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.

**Reduced Vulnerabilities and Risk Visibility**
- Into Platform Integrity
- Faster Identification and Remediation of Threats

**CISCO SDL PHASE OVERVIEW**
- **Plan**
  - Threat Modeling & Security Requirements
- **Launch**
  - Security Readiness Criteria
- **Develop**
  - Secure Modules & Static Analysis
- **Validate**
  - Security Vulnerability Testing
- **Monitor**
  - Continuous Monitoring & Updates
- **Operate**
  - Security & Operational Management Process

ISO 27034 Compliant
- 3,000 Products Reviewed Since 2006

Processes are the backbone of pervasive security. Embedding processes into the business help us identify vulnerabilities and remediate issues quickly.

**Global Government Certifications**
- All Cisco customers benefit from rigorous testing and certification requirements.

**Training and Education**
- 11 Years of SecCon, the Cisco Security Conference
- 100,000 Employees with Continuous Security Education

**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

**CISCO SECURE DEVELOPMENT LIFECYCLE (SDL)**
- A repeatable and measurable process designed to increase the resiliency and trustworthiness of Cisco products.

**Trustworthy Technologies**
- Embedded security features that provide an added layer of protection across the network.

- **Trust Anchor module**
  - Authenticates hardware and provides:
    - Cryptographic functions
    - Immutable device identity
    - Secure storage

- **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.

**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**
- **Security Technologies**
  - Physical Security Practices
  - Logical Security

**Addressing Threats and Exposure at Every Stage:**
- Counterfeit
- IP Misuse/Information Security Breach
- Espionage

**A Layered Security Approach:**
- At Cisco, our policy, processes, and technology are designed to deliver identity and security protection.