Symantec Software Security Process

LAST REVIEWED: 10/20/2016

Symantec™

TABLE OF CONTENTS

INTRODUCTION

Symantec firmly believes in a proactive approach to secure software development and implements security review into various stages of the software development process. Additionally, Symantec is committed to the security of its products and services as well as to its customers' data. Symantec is committed to continually improving its software security process. This document provides an overview of the current Secure Development Lifecycle (SDLC) practice applicable to Symantec's product and service teams as well as other software security related activities and policies used by such teams. This document is intended as a summary and does not represent a comprehensive list of security testing and practices conducted by Symantec in the software development process.

SOFTWARE SECURITY GROUP

The Software Security Group (SSG) is a group of dedicated software security experts within Symantec's Office of the Chief Technology Officer (CTO) with a presence in most major development sites. SSG is responsible for creating and advocating the proper implementation and adoption of Symantec's SDLC and Software Security Best Practices, which are a series of software security best practices. Furthermore, SSG leverages local talent, analyzes practices conducted by different teams in different regions and promotes the use of best practices. Working closely with the product and service development teams gives SSG deeper insights into the current project status and allows SSG to better align with the teams' security needs and tie such needs' in with overall security goals of Symantec.

Software Security Architect and Security Champion

In addition to SSG, every product and service development team within Symantec is encouraged to have at least one Security Champion and at least one Software Security Architect. These security experts work closely with SSG as well as their organizations to tailor best security practices accordingly and help disseminate relevant and pertinent security related discussions through the proper channels.

Security Leads

Similarly, each product and service development team at Symantec is recommended to have one Security Lead, who works closely with his/her own teams as well as to consult with his/her organization's Software Security Architect and/or Security Champion as needed. The role of the Security Lead is to facilitate his/her team's security issues by becoming the local security specialist and champion, evangelizing and motivating software security initiatives within his/her teams.

SYMANTEC'S SECURE DEVELOPMENT LIFECYCLE (SDLC)

In general, SDLC as a mandatory practice is intended to deliver software security best practices across all stages of development. In particular, SDLC is structured to help ensure that proper due diligence takes place to a great degree during the earlier stages of a product and/or service's development. For example, threat modeling and code reviews are an integral part of this early stage process, where product and service development teams take care to perform related security activities diligently.

By working closely with software development teams at Symantec and consulting with other software vendors through various channels, SSG continues to diligently improve Symantec's SDLC and makes it easier for teams to conform to. Simplicity and ease of implementation are among the most important features of the latest SDLC version, which has the following seven focus areas.

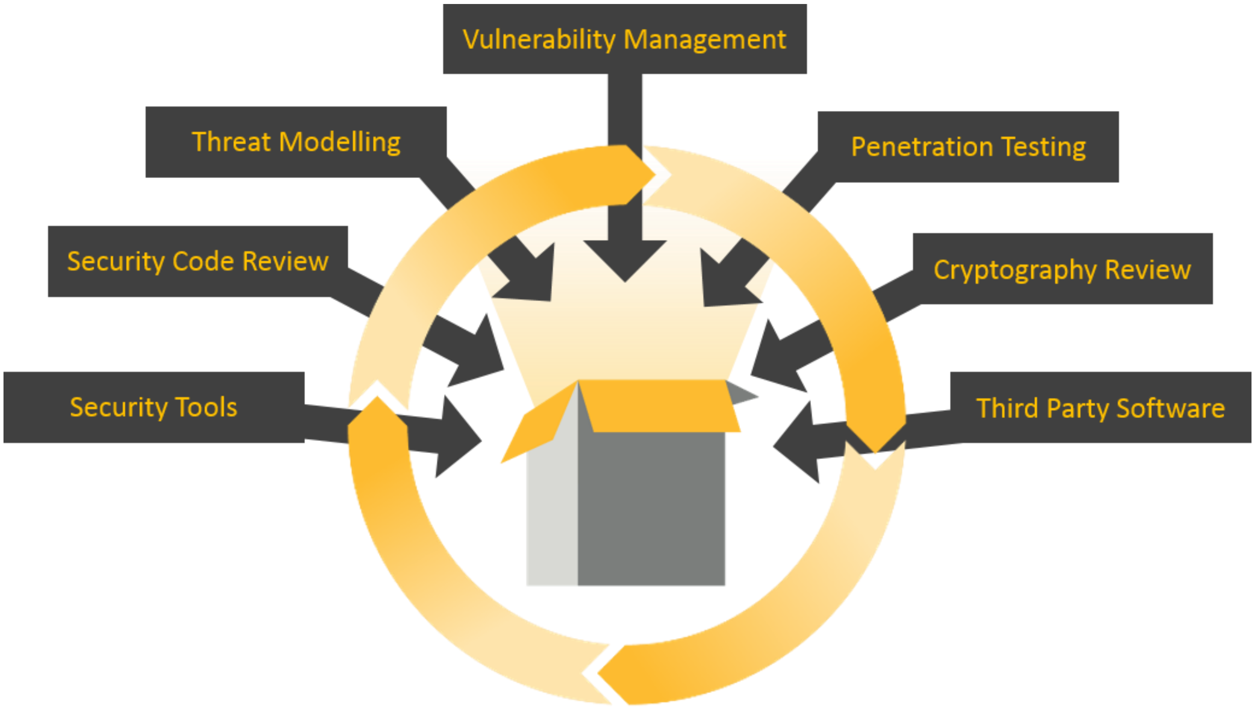

Figure. Symantec's Secure Development Lifecycle

Threat Modeling

Every software development team is required to create and maintain an up-to-date threat model using threat modeling tools. Moreover, cross-team representation from developers, quality assurance, and architects are required during this process. SSG is available for consultation. The Threat Modeling process at Symantec is structured to enhance the team's ability to expose architectural security flaws and, in some cases, implementation-related security defects. The process forces teams to critically think about security of the system, thus growing the teams' security mindset in addition to finding security issues in the system.

Security Code Review

All source code is required to be reviewed from a security perspective. Software development teams with significant amounts of legacy code are expected to use the Threat Modeling process to identify security-sensitive and critical areas to code review. Also, teams are encouraged to use code reviewing tools to facilitate the code review process.

Security Tools

SSG maintains an extensive list of security tool recommendations, including details on their usage (e.g. fuzzing, static analysis, network monitoring). Moreover, information hosted on Symantec's internal network are dedicated to the recommended tools, including specific steps on what options to turn on and how to configure for optimal results. Security tools is one area that SSG strongly recommends for all teams to automate as part of their Configuration Management (CM) builds, and for which numerous Symantec teams have successfully implemented. SSG closely works with teams to identify gaps with security and quality tools, evaluates new tools, develops guidance and helps to ensure that development teams are properly trained and enabled to use recommended tools effectively.

Third Party Software

Teams must comply with multiple policies regarding the use of open source and third party software. For example, each team is required to seek approval from the Open Source Review Board (OSRB) for its use of open source software. Both legal and technical reviews are performed as part of the OSRB review process. Industry-leading tools are used to track and update the list of 3rd party components and any corresponding vulnerabilities. This process helps to confirm that all non-Symantec open source software is compliant with applicable licenses and does not pose a security risk to our products.

Cryptography Review

Teams must comply with a list of ciphers and recommendations that are provided by the company's Cryptography Review Board (CRB). If for any reason a team must deviate from the CRB recommended list, they must submit a survey form about any cryptography usage within their code for approval by CRB. Symantec's CRB consists of senior cryptography experts from across Symantec.

Penetration Testing

Every team is required to coordinate with SSG in scheduling a penetration test for every major release or at least once every 12 months. SSG works with Symantec's internal penetration test team as well as top penetration testing companies to conduct Symantec's penetration tests. All product and service teams are required to work with SSG to arrange for penetration testing. SSG typically recommends the gray-box penetration test to such teams.

Vulnerability Management

Symantec has a formal process for handling and managing vulnerabilities. For any externally reported issues, SSG follows the process outlined in ISO 29147, Information technology — Security techniques — Vulnerability disclosure ([ISO/IEC 29147:2014(E)]).

SSG works with the impacted team(s) to:

- Recreate the environment and issue within Symantec's labs for an expedited resolution
- Facilitate a prompt and accurate response
- Avoid delays in new Symantec releases

By following this established process, releases are of a higher quality.

SECURITY ASSESSMENT TOOL

To enable product and service teams to accurately assess their implementation of the SDLC, SSG has implemented a Security Assessment Score tool (SAS). SAS is an internal software security tool developed by SSG in order to help the teams determine their SDLC maturity level, and help them continuously improve their software security practices.

REVIEW BOARDS

Although Symantec has several review boards, this section will focus on the most active and impactful boards.

Cryptography Review Board (CRB)

Symantec's CRB is a global board consisting of encryption experts from various groups within Symantec. CRB meets on a regular basis to discuss changes impacting various aspects of cryptography in order to provide product and service teams with the optimal and most up-to-date suggestions and recommendations pertaining to cryptography. CRB's goal is to help products meet or exceed Symantec's high standards for cryptographic security.

Additionally, CRB's provides information and guidance on best practices and common pitfalls to avoid. This includes analysis of data assets and configuration settings for appropriate categorization of risk and criticality, selection of cryptographic algorithms and associated key lengths, selection of hashing/message digest algorithms, appropriate key management, credential storage/transmission techniques (e.g. salting, hashing), and handling of sensitive data in memory and at rest.

Open Source Review Board (OSRB)

Symantec's OSRB is also a global team comprised of technical as well as legal resources. The OSRB sets the open source policy for Symantec and maintains Symantec's open source governance procedures. By tracking and reviewing the use of open source software, OSRB can effectively monitor public sources and alert product and service teams of vulnerabilities in their open source components and any subsequent new releases of the components.

SECURITY TRAINING

Symantec provides several types of security training ranging from multi-day role-based instructor-led training (ILT) taught by SSG security experts to short and convenient, up-to-date computer-based trainings (CBT) developed both internally as well as purchased from leading software security training organizations. When it comes to ILT, over the years SSG has developed a rich software security curriculum covering a wide range of topics, ranging from generic software security awareness, threat modeling, security tools, to multi-day secure development and security testing classes.

EXTERNAL PARTICIPATION IN THE SECURITY INDUSTRY

As a leader in software security, Symantec is heavily involved within the software security industry and participates with several organizations in an effort to discuss and help improve Symantec's secure development lifecycle. Additionally, SSG experts are also board members at some of these organizations.

Building Security in Maturity Model (BSIMM)

Symantec is an active contributor to the BSIMM community where Symantec frequently shares its software security practices with the rest of the BSIMM community. Additionally, Symantec strives to improve its security practices based on knowledge obtained from the BSIMM community.

Software Assurance Forum for Excellence in Code (SAFECode)

Symantec is one of the founding members of SAFECode and has been SAFECode's charter/board member since SAFECode's inception in 2007. Symantec leads SAFECode's Technical Leadership Committee (which promotes technical exchange/collaboration among SAFECode member organizations, identifying and solving common software security-related challenges, and produces various artifacts for sharing with the rest of the industry). Symantec actively participates and collaborates with other software vendors regarding the latest and best software security practices.

At the same time, via Symantec's collaboration with the rest of SAFECode community, Symantec ensures that its software security practices are in-line with the rest of the SAFECode community. Some of the examples of work produced as a result of Symantec's collaboration with the SAFECode community include various white papers on fundamental software security practices, security in Agile, security in the cloud, as well as many secure development and security testing training modules, all available for free on-line.

Open Web Application Security Project (OWASP)

Symantec is an official OWASP sponsor. Various SSG members are active within the OWASP community (e.g., hosting on-site regular meetings at various Symantec locations, participating on boards of local chapters, and actively assisting with OWASP community conferences).

IEEE Computer Society Center (IEEE-CSD)

Symantec collaborates with the rest of the software security industry through membership and active participation with IEEE's Center for Secure Design.

ABOUT SYMANTEC

Symantec Corporation is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

For specific country offices and contact numbers, please visit our website.
For product information in the U.S., call toll-free 1 (800) 745 6054.