FINRA Leverages SD Elements to Mitigate Risks and Improve Time to Market

Scaling security resources and enabling DevOps teams to execute threat modeling

COMPANY	LOCATION	PERSON AND ROLE
FINRA	**U.S.**	**Jeremy Ferragamo** Director of Cyber & Information Security

The Financial Industry Regulatory Authority (FINRA), overseen by the SEC, is a not-for-profit organization dedicated to investor protection and market integrity. It regulates brokerage firms doing business with the public in the United States, and also provides market surveillance and other regulatory services. FINRA leverages innovative technology to detect potential abuses as they oversee tens of billions of market transactions every day.

Challenge

FINRA has had various forms of threat modeling since at least 2008. In 2010, they launched an Application Security Architecture (SecArch) team to evolve threat models for business-critical applications. This process, which included diagramming, interviews, security requirements planning sessions, data classification, threat actor identification, formal monolithic reporting, etc., could take up to two weeks to complete for each project.

To improve their processes, the SecArch team developed a proprietary, characteristic-based threat modeling tool. This tool, however, was not self-service and relied heavily on security experts for day-to-day operations. It was also not integrated with their DevOps tools. Consequently, it could not be scaled to identify customized security weaknesses and corresponding countermeasures early in the Secure SDLC (SSDLC) to benefit the entire portfolio.

Copyright © 2020 Security Compass. All Rights Reserved.

Over the years, the SecArch team's focus expanded to other initiatives such as defining data protection governance, deploying and operating encryption and sanitization infrastructure, and spearheading the cloud security initiative. At the same time, the size of their application portfolio more than doubled. These factors, coupled with some manual processes, progressively limited their bandwidth for supporting threat modeling activities. As a result, less than 20 percent of the application portfolio was prioritized for this activity when they re-evaluated the buy-versus-build decision and decided to pivot to a self-service model.

Solution

To identify and mitigate threats at the speed of software delivery, FINRA began evaluating solutions from different vendors. For the trial, they involved five internal teams to evaluate these solutions. At the end of this exercise, SD Elements emerged as the clear winner as participants perceived it to be the best solution in terms of intuitiveness and maturity of knowledge base. It also satisfied the SecArch team's objectives of scalability, process simplification, and ability to defend against audit criteria.

The SecArch team then re-defined and published their governance process to lay down the foundation for long-term success. This involved vetting their SSDLC process with all key technology stakeholders, and overhauling their application security policies, standards, guidelines, and procedures. Two key requirements were defined that necessitated every application team to use SD Elements, including leveraging it to prioritize the entire application portfolio for subsequent security activities throughout the SSDLC. The team also customized the content and certain functionalities in SD Elements to improve their application teams' user experience and their management of the service.

SD Elements provided the framework that allowed us to achieve a rapid, self-service engagement model that unifies stakeholders across various programs. It is a multi-purpose solution that should be a crucial part of any mature or maturing Information Security program.

Jeremy Ferragamo,
Director of Cyber & Information Security

Copyright © 2020 Security Compass. All Rights Reserved.

How FINRA Leverages SD Elements for Application Security

Today, FINRA leverages SD Elements to protect a portfolio of business-critical web applications, web services, and batch processes. Most of these are hosted on Amazon Web Services (AWS), leveraging over 100 AWS web services.

SD Elements provides FINRA with multiple operational benefits:

Firstly, it enables a speedy, risk-based triage process for all applications. SD Elements helps determine the risk category and score of applications, which aids in prioritizing subsequent security activities and associated frequencies.

Secondly, SD Elements makes threat modeling possible across in-scope applications. This allows FINRA to identify active risk issues that application teams receive as a risk ticket along with developer-centric security guidelines to mitigate the risks.

Finally, the pre-vetted data classification collected through SD Elements enables them to inform other tooling, like compliance monitoring, and identify discrepancies with other processes, like the Privacy Impact Assessment, in a rapid and timely manner.

Overall, FINRA has achieved its goals of identifying and mitigating risks earlier in their SSDLC, as well as reducing the feedback cycle for the application teams by leveraging SD Elements.

Business Impact

Improved time to market for secure software: SD Elements helps FINRA identify and mitigate software flaws earlier in their SSDLC, which allows them to provide tailored security guidance to DevOps teams at the speed of delivery.

Scalability: SD Elements not only rebuilt FINRA's threat modeling capabilities but is also helping them scale those capabilities to the entire application portfolio, regardless of the size or complexity of any given application.

Enhanced efficiency: SD Elements has enabled FINRA's security experts to focus on R&D activities that ensures the latest security risks are captured in their proprietary knowledge base, which the entire portfolio can now benefit from.

Security Compass is a leader in helping customers proactively manage cybersecurity risk, without slowing down business through Balanced Development Automation.

Disclaimer: At the sole discretion of Security Compass product inclusions and descriptions may be modified or withdrawn at any time and without notice.

Copyright © 2020

SecurityCompass
securitycompass.com
1.888.777.2211
info@securitycompass.com