Security Differently

John Willis
Senior Director Global Transformation
Red Hat

DEVOPS ENTERPRISE SUMMIT
AN IT REVOLUTION EVENT

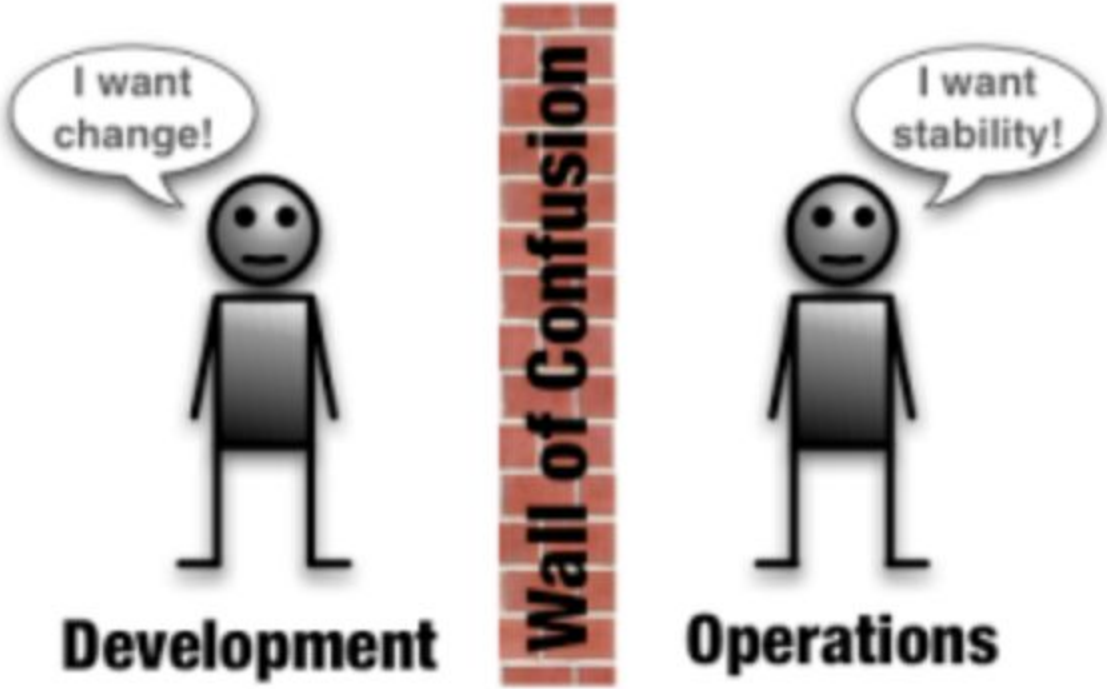
Global Transformation Office

Red Hat

“What would DevSecOps look like if DevOps never existed?”

The Three Lines of Defense Model

Source: The Institute of Internal Auditors


I want change!
Wall of Confusion
I want stability!
Development
Operations

Conway's Law

"An adage stating that organizations design systems mirror their communication structure."

The Three Lines of Defense Model

Source: The Institute of Internal Auditors

Minimal Viable Security

1. How do we prove that we're safe?
2. How do we demonstrate that we're secure?
3. How do we do both?

Modern Governance

Move from implicit security models to explicit proof based.

Cyber Transition

Changing Subjective to Objective and Verifiable.

Cyber Transition

	Subjective	Objective	Verifiable
Risk	Change Management	Attestations and Control	Continious Verification
Defense	Detect and Respond	Intelligence Data Lakes	Adversary Analysis
Trust	Perimeter Based	Zero Trust Architecture	Distributed Trust

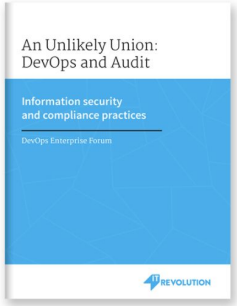
Three Novel Ideas

1. Devops Automated Governance
2. Cyber Data Lakes
3. Distributed Trust Models for Identity and Secrets

Risk Differently

Modern Risk Goals

- Reduce audit toil
- Increase audit efficacy
- Automated, objective and immutable evidence
- Continuous audit and verification



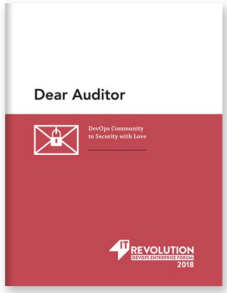
AN UNLIKELY UNION: DEVOPS AND AUDIT

October 1, 2015

DEVOPS AUTOMATED GOVERNANCE REFERENCE ARCHITECTURE

September 17, 2019

2015 2018 2019



DEAR AUDITOR

August 27, 2018

EXPLORE

Focusing on the DevOps Pipeline

Creating Better Pipelines

So how do we design, measure, and improve our pipelines to avoid the above?

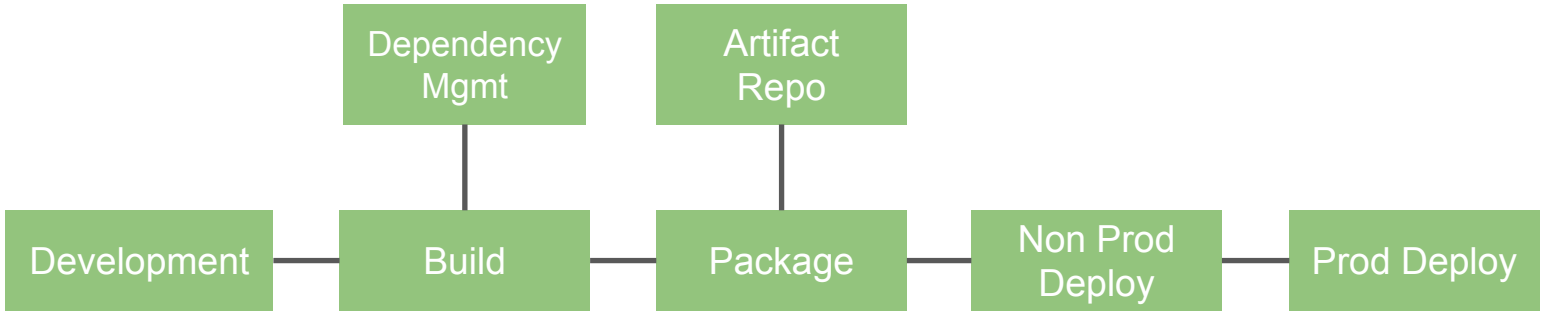
Pipeline Design

At Capital One, we design pipelines using the concept of the "16 Gates". These are our guiding design principles and they are:

- Source code version control
- Optimum branching strategy
- Static analysis
- >80% code coverage
- Vulnerability scan
- Open source scan
- Artifact version control
- Auto provisioning
- Immutable servers
- Integration testing
- Performance testing
- Build deploy testing automated for every commit
- Automated rollback
- Automated change order
- Zero downtime release
- Feature toggle

These gates are used to understand each and every product's progress through the DevOps process.

Devops automated Governance Reference Architecture



Common Control

1. Access Control
2. Audit Train/log
3. Everything source control
4. Usage policies

Common Actors

1. Auditor, Risk/Compliance Office
2. (system)
3. Tools Admin

Development Stage (Controls and Attestations)

Attestation Name	Stage	Attestation	Source	Example
Code Quality	Development	Numeric	SonarQube	<4
Information Leakage	Development	Pass/Fail	Custom	pass
Unit Test Coverage	Development	Percentage Code Coverage	SonarQube	80%
Unit Test Execution	Development	Pass/Fail	SonarQube	Pass
Change Size	Development	Pass/Fail	Jenkins	Pass
Cyclomatic Complexity	Development	Pass/Fail	SonarQube	Pass
Pull Request	Development	Number of Approvers	Source Control	
Branching Strategy	Development	Pass/Fail	SonarQube	Pass
Clean Dependencies	Development	Validation	Nexus	validated

Build Stage (Controls and Attestations)

Attestation Name	Stage	Attestation	Source	Example
Build	Build	ID	Source Control	2.0.3-16-98092ba
Build Performance	Build	Verification		verified
Build Version	Build	Version	Source Control	98092ba
Build Conconfiguration	Build	Config Identification	Source Control	
Linting	Build	Pass/Fail	SonarQube	Pass
SAST Scan	Build	Validation	Sonarqube	Invalid

Package Stage (Controls and Attestations)

Attestation Name	Stage	Attestation	Source	Example
Artifact Versioning	Package	Pass/Fail	Nexus	Pass
Package Metadata	Package	Pass/Fail	Nexus	Pass
Code Signing	Package	Validation	Cryptographic Hash	validated
Container Scan	Package	Validation	Openscap	validated

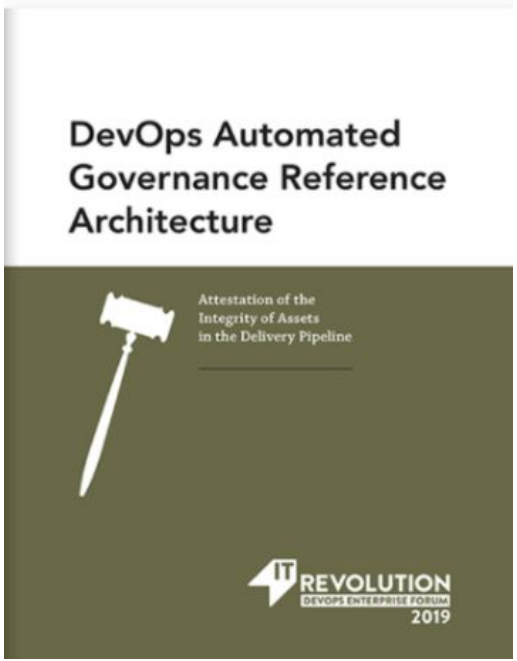
PreProd Stage (Controls and Attestations)

Attestation Name	Stage	Attestation	Source	Example
Trusted Packages	Pre-Prod	Validation	Openscap	validated
Approved Configuration	Pre-Prod	Validation	Ansible	validated
Threat Monitoring	Pre-Prod	Validation	Tanium	validated
Automated Alert Tooling	Pre-Prod	Validation	Dynatrace	validated
Deployment Strategy	Pre-Prod	Validation	Ansible	validated

Risk as Code (Policy DSL

- Human Readable (YAML)
- Machine Interpreted
- Version Controlled
- Models Attestations and Enforcement

```yaml
apiVersion: pac/v1
kind: Policy
metadata:
  name: azn_services
  labels:
    mnemonic: azn
    app: azn_web
    requirements:
    #Versioning
    pipeline:
      versioning:
        verify: True
        pattern: `^(\d+)\.(\d+)\.(\d+)-(\d+)\-([A-Faa-f0-9]+)$`
    #Build server Verification
    build_server:
      verify: True
    #Artifact Server Verification
    artifact_server:
       verify: True
    #Artifact Verification
    artifact_hash:
       verify: True
    #Unit Testing
    unit_test_coverage:
       verify: True
       percentage_coverage: at_%_coverage
    #Git Pull Reguest
    pull_request_approval:
       verify: True
       pull_request_approver_count:
```

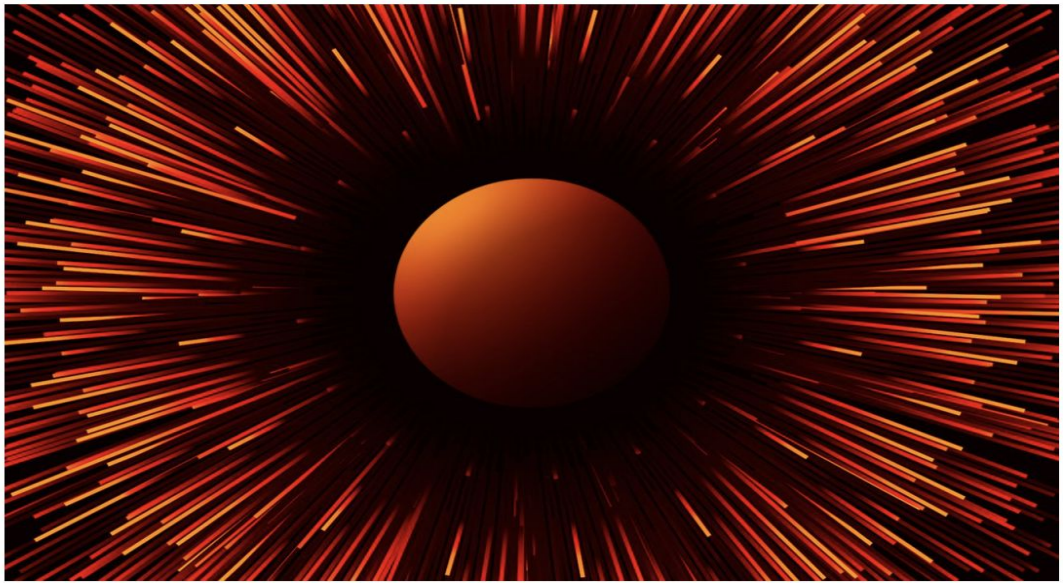

DevOps Automated
Governance Reference
Architecture
Attestation of the
Integrity of Assets
in the Delivery Pipeline
IT REVOLUTION
DEVOPS ENTERPRISE FORUM
2019

2021


Version 2
DevOps Automated
Governance Reference
Architecture
Attestation of the
Integrity of Assets
in the Delivery Pipeline
"Investments Unlimited"
IT REVOLUTION
DEVOPS ENTERPRISE FORUM
2019

SUNSPOT: An Implant in the Build Process

January 11, 2021 CrowdStrike Intelligence Team Research & Threat Intel



In December 2020, the industry was rocked by the disclosure of a complex supply chain attack against SolarWinds, Inc., a leading provider of network performance monitoring tools used by organizations of all sizes across the globe. CrowdStrike and another firm have been supporting SolarWinds in its

CATEGORIES

ENDPOINT & CLOUD SECURITY (207)
ENGINEERING & TECH (25)
EXECUTIVE VIEWPOINT (107)
FROM THE FRONT LINES (120)
IDENTITY PROTECTION (11)
PEOPLE & CULTURE (18)
REMOTE WORKPLACE (18)
RESEARCH & THREAT INTEL (136)
TECH CENTER (107)

CONNECT WITH US

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

DELIVER UNCOMPROMISED: SECURING CRITICAL SOFTWARE SUPPLY CHAINS

PROPOSAL TO ESTABLISH AN END-TO-END FRAMEWORK FOR SOFTWARE SUPPLY CHAIN INTEGRITY

by Charles Clancy, Joseph Ferraro, Robert Martin, Adam Pennington, Christopher Sledjeski, and Craig Wiener

Tactic	ID	Technique	Attestation	Attestation Source	Observation
Reconnaissance	T1592.002	Gather Victim Host Information	Custom	Pipeline as Code/Ploigos	StellarParticle had an understanding of the Orion build chain before SUNSPOT was developed to tamper with it.
Resource Development	T1587.001	Develop Capabilities – Malware	Custom	Pipeline as Code/Ploigos	SUNSPOT was weaponized to specifically target the Orion build to replace one source code file and include the SUNBURST backdoor.
Defense Evasion	T1140	Deobfuscate/Decode Information	Configuration	Ansible	The configuration in SUNSPOT is encrypted using AES128-CBC. It contains the replacement source code, the targeted Visual Studio solution file name, and targeted source code file paths relative to the solution directory.
Defense Evasion	T1027	Obfuscated Files or Information	Configuration	Stackrox,SonarQube	The log file SUNSPOT writes is encrypted using RC4.
Defense Evasion	T1480	Execution Guardrails	Code Signing	Cryptographic Hash	The replacement of source code is done only if the MD5 checksums of both the original source code file and backdoored replacement source code match hardcoded values.
Defense Evasion	T1480	Execution Guardrails	Image Scanning	OSCAP	The replacement of source code is done only if the MD5 checksums of both the original source code file and backdoored replacement source code match hardcoded values.
Defense Evasion	T1036	Masquerading	Custom	Sigstore	SUNSPOT masquerades as a legitimate Windows Binary, and writes its logs in a fake VMWare log file.

MITRE ATT&CK Framework Analysis from “Crowdstrike Blog - SUNSPOT: An Implant in the Build Process

Modern Risk Solutions

- Devops Automated Governance
- Software Factory (Ploigos)
- Sigstore, Grafeas, In-ToTo
- Openshift Compliance Operator/ACM Policy
- Software Bill of Materials (SBOM)
- Continuous Verification

SBOM

- CycloneDX (OWASP)
- SPDX (Linux Foundation)
- Software Transparency (NTIA)
- Toot-to-Tool 3T SBOM (MITRE)

Defense Differently

Modern Defense Goals

- Reduce defense toil
- Increase defense efficacy
- A unified approach to SIEM and SOAR
- Cyber Data Lakes/Intelligence
- Deception technology
- Adversary Analysis

Cloud Automated Governance

ONUG AUTOMATED CLOUD GOVERNANCE WORKING GROUP MEMBERS

DON DUET

concourse labs

RAJ BALASUBRAMANIAN

IBM

JONATHAN BITLE

KAISER PERMANENTE

PETER CAMPBELL

Cigna

YURI CANTOR

Goldman Sachs

ZHEN FAN

FedEx

LENNY GRINBERG

Pfizer

JOE LOOMIS

ONUG

PRIYA GNANASUNDAR

KAISER PERMANENTE

ALI ILOGLU

UBS

ANURAG JAIN

Goldman Sachs

ALEX KVYAT

KAISER PERMANENTE

CARLOS MATOS

JPMorgan Chase & Co.

PAUL MATUSIK

Raytheon Technologies

JOHN WILLIS

Red Hat

CHARLENE O'HANLON

PAT O'NEIL

FedEx

ANATOLIY PANASYUK

Microsoft

SMRITI TALWAR

IBM

MICHAEL WHEELER

Cigna

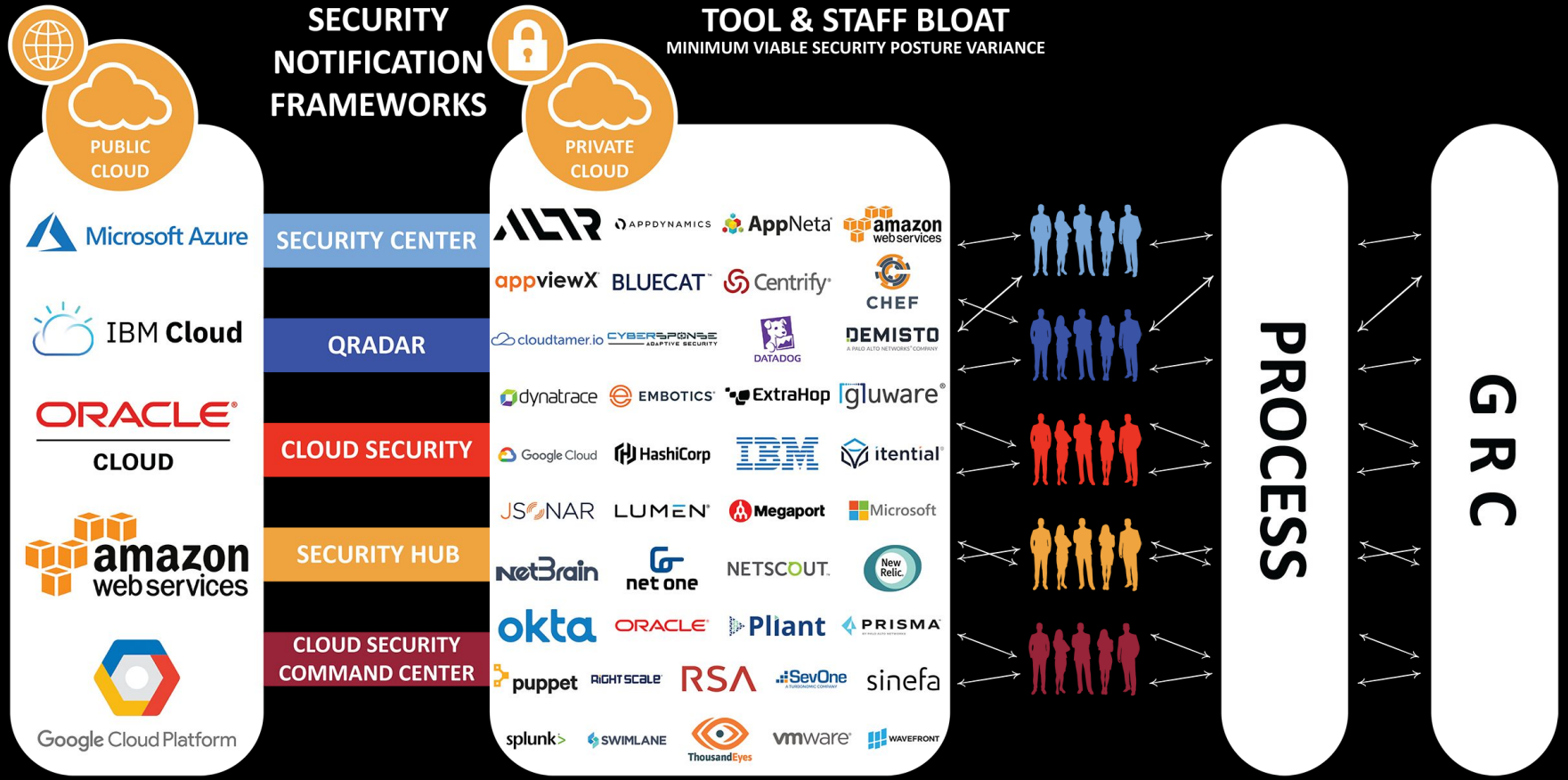
RANDY SHORE

cloudtamer.io

JOSEPH SPURRIER

cloudtamer.io

CLOUD CONTROL PROBLEM EMERGING



CSNF Cloud Security Notification Framework

Metadata: Delivers Standardization + Enrichment

including NIST + MITRE + Asset Value index...

	Definitions:
Account `account`	The account or subscription that the event or finding applies to
Resource `resource`	A set of resource data types that describe the resources that the finding refers to.
Event Name `eventName`	The description of the event or finding. This field can be nonspecific boilerplate text or details that are specific to the instance of the event or finding.
Event Type `eventType`	One or more event or finding types that classify a finding
Severity `severity`	The event or finding's severity

```
CSNF Schema:

{
    "header": {
        "version": 1,
    },
    "payload": {
        "account": { id },
        "resource": { id },
        "eventName": { string },
        "eventType": { string },
        "severity": { string }
    }
}
```

Modern Defense Solutions

- Intelligent Cyber Data Lakes
- ONUG Automated Cloud Governance CNSF
- MITRE ATT&K Framework Integration
- SCAP/OpenSCAP
- Cyber Range/Honey Pots
- Custom Built Advisory Analysis Tools

Trust Differently

Modern Trust Goals

- Zero Trust Architecture
- Automated Control-Based Assessments
- Distributed Secrets Management
- Distributed Trust

Modern Trust Solutions

- NIST 800-207 - Zero Trust Architecture
- SPIFEE
- Sigstore

Thank You

jwillis@redhat.com
@botchagalupe