# Building Trustworthy Systems with SDL

Chris Shenefiel

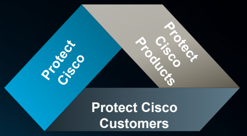
Protect Cisco

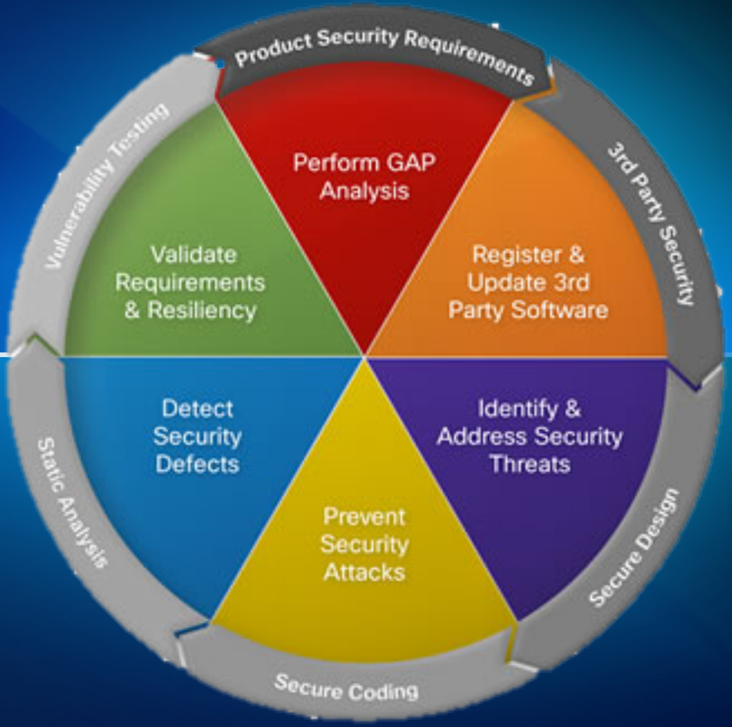
Protect Cisco Products

Protect Cisco Customers

# Agenda

- The Threat Problem
- The SDL Wheel
- SDL Implementation Across Cisco
- SDL Value





# The Threat Problem

Increasing Threats via the Networked Infrastructure

Increasing Product Security Incidents

Security Knowledge Base Needs to Be Expanded Across All Products

# The SDL Wheel

Product Security Requirements

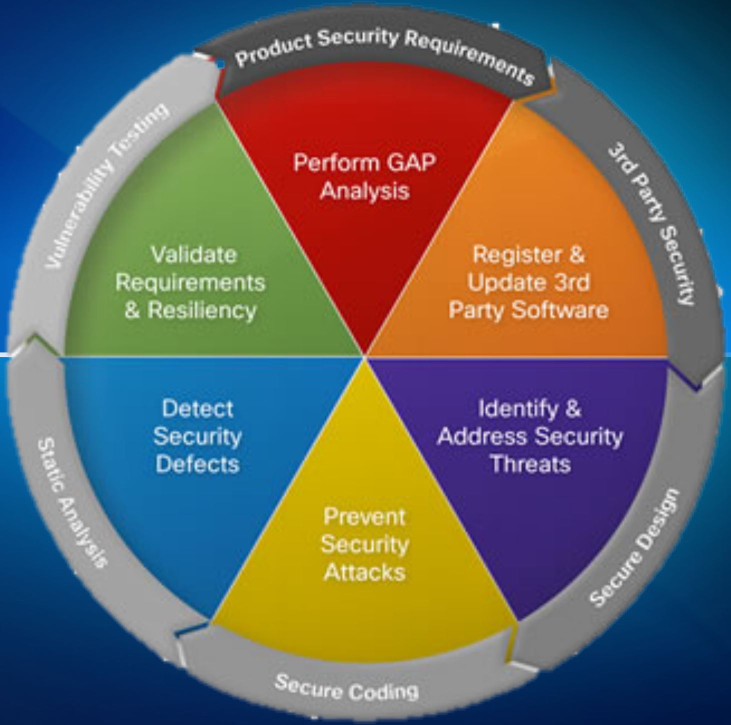
3rd Party Security

Secure Design

Secure Coding

Static Analysis

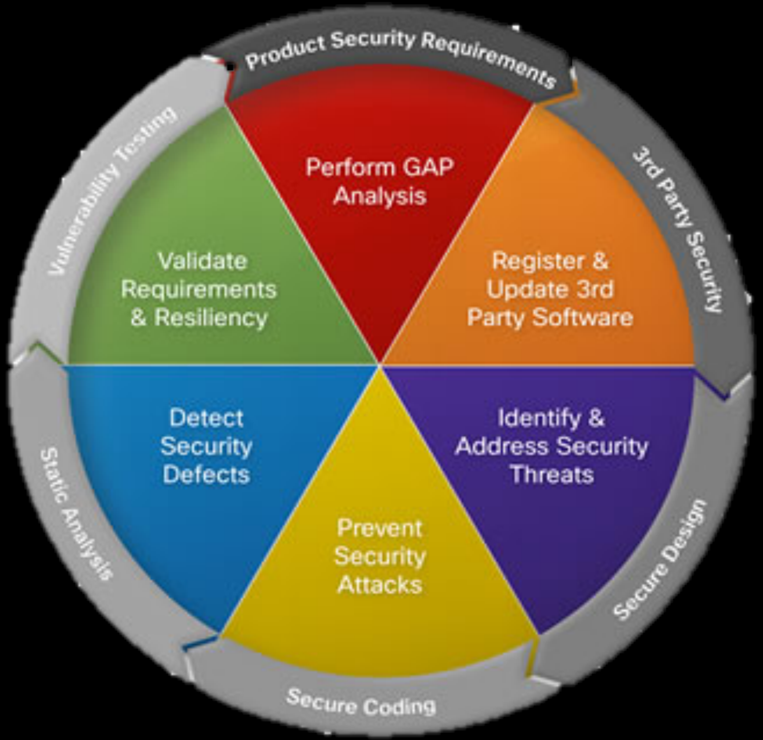
Vulnerability Testing



# The SDL Wheel & its Trusses

The SDL Wheel is a structure comprised of multiple triangular units (trusses).  Each add structural security stability to our products just as construction trusses add structural stability to buildings, bridges, and towers.

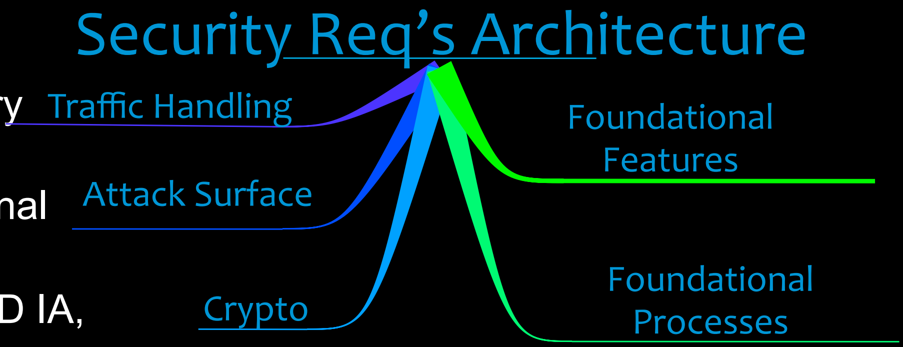
When applied as the entire wheel, SDL trusses connected to span the overall distance of the product development lifecycle.



# Product Security Requirements

Protect Cisco
Protect Cisco Products
Protect Cisco Customers

- Security Baseline Requirements
  - Insures consistency when implementing industry recognized standard practices
  - Incorporates requirements into product Functional Spec(s) and Test Plan(s)
  - Aligns with Public sector compliance (FIPS, DoD IA, Common Criteria)
- Product Security Baseline (PSB) Gap Analysis
  - Conduct at beginning of product lifecycle to drive additional requirements
  - Conduct prior to customer release as part of verification
    - Completed PSB GAP Worksheet



Security Req's Architecture

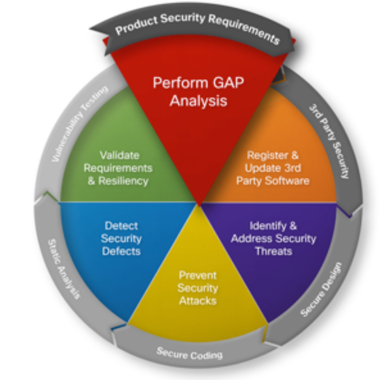
Traffic Handling

Attack Surface

Crypto

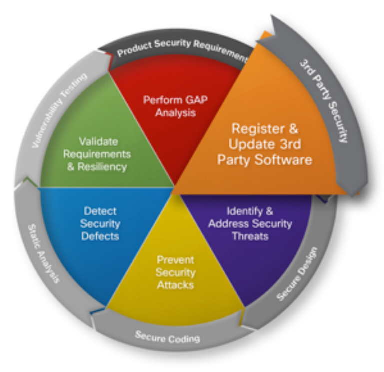
Foundational Features

Foundational Processes



# 3rd Party Software – Fundamentals

- Ensure your product as a whole is secure
- Minimize exposure by considering hidden costs in your decision process
  - Perform gap analysis
  - Establish maintenance plan
  - Verify no backdoors
  - Address all known vulnerabilities before ship
- Manage 3rd party security alerts
  - Register components in a centralized database
  - Contract support for critical security fixes
- Planned response to security issues
  - Follow established maintenance plan



# Secure Design – Threat Modeling

Methodology to identify & assess risk, and mitigate security problems in feature development

- Leads development engineers to consider how a feature can be attacked and how best to mitigate the attack
- **Not** a one-time event, it's a way of thinking about security for every feature

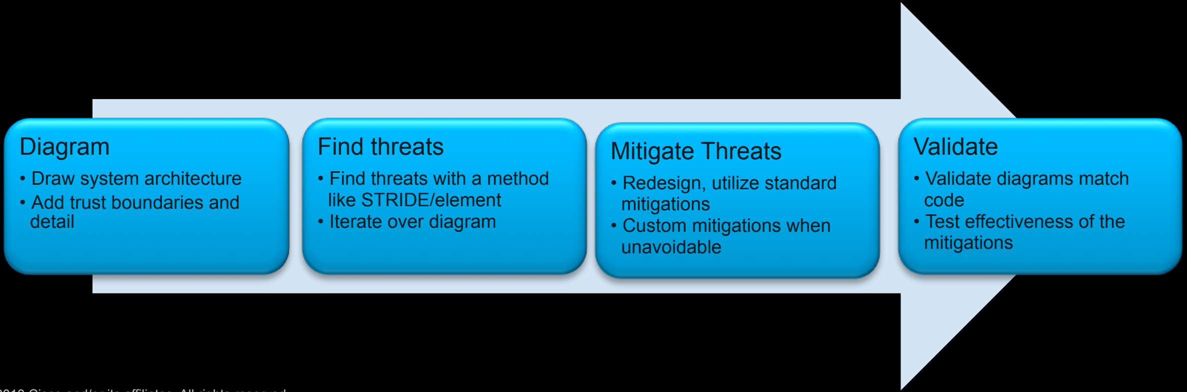
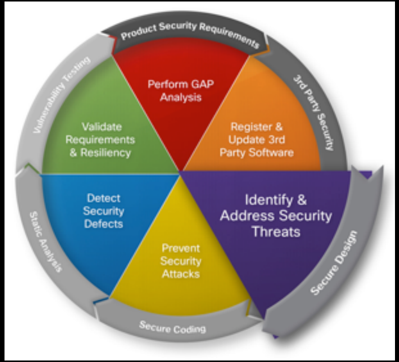


Diagram
- Draw system architecture
- Add trust boundaries and detail

Find threats
- Find threats with a method like STRIDE/element
- Iterate over diagram

Mitigate Threats
- Redesign, utilize standard mitigations
- Custom mitigations when unavoidable

Validate
- Validate diagrams match code
- Test effectiveness of the mitigations



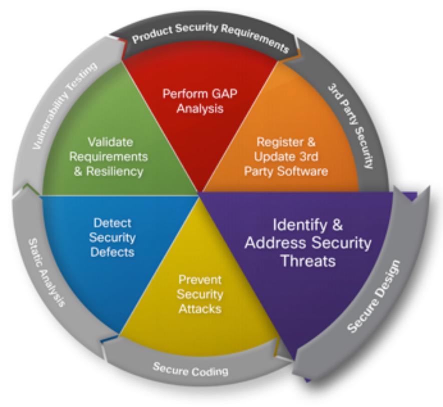
# Secure Design: Image Signing

## Image Signing

**Tamper protection for Cisco software**

Digital signature creation and verification using asymmetric key pairs

- Rommon
- Boot loader
- Image Base
- Packages



**Value Statement: Provide increased integrity and authenticity assurance, support the requirements of FIPS 140-3 and provide authentic software when securely booting the platform.**

# Secure Coding: Run Time Integrity

Protect Cisco

Protect Cisco Products

Protect Cisco Customers

## Run Time Integrity

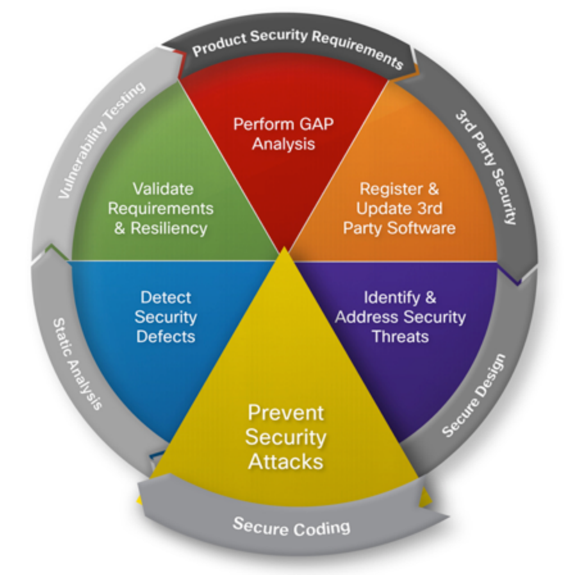
Common Code Across Product Line

- Object Size Checking
- Address Space Layout Randomization
- X-Space

Use “safe” libraries

Perform complete input validation

Best Practices Guidelines for each OS



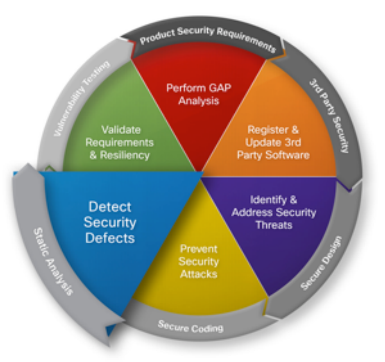
**Value Statement: Run Time Integrity and the other secure coding processes prevent many security attacks.**

# Static Analysis

- Established as part of the development process
- Security Checkers are very effective at finding key vulnerability types, such as certain buffer overflows
  - Run SA with Security Checkers enabled

Ongoing work to improve performance (find more actual and important bugs, fewer false positives)

- C/C++ switch from Klocwork to Coverity driven by significant performance improvement



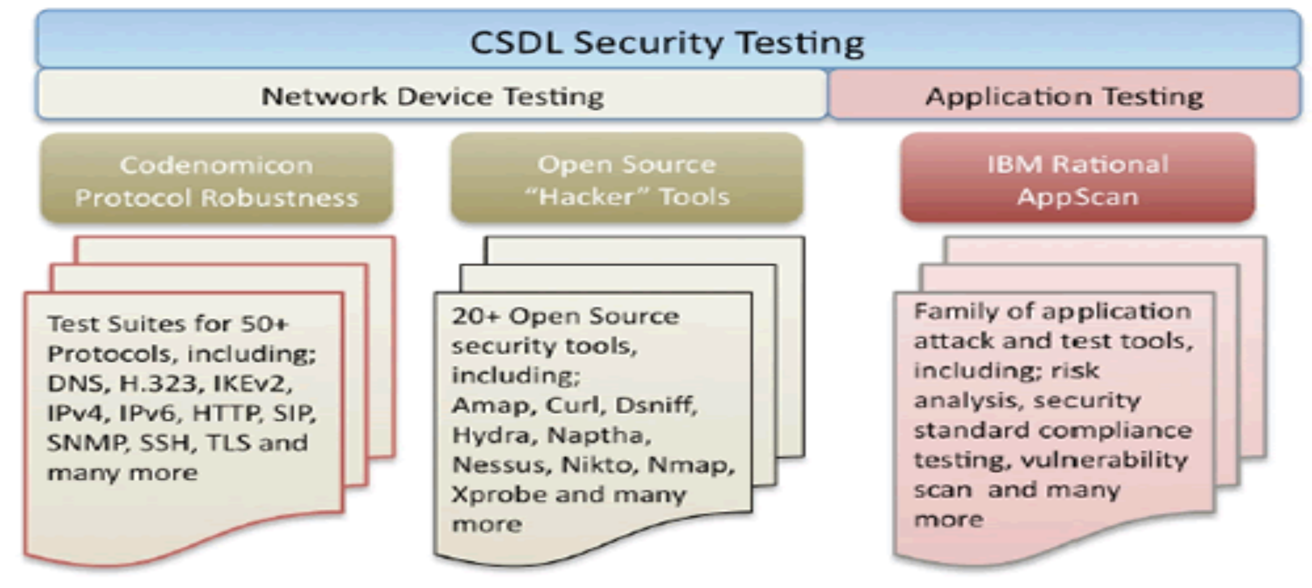
# Vulnerability Testing

Protect Cisco

Protect Cisco Products

Protect Cisco Customers

- **Check Protocol Robustness for** implementation of RFC, input validation and packet fuzzing
- **Duplicate Hacker Attacks** using open source tools to Penetrate, scan and attack



CSDL Security Testing

Network Device Testing

Application Testing

Codenomicon Protocol Robustness

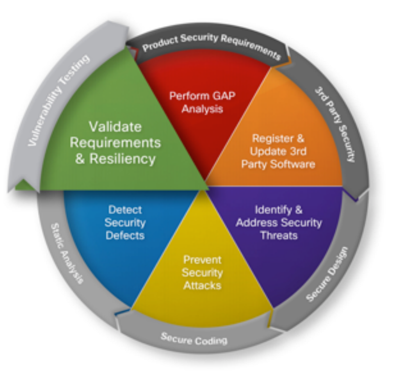
Test Suites for 50+ Protocols, including; DNS, H.323, IKEv2, IPv4, IPv6, HTTP, SIP, SNMP, SSH, TLS and many more

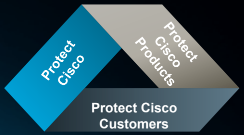
Open Source "Hacker" Tools

20+ Open Source security tools, including; Amap, Curl, Dsniff, Hydra, Naptha, Nessus, Nikto, Nmap, Xprobe and many more

IBM Rational AppScan

Family of application attack and test tools, including; risk analysis, security standard compliance testing, vulnerability scan and many more





# The Implementation of SDL

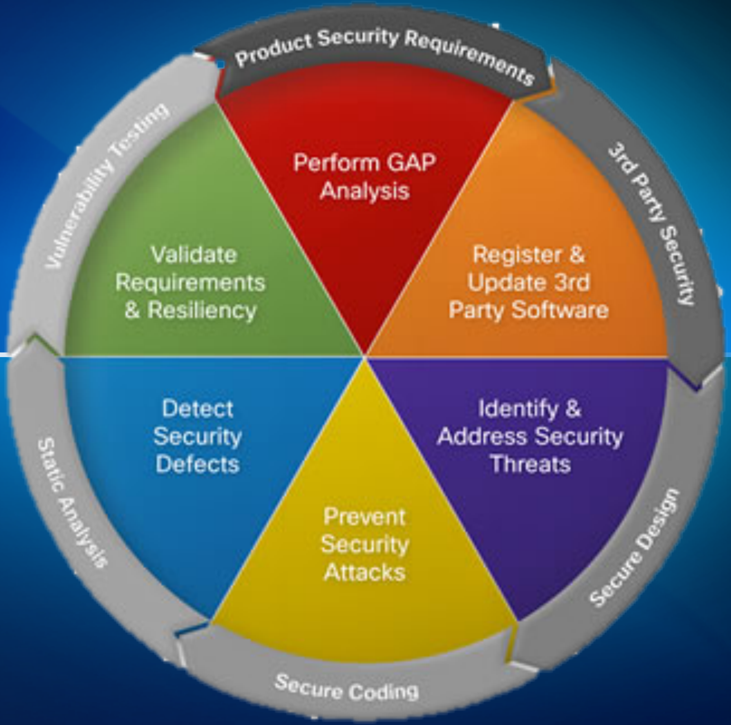
Maintaining Product Security Requirements

Training

Consulting with Security Engagement Managers & Security Advocates

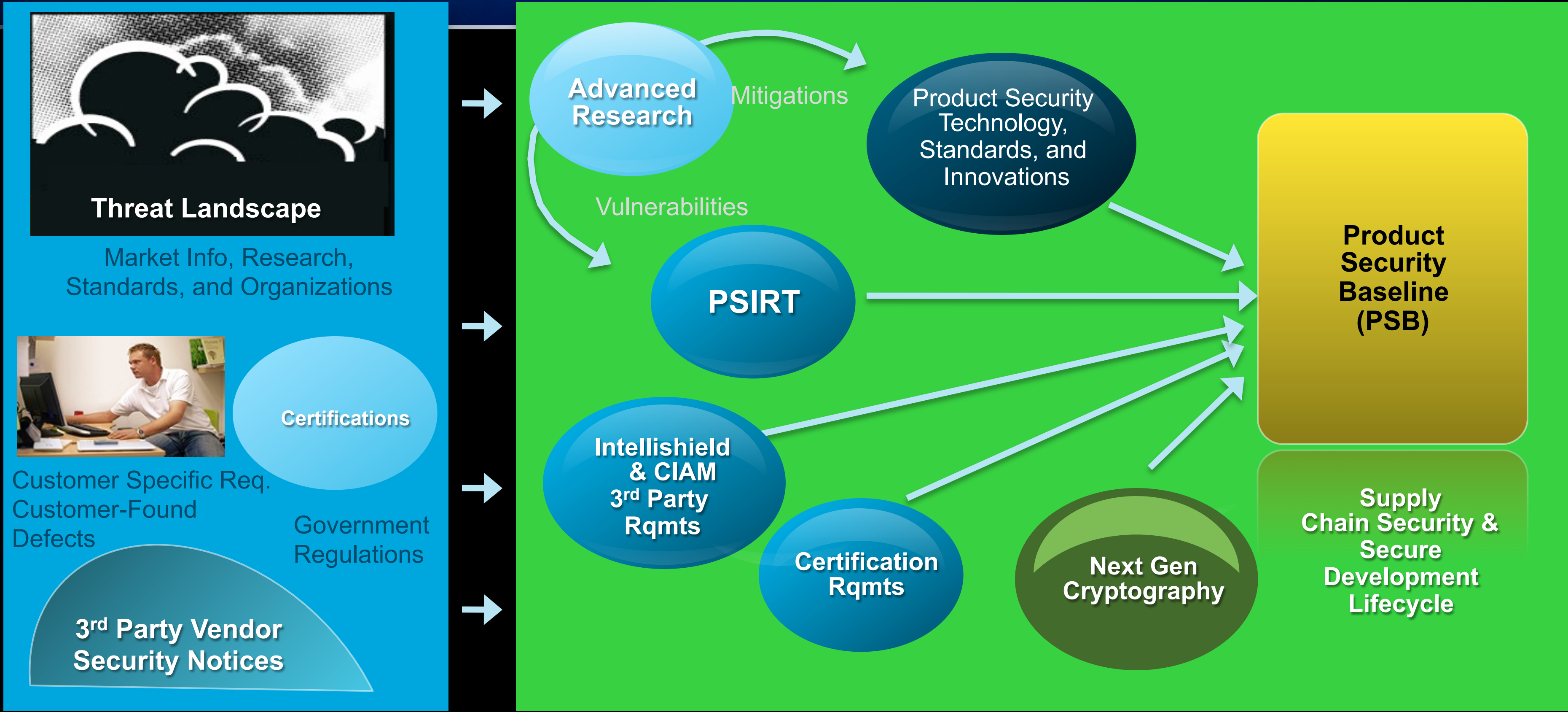
Accelerating via shared Security Technology Modules

Tracking and reporting compliance



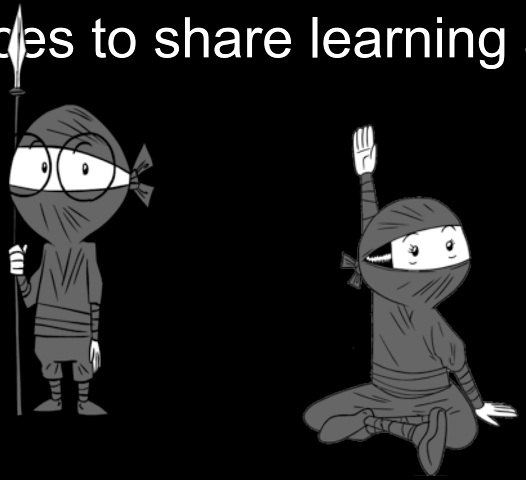
# SDL Maintenance: Constant Improvement Given New Threats, Mitigations, Technologies, and Applications

Protect Cisco
Protect Cisco Products
Protect Cisco Customers


Threat Landscape
Market Info, Research, Standards, and Organizations
Certifications
Customer Specific Req.
Customer-Found Defects
Government Regulations
3rd Party Vendor Security Notices
Advanced Research
Mitigations
Product Security Technology, Standards, and Innovations
Vulnerabilities
PSIRT
Intellishield & CIAM 3rd Party Rqmts
Certification Rqmts
Next Gen Cryptography
Product Security Baseline (PSB)
Supply Chain Security & Secure Development Lifecycle

# On-going Training: e.g., Cisco Security Ninja Program

- Computer based training to increase one’s “Security IQ”
- Multiple modules on a variety of product security topics
- Pass the assessment test and earn your belt
- Security conferences to share learning and best practices



Security IQ

# Consulting: Security Engagement Managers

- Accelerating SDL Implementation By Market Segments
- Security Experts Dedicated by Market Segment
- Works Cross Functionally to increase the Security IQ for the product teams

# Consulting: Security Advocates

## Accelerating SDL Implementation within the Development Team

- Security Advocate = a person who speaks in support of making products secure.
- Training every month on threats, mitigations, and solutions which they can apply in their product families.
- On-going Social Community for discussions, updates, and knowledge exchange.

Protect Cisco
Protect Cisco Products
Protect Cisco Customers

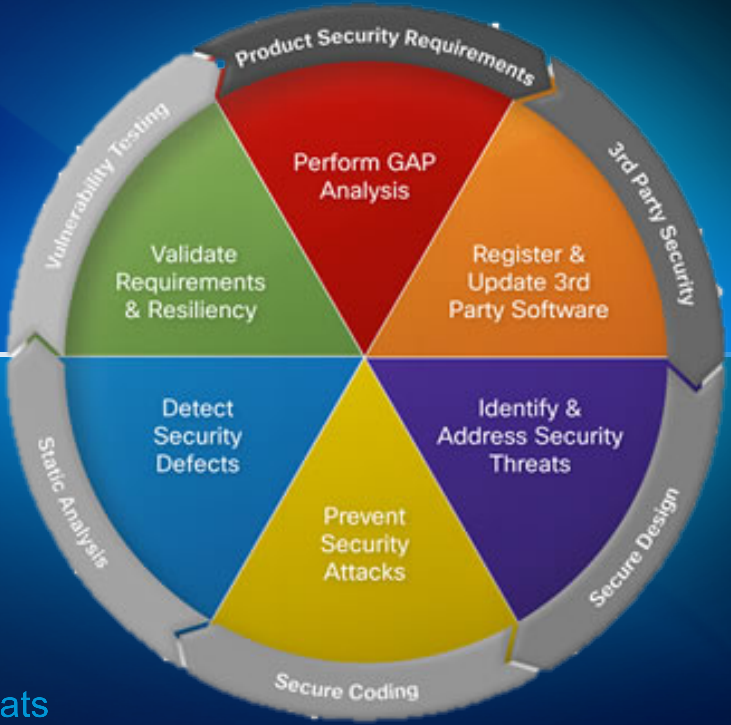
# The Value of SDL

Efficient Use of Development Resources

Consistency  in Product Security Technology Design And Maintenance

Alignment to Standards

Foundational Proactive Defense Against Known Threats

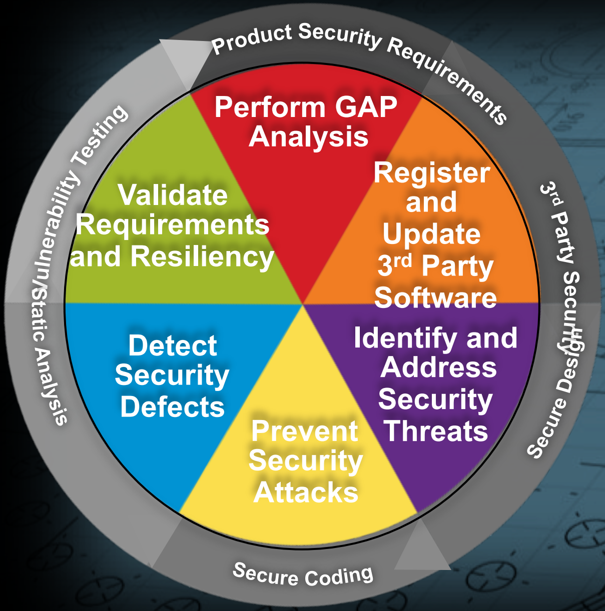


# Secure Development Lifecycle (SDL)

Protect Cisco

Protect Cisco Products

Protect Cisco Customers



## Why Security is Good Business Sense:

Reduced cost of fixing bugs

Remove expense and pain of changing security architecture

Reduces TTM (time to market) over time

Day-one advantage over our less security savvy competitors

Improve customer satisfaction

Lower PSIRT and CAP cases

Protect Cisco

Protect Cisco Products

Protect Cisco Customers

# Aligning to Standards

- CSDL conforms with the guidelines of ISO 27034
    - Following CSDL is part of Cisco’s ISO compliance
    - In 2013, Cisco used ISO/IEC 27034-1, as a baseline to evaluate CSDL.

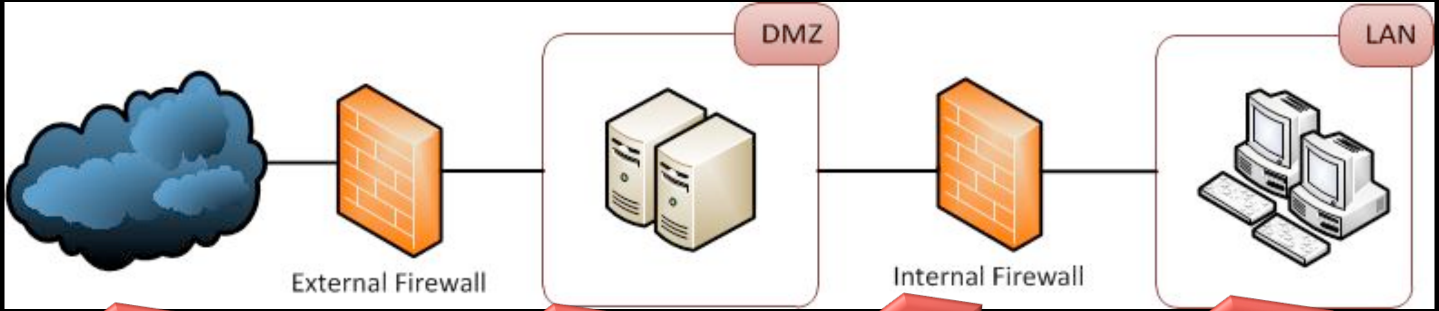
      “All current mandatory application security related policies, standards, and procedures along with their supporting people, processes, and tools meet or exceed the guidance in ISO/IEC 27034-1 as published in 2011.”
- Product Security Baseline aligns with Common Criteria certification requirements

# SDL: Foundational Layer for Effective Threat Defense in a multi-layered approach

Remote, Adjacent and Local attack protection

Protect Cisco<br>Protect Cisco Products<br>Protect Cisco Customers

The network is the first attack point. Once in, attackers can infiltrate and steal, disrupt and monitor



Initial Penetration – Network Edge

Next Penetration - DMZ

Break internal firewall to enter the LAN

Once inside Enterprise network, external hacker infiltrates to act

# Once in, attackers further infiltrate, looking for prized targets

Once in the Enterprise, attackers typically expand access to multiple systems in order to steal information or disrupt operations

Multiple levels of security inside and outside the network make infiltration and theft much more difficult

# Theft is a growing motivation for attacks:

## Verizon 2015 DBIR

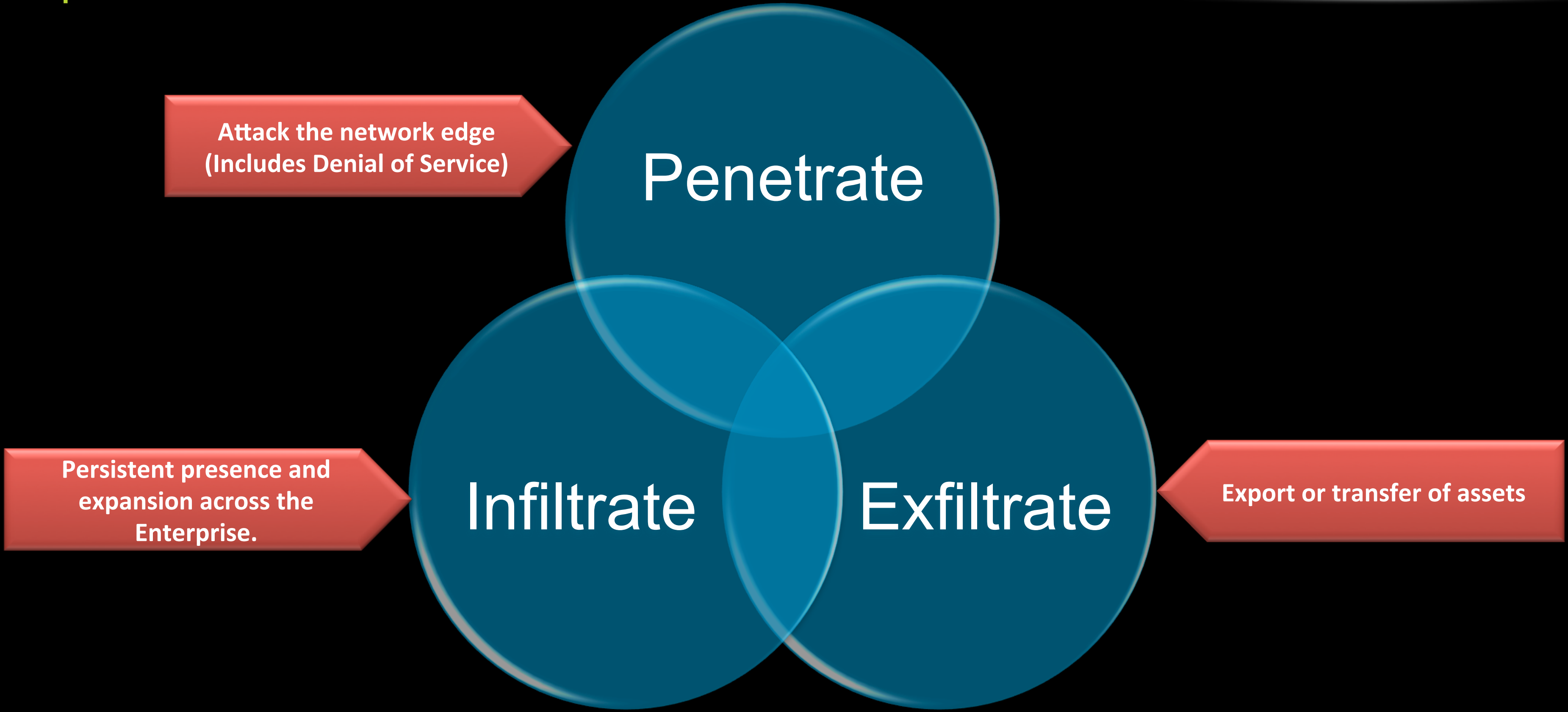
- The 2015 Data Breach Investigations Report (DBIR) analyzes 79,790 incidents and 2,122 confirmed breaches
- The highest number of breeches affected public sector institutions (60%)
- 92% of breaches were perpetrated by outsiders
- 70% of attacks with known motives targeted secondary victims
- 60% of attacks compromise victims in minutes
- More than 70% of attacks used well known vulnerabilities

http://www.verizonenterprise.com/DBIR/

# Profile Attacker Threat Activities

## Implication to Systems Development and Operations Requirements

Protect Cisco
Protect Cisco Products
Protect Cisco Customers



Attack the network edge (Includes Denial of Service)

Penetrate

Persistent presence and expansion across the Enterprise.

Infiltrate

Exfiltrate

Export or transfer of assets

# DBIR Profile of Attack Patterns
## Financial Services

Protect Cisco

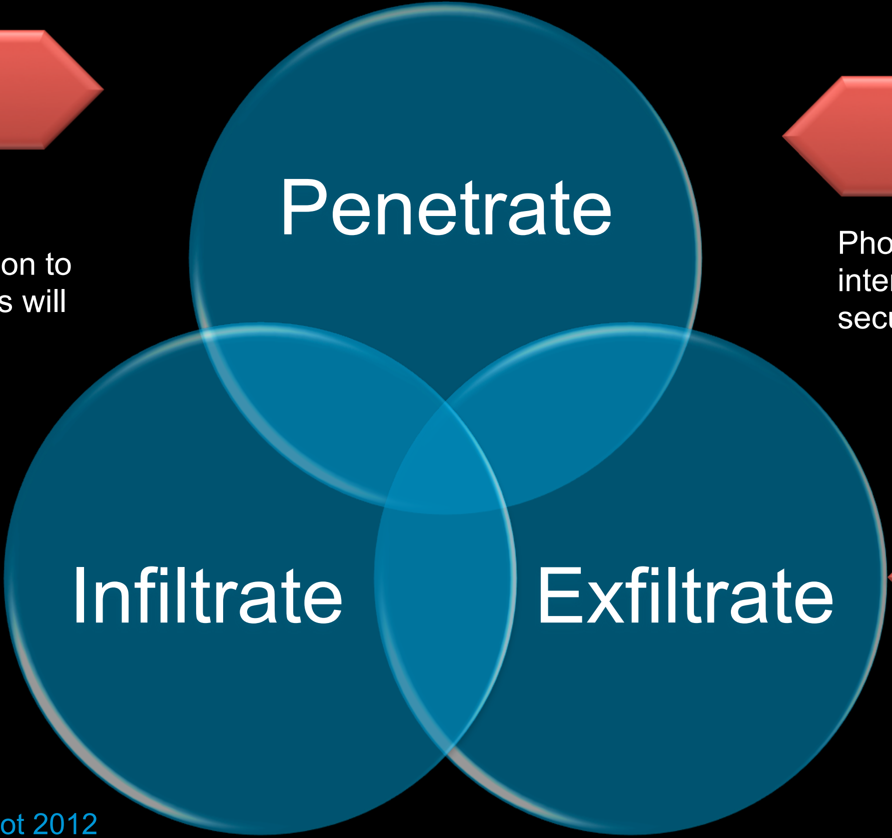
Protect Cisco Products

Protect Cisco Customers

**Persistent Poking**

Financial Services and Insurance companies must pay special attention to the Penetrate phase since attackers will persist at the edge until they find a vulnerability.

**Malware used after penetration**



Penetrate

Infiltrate

Exfiltrate

**Social Engineering**

Phone calls or emails impersonating internal authorities seeking security credentials.

**Export financial account information or money**

Source Verizon DBIR Industry Snapshot 2012

# DBIR Profile of Attack Patterns

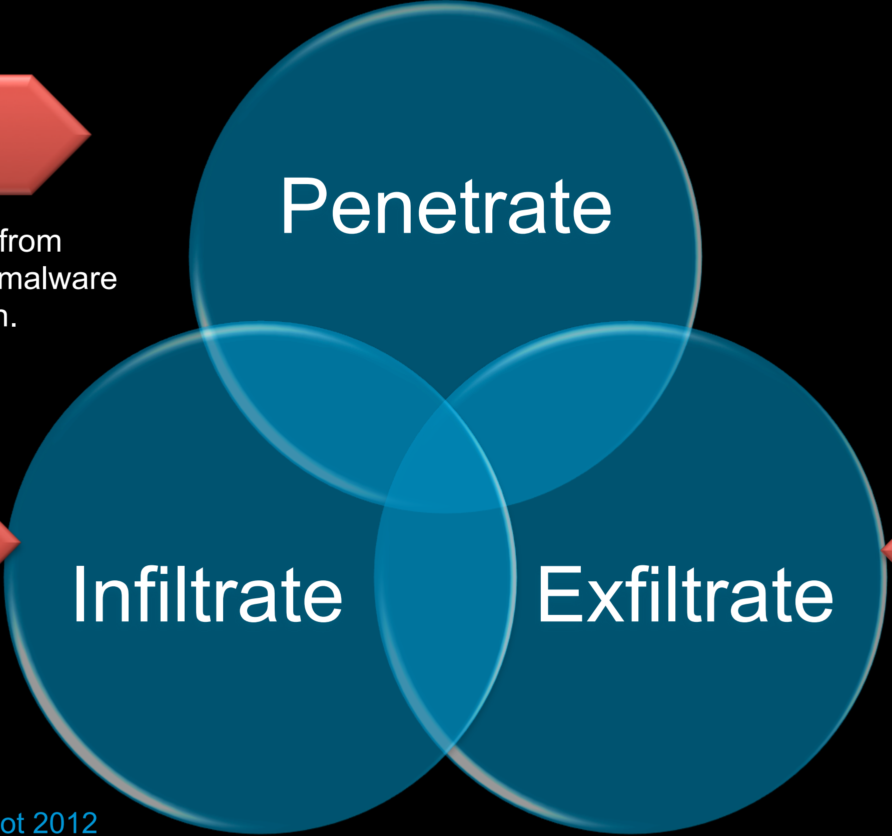
## Information/Public Sector Companies (Manufacturing, Government, IT Services)

**Social Engineering**

Majority of compromises resulted from combined social engineering and malware which stole credentials/information.

**Initial attack to penetration (hrs)**
**Initial compromise to discovery (yrs)**

Objective is most often intellectual property so the goal is to stay in as long as possible

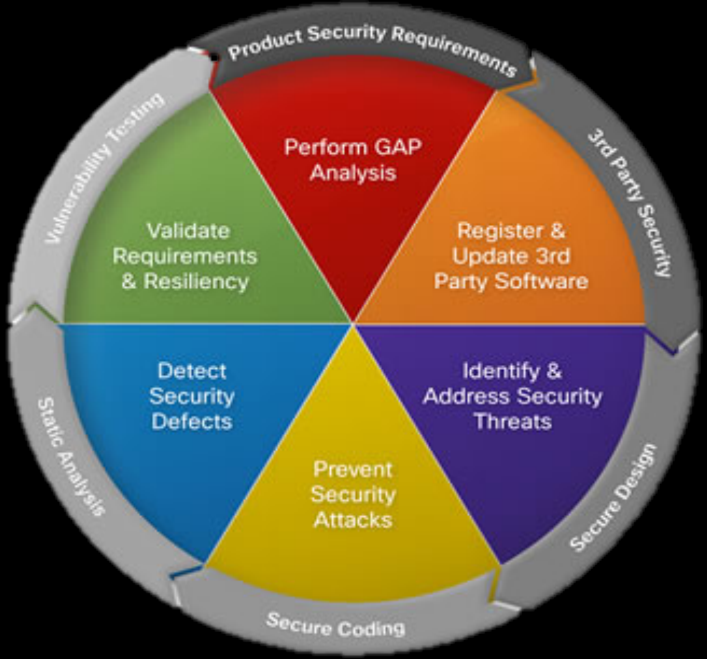


Exfiltrate assets (backdoors, spyware, steal credentials)

Source Verizon DBIR Industry Snapshot 2012

# How Secure Development Protects Software Products

- Secure Development builds security into the products that protect the network from
  - Penetration
  - Infiltration
  - Exfiltration



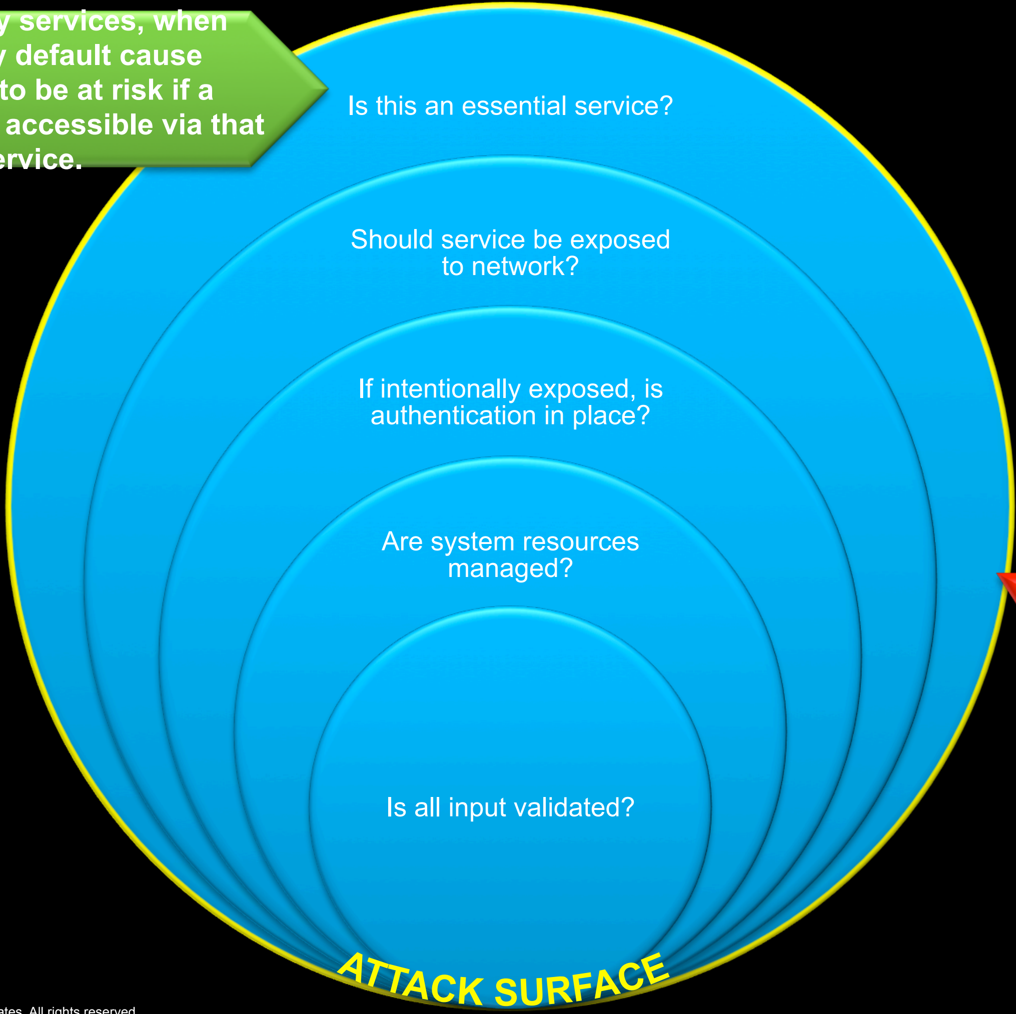
The following represents a select subset of Cisco's Product Security requirements

Protect Cisco

Protect Cisco Products

Protect Cisco Customers

**Unnecessary services, when enabled by default cause customers to be at risk if a vulnerability is accessible via that service.**


Is this an essential service?
Should service be exposed to network?
If intentionally exposed, is authentication in place?
Are system resources managed?
Is all input validated?
ATTACK SURFACE

# Penetrate RISK

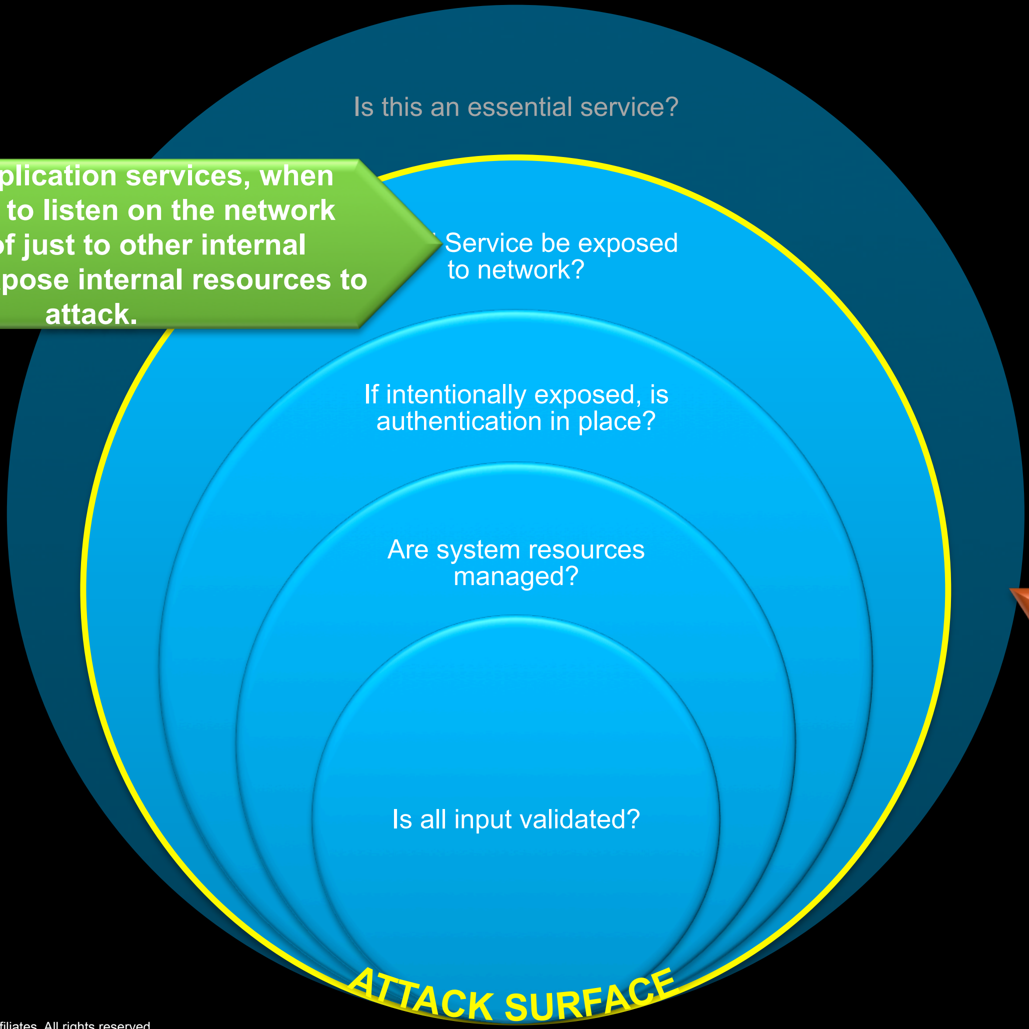
Perform GAP

**Product Security Requirements**

**Prohibit non-essential services and requires scans to reveal listening services**

| Industry | Reference |
|---|---|
| Defense | APP STIG 6030 |
| NERC CIP | R2 |

Protect Cisco
Protect Cisco Products
Protect Cisco Customers



Is this an essential service?
Service be exposed to network?
If intentionally exposed, is authentication in place?
Are system resources managed?
Is all input validated?
ATTACK SURFACE

**Internal application services, when configured to listen on the network instead of just to other internal processes expose internal resources to attack.**

# Penetrate RISK

Identify & Address Security Threats
Secure Design

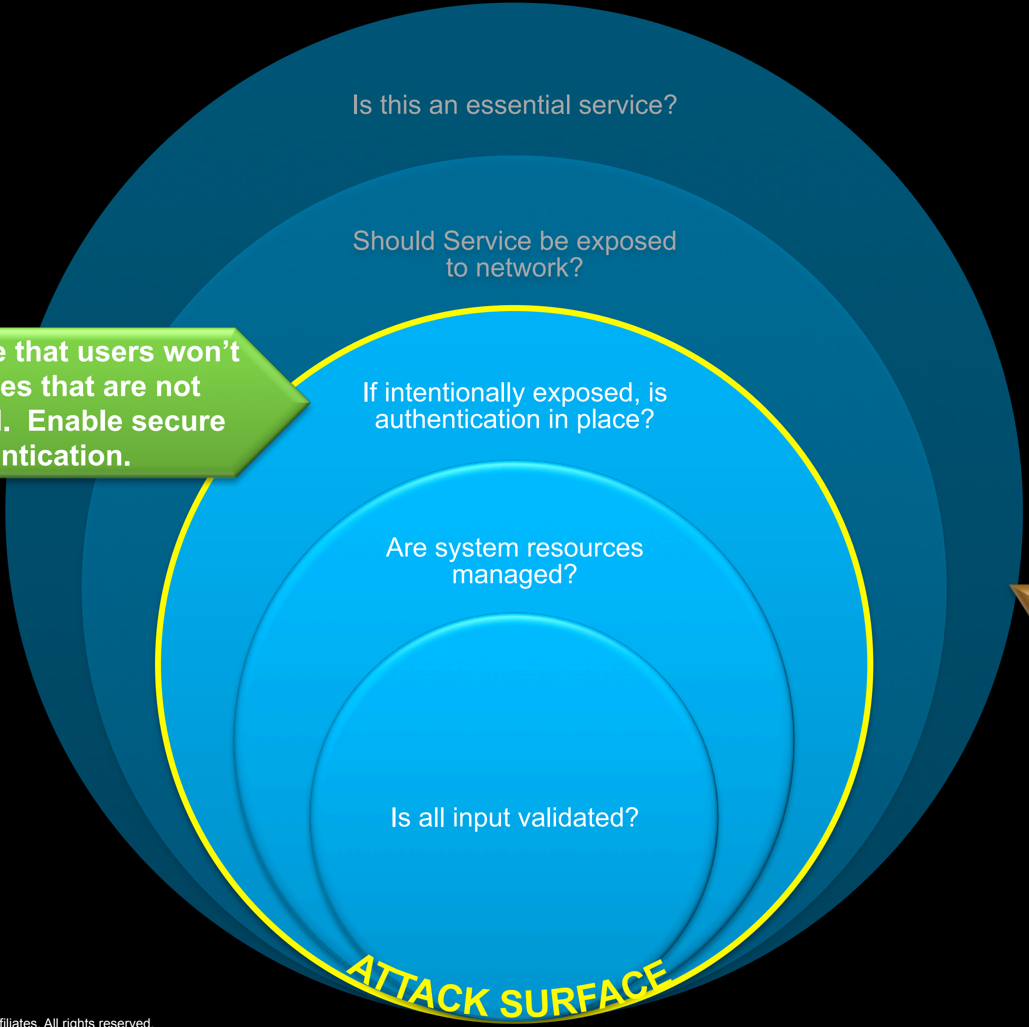
**Threat Modeling analyzes what needs to be exposed to whom and how.**

| Industry | Reference |
|---|---|
| Defense | APP STIG 6300<br>NET STIG 0135 |
| NERC CIP | R2.1, R2.2 |

Protect Cisco

Protect Cisco Products

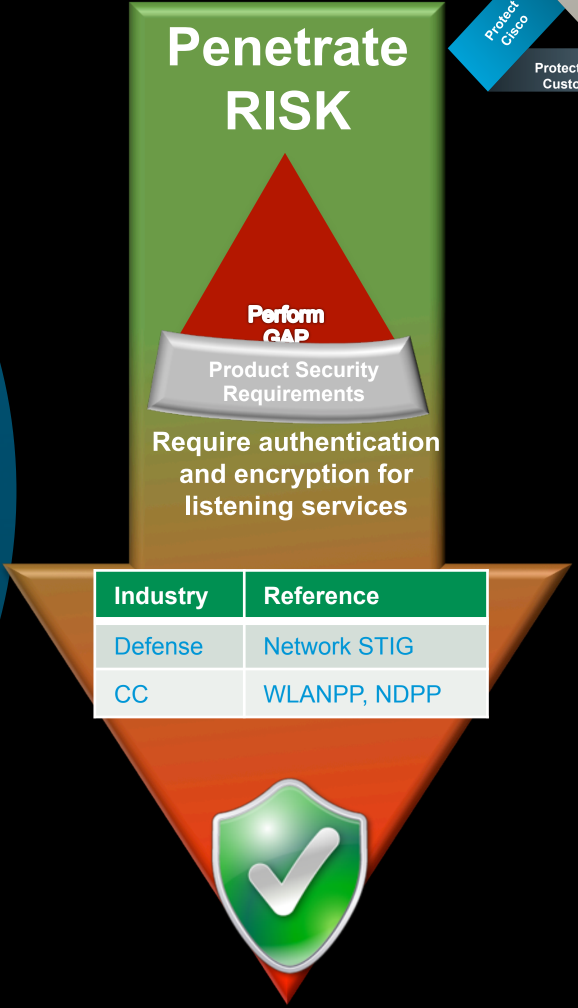
Protect Cisco Customers



Is this an essential service?
Should Service be exposed to network?
If intentionally exposed, is authentication in place?
Are system resources managed?
Is all input validated?
ATTACK SURFACE

Don’t assume that users won’t find services that are not documented. Enable secure authentication.

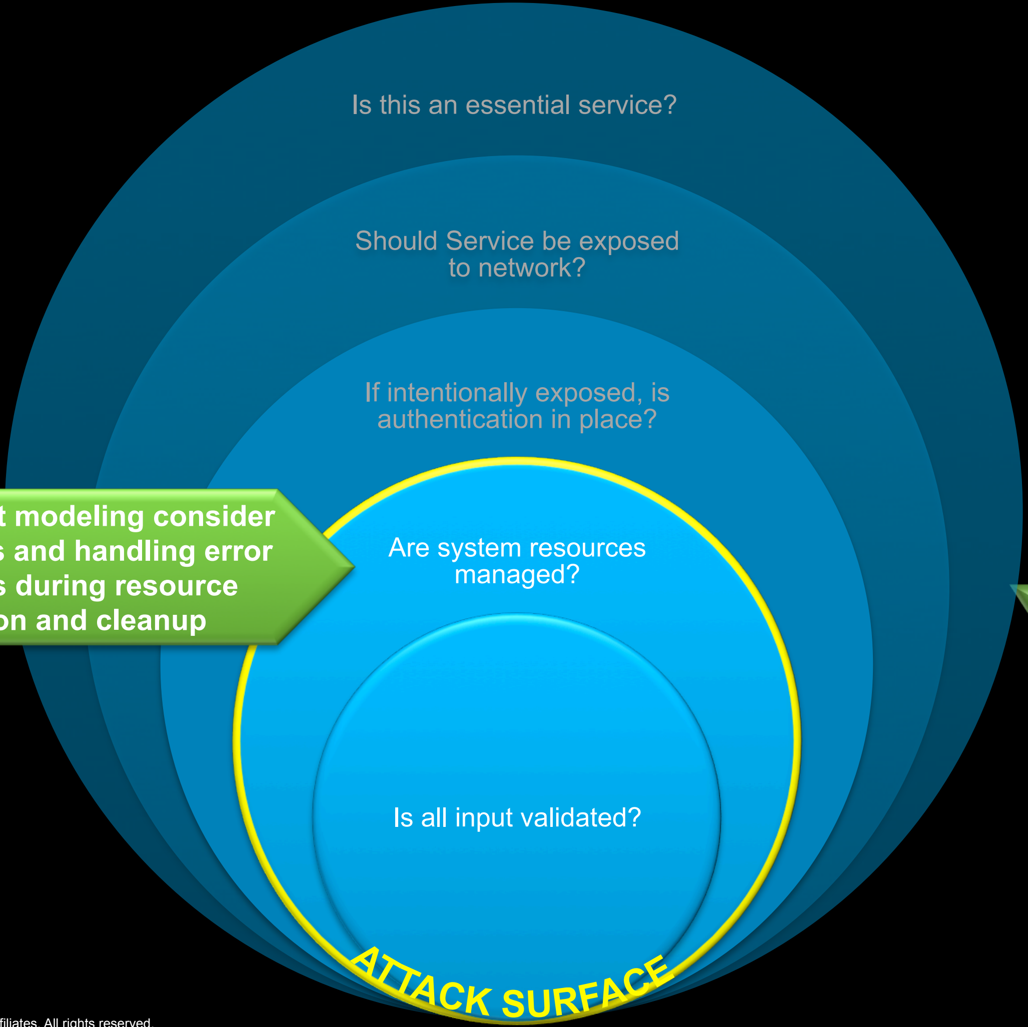
# Penetrate RISK



Require authentication and encryption for listening services

| Industry | Reference |
|---|---|
| Defense | Network STIG |
| CC | WLANPP, NDPP |

Protect Cisco
Protect Cisco Products
Protect Cisco Customers


Is this an essential service?
Should Service be exposed to network?
If intentionally exposed, is authentication in place?
Are system resources managed?
Is all input validated?
ATTACK SURFACE

**During threat modeling consider setting limits and handling error conditions during resource allocation and cleanup**

# Penetrate RISK

Validate Reqs & Resiliency
Vulnerability Testing

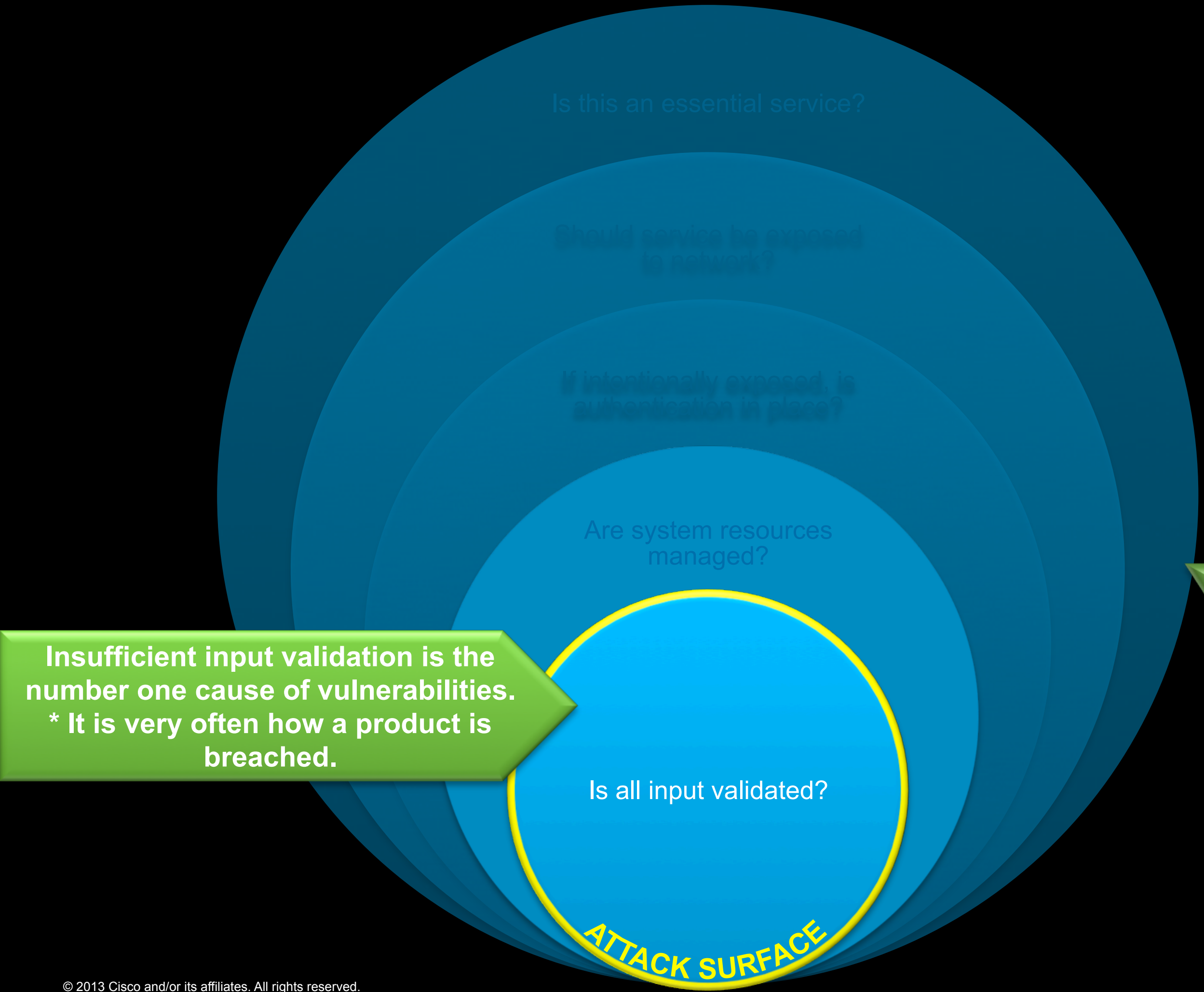
**Testing Requirements with flooding and fuzzing tools.**

| Industry | Reference |
|---|---|
| Defense | APP STIG 3760/3780/6080<br>NET-IDSPS-010/012,<br>UCR 5.4.6.2.5-2.b<br>UCR 5.3.5.4.7-14.3<br>NET STIG 0375 |

Protect Cisco

Protect Cisco Products

Protect Cisco Customers


Is this an essential service?
Should service be exposed to network?
If intentionally exposed, is authentication in place?
Are system resources managed?
Is all input validated?
ATTACK SURFACE

**Insufficient input validation is the number one cause of vulnerabilities. * It is very often how a product is breached.**

# Penetrate RISK

**Secure coding practices and Safe Libraries. Treat all input as suspect.**

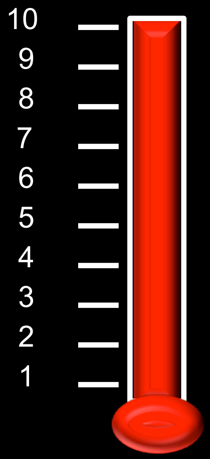
| Industry | Reference |
|---|---|
| Defense | APP STIG 6030 |

# Estimating Risk: Common Vulnerability Scoring System

- Common Vulnerability Scoring System sponsored by the Forum of Incident Response and Security Teams (FIRST)
  - Used by industry to attempt to quantify the risk of a given vulnerability
  - Enterprises use CVSS score to prioritize mitigation
- We will use CVSS scoring in this presentation to hypothetically illustrate how CSDL mitigates vulnerability risk

http://nvd.nist.gov/cvss.cfm?calculator&version=2

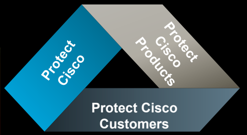
# System Risk Estimate using CVSS: Penetration Phase



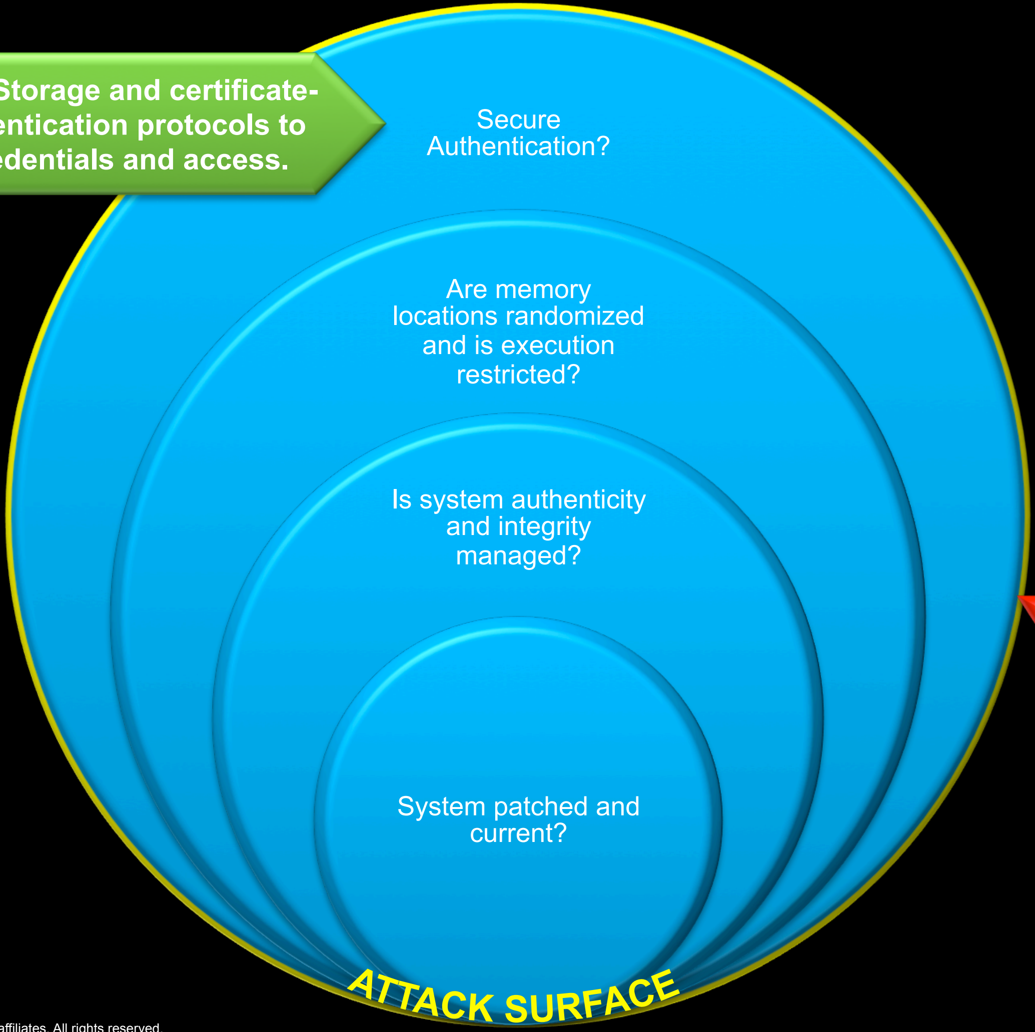
CVSS Risk Estimate

| CSDL Requirement | CVSS Factor Impact |
|---|---|
| Restrict Non-Essential Services | Related exploit range: Adjacent Network |
| Threat Modeling | Attack Complexity: Medium |
| Secure Authentication | Level of Authentication: Single |
| Manage System Resources | Impact Metrics: Partial |
| Input Validation | Attack Complexity: High |

CVSS scores indicate estimated risk and may not reflect real-world experience



**Use Secure Storage and certificate-based authentication protocols to protect credentials and access.**


Secure Authentication?
Are memory locations randomized and is execution restricted?
Is system authenticity and integrity managed?
System patched and current?
ATTACK SURFACE

# Infiltrate RISK

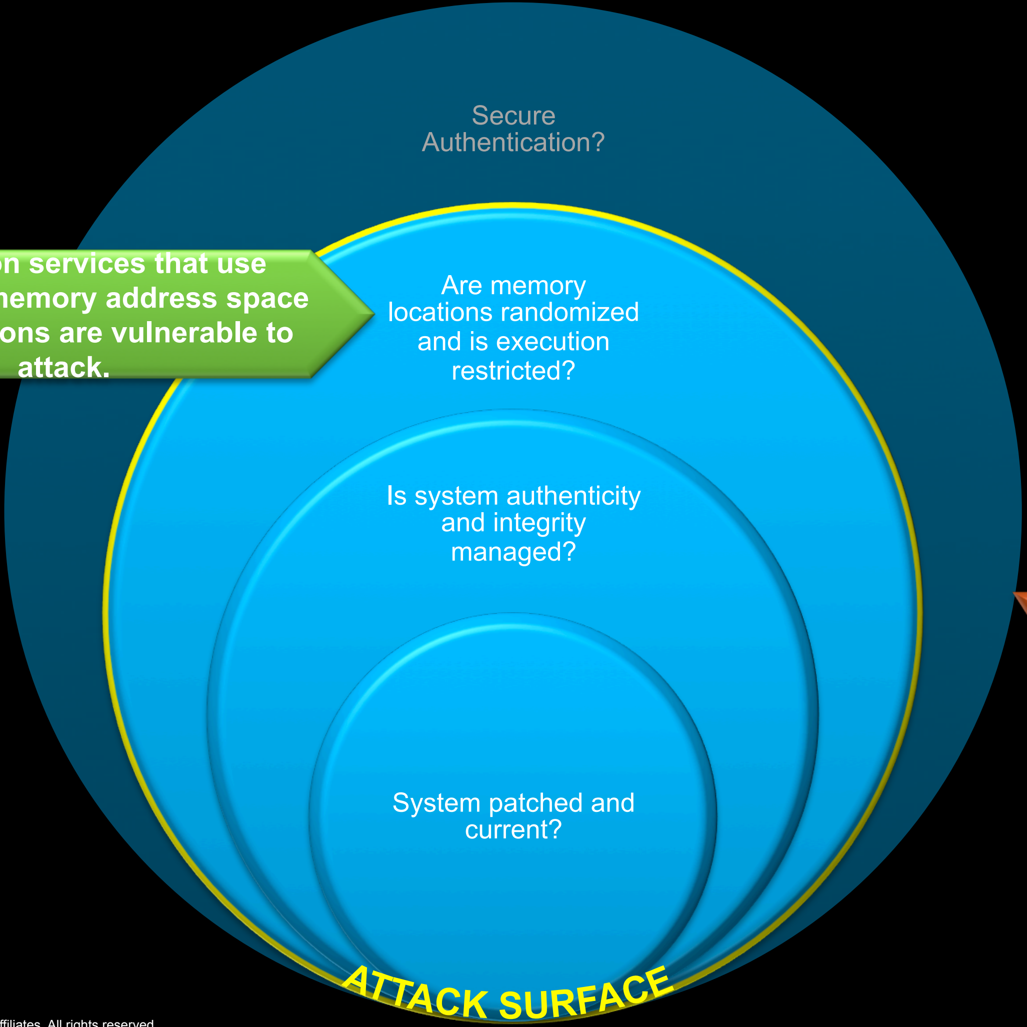
**Perform GAP Analysis**

**Product Security Requirements**

**Require secure credential management and authentication for remote access.**

| Industry | Reference |
|---|---|
| Defense | Network STIG |
| CC | WLANPP, NDPP |

**Application services that use predictable memory address space or file locations are vulnerable to attack.**


Secure Authentication?
Are memory locations randomized and is execution restricted?
Is system authenticity and integrity managed?
System patched and current?
ATTACK SURFACE

Protect Cisco

Protect Cisco Products

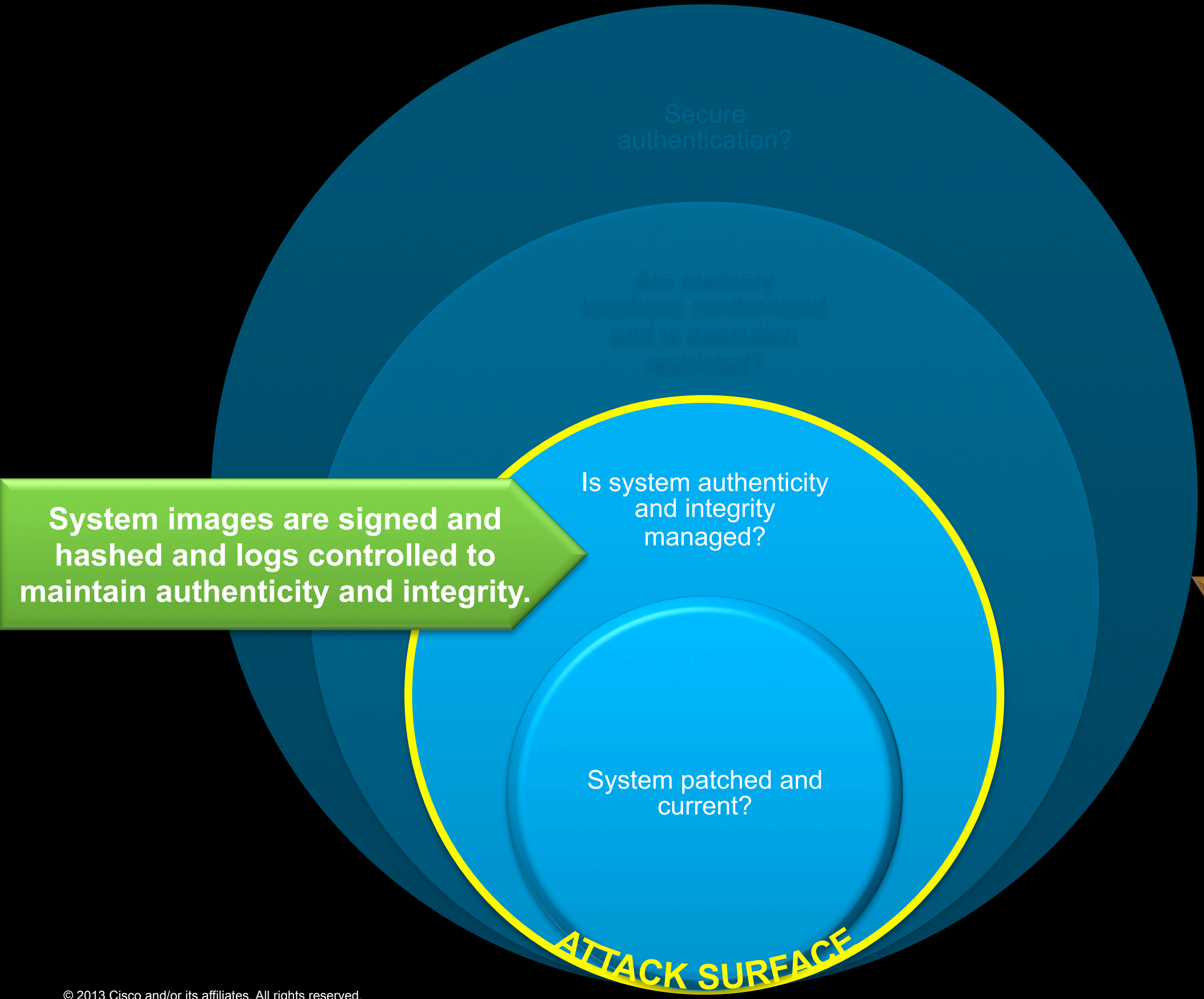
Protect Cisco Customers

# Infiltrate RISK

Prevent Security Attacks
Secure Coding

**Requires ASLR and XSPACE.**

| Industry | Reference |
|---|---|
| Defense | OS Red Hat GEN008420 |

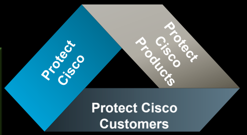

Secure authentication?
Are memory locations randomized and is execution restricted?
Is system authenticity and integrity managed?
System patched and current?
ATTACK SURFACE

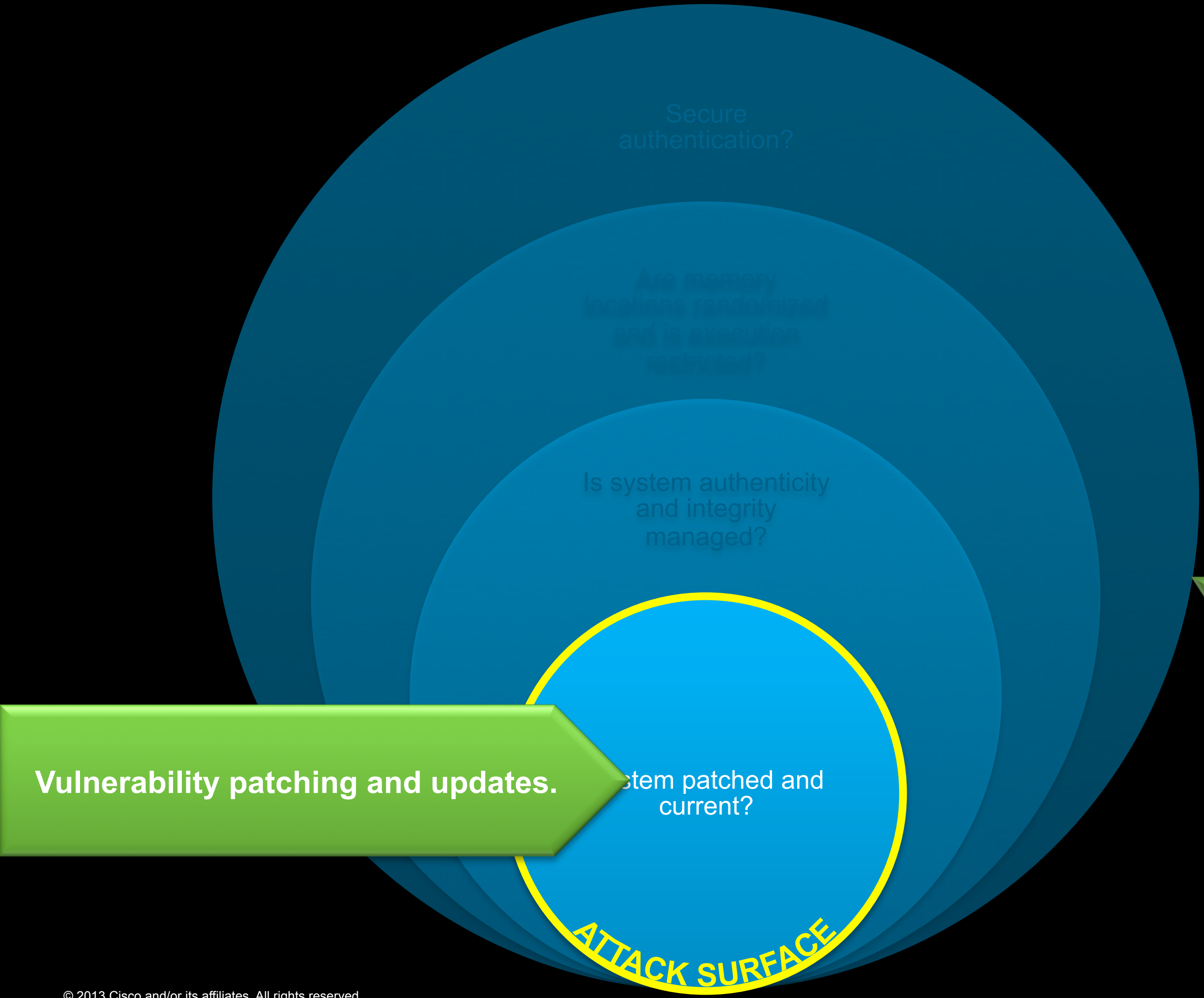
System images are signed and hashed and logs controlled to maintain authenticity and integrity.

Infiltrate RISK
Prevent Security Attacks
Secure Coding

Require Mandatory Access Control and Cisco signed images.

| Industry | Reference |
|---|---|
| Defense | VvoIP1201/1710/1935 |
| CC | FMT_SMF.1,<br>FPT_TUD_EXT.1 |




Secure authentication?
Are memory locations randomized and is execution restricted?
Is system authenticity and integrity managed?
stem patched and current?
ATTACK SURFACE

**Vulnerability patching and updates.**

# Penetrate RISK

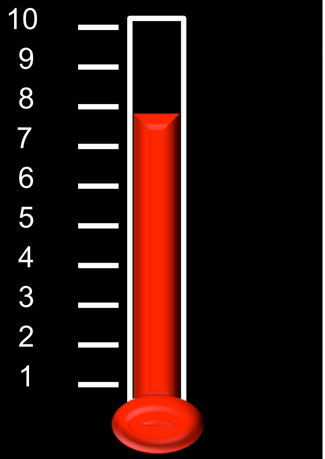
Register & Update 3rd Party Software
3rd Party Security

**Require software and 3rd Party vulnerability updates**

| Industry | Reference |
|---|---|
| Defense | APP6050, DSN17.04/05 DSN02.04, EN020, NET0384. GEN000120, VVOIP1700 |
| NERC CIP | R4.2 |

# System Risk Estimate: Infiltration Phase

CVSS score animates in presentation mode



CVSS Risk Estimate

| CSDL Requirement | CVSS Factor Impact |
|---|---|
| Secure Authentication | Related exploit range: Local<br>Level of Authentication: Multiple |
| ASLR/XSpace | % Vulnerable: 26-75 |
| Image Signing | |
| System patched and current | Vulnerability Temporal Score: Unproven, Official Fix |

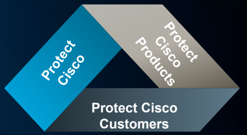
CVSS scores indicate estimated risk and may not reflect real-world experience

# Exfiltrate Detection and Mitigation support

## Network Product Contribution

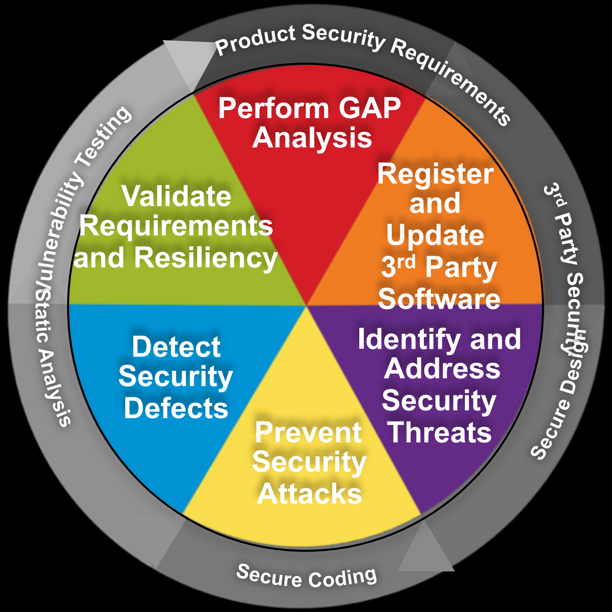
- Most exfiltration occurs in application domains
- Networks can help to detect suspicious activities through:
  - Anomaly detection and policy violations
  - Confirmation and Compliance Management Systems
  - Decreasing Infiltration directly reduces Exfiltration

# Consistency through Secure Development Lifecycle (CSDL)



**SDL is the approach to use for ensuring product security:**

- Incorporate security requirements in Product Security Baseline, Identify security threats and mitigations during design phase with Threat Modeling
- Prevent security defects using Safe Libraries and Static Analysis tools with appropriate security rules
- Defend against exploits using Runtime Defense techniques, while Validating system through Security Testing


Product Security Requirements
3rd Party Security
Secure Design
Secure Coding
Static Analysis/Vulnerability Testing
Perform GAP Analysis
Register and Update 3rd Party Software
Identify and Address Security Threats
Prevent Security Attacks
Detect Security Defects
Validate Requirements and Resiliency

**Value Statement:** Ensures consistent product security through proven techniques and technologies, reducing the number and severity of vulnerabilities in software

# Glossary of Referenced Industry Requirements/Specifications

Protect Cisco

Protect Cisco Products

Protect Cisco Customers

| Industry Standards | Specifications |
|---|---|
| Common Criteria (CC) | Protection Profiles:<br>• Wireless LAN (WLAN)<br>• Network Device (ND)<br>• Firewall (FW)<br>• VPN |
| Defense | Secure Technical Implementation Guide (STIG):<br>• Application (APP)<br>• Network (NET)<br>• Unified Capabilities (UCR)<br>• VoIP (Voice over IP)<br>• Defense Switched Network (DSN) |
| NERC CIP | North American Electric Reliability Corporation Critical Infrastructure Protection |
| Cisco | Cisco Secure Development Lifecycle (CSDL)<br>Product Security Baseline (PSB) for all Cisco products |