Using SAINT to support IT Change Management: Critical Security Control for Continuous Vulnerability Assessment and Remediation

Background

The operational security assurance team's primary mission is the developing and administering a fully functional and broad-reaching information system security assurance program in support of a key general support system (GSS) for a civilian Federal agency. The services delivered by the team and the program includes all phases of the security life cycle for the GSS and are far-reaching as the security assurance team works with system owners, developers, and operation staff within the agency as well as other agencies throughout the department. Some of the activities include supporting the agency's change management process, providing security architecture and engineering support, incident reporting, maintaining secure server and end-user operating system configurations, managing security tools, conducting routine vulnerability and compliance assessments, reviewing and responding to security advisories, supporting FISMA and FISCAM audit activities, developing and maintaining MOUs/ISAs, contingency plan testing, etc. The GSS supports over 3,000 agency personnel distributed across the continental United States, consist of more than 3,500 end-user systems, has approximately 300 servers and over 500 network devices in numerous data centers.

Due to the sensitive nature of the implementation, the organization is not identified in this case study. However, the usage of the SAINT product in support of this organization's functions are described to highlight how SAINT is being deployed and adding value in the continuous vulnerability assessment and remediation activities undertaken by the stakeholders of this organization.

Continuous Vulnerability Testing and Remediation

As you can imagine, with a mission this extensive and over 4,000 technology assets deployed throughout the continental U.S., protecting these assets is no small job. With this much at stake, there is an absolute necessity to develop a holistic approach to management and security of these resources, and put this responsibility into the hands of professionals that can get the job done. For this activity, this responsibility fell on the shoulders of Steve Narro and his team, [IT Phenoms, Inc.]. After evaluating a number of options, the team selected SAINT® in 2007, in support of a critical need to establish a program and associated processes, to provide continuous Vulnerability Assessment and Remediation. SAINT was also integrated into the overall IT change management process (pre and post deployment); for Security Certification Test and Evaluations (SCT&Es) and System Security Assessments (SSAs); vulnerability assessments of hosted systems; and for conducting penetration testing on systems in our Quality Assurance (QA) environment.

SAINT is invaluable in identifying weakness and providing details for analysis in that process, as well as initiates remediation for noted weaknesses. SAINT ensures that the change management process is effective in identifying issues by ensuring that weaknesses are corrected and validated prior to their deployment into production.

-STEVEN NARRO, IT Phenoms Inc.

In addition to conducting scans, exploits and reporting for vulnerabilities SAINT is capable of testing for, the team uses SAINT to create custom profiles to ensure required baseline configuration settings are being applied per internal policy. This is an ongoing process. On a weekly basis, they have a queue of change requests that require them to conduct a security assessment, the results of which are used to approve or disapprove the change. As noted by one user… ***"This was easy to do… it automated a once manual process."***

CONTINUED ON NEXT PAGE

Benefits

The benefits of using SAINT have been tangible from the very beginning. Mr. Narro noted that a SAINT-based assessment can be initiated in a matter of minutes. Left running, unassisted, and once complete, SAINT provides a detailed list of issues for the technical staff to review and report on.

Had SAINT not been used for assessments, the work would take a significant number of man-hours. SAINT often enables our technical staff the ability to provide an initial assessment in less than an hour, sometimes within minutes, of SAINT completing its scan.
-STEVEN NARRO, IT Phenoms Inc.

The team also needed a product that would not impact the operating environment. SAINT's vulnerability scanning capabilities is used for the 4,000+ hosts, in multiple time zones. It is very important to be able to run scans, when needed, without impact to system resources or the users during these activities. Steve states "even the most extensive scans have not had a negative impact to the environment. SAINT can be configured such that it can be non-impacting and, thus, can be run to assess Production systems without degrading performance when it is essential to do so.

The team also uses many of the pre-configured and customizable reporting features of the integrated SAINTwriter. Reporting is important to all phases of the change management process, but has been especially important to vulnerability assessment of the host systems, as well as evaluating the results of penetration testing, and support remediation activities essential to ensuring a secure environment for the user community.

SAINT, SAINTexploit, and SAINTmanager have proven to be invaluable tools in the security assurance arsenal for (1) the ability to quickly and accurately identify system and application weaknesses, (2) providing technical details for identified weaknesses in addition to steps for their remediation, (3) ease of use and deployment in the environment, (4) stability and high-availability (to date, there has never been an instance where SAINT was not functional), (5) the ability to schedule future and recurring assessments, (6) automated application and vulnerability updates, (7) customizable and automated reports with multiple output format options, and (8) permitting the development of customized assessments.

Collectively, using SAINT's vulnerability scanning, exploit, management console and reporting capabilities have enabled the team to develop an environment consistent with the tenets of CAG, as well as supporting a central theme and the central tenet of the US Comprehensive National Cybersecurity Initiative (CNCI) - "offense must inform defense". The resulting implementation has created a more holistic approach to the overall change management process, and protecting the valued resources essential to the everyday business, throughout this organization.

SAINT®

SANS

About SAINT Corporation

SAINT, headquartered in Bethesda, MD, is a leader in delivering integrated solutions in vulnerability scanning, assessment, exploit and compliance solutions. SAINT® product suite offers a complete solution to evaluate the threats and vulnerabilities to your IT resources. SAINT offers solutions for federal, state and local government agencies, as well as commercial organizations, academic institutions, and service providers, throughout the United States and worldwide. For more information, contact SAINT Corporation at http://www.saintcorporation.com.