



ThreatModeler Managed Threat SERVICE

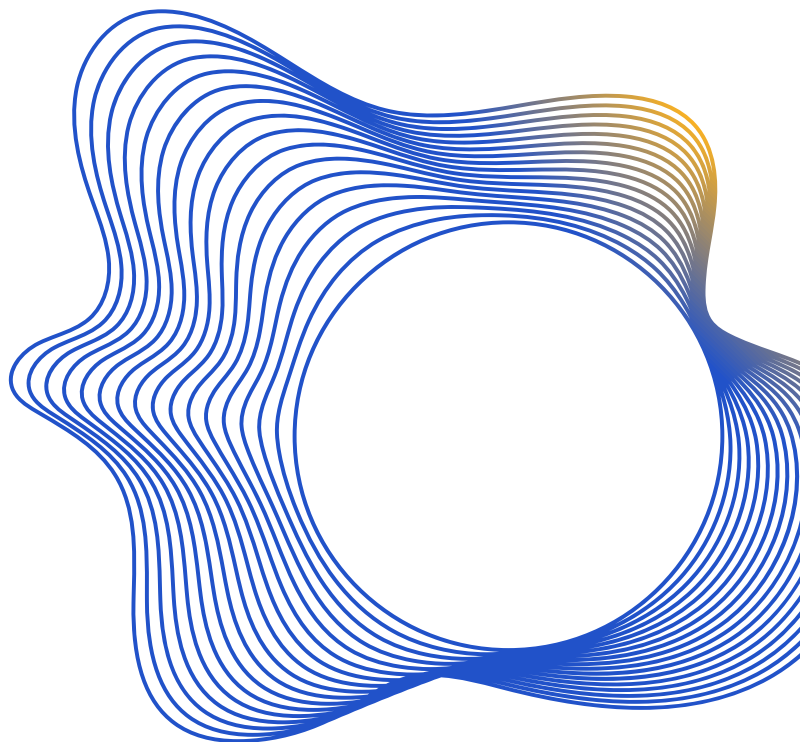
**Managed component and threat
mapping for your business**



Overview

The ThreatModeler Managed Threat Service provides a managed extension of ThreatModeler's extensible threat framework. It delivers architecture-specific content, including custom components, threats, and security requirements, tailored to your organization's architecture, technology stack, and security framework requirements.

With an expertly curated library maintained by the ThreatModeler Threat Research Center, ThreatModeler Managed Threat Service accelerates the roll-out of your threat modeling program, reduces overhead, and speeds up adoption.



What the Service Delivers

CUSTOM ENTITY DEVELOPMENT AND MAINTENANCE

ThreatModeler will develop and manage proprietary components, threats, and security requirements tailored to your architecture and control environment. These entities will be designed to extend frameworks including STRIDE and MITRE ATT&CK, ensuring alignment with how your systems are designed, secured, and governed.

Once delivered, these custom entities can be reused across models and will be continuously updated by ThreatModeler for the length of the service.

CONTENT MAPPING

Custom content delivered through the service is structured to integrate seamlessly with ThreatModeler's automated mapping engine. The ThreatModeler Threat Research Center ensures that every component, threat, and requirement is designed with the necessary context to support accurate traceability, risk analysis, and control validation, enabling you to fully benefit from platform-driven logic without manual upkeep.

- **Mapping to components and threats:** ThreatModeler formats and categorizes custom entities to ensure correct associations within the platform.
- **Maintaining alignment between components, threats, and controls:** ThreatModeler supports the connections between components, threats, and security requirements as part of each update cycle.
- **Preserve traceability over time:** ThreatModeler ensures relationships between components, threats, and controls remain accurate as your architecture and threat landscape evolve, so models stay auditable and actionable.

Quarterly Content Updates

ThreatModeler delivers quarterly updates to ensure your custom threat content evolves in tandem with changes in your architecture and the evolving threat landscape. These reviews go beyond simple refreshes—they include expert input to validate relevance, extend coverage, and maintain compliance alignment over time—all through the ThreatModeler Threat Research Center.

- **Expert-driven content reviews** evaluate and update components, threats, and security requirements to reflect architectural and organizational changes.
- **Incorporation of emerging threats** through continuous tracking of the evolving threat landscape—including new attack vectors, vulnerability classes, and exploit techniques—to keep threat content up to date.
- **Compliance alignment support** maintains alignment with evolving standards, including PCI DSS, NIST 800-53, and ISO 27001.
- **Proactive collaboration with your team** through quarterly working sessions to review updates, validate mappings, and ensure continued alignment with your environment and goals.

Service Benefits

ThreatModeler Managed Threat Service delivers measurable outcomes that support continuous modeling workflows, improving model accuracy, governance, and long-term alignment with organizational and environmental change.

Benefit	Description
Accelerated Threat Modeling	Focus risk analysis and mitigation on your specific environment and attack surface.
Zero Overhead	In addition to initial delivery, quarterly updates are provided—enabling you to focus on reducing risk rather than building content.
Simplified Governance	Streamline risk decisions, control validation, and audit readiness with business-specific context.
Broader Adoption	Business-specific content eliminates learning curves and overhead, enabling more teams to threat model faster.

Built for Your Environment

ThreatModeler Managed Threat Service is designed for teams that require more than off-the-shelf content. It supports organizations with unique architectures, dynamic threat surfaces, and regulatory pressures to demonstrate secure-by-design practices—without the overhead of managing threat libraries in-house.

- **Model unique architectures with precision:** Support custom-built applications, APIs, and microservices that fall outside standard templates.
- **Extend standard frameworks with tailored content:** Add proprietary threats, components, and requirements to STRIDE, MITRE ATT&CK, CSA, MITRE ATLAS and more.
- **Drive audit-ready traceability:** Maintain end-to-end mappings that simplify compliance reporting and risk governance.
- **Maintain modeling accuracy across constant change:** Ensure your threat model stays accurate and aligned as your systems, teams, and threat landscape evolve.

Learn More

To learn how ThreatModeler Managed Threat Service aligns with your security strategy, please contact our team to schedule a personalized demo or discovery session. We'll walk you through real-world use cases and show how tailored threat content can support your architecture, risk profile, and compliance needs.

Visit www.threatmodeler.com or [contact our solutions team](#) to get started.

