Enhancing DevSecOps with Observability and Automation

Mike Polisky
Consulting Sales Engineer – Security (Civilian)
January 2021
Agenda

DevSecOps
• What is it?
• The Mission
• What it requires

How Splunk Supports the Mission
• Observability
• Automation
• Security Analysis & Response

How to get started
• Leverage existing resources, deployment templates
What is DevSecOps Anyway?

Just the latest industry buzz word? No…
Independent Missions

**Development** – build a great application or service

**Operations** – Ensure that application or service is available

**Security** – Protect the entire enterprise, all attack surfaces.
DevOps Model - Traditional
Cloud is a Critical Enabler of Transformation, but **Increases Complexity**

1. **LIFT & SHIFT**
   - VELOCITY: 1x Release Per Year
   - COMPLEXITY: Primarily Cloud IaaS

2. **RE-ARCHITECT**
   - VELOCITY: 10x Release Per Quarter
   - COMPLEXITY: More Modular, but Dependent App Components

3. **CLOUD-NATIVE**
   - VELOCITY: 100x Release Per Month
   - COMPLEXITY: Loosely Coupled Microservices, and Serverless Functions

**What’s Different**

- “You Build It, You Run It”
- Complex Dependencies
- Dynamic, Short-lived Infrastructure

**What’s Different**

- Private
- Public
- VM
- VM
- VM
- VM
- VM
- VM
DevSecOps Model
DevSecOps Mission

DevSecOps is an organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to improve customer outcomes and mission value by automating, monitoring, and applying security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor.

DevSecOps Requirements

One size does not fit all

Top 5

- Collaboration/Ownership (People)
- Education (People)
- Set Policy from the top (Process)
- Visibility (Technology)
- Automation (Technology)
DevSecOps

**Organization**
- Culture shift & buy-in
- Communication & collaboration
- Security/QA throughout
- Learn from success/failure
- Feedback and user-driven change

**Process**
- Collaborative design
- Test-driven development
- Common and automatable tasks
- Continuous adaptation and improvement
- Continuous ATO

**Technology**
- Tool adoption
- Automation and orchestration
- Cloud and containerization
- Infrastructure as Code
- Security as Code

**Governance**
- Built-in governance control
- Uniform policy enforcement
- Data-driven validation
- Enhanced visibility
- Inherited certifications and authorizations

---

DevSecOps Alignment
...We Are In This Together (Like It Or Not)

**AppDev**
- Agile / Lean
- Containers
- Experimentation & PoCs
- Fast Feedback
- CI/CD
- Automation
- MVP
- Modern / Open
- Scalable / Elastic
- Test-Driven

**Security**
- Compliance
- Integrity
- Availability
- Confidentially
- Auditable
- Non-Repudiation
- Protectable / Guardable
- Observabe / Visible
- Resilient
- Loss / Risk Reduction

**Operations**
- Change Management
- Uptime
- Performance
- Sustainable
- Repeatable / Consistent
- Recoverable
- Controllable
- Manageability
- Supportability
- Reliable

...We Are In This Together (Like It Or Not)
How Splunk Helps Today

Observability
Automation
Security Analysis & Response
Example Across Tool Chain

- Plan
- Code
- Build
- Config
- Test/QA
- Stage
- Release
- Monitor

Secure

API

SDKs

UI

Splunk

Incident Response

On-Premise, Cloud, Hybrid

Escalation/ Collaboration
Example Splunk Implementation
A CI / CD Pipeline

- Splunk Enterprise / Splunk Cloud
- Security & Performance Testing
- Operational Security Metrics
  - SignalFX APM + Omnition
  - Observability

Value Stream

- CODE
- BUILD
- TEST
- RELEASE
- DEPLOY
- OPERATE
- MONITOR
- RESPOND

- Source Code Analysis / Software Composition Analysis
- Artifact Scanning / Dependency Tracking

- Automation
  - Phantom
  - ITSI & On-Call

Splunk Enterprise / Splunk Cloud
Splunk APM

For Security, this delivers deep context:
Take the Right Action Quickly and Accurately

Splunk provides the framework and integrations to respond quickly when speed is key

A Single Source of Truth

- Enrich with context from cloud resources, share intel across teams within platform.

Respond Faster

- Reduce dwell times with automated investigations.
- Reduce response times with playbooks that run at machine speed.

In-Context Collaboration

- Work as team to increase situational awareness with integrated chat and shared notes.

Level Up Standards

- Use response templates and prebuilt searches to guide junior analysts

Report and Measure

- Track KPIs to find bottlenecks and guide improvement projects
~500 Free Example Detections from Splunk Security Essentials

https://splunkbase.splunk.com/app/3435

Cloud APIs Called More Often Than Usual Per User
Cloud Provisioning Activity from Unusual Country
Cloud Provisioning Activity from Unusual IP
Instance Created by Unusual User
Instance Modified by Unusual User
New Cloud API Call Per Peer Group
New IaaS API Call Per User
Public Cloud Storage (Bucket)
Unusual Cloud Regions
Unusual Number of Modifications to Cloud ACLs
Example Detections from Splunk ES Content Updates


Cloud Cryptomining
Container Implantation Monitoring & Investigation
Kubernetes Scanning Activity
Kubernetes Sensitive Object Access Activity
Kubernetes Sensitive Role Activity
Cloud Compute Instance Created By Previously Unseen User
Cloud Compute Instance Created With Previously Unseen Image
Cloud Compute Instance Started In Previously Unused Region
Investigate Cloud Compute Instance Activities
Investigate User Activities in All Cloud Regions
Investigate User Activities in Single Cloud Region
## Kubernetes Sensitive Object Access Activity

**Description:**
This story addresses detection and response of accounts accessing Kubernetes cluster sensitive objects such as configmaps or secrets providing information on items such as user, group, object, namespace and authorization reason.

**Narrative:**
Kubernetes is the most used container orchestration platform, this orchestration platform contains sensitive objects within its architecture, specifically configmaps and secrets, if accessed by an attacker can lead to further compromise. These searches allow operator to detect suspicious requests against Kubernetes objects.

## Kubernetes Sensitive Role Activity

**Description:**
This story addresses detection and response around Sensitive Role usage within a Kubernetes clusters against cluster resources and namespaces.

**Narrative:**
Kubernetes is the most used container orchestration platform, this orchestration platform contains sensitive roles within its architecture, specifically configmaps and secrets, if accessed by an attacker can lead to further compromise. These searches allow operator to detect suspicious requests against Kubernetes role activities.
Splunk Helps By:

• Creating visibility into the delivery chain from Dev to Prod
• Help identify configuration drift between Dev and Prod
• Support shared accountability for Security
• Give application level context for incident response
• Make the “shift-left” concept sustainable
Getting Started
Start Collecting Data
Plan the Pipeline

Summary

1) DevSecOps - Core Mission
   Mindset + Org integration
   Not just toolset

2) How Splunk Helps Today
   Get visibility into entire process
   Leverage Automation
   Focus on the metrics important to your organization

3) Take the first step, and stay in motion
   Leverage existing tools
   Consult Existing Reference Designs
Thank you!

Mike Polisky
Consulting Sales Engineer – Security (Civilian)
mpolisky@splunk.com
www.linkedin.com/in/michaelpolisky