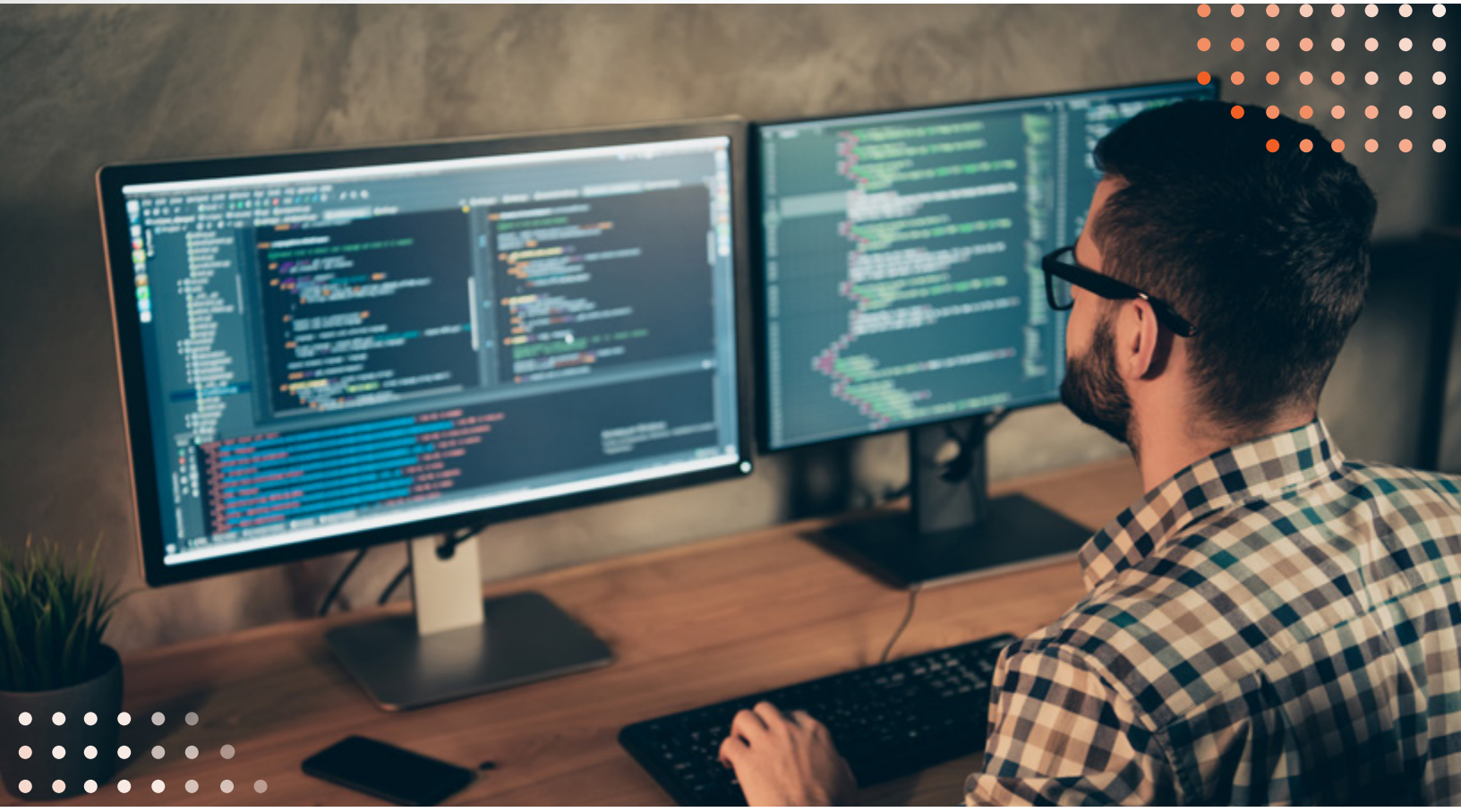
WHITEPAPER

How to Automate Threat Modeling in a DevSecOps World: A Buyer's Guide



Security Compass

The Threat Modeling Movement

By anticipating threats to systems before features and controls are implemented to mitigate those risks, organizations can create more secure software. When done correctly, it can also accelerate development and reduce rework from vulnerabilities found late in the development process.

Traditional approaches to threat modeling make wide adoption difficult. The manual threat modeling process requires work from increasingly scarce security experts and software architects to build detailed models and "trust boundaries." Threat mitigation controls can be inconsistent and rely on the opinion and expertise of those building the threat model. And communicating those controls to developers for implementation is largely manual. Validating that all non-functional security requirements are executed correctly is also difficult.

As a result, organizations utilize threat models on only a few of their most critical applications, leaving the rest of their portfolio poorly protected. When vulnerabilities are later discovered, remediation is also laborious and costly.

Automating Threat Modeling

A new class of solutions that automate threat modeling promise to help organizations build and release secure software quickly. Automated threat modeling enumerates threats based on the technical stack of the application, including programming languages, frameworks, and deployment environments. Some solutions can also recommend mitigation controls. Properly implemented, this allows organizations to scale threat modeling across their entire application portfolio.

This paper will discuss some of the challenges organizations face in selecting and adopting these tools and provide a checklist for evaluating solutions.

Challenges of threat modeling solutions

In most organizations, threat modeling begins as a manual activity. Application owners are questioned about use cases. Risk personnel decide which regulatory standards must be adhered to. Architects diagram how data flows through the application. Security recommends controls.

As organizations turn to automated threat modeling, many begin with diagrammatic threat modeling solutions, some of which are available without cost; however, manual and diagrammatic solutions pose several challenges:

- **Scalability >** The goal of threat modeling is to protect applications across an organization's portfolio. Security is only as good as its weakest link. Criminals will attack at the weakest point possible, then traverse an organization to steal sensitive data, conduct ransomware attacks, or disrupt operations. Allocating days or weeks for threat modeling exercises for every project is not practical in most organizations, even if the personnel can be found and retained, and impossible in a rapidly changing DevSecOps environment.

- **Completeness and control implementation >** Manual threat modeling typically focuses on a subset of security threats and mitigations for software and its environment. Because of time restraints, it falls short on detailing and prioritizing technical steps to mitigate those threats. Likewise, mitigations generated by some semi-automated threat modeling tools are not prescriptive enough for developers, burdening security experts in supporting developers post-threat analysis to implement the mitigations. In both cases, specific steps to validate that appropriate controls are in place are typically ignored

- **Consistency >** Diagrammatic modeling relies on the judgements, preferences, and expertise of those people building the models. While experienced personnel can apply consistency, their less experienced counterparts are likely to be less insightful and complete. Individual judgement can also result in inconsistent security controls, some of which may not satisfy internal and external requirements.

- **Validation and auditability >** Tracking individual projects in discrete spreadsheets or shared documents complicates developers' tasks and security's role in validating hundreds of threat mitigation controls. As the regulatory landscape expands security and compliance personnel need to account for new requirements each day and be able to provide documented compliance in the event of an audit.

- **Complexity >** Applications become more complex each year. The adoption of microservices and complex APIs require special attention. The move to cloud platforms also demands the attention of security teams, as each platform presents unique risks that must be considered. The rise in complexity and pace of changes are happening rapidly. Most organizations – and diagrammatic tools – lack the depth of knowledge required to identify and mitigate risk from multiple threat vectors and the capacity to keep manual threat models up to date.

- **Developer pushback >** Reactive and inconsistent security measures create friction between security and development. Adding extra steps to the development process can slow down development teams that have committed to deliver a specific set of features by a specific date.

Choosing an Automated Threat Modeling Solution

Organizations starting or improving their DevSecOps processes require a threat modeling solution that identifies risks to the organization early and often in the development process, and provides guidance in mitigating these risks in a consistent, scalable, and auditable manner. It must support complexity in the organization's technology stack, deployment environment, and development and testing tools. Beyond preventing attacks caused by weaknesses in the code, infrastructure, APIs and devices, the right threat modeling solution should also help satisfy crucial business requirements around privacy, availability, compliance, and auditability. Specifically, it must be able to:

- Identify weaknesses that threats target in diverse development environments (Microsoft and otherwise).
- Identify weaknesses in all major cloud platforms.
- Integrate with popular development and security testing tools.
- Enable collaboration among privacy, compliance, engineering, and security.
- Automatically identify appropriate, consistent mitigations to prevent or eliminate weaknesses.
- Integrate compliance with a wide range of standards and regulations in software development.
- Continuously update security controls as systems and standards change.
- Simplify implementation of mitigations for development teams.

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 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.**

Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to build more secure software faster. Our flagship product, SD Elements, helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. Security Compass is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @ securitycompass or visit us at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
USA 94108

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001