Strengthening Cisco Products

The Cisco Secure Development Lifecycle (CSDL) is a repeatable and measurable process designed to increase Cisco product resiliency and trustworthiness. The combination of tools, processes, and awareness training introduced in all development lifecycle phases ensures defense-in-depth, provides a holistic approach to product resiliency, and establishes a culture of security awareness.

CSDL applies industry-leading practices and technology consistently across the Cisco Product Line. Customers gain Tangible benefits through high-quality and trustworthy products that have fewer field-discovered product security incidents.

CSDL is better described by examining its compositional elements

- Product Security Requirements
- 3rd Party Security
- Secure Design
- Secure Coding
- Secure Analysis
- Vulnerability Testing

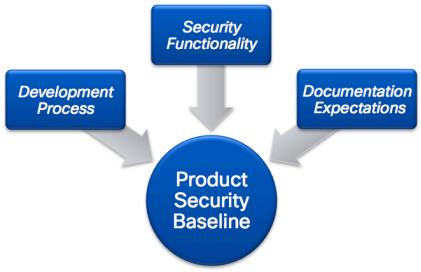
Product Security Requirements

Product Security Requirements define the internal and market based standards to which Cisco products must comply. These requirements have been assembled from internal and external sources, based on known risk, customer expectations and industry best practices. Products must address two types of product security requirements:

- *Cisco Internal Requirements:* Defined by the Cisco Product Security Baseline (PSB)
- *Market-based Requirements:* Outlined by the industry or space to which a product is deployed

Cisco Internal Requirements

The Cisco PSB is a living body of requirements that defines the security-related functionality, development process, and documentation expectations for the entire Cisco product portfolio. The PSB focuses on important security components such as credential and key management, cryptography standards, anti-spoofing capabilities, integrity and tamper protection, and session/data/stream management. Minimum requirements for resilience and robustness, sensitive data disposal, and logging are also prescribed in the PSB. This critical body of requirements is continually enhanced to incorporate new technologies and standards with the goal of building in inherent protections against evolving threats.



Market-Based Requirements

Markets and industries like finance, government, and medical, often place additional security requirements on Cisco customers. While these requirements may exceed those outlined by the PSB, Cisco strives to meet or surpass the industry demands.

Requested product certifications may include:

- Common Criteria Certification
- Cryptographic validation for products containing encryption functionality
- IPv6 certification
- Department of Defense (DoD) Unified Capabilities Approved Products List
- North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC-CIP)

Third-Party Security

A common industry practice is to incorporate both commercial and open source third-party software into product offerings. Consequently, products and customers may be affected when third-party vulnerabilities are discovered. To minimize the impact, Cisco uses integrated tools to gain visibility into its potential third-party software security threats, including:

- *Central Repository of Intellectual Property*: Cisco internally tracks products using third-party software through a centrally maintained repository. This single point of reference requires entry of any metadata associated with third-party code distributed outside the company, and allows for rapid identification of all affected Cisco products should a vulnerability be found.
- *Tooling to Facilitate Accuracy and Quick Response to Third-Party Vulnerabilities*
    - *Notification of Third-Party Software Threats and Vulnerabilities*: Cisco automatically alerts product teams from a continuously updated list of known third-party software threats and vulnerabilities, enabling quick investigation and mitigation.
    - *Scanning and Decomposition*: Cisco employs tools to inspect source code and images to improve third-party repository accuracy and completeness.

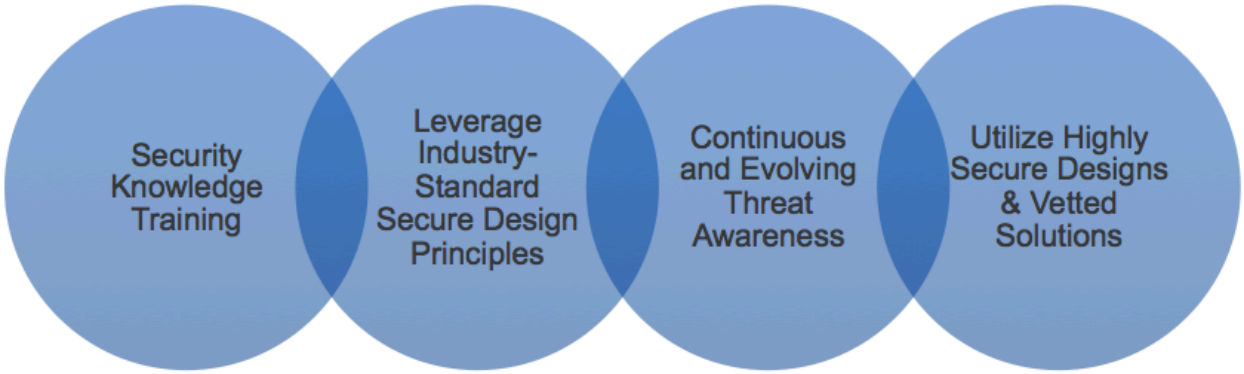
Secure Design

Making a product more secure begins with architecting a secure design. For Cisco, two complementary activities are key:

- Designing with Security in Mind
- Threat Modeling to Validate the Design's Security

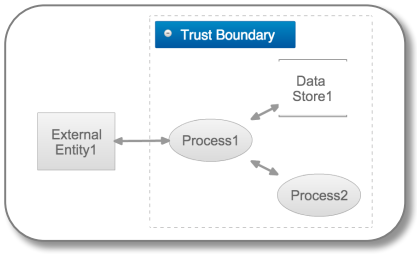
Designing with Security in Mind

Secure design requires an ongoing commitment to personal and professional improvement. Internal security training programs inspire all employees to become security aware, while compelling development and test teams to dive deep into security learning. Through continuous and evolving threat awareness, and by leveraging industry-standard principles and highly secure vetted solutions, Cisco strives to create products that are more secure by design.



Threat Modeling to Validate the Design's Security

Threat modeling is an organized and repeatable process designed to understand and prioritize a system's security risks. Cisco engineers follow the flow of data through a system and identify trust boundaries and inflection points where the data might be compromised. Once potential vulnerabilities and threats are identified, mitigation strategies can be put in place to minimize the risk. Cisco's Threat Modeling tool facilitates the process by exposing applicable threats based on the developers' diagram of the data flow and trust boundaries.



Secure Coding

Secure Coding Standards

Cisco's coding standards compel programmers to follow a uniform set of guidelines, aligned with industry best practices and determined by the requirements of the project and organization. Veteran developers know that coding and implementation errors can result in potential security vulnerabilities. While this knowledge comes with experience and training, Cisco developers at all levels are tasked to follow guidelines that help ensure threat-resistant code. An extensive security training program helps developers learn secure coding mechanisms and best practices.

Common Security Modules

To complement secure coding best practices, Cisco leverages a growing number of vetted common security modules. These Cisco-maintained libraries are designed to reduce security issues while enhancing the engineers' ability to confidently deploy security features. CiscoSafeC, CiscoSSL and other libraries focus on secure communications, coding, and information storage, while offering a centralized mechanism for security code updates.

Static Analysis

CSDL identifies key security checkers for Static Analysis (SA) tools to detect vulnerabilities in both C and Java source code. Through internal analysis, field trials, and limited business unit deployments, a set of checkers has been identified to maximize detection of security issues. Potential buffer overflows, tainted inputs, and integer overflows are targeted while false positives are minimized. All Cisco development teams are required to run Static Analysis with security checks enabled, review any generated warnings, and fix high-priority issues.

Vulnerability Testing

Vulnerability testing helps ensure that all Cisco products are tested consistently for security defects. The analysis is customized for each product by first identifying:

- All protocols that are implemented in the product
- Ports and services that are enabled by default
- Protocols, ports, and services that will be used in a typical customer configuration

Products are then evaluated to determine their ability to withstand probes and attacks with a minimum of three regiments of CSDL Vulnerability Testing:

- Protocol robustness testing
- Common attacks and scans by common open source and commercial hacker tools
- Web application scanning

Executing an effective security test plan requires the use of a variety of security tools from multiple sources. Cisco's Security Test Package combines them all into a single, easy-to-install collection of tools. This helps Cisco engineers test for security defects in a consistent and repeatable manner. Product teams also build custom tests to supplement the standard security test suite.

Dedicated penetration testing and security risk assessment engineers are also available to further identify and resolve potential security weaknesses. Vulnerabilities found during testing are triaged by the product teams and reviewed by Cisco's Product Security Incident Response Team (PSIRT).

Compliance with CSDL

CSDL Compliance is mandatory for all Cisco offerings. The process is built in to our standard engineering practices and is tracked internally. Cisco continues to improve the automation, streamlining, and CSDL validation efforts to assure complete coverage across products. Committed to customer success, Cisco strives to build trust into its offerings, and ensure consistent product security through proven techniques and technologies.