Enhancing DevSecOps with Observability and Automation

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

splunk> turn data into doing™

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…

splunk> turn data into doing™

Independent Missions

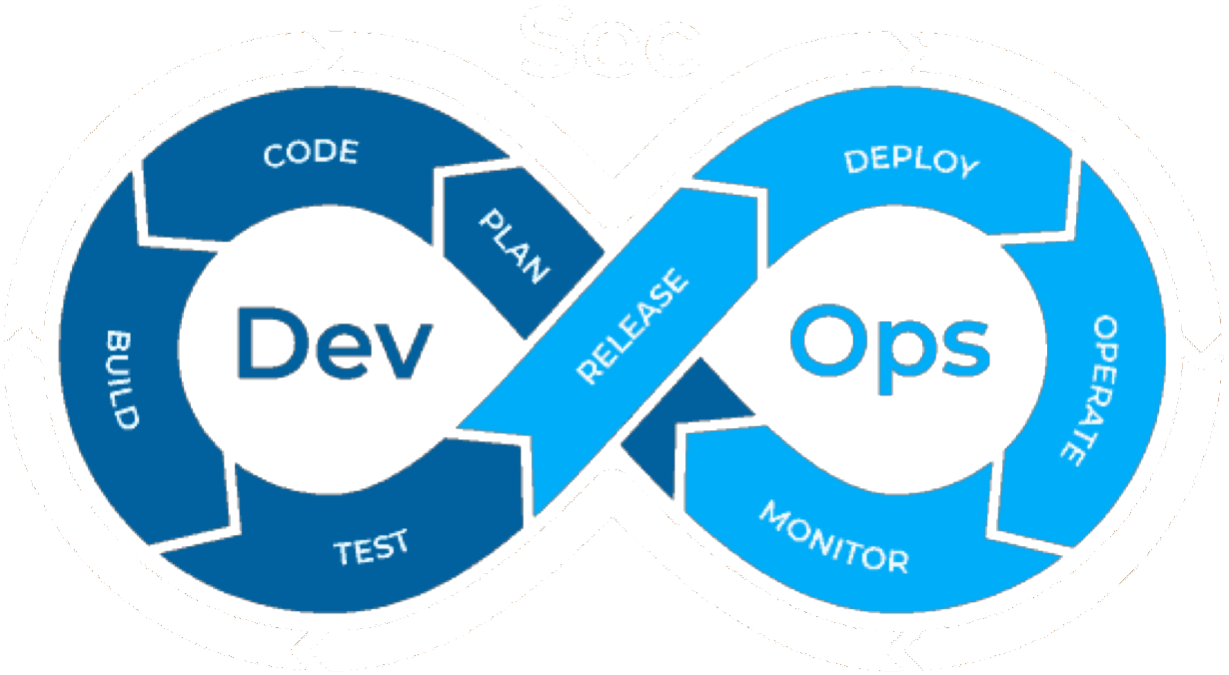
Development – build a great application or service

Operations – Ensure that application or service is available

Security – Protect the entire enterprise, all attack surfaces.

splunk> turn data into doing™

DevOps Model - Traditional



Cloud is a Critical Enabler of Transformation, but Increases Complexity

What's Different

VELOCITY

COMPLEXITY

1 LIFT & SHIFT

DEV ⟷ OPS

1x Release Per Year

CLIENT SERVER

DATABASE

JAVA APPLICATION SERVER

Primarily Cloud IaaS

DC

VM VM VM VM VM VM

Private

Public

2 RE-ARCHITECT

DEV OPS

10x Release Per Quarter

More Modular, but Dependent App Components

VM VM VM

Private

Public

3 CLOUD-NATIVE

DEV OPS

100x Release Per Month

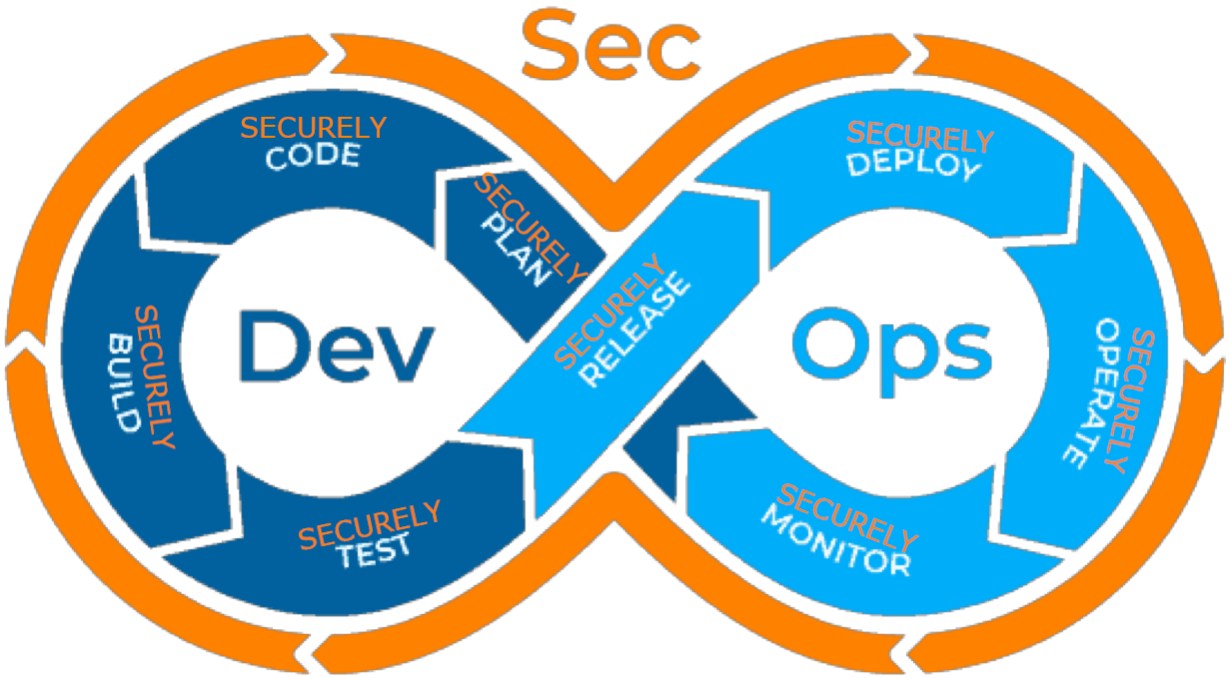
Loosely Coupled Microservices, and Serverless Functions

Private

Public

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

DevSecOps Model



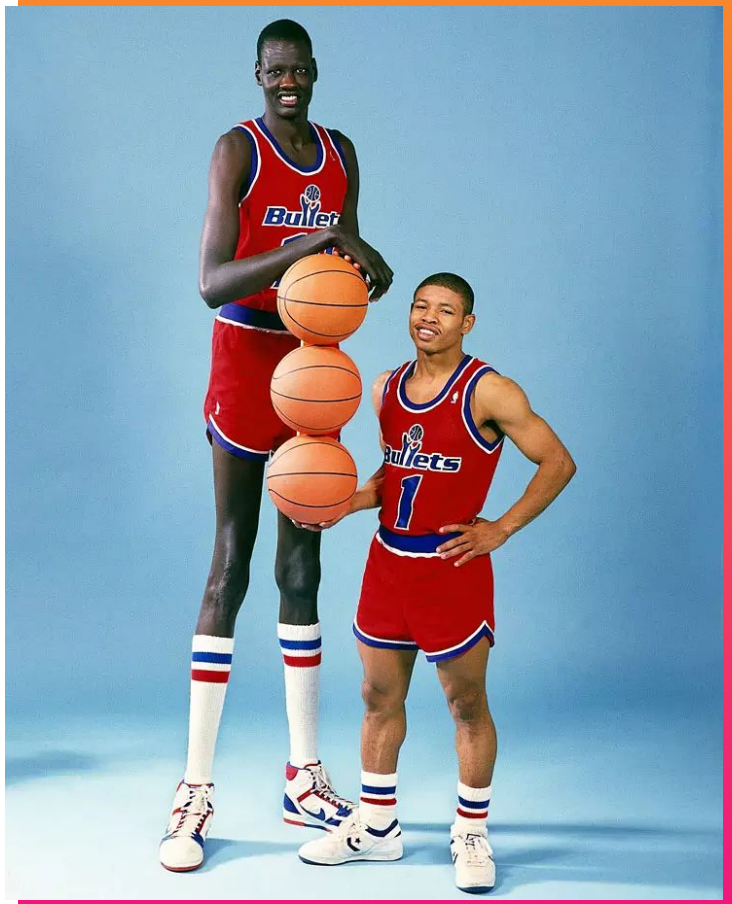
DevSecOps Mission

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.

https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf

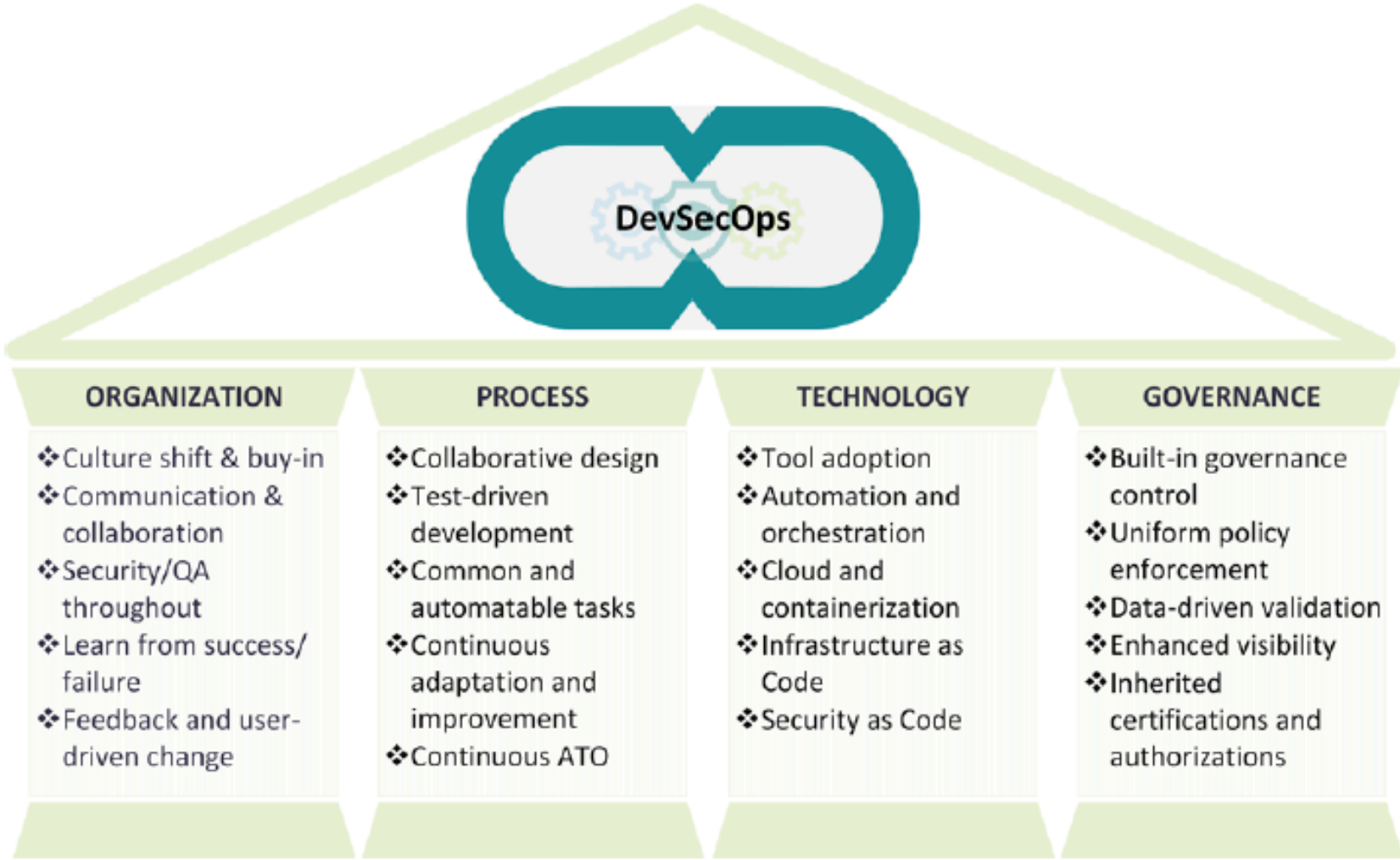
DevSecOps Requirements

One size does not fit all



Top 5

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



https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf

DevSecOps Alignment

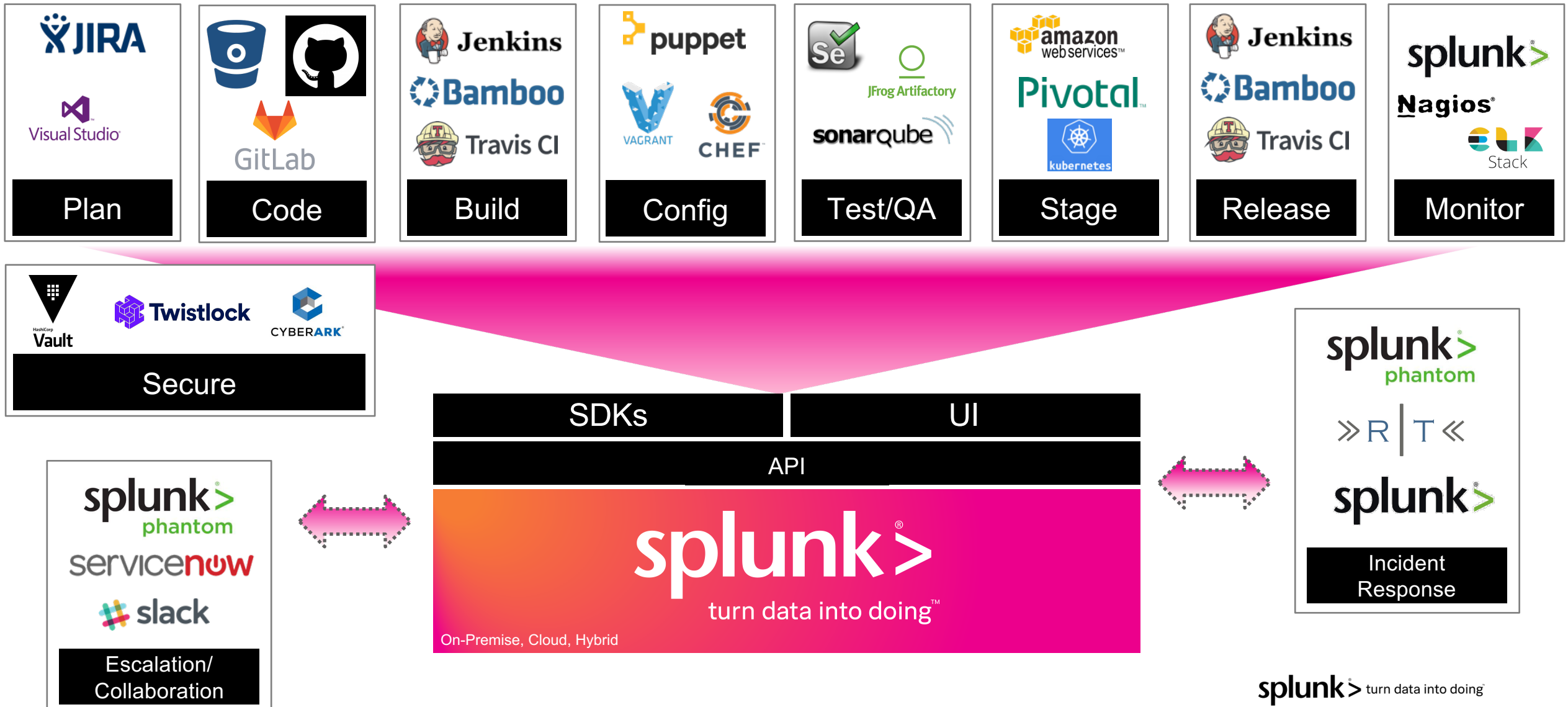
…We Are In This Together (Like It Or Not)

How Splunk Helps Today

Observability
Automation
Security Analysis & Response

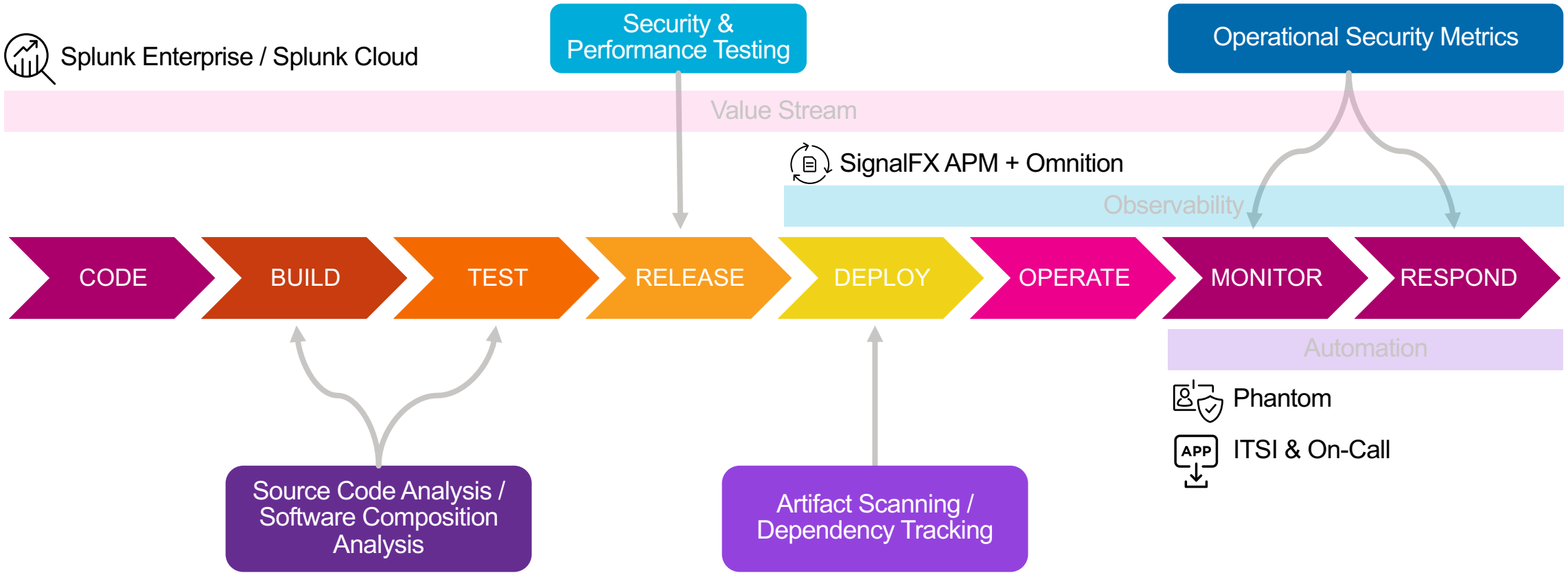
splunk> turn data into doing™

Example Across Tool Chain



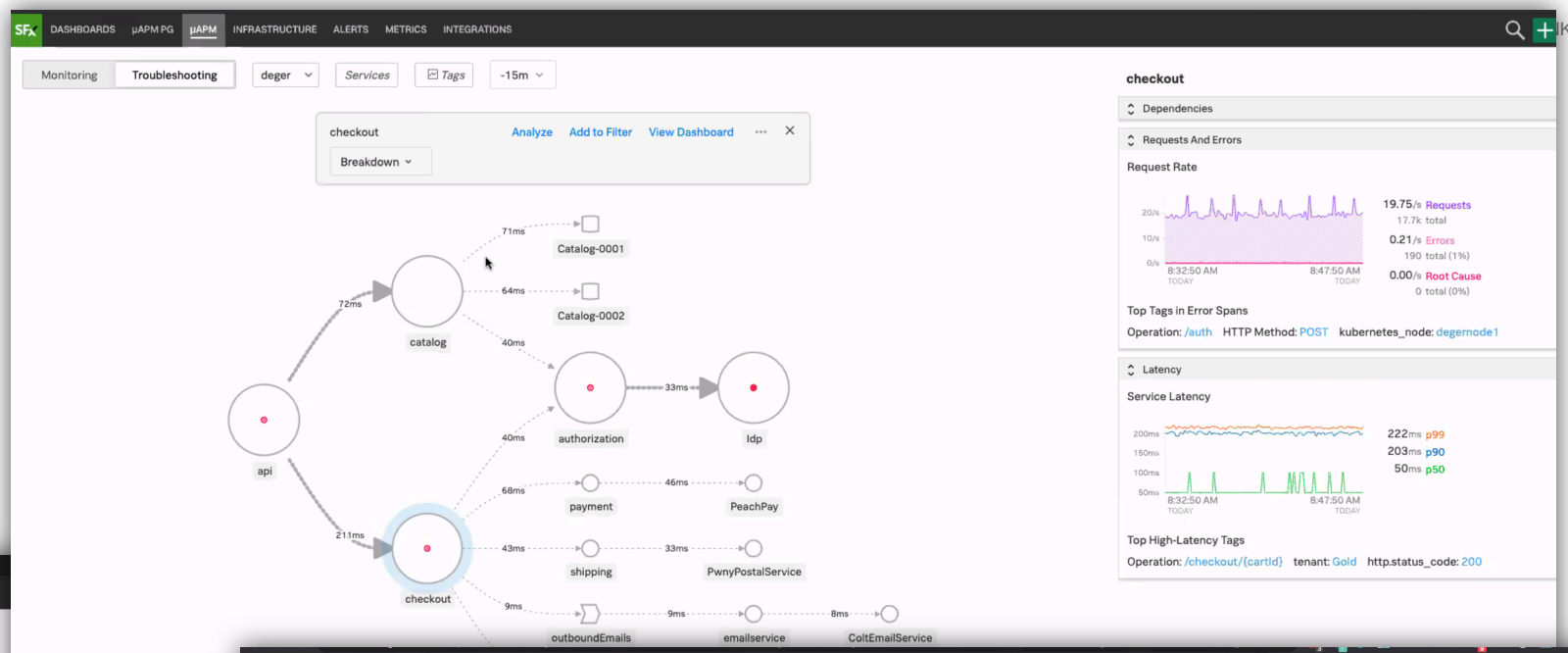
Example Splunk Implementation

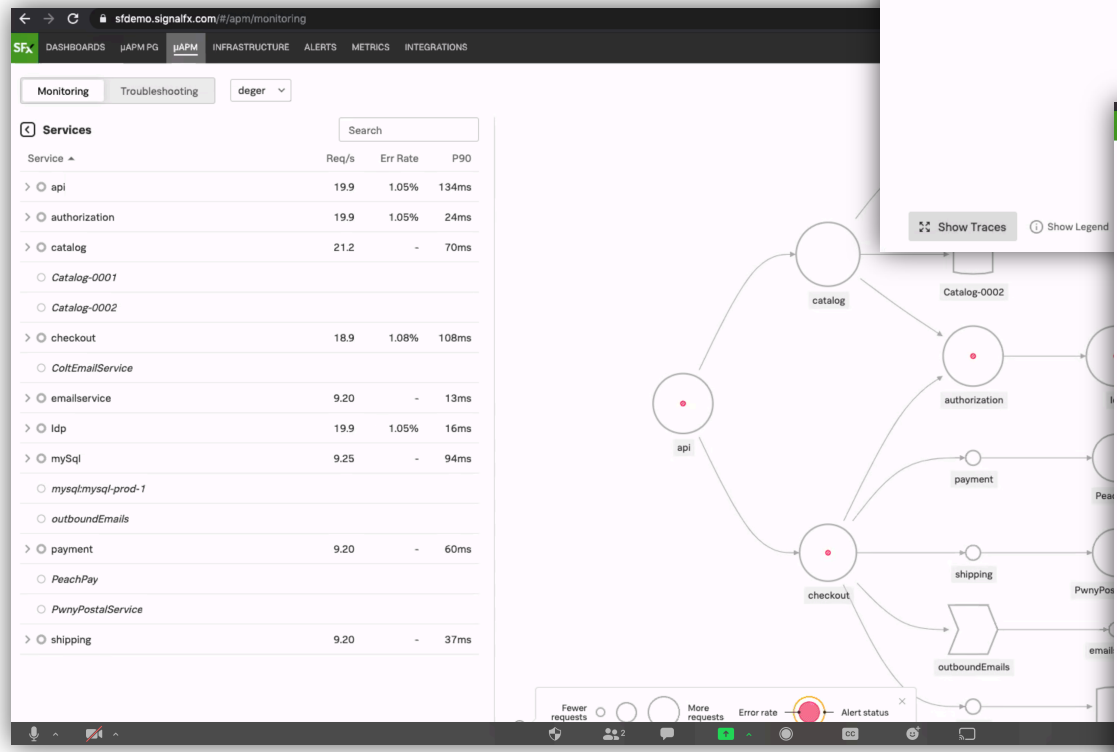
A CI / CD Pipeline

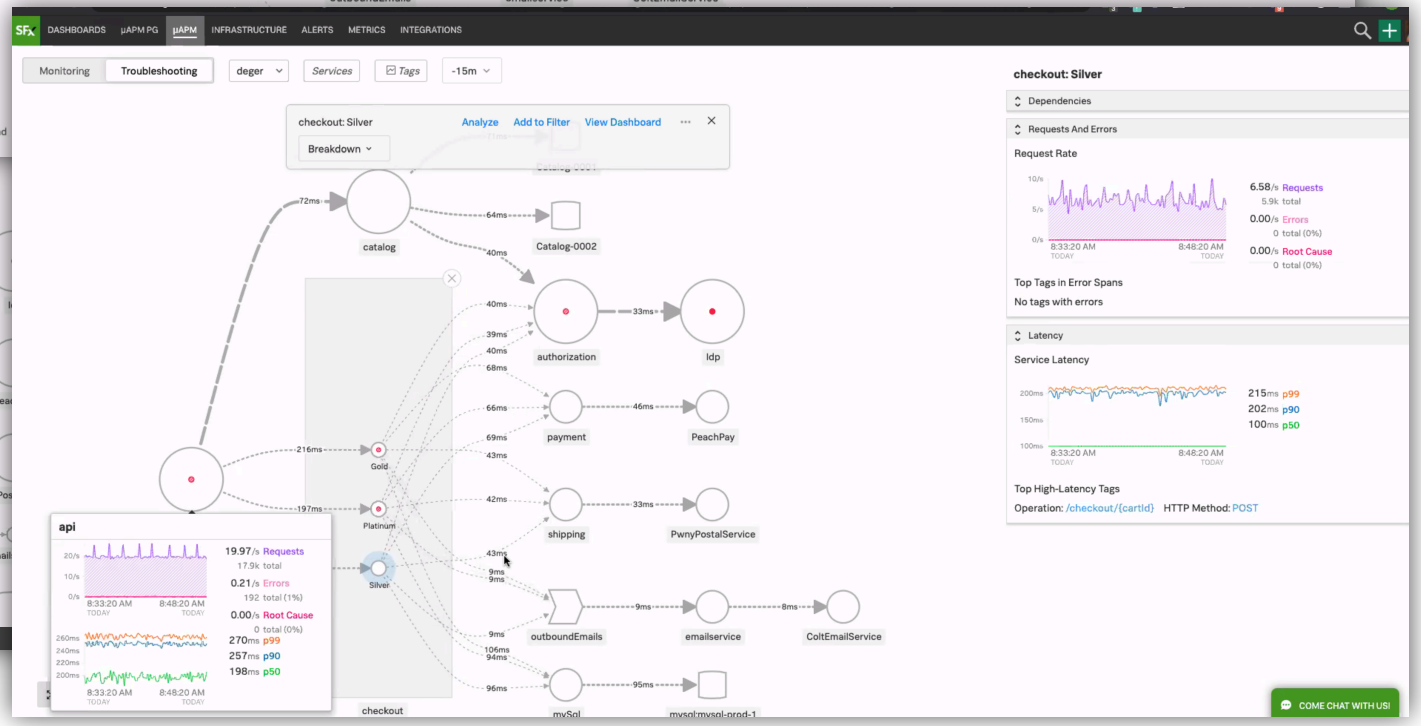


Splunk APM

For Security,
this delivers deep context:



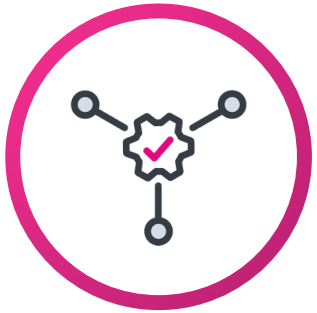




Take the Right Action Quickly and Accurately

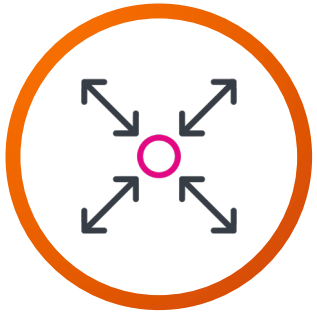
Splunk provides the framework and integrations to respond quickly when speed is key

A Single Source of Truth



Enrich with context from 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

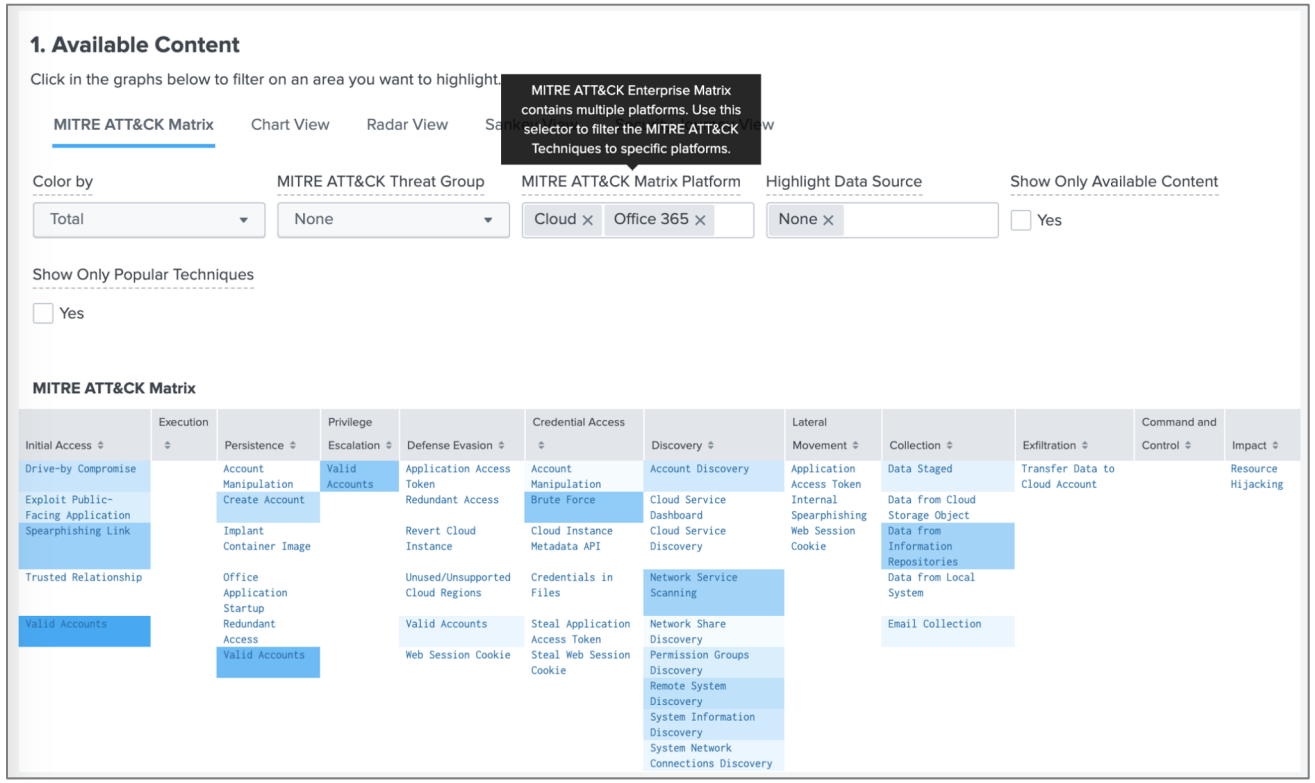
New Cloud API Call Per Peer Group

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

https://splunkbase.splunk.com/app/3449/ & https://github.com/splunk/security-content

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

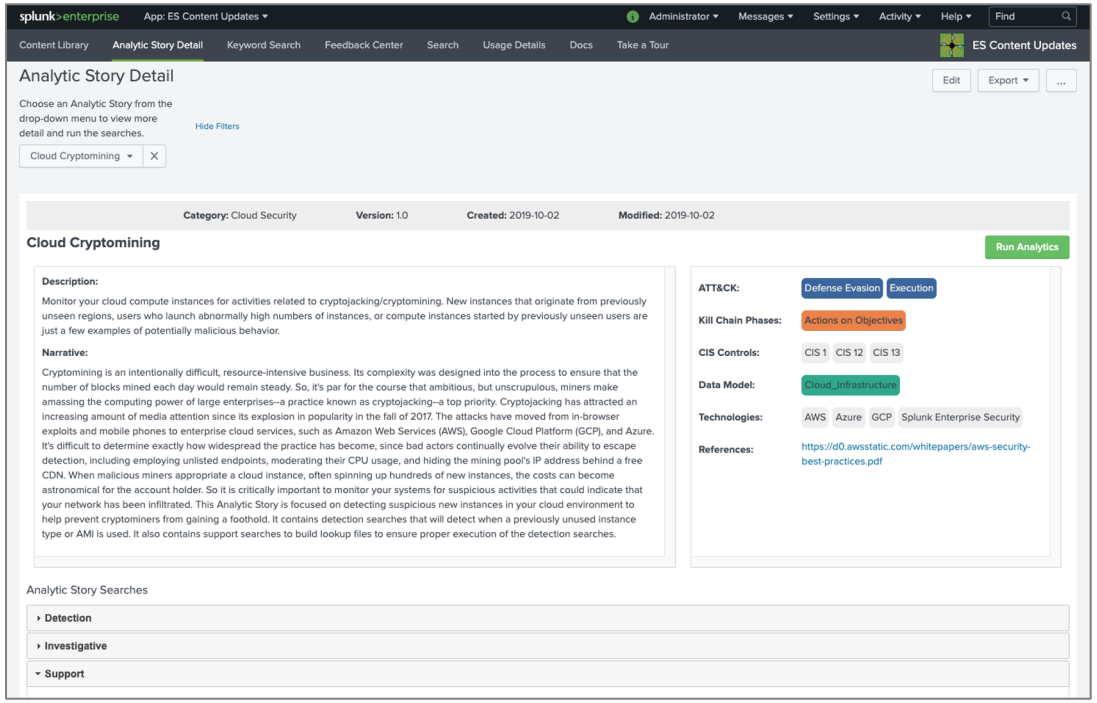
Cloud Compute Instance Created With Previously Unseen Image

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



Analytic Story Detail

Show Filters

Edit | Export | ...

Category: Cloud Security **Version:** 1 **Created:** 2020-05-20 **Modified:** 2020-05-20

Kubernetes Sensitive Object Access Activity

Run Analytics

Description:

This story addresses detection and response of accounts acccesing Kubernetes cluster sensitive objects such as configmaps or secrets providing information on items such as user 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

ATT&CK:

Kill Chain Phases: Lateral Movement

CIS Controls:

Data Model:

References: https://www.splunk.com/en_us/blog/security/

Category: Cloud Security **Version:** 1 **Created:** 2020-05-20 **Modified:** 2020-05-20

Kubernetes Sensitive Role Activity

Run Analytics

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

ATT&CK:

Kill Chain Phases: Lateral Movement

CIS Controls:

Data Model:

References: https://www.splunk.com/en_us/blog/security/appr
kubernetes-security-detecting-kubernetes-scan-with-splunk.html

Splunk Helps By:

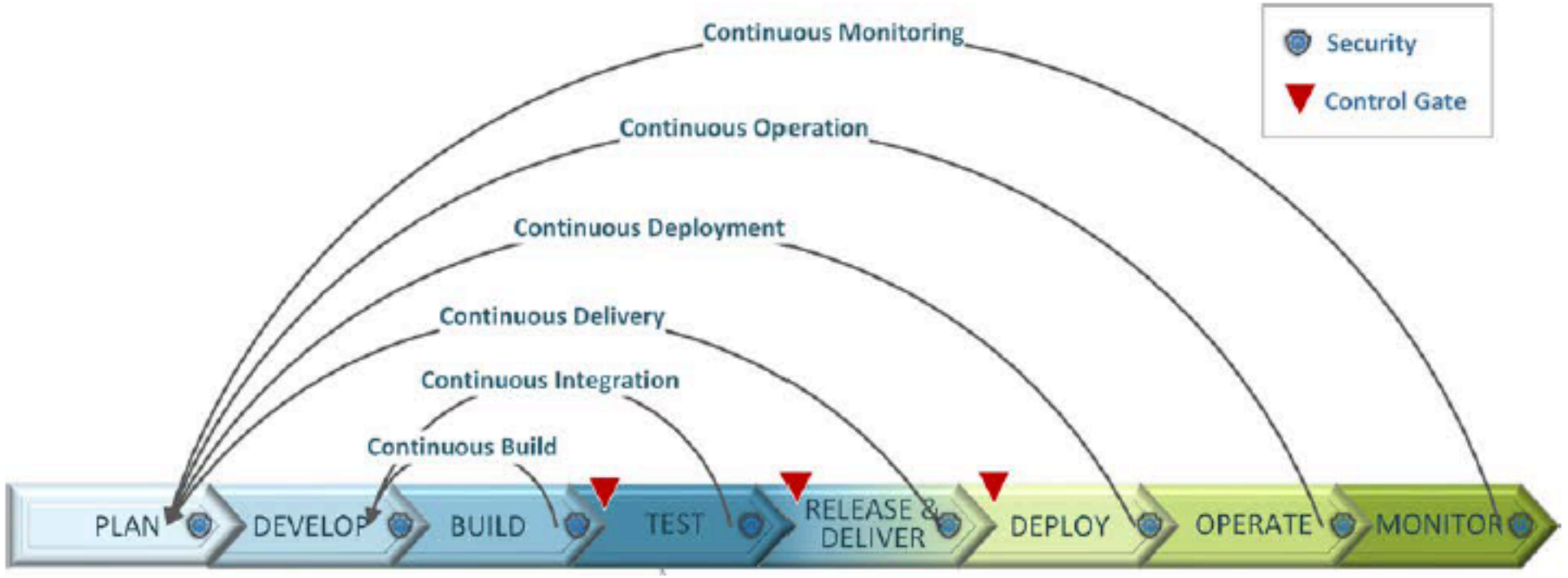
- Creating visibility into the delivery chain from Dev to Prod
- Help identify configuration drift between Dev and Prod
- Support shared accountability for Security
- Give application level context for incident response
- Make the “shift-left” concept sustainable

Getting Started

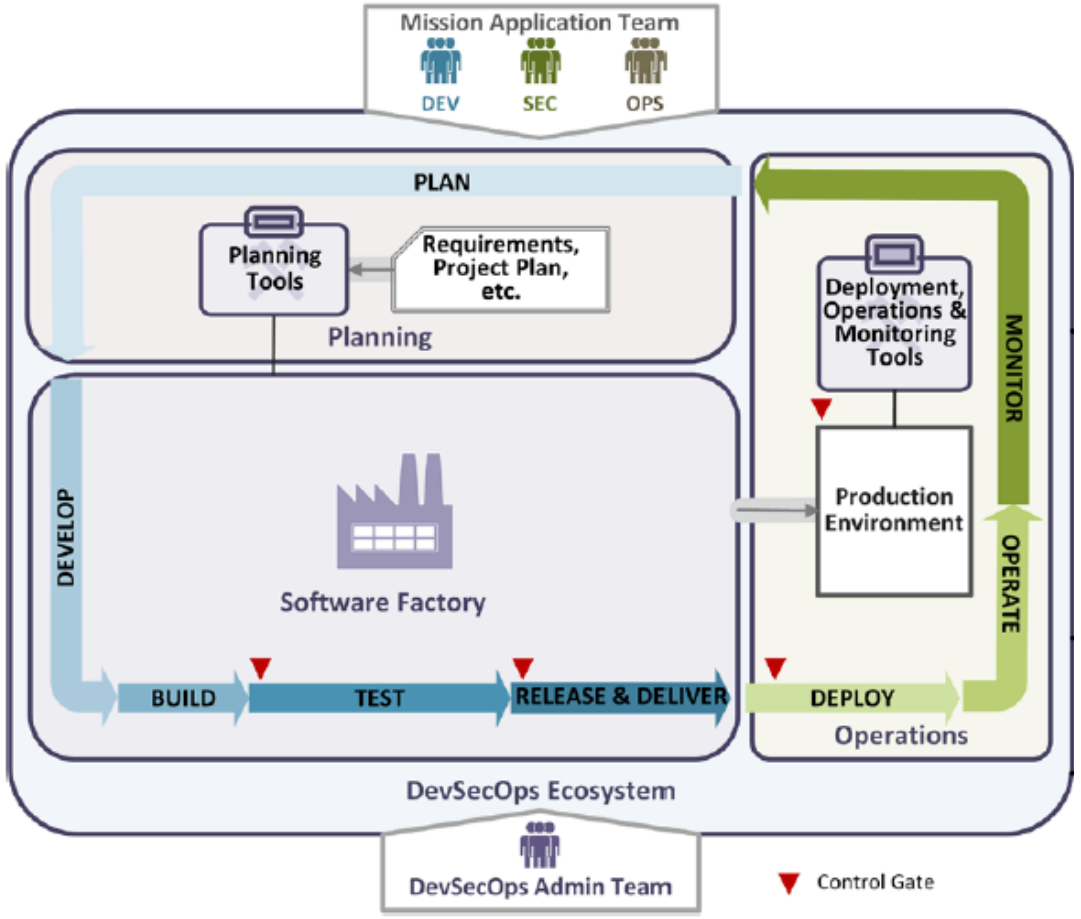
splunk> turn data into doing™

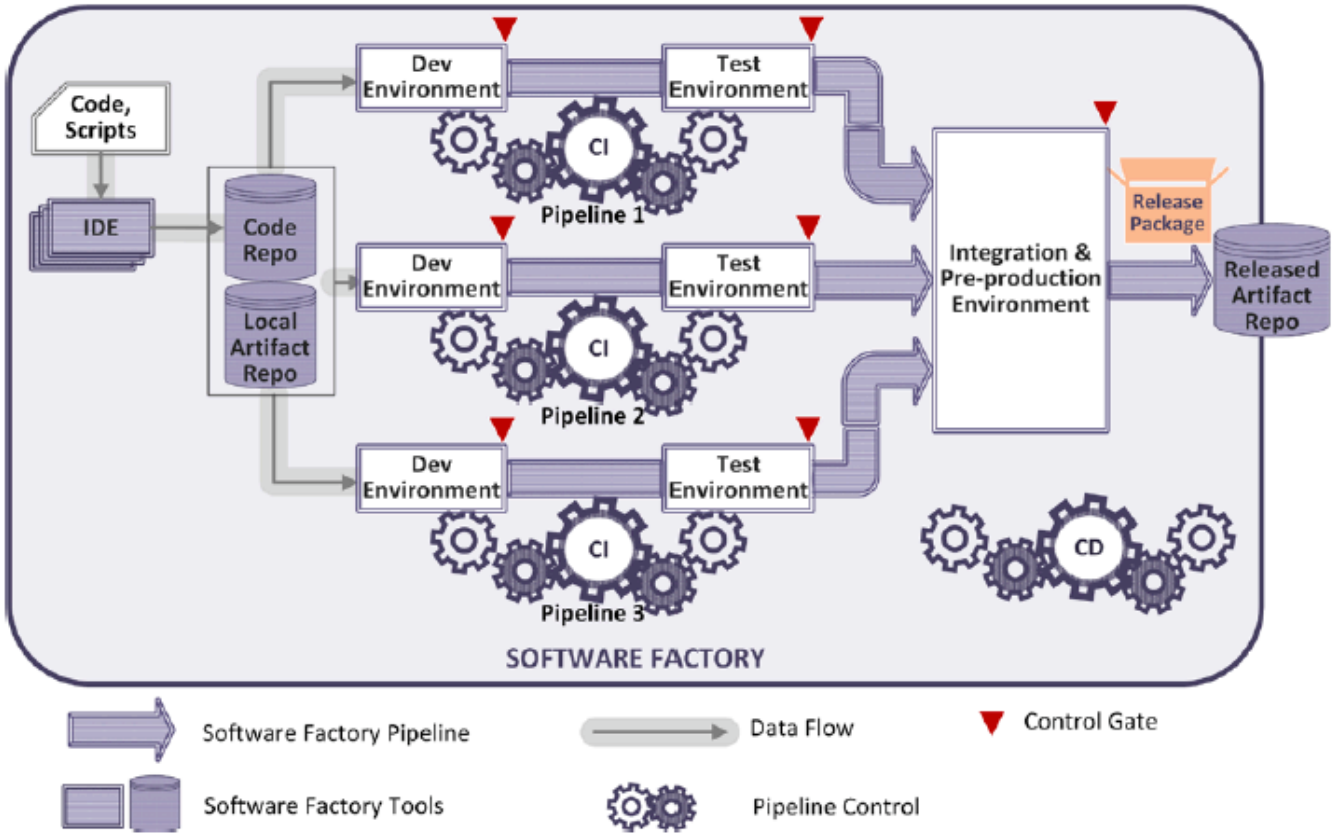
Start Collecting Data

Plan the Pipeline



https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf





https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf

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

splunk> turn data into doing™