THE THREE WAYS OF SECURITY

Jeff Williams
Co-founder and CTO
Contrast Security
1. TODAY’S “AVERAGE” APPLICATION IS A SECURITY DISASTER

- 21% CUSTOM CODE
- 26.7 SERIOUS VULNERABILITIES
- 8.5% ACTUALLY INVOKED LIBRARY CODE ACROSS 27 LIBRARIES
- 70.5% UNUSED LIBRARY CODE ACROSS 30 LIBRARIES
- 2.0 VULNERABILITIES (CVE)
2. SOFTWARE IS LEAVING SECURITY IN THE DUST

- Typical enterprise has hundreds or thousands of applications
- Applications are by far the leading cause of breaches (Verizon DBIR)
3. SOFTWARE SUPPLY CHAIN SECURITY IS TOTALLY BROKEN

March 7
CVE-2017-5638
Disclosed, Apache releases fixed version

Mid-May
Equifax breach occurs

July 29
Equifax learns of breach

Sept 7
Equifax discloses, Four more Struts2 CVEs disclosed

Livin’ la vida loca

Equifax ignores

Equifax unaware

Disaster

Jan  Feb  Mar  Apr  May  Jun  Jul  Aug  Sept  Oct

Prepared

Protected

March 8
We observed widespread attack probes
**DIAGNOSIS: GOALS UNCLEAR, TIME WASTED**

**What we are delivering:**

Application/API portfolio

- [x] “I ran a scanner”

**What we must deliver:**

Application/API portfolio

- [✓] Right defenses in place
- [✓] Defenses are effective
- [✓] Attacks detected/blocked
PUPPY MONKEY BABY

DEV SEC OPS
SO WHAT IS DEVOPS?

The “Three Ways”

1. Establish work flow
   - (Business) → (Customer)
   - Dev → Ops

2. Ensure instant feedback
   - Dev → Ops

3. Culture of experimentation
   - Dev → Ops → Dev → Ops → Dev → Ops → Dev → Ops → Dev → Ops
Small batch sizes

Tight feedback loops

Swarm on problems

Optimize for downstream consumers

Produce awesome software
QUESTION: CAN DEVOPS HELP SECURITY?

• **Problem:** software is poor quality, late, slow, and doesn’t provide business value.

• **Approach:** DevOps

• **Outcomes:**
  • 5x lower change failure rate
  • 96x faster MTTR service
  • 2x likely to exceed bus. goal

• **Problem:** security is poor quality, late, slow, and doesn’t provide business value.

• **Possible Approach:** DevOps

• **Required Outcomes:**
  • 10x increase in portfolio coverage?
  • 80% reduction in vulns to prod?
  • 0x increase in time to market?
SHOVING LEGACY SECURITY TOOLS AND PROCESSES INTO SEC
The “Three Ways” of Security*

1. Establish security work flow
   - Build a concrete security story over time
   - Enable development to build security
   - Rip, mix, and burn security work

2. Ensure instant security feedback
   - Enable self-inventory
   - Get real application threat intelligence
   - Create security notification infrastructure

3. Build a security culture
   - Migrate to “positive” security
   - Accelerate evolution of your security story
   - Promote “security in sunshine”

* Shamelessly adapted from The Phoenix Project, by Gene Kim
Establish Security Work Flow

Optimize delivery of security work that is valued by the business
UMM.... WHAT IS SECURITY “WORK”?

1. Business Security Projects
   Building defenses, compliance, reporting, etc...

2. Internal Security Work
   Threat modeling, security architecture, security research, vulnerability assessment, tools

3. Operational Security Jobs
   Remediation, updates, analytics, alerts, tickets, etc...

4. Unplanned Security Tasks
   Security “firefighting,” response, recovery, public relations, etc...
FIRST WAY – BUILD A CONCRETE SECURITY STORY OVER TIME

IT'S NOT WHAT YOU KNOW

IT'S WHAT YOU CAN PROVE

* Shamelessly lifted from the Rugged Software Project
Leverage existing DevOps processes and tools. Refactor monolithic security tasks into small batch sizes. Deliver security one little piece at a time.
FIRST WAY – WORK ON BIGGEST THREATS, ONE AT A TIME

Add a single risk to threat model
• Create JIRA ticket: Prevent XXE

Create defense strategy
• Update JIRA Ticket
• Standardize parser config
• Log & block attacks

Implement defense
• XML library
• Update training

Establish continuous assessment
• Research typical failures
• Build custom test cases
• Enable IAST XXE rule

Establish attack protection
• Enable RASP XXE rule

Monitor DEV and OPS
• Vulns go to JIRA with Slack alert
• Attacks go to Splunk and VictorOps

Do you really need security experts for all these tasks?

Updated Security Story
The Second Security Way

Ensure Instant Security Feedback

Establish tight security feedback loops across the lifecycle
SECOND WAY – ENABLE SELF-INVENTORY

• You need to know the exact version of every app, api, and library running on every server in every environments

• Not hard to fully automate self-inventory

Automatic Application Inventory
SECOND WAY – GET REAL APPLICATION THREAT INTELLIGENCE

Establish the infrastructure to...

- Know who is attacking you
- Know what techniques they’re using
- Know what they’re targeting
- ... and protect within hours
SECOND WAY – ESTABLISH A REALTIME APPSEC CONTROL PLANE
The Third Security Way

Build Security Culture

A culture that constantly advances security with the threat through experimentation and learning.
THIRD WAY – MIGRATE TO “POSITIVE” SECURITY

Testing for all the ways you might introduce XSS

Measure positive security directly from your running application

Testing to verify your XSS defense
THIRD WAY – ACCELERATE THE EVOLUTION OF YOUR SECURITY STORY

Celebrate new big risks without recrimination

Focus on strength and simplicity

The faster you cycle, the faster you get secure
THIRD WAY – PROMOTE SECURITY IN SUNSHINE

We Trust

We Hide

We Blame

AppSec Visibility Cycle

Architects

Define Security Defenses

Developers

Implement Security Defenses

Infosec

Share Intelligence

Audit

Business

Understand Laws

Verify Compliance

Legal

Users

Understand Stakeholders

Monitor Threat

Research

Create Security Story

We Trust

We Hide

We Blame

Understand Stakeholders

Monitor Threat

Create Security Story

Define Security Defenses

Implement Security Defenses

Share Intelligence

Verify Compliance

Legal

Business

Audit

Infosec

Developers

Architects

We Trust

We Hide

We Blame

Understand Stakeholders

Monitor Threat

Create Security Story

Define Security Defenses

Implement Security Defenses

Share Intelligence

Verify Compliance

Legal

Business

Audit

Infosec

Developers

Architects

We Trust

We Hide

We Blame

Understand Stakeholders

Monitor Threat

Create Security Story

Define Security Defenses

Implement Security Defenses

Share Intelligence

Verify Compliance

Legal

Business

Audit

Infosec

Developers

Architects
“Don’t hate the playa
Hate the game”

-- Ice T
The first rule of security is...

...You do not talk about security...
The “Three Ways” of Security*

1. **Establish security work flow**
   - Build a concrete security story over time
   - Enable development to build security
   - Rip, mix, and burn security work

2. **Ensure instant security feedback**
   - Enable self-inventory
   - Get real application threat intelligence
   - Create security notification infrastructure

3. **Build security culture**
   - Migrate to “positive” security
   - Accelerate evolution of your security story
   - Promote “security in sunshine”

* Shamelessly adapted from The Phoenix Project, by Gene Kim
CLOSING THOUGHTS – TURNING SECURITY INTO CODE

• Don’t focus on how to build software securely...

• Make software security into something you build!
Ask me anything.

@planetlevel

contrastsecurity.com