SECURITY COMPASS WHITEPAPER

The New Reality - A Complex and Constantly Changing Environment

Security Compass

Maintaining secure software and systems has become more complicated as the types of software running in organizations multiply.

Where once software was either commercial applications or in-house code, we now have BYOD devices on networks, cloud applications and infrastructure, and Internet-of-Things devices with embedded software. Most of these run a combination of open source operating systems and libraries, commercial 3rd party components, and custom code. The adoption of DevOps brings benefits, but also means rapid and continuous changes to the IT environment.

Well-run organizations work hard to secure their systems because protecting sensitive information is important to their business goals, reputations, and bottom lines. Formal policies for required security activities are a critical component of a good security plan. These policies would dictate secure coding guidelines for internal software engineering projects. Depending on the criticality and type of project, this could include conducting static and dynamic analysis, penetration tests, data encryption at rest, and the ensuring of secure communications. If a commercial IoT device is being deployed internally, policies may require a penetration test, the changing of default passwords, and the configuration of the device with an internal TLS certificate.

In addition to internal policies, software and systems may be subject to regulatory standards. PCI-DSS standards apply to any firm handling credit card information. In the US, HIPAA, GLBA, and the California Privacy Act and IoT Cybersecurity Act all require that organizations protect sensitive information. In Canada, the Personal Health Information Protection Act (PHIPA) and OSFI regulatory standards demand similar measures. Any firms dealing with consumers in the EU are also subject to GDPR standards and fines of up to €10 million or 2% of the company’s global annual revenue for an initial offense.

The Policy-to-Execution Gap

As applications, regulations, and threats proliferate, security teams struggle to track compliance with internal and external policies for each application, device, or system entering their infrastructure. In the event of an incident, auditable evidence that appropriate risk reduction activities were performed is critical to senior management and regulators. Good security policies are required to reduce risk, but demonstrating compliance with internal and external requirements can be difficult for teams relying on manual processes. This results in a gap between stated security policies and the execution of those policies.

There are many reasons for this gap. Risk assessments and threat modeling exercises that rely on scarce security resources do not scale in today's complex environment, so implementation of recommended controls is often never confirmed. Likewise, the completion of secure development requirements may not be documented. While many companies have implemented security training, it is often an annual event and cannot address the numerous combinations of software stacks seen by developers. Finally, even if the many security activities are completed, compliance requires continuous monitoring as new vulnerabilities are disclosed and the threat space evolves.

Documenting Policy Compliance

The first step in closing the policy-to-compliance gap is understanding the requirements for each new project or system without a lengthy manual risk assessment or threat modeling exercise. Classifying projects by technology stack and the type of data the systems process can provide guidance on security requirements. For example, Internet-facing applications that process sensitive data present inherent risk irrespective of vulnerabilities that may be introduced through coding or configuration errors and would therefore be subject to specific security policies. Similarly, if the system manages personal health information, compliance with HIPAA, PHIPA, and/or GDPR is required.

Next, appropriate controls must be identified for each risk. To make these actionable and auditable, controls should be described as operational activities that can be assigned to individuals or teams. Standardizing these activities across projects accelerates progress; having a standard testing protocol for OWASP Top 10 or SANS Top 25 vulnerabilities simplifies security testing as testers need not develop unique plans for each project. Ideally, teams will develop a library or database of these controls that can be mapped to risks. Adding these activities to issue trackers makes it simple for security, compliance, and senior management to assess progress against goals and audit required tasks for completion.

SD ELEMENTS
Scaling Compliance with Security Policies

The new SD Elements provides security and compliance teams with the ability to automate and scale risk assessments, automatically generate security controls, and continuously track compliance with internal and external requirements goals in an auditable way. SD Elements works in 5 steps:

1. SD Elements leverages information from surveys, asset management systems, and source code repositories to identify inherent risk in a new or existing project automatically. This reduces time spent on risk assessments by up to 50% so security teams can expand project coverage without imposing on development resources.

2. SD Elements automatically generates controls in the form of operational activities to mitigate risk. These can include sample code and test plans to confirm the recommended actions were performed. SD Elements knowledgebase of controls is maintained and continuously updated by a team of security experts and can be configured to accommodate an organization's own policies and controls.

3. Control activities are assigned and progress monitored through integrations with ticketing systems and issue trackers, like Jira. When tests are conducted using static and dynamic analysis, results are automatically imported and activities updated. SD Elements also integrates with network vulnerability assessment tools, like Nessus, to address vulnerabilities in the deployment environment.

4. All activity is logged in SD Elements and reports are generated to provide auditable evidence of compliance with internal or external standards, frameworks, and policies. Integrations with DevOps tools, like Jenkins, provides teams to near-real-time visibility to compliance with policies.

SD Elements provides security and compliance teams with an automated system that tracks security and compliance standards and translates them into actionable tasks across any software stack. It reduces reliance on manual processes for managing and monitoring security, reduces costs by proactively protecting software and systems, and provides auditability to completion of security controls.

Security Compass

Security Compass believes in a world where people can trust technology, and it is our mission to help customers proactively manage cybersecurity risk, without slowing down business. Our holistic program offerings are tailored to your organization's needs. Through advisory services, training, and SD Elements, our award-winning policy-to-execution platform, we set you up with all of the resources and tools your organization needs to develop secure software. Security Compass serves some of the world's largest enterprises, including 16 of the largest financial institutions in North America, South America, and Asia, as well as 4 of the largest tech companies in the world.

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
1001 Bayhill Drive
2nd Floor
San Bruno, California
USA 94066

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