Threat Modeling Solutions Evaluation Checklist

Leverage the following checklist to help you identify which threat modeling solution can best meet the needs of your organization.

Important Note: If you marked more than half of the features as a must-have for your organization, especially those highlighted with an asterisk (*), consider a different and automated approach to threat modeling to enjoy differentiated benefits.

Risk Visibility and Audit Readiness

The most important feature of an automated threat modeling solution is to enumerate all risks to a system and provide recommended risk metrics. The solution should also provide managers and auditors with near real-time reporting on the status of weaknesses that attackers can exploit and appropriate mitigations.

Feature	Must-Have	SD Elements	Other Solution
Reporting of weaknesses found by system component	**Yes / No**	✔	
Reporting of mitigation implementation status by system component or across multiple lines of business, systems, and/or system components	**Yes / No**	✔	
Reporting of outstanding mitigations to achieve compliance with specific standards or regulations by project	**Yes / No**	✔	
Dashboards & reporting • Robust filtering options • Export capability	**Yes / No**	✔	
Ease of demonstrating security controls generated relating to security weaknesses found	**Yes / No**	✔	

Triage Speed

Rapid development environments like DevSecOps and Continuous Integration - Continuous Deployment (CI/CD) require automation and speed. When new systems are built or changes are made to an existing system, stakeholders in security and development need to have that information quickly to decide what, if any, risk mitigations are needed and in which order.

Feature	Must-Have	SD Elements	Other Solution
Customizable questionnaire to better model a project	**Yes / No**	✔	
Notification when events happen or have not happened for specific periods: • New projects are added • Mitigations are updated • Integration process with scanning tools is run/has not been run to verify mitigation implementation	**Yes / No**	✔ ✔ ✔ ✔	
Built-in prioritization of mitigations	**Yes / No**	✔	

Quality of Content

The threat space is not static and different organizations have different mitigation strategies. The ideal solution will include a comprehensive database of weaknesses and mitigations. It should also provide the ability to modify that content to match an organization's security policies.

Feature	Must-Have	SD Elements	Other Solution
Full content customization* • Modify original content (issues, compliance requirements, mitigations)* • Add new content (issues, compliance requirements, mitigations)* • Ease of configuring rules to define the applicability of weaknesses to projects*	**Yes / No**	✔ ✔ ✔ ✔	
Continuous update of security controls • Automatic notification of and option to accept the latest updates in security controls applicable to a system or component	**Yes / No**	✔	

Efficiency of Analysis

To accelerate adoption and reduce friction, an automated threat modeling solution must be accessible and promote collaboration. Solutions that are difficult to implement or lack coverage for major languages, platforms, or regulatory standards will provide an incomplete solution and hamper adoption.

Feature	Must-Have	SD Elements	Other Solution
Expedited onboarding of projects using templates or through integrations	**Yes / No**	✔	
Support for project collaboration to allow other teams (e.g. privacy) to participate*	**Yes / No**	✔	
Automatic identification of potential weaknesses that threats target and appropriate security controls specific to the project's technologies* • Inclusion of potential weaknesses and recommended mitigations in the application's deployment environment specifically applicable to major cloud providers (AWS, Microsoft Azure and Google Cloud Platform) or universally applicable to all other cloud providers*	**Yes / No**	✔ ✔	
Compliance support* • Automatic translation and mapping of regulations, standards and best practices (e.g., NIST 800-53, OWASP Top 10, CSA Cloud Controls Matrix (CCM), GDPR, PCI, FedRAMP) into security controls*	**Yes / No**	✔ ✔	

Mitigation Implementation

Ultimately, the purpose of software threat modeling is to reduce security risk to the organization. Simply listing threats and leaving it to individual engineers to develop mitigation strategies results in inconsistent and difficult to maintain controls, creating uncertainty about the organization's security posture. The best automated threat modeling solutions translate potential security risks into specific, actionable controls – through the tools developers use – that can be quickly implemented.

Feature	Must-Have	SD Elements	Other Solution
Automatic provision of technology-specific security guidance to aid development teams in implementing mitigations* • Inclusion of code samples* • Inclusion of brief and contextual secure coding training videos specific to the project's technology stack*	**Yes / No**	✔ ✔ ✔	
Automatic provision of testing guidance to help verify implemented mitigations	**Yes / No**	✔	
Automatic creation of issue tracker tickets via integration with tools like Jira, GitLab and ServiceNow IT Service Management* • Bi-directional synchronization of ticket statuses in projects between the platform and the issue tracker	**Yes / No**	✔ ✔	

User Experience

While traditional threat modeling exercises were the domain of senior security, development, and compliance personnel, the best automated solutions are also understandable to development, non-technical managers, and auditors. To increase adoption and reduce friction, look for solutions that integrate well with the tools used by all stakeholders.

Feature	Must-Have	SD Elements	Other Solution
Developer-friendly - approachable for developers from modeling to implementation of mitigations*	**Yes / No**	✔	
Integration with the development toolchain (issue tracking systems, security testing tools, CI/CD build tools, GRC platforms, etc.)*	**Yes / No**	✔	
Intuitive user interface	**Yes / No**	✔	
Onboarding training services for users and administrators	**Yes / No**	✔	
Ongoing support services for administrators	**Yes / No**	✔	

Deployment and Administration

Every enterprise solution must be adaptable to an organization's environment. This includes the ability to run on-premises or in the cloud, support enterprise identity and access management solutions, and provide programmatic access to and from other solutions.

Feature	Must-Have	SD Elements	Other Solution
Deployment options for SaaS and On-Premises	**Yes / No**	✔	
Single Sign-On (SSO) support via LDAP and SAML authentication	**Yes / No**	✔	
Role-based access to projects	**Yes / No**	✔	
Documented REST API for programmatic access to the platform	**Yes / No**	✔	

Contact us to learn how SD Elements can help automate and scale your organization's threat modeling process.