WHITEPAPER

How Automated Threat Modeling Can Protect Your Migration to the Cloud

Security Compass

We're all moving to the cloud – now what?

Companies of all sizes are accelerating their digital transformation efforts to streamline IT operations and lower overhead. According to IDG's 2020 Cloud Computing Survey, 92 percent of organizations have an IT environment at least partially in the cloud. This makes sense. Moving to the cloud alleviates the burden of purchasing, expanding, and maintaining physical infrastructure such as servers, storage, and network devices.

For all its benefits, moving to the cloud can also introduce new threats and risks. Organizations that simply reinstall internally hosted applications on cloud platforms open themselves up to known weaknesses that bad actors can and will exploit.

Server misconfigurations are consistently exploitable. With applications in the cloud, a misconfigured cloud storage bucket can expose your sensitive data to anyone looking for it (even if you are Microsoft).

- Personal data on 198 million voters was exposed on an unsecured Amazon Web Services S3 bucket
- A cloud storage bucket managed by defense and intelligence contractor Booz Allen Hamilton exposed classified geospatial intelligence
- Nissan leaked source code and other intellectual property through a Bitbucket Git server with the default credentials of *admin/admin*

How common are breaches caused by misconfigurations? The 2021 Verizon Data Breach Investigation Report found that misconfigurations were the leading factor in breaches within the information industry (including software publishing and data processing), far surpassing programming errors by developers.

Threats change when you move to the cloud

To be clear, a cloud environment is not inherently less secure than an internally managed environment. Cloud service providers have the resources (spread across their customer bases) to harden their environments, monitor for threats around the clock, and employ extensive security controls; however, not every deployment includes all of these services across all applications.

The problem goes beyond configuration issues and requires a different approach to securing applications and infrastructure. Cloud Service Providers (CSP) use a "shared responsibility" model for security. CSPs provide and manage the hosting facilities, physical hardware, and network infrastructure, while cloud users deploying applications are responsible for secure coding. Other aspects of application security, however, vary with the CSP and pricing model. Some provide firewalls and identity and access management (IAM) services, while the user is responsible for firewall rules and managing the IAM permissions. Some provide no support for IAM.

When building applications that will run on a CSP platform, organizations must consider the additional responsibilities, and clearly understand whether the CSP employs appropriate controls for each application. The European Network and Information Security Agency (ENISA) publication "*Cloud Computing. Benefits, risks and recommendations for information security.*" describes almost two dozen discrete risks across policy, organizational, technical, and legal categories. These include:

Governance – CSPs monitor and manage the hosting facilities, leaving the application developers dependent on the policies, procedures, monitoring, and reporting of the cloud provider. Organizations deploying applications subject to regulatory oversight must be sure the CSP can provide detailed reporting and logging information needed for standards such as PCI DSS. Similarly, if a critical application requires special host configurations for hardening, the CSP must be able to support such configurations and change management procedures.

Multi-tenancy and isolation failure – Two defining features of the cloud are shared resources and multi-tenancy. By sharing computing resources across multiple users, clouds allow rapid scaling without requiring application owners to maintain permanent resources for peak capacity. If not managed properly, this can lead to "guest-hopping" attacks where one tenant has access to another tenant's resources or data.

Insecure or incomplete data destruction – Many regulatory standards and organizational policies require secure destruction of data that is no longer needed. In a cloud environment, that data may be on shared resources including disks, databases, and other storage devices. "Wiping" these resources is often not an option.

Changes of jurisdiction – Many CSPs maintain facilities in multiple geographic locations to provide redundancy and continuous operations in the event of outages or a natural disaster. Data is subject to laws and data disclosure regulations in each of those jurisdictions. Tracking these varied regulations in secure coding standards for each application can be challenging.

Policies / execution

Modern organizations recognize that safeguarding data and systems requires consideration of changing responsibilities and technology stacks. To ensure proper security, many organizations have processes in place for classifying applications. Some also have secure coding standards and controls to account for critical applications and regulatory demands.

Simply having policies, however, does not ensure those policies are consistently followed and enforced across each application and system. Translating regulatory standards into actionable security controls is complicated. Manual and homegrown tracking systems suffer from several shortcomings.

- **Consistency of identifying risks –** Manual methods are only as effective as the employees reviewing the applications and systems are. An individual or team with less experience is likely to miss threats that would be obvious to more experienced individuals or teams. A team under schedule pressure might take shortcuts that would not

be advisable in the absence of time pressure. Consistency can be difficult even when using written questionnaires, as answers to questions may not be clear or may require narrative responses, complicating the assessment process.

- **Consistency applying controls –** Standardized controls help organizations scale their security programs; however, manual assessments often result in inconsistent controls for any given threat. Written policies can help, but remembering each use case and correctly mapping "official" controls is dependent on the diligence and experience of each employee.

- **Scalability –** The shared responsibility model for CSP can be different for each application and cover the infrastructure, metastructure, infostructure, and applistructure layers of the environment. While a team of senior security, compliance, and development professionals can conduct an effective threat model or risk assessment, these resources are scarce in even the largest organizations. When attempting to assess hundreds or thousands of projects and CSP policies, manual tracking methods quickly break down.

- **Auditability –** Reporting for current security posture can be difficult with manual methods that rely on spreadsheets or shared documents. Without adequate change control features, such methods provide poor evidence of compliance with corporate policies and regulatory standards.

Enter: SD Elements

SD Elements solves the problem of complicated regulatory standards, shared responsibility models, and secure coding guidelines – at scale. It provides a centralized platform to automate threat modeling and risk assessments, and translate threats into clear, actionable controls that can be implemented by the DevSecOps team.

- **Consistent –** SD Elements starts with a survey to describe the software project for Development, Governance, and Security teams. This includes the technology stack and frameworks, deployment environment, shared responsibility models, and dozens of regulatory standards to which the application may be subject. From this, SD Elements generates a complete list of known threats to those characteristics of the project.

- **Cloud aware –** SD Elements understands the cloud environment and threats. The process translates the risks inherent in the technology stack and deployment environment into controls to satisfy secure coding standards for each project. This includes:

- **Cloud Services Configurations –** Each service in cloud deployment, installation, and maintenance requires specific configurations to minimize risk. SD Elements anticipates these threats, identifies mitigating controls, and assigns controls and test validation plans to personnel. Threats and controls include Identity and access management (IAM), storage services, domain name services (DNS), notification services, key management services, and load balancing.

- **Mapping to regulatory standards –** To ensure compliance and simplify audits, SD Elements' knowledge base includes standards and controls for over 50 industry and regulatory standards, and translates these requirements into actionable tasks, including code samples and test plans.

- **Support for cloud frameworks –** SD Elements supports numerous security frameworks and standards, including the Cloud Security Association's Cloud Controls Matrix (CCM). The CCM provides over 130 security controls across 16 domains, including application and API security, audit assurance, encryption and key management, and data security and information lifecycle management.

- **Scalable –** SD Elements automates threat modeling for applications moving to the cloud, which allows consistent and accurate assessments of all applications. While manual threat models are warranted for an organization's most critical applications, up to 90 percent of the threats to an application are a function of the programming language, frameworks, and other aspects of the application's technical stack.

- **Auditable –** SD Elements provides a centralized and controlled environment for recording all activity regarding the threats, controls, and mitigation efforts for each software project. If an auditor requests a demonstration of which controls were in scope, who implemented them and when, who validated them and when, and if any notes were attached to those activities, teams can generate a report without interviewing software engineers.

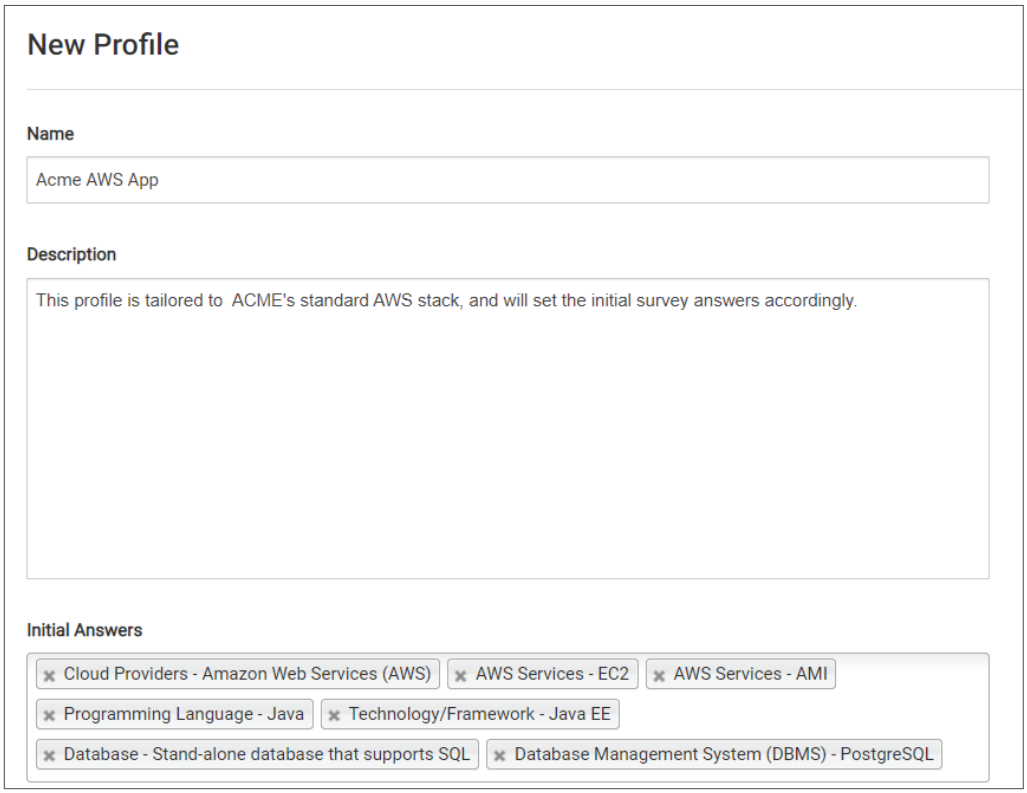
How it works

Ensuring secure cloud development practices with SD Elements is a simple, step-by-step process, both for initial setup and development workflow.

Configuration

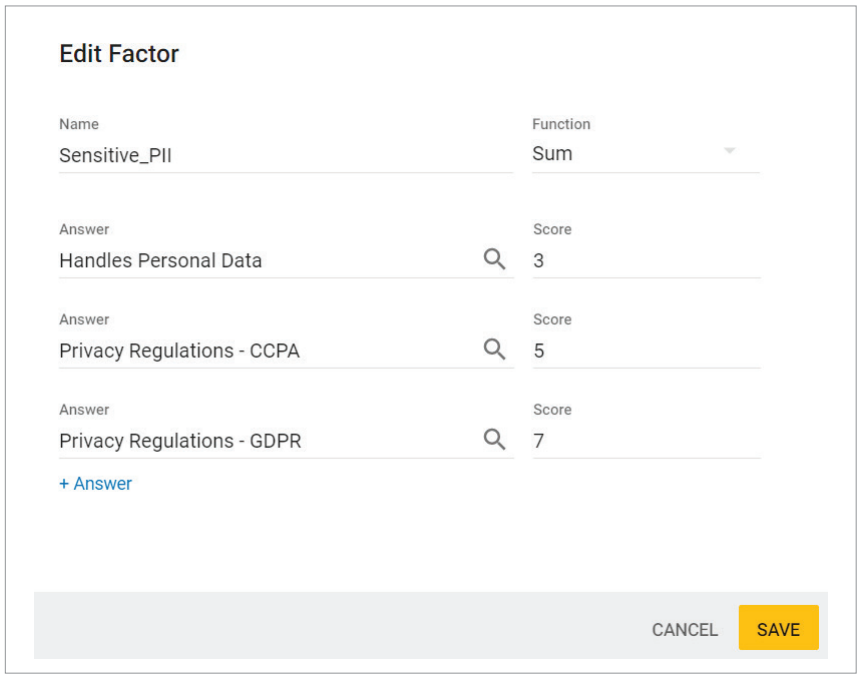
The initial configuration process in SD Elements lets you establish the specifics of the various development environments in your organization – no matter how diverse your cloud development projects may be.

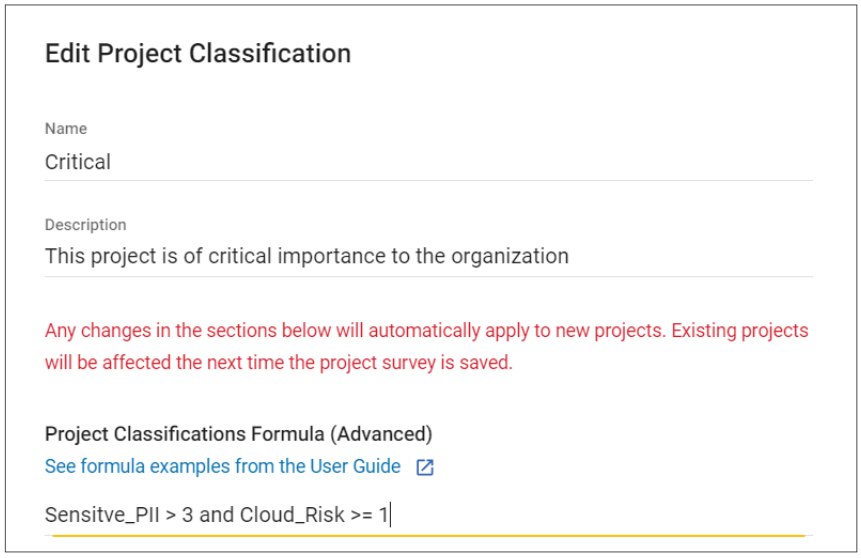
Step 1: Create Profiles for your applications – SD Elements' survey tool automatically characterizes the technical stack of an application including all cloud attributes. If your company has common or standard technology stacks, you can create Profiles which automatically apply a predefined set of answers to a project's survey. For example, you can create a profile called "Acme AWS App", which automatically includes specific AWS services, Java and Java EE, a database management system, and other components to the stack. Using profiles significantly decreases the time required by your DevOps team to start modeling their projects in SD Elements.



Step 2: Classify the application and apply Policies – You can configure SD Elements to classify your cloud applications based on a risk level derived from the information gathered in the project survey. You can also mirror your own risk classification scheme with advanced formulas in SD Elements.

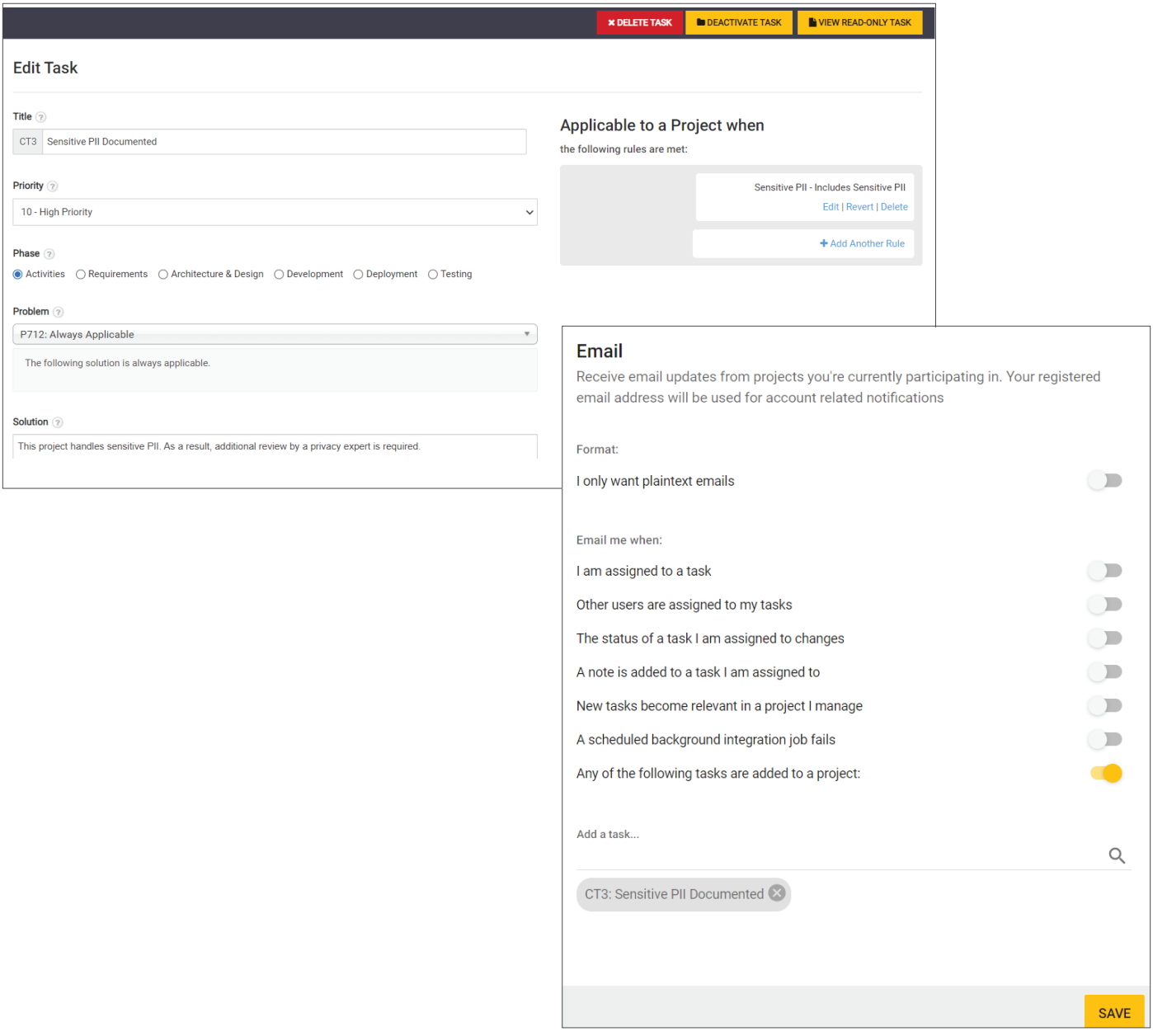
Each classification can be associated with one or more Policies your organization implements. These policies define the level of rigor your team should apply as they implement security and compliance measures. For example, you can specify that you want developers to focus only on high-priority tasks that are in scope for GLBA or ISO 27001.



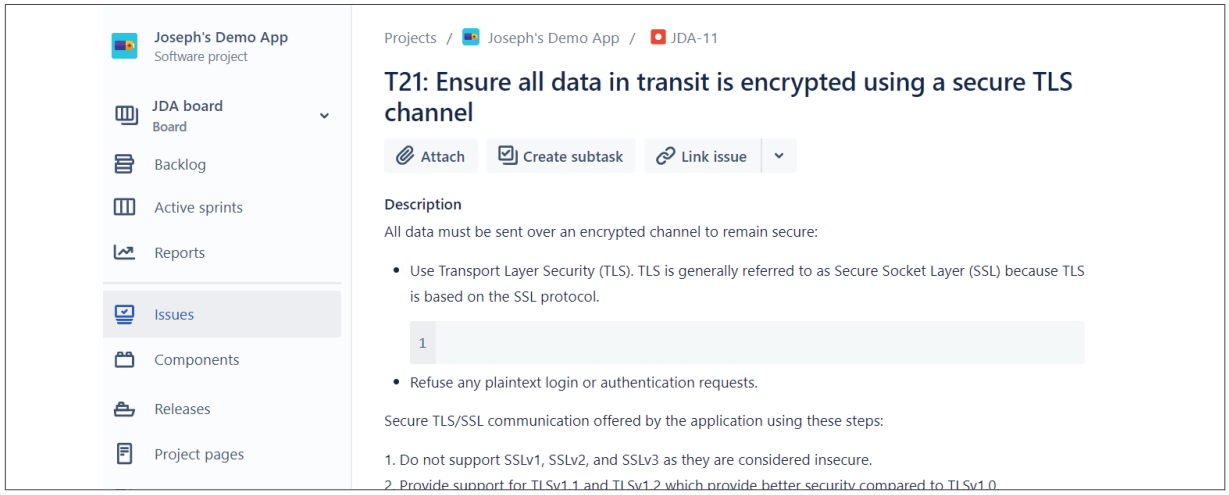


Step 3: Create Automations & Notifications – SD Elements provides your DevOps teams with a self-service interface, however, there may be times when you want to involve a security architect, enterprise architect, compliance expert, or other party. For example, you may want to have a privacy expert involved in any project that manages sensitive personally identifiable information (PII).

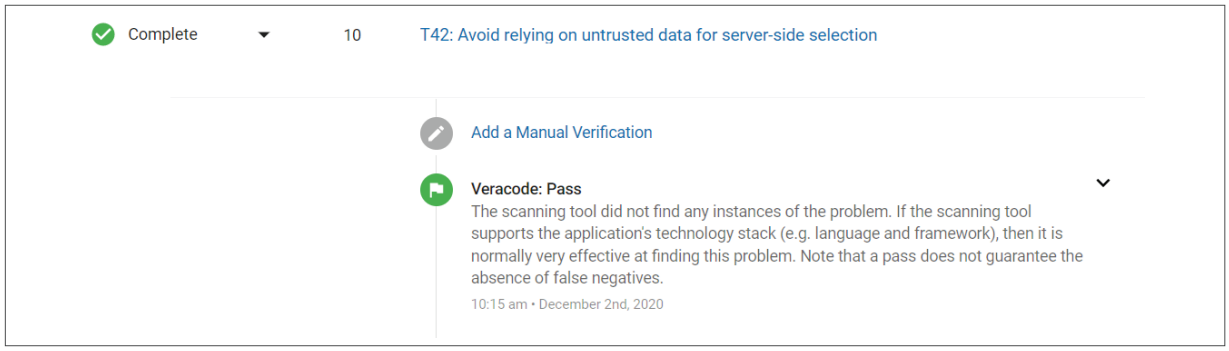
SD Elements enables this through Tasks. In this example, the task would require a privacy expert's review whenever Sensitive PII is selected in the survey. You can then have that privacy expert subscribe to the project to be notified every time a project is created that requires their expertise.



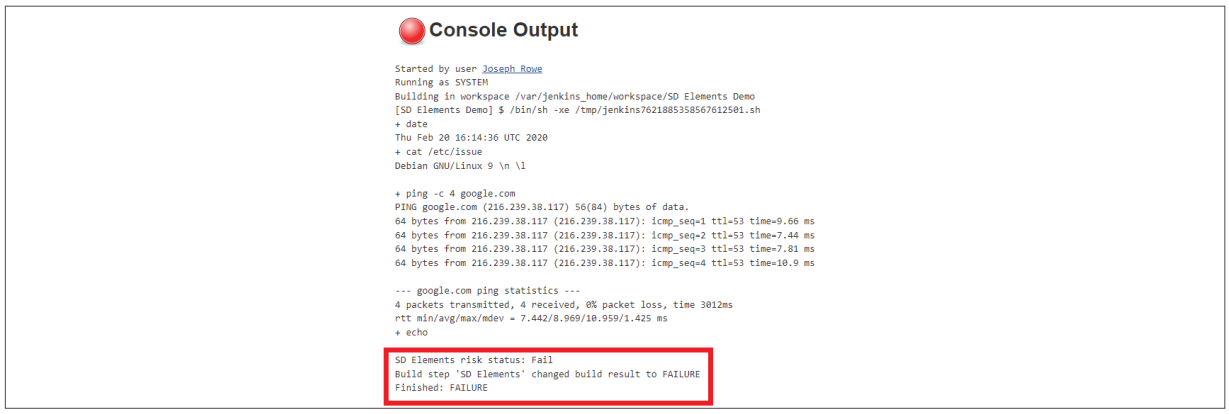
Step 4: Integrate SD Elements with your workflow – SD Elements integrates extensively with tools your team may already be using. One of the most common integrations is the synchronization of SD Elements and issue trackers like JIRA or Microsoft Azure DevOps, which allows DevOps teams to access SD Elements content directly from their tool of choice.



SD Elements also integrates with application security testing tools such as Veracode, Checkmarx, and Fortify to verify and close tasks automatically if scans indicate the required work has been completed.



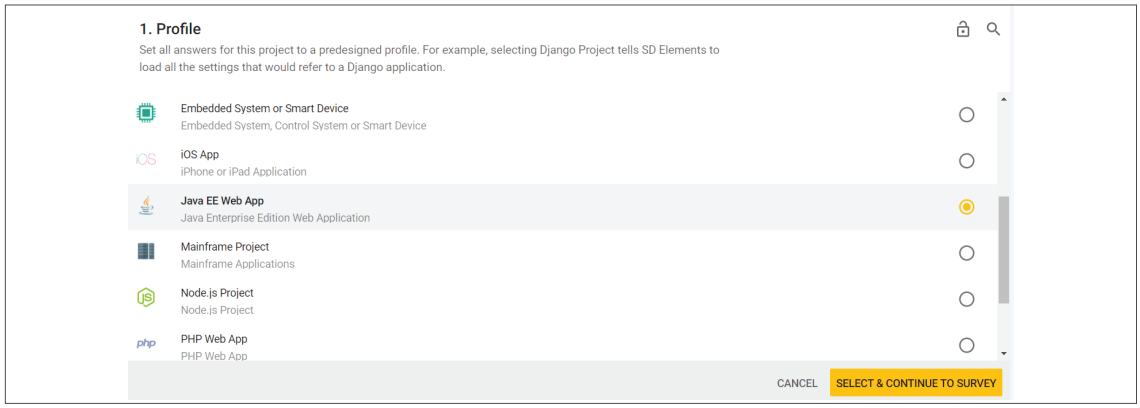
In addition, you can configure CI/CD tools such as Jenkins to fail a build if the mandated minimum subset of tasks from SD Elements are not completed or verified.

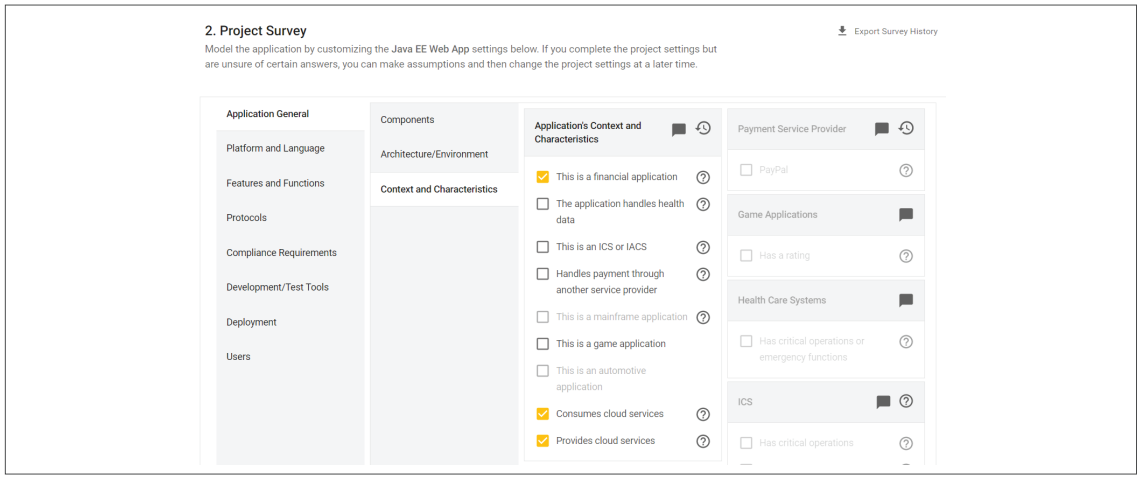


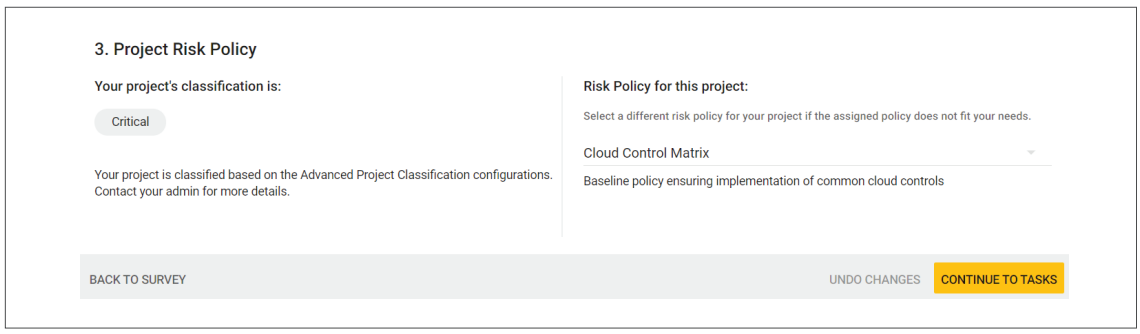
Workflow

Once initial setup is complete, a project team responsible for a migration can use SD Elements to help ensure their projects meet minimum security and compliance requirements.

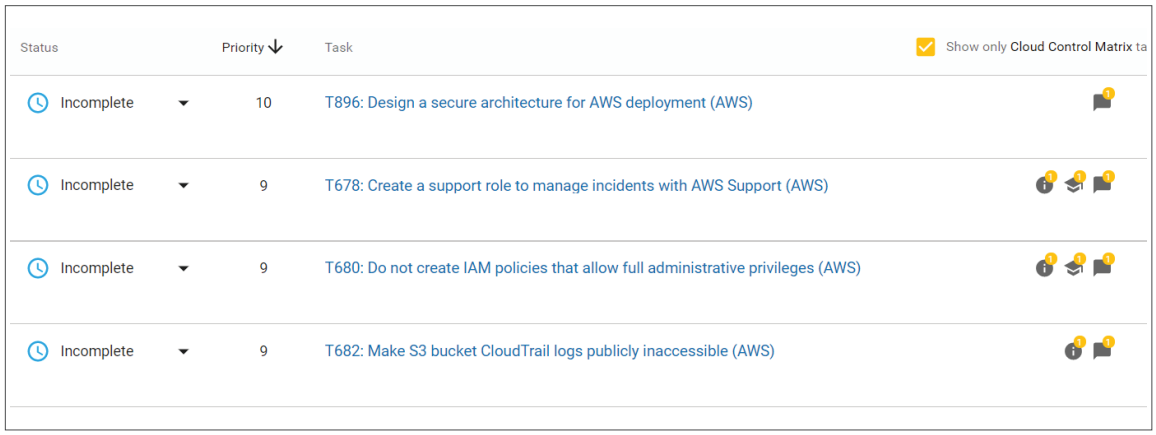
Step 1: Information gathering - Select one of your application profiles and then answer more specific questions about the application's intended use and technical stack. This will generate a tailored set of tasks for the project, based on the application's inherent risk classification.



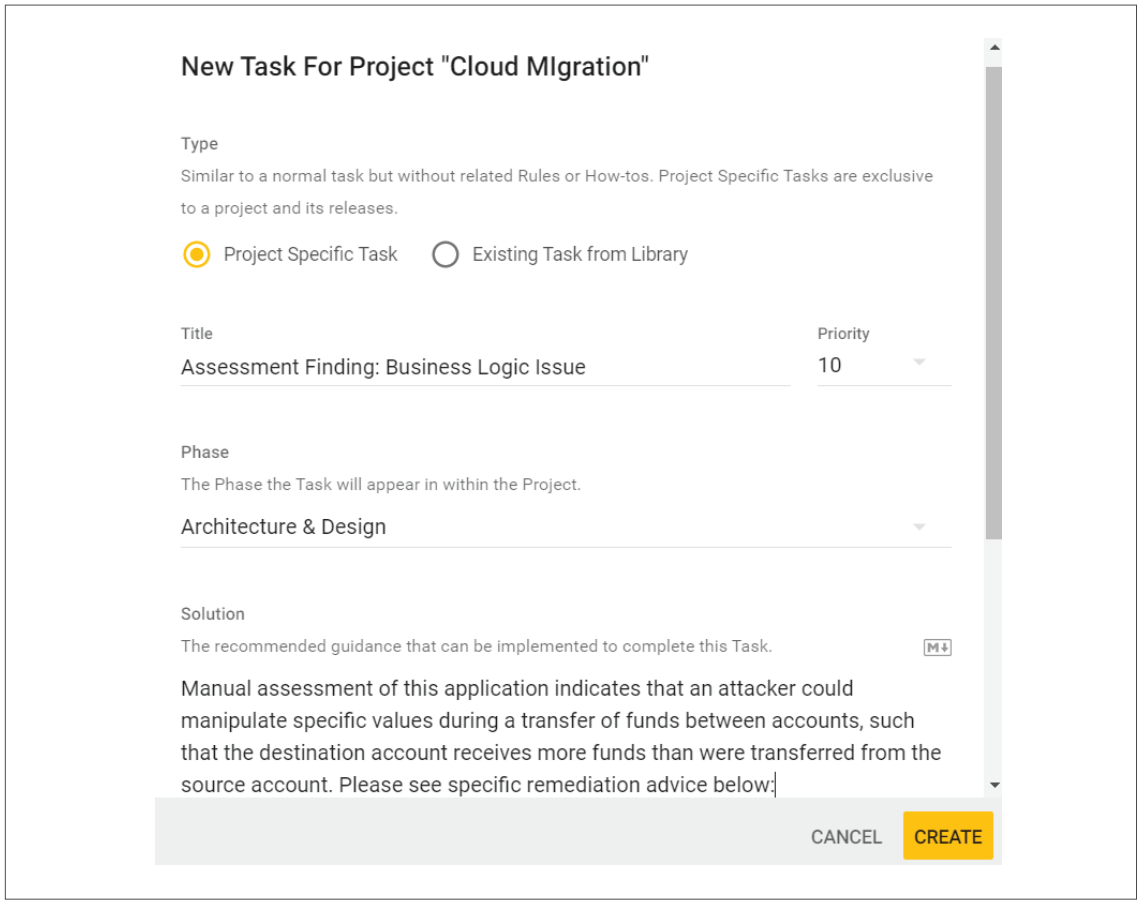




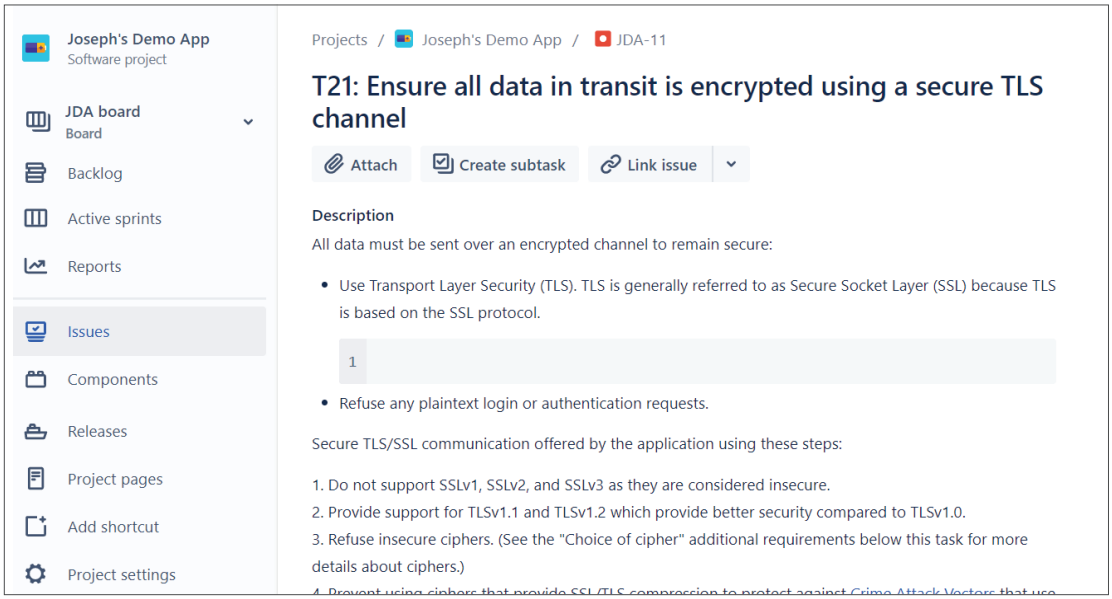
Step 2a: Expert assessment - Tasks will be added according to the rules-based logic and classification scheme you configured during initial set up. Tasks can include sample code and recommended test plans.

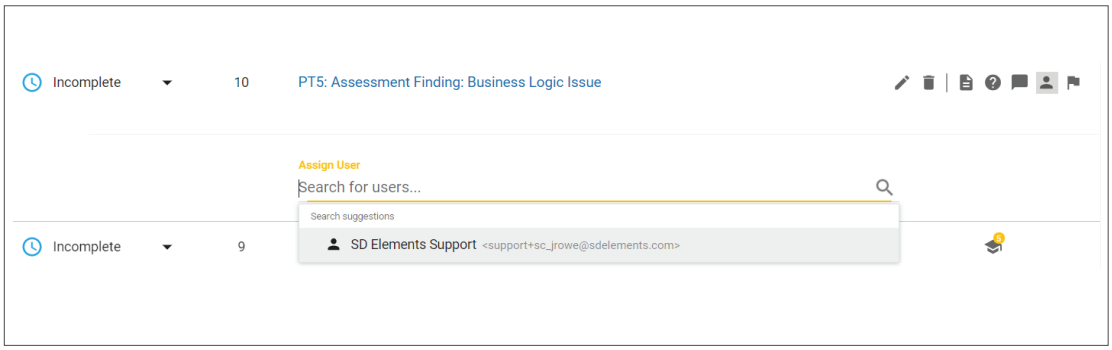


Step 2b: Manual additions - If you set a trigger to involve an expert because, for example, the project will handle sensitive PII, that expert can review the list of relevant tasks and, if necessary, add further recommendations manually following their own assessment of the application.

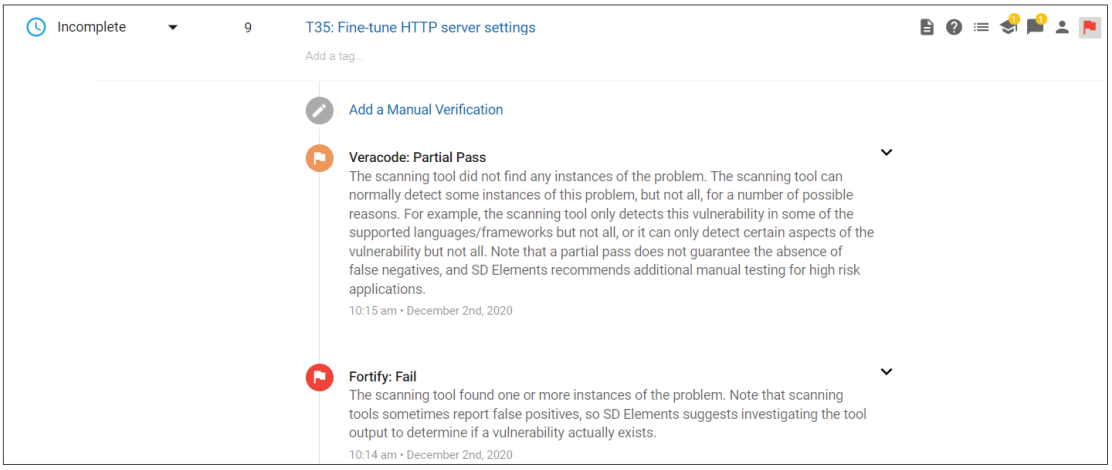


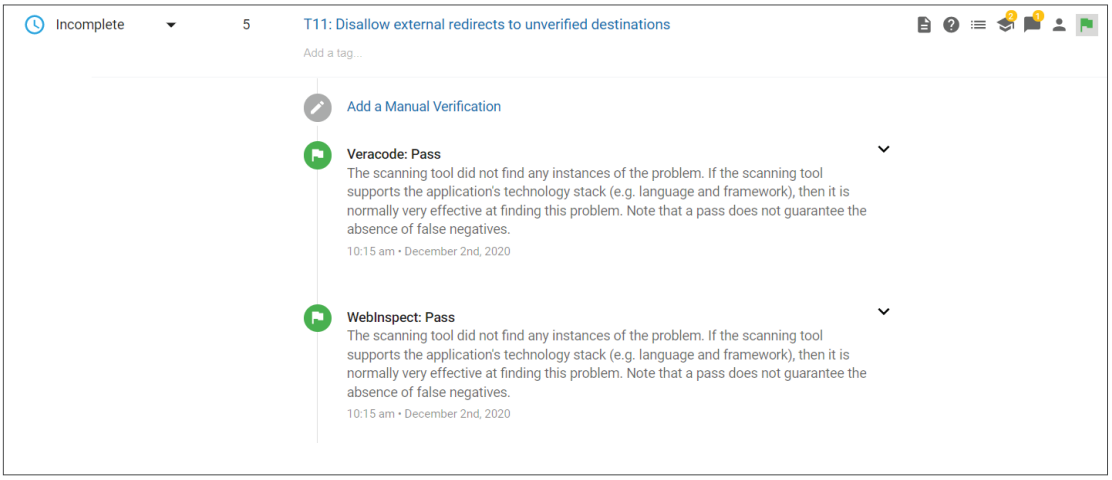
Step 3: Recommendations – SD Elements exports the tasks into an issue tracking system like JIRA or uses its built-in interface to assign tasks to engineering, security, and operations personnel.





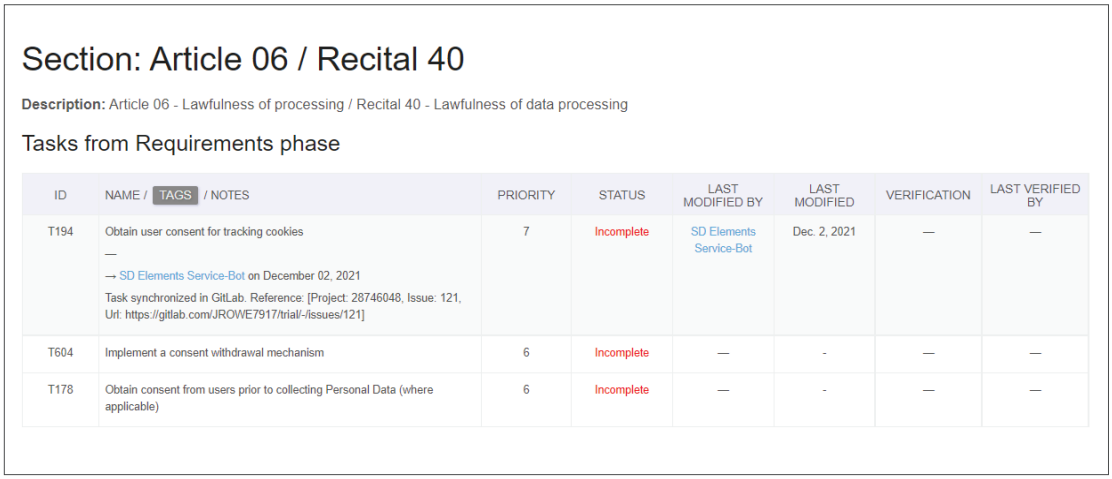
Step 4: Validation – When desired, SD Elements can import test results from scanners to automatically validate whether tasks have been completed.





Reporting and auditing

SD Elements includes reporting for several supported regulations including PCI-DSS, HIPAA, PIPEDA, GLBA, GDPR and other privacy related standards, along with any custom regulations you add to the system. These reports provide evidence of compliance with corporate policies and regulatory standards, including information about which tasks are completed, who completed them, and when. When synchronizing with an issue tracker, reports also include links to the specific ticket.



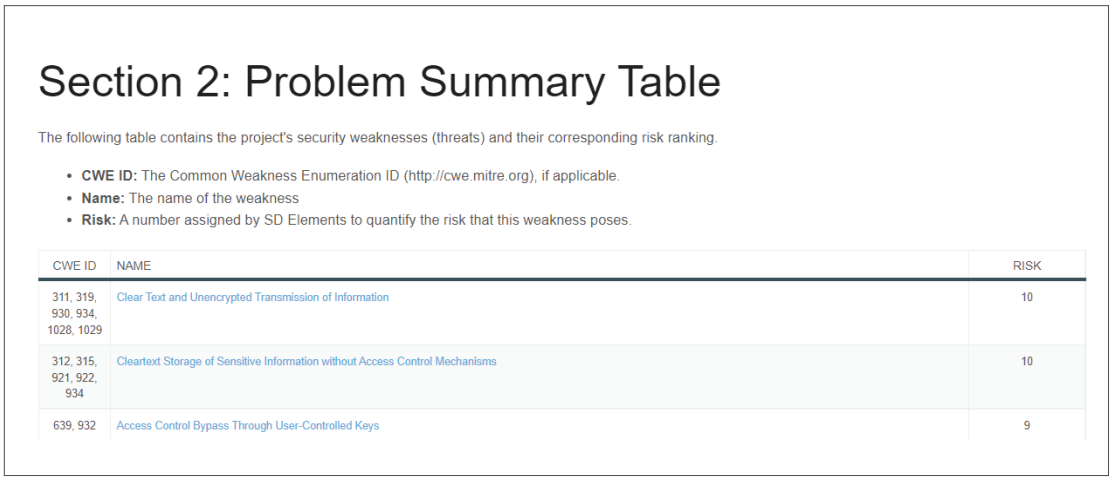
Section: Article 06 / Recital 40

Description: Article 06 - Lawfulness of processing / Recital 40 - Lawfulness of data processing

Tasks from Requirements phase

ID	NAME / TAGS / NOTES	PRIORITY	STATUS	LAST MODIFIED BY	LAST MODIFIED	VERIFICATION	LAST VERIFIED BY
T194	Obtain user consent for tracking cookies — → SD Elements Service-Bot on December 02, 2021 Task synchronized in GitLab. Reference: [Project: 28746048, Issue: 121, Url: https://gitlab.com/JROWE7917/trial/-/issues/121]	7	Incomplete	SD Elements Service-Bot	Dec. 2, 2021	—	—
T604	Implement a consent withdrawal mechanism	6	Incomplete	—	-	—	—
T178	Obtain consent from users prior to collecting Personal Data (where applicable)	6	Incomplete	—	-	—	—

SD Elements also produces a Problem Summary Report showing all issues the system identified, along with data about relevant countermeasures.



Section 2: Problem Summary Table

The following table contains the project's security weaknesses (threats) and their corresponding risk ranking.

- **CWE ID:** The Common Weakness Enumeration ID (http://cwe.mitre.org), if applicable.
- **Name:** The name of the weakness
- **Risk:** A number assigned by SD Elements to quantify the risk that this weakness poses.

CWE ID	NAME	RISK
311, 319, 930, 934, 1028, 1029	Clear Text and Unencrypted Transmission of Information	10
312, 315, 921, 922, 934	Cleartext Storage of Sensitive Information without Access Control Mechanisms	10
639, 932	Access Control Bypass Through User-Controlled Keys	9

Conclusion

Moving applications to the cloud can be a daunting project for development, security, and operations. New threats and challenges require a different way of thinking about security, and the shared responsibility model requires a clear understanding of the capabilities and controls of CSP.

SD Elements provides teams with the ability to accelerate time to market while ensuring that threats are identified and appropriate security controls are applied consistently and at scale. With SD Elements, organizations can build applications that include all critical security controls nearly as fast as if they were developed without worrying about security or compliance.

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. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on how organizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them 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