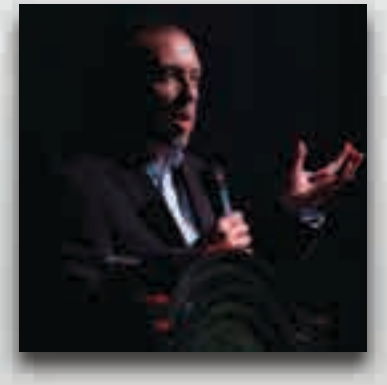
HOW TO BUILD A PRODUCT SECURITY PROGRAM WITH SDL & CERTIFICATIONS

ICMC 2016

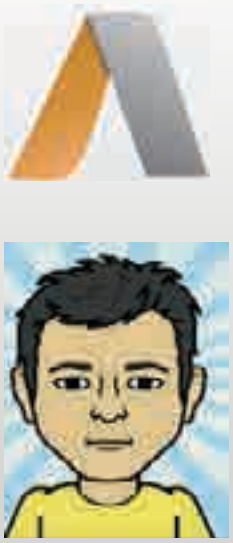
About Chris Romeo

- CEO / Principal Consultant @ Security Journey
- 20 years security experience
- 10 years at Cisco, leading the Cisco Security Ninja program & CSDL
- Speaker at RSA, AppSec USA, AppSec EU, & ISC2 Security Congress



About Ashit Vora

- Co-Founder and Lab Director @ Acumen Security
- 13 years certification and security experience
- Led Cisco's FIPS and CC certification teams



Overview

- The Problem Space
  - *State of the vulnerability*
  - *Certification Challenges*
- The Product Security Program
- How to overlay certifications into an SDL
- Implementing a product security program
- Top six tips for successful collaboration between SDL & Certifications

Security vulnerabilities and bug counts continue to rise

Vulnerabilities & Cert Requirements

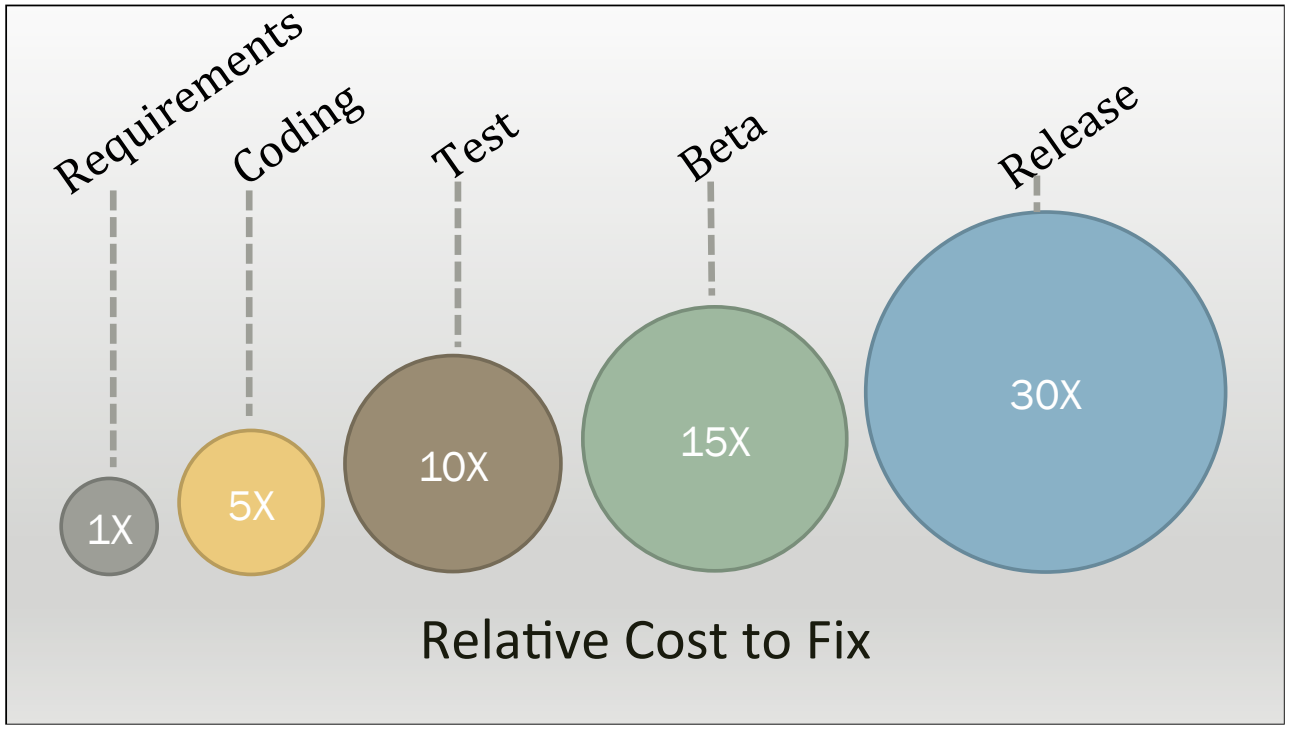
Budgets

The Impact of Vulnerabilities

- 3 out of 4 applications produced by software vendors fail OWASP Top 10 when first assessed*
- 63% of internally developed applications are out of compliance with OWASP Top 10 when first assessed*

OWASP Open Web Application Security Project

VERACODE STATE OF SOFTWARE SECURITY
Focus on Application Development
SUPPLEMENT TO VOLUME 6



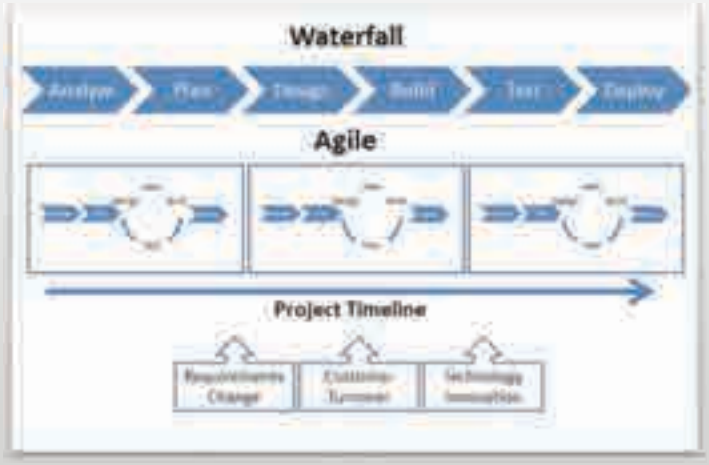
Certification Pain Points

V/S

Bolted On

Baked In

Certification Pain Points



Aligning timelines with dev schedules and business cycles

Certification Pain Points

Certificate Maintenance

Certification Pain Points

Alphabet Soup of Standards

Solution?

The Pieces of a Product Security Program

Education

SDL

Tools

Community

"Sales"

Consulting

PSIRT

Certifications

Goals of a Product Security Program

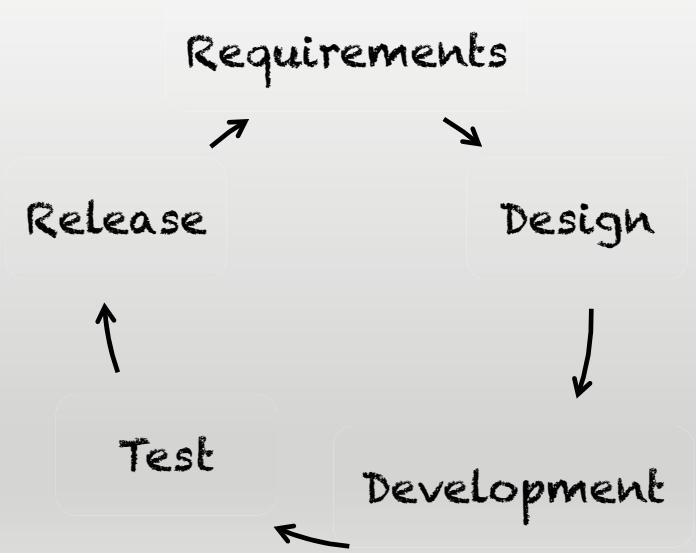
- Lower cost and time to fix of security bug counts
- Security evangelization
- Baking in certification requirements
- Trustworthy products at a lower cost

Product Security Program Scale

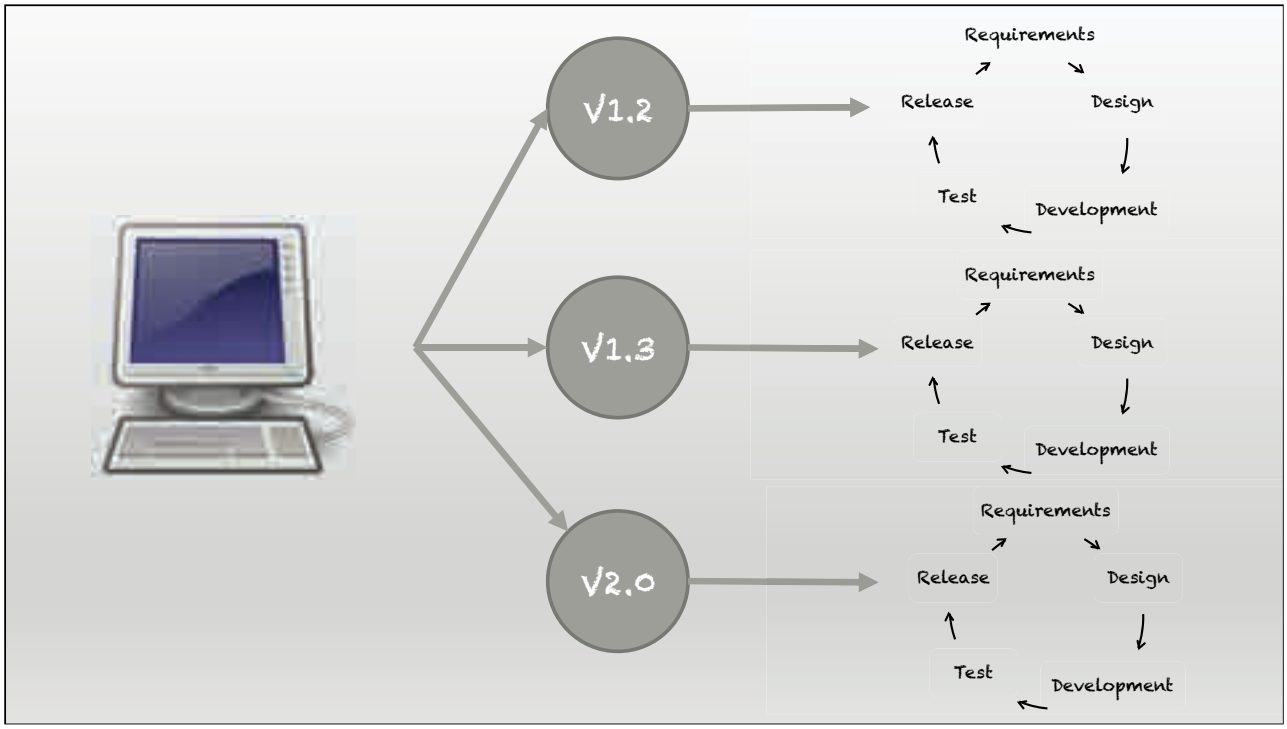

Big vs. Small


Many Hats

A Secure Development Life Cycle



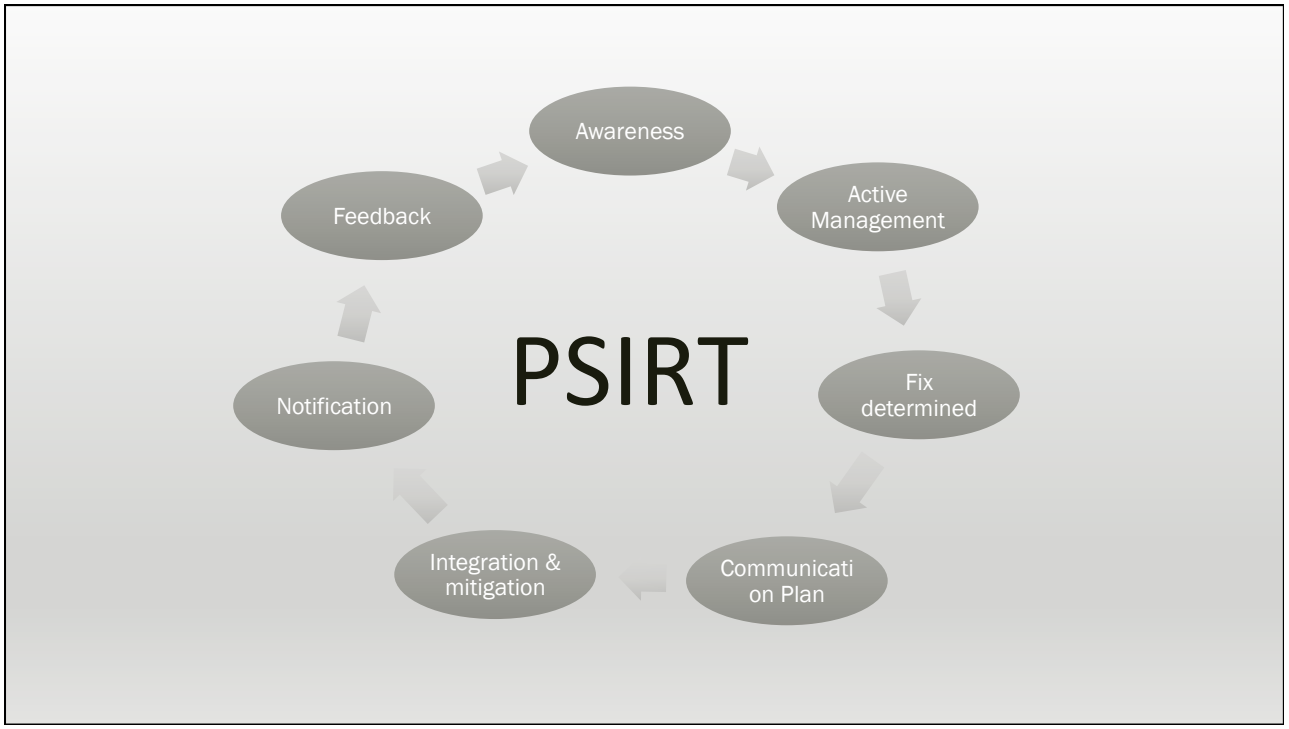
SDL is the foundation for any Product Security Program.


V1.2
V1.3
V2.0
Requirements
Design
Development
Test
Release
Requirements
Design
Development
Test
Release
Requirements
Design
Development
Test
Release


• SDL?
• Security requirements
• Threat modeling
• FIPS 140
Consulting


Tools

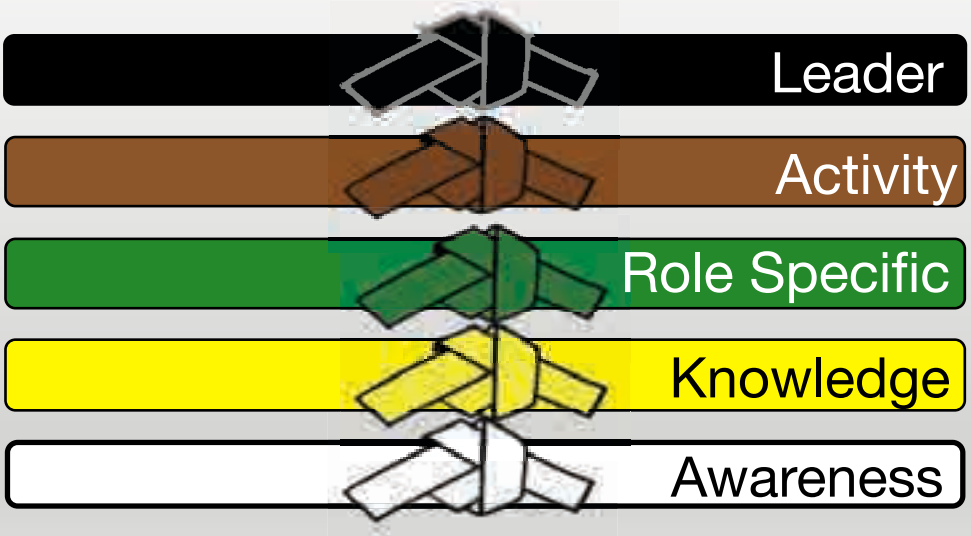

Executive Account
Management


PSIRT
Awareness
Active Management
Fix determined
Communicati on Plan
Integration & mitigation
Notification
Feedback


Security Community

Certifications

Education



Overlaying Certifications with SDL

Building a Team

Certifications Overlay Requirements

Certifications Overlay Design

Plan

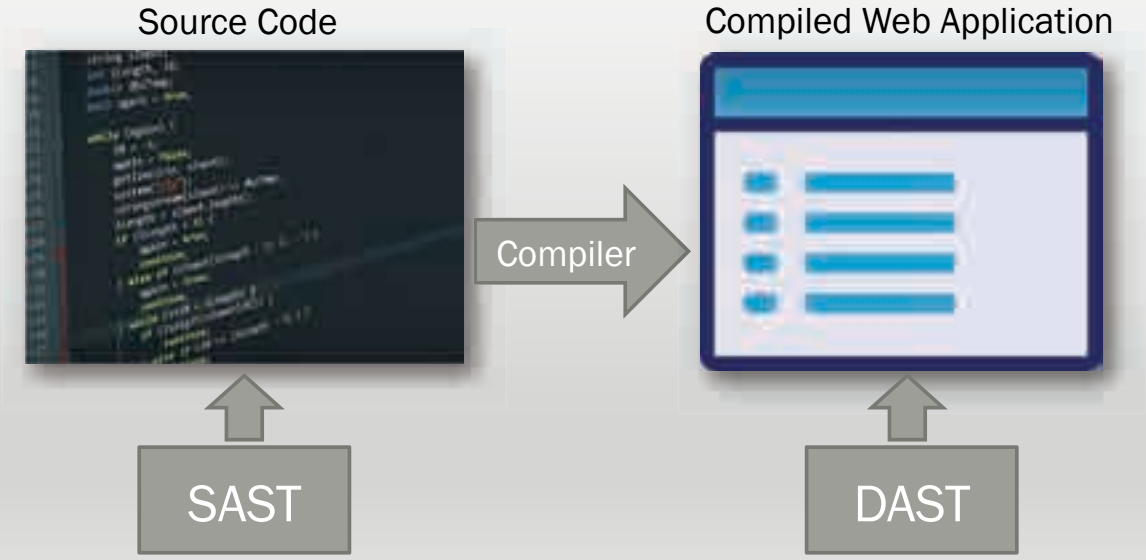
Meet or Exceed

Certifications Overlay Design

Threat Modeling…

Certifications Overlay Implementation

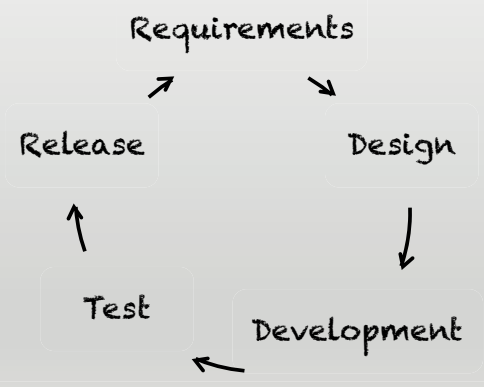
Certifications Overlay Implementation

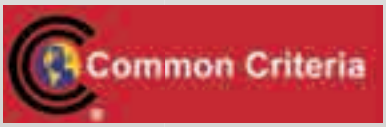


Certifications Overlay Test Integration and Automation

Certifications Overlay Release

Top 6 tips for Collaboration between SDL & Certifications





1. Teamwork: make certifications part of the product security program

2. Education: teach the business case for certifications

3. Partnerships: work together towards the common goal

4. Harness the security value of certifications, vote No on checkbox compliance!

5. Do not create custom versions of products to meet cert requirements

6. Treat your internal certification folks well!

Summary

- Vulnerabilities are present, and cert challenges are real
- The Product Security Program meshes nicely with the certification mission
- Collaboration results in a better secure, certified product

Call to Action: Think of certifications as more than a check box

Thank you!

Chris Romeo, CEO / Principal Consultant
chris_romeo@securityjourney.com
www.securityjourney.com
@edgeroute

Ashit Vora, Co-Founder and Lab Director
avora@acumensecurity.net
www.acumensecurity.net
@acumensec