2107 Wilson Boulevard
Suite 510
Arlington, VA 22201

703.841.5500 tel
703.841.5501 fax

www.onpointcorp.com

Security and the System Development Lifecycle (SDLC): Security is the first step!

April, 2015
Tim Smith, President
OnPoint Consulting, Inc.

Embracing the rapid pace of technology has provided government agencies with the opportunity to develop new products, services, models and enhance their digital experience. But in a world with greater dependence for always-on, always-connected systems, the risk of cyber threats increases as our customers embrace the digital world.

Intellectual property and assets are now accessible online and are vulnerable to attack; cyber criminals have new opportunities for financial theft, intellectual property theft, fraud and disruption of customer channels. And as the cost of entry into cybercrime goes down, as technology costs decrease, the number of attacks will only increase.

With this in mind, OnPoint is advising our customers to embrace an approach of identifying security requirements early in the application development process, for both their major and minor systems, and incorporating them throughout the system development lifecycle (SDLC). The SANS Institute maintains a running list of the Top 25 Most Dangerous Software Errors and has broken that list into three categories 1) Insecure interaction among software components 2) Risky resource management when coding and 3) Porous defenses. All three of these areas outline the concern that application bugs and coding errors continue to cause security flaws and events (SANS Institute, Integrating Security into Development, No Pain Required, September 2011).

Government agencies need to consider security early in the SDLC for the benefit of delivering a more secure system from the beginning of development and also avoiding higher costs later on during product operation and maintenance. In many cases we have provided both the application development and security resources throughout the SDLC and truly believe an integrated team working together throughout the system lifecycle is the most efficient and cost effective method.

OnPoint has adopted the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-64 Revision 2, Security Considerations in the Information System Development Life Cycle, are our guide to help organizations integrate security requirements and cost-effective security controls, in their planning for every phase of the system life cycle. NIST SP 800-64 outlines the selection of a life cycle model by the organization and the responsibilities of the organization for conducting the system development process. While NIST SP 800-64 describes security and a generic system development life cycle for illustrative purposes, OnPoint has applied this model, with tailoring, to many SDLC models.

There are dozens of SDLC models and most integrate security in different ways. The traditional Waterfall SDLC has been used for many years and while many versions of the model exist, the SDLC generally begins with a Requirements phase followed by Design, Implementation, Integration/Testing and Operations/Maintenance (O&M).

Requirements	Design	Implementation	Integration/ Testing	Operations/ Maintenance
Determine & Document Your Security, Privacy and Access Control Needs	Perform Risk Assessment; Identify known threats and potential vulnerabilities to your system Design your security plan	Security controls and switches are enabled Security analysis of your code OMB Circular A-130, Appendix III, requires that the system be certified	Run security tests Develop security response plan (what-if scenarios)	Configuration Management and Control; establish a baseline and monitor for changes Continuous Monitoring

Many organizations integrate security at the end of each phase, often using security as the "gate" to allow development to proceed to the next phase. OnPoint believes that while this approach can exist, a better approach to ensure that security is emphasized throughout the phase and in many cases should be addressed at the beginning of the phase in order to guide your developers.

A widely used development cycle is Agile; OnPoint has had a great deal of success implementing the Agile methodology for our customers with teams that are known to produce reliable and high quality code quickly. Agile development focused on collaboration and personal interaction amongst development team members and encourages rapid and flexible response to change.

Some theorize that an approach, like Agile, with the pressure to deliver quickly might result is "short cuts" in code reviews, testing and ultimately security. However, OnPoint believes that the true nature of Agile….with cross-collaborating teams, enhance communication and an understanding of all the roles within a development cycle can actually lead to more secure code and ultimately systems.

The "trick", which is true for any development model, is that security must be ingrained within the team like any other quality practice. Threat modeling, as one example, doesn't have to change simply because the team chooses to build software incrementally. Changes that are done in a one or two week sprint or iteration, a regular, repeatable work cycle, are small and incremental and therefore shouldn't take a long time to review from a security perspective.

Ultimately organizations must work towards improving the working relationships between development and security teams. Simple steps can be taken to significantly improve your development methodology, from a security perspective, and can include:

- Assigning a security team to every development project: Have individuals assigned to the development team and integrated at every process; make it known that they are a critical part of the team.
- Educate your developers about security and the attack surface: All developers should understand the importance of security and the exposure points of the applications such as user inputs, expose function calls and web-facing code for example.
- Evaluate your policies and procedures: Review your existing policies and procedures and in certain cases create new policies and procedures focused on security.
- Measure Success: Evaluate the entire process when implementing secure code; hopefully you find that building security into the SDLC reduces errors, reduces costs and creates a more secure application.

OnPoint has provided many of our customers with cyber subject matter experts and teams to help meet these needs. Providing cyber thought leadership to our customers ensures that they are always aware of the latest risks and are prepared to respond swiftly and effectively to mitigate new risks. As every business's needs are different, we tailor our approach accordingly.

About OnPoint

OnPoint Consulting, Inc (OnPoint) is a cybersecurity and technology firm delivering secure IT infrastructure, enterprise systems, and classified solutions for the U.S. federal government. Our specialized strategy, cyber and technology capabilities are changing the way our clients improve performance, effectively deliver results and manage risk. OnPoint holds ISO 9001:2008, ISO 20000-1:2011, ISO 27001:2005 certifications and a CMMI Maturity Level 3 rating. OnPoint is a wholly owned subsidiary of Sapient Government Services, a global consulting company part of Publicis.Sapient. Follow OnPoint on Twitter, LinkedIn and Facebook.