ThreatModeler® + IriusRisk

Whitepaper

Threat Modeling Maturity Model

A Practical Framework for Advancing Secure by Design

Executive Summary

Threat modeling is one of the most effective design-time security practices. It identifies how systems can be attacked, reveals architectural weaknesses, and guides teams toward safer design decisions before any code is written or cloud resources are deployed. Yet organizations often struggle to scale threat modeling: practices are inconsistent, models are created too late, and tooling investments focus heavily on reactive scanning rather than proactive design assurance.

To help organizations modernize effectively, this whitepaper introduces the **Threat Modeling Maturity Model**, a practical framework that enables teams to:

1. Evaluate the current state of their threat modeling practice.
2. Understand the capabilities required for Secure by Design.
3. Identify clear steps to advance maturity.
4. Integrate threat modeling alongside cloud, AI, and DevOps.
5. Maximize the value derived from design-time security.

The model outlines four maturity stages: **Emerging, Scaling, Leading, and Continuous Secure by Design**. It also evaluates progress across five dimensions: Coverage & Scope, Method & Consistency, Integration & Collaboration, Governance & Reuse, and Outcomes & Value Realization.

This framework is designed to help CISOs, CIOs, architects, platform leaders, and product teams understand where they stand today and build a roadmap toward continuous, architecture-driven security.

The ThreatModeler Advantage

ThreatModeler supports organizations at every maturity stage, from early exploratory modeling to **continuous, cloud-integrated Secure by Design**, without requiring a disruptive transformation.

Why a Threat Modeling Maturity Model Is Needed

Modern engineering environments are fast-moving and complex. Applications consist of microservices, APIs, serverless functions, data pipelines, ephemeral cloud resources, and third-party integrations. Architecture evolves constantly. AI accelerates development, while attackers increasingly target design patterns rather than individual vulnerabilities.

These conditions expose the limits of purely reactive security practices.

In most organizations, vulnerability scanning has become the first line of defense, as *manual* threat modeling has failed to keep pace with modern development practices. ASPM, CSPM, SAST, DAST, IaC scanning, and cloud posture tools are important, but they all share a fundamental limitation: They operate *after* architecture and design decisions are already made.

Even with extensive scanning, teams still encounter challenges such as:

Critical issues are discovered too late

Higher remediation costs

Review cycles slow delivery

These delays also mean architectural flaws go unnoticed, and findings often generate noise rather than clarity, making it harder to prioritize true risks.

To compensate, some teams turn to generative AI in hopes of accelerating threat identification by creating “threat models.” But without architectural context (data flows, dependencies, trust boundaries), AI produces:

Long lists of generic threats

Compliance-style checklists

Inconsistent or hallucinated results

This is simply **checklist security at scale**, not true threat modeling.

Why the Maturity Model Matters

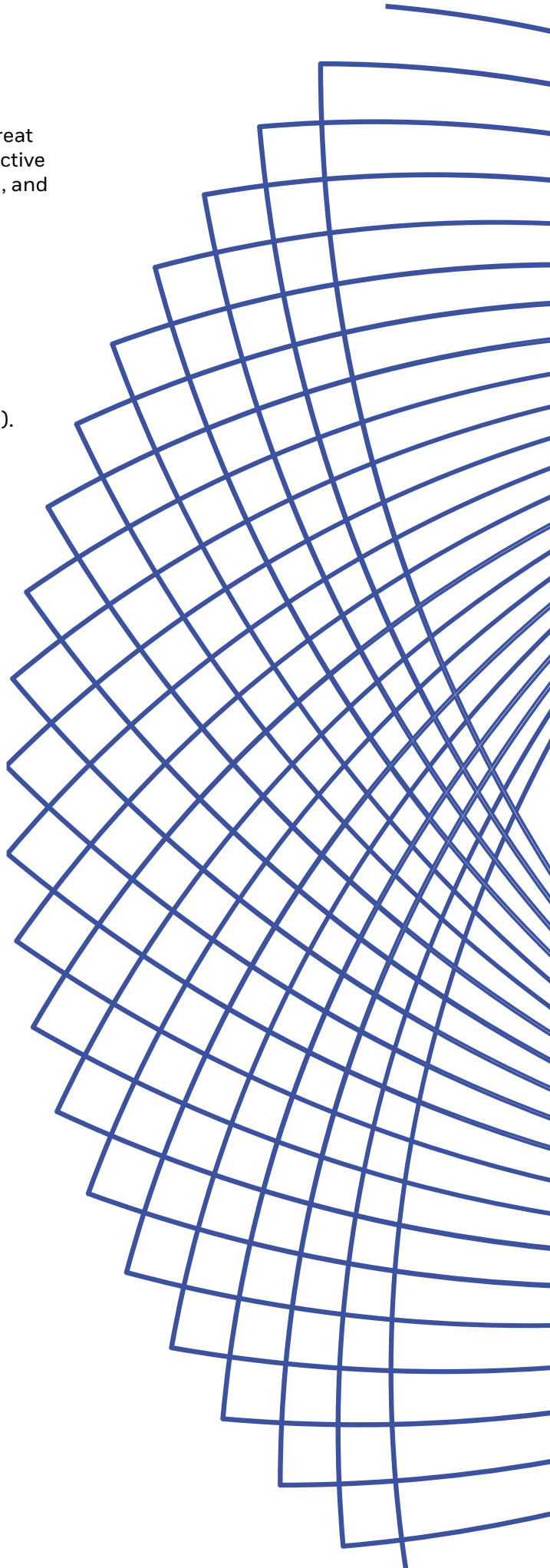
These challenges reveal why a structured approach is needed. Threat modeling is not a binary capability. Organizations evolve from reactive detection to checklist-driven processes, to architectural modeling, and ultimately to continuous Secure by Design.

A structured maturity model helps organizations:

1. Understand their current state.
2. Avoid false summits (like checklist-based automation).
3. Prioritize impactful next steps.
4. Build alignment between security and engineering.
5. Measure progress across meaningful dimensions.

The ThreatModeler Advantage

ThreatModeler provides the structured modeling, reusable content, and automation that help organizations progress efficiently through each maturity stage.



Threat Modeling as the Foundation of Secure by Design

Secure by Design requires several foundational capabilities:

Architectural visibility

Early identification of structural weaknesses

Repeatable design guardrails

Integrated workflows across engineering and security

Organizations must also account for drift over time and rely on augmented intelligence that supports decision-making at scale. These capabilities only emerge when security is anchored in a clear understanding of system architecture: how components interact, how data flows, and where trust boundaries are established.

Threat modeling is the foundation that enables all of these outcomes.

It shifts security from:

1. Runtime detection → **design-time prevention**
2. Late-cycle rework → **early clarity**
3. Generic checklists → **architecture-driven insight**
4. Siloed security → **collaborative decision-making**

By grounding security discussions in real architecture rather than assumptions or checklists, threat modeling provides the structure that Secure by Design depends on. It gives teams shared visibility, a common language, and a systematic way to evaluate risk early, long before code is written or cloud resources are deployed.

Organizations adopt Secure by Design by advancing through the maturity stages described below, strengthening **architecture-first collaboration** at each step.

The Threat Modeling Maturity Model

This model describes four maturity stages and the capabilities required to progress from one to the next. As businesses mature through the stages and strengthen Secure by Design adoption, the value and impact of threat modeling increase.

Every organization begins at a different point in this journey. The goal is not to reach the highest stage immediately, but to understand the path forward and identify the most impactful next steps.

Each stage represents meaningful progress toward a more consistent, architecture-driven Secure by Design practice.

How to Use This Model

Use this model as a lens for honest self-assessment, not as a compliance score. Most organizations will find themselves at different stages across the five dimensions, and that variability is expected. First, identify the stage that best reflects your current state, then use the dimension-level descriptions and roadmap guidance to choose a small number of practical improvements. The objective is steady progress toward more architecture-driven, continuous practices rather than a rush to achieve Continuous Secure by Design in a single step.

Stage 1: Emerging

At this early stage, threat modeling begins to take shape, often through **manual, inconsistent, or reactive efforts**. Security typically engages late in the lifecycle, relying on scanning tools to identify issues after design decisions have been made. AI usage is ungoverned and produces generic lists rather than architectural insight, but it signals the organization's first attempts to explore automation.

Typical Stakeholders and Roles

Security architects and security analysts:
Perform threat modeling on an ad hoc, manual basis.

Developers:
Not actively involved in threat modeling; typically only engaged when severe issues are escalated late.

Executives:
Minimal awareness; threat modeling is viewed as a tool experiment rather than a strategic practice.

How AI fits at This Stage

Unstructured, prompt-based AI is occasionally used by security staff but remains unguided and inconsistent.

Characteristics

- Modeling is inconsistent.
- Only a few critical systems are reviewed.
- No clear prioritization or architectural criteria.
- High dependency on individual SMEs.
- Security is perceived as a late-stage blocker.
- Vulnerability scanning drives risk decisions.

Where Maturity Begins to Develop

Even at the Emerging stage, organizations start to recognize the value of architectural visibility and earlier collaboration. This awareness becomes the catalyst for progressing toward more structured, scalable practices.

Stage 2: Scaling

As organizations progress into the Scaling stage, they introduce templates, checklists, or AI-generated lists to add structure. This marks a significant advancement: teams expand coverage, improve documentation, and begin establishing repeatable patterns.

However, because these approaches are not yet grounded in architecture, they can create a **false sense of maturity**, an impression of efficiency that doesn't translate to deeper security insight.

Typical Stakeholders and Roles

Central Product Security Architects:
Define standard threat modeling checklists, templates, and early review workflows.

Functional Security Architects:
Gather information and complete checklist-based threat assessments within their domains.

Developers:
Respond to findings and provide evidence of remediation, but are not yet involved in architectural reasoning.

Solution and Application Architects:
Share architecture diagrams and participate in early, structured reviews.

Executives:
Awareness increases through shift-left initiatives, but sponsorship remains limited.

How AI fits at This Stage

Prompt-based AI is used to generate threat or requirements lists, but output remAIns ungoverned and disconnected from architecture.

Characteristics

- More system coverage, but shallow depth.
- Lists, spreadsheets, and requirement templates dominate.
- Security communicates earlier, but still reacts to designs.
- Rework persists because architecture is not evaluated.
- Teams hit diminishing returns from checklist security.

Case Example: Escaping the Checklist Trap

One engineering organization adopted a checklist-based threat modeling approach because it seemed faster and easier. Teams applied the same list of generic threats to every component and evaluated them for relevance.

It quickly became unscalable.

Two patterns emerged:

1. **"Check-the-Box" Security**
   Teams completed lists without deeply assessing design, leading to security theater rather than meaningful evaluation.

2. **"Groundhog Day" Security**
   Every project repeated the same generic threat evaluation without accumulating learning or speed.

Progress stalled. Teams were overwhelmed.

When they shifted to architecture-aware, AI-assisted threat modeling, everything changed. Threats were mapped automatically based on real architecture, irrelevant threats disappeared, and reviews focused on the decisions that mattered most. Teams broke out of repetitive work cycles, and threat modeling accelerated instead of slowing down.

This is the heart of the Scaling stage:
Recognizing checklist approaches as a false summit and preparing to move toward architecture-driven practices.

Where Maturity is Heading

By this stage, organizations begin to understand that consistency must evolve into **architectural clarity**. This realization becomes the catalyst for advancing into the Leading stage. As organizations move beyond checklist-driven approaches, they also begin to understand where AI can meaningfully contribute, not by generating generic lists, but by enhancing architecture-aware modeling as maturity increases.

Stage 3: Leading

In the Leading stage, organizations adopt **architecture-driven threat modeling** as a standard practice. Security becomes a partner, engaging earlier in the process rather than reacting to late-stage findings. Engineering, architecture, and cloud teams collaborate using shared models, and AI becomes governed, consistent, and context-aware, supporting deeper insight without replacing architectural reasoning.

Typical Stakeholders and Roles

Central Product Security Office:
Defines standardized blueprints, templates, and reusable patterns for architecture-driven threat modeling.

Functional Security Architects:
Apply these patterns within their product domains and support architecture-first modeling.

Application Security Teams:
Use threat models to guide targeted testing and validation.

Business Application Owners:
Establish application criticality and ensure threat modeling aligns with business priorities.

Developers:
Engage earlier in the lifecycle and contribute to modeling discussions as part of standard design and implementation work.

Executives:
Provide sponsorship that reinforces architecture-driven practices as the organization scales.

How AI fits at This Stage

Governed, context-aware AI assists with summarization and pattern recognition, grounded in architecture.

Characteristics

- Architecture is the starting point for threat modeling.
- Automated threat and mitigation mapping is standard.
- Models support design reviews and engineering trade-offs.
- Teams collaborate across functions.
- Reusable components, patterns, and libraries improve consistency.

Case Example: Early Collaboration That Accelerated Delivery

A product team resisted adding threat modeling to the design stage, fearing it would introduce delays and rework. Historical security reviews had conditioned them to expect late-breaking issues and friction.

But when they piloted **architecture-driven threat modeling** early in design, with security architects included from the outset, they discovered the opposite.

Threat modeling:

1. Simplified the architecture.
2. Revealed unnecessary components.
3. Clarified data flows and trust boundaries.
4. Identified low-effort mitigations early.
5. Eliminated rework that typically surfaced late.
6. Increased confidence during architecture review.
7. Strengthened collaboration across teams.

Instead of slowing them down, threat modeling became the accelerator that helped them deliver faster. Teams described it as **“finding the shortcut through the design phase.”**

This is the essence of the Leading stage:
Security and engineering co-designing systems for both safety and speed.

Where Maturity is Heading

Reaching this stage positions organizations to evolve from periodic modeling to **continuous assurance**.
With architecture-driven practices established, they are ready to integrate threat modeling directly into cloud and CI/CD workflows, unlocking true Continuous Secure by Design maturity.

Stage 4: Continuous Secure by Design

In the Continuous Secure by Design stage, threat modeling becomes continuous and deeply integrated into cloud workflows, CI/CD pipelines, and runtime tools. Architecture models update automatically as systems evolve, ensuring that teams always work from accurate, current insight. AI becomes **deterministic**, **governed**, and **deeply contextual**, supporting continuous analysis and helping teams understand the impact of every change in real time.

Typical Stakeholders and Roles

Business Application Owners:
Ensure continuous threat modeling supports business priorities and criticality.

Central Product Security Office:
Maintains governance, reusable patterns, and AI usage guidelines across teams.

Enterprise Architecture:
Ensures threat modeling remains aligned with target architectures and modernization plans.

Governance, Risk, and Compliance (GRC):
Aligns continuous modeling with risk criteria, regulatory needs, and audit processes.

SDLC Owners:
Integrate threat model findings into everyday development workflows and CI/CD processes.

Application Security / Penetration Testers:
Use models to inform test cases and validate architectural risks.

Product Management / Engineering Teams:
Maintain models as part of daily workflows and evaluate changes through automated updates.

Developers:
Use continuously updated models to validate implementation choices and proactively address risks.

Executives:
Provide enterprise-level sponsorship and visibility at the board level.

How AI fits at This Stage

Deterministic, context-aware AI supports impact analysis, continuous analysis, summarization, and continuous review under enterprise governance.

Characteristics

- Threat models update automatically with architectural changes.
- Cloud configuration sources (including IaC repositories), cloud deployments, and pipelines drive continuous assurance.
- Drift detection identifies deviations from intended design.
- Security policies and patterns enforced through automation.
- Runtime scanning validates design expectations.
- System-wide governance and reuse create compounding value.

Case Example: Continuous Modeling Accelerates Cloud Transformation

A major financial institution set aggressive deadlines for a large cloud transformation effort. Initial concerns were that threat modeling would slow progress and become a blocker.

But once they integrated ThreatModeler with their cloud provider and IaC workflows, threat modeling became one of their key accelerators.

Cloud architectures and IaC templates were:

1. Modeled automatically as they were built.
2. Evaluated for threats and mitigations in real time.
3. Compared against evolving cloud infrastructure to detect drift.
4. Automatically triggering reviews when discrepancies emerged.

Instead of modeling after deployment, threat modeling and cloud architecture evolved together, creating **a continuous, shared source of truth**.

Security became a partner, not an obstacle. Engineering moved faster with confidence. Drift detection kept systems aligned with intended design.

Threat modeling no longer slowed transformation; **it enabled it**.

This is the Continuous Secure by Design stage:
Threat modeling integrated deeply into engineering, DevOps, and cloud workflows, **continuously adapting to change**.

Where Maturity Comes Together

At this stage, organizations realize the full potential of Secure by Design: a self-updating, architecture-driven security practice that reduces risk, accelerates delivery, and provides continuous assurance across complex, rapidly evolving environments.

The Five Dimensions of Threat Modeling Maturity

The five dimensions of threat modeling maturity offer a practical way to assess how your organization approaches design-time security today, and where growth will create the greatest impact. Each dimension reflects a critical aspect of Secure by Design, from visibility and consistency to collaboration, governance, and measurable outcomes.

Viewed collectively, the dimensions highlight both strengths and opportunities for growth, helping organizations identify the most meaningful next steps in their journey toward Continuous Secure by Design.

1 Coverage & Scope

This dimension reflects how broadly and deeply an organization models its systems and where architectural visibility currently exists. As coverage expands and becomes more architecture-based, threat modeling delivers higher-value insight and supports more consistent Secure by Design practices.

Emerging

- Only a few critical systems are modeled.
- Architecture visibility is limited.
- Scanning, rather than design intent, drives priorities.

Scaling

- More systems are analyzed, but models remain shallow.
- Architecture is captured inconsistently.
- API and cloud coverage are incomplete.

Leading

- Architecture-based modeling is applied across key applications.
- Clear criteria guide for what gets modeled.
- Cloud designs and deployment configurations consistently included.

Continuous Secure by Design

- Modeling extends across the full portfolio.
- Cloud integrations and deployment sources automatically update models.
- Runtime tools validate expected security controls in real time.

How This Dimension Drives Maturity

As organizations expand coverage from a handful of critical systems to full, architecture-based visibility, threat modeling becomes a **consistent source of truth**, supporting earlier collaboration, better prioritization, and continuous assurance.

2 Method & Consistency

This dimension evaluates **how systematic, governed, and repeatable** an organization's threat modeling approach is. As methods evolve from manual diagrams to architecture-driven automation, results become more predictable, auditable, and aligned with Secure by Design.

Emerging

- Manual diagrams and whiteboards.
- No standard method.
- AI-generated lists used inconsistently.

Scaling

- Templates and checklists add structure.
- Processes vary across teams.
- AI generates lists, but lacks architectural grounding.

Leading

- Automated threat and mitigation mapping.
- Architecture-driven models guide design discussions.
- Governed, context-aware AI improves consistency.

Continuous Secure by Design

- Workflows become fully automated.
- Architecture-as-data ensures consistency.
- Deterministic AI assists continuous assurance.

How This Dimension Drives Maturity

Advancing along this dimension transforms threat modeling from a manual, variable activity into a **governed, repeatable practice**. Consistency enables teams to trust the process, eliminate rework, and apply Secure by Design principles reliably across the organization.

3 Integration & Collaboration

This dimension reflects **how well threat modeling fits into everyday engineering workflows** and how effectively security, development, and architecture teams collaborate. As integration deepens, threat modeling becomes a natural part of design and delivery, not an external review.

Emerging

- Security consulted late.
- Threat modeling outside normal workflows.
- CI/CD integrates scanning, not modeling.

Scaling

- Early sharing of requirements.
- Limited architectural collaboration.
- AI is used for documentation, but not decision-making.

Leading

- Threat modeling is integrated into design reviews and DevOps processes.
- Cross-functional collaboration around shared models.
- Scanning findings mapped back to architecture.

Continuous Secure by Design

- Embedded into CI/CD and cloud workflows.
- Cross-team collaboration is automated.
- AI supports impact analysis and continuous review.

How This Dimension Drives Maturity

As threat modeling becomes embedded in design, development, and deployment workflows, teams shift from **reactive coordination to shared ownership**. Integration reduces friction, improves delivery speed, and strengthens the alignment needed to support Secure by Design at scale.

4 Governance & Reuse

This dimension captures how well organizations manage, govern, and reuse the knowledge generated through threat modeling. As governance strengthens, teams build on prior work instead of starting from scratch, and insights become more consistent, scalable, and strategically valuable.

Emerging

- No reusable libraries.
- Each model is built from scratch.
- Findings inconsistently documented.

Scaling

- Basic reuse of documents or templates.
- Libraries exist, but are unmanaged.
- AI output is inconsistent and ungoverned.

Leading

- Central libraries of threats, mitigations, and patterns.
- Purple-team and pentest insights incorporated.
- AI enriches reusable components with context.

Continuous Secure by Design

- Enterprise-wide governance.
- Drift detection and guardrails enforce patterns.
- Continuous learning across runtime, cloud, and architecture.

How This Dimension Drives Maturity

Progress in governance and reuse turns threat modeling into a **compounding capability**. When organizations standardize libraries, incorporate real-world insights, and enforce guardrails, every model becomes faster to build, more consistent, and more aligned with enterprise design patterns, accelerating Secure by Design across teams.

5 Outcomes & Value Realization

This dimension focuses on the measurable impact of threat modeling: how effectively the practice reduces risk, improves delivery, and strengthens confidence across engineering and security. As organizations progress, outcomes shift from reactive issue discovery to predictable delivery and clear, continuous value.

Emerging

- Late-stage issues are common.
- Security is perceived as a blocker.
- Delivery timelines unpredictable.

Scaling

- Documentation improves.
- Rework decreases, but persistent design flaws remain.
- Efficiency gains are limited.

Leading

- Fewer late-stage defects.
- Predictable and more successful delivery.
- Stronger collaboration and shared trust.

Continuous Secure by Design

- Measurable risk reduction.
- Faster delivery and modernization.
- Lower remediation cost.
- Clear auditability and architectural assurance.

How This Dimension Drives Maturity

Advancing through this dimension transforms threat modeling from a process into a **strategic enabler**. As outcomes become more predictable and measurable, organizations gain confidence in their designs, accelerate delivery, reduce cost, and demonstrate the value of Secure by Design across the business.

From the “Department of NO” to the “Department of KNOW”

Early-stage security teams often operate with limited architectural visibility and reactive insight. Without a clear understanding of how systems are designed, the safest answer often becomes “no,” leading to friction and reinforcing the belief that security slows progress.

As organizations mature across the five dimensions, this dynamic begins to change:

1. Architecture becomes visible.
2. Threats become predictable.
3. Cloud configuration guardrails operationalize security controls.
4. AI provides consistent, context-aware insights.
5. Governance aligns design, engineering, and security.

These advancements replace last-minute scrutiny with **shared understanding**. Security becomes a partner in shaping design rather than a blocker responding to it.

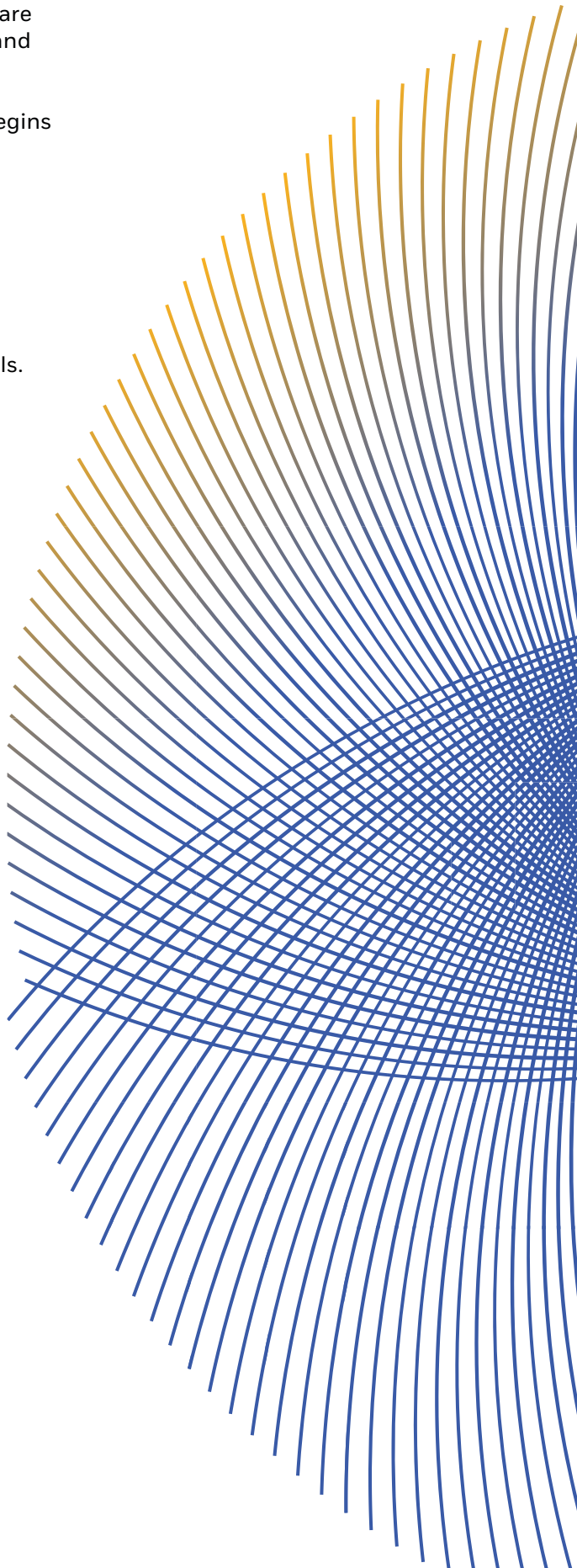
Security transforms from:

The Department of NO (reactive gatekeepers)

into:

The Department of KNOW (informed partners enabling safe, fast delivery)

Threat modeling maturity is what makes this transformation real, shifting from late-stage decisions to early, architecture-driven collaboration that **accelerates both safety and speed**.



Threat Modeling Maturity Assessment

Use the following assessment to understand your organization's current maturity level across the five dimensions. There are no wrong answers. Each level represents a valid point on the journey toward Secure by Design. Review your selections across the five dimensions and note which stage appears most frequently. This provides your maturity baseline. Most organizations find it helpful to identify one or two dimensions to strengthen first rather than trying to advance all areas at once.

Coverage & Scope

A = Limited; scanning-driven.
B = Broad but shallow.
C = Architecture-based
D = Continuous via cloud and CI/CD integration.

Method & Consistency

A = Manual.
B = Templates/lists.
C = Architecture-driven and automated.
D = Fully automated; pattern-driven.

Integration & Collaboration

A = Security involved late.
B = Partial collaboration.
C = Integrated into design reviews.
D = Embedded into CI/CD and cloud workflows.

Governance & Reuse

A = None.
B = Limited reuse.
C = Centralized libraries.
D = Enterprise governance and drift detection.

Outcomes & Value

A = Late issues.
B = Moderate improvement.
C = Predictability and fewer defects.
D = Faster delivery, modernization ROI, measurable reduction in risk.

Interpretation

Mostly As ⟶ Emerging.
Mostly Bs ⟶ Scaling.
Mostly Cs ⟶ Leading.
Mostly Ds ⟶ Continuous Secure by Design.

This quick assessment helps teams recognize strengths, uncover gaps, and establish a shared view of their current state, enabling alignment to move confidently to the next stage of maturity.

Building Your Roadmap

Your maturity assessment highlights where your organization stands today. Use those results to identify the most impactful next steps. The goal is not to advance every dimension at once, but to choose a practical set of improvements that move you steadily toward Secure by Design. Each stage below outlines the actions that typically create the most significant progress.

If Emerging:

Focus on establishing visibility and moving away from reactive processes.

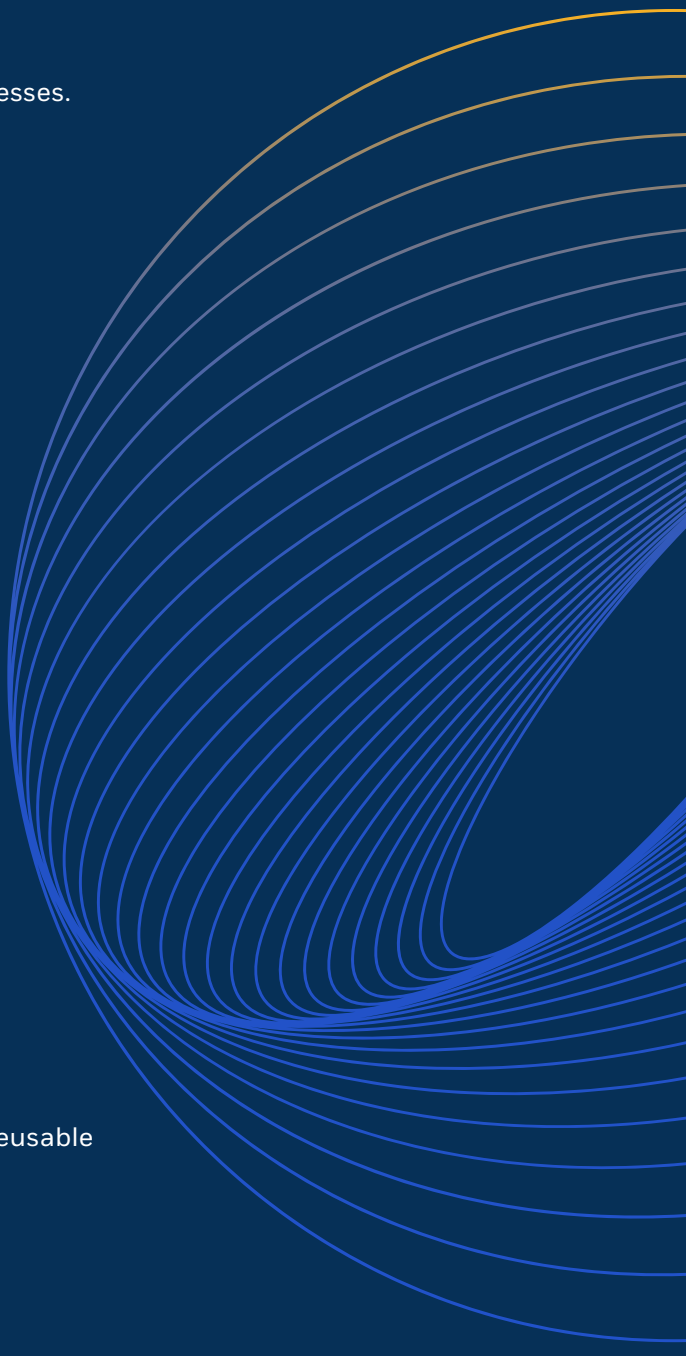
1. Reduce dependence on scanning as first-line discovery.
2. Avoid using AI for generic, uncontextualized threat lists.
3. Begin modeling a few key systems using shared patterns.
4. Establish architectural visibility across critical workflows.

At this stage, improving architectural visibility almost always unlocks the most meaningful uplift.

If Scaling:

1. Move beyond templates and checklists.
2. Adopt architecture-driven modeling.
3. Develop reusable libraries.
4. Connect threat modeling with cloud and delivery teams.

Most organizations gain the fastest traction here by standardizing reusable components and shifting from lists to architecture.



If Leading:

Focus on embedding threat modeling directly into engineering workflows.

1. Integrate threat modeling into CI/CD and design workflows.
2. Use governed, architecture-aware AI.
3. Standardize reusable components and patterns.
4. Map scanning results to architecture.

At this stage, consistency and integration start to compound, enabling teams to collaborate more effectively and reduce rework.

If Continuous Secure by Design:

Reinforce automation, governance, and enterprise-wide alignment.

1. Treat scanning as validation, not discovery.
2. Implement deterministic AI for continuous assurance.
3. Strengthen KPIs, governance, and enterprise alignment.
4. Scale Secure by Design to full portfolio coverage.

Organizations operating at this level benefit from expanding continuous practices across all systems and maintaining architectural accuracy through integrations and drift detection.

Supporting Research

This Threat Modeling Maturity Model is informed by applied research into architecture-driven security, intelligent automation, and the responsible use of AI in Secure by Design programs. The following white papers expand on key concepts introduced throughout this model:

Intelligent Threat Modeling: A New Era of Secure by Design

Examines the evolution from manual and automated threat modeling to Intelligent Threat Modeling. The paper defines the foundational requirements needed to support Secure by Design at scale, including architecture-aware modeling, guided security insights, continuous risk awareness, and enterprise-wide visibility across cloud, infrastructure, and applications.

Operationalizing AI in Threat Modeling

Explores the risks and limitations of ungoverned, prompt-based AI in security and introduces a structured approach to using AI responsibly. The paper explains why threat modeling requires determinism, governance, and architectural context, and how AI can be operationalized to extend expert judgment without replacing it.

Conclusion

Threat modeling is the discipline that transforms security from **reactive and checklist-driven** to **proactive, architectural, and continuous**. But no organization reaches that level overnight.

The Threat Modeling Maturity Model provides a clear roadmap from:

Emerging ⟶ Scaling ⟶ Leading ⟶ Continuous Secure by Design

By strengthening coverage, consistency, collaboration, governance, and measurable outcomes, organizations move beyond late-stage discovery and build a modern Secure by Design program that scales with cloud, AI, and evolving architectures.

Together with the supporting research referenced above, this model offers a practical, experience-driven framework for advancing Secure by Design with confidence.

Next Steps

Understanding your threat modeling maturity is the first step. The next is applying it.

Organizations use this maturity model to:

1. Assess their current state across architecture, integration, governance, and outcomes.
2. Identify where reactive practices are limiting Secure by Design adoption.
3. Prioritize practical, high-impact improvements rather than one-time transformations.
4. Align security, engineering, and architecture teams around shared design-time decisions.

To explore how these maturity stages map to your environment, or to walk through a tailored threat modeling maturity assessment, **connect with the ThreatModeler team**.