NetSPI Addressing Financial Services Security Challenges Head-On

Broadridge

The Challenge

It's a common scenario: a company targets security in one area and implements a point solution. Soon after, another threat at another point of entry leads to a separate point solution. Before long, the enterprise is struggling to manage an immense amount of data from disparate sources in an attempt to effectively assess overall vulnerabilities and protect the business from attack.

At Broadridge Financial Services, Inc., this scenario had created a significant business challenge. With no automated workflows to help manage security concerns, coupled with a lack of interaction among developers, application security staff, and business owners, the organization was wasting an immense amount of time and resources. Tracking and following up on email trails was extremely difficult, and because vulnerability reports were being generated manually, the inconsistency and poor quality of the reporting made obtaining prompt, accurate metrics nearly impossible.

Integrating Disparate Processes with a Cohesive Strategy

To address the challenge, NetSPI was engaged to create a one-stop shop for the company's "vulnerability triage"—a set of tools and processes designed to emulate a medical triage where personnel are armed with tools and processes to quickly evaluate the severity of a condition, determine the most urgent treatment needed, and take immediate action. The team began by building a complete integration and collaboration plan that included:

- Implementing NetSPI 's CorrelatedVM™ (CVM) platform to manage vulnerabilities across the enterprise
- Integrating various vulnerability security scanners to consolidate the many disparate data formats and conflicting remediation recommendations
- Integrating CVM with the platform's complementary SaaS portal

About Broadridge

Broadridge Financial Solutions, Inc. is the leading global provider of investor communications and technology-driven solutions for broker-dealers, banks, mutual funds and corporate issuers.

The Challenge

Broadridge faced an immediate need to improve vulnerability assessment workflow and efficiency across its environment. Because the company was using a wide variety of tools and processes to produce security data and reports, information was being delivered in varying formats and syntaxes, all of which required tedious manual review and correlation.

Please note CorrelatedVM (CVM) is now known as Resolve.

- Integrating CVM with the RSA® Archer eGRC Suite to support exception processes and aggregation with other GRC information
- Providing a single repository to house detailed information on all security vulnerabilities, including current and historical data
- Enabling consistent reporting standards, customized to fit company standards and industry compliance regulations

Bringing It All Together with CorrelatedVM™

To support its many business functions and security requirements, Broadridge relies on a wide variety of tools to gather security data across its business operations. The use of these disparate tools made it necessary for security personnel to manually review and correlate multiple silos of information, all in varying formats and syntaxes, creating a mountain of data that was nearly impossible to navigate or act on in any structured manner. Confirmed vulnerabilities had to be manually uploaded to RSA® Archer eGRC Suite, then used to track policy exceptions and manage risks associated with each vulnerability.

All of these tasks relied on outdated tools and processes, including storing data and scheduling assessments in SharePoint, sharing critical data with developers and management via cumbersome Excel spreadsheets and PDF reports, and communicating vulnerabilities and escalation decisions via detailed emails that were difficult to track and trace.

Using CorrelatedVM, these separate solutions now function in a seamless, closed-loop environment using effective, accurate data integration. The benefits exceeded the objectives of the project and continue to deliver outstanding results.

Wide variety of tools and methods results in wide variety of data formats

- Network vulnerability scanners
- Dynamic application scanners
- Static application analysis tools
- Manual testing
- Third-party vulnerability assessments

Data collected, correlated, normalized, and scored in CVM™

- Accessible to Developers, Security Analysts, and more
- Online project management
- Findings management
- Efficient integration of multiple data sources
- Customizable reporting

Concise, actionable data set sent to RSA® Archer eGRC Suite™

- Accessible to GRC Staff, Business Unit Management
- Policy exception tracking
- Risk ranked and actionable
- Exception processes
- Aggregation with other GRC information

Please note CorrelatedVM (CVM) is now known as Resolve.

The Solution

NetSPI's CVM platform was employed to centrally collect all vulnerability data from any disparate sources. The NetSPI team integrated CVM with existing tools and third-party applications, and applied a SaaS portal to provide a seamless view for developers, application security engineers, and network security engineers.

The Results

By integrating previously disparate processes and applications, the CVM platform made it possible for Broadridge to create a concise, actionable data set. The project streamlined workflows, significantly reduced the time required to manage vulnerabilities, and created a one-stop-shop for the company's vulnerability triage processes.

By integrating and implementing these mission-critical tools and processes, NetSPI was able to create a solution that provided developers, application security engineers, and network security engineers with a seamless view of all reported vulnerabilities and supporting data. CVM ranks each vulnerability by level of risk, and data is provided to help address each instance in order of severity according to pre-determined, policy-driven timelines.

Objectives Achieved After Deploying NetSPI CVM:

- Integration of numerous vulnerability security scanners with disparate data formats, conflicting remediation recommendations, and differing report formats
- Correlation and normalization of all data
- Vendor-agnostic, consistent report format
- Integration of vulnerability feeds from all tools and third party providers
- Integration with the RSA® Archer eGRC Suite
- Data is normalized from all integrated sources before automatic export to RSA Archer
- Import of historical vulnerability data without having to recreate it
- Consistent assessment processes and procedures
- Establishment of a portal for cross-team collaboration
- Technologists have a single place to get detailed information on all vulnerabilities, which includes screenshots, notes and verification information
- Provides role-based access control to data for all stake holders
- Developers are engaged in the vulnerability remediation process and have direct access to technical details without having to sift through emails
- Provides the ability to document in one common portal how a vulnerability could be exploited in the environment

> Prior to deploying NetSPI CVM, we relied on a collection of manual processes to manage our vulnerability data. There was no workflow capability and the process required a tremendous amount of manual effort. The NetSPI CVM solution allowed us to streamline the process, providing a one-stop shop for our vulnerability triage processes.
>
> **Jonathan Klein**
>
> *Chief Information Security Officer at Broadridge Information Security Group*

Key CVM Benefits

- Successful automation of all vulnerability processes.
- Complete integration of all existing vulnerability security scanners to deliver data correlation and normalization and a consistent reporting format across the board.
- Complete integration of vulnerability feeds from all tools and third-party providers.
- Integration between CVM and RSA® Archer eGRC Suite to normalize all data before exporting to RSA Archer.
- Creation and execution of consistent assessment processes and procedures.
- Cross-team collaboration via an enterprise-wide user portal that delivers:
  - Role-based access to a single source for detailed information (screenshots, notes and verification information) for all vulnerabilities
  - The ability to engage developers in the vulnerability remediation process by providing direct access to technical details—without having to sift through lengthy email chains
  - Clear documentation of how each vulnerability can be exploited—all in a single, common portal
  - Improved collaboration between developers and application security engineers and business leaders

Please note CorrelatedVM (CVM) is now known as Resolve.

Conclusion

The NetSPI CVM platform has enabled Broadridge to successfully automate the workflow of manual vulnerability processes and to improve collaboration between developers and application security engineers and business leaders. The success of the program has led Broadridge to greatly expand the scope of their program and request additional customization to automate integration of vulnerability network scan results to the CVM portal and integrate their business risk scoring matrix. The flexibility of the NetSPI CVM platform, and the collaboration with the NetSPI engineers, is enabling the program to evolve with new technologies and business initiatives.

Please note CorrelatedVM (CVM) is now known as Resolve.

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.

Website
www.netspi.com

Email
info@netspi.com

Phone
612.465.8880