IriusRisk

Secure Software by Design. Automated.

Automate Threat Modeling to fit your existing SDLC.
Shift left. To secure design right from the start.

IriusRisk

About us
We makes secure design fast, reliable and accessible, even to non-security users, thanks to our automated and intelligent Threat Modeling Solution.

Why threat modeling?
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.

What you get with IriusRisk Threat Modeling Tool

AI-Augmented Threat Modeling
Our powerful AI Assistant saves you time and aids your diagram creation but keeps you in the threat modeling driver's seat.

Diagramming
Canvas your threat models at speed using an embedded proprietary version of draw.io for all your data flow diagramming needs

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

Trust Boundaries
Editable list of global trust boundaries and zones

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

Rules Engine
Enterprise grade rules engine (JBoss Drools) to generate associated threats and countermeasures

The Open Threat Model (OTM) Standard
IriusRisk is the creator of the 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, complete with associated threats and countermeasures

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

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

Integrations

Diagram Import

- ✔ AWS CloudFormation
- ✔ HashiCorp Terraform
- ✔ Lucidcharts
- ✔ Microsoft Visio
- ✔ Microsoft Threat Modeling Tool
- ✔ Draw.io

ALM Integrations

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

Security Tools

- ✔ Fortify SCA
- ✔ Fortify SSC
- ✔ OWASP ZAP

Testing Frameworks

- ✔ BDD-Security
- ✔ Cucumber
- ✔ JBehave
- ✔ JUnit

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

Regulatory & Compliance
CCPA, EU-GDPR, FedRAMP, HIPAA, IEC/ANSI 62443,ISO/ IEC 27002: 2013 ISO/ SAE 21434, NIST Cyber-security Framework, PCI-DSS v3.2.1, PCI-DSS v4.0, PCI Software Security Standard, SAMM and UNECE WP.29 Cybersecurity Regulation (CSMS)

Industry Standards
CWE Top 25, MITRE ATT&CK Enterprise & ICS, Mitre D3FEND Framework, NIST Cybersecurity Framework, NIST SSDF, NIST 800-190, NIST 800- 204, NIST 800-53, NIST 800-63, OpenCRE, OWASP API Security Top 10, OWASP ASVS v4, OWASP CSVS, OWASP Kubernetes Top 10 2022, OWASP MASVS, OWASP Mobile Top Ten 2016, OWASP Top 10 2021, OWASP Web Security Testing Guide (WSTG) and SWIFT Cyber Security Controls Framework (CSCF)

Operational Technology
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, Oracle Cloud Infrastructure Foundations, and OWASP Docker Top 10 2018

Cloud |

AWS Components, Google Cloud Platform Components, Microsoft Azure Components, Oracle Cloud Platform and Alibaba Cloud

Operational Technology |

IEC/ ANSI 62443 3-3 and 4-2 and UNECE WP.29 Cybersecurity Regulation (CSMS)

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, Machine Learning and Artificial Intelligence

Deployment |

Docker Container, Docker Swarm, Docker Linux Host Internal Server

MITRE |

MITRE ATT&CK Enterprise & ICS, CAPEC and CWE

Reports & Dashboards

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 |

(HTML, Docx, XIsx, PDF) | Risk Summary, Technical Threat Report, Technical Countermeasure Report, and Compliance Report

Excel |

List of threat models, List of threats, List of countermeasures

Dashboards |

Customizable dashboard views

How we charge our users, and choice of hosting

Licensing Model |
Annual subscription based on number of projects managed

Deployment Options |
Dedicated Server SaaS, On-Premise Single Sign-On, SAML 2.0

Product Tiers |
Community Edition (free-version) and Enterprise Edition

User Management/RBAC |
Internal standalone authentication and authorization LDAP/ Active Directory

> *" IriusRisk isn't just our tooling. We see IriusRisk as a co-creator of the successful adoption, rollout, and scaling of threat modeling within the Bank, both across the organization globally, and beyond the security team to DevOps. This partnership doesn't stop there; we look forward to exploring the possibilities of enhanced reporting and integration with the other existing tooling in our value chain.*

Global Head of Security Engineering, and Programme Lead, European Bank

Considering IriusRisk?

Get in touch with the team to get all of your questions
answered, email us at **info@iriusrisk.com**