

# SECURITY&TRUST

Cisco is committed to building trustworthy solutions. The combination of secure development processes and technology is part of how we provide a more secure network foundation.



# CISCO SECURE DEVELOPMENT LIFECYCLE (SDL)

A repeatable and measurable process designed to increase the resiliency and trustworthiness of Cisco products.



Training and Education

Years of SecCon, the Cisco Security Conference

100,000 Employees with Continuous Security Education

**Monitor** 

Continuous

...

Threat Modeling Identify, Assess and

**Mitigate Risk** 

1,000+ Features Per Quarter



Product Security Baseline

200+ Specific Security Requirements



Vulnerability Testing

Whitehat Hacking

Leverages Several Automated Vulnerability Testing Tools

Checks Protocol



Threat Modeling & Security Requirements

## Develop

Secure Modules



# GLOBAL GOVERNMENT CERTIFICATIONS

All Cisco customers benefit from rigorous testing and certification requirements.











# Why authenticate?

Because counterfeit products have a higher risk of downtime, backdoors, logic bombs, built-in malware and spyware, inferior components, and greater potential for denial-of-service attacks.

# TRUSTWORTHY TECHNOLOGIES

Embedded security features that provide an added layer of protection across the network.



#### **Trust Anchor module**

Authenticates hardware and provides:

- Immutable device identity
  - Cryptographic functions
- Secure storage
- Random number generator with entropy source



#### **Secure Boot**

Helps ensure only authentic and unmodified Cisco software boots up on Cisco platforms.

Mitigates advanced persistent threats, physical possession and part replacement attacks.



### **Image Signing**

Digitally signed software protects against insertion of counterfeit and tampered software.

Cryptographically signed images ensure software is authentic and unmodified.



### **Modern Crypto**

Up-to-date and secure algorithms with support for international ECC curves.

Research and standards collaboration on Postquantum Crypto and Internet of Things.



#### **Runtime Defenses**

Protect running devices from attacks that change product software execution.

Built-in operating system protections that increase system resilience.

# VALUE CHAIN SECURITY

Leveraging Cisco's third party ecosystem to deliver security throughout the solution lifecycle.



### **A Layered Security Approach:**



At Cisco, our policy, process, and technology are designed to deliver trustworthy, secure products.

**trust.cisco.com** © 2024 Cisco and/or its affiliates. All rights reserved.