SECURITY COMPASS WHITEPAPER

Designing NextGen Threat Identification Solutions

Security Compass

Introduction

Threat Modeling is an essential part of an organization's Risk Management strategy. Through threat modeling, teams are able to anticipate attack patterns and build controls into the software to mitigate risk.

Threat identification is one of four steps in the threat modeling process, as shown in Figure 1. There are several approaches organizations can take to identify and enumerate threats in different scenarios and systems. This paper analyzes traditional threat identification methods and their suitability and challenges in today's product development scenarios, then identify and propose key elements to consider when designing new threat identification solutions.

Background

More than a dozen risk and threat model approaches have been proposed by security researchers over the last two decades. Some are very prominent and have been adopted widely by practitioners, demonstrating the industry's commitment to threat modeling and the benefits of a "shift left" approach.

Though traditional approaches to risk assessments and threat models can work well there have been mixed response regarding outcomes due to a) the completeness of approaches in threat coverage, or b) the ability of an organization to rigorously follow the threat identification process. The lesson is that not every approach is appropriate for every scenario. A careful study is warranted before the threat identification process.

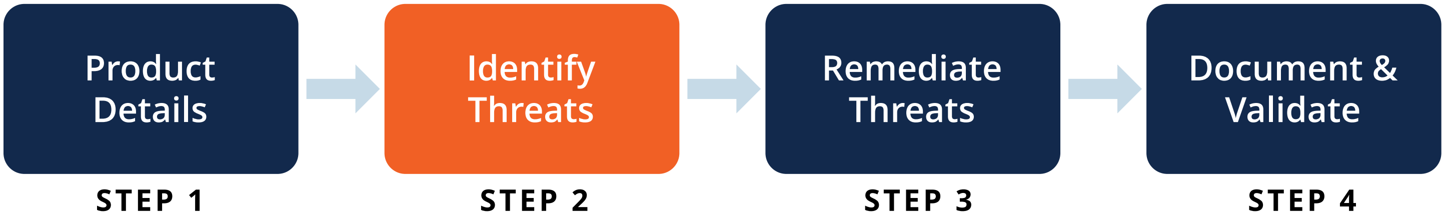


Figure 1.

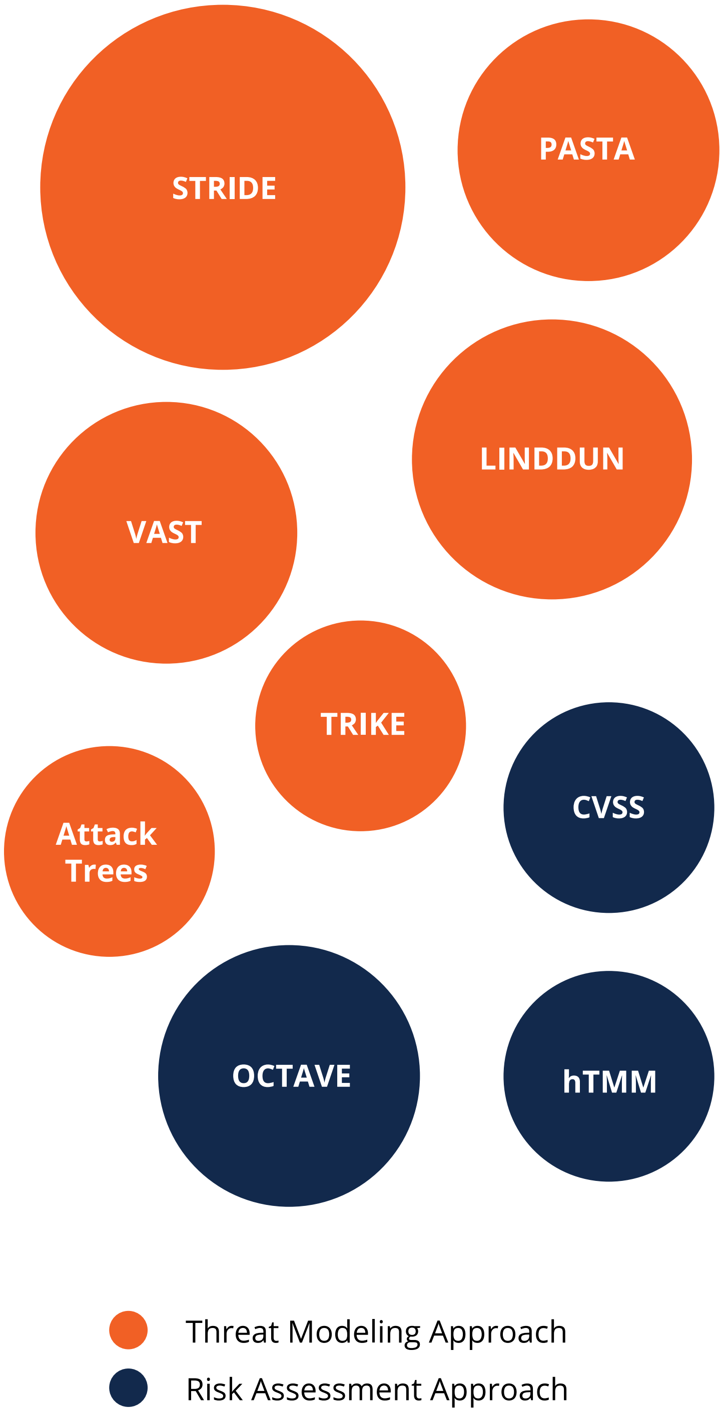
Traditional Threat Modeling and Risk Assessment Approaches

Though there are many approaches of discovering threats, we focus on the 12 methods detailed in the 2018 Carnegie Mellon Software Engineering Institute (SEI) whitepaper: STRIDE, PASTA, LINDDUN, CVSS, Attack Trees, Persona non Grata, Security Cards, hTMM, Quantitative Threat Modeling Method, Trike, VAST Modeling, and OCTAVE.

Traditional Approach Benefits

Widely adopted threat model and risk assessment methodologies like STRIDE and OCTAVE provide teams with many benefits, including:

- **Trustworthiness** – Many of these approaches have been used for years and provide clear security benefits. Stakeholders have confidence in the methodologies.
- **Adaptability** – The approaches are quickly grasped by security and engineering and are applicable to a variety of software and system projects.
- **Coverage** – The approaches are thorough and identify a high proportion of security threats and risks.
- **Alignment** – The approaches track well with accepted security concepts and development methodologies



Concerns with Traditional Approaches

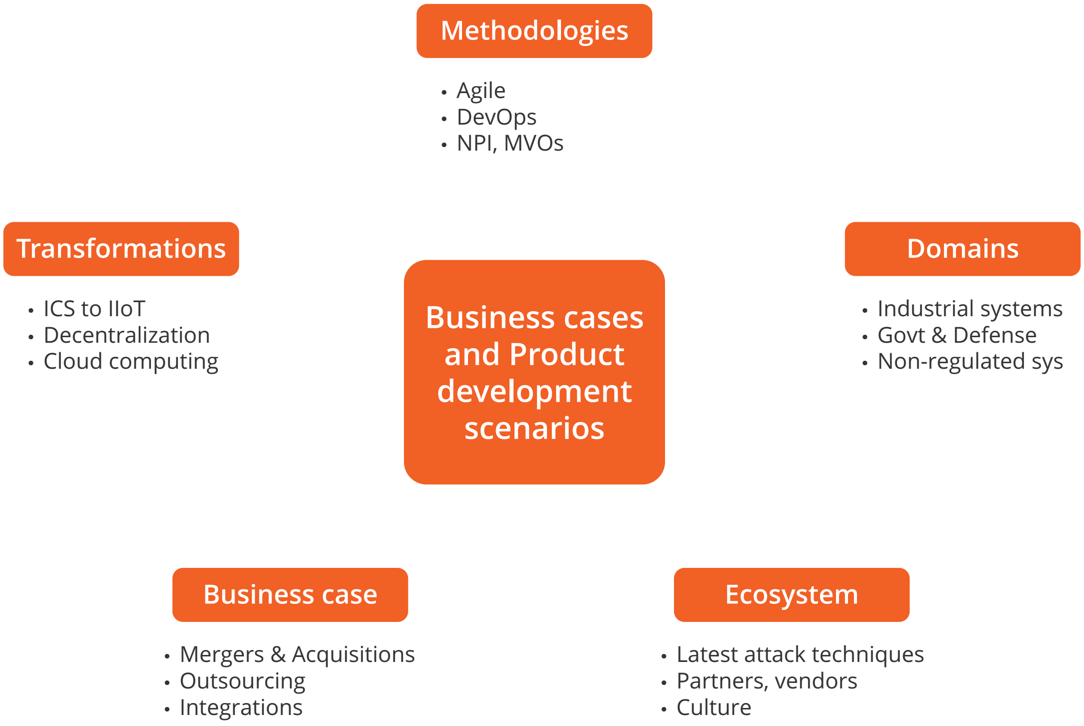
The benefits of threat modeling are clear, and in many cases overshadow concerns that only become clear when we implement the different methodologies across a variety of products and business scenarios.

It is important to note that there is no concern with threat modeling in general or with the methods as a whole. Instead, the concern is mostly when we follow them as strict processes which may not fit well with today's rapid development environment. For an easier understanding, we have grouped together the concerns in three areas.

a) Concerns with Approach

Software development processes have evolved rapidly over the past decade. Where engineering once relied heavily on the waterfall development process with separate security teams, rapid development and deployment methodologies have made the ability to deliver new software quickly a distinct competitive advantage. These changes bring enhanced benefits to customers and revenue to the business, but also change the products and infrastructure, introducing new threats and risks, including business-related threats that may not be visible to the security teams focused on the technical design of product.

The graphic below provides business cases and scenarios where the application of traditional methods may not be ideal for discovering threats, especially those that can only be discovered on the completed system, post-deployment.



b) Concerns with Process

Product development is a multi-disciplinary activity, involving professionals at different levels and roles at every stage of the development lifecycle. Commonly observed roles include:

- Business Unit Leads
- Business Analysis
- Domain Specialists
- Product Architect
- Product Developers
- Data Analysts
- Infrastructure Specialists
- Legal teams
- Functional Auditors
- IRM team
- System Admins
- Customer Support
- Vendor Manager
- User Exp Lead
- Solution Engineer
- Program Manager
- Quality Analysts
- Cross functional teams

Most of the times threats are identified after gathering information about the product design from the Product Architect and Product Developers. This is fine if the intent is to discover threats present in the application design or a specific module or subset of the product. If the goal is to discover threats for the complete system, however, then it is important to gather complete information about every aspect and operating scenario from multiple roles and functions. This raises two questions on the process:

- **What is the impact on resourcing?** - Security professionals are scarce in organizations of all sizes, and product and development teams are under constant pressure to deliver new code. Demands on their collective time, budgets, and project scope makes it challenging to collect complete information for the threat model.

- **When and how many times do we conduct threat analysis?** – Threat modeling new applications is important, but these exercises often overlook the associated systems and deployment environments. This includes threats that may cascade from the new software to existing systems, and vice versa. Performing a threat analysis only once during the design or in the pre-development stages of the project and ignores threat discovery approaches in other stages.

c) Concerns with Outcome

There are two important concerns with the outcome of the Threat Identification.

1. **Risk Management: Risks are the measurable outcome** of a threat modeling or risk assessment. It is these risks that define how well the threat analysis have been performed. Further, residual risk will always remain. In most product assessments, the risk management strategies are defined by the security team in isolation. This makes it challenging for business and project leads to prioritize and address the identified risks from risk initiation stages to risk closure stages. Since the product teams know product and customer priorities better and better understand acceptable risk from a business standpoint, they must be included in the risk management strategies.

2. **Threat Analysis Reports:** Security teams typically follow a **security first approach** when identifying and reporting the threats in the threat assessment report. This can defeat the overall purpose of Threat Modeling or Risk Assessment activity, as it becomes difficult for project teams to understand the security language (e.g., ranking

threats, classifying threats, risk posture, detecting misuse cases, etc.) and act upon them. A better strategy is to convey the threats identified and their impact in the **business language** that both technical and non-security analysts can easily follow.

While these are common concerns with the approaches and processes followed, organizations also face many other project challenges, including but not limited to:

- The scarcity of qualified security professionals in the industry capable of performing proper threat assessments.

- Insufficient efforts spent on threat assessments leading to scope imbalance in project executions.

NextGen Threat Identification Solutions

Efforts to address challenges

While these challenges are real, they do not make threat analysis an optional security activity Stakeholders continue to demand better security in general and regulators and auditors require periodic secure design reviews at all stages of system development. Inevitably, this includes an assessment of risk and threats and a plan for addressing the same.

Some organizations have taken measures to address the resource constraint, including training developers and architects to perform threat analysis on their own, but there is minimal appropriate guidance for doing so. Some have leveraged commercial tools and a combination of threat analysis approaches to obtain better outcomes. While some companies have achieved partial success, issues remain with the process. Items like standardization are still missing, including crucial aspects for threat discovery reports in the product development lifecycle.

Key objectives to consider

Given the many challenges with existing approaches and processes, a new threat analysis solution is needed to suit current and future needs. The new solution must not only address the technical aspects of discovering threats, but also discuss the feasibility of implementing the solution as part of the complete product development process and ensuring the mandatory participation of all stakeholders in the process.

The key issues the new solution must overcome, and address include:

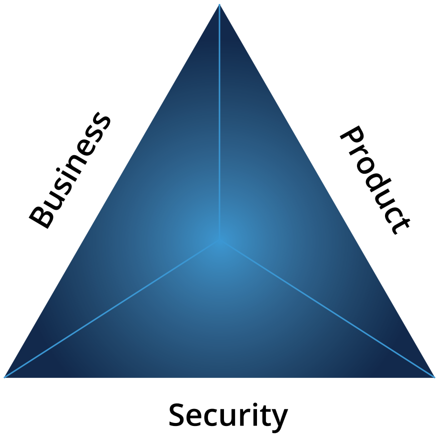
- Inform **security professionals** on business objectives, project needs, and appetite for risk

- Assist **business owners** in obtaining executive buy-in and the need to focus on security throughout the product lifecycle.

- Educate **product teams** on the benefits of the Threat Analysis to product deliverables and that it need not be complex task.

These are important parameters to consider while creating a new threat analysis solution. They help identify the key stakeholders (and their teams) who must be involved in threat analysis solutions, their present challenges, and the efforts needed to overcome the challenges. In short, the key stakeholders of a Threat Analysis report are the same as the stakeholders involved in the project – The Business owner, Product development team, and the Security team.

We will see in the section below how any new threat analysis solution should implicitly consider and convey the objectives of each team, including the goals of the processes and incorporating the solution within an organization's culture.



Stakeholders Goals

Business

I. Ownership

The business owner should take complete responsibility for any risk assessment or threat modeling process. This means initiating the threat assessment activity, creating the process documents (e.g., defining the standard operating procedure) and gathering the required teams. Importantly, this brings standardization of the process across a variety of products.

II. Accountability

With responsibility comes accountability; making business owners responsible for determining acceptable risk levels makes the outcome more tangible and helps determine the depth of the threat analysis process. With strong executive buy-in it is easier to establish appropriate good governance in the threat analysis activity. A good example is creating escalation matrices for dealing with threats reported.

Product

I. Empowerment

Since the product team knows the operations and environmental usage of the best, they should be trained and empowered to perform basic threat analysis. Instead of waiting for security teams to complete an end-to-end threat analysis activity, product teams can capture basic relevant threats they find in their work. These could be validated and augmented by the security team later, including capturing advanced levels of threats, making better use of security professionals time.

II. Responsibility

Product management must prioritize security as a critical job responsibility alongside the role-based requirements. This must include educating development on security concepts and basic threat analysis activity, allowing development to identify threats as they work on use case scenarios. This also requires increased collaboration between business and security teams to create a usable threat analysis process that includes product teams.

Security

I. Evangelism

For the business and product teams to succeed, security must lead the effort and be the catalyst at every step of the initiative. The security team should be able to articulate the guidelines for threat discovery process clearly. This is achieved through ongoing training sessions, including awareness of new threats and techniques. Including cross functional teams like legal and compliance teams for training in ethics and principles is also helpful.

II. Versatility

A threat identification solution should be customizable for different product scenarios (e.g., inclusions of security principles and design parameters). This means the various elements to consider for threat analysis will be different for each product; one size doesn't fit all. Also, security people should work with the product team to think beyond the application and address all business cases. The goal is a threat analysis solution that can be an adopted by all members involved in the project, even those with limited security knowledge.

Process Goals

The objectives regarding process are determined by a few important parameters which we normally consider in a Threat Identification process.

I. Approach

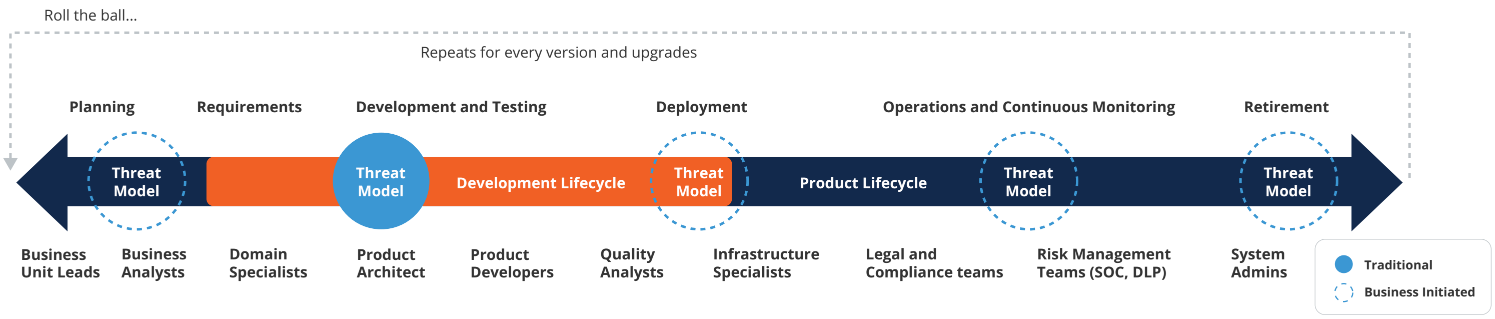
Attacker-centric threat analysis is an approach widely used by security people. Methods like STRIDE, Attack Trees, etc. help the security professional to "think like an attacker" to discover threats. However, it's important to note that threats are not limited to malicious attempts by adversaries. Purposeful and accidental insider threats result from disgruntled employees, accidents caused by Admins, and employees simply not following legal and compliance policies. Hence, we must apply multiple approaches and not just think like an attacker, but also think like a regulator, think like a competitor, and think like a consumer.

No one team or security professional can think like this alone. This type of approach can be achieved only by having a collaborative approach; a security team working with all stakeholders. The process must be equipped with the required procedural documents, reporting templates, feedback documents, training documents, knowledge repositories, and governance mechanism. It must be simple to follow so the process becomes repeatable.

II. Scope of Threat Analysis

We have seen the importance of including all stakeholders in the threat analysis process and continuing the threat analysis throughout the lifecycle of the product; performing threat analyses from the planning stages through the sunsetting stages of a product. This includes training and empowering every member to capture the basic threats, while security validates those and captures advanced threats.

Threat Modeling throughout the Product Lifecycle



Project management should consider the risk associated with each project and scope the threat analysis accordingly, including whether to perform threat analysis in a specific stage or throughout the product lifecycle. Overall, this revised process should not negatively impact the project managers and project sponsors.

This figure depicts the recommended approach of how projects could plan to define the scope of threat modeling process throughout the product lifecycle. This includes the different roles that can participate in threat modeling with the required assistance and oversight from security teams

Solution Design

As conveyed above, any new threat analysis solution should address the concerns of traditional methods, the process gaps, and consider the goals of the stakeholders. It must also accommodate any methodologies or internal processes and be adaptable across different product disciplines. Ideally, it should cover the following key points:

- **Business-driven approach** – The business should take the lead, creating the process, initiating the activity, determining the risk levels, and successfully rolling it out in the project lifecycle.

- **Developer-empowered approach** – Empower every member of the development process to perform threat analysis at any point of the product lifecycle.

- **Continuous and customizable approach** – The threat modeling process should accommodate a variety of products and have precise guidelines, allowing it to be adoptable by everyone with limited assistance.

- **Standardized but flexible approach** – The process should be well defined and deliver consistent results across multiple projects and teams, bringing standardization and flexibility to ensure there is no additional overhead to project and business teams.

- **Collaborative approach –** The process should dictate that governance, accountability in threat analysis process, and risk management strategies are well dealt.

Conclusion

The world of software development and security is changing. The emergence of many new technologies and trends in product development has made older approaches to threat identification inefficient. In addition, the absence of de facto standards for threat identification activity has forced security professionals rethink how threat identification solutions must be designed for the next generation of products and business cases. The goal is to ensure that good design principles are followed when building such solutions and that the solutions must be well tested in different scenarios.

Security Compass

Security Compass believes in a world where people can trust technology, and it is our mission to help customers proactively manage cybersecurity risk, without slowing down business. Our holistic program offerings are tailored to your organization's needs. Through advisory services, training, and SD Elements, our award-winning policy-to-execution platform, we set you up with all of the resources and tools your organization needs to develop secure software. Security Compass serves some of the world's largest enterprises, including 16 of the largest financial institutions in North America, South America, and Asia, as well as 4 of the largest tech companies in the world.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

Author: Arun Prabhakar

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
1001 Bayhill Drive
2nd Floor
San Bruno, California
USA 94066

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001