IriusRisk

www.iriusrisk.com

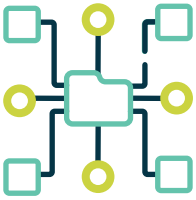
Threat Modeling Datasheet

IriusRisk is the only open threat modeling company that helps developers design secure software from the start.

IriusRisk is an open Threat Modeling platform that can be used by any development and operations team – even those without prior security training. Whether your organization follows a framework or not, we can work with all the threat modeling methodologies, such as STRIDE, TRIKE, OCTAVE, PASTA and more.

Generate threat models and a list of security requirements without needing to engage with the security team. Requirements are pushed and synced directly with issue trackers so there's no need to use yet another system to manage them.

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. See Open architecture for more

Data Flow Diagram | Editable data flow diagram in an embedded draw.io instance using components, trust boundaries, data flows & data assets

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 | https://app.swaggerhub.com/apis/continuumsecurity/IriusRisk

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 | Import diagrams from other tools such as AWS CloudFormation, HashiCorp Terraform and Microsoft Visio

ALM Integrations | Jira Cloud & Server, CA Rally, Microsoft TFS, Azure, DevOps, Redmine

Security Tools | Fortify SCA, Fortify SSC, ThreadFix, OWASP ZAP

Testing Frameworks | Cucumber, JBehave, JUnit, BDD-Security

Content Libraries

Comply with industry standards and automate risk mitigation for your applications. These libraries come as standard

Regulatory & Compliance | CIS: Amazon Web Services Foundations Benchmark, Three-tier Web Architecture, Benchmark, Docker, EU-GDPR, HIPAA, ISO/IEC 27002:2013, NIST 800-53/NIST 800-63, OWASP Application Security Verification Standard (ASVS), Mobile Application Security Verification Standard (MASVS), API Security Top 10 Standard, Top 10-2017, Mobile Top 10, Docker Top1, IoT Security Compliance Framework from IoT Security Foundation (IoTSF), PCI-DSS v4 and PCI-SSS, IEC 62443

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 | 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

Advanced Analytics | 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 applications managed

Product Tiers | Community (free-version), Enterprise

Deployment Options | Dedicated Server SaaS, On-Premise

Single Sign-On | SAML 2.0

User Management/RBAC | Internal standalone authentication, LDAP/ Active Directory