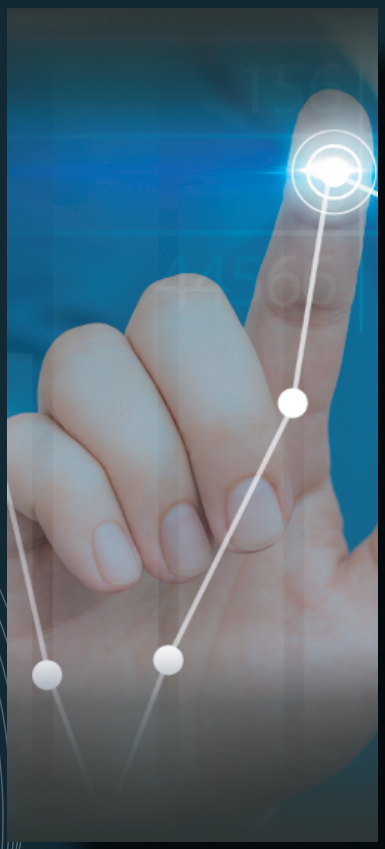
CASE STUDY



Financial Services

Large financial services company with over 3,000 offices worldwide in over 60 countries with more than $1 trillion in assets.

CODESentry®
GRAMMATECH

Quickly perform binary analysis on software applications with CodeSentry to identify third-party and open source components, generate a comprehensive SBOM, detect 0-Day and N-Day vulnerabilities and get an overall risk score.

GRAMMATECH

Multinational Financial Services Company Reduces Application Authorization from Months to Weeks

Utilizing software supply chain security platform achieves 94% reduction in time spent authorizing new software applications for the enterprise

A large multinational financial services company has more than 3,000 software applications that they use internally to support business-critical functions as well as day-to-day productivity. From widely used commercial off-the-shelf (COTS) software applications such as productivity suites, browsers, messaging and video conferencing, it is these applications that support individual departments as well as the organization's global employees. Gartner estimates that more than 50% of all software that banks use is purchased off the shelf and a significant majority of companies in financial services, consider security of open source and third-party software to be a top concern.

In fact, security issues with third-party software are such a serious concern, this institution tests and evaluates all software prior to being implemented internally. The risks due to data breaches, malware and vulnerabilities are too high in the financial services industry because a potential compromise can lead to regulatory violations, financial loss and reputational damage.

There have been numerous attacks that have taken advantage of open source vulnerabilities that exist in COTS – such as the data breach at Equifax, the high profile SolarWinds supply chain attack and the recent Microsoft Exchange vulnerabilities. In fact, a recent survey by Crowdstrike showed that two-thirds of respondents had experienced a software supply chain attack.

To mitigate the risk associated with third-party software, this company has a dedicated software testing team to evaluate COTS using penetration testing techniques – rigorously testing each application (of the 3,000) prior to it being deployed internally. Because of the weaknesses in the software supply chain, this company's application security testing team must scrutinize and vet all applications for potential security vulnerabilities that can introduce risk into the organization.

"With CodeSentry, we've reduced the time it took to authorize third-party software from 4 months down to only one week. Additionally, we also vastly improved the confidence in our authorization process and the security of our software."

- Head of application security testing for financial services company

CHALLENGE

This institution had a few problems with this approach: It took up to 4 months to validate and authorize an application for use. This length of time was unacceptable to the business units they support. The application testing team was viewed unfavorably as a bottleneck. There were also negative revenue implications by delaying authorization for software applications since the software could not be deployed for up to four months.

The other key and perhaps most important problem was that the application testing team was not confident they were able to uncover all the possible vulnerabilities in the software they were authorizing. The application testing techniques they rely on like penetration testing were not completely effective and they need an automated way to support their authorization process.

SOLUTION

GrammaTech has developed an automated method of testing software applications based on our 10-year research history with the DoD and DARPA. GrammaTech CodeSentry scans applications in binary form – including COTS - to detect virtually all open source and third-party components as well as known vulnerabilities in the software. This technology achieves deep scalable analysis without the need for source code and is suitable for enterprise-wide adoption.

Binary analysis is both efficient and less error prone than conventional source-based software composition analysis (SCA) tools. CodeSentry's high precision and recall scans deliver fewer missed vulnerabilities and fewer false positives. The key advantage of CodeSentry is the ability to interrogate – at the binary level - both open source and third-party software.

"With CodeSentry, we've reduced the time it took to authorize third-party software from 4 months down to only one week," explained head of application security testing for financial services company. "Most importantly, we vastly improved the confidence in our authorization process and the security of the software we are deploying."

CodeSentry binary analysis removed the bottleneck in the authorization process and provided internal customers with a complete software bill of materials (SBOM) and vulnerability report for their third-party applications.

CodeSentry also accelerated the remediation process. Finding vulnerabilities in third-party software often requires going to a vendor or project and requesting fixes. The detailed information provided by the CodeSentry SBOM greatly assists this process by pinpointing the exact vulnerable component. This institution now operates with much better information for risk management and decision making.

This institution has since evolved their usage of CodeSentry and incorporated it into their own platform. By using CodeSentry's API, they purpose-built an application testing platform, further automating and ultimately streamlining their authorization process.

GRAMMATECH

For more information:
www.grammatech.com
Email: info@grammatech.com

GrammaTech Headquarters:
6903 Rockledge Drive, Suite 1250
Bethesda, MD 20817
U.S. sales: 888-695-2668
International sales:
+1-607-273-7340
Email: sales@grammatech.com