Trellix Product Security Practices

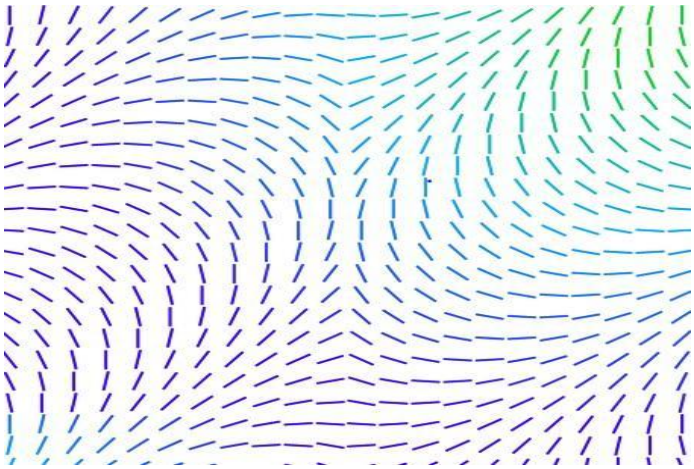

Table of Contents

1. The Importance of Security

Trellix recognizes the importance of security throughout the software development lifecycle and has both policy and practices which require that published software utilize the Trellix Security Development Lifecycle (SDL). Trellix SDL is a collection of practices focused on security aspects of software development which identify risks and vulnerabilities with published software for customers.

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 Company branded products as well as customer facing IT and web applications.

2. Trellix Security Development Lifecycle (SDL)

Trellix benefits from formal internal *Security Development Lifecycle* (SDL) software development practices which have been augmented with NIST SP 800-218, "Secure Software Development Framework" (SSDF) practices. The Trellix SDL includes the following practices, as applicable:

SDL.T1 Security Definition of Done (DoD)

The DoD document consolidates into a single location all security requirements for a product based on its risk and various factors including regulatory and industry frameworks that must be considered when developing a new software release. These requirements are addressed in each of the eighteen different SDL practices and are used by the Trellix Product Security team to reach a Go/No-Go decision to authorize a release.

SDL.T2 Security Architecture & Design Reviews

At inception and when new architectural patterns are introduced, a refresh and review of security architecture and design is performed for major releases to ensure that approved architectural patterns are present, and architectural antipatterns are not present. This information is used by the Product Security team to reach a Go/No-Go decision to authorize a release.

SDL.T3 Threat Modeling

At inception of a new product and when new threats are identified, a threat modeling document is refreshed and reviewed to identify applicable compensating controls that are applicable and that document how an inherent risk rating may be reduced to a lower residual risk rating which directly addresses potential risks. This information is also used to drive efforts to eliminate categories of threats in support of CISA's "Secure by Design" pledge, and NIST SP 800-218 practices to identify and prevent threats. Trellix utilizes multiple threat modeling paradigms that would be commercially recognized by software developers.

SDL.T4 Privacy & Data Protection Review

At inception of a new product or when privacy or data protection issues emerge (such as regulatory policies or legislation), or when new data sources for sensitive information are introduced, then a privacy and data protection review is performed which results in a Go/No-Go decision to authorize a release. This review is performed by our Trellix Legal department which provides for privacy and data protection personnel to perform the review.

SDL.T5 Secure Coding Standards

Trellix policy and practices require technical standards be identified for secure coding practices regarding both source code language level standards, in addition to functional standards including authentication, logging, encryption. Secure coding standards include language level constructs, practices, and will vary based upon the language(s) present within each product. By default, and where technically applicable, Trellix applies Open Worldwide Application Security Project (OWASP) analysis to source code to identify common weaknesses which is implemented in SDL.T9 SAST.

SDL.T6 Manual Code Review

Trellix restricts the ability (Principle of Least Privilege) for merging proposed changes into our source code by requiring a peer review (a “maker-checker” practice). This is to be performed by a senior project team member who is experienced in source code being modified to authorize merging of the proposed changes.

This practice is performed for all software merges without exception. This is used to ensure no unauthorized changes are introduced into source code within our products and that the changes proposed are consistent with the approved feature/function/fix approved by our product owners.

SDL.T7 Open Source & 3rd Party Libraries

Trellix policy and practices require formal approval for introducing any open source or third party commercial software as part of our Software License Compliance (SWLC) program. This creates an Intellectual Property Plan (IP Plan) which specifies open source, license compliance and purpose of the software component.

This is performed on a Trellix basis for approved/prohibited software, and also creates a required product specific IP Plan which is reviewed by Product Security as part of Go/No-Go decision to authorize a software release.

SDL.T8 Vendor Management

Trellix requires third party risk assessment for commercially source software and both security and operational risk for open source software. This includes software component registration, inbound and outbound license obligations, and provenance and traceability information.

SDL.T9 Static Security Testing (SAST)

Trellix policy requires automated Static Application Security Testing (SAST) analysis of source code which identifies industry standard Common Weakness Enumeration (CWEs) coding risks and provides Common Vulnerabilities and Exposures (CVEs) which are reviewed and dispositioned during each major, minor, or hotfix software release.

SDL.T10 Interactive Security Testing (IAST)

Trellix has deployed solutions that, when appropriate, are used to perform a combination of both white box and black box testing to assess security of our published software.

SDL.T11 Dynamic Security Testing (DAST)

Trellix has deployed multiple solutions performing automated vulnerability analysis of binaries and other runtime software artifacts by analyzing software interfaces that are based upon HTTP/HTTPS and HTML protocols for web-enabled application interfaces.

SDL.T12 Fuzz Testing

As appropriate or as needed due to new functionality or changes to existing interfaces, Trellix provides multiple solutions to perform automated testing of binary executables by probing all inputs, protocols, and file formats present in the executable. Results are reviewed by the Product Security team members and by Product Engineering team members and dispositioned.

SDL.T13 Vulnerability Scan

Trellix has multiple solutions deployed to perform automated analysis of an operating instance of our product/service to locate Common Vulnerabilities & Exposures (CVEs) which are then reviewed by both Product Engineering team members and Product Security Team members and dispositioned.

SDL.T14 Penetration Testing

Trellix uses both internal (self-performed) and external third party penetration testing for products which are human-led and curated assessments of products. Internal testing is performed using multiple tools/solutions and includes Web Application Security (WAS) scanning and industry recognized vulnerability scanning solutions.

SDL.T15 Security Testing & Validation

Trellix performs testing of security functions to ensure requirements are satisfied and are verified by both Product Engineering team members and Quality Assurance (QA) team members for mobile and Windows applications.

SDL.T16 Operating Environment

Trellix assesses non-cloud infrastructure related to operating products and focuses on review, remediation, disposition and management of both configuration related risks and common vulnerabilities & exposures (CVEs) directly supporting a specific product about to be deployed as a major, minor, or hotfix release. This information is used to support a Go/No-Go decision by Product Security and Product Engineering leadership.

SDL.T17 Cloud Environment

Trellix assesses cloud-only infrastructure related to operating products and focuses on review, remediation, disposition and management of both configuration related risks and common vulnerabilities & exposures (CVEs) directly supporting a specific product about to be deployed as a major, minor, or hotfix release. This information is used to support a Go/No-Go decision by Product Security and Product Engineering leadership.

SDL.T18 Record Evidence

Trellix uses an evidence-based approach to ensure consistent performance of mandatory practices related to risk, compliance, and Product Security areas. Evidence is prepared by the Product Engineering team members for software releases and is reviewed by the Product Security team to ensure consistent performance as necessary. Any risks resulting from review automatically result in Trellix risk registration & management practices. All of the information in the evidence package creates an immutable record as to the effective security posture and practices that relate to a specific software release. This evidence package supports the review and Go/No-Go decision by the Product Security team.