

# 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

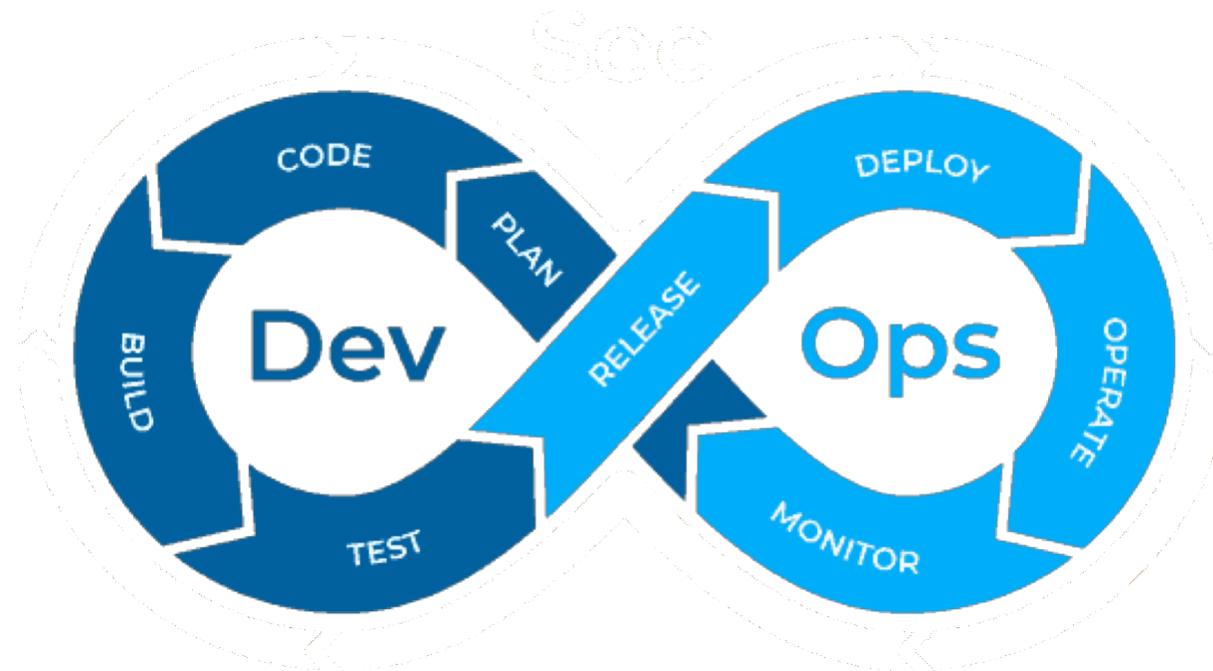
**Development** – build a great application or service

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

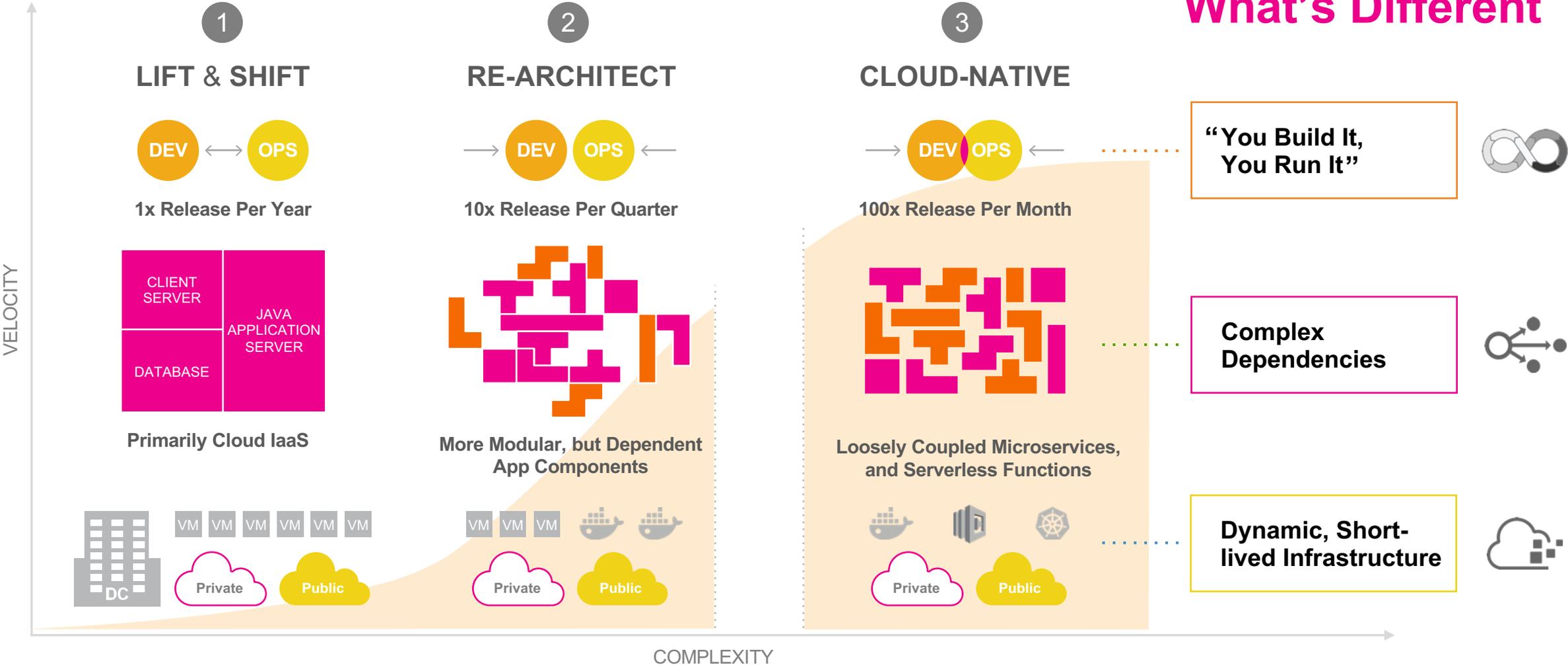
**Security** – Protect the entire enterprise, all attack surfaces.



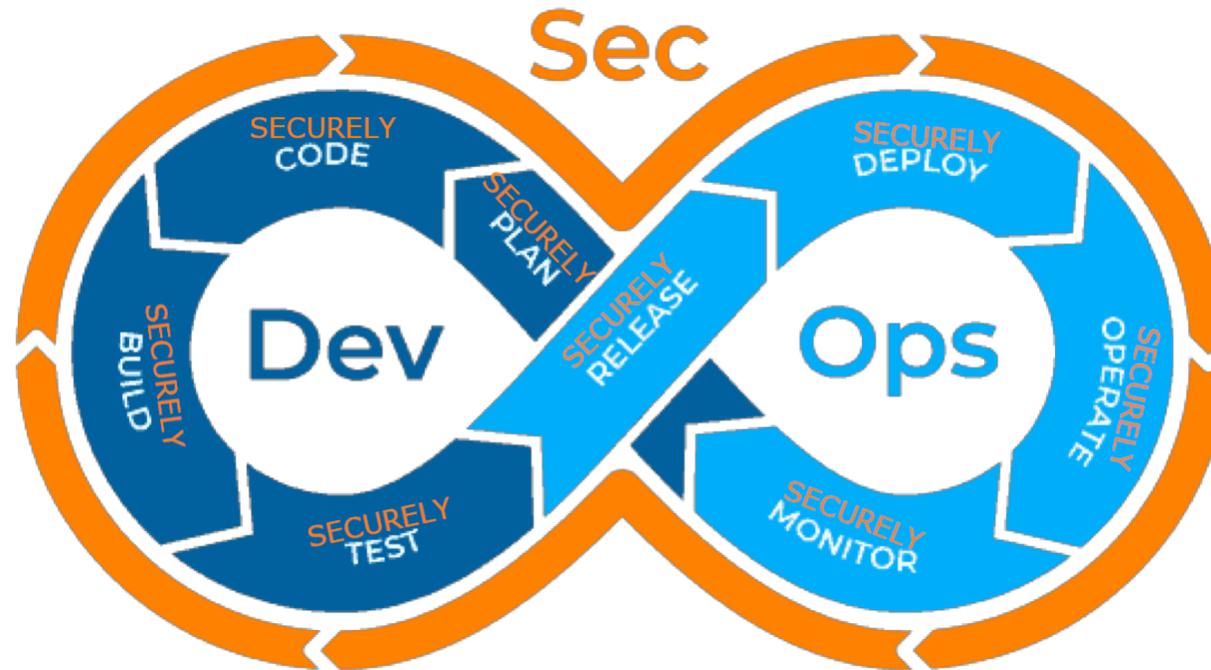
# DevOps Model - Traditional



# Cloud is a Critical Enabler of Transformation, but **Increases Complexity**



# 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.

**splunk**<sup>®</sup> > turn data into doing<sup>™</sup>

[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)

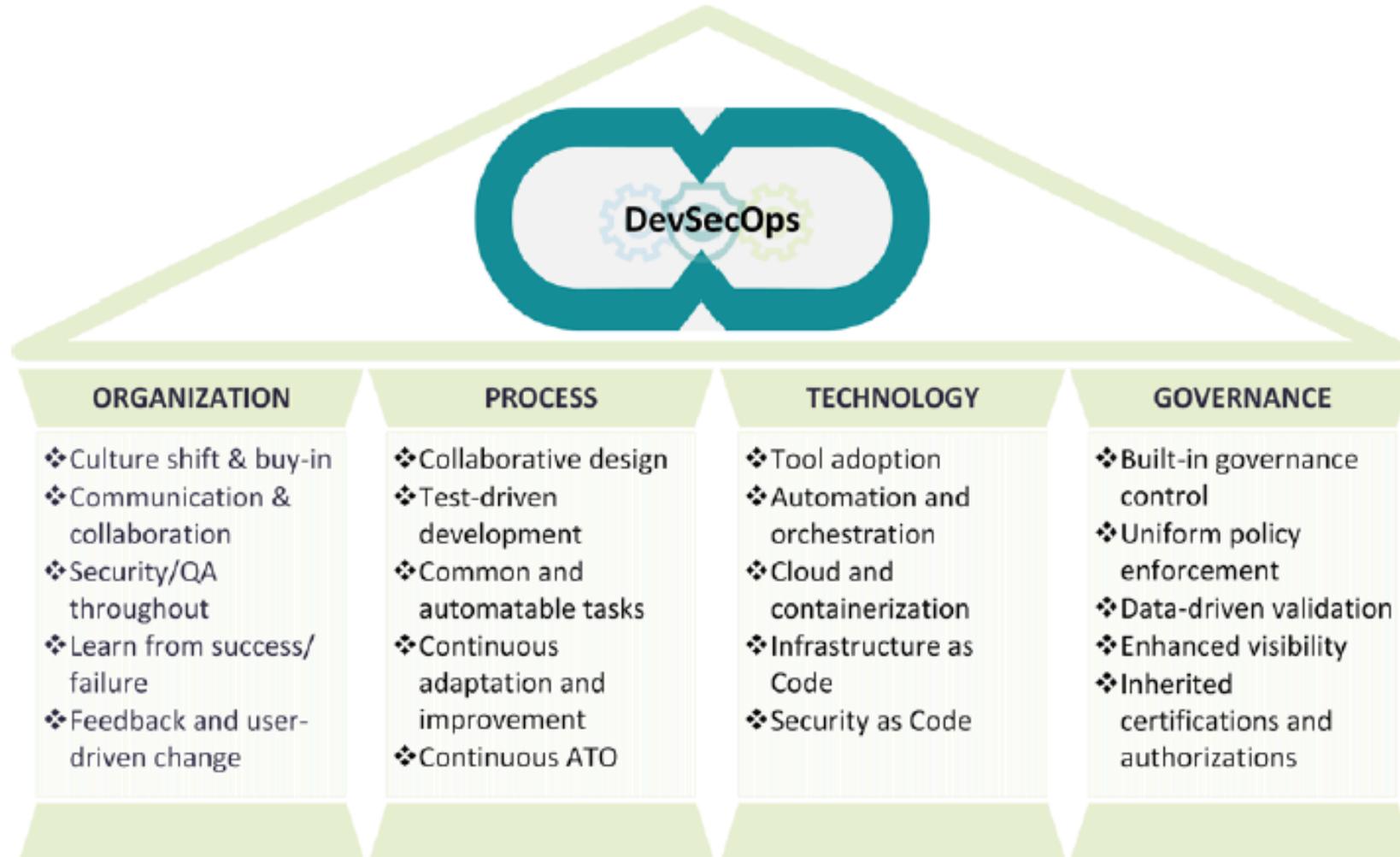
# DevSecOps Requirements

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](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)

## 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
- Observable / Visible →
- Resilient →
- Loss / Risk Reduction →

## Operations

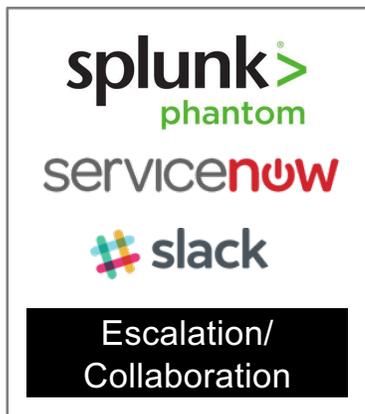
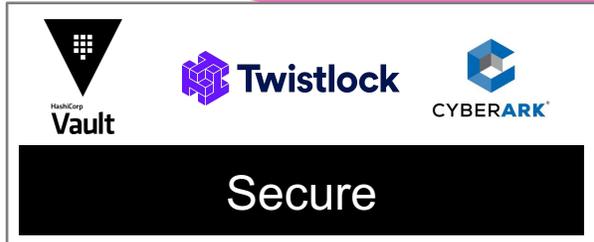
- Change Management
- Uptime
- Performance
- Sustainable
- Repeatable / Consistent
- Recoverable
- Controllable
- Manageability
- Supportability
- Reliable

# How Splunk Helps Today

Observability  
Automation  
Security Analysis & Response

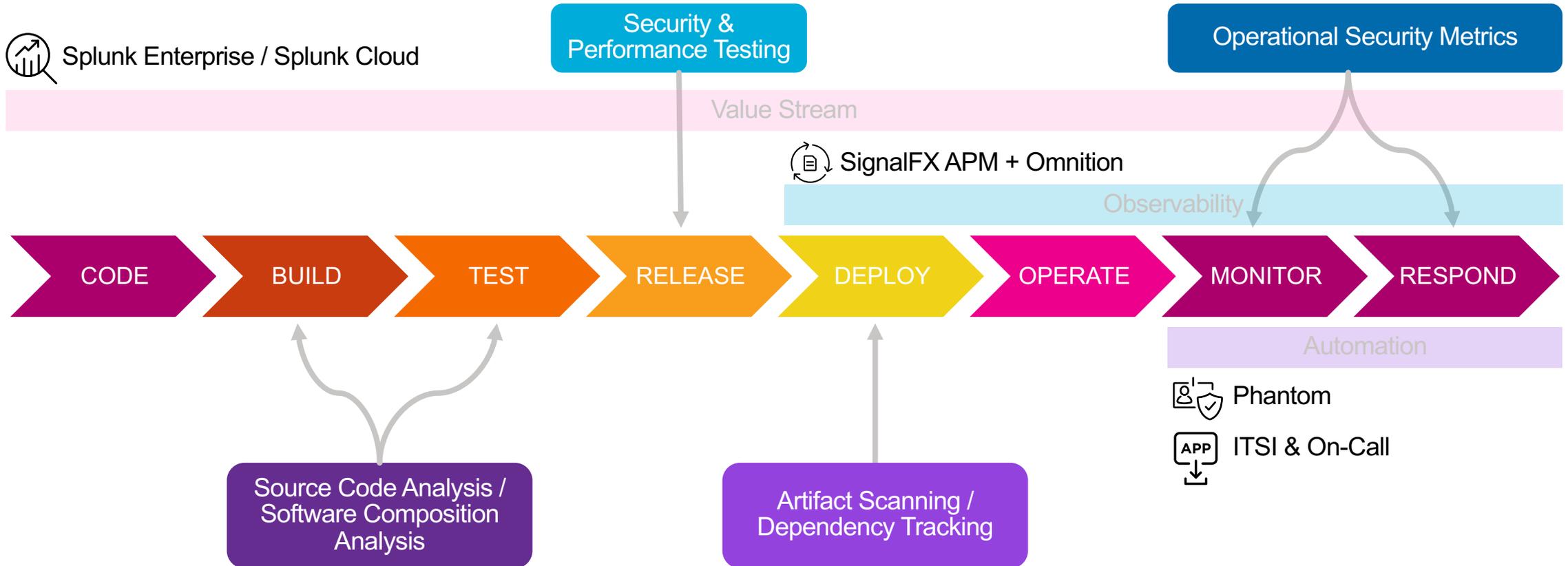
splunk<sup>®</sup> > turn data into doing<sup>™</sup>

# Example Across Tool Chain



# Example Splunk Implementation

## A CI / CD Pipeline



# Splunk APM

For Security,  
this delivers deep context:

Services

Service	Req/s	Err Rate	P90
api	19.9	1.05%	134ms
authorization	19.9	1.05%	24ms
catalog	21.2	-	70ms
checkout	18.9	1.08%	108ms
emailservice	9.20	-	13ms
Idp	19.9	1.05%	16ms
mysql	9.25	-	94ms
payment	9.20	-	60ms
shipping	9.20	-	37ms

checkout

Breakdown

Request Rate: 19.75/s Requests, 0.21/s Errors, 0.00/s Root Cause

Service Latency: 222ms p99, 203ms p90, 50ms p50

Top High-Latency Tags: Operation: /checkout/{cartId} tenant: Gold http.status\_code: 200

checkout: Silver

Request Rate: 6.58/s Requests, 0.00/s Errors, 0.00/s Root Cause

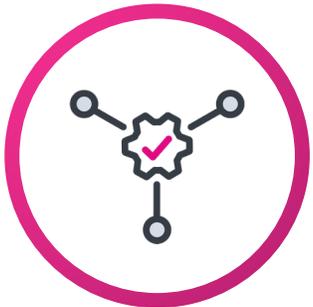
Service Latency: 215ms p99, 202ms p90, 100ms p50

Top High-Latency Tags: Operation: /checkout/{cartId} HTTP Method: POST

# Take the Right Action Quickly and Accurately

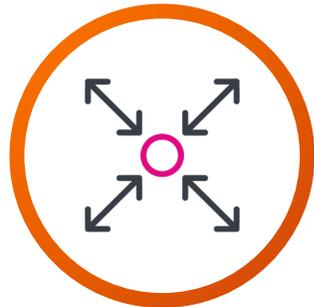
Splunk provides the framework and integrations to respond quickly when speed is key

## 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

**1. Available Content**

Click in the graphs below to filter on an area you want to highlight

**MITRE ATT&CK Matrix** Chart View Radar View Search

MITRE ATT&CK Enterprise Matrix contains multiple platforms. Use this selector to filter the MITRE ATT&CK Techniques to specific platforms.

Color by MITRE ATT&CK Threat Group MITRE ATT&CK Matrix Platform Highlight Data Source Show Only Available Content

Total None Cloud x Office 365 x None x Yes

Show Only Popular Techniques  Yes

**MITRE ATT&CK Matrix**

Initial Access	Execution	Persistence	Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise		Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data Staged	Transfer Data to Cloud Account		Resource Hijacking
Exploit Public-Facing Application		Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Cloud Storage Object			
Spearphishing Link		Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Information Repositories			
Trusted Relationship		Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data from Local System			
Valid Accounts		Redundant Access	Valid Accounts		Steal Application Access Token	Network Share Discovery		Email Collection			
		Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery					
						Remote System Discovery					
						System Information Discovery					
						System Network Connections Discovery					

# 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

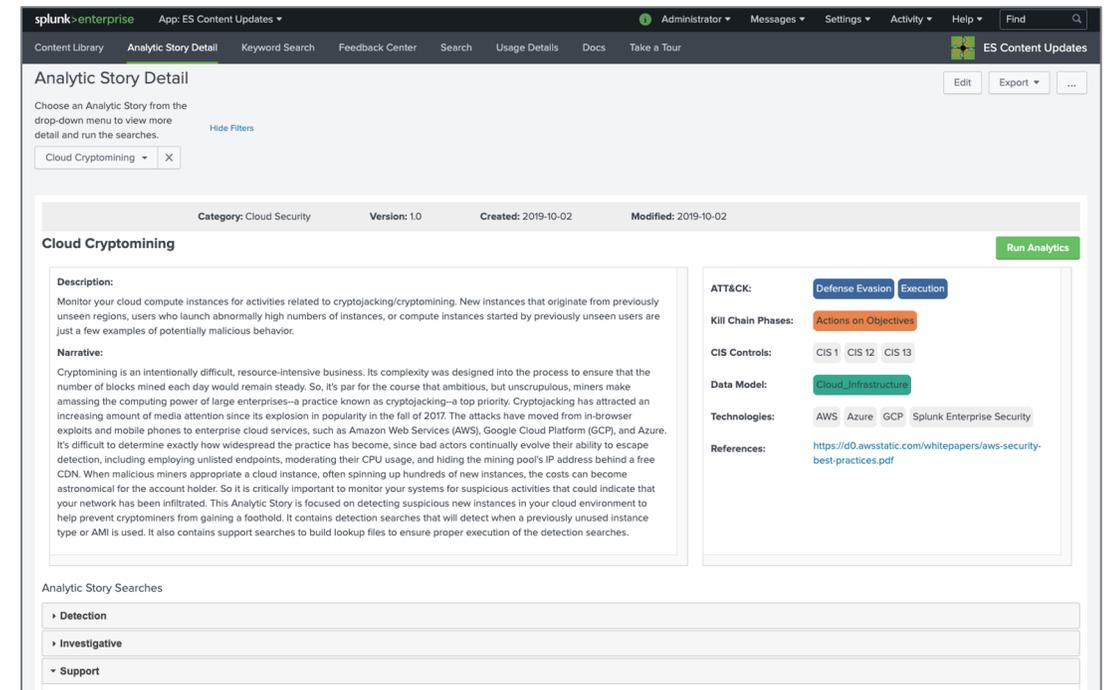
Cloud Compute Instance Created With Previously Unseen Image

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



The screenshot displays the Splunk ES Content Updates interface for the 'Cloud Cryptomining' analytic story. The interface includes a navigation bar with 'splunk>enterprise' and 'App: ES Content Updates'. Below the navigation bar, there are tabs for 'Content Library', 'Analytic Story Detail', 'Keyword Search', 'Feedback Center', 'Search', 'Usage Details', 'Docs', and 'Take a Tour'. The main content area shows the 'Analytic Story Detail' for 'Cloud Cryptomining', with a 'Run Analytics' button. The story details include a description, narrative, and various tags for ATT&CK, Kill Chain Phases, CIS Controls, Data Model, Technologies, and References.

**Category:** Cloud Security **Version:** 1.0 **Created:** 2019-10-02 **Modified:** 2019-10-02

**Cloud Cryptomining** Run Analytics

**Description:**  
Monitor your cloud compute instances for activities related to cryptojacking/cryptomining. New instances that originate from previously unseen regions, users who launch abnormally high numbers of instances, or compute instances started by previously unseen users are just a few examples of potentially malicious behavior.

**Narrative:**  
Cryptomining is an intentionally difficult, resource-intensive business. Its complexity was designed into the process to ensure that the number of blocks mined each day would remain steady. So, it's par for the course that ambitious, but unscrupulous, miners make amassing the computing power of large enterprises—a practice known as cryptojacking—a top priority. Cryptojacking has attracted an increasing amount of media attention since its explosion in popularity in the fall of 2017. The attacks have moved from in-browser exploits and mobile phones to enterprise cloud services, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Azure. It's difficult to determine exactly how widespread the practice has become, since bad actors continually evolve their ability to escape detection, including employing unlisted endpoints, moderating their CPU usage, and hiding the mining pool's IP address behind a free CDN. When malicious miners appropriate a cloud instance, often spinning up hundreds of new instances, the costs can become astronomical for the account holder. So it is critically important to monitor your systems for suspicious activities that could indicate that your network has been infiltrated. This Analytic Story is focused on detecting suspicious new instances in your cloud environment to help prevent cryptominers from gaining a foothold. It contains detection searches that will detect when a previously unused instance type or AMI is used. It also contains support searches to build lookup files to ensure proper execution of the detection searches.

**ATT&CK:** Defense Evasion Execution

**Kill Chain Phases:** Actions on Objectives

**CIS Controls:** CIS 1 CIS 12 CIS 13

**Data Model:** Cloud\_Infrastructure

**Technologies:** AWS Azure GCP Splunk Enterprise Security

**References:** <https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf>

**Analytic Story Searches**

- Detection
- Investigative
- Support

**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 accessing 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/kubernetes-security-detecting-kubernetes](https://www.splunk.com/en_us/blog/security/kubernetes-security-detecting-kubernetes)**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/app/kubernetes-security-detecting-kubernetes-scan-with-splunk.html](https://www.splunk.com/en_us/blog/security/app/kubernetes-security-detecting-kubernetes-scan-with-splunk.html)

# Splunk Helps By:

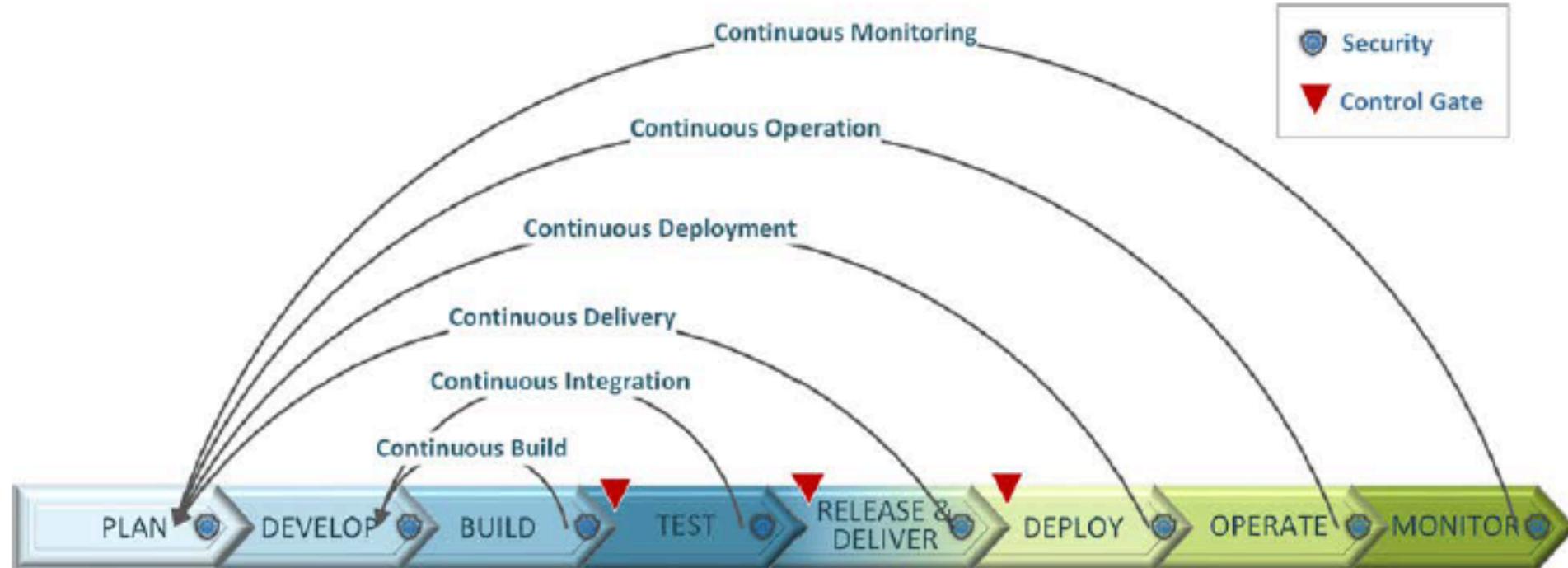
- Creating visibility into the delivery chain from Dev to Prod
- Help identify configuration drift between Dev and Prod
- Support shared accountability for Security
- Give application level context for incident response
- Make the “shift-left” concept sustainable

# Getting Started

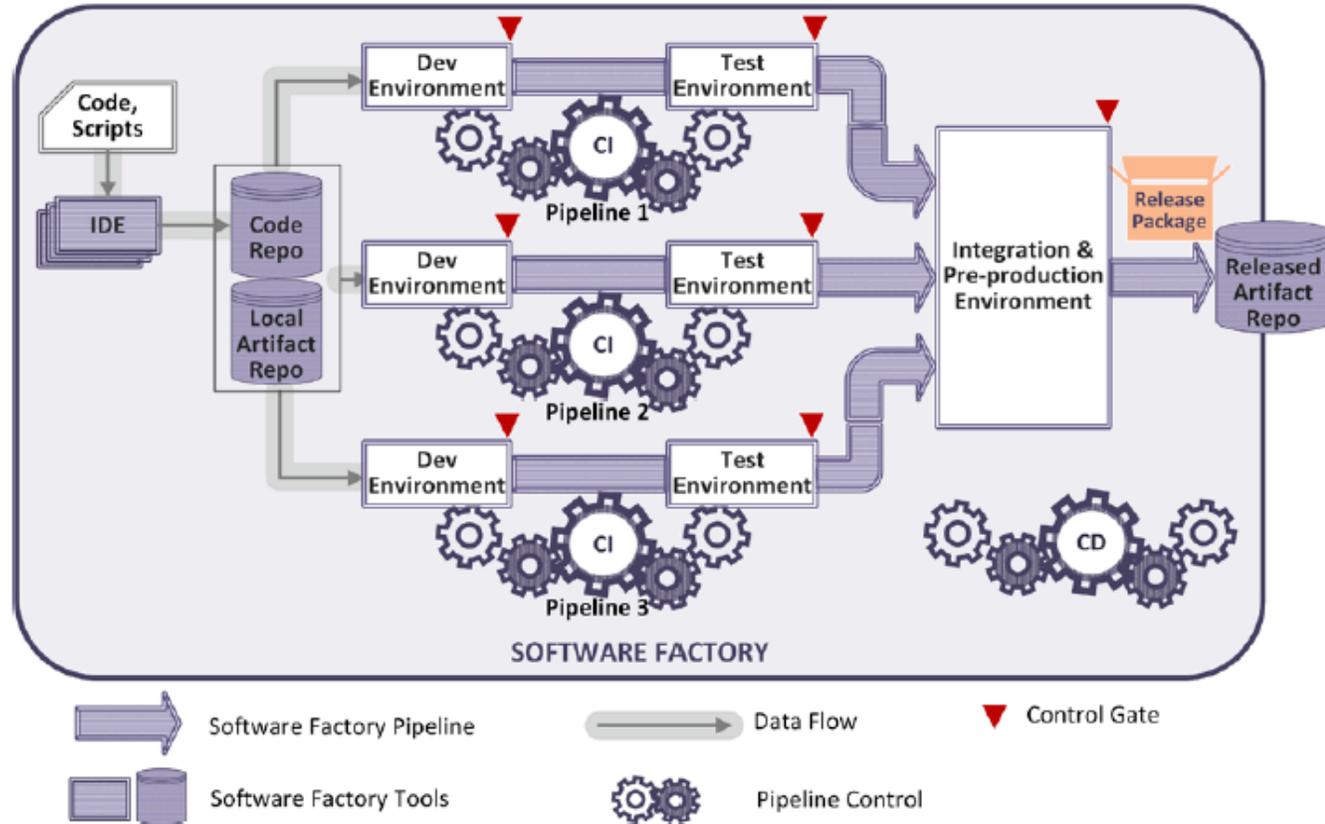
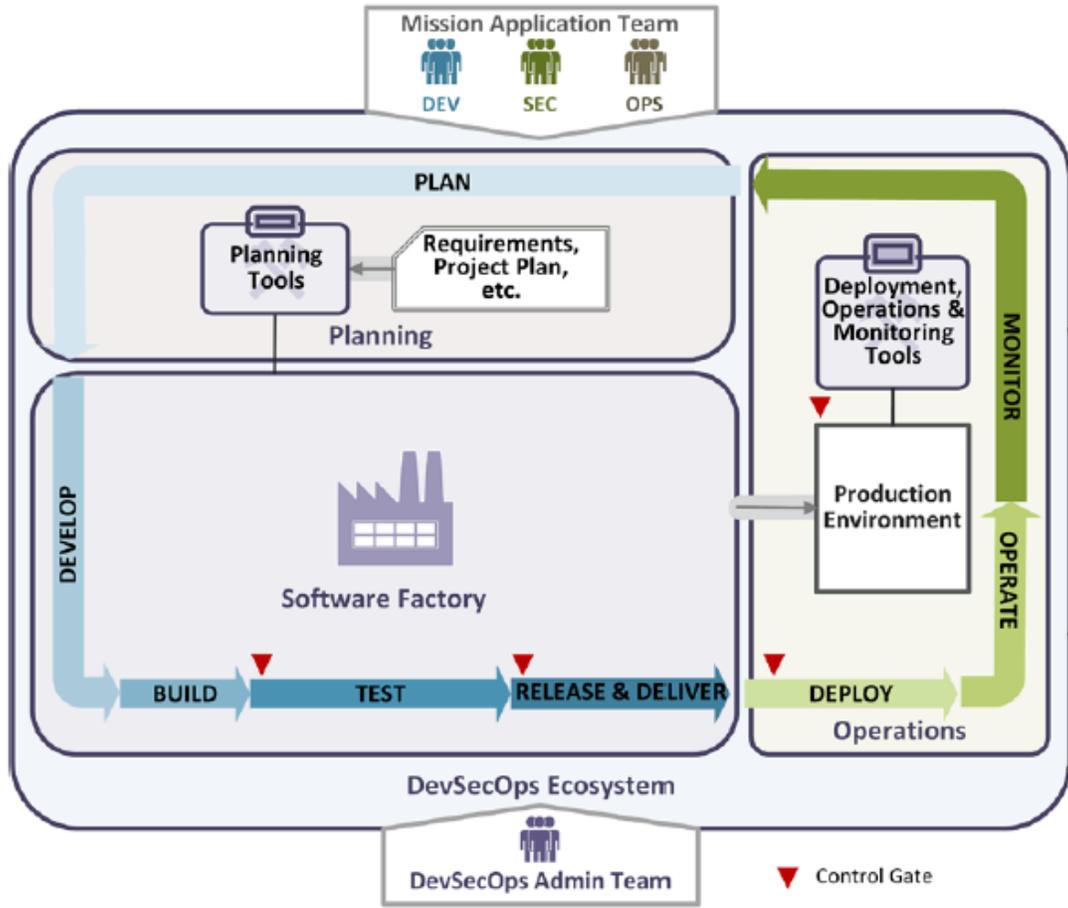
splunk<sup>®</sup> > turn data into doing<sup>™</sup>

# 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)



[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](http://www.linkedin.com/in/michaelpolisky)

**splunk**® > turn data into doing™