Contact:
Shannon Todesca
CHEN PR, Inc.
stodesca@chenpr.com
781-672-3147

SAFECode Makes Corporations Smarter Consumers with Release of "Principles for Software Assurance Assessment"

New Paper Offers Framework for IT Buyers and Suppliers to Assess the Assurance of Procured Software

Wakefield, Mass. – November 23, 2015 – The Software Assurance Forum for Excellence in Code (SAFECode) today announced a new paper that provides clear and actionable recommendations – with real world examples from high profile organizations including Boeing and the FS-ISAC – for ensuring confidence and quality in the security of purchased software. This framework provides a comprehensive and universal platform from which any organization can create an organizational approach and specific processes that fit their business needs and risk profile.

"Today's threat landscape, combined with burgeoning complexity and connectedness in software and services, requires organizations to create and implement a comprehensive risk management strategy that extends into the software supply chain," said Professor Howard A. Schmidt, Executive Director of SAFECode. "Complicating matters is a lack of uniform standards for assessing the security of procured software. While there can never be a one-size-fits-all strategy, the lack of coherent, independent and specific guidance in all but a few sectors, can create confusion and affect organizations' ability to adequately assess and address risk. Efforts such as ISO 27034 in application security and IEC/ISA-62443 for automation and control systems are strong for what they measure, but there needs to be additional resources to fill in the gaps in industry segments and business categories where similar efforts do not exist."

"There are no silver bullets in software security," said Eric Baize, SAFECode chairman and Senior Director, Product Security and Trusted Engineering for EMC Corporation. "There must be an open and collaborative dialog between vendors and customers to ensure that IT investments drive business value without introducing risk or eroding trust. SAFECode was founded, and has worked over the last eight years, to draw the best recommendations from the collective experience and expertise of its members, and the larger community. This framework embodies these efforts. It is the first step in what will need to be an ongoing process of collaboration between software buyers and suppliers to improve methods for assessing software assurance and to enhance trust in software."

As with all other SAFECode work, this paper is grounded in an extensive analysis of the proven best practices that SAFECode member and large customer organizations actually follow in their day-to-day software assurance efforts. It was created from a rigorous review of the types of security documentation provided to customers, the questions and documentation most often requested by customers, their experiences with current standards and evaluation methods, and their assessments of the impact of customer security reviews on their internal secure development processes.

The paper provides a foundation and framework for examining the secure development process of commercial technology providers by recognizing that providers fall within different levels of maturity of their software assurance programs. For those providers lacking a mature process for software security, or are unable or unwilling to provide information on their process, the burden of evaluation falls to the IT buyer to determine the integrity and security of product code. For this category, SAFECode recommends a tool-driven approach, such as binary code analysis tools.

Other, more mature providers differ in the best practices assessment guidance available/applicable to them. Some providers have a mature, process based assessment grounded in and driven by international standards. For these providers SAFECode recommends that these standards be used as the foundation for assessment. Another type of mature providers have solid software assurance processes, but do not have an established international standard that exists, or one that can be easily aligned with the risk profile of the organization to adequately drive assessments.

The main focus of the paper is helping readers to select the most appropriate evaluation method for category two assessments. It assists organizations in gauging the maturity of a vendor's software security process and reviewing the merits and fit of different solutions as part of a supplier assessment. For category two assessments, it breaks down three main categories

- **Secure development and integration practices** – by what process and procedures do vendors test, improve and quantify the security of the final product? This includes techniques such as threat modeling, sandboxing, fuzz/robustness testing, penetration testing and static code analysis.
- **Product security governance** – is security imbued in the vendor organization, and made a priority at all levels? This includes questions of whether the vendor requires security training/enrichment for the development team, is security posture reviewed and signed off on by multiple levels of management, are there specifics in the roadmap for future secure development work, and is there a clear and documented process of remediation of vulnerabilities?
- **Vulnerability response process** – is the vendor open and collaborative with customers who identify flaws, and is there a transparent and expedient mechanism for vulnerability discovery/reporting, communication, and CVE submission.

About SAFECode

The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. Its members include Adobe Systems Incorporated, CA Technologies, EMC Corporation, Intel Corporation, Microsoft Corp., SAP AG, Siemens AG and Symantec Corp. For more information, please visit www.safecode.org.

###

Product and service names mentioned herein are the trademarks of their respective owners.