Go Beyond DevSecOps to Continuous Security
• This is the reality for most....Is it any different to waterfall?
Where do we start with Security?

**Design & Plan**

**Code**

**Automate**

**Test**

**Security Gate**

### Gate Conditions
- Build process controls
- Pass / Fail Build
- Delta Scans (new issues reported)

### Gate Conditions
- All High risk issue resolved
- All Medium risk issues > 30 days resolved
- Any Low risk issues > 90 days resolved

**Gate Conditions**

**AST Automation**

**DAST Automation**

**Security Audit / Pen Testing**

- Deep dive review of the application
- Dynamic Analysis
  - DAST Scans
- Static Analysis
  - SAST Scans
- Manual Pen Testing

**Deep dive**

**IDE Static Assessment**

**Continuous Integration**

**CI - Development Gate**

**Run**

**HCL SOFTWARE**

**DEVOPS**

Copyright © 2019 HCL Technologies Limited | www.hcltechsw.com
What is Continuous Security?

**Construct**
Secure by design and secure automation. This is the Secure DevOps piece or DevSecOps, but we need to expand security beyond just this...

**Intensify**
Magnifying the effort and impact, change the security culture, continue to improve. Education and governance drive this success.

**Assure**
Ensuring the controls are in place to meet the guidelines and standards we have in place. Secure Audit and Metrics are key to assure the program.
CONSTRUCT PHASE

**DESIGN:** Security Right From the Start.

- Use Cases / Epics / Hill Statements / Requirements
- Mature Orgs: Security actively involved in Design
- Developers are regular part of threat modeling
  - #1 practice to improve security posture

  *Puppet Labs
  2019 State of DevOps*

**AUTOMATE:** Find & Fix Fast to Lower Risk

- Consumable, Actionable Reporting
- 56% - ability to quickly fix identified vulnerabilities using automated tools
- 52% - automate vulnerability scanning at every stage of SDLC

  *2020 Ponemon study*
Intensify Phase

GOVERN: Make it Easy To Do Right

• Measure outcomes more than just behavior
• 56% - testing conducted throughout the SDLC
• 74% delays due to code needing security evaluation
  - Ponemon 2020 Study

EDUCATE: Continual Learning

• Security Champions / Advocates
• 56% - secure coding required, but only 47% ensure training.
  - Ponemon 2020 Study
• Developers get secure coding training are 5x more likely to be happy
  - Sonatype 2020 Survey
Assurance Phase

AUDIT: We Do What We Say For Controls
- Pen-testing and Run-time info aligns with SDLC
- Average time to patch:
  - Internal sys – 50 days, Public facing – 71 days
  EdgeScan 2019 Report
- Mature teams
  - 2x more likely automated governance & compliance.
  - 69% follow Open Source policies
  Sonatype 2020 Survey

MEASURE: Data Not Guesses
- Accurately identify and manage organizational risk
- Confidently make trade-off decisions based on solid data instead of hunches
- Get Healthier over time
Continuous Security

Design & Plan

Code

Automate

Test

Run

Compliance
Security Requirements

Threat Model
Secure Coding
Security Standards

RASP
(Shure Protection)

SIEM
(Security Info & Event Management)

SAST

DAST

Manual Pen Testing

Metrics & Reporting

Security Audit

HCL Accelerate

IAST

HCL Launch

Maven Bamboo

DAST Automation

HCL OneTest

SIEM

Compliance
Security Requirements

Governance

Threat Model
Secure Coding
Security Standards

DAST

Automation

Automation

SAST

IDE Scanning