**h3 Should Tero wear a helmet?**

**1. Threat modeling manifesto**

Threat modeling is described in the Manifesto as the process of highlighting security and privacy features in system models. That and much more is what threat modeling is. Through threat modeling, developers and testers may learn about security from a different perspective then the normal. It’s all about basic important questions like What are we attempting to defend? What kind of disaster might possible affect our system? How do we intend to counteract these conceivable problems? Do we performed a systematic job of protecting our system, to sum it up?

When performing threat modeling, we begin to recognize what can go wrong in our system. It allows us to pinpoint design and implementation issues that require mitigation, whether it is early in or throughout the lifetime of the system. The output of the threat model, which are known as threats, informs decisions that you might make in following design, development, testing, and post-deployment phases of the system.

It also recommends adopting several perspectives to approach issues and potential solutions, being pragmatic rather than ideal, and staying away from errors like putting too much faith in a single solution to handle everything or becoming bogged down in the finer points.

**2. Welcome to the Worlds Shortest Threat Modeling Course**

Mr. Shostack discusses in these videos about the threat modeling and highlighting the core importance of outlining the issues, collaboration by asking questions related to security, privacy and recording these threats through modeling them.

It shows what to do and how to do them in systematic way, because they are closely related to threat modeling and dangers frequently follow data, as in data flow diagrams. The five symbols used in these diagrams are external entities, processes, data flows, and small drums, which stand in for any running code that is under your control but not under the control of external entities, such as an app. The final component is the trust border, where we demonstrate that various components are run by various entities with various personnel and operational procedures.

In this short course Shoskack help to understanding of systems issues, particularly from a risk perspective. It ensures more effective threat prioritization, informing everything from decisions to mitigation efforts.

**3. Chapter 1 - Dive In and Threat Model!**

Dive in and Threat Model, Chapter 1, "Diving in and Threat Modeling," of "Threat Modeling: Designing for Security," demonstrates with examples how to use the four important questions in practice:

1. What do you have in place?

2. What might go wrong?

3. What should you do in response to potential negative outcomes?

4. Did we perform a satisfactory analysis?

Any technical expert can master the useful skill of threat modeling. Combining two models—one representing prospective problems (threats) and the other, a diagrammatic representation of the software being created or deployed requires this.

STRIDE model that explain, pretending to be something or someone you're not is known as spoofing. Modifying something you're not supposed to modify is tampering. It may consist of bits stored on disk, bits in memory, or packets transmitted over a wire or wirelessly. Repudiation is the act of denying doing something, regardless of whether you actually did it or not. Exposing information to those who are not allowed to see it is known as information disclosure. Denial of service attacks aim to stop a system from providing services, such as by crashing it, making it too slow to use, or using up all of its storage. When a program or user has a technical right to do something they shouldn't, this is known as elevation of privilege.

**4. Threat Modeling Cheat Sheet**

Threat modeling is a systemic method to identify and prioritize potential threats which help in for both new and existing systems. It's impotent for us in software development, not just security experts, and also save resources when applied initially. While creating a threat model are:

1). Analyze data flow for vulnerabilities.

2). Document potential threats.

3l. Note security measures for mitigation.

Systems and applications can both benefit from this strategy. Understanding the skills and motivations of threat agents, or people who can carry out threats, is crucial. While likelihood evaluates the likelihood of a threat, impact quantifies the possible harm. There are two types of controls: “preventions” that thwart dangers and “mitigations" that lessen their effects. Information flow and trust transitions in the system are made more understandable by data flow diagrams and trust boundaries.

**a) Security hygiene. What basic security practices should everyone follow?**

Best security practices should be as follow:

Regular Software Updates

Multi-Factor Authentication

Strong password and password manager

Secure browsing behaviors

Data backup frequently

Privacy Settings and firewall enable

Physical security of devices

Regularly check system health and data communication.

**b) Make-belief boogie-man - a threat model for imaginary company:**

My company is small IT Service provider where cybersecurity threats are the core value of the business, It face both opportunities and challenges. Our IT company, "ITCS," aims to provide a seamless and secure experience for our consumers while enhancing our operations through innovative technology. To achieve this, we recognize the critical need for a threat model that encompasses all aspects of our business.

**What are we working on?**

Our team are working on creating a systemic and unique calibration with our customers that leverages cutting-edge technology to enhance customer experience, streamline operations, and protect sensitive customer information. Our core resources include:

Customer database

Communication and channel

Sales and marketing

Platform and infrastructure

Website, mobile app, application and software

Billing and invoicing system

Datacenter, Server and network

By maintaining the security of our business core assets like website, mobile app, and social media is crucial to protect our digital brand. Our cyber security team directly supports our business goals by ensuring the trust and safety of our customer relation system, database and digital media through look after the potential threat actively.

**What can go wrong?**

To identify the potential threats, our security team follow the STRIDE model, which further categorizes these threats into categories: like Access control, Deceiving, Tampering, Repudiation, Information disclosure, Denial of Service, and Limited Access Privilege along with DOS attack.

Data breaches, website tampering, and weaknesses in system, data processing are high-priority issues. Due to their potential impact on customer trust and financial losses, these risks have a high expected value. We might also be the target of other particular threat actors, such as competitive industrial surveillance or financially motivated cybercriminals. It is essential to comprehend their potential, prospects, and goals.

**What are we going to do about it?**

To mitigate the known and unknown risks our team developed a systemic strategy, which may reduce the impact or make is costly to breach the system. These are:

Constant monitoring

Regular Software Updates

Multi-Factor Authentication

Strong password and limited access

Data backup frequently

Privacy Settings and firewall enable

Physical security of devices

Regularly check system health and data communication

**Did we do a good enough job?**

We'll undertake recurrent security audits, penetration tests, evaluations, and ongoing threat modeling to gauge how well our security measures are working. We'll keep up with new threats and adjust our security procedures as necessary. To earn our customers' safety and trust, we strive to go above and beyond regulatory requirements. Most significantly, there is no impact on business continuity.