Building a Mature, Enterprise-Level Threat Modeling Process in 7 Easy Steps

Anurag “Archie” Agarwal
Chief Technical Architect of ThreatModeler
Table of Contents

Introduction ............................................................................................................................................. 2
    The Conceptual Basis of Early Threat Modeling Methodologies ....................................................... 2
    The Need for a Scalable Threat Modeling Process ............................................................................ 2

7 Steps to Building a Mature Threat Modeling Process ........................................................................ 5
    Step 1: Define the Threat Modeling Objectives & Goals ................................................................. 5
    Step 2: Identify the Stakeholders & Assign Responsible Parties ..................................................... 9
    Step 3: Choose a Threat Modeling Methodology and Tool .............................................................. 10
        Determining a Methodology for the Organization ........................................................................... 11
        Considerations for Selecting the Proper Tool ............................................................................... 11
    Step 4: Secure Buy-In from all Stakeholders .................................................................................. 13
        Securing Security Executive Buy-In ............................................................................................. 13
        Generating Security Team Buy-In .................................................................................................. 14
        Securing Buy-In from the DevOps Teams ...................................................................................... 15
    Step 5: Map Out the Implementation Process .................................................................................. 16
    Step 6: Deploy the Threat Modeling Process in a Phased Roll-Out ................................................ 18
    Step 7: Measure, Measure, Measure ............................................................................................... 20

A Mature Threat Modeling Process is Within Reach ......................................................................... 21

Additional Reading ................................................................................................................................... 22

About the Author ..................................................................................................................................... 22
**Introduction**

Today’s enterprises increasingly rely on the highly interconnected nature of the current cyber-ecosystem for nearly every aspect of their operations and management. That interconnectivity generates tremendous value and autonomous efficiencies. At the same time, though, it is also the daily source of a nearly uncountable number of newly introduced threats. Isolation from the cyber-ecosystem is not a viable option for most organizations, but allowing malicious individuals or groups to gain unfettered access to valuable organizational assets is equally unacceptable.

In response, enterprise spending on defensive cybersecurity is predicted to continue growing by double digits each year through 2021. A significant casual factor driving the growth of cybersecurity spending is the defensive or forensic nature of most security technologies, coupled with the fact that it is impossible to defend against unknown threats or to stop attacks utilizing unrecognized attack patterns. On the other hand, however, attackers continuously exploit creative and inventive means to overwhelm servers, breach customer data, and compromise corporate knowledge assets.
CISOs and other decision-makers realize that they need a means to prioritize their security budgets. The only way to make intelligent, quantifiable management decisions, though, is to gain a deep understanding of the organization’s comprehensive attack surface from the attacker’s perspective. Gaining that perspective and developing meaningful, quantifiable, actionable outputs based on it is the purpose of a mature, enterprise-level threat modeling process.

Many organizations have, indeed, initiated a threat modeling process. Often, however, they struggle to objectively define what they want out of their threat modeling practice, let alone how to mature that process. They are challenged to feed their threat modeling outputs into their risk management process. And, most significantly, they are challenged to scale their process to a level of hundreds if not thousands of threat models.

In this whitepaper, we will not only provide consideration of all these issues, but also show how enterprises can mature and scale their threat modeling process such that it will address all their applications and underlying infrastructure. This goes well beyond simply identifying a list of potential threats and enumerating the appropriate mitigations on a per-application basis. Matured threat modeling is an organization-wide, value-generating, strategic initiative with measurable ROI, quantifiable insights, and actionable outputs for all stakeholders. A sophisticated and scalable process will allow organizations to understand their overall attack surface better and to change their security position from defensive and reactive to productive and proactive. Moreover, a mature, scalable threat modeling process will allow the organization to more effectively prioritize their risk management strategy, utilize their security budget allocation more intelligently, and prioritize the inevitable daily fires.

The Conceptual Basis of Early Threat Modeling Methodologies
Theoretical work on architectural styles, attacker profiles, and threat trees began back to the mid-1970s. By the early 2000s security professionals incorporated this work to allow threat modeling to enter the security mainstream. The limited goal of early threat modeling was to identify and enumerate potential threats to individual applications during the design phase.

Development teams used the contextually prioritized threats and mitigating security controls to significantly reduce vulnerabilities discovered during the scanning and pen-testing phase. Nonetheless, since threat modeling was a relatively new process, organizations cautiously applied it only on an ad hoc basis for applications considered critical and high risk in isolation from other considerations.

The Need for a Scalable Threat Modeling Process
Early application threat modeling proved its worth and organizations continued to utilize threat modeling as an integral part of their application SDLC initiative. However, the conceptual basis of early threat modeling methodologies inherently made scaling the process difficult. As a result, even today many organizations have yet to realize the full benefits of an enterprise-level threat modeling process. There are a number of reasons for this:
Building a Mature, Enterprise-Level Threat Modeling Process in 7 Easy Steps

- **Early threat modeling methodologies** were specifically designed to analyze one application at a time; analyzing more than one application at a time using traditional methodologies is too complicated. Furthermore, analyzing an application in isolation inherently misses threats or vulnerabilities that arise from application interactions, shared components, and 3rd party elements common to the contemporary highly interconnected cyber-ecosystem.

- **Creating and using system engineering abstractions** is resource-intensive. Creating fifty threat models with conventional processes may be doable. However, using those same methods to generate actionable outputs for all stakeholders from hundreds or thousands of unique threat models would require a substantial commitment of budget and personnel resources. Attempting to keep each threat model updated for each application design modification and every new relevant threat cataloged would quickly become untenable. Realistically, then, organizations using traditional threat modeling methodologies must prioritize which applications to threat model and how far each threat model can be pressed for outputs.

- **Development teams tend to resist** implementation of traditional threat modeling. The reason is understandable: Developers are under pressure to create functional applications under tight deadlines. Traditional threat modeling processes tend to complicate their workflow because the threat modeling methodologies require users to have security subject matter expertise.

From the vantage of improving upon the threat modeling successes which organizations have realized thus far, building a scalable process is more than simply asking security teams to do more of the same process. A genuinely enterprise-level, scalable threat modeling process will meet the following criteria:

- It will be driven by the DevOps teams, thereby ensuring integration with their existing Agile methodology, workflow, and toolchains;

- It will enhance InfoSec and OpSec teams’ ability to enforce security policy organization-wide;

- It will provide real-time analysis of the organization’s comprehensive attack surface in a way that allows security teams to drill down to investigate individual threats from their origin and allows CISOs a high-level overview of the organization’s cybersecurity profile;

- It will provide quantifiable insights, measurable results, and yield concrete, consistent, and actionable output for all stakeholders, including reportable financial and performance metrics that sync with the organization’s other strategic initiatives for senior executives.

The 7-step process for developing a mature, scalable threat modeling process outlined herein was developed from years of helping Fortune 1000 companies overcome the limitations with traditional threat modeling processes. The enumerated points are designed to address the specific challenges that are most frequently presented as roadblocks to rolling out an enterprise-level process.
A matured and scaled threat modeling process can transform and prioritize an organization’s entire cyber security effort through

- Providing key insights to attackers’ means, motives and opportunities;
- Identifying and mitigating security weaknesses throughout the DevOps portfolio;
- Driving consistent security policy organization-wide;
- Engaging all stakeholders in role-appropriate, collaborative engagement in the security process; and
- Yielding the data-driven understanding of the organization’s overall cybersecurity profile necessary for security executives to create quantifiable plans with objective results that can be measured over time.

Traditional threat modeling processes have some HOC AD value and are a good start. However, they simply cannot provide the maturity today’s organizations need.
7 Steps to Building a Mature Threat Modeling Process

On a very simple level, everyone agrees that the output of a threat model includes – at a minimum – a list of threats which can be categorized by a rating scheme. This level of output was acceptable a few years ago when threat modeling was done for a few applications on an ad hoc basis. However, today’s organizations need to build threat models for hundreds if not thousands of DevOps initiatives. Moreover, these initiatives will be deployed in a highly interconnected cyber-ecosystem in which applications interact with each other and use shared components like a key management server, single sign on, and so forth. The evolution toward an interconnected cyber-ecosystem is augmented by the move toward cloud deployments and the increasing dependency on the scalability of IaaS and PaaS environments.

As organizations seek to mature their threat modeling process, they have realized that the ad hoc threat modeling process is insufficient not only in its output but also in its capability. A mature threat modeling process, however, will provide organizations with output that goes beyond a list of threats. Scalable threat modeling provides additional information such as attribute-based attacker profiles, per-asset data exposure, impact analysis, threat traceability and much more.

There are seven basic steps to realizing such a matured, scalable threat modeling process which will engage key stakeholders throughout the organization:

**Step 1: Define the Threat Modeling Objectives & Goals**

Before an organization can start building a threat modeling process, it needs to define its desired goals and objectives.

Whatever the organization’s threat modeling objectives and goals, all outputs should lead to the primary goals of reducing overall organizational risk, prioritizing mitigation strategy, and providing a better understanding of the organization’s overall attack surface.

Furthermore, the organization would do well to map threat modeling goals and objectives to the various roll-out stages:

1. Throughout the initial roll-out stage, wherein the stakeholders are understanding threat modeling on the individual DevOps initiative basis, goals and objectives will be concerned with receiving outputs for the DevOps teams. Possible goals may include:
• **Generating a list of threats categorized by priority** – Every threat modeling process promises to provide a list of potential threats. These potential threats may then be further classified by priority, based on the mitigation strategy of the organization. Such classification is required to enable security teams and senior executives the analysis they need to fine-tune their mitigation strategy and deploy security resources.

• **List of relevant mitigating controls for each threat identified** – After identifying potential threats, it is a simple step to provide the appropriate mitigating controls to the DevOps teams. This will include both the high-level security policies and the specific secure coding and implementation checklist. This allows the DevOps teams timely access to the level of information they need to produce secure initiatives initially. It also provides the security team a convenient means to verify the implementation of security policy.

• **A Data exposure report** – A threat modeling process that analyzes one application at a time is an acceptable start. However, if the process scales to incorporate an end-to-end view of the entire operational infrastructure, the security teams will be able to analyze their entire IT environment from the attacker’s perspective. This, of course, is necessary both for determining the exposure of high-value targets to potential attack and providing real-time data for the organization’s ERM policy.

2. As the roll-out progresses, stakeholders should anticipate more useful, actionable outputs from the threat modeling process. At a mid-level roll-out, the threat modeling process will mature to a level such that the security team will be able to prioritize their activities based on a full understanding of the relevant attacker population, the targeted assets and system capabilities, and the organization’s comprehensive attack surface. At this stage the possible objectives may include:

• **Developing a real-time threat portfolio** – Security professionals are well acquainted with the pace with which the threat landscape is evolving and the urgency to identify and assess the impact of new threats. In an enterprise-level threat modeling process, organizations should be able to quickly understand which threat models are affected by the newly identified threats. Decision-makers can then immediately review if and where a potential threat is relevant to their organization and the possible ramifications should the threat be realized.

• **Acquiring the ability to trace threats to their origin across the DevOps portfolio** – From an enterprise perspective, the ability to examine a threat and drill down to its source(s) at the individual application level provides much value for all stakeholders involved. This is especially true when the organization identifies new attack vectors and must determine the appropriate mitigation strategy adjustments across all applications.
Building a Mature, Enterprise-Level Threat Modeling Process in 7 Easy Steps

- **Threat profiling** – Threat profiles provide organizations a contextualized view of the technical and business impact should a potential threat be realized, allowing better precision in mitigation strategy prioritization.

- **Creating a real-time list of top ten threats** – One of the most challenging security tasks is to keep up with the continuously evolving threat landscape. The ability to maintain a real-time rolling list of the top ten threats to the organization – based on real-world, objective data – provides critical insight to the organization’s current security posture. A top-ten rolling list will also provide vital information about the organization’s security policies and contextualized risk posture.

- **Real-time threat intelligence** – A threat model is only as good as the threat intelligence it incorporates. In this respect, the gold-standard will be to keep all threat models up to date with real-time intelligence organization-wide. This allows the organization to instantly identify new high-risk threats as they are introduced into the cyber-ecosystem.

- **Understanding the downstream impact from a shared component** – Increasing interconnectivity means a compromised component will impose an impact to other parts of the cyber ecosystem. Organizations will only achieve the capacity to understand and trace downstream impact as they scale their threat modeling process end-to-end across their entire DevOps portfolio.

- **Tracking the organization’s comprehensive attack surface over time** – The attack surface of an application is a sum of all the ways malicious actors can attack the application’s use cases and thereby progress toward the targeted assets. The organization’s comprehensive attack surface is the expansion of this concept to the entire DevOps portfolio in a unified, cohesive manner. The comprehensive attack surface then becomes an input for understanding and objectively measuring the organization’s overall technological and business exposure associated with the real-time threat profile.

3. At full-implementation the organization should be able to realize and measure the value-add of the threat modeling process on equal footing with the organization’s other strategic initiatives. At full-implementation, all stakeholders throughout the organization are collaboratively involved in role-appropriate threat modeling activities. Thus, the goals and objectives may mature to include:

- **Understanding the strength of implemented compensating controls** – Every security team has limited resources. The ability to understand the unique attacker population faced by the organization is a tremendous advantage in quantifying the strength of existing controls and deploying limited resources. Moreover, an analysis of the comprehensive attack surface relative to the attacker population will indicate if additional compensating controls are required to achieve the requisite security level.
• Driving security policy organization-wide – One of the greatest challenges of cyber security is to drive security policy throughout the organization. While security teams may press the issue, driving security throughout the organization necessarily requires C-level involvement. A matured threat modeling process communicates the organization’s threat posture into familiar financial and strategic terms for senior executives. This allows them to evaluate security policies and the threat modeling initiative on equal footing with other fiduciary concerns.

• Realizing enterprise-wide collaboration – Traditionally securing applications and infrastructure projects is done through an iterative test-remediate-repeat process conducted in a team-specific silo. In an Agile environment with tight deadlines and continuously added business requirements, a team may find it necessary to extend the due date or to petition for a security exception. Undoubtedly, either option impacts the whole organization’s risk portfolio and financial bottom line. A matured and scaled threat modeling process creates enterprise-wide collaboration to align the priorities of Agile DevOps teams, security professionals, and senior executives with the organization’s overall strategic objectives.

• Maturing the threat modeling process into a self-serve model – With a self-serve model, each stakeholder can actively obtain the necessary outputs relative to their role without interfering with or waiting on the interaction of other stakeholders. DevOps teams receive the secure mitigating controls relative to the project upon which they are working without altering their Agile stride. Security teams provide consistent and actionable intelligence to each threat model, monitor the implementation of security policy in real-time, and verify the implementation of mitigating controls during scanning and testing. Senior executives receive high-level, actionable reporting in familiar terms with the capacity to drill down, correlate, and summarize the data at will.

• Create measurable, sustainable reductions in devops production costs – A stated goal of many traditional threat modeling processes is to reduce the high cost of vulnerability remediation by identifying threats during the design phase and mitigating them during the initial coding phase. A matured threat modeling process that is fully scaled will create a measurable and sustainable ROI as DevOps teams drive the threat modeling process and reduce the remediation time and costs on their respective projects.

• Produce a marketable competitive advantage around cyber security – Recent consumer surveys indicate that cyber security is increasingly becoming an important
decision-point for potential clients and customers. A matured, scaled threat modeling process will objectively demonstrate that the organization is proactively taking every reasonable measure to ensure the security of confidential and private information.

**Step 2: Identify the Stakeholders & Assign Responsible Parties**

Threat modeling, like any other strategic initiative, needs to be championed throughout each roll-out stage. The strategic initiative lead person will direct the phased roll-out of the threat modeling initiative and ensure the development of the stated goals and objectives. Of primary concern for this person will be demonstrating the strategic effectiveness of the invested resources and maximizing the initiative’s ROI. One of the first tasks of the strategic initiative lead person will be to choose a technical subject matter expert who understands security. Together these two individuals will promote the technical and business success of threat modeling across the organization.

The strategic lead and technical expert will need to identify the issues involved and hurdles to overcome if the organization’s threat modeling goals are to be met. Certainly discussion will need to include whether or not the threat modeling process will be a part of any existing Agile methodology, the level of participation on the part of the DevOps team, how the threat modeling outputs will be implemented, and how implementation of those outputs will be verified. Furthermore, the leads will need to determine the appropriate level of decentralization of the threat modeling process for each phase of the roll-out and – very importantly – if the roll-out will be limited or global (e.g. covering all DevOps initiatives). The strategic lead and technical expert should meet regularly with the CISO or other security executive throughout these early discussions to ensure the development of the threat modeling initiative aligns with the organization’s overall strategic priorities and direction.

As these stakeholders and process owners are identified, the strategic initiative lead will communicate the scope of each stakeholder’s responsibilities and the targeted time frame for each phase of the roll-out. The strategic lead will need to articulate the skillset or expertise required for each process, and map those skillsets to the various stakeholder groups:

- There must be a stakeholder group or party responsible for curating the relevant, real-world threat intelligence and the appropriate mitigating security controls. Since this party needs to be security subject matter experts, the security team will be a natural fit. Primary responsibilities relative to the threat modeling initiative should include:
  - Developing and maintaining a centralized threat library from which all threat models can access the same threat intelligence;
  - Producing a detailed understanding of the organization’s attacker population based on the attributes required to target the organization’s cyber assets starting from open and unmitigated threats; and
  - Developing, implementing, and verifying the security policy that will effectively mitigate the attacker population’s ability access the organization’s cyber assets;
Building a Mature, Enterprise-Level Threat Modeling Process in 7 Easy Steps

- Updating threat models with each update to the organization’s central threat library.

- If scalability is an organizational goal, a stakeholder group other than the security team should be responsible for creating, modifying, and updating threat models and implementing the relevant security controls. Since this party will benefit greatly from familiarity with the architecture of the various development and operations initiatives and an intimate understanding of the existing Agile methodology and any existing workflows, the DevOps teams should be considered for this role. Primary threat modeling responsibilities may include:
  - Creating threat models for new and existing DevOps initiatives during the initiatives’ design phases;
  - Implementing prioritized mitigating controls during the coding and implementation stages;
  - Verifying the threat models and control implementation during the scanning and testing phases;
  - Modifying threat models as the architecture or business requirements of the DevOps initiatives are periodically updated.

- If the threat modeling process is contemplated as an enterprise-level strategic initiative, then a third stakeholder group will need to be responsible for managing the organization’s comprehensive threat profile and security posture. This party needs to be intimately familiar with the organization’s overall strategic direction, and have the authority to implement policy and changes as needed to achieve the overall threat modeling goals. As such, the natural choice for this role is the CISO or equivalent security executive. Primary areas of responsibility may include:
  - Managing and tracking changes to the organization’s comprehensive attack surface;
  - Measuring the effectiveness of existing controls and quantifying the expectations of new controls;
  - Driving the threat modeling initiative across all stakeholder groups to achieve maximum ROI from the threat modeling initiative and realize the organizational objectives.

**Step 3: Choose a Threat Modeling Methodology and Tool**

Some threat modeling proponents suggest that all threat modeling methodologies are equal. After all, each methodology, at least theoretically, can lead to the identification and enumeration of potential threats. However, the efficacy with which threats are identified, the capacity for scaling, and the outputs which can be realized varies considerably between different methodologies.6 The strategic lead and technical expert will next need to choose an appropriate threat modeling methodology based on the overall goals to be achieved and the capacity for implementation of the identified stakeholders.
Determining a Methodology for the Organization
When selecting a threat modeling methodology, carefully consider the inputs and desired outputs.

- Inputs include, but are not limited to:
  - Developers providing expertise regarding application architecture;
  - Operations teams providing expertise regarding IT system architecture;
  - Security teams providing expertise regarding threat intelligence and mitigating controls;
  - Security executives providing business requirements and organizational strategic direction.

- Desired outputs from step one may include:
  - Technical Outputs
    - Identify & contextually prioritize threats
    - Enumerate the appropriate mitigating controls
    - Create a threat traceability matrix
    - Build and maintain a threat library
    - Develop list of test cases
    - Create a threat exposure report
    - Build an asset exposure report
    - Identify enterprise top 10 threats
    - Enumerate top 10 vulnerable applications
    - Update threat models with every new release and new threat
    - NVD integration
    - Create downstream impact of shared components
    - Develop contextual risk report
  - Organizational Outputs
    - Lower cyber insurance premiums
    - Integrate with and inform ERM team
      - Yield financially reportable metrics
      - Be comparable to other organizational strategic initiatives

Considerations for Selecting the Proper Tool
The organization will next need to choose a tool which can be used to effectively support the methodology to the scale required and which will provide the desired outputs.

One of the pillars of a scalable threat modeling practice is automation. If the threat modeling process is to scale to allow the creation and modification of hundreds or thousands of unique threat models annually, the chosen tool
must be capable of significant automation of the threat modeling process:

- Security’s subject matter expertise must be consistently and uniformly applied to each threat model. Only then will it not be necessary for security personnel to be personally involved in the creation and modification of each threat model.

- The DevOps team can quickly create and modify individual threat models if they have a repository of reusable templates based on frequently used architectural components.

- The ability to chain threat models together – that is, to nest one threat model into another ad infinitum – will automate the analysis and understanding of the organization’s comprehensive attack surface, yielding useful output for security executives.

A second pillar of a scalable threat modeling practice is integration with the organization’s existing workflow and toolchain. Most organizations seeking an enterprise-level threat modeling practice already have a mature SDLC process in place. That process will include various tools for automating the security process of DevOps work at different stages such as CMDB, Developer IDE, Bug Tracking, and so forth. The organization will have invested significant resources maturing these tools, and various stakeholders will be comfortable with their use.

A mature, scaled threat modeling practice will be validated by the use of these existing tools and security processes as the prioritized threats identified by the threat modeling process and addressed during the initial build cycle will not be returned for remedial work. This will greatly reduce or even eliminate the production bottleneck caused by required remediation after scanning and testing.

The third pillar of a scalable threat modeling practice is organization-wide collaboration, requiring a threat modeling tool that encourages and enhances synergistic work across the various stakeholder groups. In a production environment where such collaboration exists, the threat modeling process will scale organically across the entire DevOps portfolio to yield an end-to-end “big picture” of the organization’s comprehensive attack surface.
Step 4: Secure Buy-In from all Stakeholders

Stakeholder buy-in is a transactional exchange. That is, up front stakeholders provide their commitment and support of the threat modeling initiative in exchange for promised benefits they will gain as the initiative rolls out. The up-front request for stakeholders’ time, energy, and commitment may carry a perceived risk. Individual stakeholders must be able to reasonably evaluate the potential benefits to be gained from the threat modeling initiative relative to their role in the organization.

The benefits stakeholders gain will, of course, flow incrementally from the threat modeling methodology and tool selected in the previous step. The benefits should also develop the framework for realizing the desired outcomes established in step one.

Garnering Security Executive Buy-In

The CISO or other security executive will necessarily have a high-level perspective of the threat modeling initiative. If threat modeling is held merely as an SDLC activity, the executive’s goal will be to contain the costs involved – particularly as it involves approval of the threat modeling tool selected – and to ensure that the verification of security issues is appropriately delegated. While such measures may be appropriate for managing an activity or cost-center, it may result in guaranteeing that the threat modeling initiative remains an SDLC cost center rather than an enterprise-level strategic initiative.

Security executives will benefit from an enterprise-level threat modeling initiative at each phase of the roll-out:

- During the initial roll-out phase, the threat modeling initiative’s primary outputs are geared toward the DevOps teams working within an Agile methodology. However, the CISO will receive two key organizational benefits:
  - A high-level data exposure report allowing analysis of the organization’s cyber assets from the prospective of potential attackers. This report provides key insights for negotiating the best cyber insurance premiums and the necessary coverage, and for providing real-time information to the organization’s ERM team.
  - As the various DevOps teams create initial secure applications and projects they will meet tight Agile deadlines without security exceptions. The security executive and ERM team will be able to measure the reduction in carried organizational risk exposure.

- As the threat modeling practice matures into the second roll-out phase, the primary outputs are geared toward the security team. However, the CISO will also continue to realize additional benefits, including:
  - The development of a rolling list of the organization’s top ten threats will help the CISO focus his or her attention on the most serious security issues facing the organization. Because this list of top ten threats is generated from the threat modeling process and not from data of what the cyber defense tools noted, the security executive gains
insight to potential attacks that have yet to happen or to attack patterns that proficiently circumvent the installed cyber defense technologies. By developing a mitigation strategy based the rolling top ten threats, the CISO can develop security initiatives that will quantifiably deliver the largest return on investment.

- The ability to track the organization’s comprehensive attack surface over time will allow the CISO to measure and objectively report to the CFO and the board the security gains made for the resources invested.

- As the roll-out matures to full, organization-wide implementation, the primary outputs are geared toward the needs of the CISO. At this stage the benefits to be gained from the threat modeling initiative include:
  - The ability to understand the strength of implemented compensating controls relative to the attacking population. A detailed analysis of the effectiveness of individual controls and of any implemented defense-in-depth is a tremendous advantage for cost-effectively managing the deployment of resources – particularly if existing controls can be configured or redeployed more effectively than purchasing new controls.
  - Security policy can be driven organization-wide as the organization’s threat posture is communicated to senior executives and the board in more familiar financial and strategic terms. Then security policy, investments, and risks can be evaluated on equal footing with other fiduciary concerns.
  - The CISO’s job is made easier as the threat modeling initiative yields quantifiable insights and enterprise-wide collaboration which aligns the individual stakeholder groups’ role-based priorities with the organization’s overall strategic priorities and objectives.

**Generating Security Team Buy-In**

The security team’s buy-in will likely be the easiest to gain. After all, the purpose of threat modeling is to provide outputs that enhance the organization’s security posture relative to its attacker population and cyber assets.

Nonetheless, an enterprise-level threat modeling practice may still represent a change from status quo, even for the security team. The threat modeling initiative strategic lead will need to communicate to the security team specific benefits which they will receive and which will make the performance of their job more effective. Certainly, an enterprise-level threat modeling practice will need to integrate and enhance security’s existing workflow and tool set throughout each roll-out phase. Specifically, the threat modeling practice should enhance security’s effectiveness to:

- Identify and contextually prioritize potential threats, and to enumerate the appropriate mitigating controls. This will prove particularly effective as the security team develops more detailed understanding of the organization’s attacking population.
• Generate reusable resources available across all threat models, especially building and maintaining a centralized threat library and a list of test cases. Having reusable resources from which all threat models can automatically draw creates a significant efficiency for the investment of security resources and effort.

• Effectively communicate details of the organization’s security posture. Particularly beneficial to the security team will be the ability to create a threat traceability matrix, a threat exposure report, and an asset exposure report. Also beneficial will be the ability to summarize the security and threat details into higher level reports including the ability to identify the top ten vulnerable applications, the downstream impact of shared components, and a contextual risk report.

• Naturally, integration with the NVD, existing bug tracking tools such as JIRA, and any GRC validation processes would be expected. A benefit beyond these that security may not anticipate from an enterprise-level threat modeling process is automated updates to every threat model with every new DevOps initiative release and every new threat added to the threat library.

**Securing Buy-In from the DevOps Teams**

Perhaps the stakeholder group for which securing buy-in for the threat modeling initiative will prove most challenging is the DevOps teams working within an Agile methodology. Traditionally a tension exists between security’s mandate to reduce the organization’s attack surface and business analysts’ mandate for functional products within very tight deadlines. The Agile DevOps team must balance this tension with every initiative undertaken. If the business analyst’s deadline for a functional product is looming, the DevOps team will be pressured to seek an extension to get the project through the testing and scanning. If an extension is disallowed, DevOps will necessarily seek an exception for the project from security at the cost of higher organizational risk.

The solution to ease the tension between the opposing mandates of security and business analysts is a threat modeling process that integrates with the existing DevOps Agile methodology – without a significant increase in their existing workload. The simplicity of this solution may be surprising.

Every DevOps initiative has a design phase in which the application or operations architect whiteboards how the business requirements will be met. The whiteboard outline leads to the specific assignments for each team member. If the selected threat modeling tool provides a canvas or whiteboard functionality for the architectural design phase, then the project design phase doubles as the threat model building stage.

The completed visual diagram will provide the DevOps team the same flow of the new project as a traditional whiteboard process, including all the architectural components to be incorporated into the project. Moreover, because the threat modeling tool’s canvas was utilized as the design whiteboard, the assigned DevOps team should have the relevant security controls immediately as they begin their initial work. Thus the threat modeling process integrated with the existing Agile workflow, creating no additional work or burden for the DevOps team.
Furthermore, because the DevOps team is thereby equipped to create a secure initial product, both the security team’s mandate to reduce organizational risk and the business analyst’s mandate for a functional product on a tight deadline will be realized. The DevOps team may need to invest an additional hour during the design phase discussing their project’s security requirements. However, that hour invested, plus checking off a list as security requirements are implemented, will save the DevOps team 300 remediation hours at the end of the project. The security team’s mandate to reduce organizational risk will be satisfied, as will the business analyst’s mandate to produce a functional product within a specified time frame.

Furthermore, with an enterprise-level threat modeling practice, the DevOps team can increase their production throughput while satisfying competing mandates. Remediation times are reduced or eliminated without the need for security exemptions as mitigating controls are initially implemented. Security teams can objectively measure the decrease in discovered vulnerabilities during testing and scanning – and they can stay on top of the organization’s threat and risk portfolio as new threats are added to the cyber environment. Business analysts receive the ordered project on time, without security exceptions, at or below cost estimates due to the significant reduction or elimination of required remediation efforts. It is a win-win for everyone.

**Step 5: Map Out the Implementation Process**

The next step in developing a mature, enterprise-level threat modeling practice is to map out the implementation process. This is the step in which role-based assignments are given to the various stakeholder groups relative to their expressed commitment to the threat modeling initiative.

The threat modeling initiative technical expert identified in step two can oversee setting up the selected threat modeling tool and ensure that the various stakeholders are equipped to effectively use it.

- **Security teams**
  - Will need to understand how to create a centralized threat library and the list of relevant mitigating controls. It may also be useful if they can document any relevant business or technological impact of potential threats.
The technical expert will need to demonstrate how the threat modeling tool allows security teams to monitor and verify that the appropriate mitigating controls are implemented.

The security teams will also need training on the use of various analysis features of the selected threat modeling tool.

- **DevOps teams**
  
  Of critical importance for integrating the threat modeling tool into an Agile DevOps workflow will be training application and system architects to whiteboard their projects with the threat modeling tool canvas.

  The DevOps team will also need to be trained on how to check off on the tool's list of enumerated security controls that they implemented the required security control.

- **Security executives**
  
  The technical expert will want to show the CISO or other security executives how to gather, understand, and utilize the tool's high-level analysis features. Of particular interest to security executives will be the comprehensive attack surface analyzer, if the tool has such a feature.

  The security executive will need to learn how to evaluate and measure the effectiveness of existing security controls relative to the attributes of the attacking population. The effectiveness of a particular security control will be determined by its ability to inhibit members of the attacking population to access specific cyber assets. The security executive will need to evaluate the effectiveness of existing controls as a single IT environment component and for their defense-in-depth contribution.

  The technical expert should also demonstrate how the threat modeling tool will provide quantification for proposed security initiatives and facilitate communications with senior executives and board members.

While the technical expert trains the stakeholder groups on how to use the selected threat modeling tool such that each group can maximize the role-based benefits received, the strategic initiative lead will map out the specific roll-out phases with the approval of the CISO or other security executive. It will be very important in this process to include the following points in the roll-out plan:

- A defined, reasonable, and obtainable implementation scope. Providing obtainable and reasonable scope of each roll-out phase is critical to realizing the desired outcomes enumerated in step one. Including too large a scope for each step will inhibit the stakeholder’s ability to incorporate the necessary process changes. Creating too small a scope for each step will not provide sufficient outputs to measure the effectiveness or efficiency of the roll-out.
• Each roll-out phase should include measurable KPIs and KRIs with a defined, objective standards of success. Only by including these will the strategic initiative lead and security executive have a basis to quantify the stakeholders’ experience with the threat modeling tool, methodology, and overall threat modeling initiative.

• A timeline for the initiation of each roll-out phase, and a proposed date for the completed evaluation of the threat modeling initiative. Mapping the roll-out phases and completed initiative evaluation to specific dates will promote continued deployment of each roll-out phase, including any necessary modifications, expansions, or improvements to the initiative based on stakeholder experience. Without timeline mapping, unforeseen challenges may lead to the threat modeling initiative stalling in an immature stage – resulting in a failure to achieve the desired outcomes enumerated in step one.

Finally, the strategic initiative lead will need to secure ongoing contingent support from the threat modeling tool vendor to ensure that each stakeholder group receives maximized benefits and that any unforeseen issues or questions are appropriately handled.

Step 6: Deploy the Threat Modeling Process in a Phased Roll-Out
Depending on the results of the preceding steps, the threat modeling initiative may be rolled out in two, three, or more phases. The most important activities for the strategic initiative lead to promote ongoing initiative success during each roll-out phase are

• Gathering and summarize the stakeholders’ experience from the preceding phases – in particular, evaluating the implementation plan for necessary modifications or improvements, and determining if the various stakeholders are realizing incremental increases in their expected benefits.
• Measuring the results obtained from the threat modeling initiative to the KPIs and standards enumerated in step five. It may also be useful at each phase to perform a side-by-side tool and methodology comparison to validate the work done in step three. Specific comparative studies may include
  o In-house comparisons of similar projects with similar business requirements utilizing different threat modeling tools and methodologies;
  o Summarizing qualitative evaluations from stakeholders relative to the initiative goals and objectives enumerated in step one;
  o Analyzing DevOps teams’ time to project completion. An effective analysis will include an averaged baseline completion time using the existing processes versus the completion times utilizing different tools and methodologies.

• Ensure that each stakeholder group understands their respective role-based scope for the upcoming phase.

In addition, it may prove beneficial during the limited roll-out phases for the strategic initiative lead to review case studies of other clients of the threat modeling tool to see how their roll-out experience compares.

The last, global roll-out phase should include a final selection of the threat modeling tool and methodology, full role-based training of the stakeholder groups, and a plan to transition from the organization’s existing process to a scalable process with each new DevOps initiative.

CHECK FOR INITIATIVE SUCCESS AT EACH STAGE OF THE ROLL-OUT.
Step 7: Measure, Measure, Measure

The ultimate standard of success for any strategic initiative is how well it produces the desired outcomes. While the nature of some outcomes may require qualitative evaluation, the strategic initiative lead and CISO should develop quantitative measures and metrics to evaluate the initiative outcomes whenever possible.

Of course, telling a convincing story with quantitative measures and metrics requires that the appropriate measurements are taken before implementing the threat modeling initiative, and then repeated over time throughout the roll-out process. Potential quantitative measures and metrics in addition to those derived from the desired outputs enumerated in step one may include:

- **Reduction in time for completion of DevOps initiatives.** Closely related will be the number of vulnerabilities discovered during scanning and testing, the average DevOps team throughput, and the profitability (or total cost) of DevOps initiatives. The difference (if any) in the average time for DevOps teams to complete initiatives as impacted by comparative threat modeling initiatives provides partial input data for the ROI of each threat modeling process.

- **Total cost of ownership of threat modeling tools and processes.** The initial or annual cost of a threat modeling tool is not the whole picture. A full analysis of any threat modeling process necessarily includes the total cost of ownership (tool cost plus the cost of resources to utilize that tool) and the cost of ownership per applied per DevOps initiative. Such an analysis provides a true, level comparison between threat modeling processes with different tools and methodologies, and provides another data-driven input for the ROI of threat modeling.

- **Total number of unique threat models that can be created annually.** Scalability is a primary underlying issue in creating an enterprise-level threat modeling practice. Different threat modeling methodologies and tools will provide varying levels of automation, integration, and
A mature, enterprise-level threat modeling process is within reach. Operating in today’s highly interconnected cyber-ecosystem is a given for contemporary enterprises. The interconnectivity produces tremendous value and efficiencies – but it also exposes organizations to a plethora of new potential threats on a daily basis. The only threat modeling process which can realistically meet the expanding needs of enterprise-level organizations is one that matures to a self-service model. Then the threat modeling process can organically scale end-to-end across the organization’s entire IT environment.

If an organization develops a mature, enterprise-level threat modeling process utilizing the steps enumerated in this paper, it will have the data-driven results it needs to demonstrate the efficacy of the threat modeling initiative. The gains in overall DevOps efficiency from initial design to production will be measurable. The reduction in the organization’s attack surface will be trackable over time. Moreover, the financial returns of the threat modeling initiative will be able to stand on equal reporting footing with the company’s other strategic initiatives.

A mature, enterprise-level threat modeling process, built upon the VAST methodology and powered by the ThreatModeler™ tool, can be realized by your organization.

For more information or to schedule a demo, please visit www.threatmodeler.com
Building a Mature, Enterprise-Level Threat Modeling Process in 7 Easy Steps

Additional Reading

- Data Flow vs. Process Flow Diagramming
- Application Threat Models vs. Operational Threat Models
- Centralized Threat Library
- Threat Modeling Methodology
- Three Pillars of a Scalable Threat Modeling Practice
- Attack Surface Analysis
- Four Key Reasons Why CISOs Need Threat Modeling
- Seven Benefits of Continuous Threat Modeling

About the Author

Anurag “Archie” Agarwal, CISSP, is the Founder & CEO of ThreatModeler, Chief Technical Architect of the ThreatModeler™ product, and the principle author of the VAST (Visual, Agile, and Simple Threat modeling) methodology. Archie has more than 20 years of real-world experience in threat and risk analysis and has been instrumental in the successful implementation of secure software development processes at a number of Fortune 1000 companies, thereby minimizing their exposure to cyber threats and improving their ability to mitigate risks. Before founding ThreatModeler, he was the Director of Education Services at WhiteHat Security.

With his advanced technical knowledge of application architectures and technologies, Archie has developed the VAST methodology - a ground-breaking threat modeling methodology which enables organizations to establish a practical and predictive mitigation posture against cyber threats and other risks to their applications, information, and infrastructures. This methodology addresses many of the shortcomings of the traditional application SDLC security process, and forwards significant improvements over other historical threat modeling approaches. Using the VAST methodology as a basis, Archie has implemented cost-efficient processes for potential threat detection and mitigation for enterprises within the financial, medical, and IoT industries.

ThreatModeler, established in 2010, is a leading threat modeling company providing guidance and practical methodology to organizations seeking end-to-end threat modeling solutions and seamless integration of application threat modeling into the entire SDLC initiative. ThreatModeler’s mission is to empower CISOs, security architects and analysts, project managers, and other stakeholders to proactively and efficiently align contextualized threats with strategic business objectives in a collaborative and interconnected organizational ecosystem.

The ThreatModeler™ product, is the first enterprise-level threat modeling software that enables professionals to identify, classify, prioritize and mitigate threats. The ThreatModeler™ process establishes a new standard for practical threat modeling. Its intuitive, easy-to-use interface allows security and non-security experts to build a comprehensive threat model in minutes. The robust process
and consistent, forward-thinking design is fueled by a team of threat modeling experts specializing in cyber security. ThreatModeler™ initiates a fundamentally new process that enables organizations to seamlessly integrate threat modeling into their application development process and infrastructure security measures.

ThreatModeler™ is utilized by leading Fortune 1000 companies in the financial, medical and IoT industries. It empowers security architects, application security directors, chief information officers, and other decision makers to plan better, prepare, and proactively protect themselves from attackers. By providing enterprises and security professionals with everything they need to test and remain abreast of current and future threats for new application and system developments, organizations utilizing ThreatModeler™ have reduced the cost of fixing production vulnerabilities by as much as 80% or more.

---
