complex business processes,
- Who would experience catastrophic business damage or reputation damage as a result of data loss,
- And any business holding sensitive data.

Why should you Threat Model?

Threat Modelling can be applied to a variety of areas, including software, web applications, systems, networks, distributed systems, Internet of Things (IoT) devices, business processes and even paper-based systems. Threat Modelling allows your business to identify security risks and take a risk-based approach to fixing security issues within your systems, devices, applications, and processes.

Threat modelling allows you to detect problems early in the development lifecycle, even before coding begins. It allows you to spot design flaws that traditional testing methods and code reviews may overlook, whilst allowing you to evaluate new forms of attack that you might not have otherwise considered.

The results of threat modelling exercises include the formation of a data flow diagram that identifies entry points into your systems to help you build a prioritised list of potential vulnerabilities, and support in the development of contingency plans.

Threat Modelling helps you to maximise your testing budget by helping you to target testing and code reviews. It enables you to remediate problems before software release and prevent costly recoding post-deployment, whilst encouraging you to think about threats, beyond standard attacks, unique to your application.

Through all of these, threat modelling supports the implementation of a robust application that highlights assets, threat agents and controls to deduce components that attackers will target.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com

When to Threat Model

When to threat model is dependant on your development approach, but ideally it will be incorporated in the design stage of a new build and done prior to deployment; this will also dramatically reduce your costs.

It is also appropriate to threat model as a result of a significant system change or update, or in response to significant world event, e.g., global pandemic, war.

Threat Modelling Approach

There are a couple of threat modelling approaches that may be utilised, System Lead and Attacker Lead.

- System Lead focuses on the system as a whole, considering each process, data store, dataflow, external entity, and trust boundary.
- Attacker Lead focuses on threat actors and how they may compromise our system. This involves understanding threat actors and focusing on entry points rather than the system as a whole. It involves focusing on critical assets, and emphasis is placed on protecting critical assets instead of the entire system.

How can Secarma help you?

Our services will educate your employees in a positive and encouraging manner, heightening awareness of threat modelling, whilst encouraging the identification of possible threats to an application or infrastructure prior to release.

Many organisations have the intention to improve the security of their applications and infrastructure, but simply don't know where to start. Secarma's mission is to support the implementation of threat modelling into your development processes and encourage security-by-design.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com