



« Secure Software by Design. Automated.

**Automate Threat Modeling to fit your existing SDLC.
Secure design right from the start.**

About us

IriusRisk is the industry leader in automated threat modeling and secure software design, working with clients that include four of the top 10 Globally Systemically Important Banks (G-SIBs).

Every sector of the global economy is being transformed by software, yet vulnerabilities are too often exposed by increasingly sophisticated cyber-attacks. By identifying security flaws in software architecture at the design phase, threat modeling makes it possible to fix issues before code is written.

IriusRisk's platform automates the threat modeling process, enabling developers to design and build secure software. At scale.

Open Threat Modeling Approach

We are methodology-agnostic, meaning we can use any framework due to a mixture of our templates, questionnaires, custom fields and rules.



Data Flow Diagram

Canvas your threat models at speed using an embedded proprietary version of diagrams.net



Trust Boundaries

Editable list of global trust boundaries and zones



Rules Engine

Enterprise grade rules engine (JBoss Drools)



Templates & Patterns

Publish any threat model as a template, create reusable content as risk patterns and import them with customizable rules



Custom Fields

Tailor your threat model risks and controls based on your industry needs, regional standards or any other unique requirements

Open architecture

IriusRisk is the creator of the Open Threat Model (OTM) Standard, a tool agnostic way of describing a threat model. Our API allows you to provide an OTM file and IriusRisk will automatically build a full threat model.



REST API

Editable data flow diagram in an embedded draw.io instance using components, trust boundaries, data flows and data assets



Import & Export

All models can be imported and exported as XML All libraries and templates, including rules can be imported and exported as



XML Rules

JBoss Drools rules engine and bespoke GUI to simplify usage

Integrations

Integrates with popular issue tracking systems, SAST, DAST, unit testing frameworks as well as an open API for anything it doesn't support natively.



Diagram Import

- AWS CloudFormation
- HashiCorp Terraform
- Lucidcharts
- Microsoft Visio
- Microsoft Threat Modeling Tool



ALM Integrations

- CA Rally
- Jira Cloud & Server
- Microsoft Azure DevOps



Security Tools

- Fortify SCA
- Fortify SSC
- OWASP ZAP
- ThreadFix



Testing Frameworks

- BDD-Security
- Cucumber
- JBehave
- JUnit

Content Libraries

Comply with industry standards and automate risk mitigation for your applications. These libraries come as standard out-of-the-box.

- **Regulatory & Compliance** | EU-GDPR, FedRAMP, HIPAA, IEC/ANSI 62443, ISO/IEC 27002: 2013 ISO/SAE 21434, NIST Cybersecurity Framework, PCI-DSS v3.2.1, PCI-DSS v4.0, PCI Software Security Standard and UNECE WP.29 Cybersecurity Regulation (CSMS)
- **Industry Standards** | CWE Top 25, MITRE ATT&CK Enterprise & ICS, NIST 800-190, NIST 800-204, NIST 800-53, NIST 800-63, OWASP API Security Top 10, OWASP ASVS v4, OWASP CSVS, OWASP MASVS, OWASP Mobile Top Ten 2016 and OWASP Top 10 2021
- **Industrial Automation** | IEC/ANSI 62443 3-3 and 4-2 and UNECE WP.29 Cybersecurity Regulation (CSMS)
- **Operational** | AWS Foundations Benchmark, AWS Three-Tier Web Architecture Benchmark, Azure Security Benchmark, Docker Community Edition Benchmark, Google Cloud Platform Foundations Benchmark, Kubernetes Benchmark, Microsoft Azure Foundations Benchmark and OWASP Docker Top 10 2018
- **Cloud** | AWS Components, Google Cloud Platform Components, Microsoft Azure Components
- **Applications** | Rich Client, Generic Service, Generic Client, Java Web Start, Web Client, Web Application, Java Applet, Kafka, Web UI, Redis, Rest/GraphQL/SOAP, Web Services
- **Mobile Applications** | Android, iOS
- **IoT Applications** | MQTT broker, MQTT client, IoT Operating System, IoT Mobile Application, IoT
- **Deployment** | Docker Container, Docker Swarm, Docker Linux Host Internal Server
- **MITRE** | MITRE ATT&CK Enterprise & ICS, CAPEC and CWE

Reports

Easily provide a full audit trail to management and regulatory authorities of all risk management activities for all products to comply with external and internal security standards.

- **Standard (Docx, Xlsx, PDF) |** Risk Summary, Technical Threat Report, Technical Countermeasure Report, Compliance Report, Pentesting Report
- **Excel |** List of threat models, List of threats, List of countermeasures
- **Analytics and Dashboarding |** Find out more here if you are a larger organization with greater analysis needs, or your are a professional looking for adoption trends or enhanced audit reporting

We help you do more with your data

How we charge our enterprise users, and choice of hosting



Licensing Model

Annual subscription based on number of projects managed



Product Tiers

- Community Edition (free-version)
- Enterprise Edition



Deployment Options

- Dedicated Server SaaS
- On-Premise Single Sign-On
- SAML 2.0



User Management/RBAC

- Internal standalone authentication
- LDAP/ Active Directory