International Financial Institution Uses Cenzic Hailstorm Enterprise ARC to Meet Critical Security Control for Application Software Security

Challenge

For a major International Financial Institution (IFI) with offices in Washington D.C., unsatisfactory self generated audit findings, growing risk and increased security incidents prompted the company's Information Security team to seek out a solution to protect their Web applications. The myriad of tools and technologies being used by different departments made it hard for the dedicated Information Security team to be certain that applications were being properly secured.

The company's 2,200 plus Web applications range from basic static informational websites to more dynamic data applications, user extranets, sensitive transactional sites, and some contain sensitive data including personal information and credit card numbers. They also varied greatly in the underlying technology, configuration and hosting arrangements.

The possibility of a successful attack against one of IFI's Web applications provided major motivation; knowing any resulting data breach would undoubtedly discredit the integrity of the institution and could potentially tarnish its name forever.

"To get organized and better protect ourselves, we were looking for a solution that would help secure our Web applications from common attacks including Cross-Site Scripting, SQL injection, Local/Remote File Inclusion and others," said an Information Security Engineer for IFI. "We also needed a solution that was flexible enough to integrate with our other business requirements including tracking systems, reporting, processes and procedures."

Solution

In 2008, IFI implemented Cenzic Hailstorm Enterprise ARC (Application Risk Controller) software to regularly perform vulnerability assessments for its growing library of Web applications and streamline the process for launching new applications. Hailstorm Enterprise ARC was able to quickly assess a large number of existing websites automatically with minimal configuration or interaction necessary, jumpstarting the new program in a matter of days.

IFI is using the ARC interface for advanced queuing, scheduling, reporting and dashboarding which all fold into a single effective portal for managing enterprise application risk. IFI takes advantage of ARC's capability for simple modification of assessments to run under Turbo (get results more quickly, e.g. by running fewer, more probable test cases) or Extreme (get more thorough results, e.g. by running a much larger set of test cases) conditions depending on the need. Being able to quickly assess sites, pass on remediation information and organize the resulting information for tracking and reporting has allowed the IFI security team to show significant improvement in a short period of time.

Once an assessment has been run, IFI has access to a summary and the detailed results displayed in the ARC portal where the team can easily prioritize individual findings for action or further investigation as needed. Using Cenzic's quantitative scoring system (HARM - Hailstorm Application Risk Metric), IFI estimates the risk with each Web application and simplifies identification of problem applications and common issues. Due to the prioritization of vulnerabilities and the higher accuracy of data, IFI was able to focus remediation efforts on the biggest problems first. As well, discovery and tracking of vulnerability trends across the enterprise provided necessary metrics and information to perform gap analyses and make non-technical improvements as well; for instance, through policy and standards revisions.

To perform the same tasks without Hailstorm Enterprise ARC would have cost IFI notable time and resources. The time savings alone for organizing the complexity of the data collected was a huge ROI. IFI has found that, the Cenzic solution yields fewer false positives and finds more "real" vulnerabilities as compared to other similar tools used, helping to minimize the costly process of dealing with false positives. The "stateful" browser contained within the Hailstorm scanning engine explains accuracy and performance for IFI, also providing a suite of session management attacks and other more advanced capabilities and features. The software – as well as the IFI security team - are kept up to date of the latest application threats and vulnerabilities with Cenzic's "Smart Attacks" and updates of the actual test modules.

CONTINUED ON NEXT PAGE

The Result

Today, IFI's Information Security team is using Cenzic Hailstorm Enterprise ARC in several functions and throughout the software development lifecycle (SDLC). Primarily, the solution is used for certification and accreditation of new and existing applications and the ongoing vulnerability assessments of those applications moving forward. Access to the ARC portal is also provided to development teams so they can perform their own assessments, analysis, and reporting.

IFI works closely with developers to educate them on building application security into the development process from the start. With a large focus on Web publishing, as is the case for most organizations, adding another step to a process is not a popular decision. Obtaining the organizational buy-in necessary to adequately secure the company's Web applications is critical to immediate success and ensuring the current efforts are sustained by improved software quality over time.

"One of the biggest accomplishments that we have made with Hailstorm has been enabling our developers with more knowledge, resources and tools to do their jobs better," said an IFI Engineer. "We have the data and reports to support the need for application security and we can leverage that when outlining what we are going to do about it. We have sparked an interest in many departments across the organization."

In the future, IFI has plans to implement Cenzic's solutions for performing more thorough testing against applications in their production environment without any production impact by using Cenzic's integration with VMware. They also plan to use API functionality to further integrate Hailstorm scans into existing publishing processes so security testing can be more seamlessly integrated into the SDLC.

About Cenzic

Cenzic, a trusted provider of software and SaaS security products, helps organizations secure their websites against hacker attacks. Cenzic focuses on Web Application Security, automating the process of identifying security defects at the Web application level where more than 75 percent of hacker attacks occur. Our dynamic, black box Web application testing is built on a non-signature-based technology that finds more "real" vulnerabilities as well as provides vulnerability management, risk management, and compliance for regulations and industry standards such as PCI. Cenzic solutions help secure the websites of numerous Fortune 1000 companies, major security companies, leading government agencies and universities, and hundreds of SMB companies -- overall helping to secure trillions of dollars of e-commerce transactions. The Cenzic solution suite fits the needs of companies across all industries, from a cloud solution (Cenzic ClickToSecure Cloud™), to testing remotely via our managed service (Cenzic ClickToSecure® Managed), to a full enterprise software product (Cenzic Hailstorm® Enterprise ARC™) for managing security risks across the entire company. For additional information please visit http://www.cenzic.com

SANS