McAfee Product Security Practices

2 June 2023

Table of Contents

Importance of Security

At McAfee, LLC we take product security very seriously. Our practices include designing for both security and privacy, in product software, IT applications, and cloud services. We have rigorous software security policies and processes designed to proactively find and remove software security defects such as security vulnerabilities. We understand that our products, IT applications, and cloud services must not only fulfill the stated function to help protect our customers, the McAfee software itself must also aim to protect itself from vulnerabilities and attackers. McAfee strives to build software that demonstrates resilience against attacks.

We also understand that our customers may, from time to time, wish to review our software security practices so that they may make their own risk-based decisions on how best to use our products and to fulfill any due diligence responsibilities they may have.

Specific policies and practices can vary by product. The summary of practices described in this statement applies to all McAfee branded products as well as customer facing IT and Web applications.

Software Development Lifecycle (SDLC) at McAfee
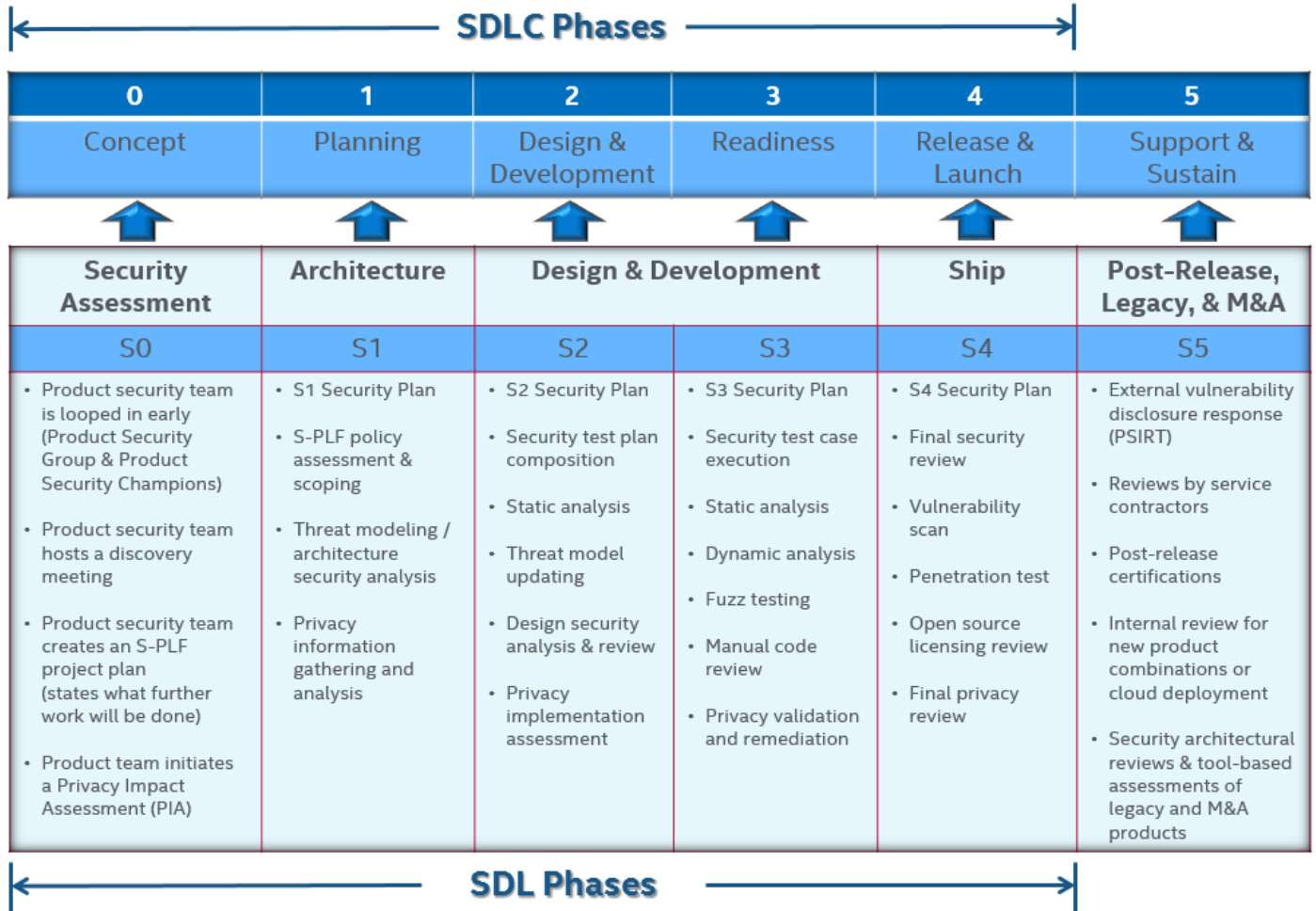
All of McAfee's software is developed using the Agile or Continuous Integration / Continuous Delivery (CI/CD) methodology. These agile and CI/CD practices are referred to as the Agile Software Development Lifecycle (SDLC). The Waterfall methodology is no longer used within McAfee. At McAfee, the SDLC is referred to internally as the Product Lifecycle Framework (PLF) v2.
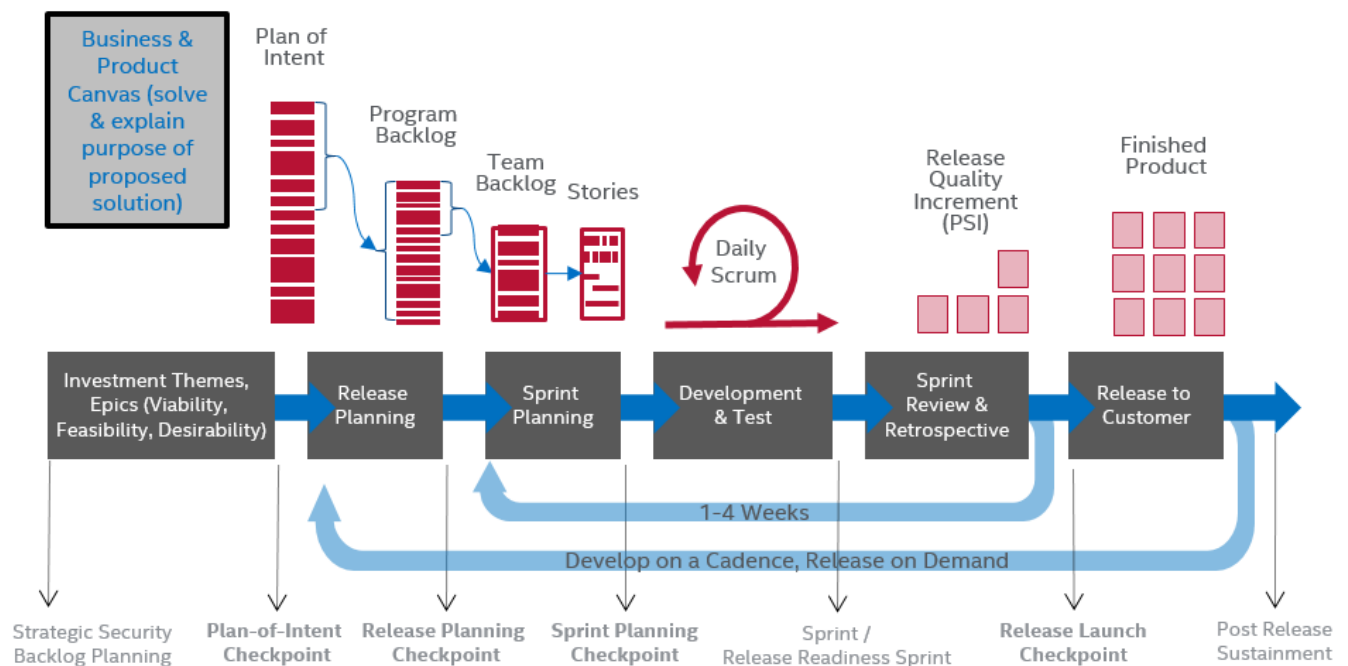
Development Methodologies

The chart below was developed for a traditional Waterfall SDLC. This chart has been adapted and redefined for McAfee's Agile SDL, which includes CI/CD. Security and privacy tasks are integrated into McAfee's SDL as a seamless, holistic process designed to produce software that has appropriate security and privacy built into it.

SDLC Phases

0	1	2	3	4	5
Concept	Planning	Design & Development	Readiness	Release & Launch	Support & Sustain

Security Assessment	Architecture	Design & Development		Ship	Post-Release, Legacy, & M&A
S0	S1	S2	S3	S4	S5
• Product security team is looped in early (Product Security Group & Product Security Champions) • Product security team hosts a discovery meeting • Product security team creates an S-PLF project plan (states what further work will be done) • Product team initiates a Privacy Impact Assessment (PIA)	• S1 Security Plan • S-PLF policy assessment & scoping • Threat modeling / architecture security analysis • Privacy information gathering and analysis	• S2 Security Plan • Security test plan composition • Static analysis • Threat model updating • Design security analysis & review • Privacy implementation assessment	• S3 Security Plan • Security test case execution • Static analysis • Dynamic analysis • Fuzz testing • Manual code review • Privacy validation and remediation	• S4 Security Plan • Final security review • Vulnerability scan • Penetration test • Open source licensing review • Final privacy review	• External vulnerability disclosure response (PSIRT) • Reviews by service contractors • Post-release certifications • Internal review for new product combinations or cloud deployment • Security architectural reviews & tool-based assessments of legacy and M&A products

SDL Phases

While the following description may appear to apply only to Waterfall development, the same set of security tasks are performed across the iterations of Agile just as they are performed in discrete phases during Waterfall. For CI/CD, SDL activities are determined by certain triggers which are set by milestones, events, and time intervals. McAfee encourages full engagement by software security architects and engineers within Agile sprints to ensure that security and privacy are integral parts of the Agile process.

Security Development Lifecycle (SDL)

In line with IT and application development industry standards such as ISO/IEC 27001, 27002, and 27034, BSIMM, and SAFECode, McAfee software development has processes designed to adhere to a Security Development Lifecycle (SDL).

McAfee's SDL covers the technical, operational, and enterprise aspects of building secure software. The SDL technical activities defined for each product, IT application, or cloud services release is the focus of this document.

Technical SDL Activities (Engineering)
- SDL.T1   Security Definition of Done (DoD)   (security **To Do** list before shipping)
- SDL.T2   Security Architecture & Design Reviews
- SDL.T3   Threat Modeling
- SDL.T4   Privacy & Data Protection Review
- SDL.T5   Secure Coding Standards   (includes cryptography)
- SDL.T6   Manual Code Review
- SDL.T7   Open Source & 3rd Party Libraries
- SDL.T8   Vendor Management   (includes software legal compliance)
- SDL.T9   Static Security Testing (SAST)
- SDL.T10   Interactive Security Testing (IAST)
- SDL.T11   Dynamic Security Testing (DAST)   (includes Web Application scanning)
- SDL.T12   Fuzz Testing
- SDL.T13   Vulnerability Scan
- SDL.T14   Penetration Testing
- SDL.T15   Security Testing & Validation
- SDL.T16   Operating Environment   (includes public cloud services)

Not all of the 16 technical SDL activities are mandatory for each product release. Some are conditionally required. The SDL.T1 Security Definition of Done (DoD) lists which activities are required for each release and is owned by the SSAs. Several activities are mandatory no matter what, such as the Security DoD (T1), Privacy Review (T4), Manual Code Review (T6), and Static Security Testing (T9).

Operational SDL Activities (InfoSec)
- SDL.O1   Program
- SDL.O2   Security Development Lifecycle (SDL)
- SDL.O3   Vulnerability Response (PSIRT/ASIRT)
- SDL.O4   People & Resources
- SDL.O5   Tools & Services
- SDL.O6   Policy & Compliance
- SDL.O7   Security Training
- SDL.O8   Metrics & Reporting
- SDL.O9   Maturity Models

Enterprise SDL Activities (IT)
- SDL.E1 Vulnerability Management
- SDL.E2 Risk Management
- SDL.E3 Asset Management
- SDL.E4 Remediation Management
- SDL.E5 Exception Management
- SDL.E6 Security Monitoring
- SDL.E7 Certifications

The following paragraphs describe, at a high level, the McAfee SDL process.

SDL.O2 High-Level SDL

For a new product, the security process typically begins at project initiation. A seasoned security architect or McAfee Software Security Architect (SSA) or Engineer (SSE) assesses a proposal for its security implications. The output of this engagement is any additional security features that will be added to software self-protection so that the software can be deployed by the different security postures of McAfee's customers.
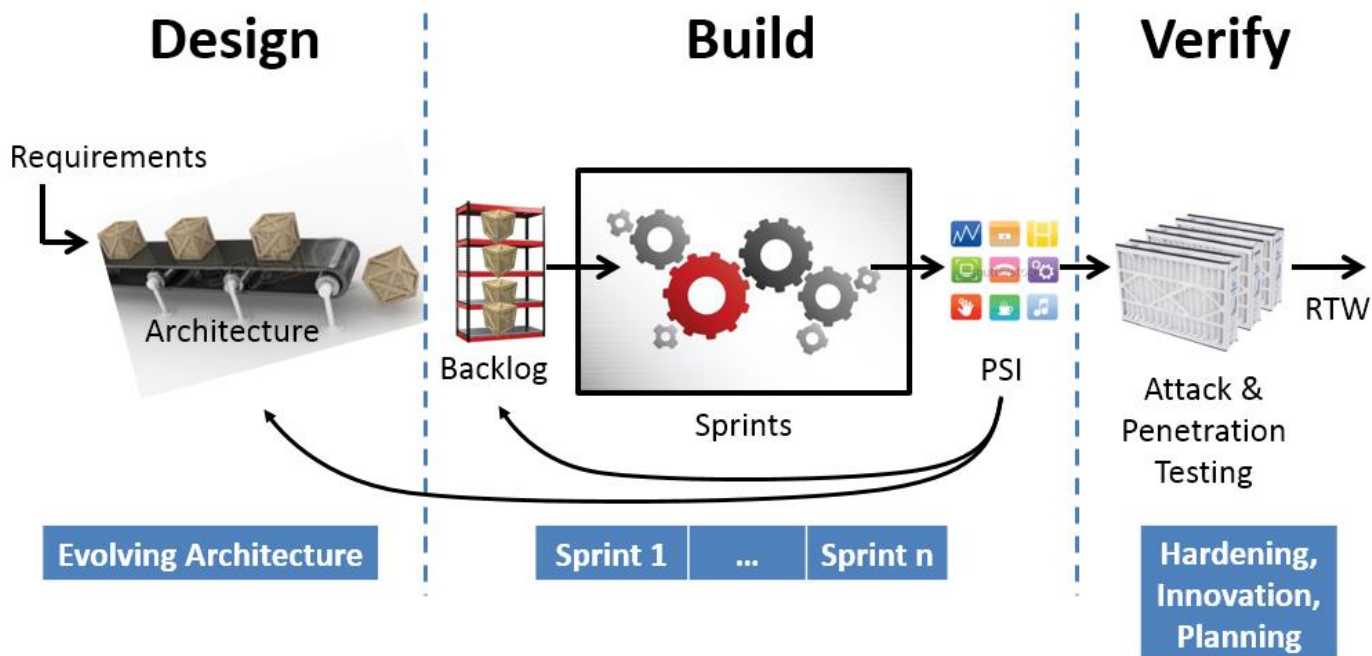
SDL.T2.1 Security Architecture Review

Any project that involves a change to the architecture of the product is required to go through a security architecture and design review. The proposed architectural and design changes are analyzed for security requirements, as well as analyzed within the whole of the architecture of the software for each change's security implications. An architecture review may be a discrete event, may be accomplished iteratively as the architecture progresses (Agile), or may be updated continuously (CI/CD).

SDL.T2.2 Security Design Review

The SDL requires that designs that contain security features or effects are reviewed to make sure that security requirements are built correctly. The SSA signs off when the design meets expectations. All functional items, including security design elements, are included in the thorough functional test plan. Like architectural reviews, a design review may be a discrete event or may be accomplished iteratively when design work occurs (Agile or CI/CD).

SDL.T3 Threat Modeling

A threat model is created or updated. The output of this analysis will typically be the security requirements that must be folded into the design that will be implemented.

SDL.T4 Privacy and Data Protection Review

In tandem with architecture and design reviews, privacy and data protection reviews are conducted. A Privacy Impact Assessment (PIA) is performed to determine if any additional privacy activities are required to protect personal data. Privacy reviews cover the whole lifecycle of personal data and often extend beyond the product collecting the data and include backend systems and infrastructure.

Sprint
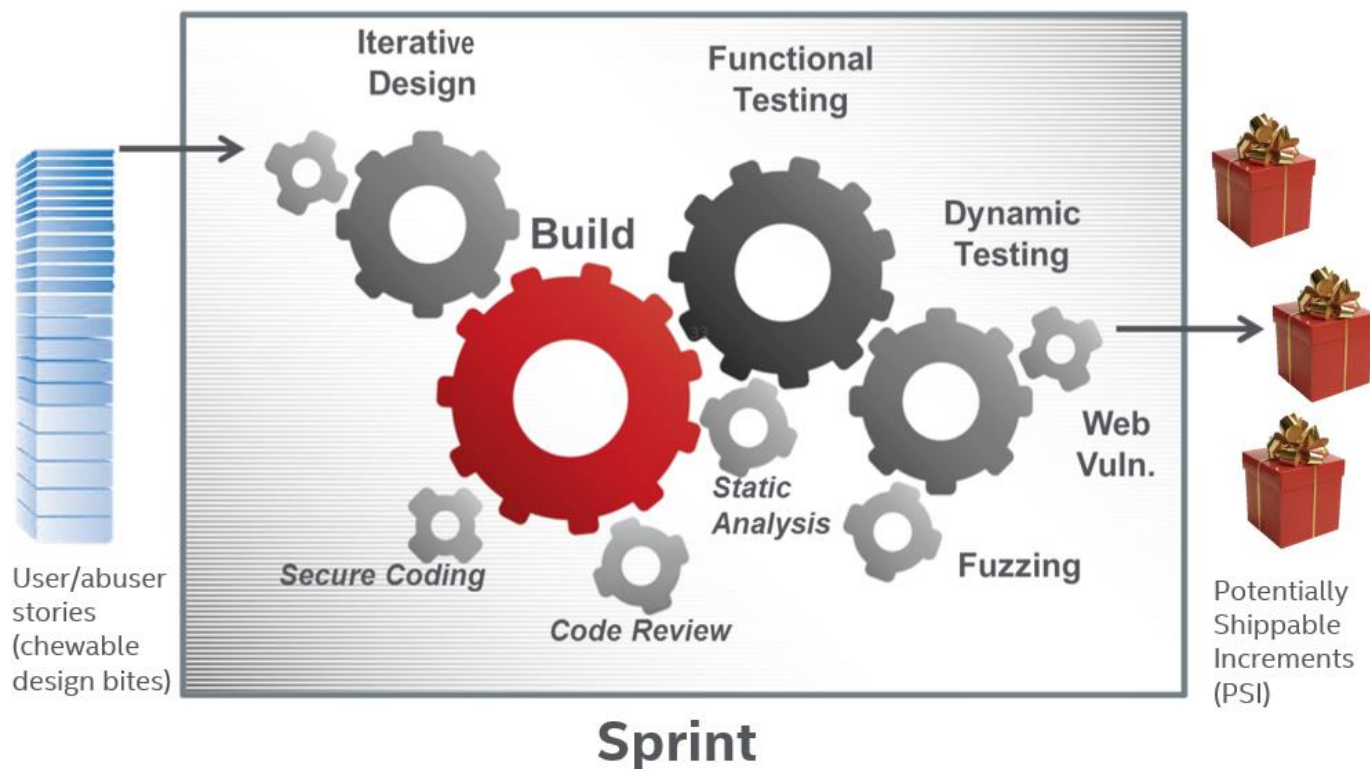
SDL.O7 Security Training

At McAfee, we foster industry standard secure coding practices. To that end, McAfee University and our McAfee Learning Management System (LMS) contains many courses on building software securely. Some are home-grown from internal subject matter experts, while others are purchased from third-party vendors. Developers are expected to pursue ongoing developer education. Self-training is encouraged.

SDL.O4 Software Security Architects

Software Security Architects (SSA) and Software Security Engineers (SSE) are assigned to each product line and IT application. Our 120+ SSAs and SSEs perform the SDL activities and help to confirm that every part of the software security process is applied appropriately.

Software Security Architect/Engineer Qualifications
1. A minimum of 3-5 years software development experience
2. A passion for or background in software security
3. Approved by the BU Engineering VP/Sr. Director & SSA BU Lead
4. Dedicate a minimum of 20% of their time doing software security tasks
5. Time to be trained in software security, reviews, tools, and processes
6. Be collocated within each engineering team / BU
7. Must not only know how to develop (build) software but also know how to deconstruct it (take it apart) while "thinking like a hacker"

SDL.T6 "Trust and Verify"

Alongside each developer's responsibility to produce secure code, McAfee has a "trust and verify" attitude. All new code must go through a manual code review. For non-sensitive and non-critical functions, this code may solely go through peer review. Critical and sensitive changes are also reviewed by staff with a sufficient level of expertise to assess critical changes.

Making use of overlapping complementary approaches, we employ several tools and automation to find security defects that may slip through manual code review. All code must be statically analyzed (unless no static analyzer exists for the language or environment). All web code is expected to undergo a web vulnerability scan. Other forms of input are routinely fuzz tested. Medium, High, and Critical severity issues must be fixed before release. Low severity issues are usually fixed or mitigated in future patches and product releases.
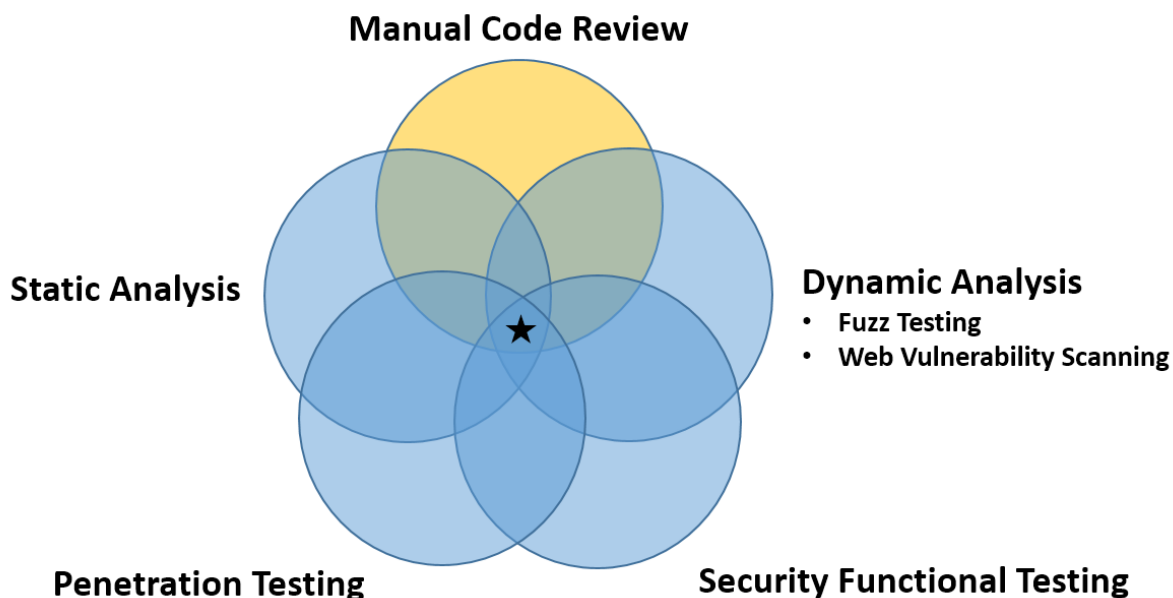
SDL.O5 Complimentary Security Testing

Critical customer-premise releases may additionally be put through a third-party penetration analysis on a case-by-case basis before release. All hosted systems are routinely vulnerability scanned and penetration tested by either our Information Security (InfoSec) department or by a third-party engagement.

We believe that the preceding is a solid plan in line with industry standards and best practices. Since no computer system can be absolutely secure, McAfee does not claim that the SDL will prevent any particular issue or any collection of issues. McAfee reevaluates and updates its SDL policies and process on a regular basis.

SDL.O6 McAfee Policies

McAfee believes that customer relations are best served through open, transparent dialogue. We encourage customer engagement, including requests about our software security process.

There are some limitations as to what we may share. For instance, we never share our source code outside of McAfee's direct control. Also, we never make available the list of vulnerabilities that are found as a result of our own internal investigations or from any of our automated testing tools. In the case of externally discovered vulnerabilities, once the findings have been addressed in a hotfix, patch, or new product release, all medium and high severity issues are documented in product release notes and in security advisories.

It is important to note that any scan of McAfee's production systems will be considered an attack. Response to a perceived attack will be rapid and decisive. Please coordinate your needs with your account manager. Availability of test systems is subject to customer need, customer cost, and timing.

SDL.O5 Software Security Tools

McAfee engineering teams apply an appropriate combination of tools depending upon the target programming language, architecture, and the execution run-time. These tools are a combination of internally developed, vendor purchased, and open-source tools. We may provide a list of utilized tools upon request. For reference, we use many of the security tools listed in OWASP's Security Testing Tools list.

SDL.O9.1 Product Security Maturity Model

The SDL describes the "what" of software security. McAfee's Product Security Maturity Model describes the "how well" of software security.

For each SDL activity, the PSMM describes 5 different levels from 0-4. These levels are:
- Level 0   None
- Level 1   Minimal   [Initial]
- Level 2   Good   [Basic]
- Level 3   Better   [Acceptable]
- Level 4   Best   [Mature]

With 16 technical activities and 9 operational activities, a perfect score is 100. McAfee software development teams assess their products annually using the PSMM. This allows us to focus our efforts on what each particular product needs the most, while measuring the overall maturity of each product line, engineering BU, and the company as a whole.
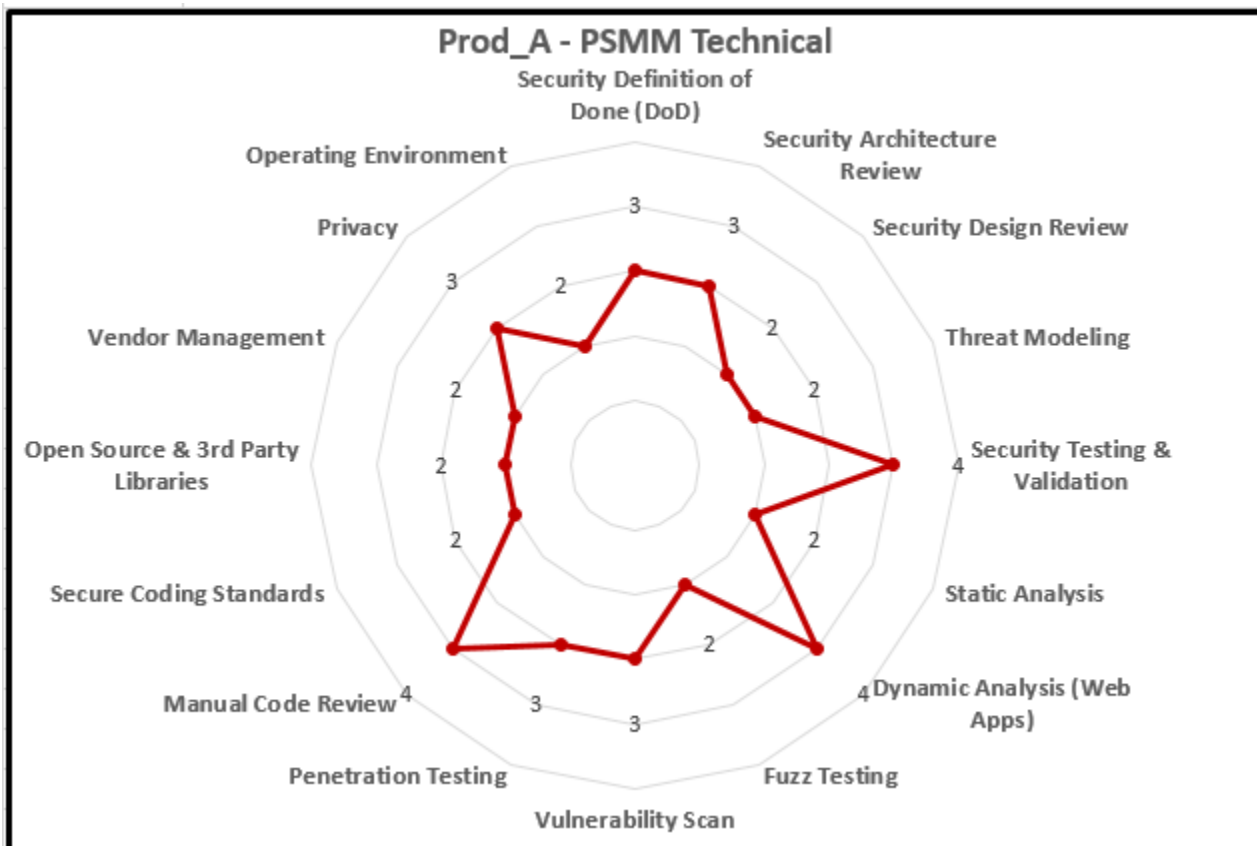
SDL.O3 Vulnerability Response

To handle vulnerabilities discovered in shipping McAfee products and live customer-facing applications, McAfee has a Vulnerability Response Team. This team consists of both PSIRT and ASIRT. The Product Security Incident Response Team (PSIRT) responds to product vulnerabilities in shipping products. They work with the discoverer and engineering to develop and deliver a patch and accompanying security bulletin. The vulnerability's severity (CVSS base-score) and business risk factors determine our fix response time (SLA). Similar to PSIRT, the Application Security Incident Response Team (ASIRT) responds to IT application and cloud services vulnerabilities in both externally and internally facing IT applications.

Disclaimer

No computer system can be absolutely secure. McAfee makes no warranty concerning any malfunctions or other errors in its hardware products or software products caused by viruses, infections, worms, or similar malicious code not developed or introduced by McAfee. McAfee makes no warranty that any hardware products or software products will protect against all possible security threats, including intentional misconduct by third parties. McAfee is not liable for any downtime or service interruption, for any lost or stolen data or systems, or for any other damages arising out of or relating to any such actions or intrusions.

Points of Contact

- Susanne Senoff, Deputy Chief Information Security Officer, McAfee LLC

Glossary

SDL   **S**ecurity **D**evelopment **L**ifecycle
A secure software development methodology that condenses the traditional waterfall methodology delivery cycles into weeks instead of month. Used by all McAfee software development teams.

ASIRT   **A**pplication **S**ecurity **I**ncident **R**esponse **T**eam
Part of the Vulnerability Response team within McAfee that responds to IT application and cloud services vulnerabilities in both externally and internally facing IT applications.

CI/CD   **C**ontinuous **I**ntegration **/ C**ontinuous **D**elivery
A time frame for releasing software updates more frequently than agile as more products become cloud-native.

DAST   **D**ynamic **A**nalysis **S**ecurity **T**esting
Run-time code review using automated tools.

GDPR   **G**eneral **D**ata **P**rotection **R**egulation
The EU's privacy regulation effective 25 May 2018.

IAST   **I**nteractive **A**nalysis **S**ecurity **T**esting
IAST is a form of application security testing that stems from a combination of dynamic application security testing (DAST) and runtime application self-protection (RASP) technologies.

PIA   **P**rivacy **I**mpact **A**ssessment
A privacy review conducted on all products to determine if additional privacy activities are required before a product is released.

PLF   **P**roduct **L**ifecycle **F**ramework
     McAfee's SDLC.

PSI   **P**otentially **S**hippable **I**ncrement
     An agile term that means that each unit produced from a series of Sprints has a quality of completion.
     A governance checkpoint determines each release. PSCs participate in release decisions. There is no
     mandate to release a PSI.

PSIRT   **P**roduct **S**ecurity **I**ncident **R**esponse **T**eam
     Part of the Vulnerability Response team within McAfee that responds to product vulnerabilities in
     shipping products. See more: https://www.mcafee.com/en-us/consumer-corporate/mcafee-
     labs/product-security-bulletins.html.

PSMM   **P**roduct **S**ecurity **M**aturity **M**odel
     Measures how well each SDL activity is being performed.

SAST   **S**tatic **A**nalysis **S**ecurity **T**esting
     Source code review using automated tools.

SDL   **S**ecurity **D**evelopment **L**ifecycle
     The security aspects of an SDLC.

SDLC   **S**oftware **D**evelopment **L**ife**c**ycle
     Describes the processes, activities, and deliverables for developing, testing, and shipping software.

SSA   **S**oftware **S**ecurity **A**rchitect
     A senior security architect within McAfee responsible for all security-related activities for a given
     product line.

SSE   **S**oftware **S**ecurity **E**ngineer
     A security engineer within McAfee responsible for all security-related activities for a given product line.
     SSEs are typically not as experienced as SSAs.

Revision History

Revision History			
Name	**Version**	**Change Description**	**Date**
Brook Schoenfield	1	Initial Draft	7 Aug 2014
Brook Schoenfield	2	Minor content updates.	28 Aug 2014
Brook Schoenfield	3	Minor content updates.	28 Aug 2014
Brook Schoenfield	4	Six-month review. Reformatted document.	9 Dec 2014
Harold Toomey	5	Six-month review. Rebranded from McAfee Inc. to Intel Security.	6 Apr 2015
Harold Toomey	9	Add Points of Contact	18 May 2015
Harold Toomey	10	Updated Software Security Tool List.	22 May 2015
Harold Toomey	14	Annual review. Added Glossary.	2 Feb 2016
Harold Toomey	15	Six-month review. Updated Agile SDL Activities list.	25 July 2016
Harold Toomey	16	Six-month review. Rebranded from Intel Security to McAfee, LLC. Removed Software from the title.	28 Mar 2017
Harold Toomey	17	Minor updates.	28 Apr 2017
Harold Toomey	18	Six-month review. Removed terms from the glossary.	12 Oct 2017
Harold Toomey	19	Six-month review. Renamed PSCs to SSAs. Added Revision History table for FedRAMP. Renamed title from Product to Software to include IT Application security. Added all SDL Activities.	2 Apr 2018
Harold Toomey	20	Added Application and Enterprise SDL activities. Removed James Ransome who left McAfee in June 2018.	5 July 2018
Harold Toomey	21	Renamed Agile SDL to McAfee SDL. Updated SDL activities list.	1 Nov 2018
Matt Valdes	22	Updated points of contact	1 June 2019
Matt Valdes	23	Six-month review. Minor content updates	18 Feb 2020
Matt Valdes	24	Minor content update.	02 Mar 2020
Matt Valdes	25	Bi-annual content review	29 June 2020
Matt Valdes	26	Renew expired links. Minor content update.	6 August 2020
Matt Valdes	27	Bi-annual content review	2 Feb 2021
Matt Valdes	28	Bi-annual content review	1 July 2021
Matt Valdes	29	Update resource links and contact information.	14 March 2022
Samir Rao	30	Bi-annual content review. Updated contact information and links.	1 July 2022
Samir Rao	31	Bi-annual content review. Minor content and contact information updated.	4 Jan 2023
Matt Valdes	32	Bi-annual content review.	2 June 2023

McAfee™

Together is power.