

Adding API Security to your DevSecOps Toolbelt

OWASP LA

January 29th, 2025



Talent · Technology · Partners

Agenda

- Introduction
- What are the Stakes?
- Why API Security
- DevOps vs DevSecOps
- Technology
- Processes
- People
- Contact

Introduction

SIS API Security and
DevSecOps Practice



Scott Bly

Director, Security Technologies

sbly@sisinc.com

Background

Noname Security

AWS

CyberSecurity Solutions Architect

Director IT, Cyber

IT/Cyber Consultant 15+ years

What are the Stakes?

- Cyber combat precedes physical combat
- Nation State APTs
- Cybercrime costs \$10 Trillion annually
- \$4.9 million average breach cost
- Regulatory fines
- Business impact
- Bankruptcy for small firms

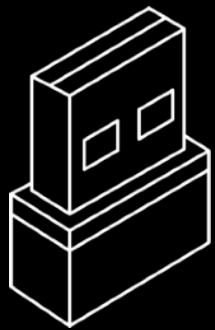


Why API Security

- **85% of web attacks are now API attacks**
- Data is the new GOLD
- DevOps success
- Increased vulnerability
- API interdependent vulnerabilities
- Fix in Dev vs Ops
- 1200:1 | Devs:AppSec
- Technology, Processes, People
- ITERATIVE LIFT not a BURDEN



API Security Foundation



Discovery

API asset inventory, change detection, network mapping, reconnaissance.



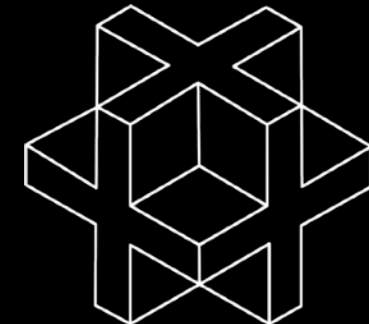
Posture Management

Configuration control, vulnerability management, remediation prioritization.



Runtime Protection

Detection and prevention of attackers and suspicious behavior in real time.



Active Testing

Secure APIs in dev to stop vulnerabilities before production.

DevOps

DevOps Software Factory

- Fast release
- Predictable results
- Infra as Code

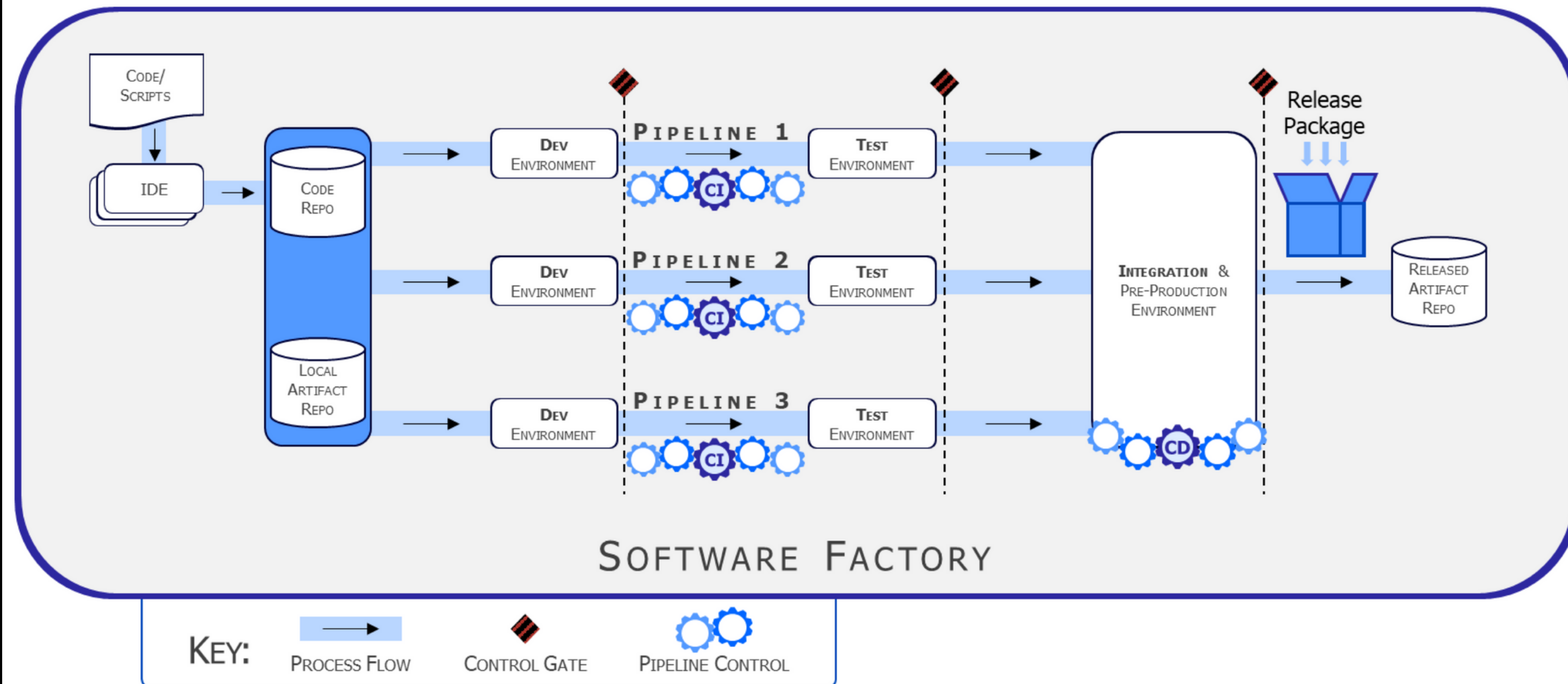


Figure 5 Normative Software Factory Construct

DevSecOps

DevSecOps Software Factory

- Shift Left
- Testing built into stages
- Not enough

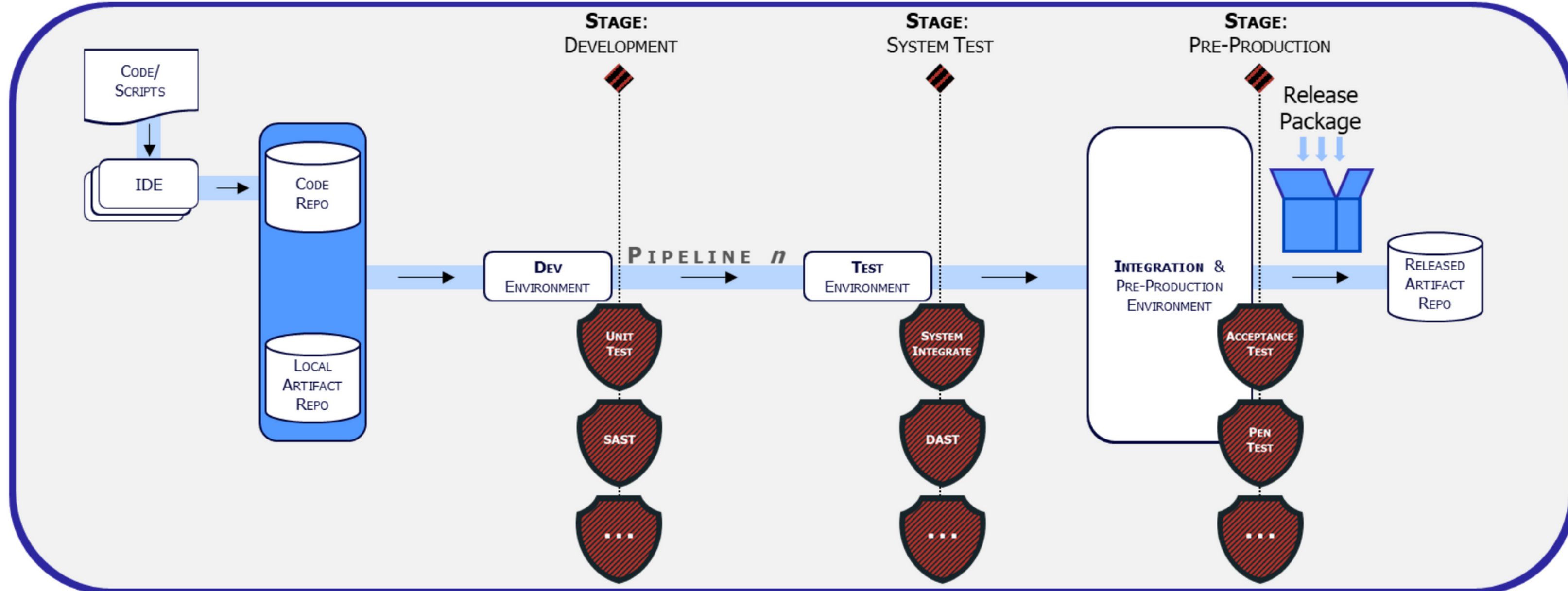


Figure 7 Notional expansion of a single DevSecOps software factory Pipeline

DevSecOps

DevSecOps Lifecycle

- DoD model
- Security at every stage
- Comprehensive code lifecycle

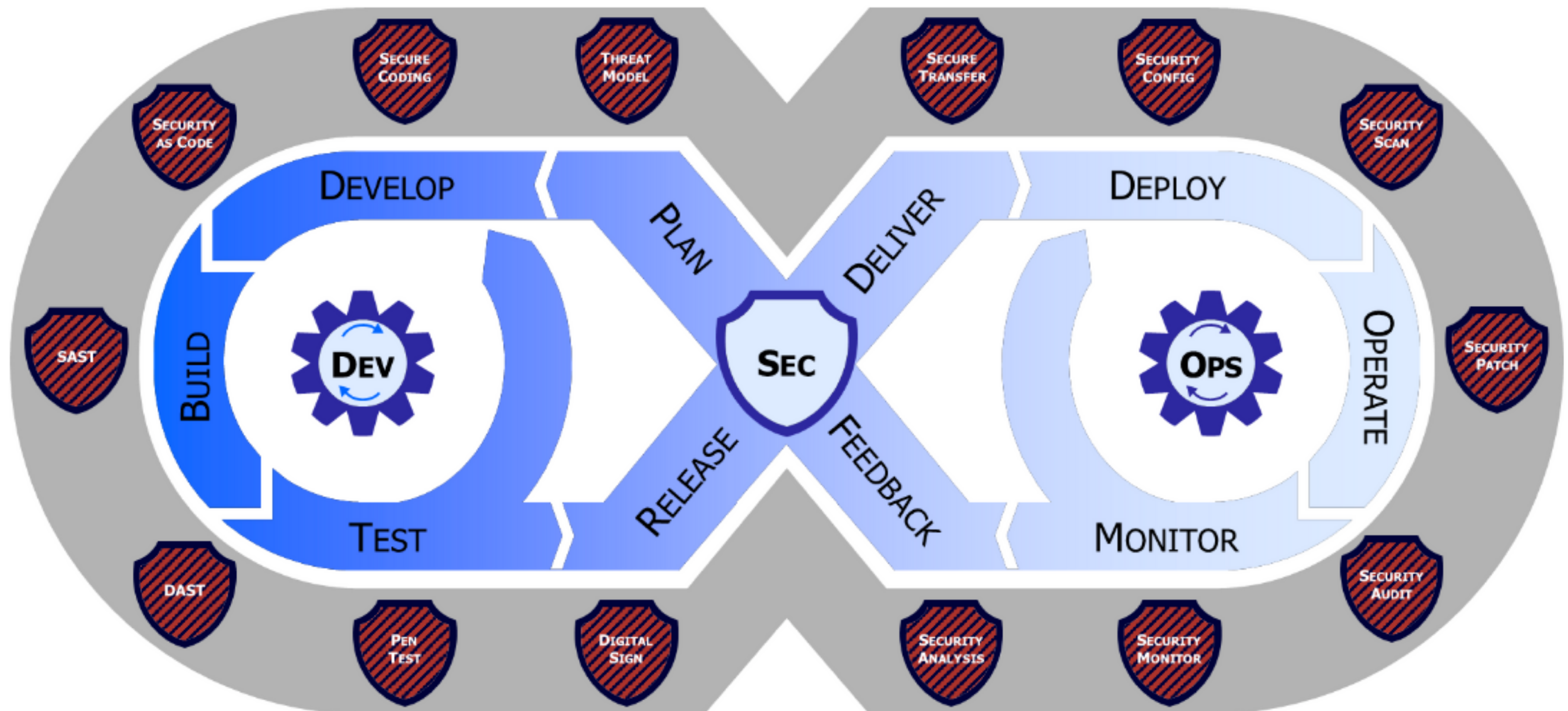


Figure 3 DevSecOps Distinct Lifecycle Phases and Philosophies

Technology

API Sec at arrows

DoD DevSecOps Security Strategy

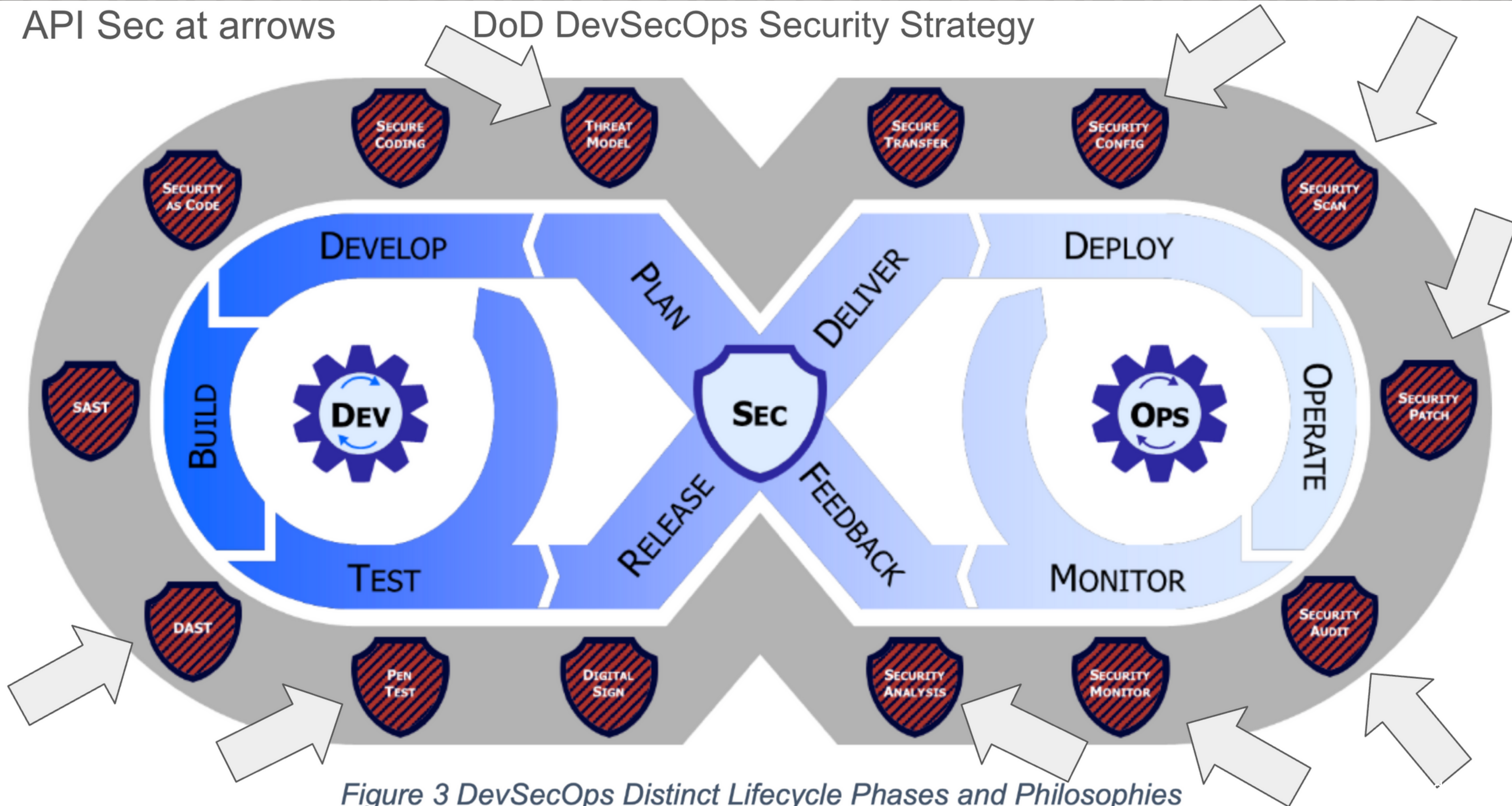


Figure 3 DevSecOps Distinct Lifecycle Phases and Philosophies

Technology

DoD DevSecOps Security Strategy

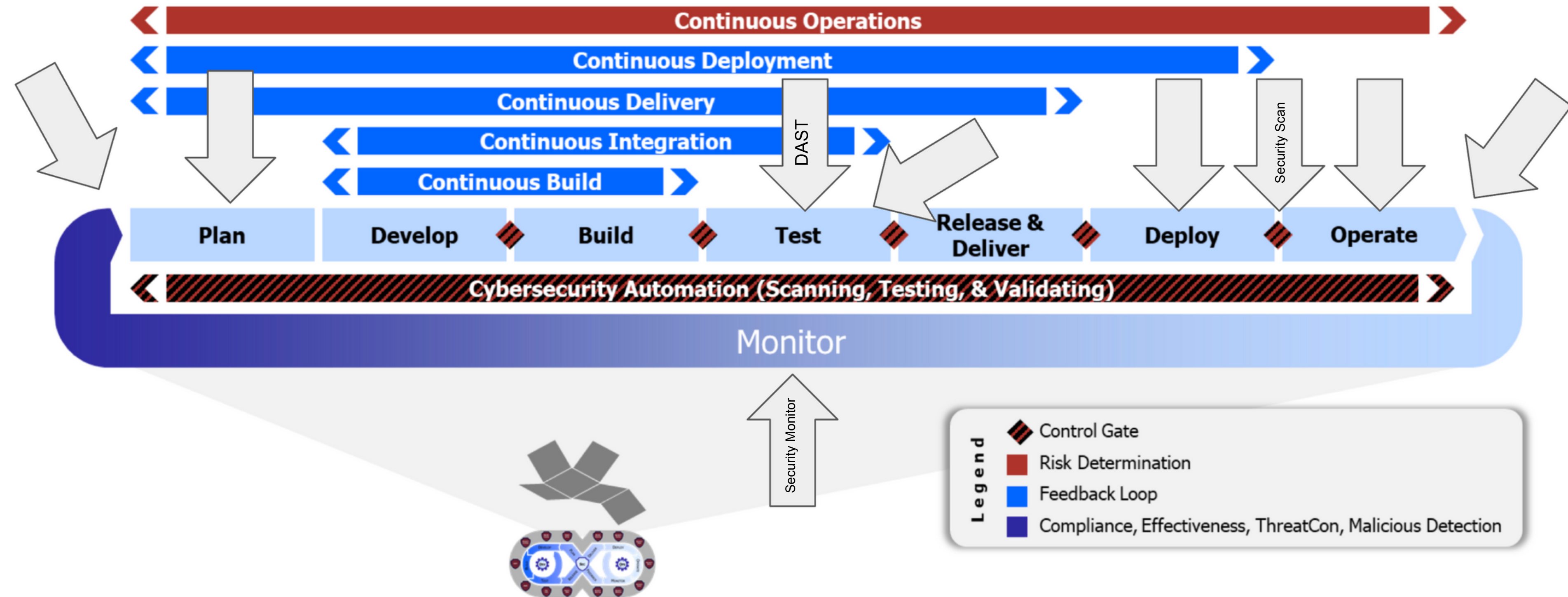


Figure 6 DevSecOps Lifecycle Phases, Continuous Feedback Loops, & Control Gates

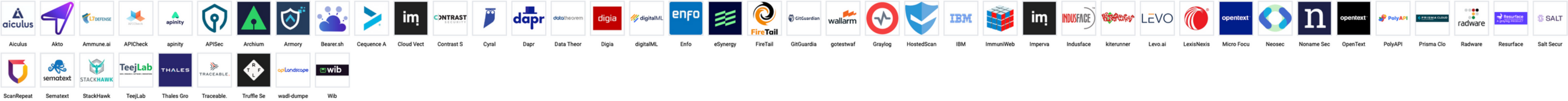


Thanks to our sponsor **boomi**

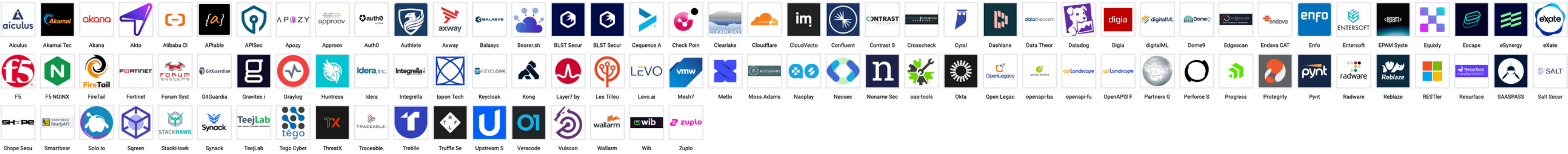


Security Pureplay ?

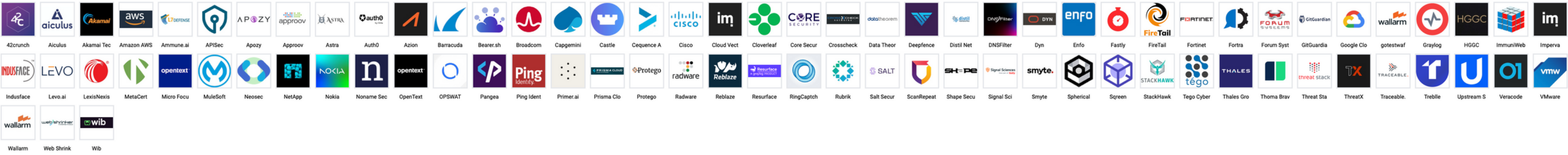
API Discovery & Risk management (49) ?



API Security (98) ?



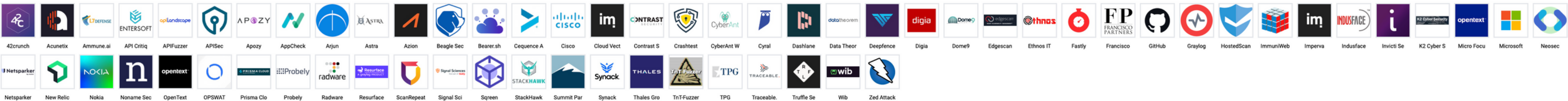
API Threat Management (83) ?



Privacy Technology (14) ?



Vulnerability Management (63) ?



Technology

OWASP API Security Tools List

https://owasp.org/www-community/api_security_tools

Summary

56 tools

36 Commercial

13 Posture (1 w/o Runtime)

13 Runtime (1 w/o Posture)

35 Testing (22 w/o RT/P)

20 Open Source

1 Posture (w/ Testing)

1 Runtime (w/o Testing)

19 Testing (1 w/ Posture)

Technology

root

Inventory

StatsAPIsChangesDatatypesInfrastructure

All APIs

Search APIs

Drag here to set row groups

Host	Path	Method	Risk	Auth	Internet Facing	Finding	Incidents	Lea
apis-ist.demo.com	/assets-locator/v1/search/branch/id	GET	5.3	header.x-api-key	Not Connected		None	
apis-ist.demo.com	/assets-locator/v1/search/Best/id	GET	5.3	header.x-api-key	Not Connected		None	
vampi.demos.commercesolutions.com:5002	/books/v1	POST	2	header.authorization.sub: JWT	HTTP			
vampi.demos.commercesolutions.com:5002	/users/v1/login	POST	4.7	body.password	HTTP	None		
vampi.demos.commercesolutions.com:5002	/users/v1/<alphanumeric>{5}/password	PUT	4.4	body.auth_token +2	HTTP	None		
vampi.demos.commercesolutions.com:5002	/users/v1/<alphanumeric>{5}/email	PUT	4.4	body.auth_token +2	HTTP	None		
vampi.demos.commercesolutions.com:5002	/users/v1/<alphanumeric>{5}	DELETE	2.1	header.authorization.sub: JWT	HTTP	None		
vampi.demos.commercesolutions.com:5002	/books/v1	GET	1.4	Not Enforced	HTTP	None	None	
ec2-3-137-177-49.us-east-2.compute.amazonaws.com:5002	/users/v1/login	POST	3.8	body.password	HTTP	None	None	
vampi.demos.commercesolutions.com:5002	/users/v1	GET	5.7	Not Enforced	HTTP	None	None	

Technology

Security Findings Detail

- Vulnerability enumeration
- What to do and why
- Evidence available

An API Accepts Expired JWT

Detection Time: 2024-08-12 08:31



Evidence

Take Action

Status
Open

What Happened

API was observed accepting JWT Token with the following expiration time:

- Request Timestamp: 2024-08-12 08:30,2024-08-12 08:30,2024-08-12 08:30,2024-08-12 08:30,2024-08-12 08:30,2024-08-12 08:30
- JWT Expiration Time: 2024-08-12 08:18,2024-08-12 08:18,2024-08-12 08:18

Why That's a Problem

By bypassing the API's authentication mechanism, attackers can gain control over other user's accounts, access their data, and perform sensitive actions on their behalf. A broken authentication mechanism is a critical risk to your organization's security.

What You Should Do

- In "Evidence", validate the issue.
- Open a critical priority ticket on the API Developer to fix the APIs authentication validation. The fix should be deployed as soon as possible.
- Block the attacker.

How To Investigate

Severity

Medium

Module

Posture

OWASP

API2:2023

+3

Response Codes

200

Technology

⋮

Drag here to set row groups

Severity	Type	Detection Time	Last Activity	Last Updated	Triggered On	Status	Incident Result	Actions
Info	API Input Validation Attack	2024-08-12 08:32	2024-08-12 08:32	2024-08-12 08:32	POST vampi.demos.commercesoluti	Open	🛡️	View Attacker
Low	API Access Attempt With Missing JWT Algorithm	2024-08-12 08:31	2024-08-12 08:31	2024-08-12 08:32	POST vampi.demos.commercesoluti	Open	🛡️	View Attacker
Low	API Access Attempt With Missing JWT Algorithm	2024-08-12 08:31	2024-08-12 08:31	2024-08-12 08:32	PUT vampi.demos.commercesolutio	Open	🛡️	View Attacker
Low	API Access Attempt With Missing JWT Algorithm	2024-08-12 08:31	2024-08-12 08:31	2024-08-12 08:32	PUT vampi.demos.commercesolutio	Open	🛡️	View Attacker
Low	API Access Attempt With Missing JWT Algorithm	2024-08-12 08:31	2024-08-12 08:31	2024-08-12 08:32	PUT vampi.demos.commercesolutio	Open	🛡️	View Attacker
Low	API Access Attempt With Missing JWT Algorithm	2024-08-12 08:31	2024-08-12 08:31	2024-08-12 08:32	GET vampi.demos.commercesolutio	Open	🛡️	View Attacker
Low	API Access Attempt With Missing JWT Algorithm	2024-08-12 08:31	2024-08-12 08:31	2024-08-12 08:32	POST vampi.demos.commercesoluti	Open	🛡️	View Attacker
Low	API Access Attempt With Missing JWT Algorithm	2024-08-12 08:31	2024-08-12 08:31	2024-08-12 08:32	GET vampi.demos.commercesolutio	Open	🛡️	View Attacker
Info	API Input Validation Attack	2024-08-12 08:31	2024-08-12 08:31	2024-08-12 08:31	POST vampi.demos.commercesoluti	Open	🛡️	View Attacker
Low	API Access Attempt With Missing JWT Algorithm	2024-08-12 08:31	2024-08-12 08:31	2024-08-12 08:31	PUT vampi.demos.commercesolutio	Open	🛡️	View Attacker

Columns

Filters

Technology

Unidentified

6 Attackers

Confidence

Search

IP: 172.31.17.121

Info

Not Active

2 weeks ago

98%

IP: 172.31.29.31

Info

Not Active

2 weeks ago

98%

JWT: admin

Low

Not Active

2 weeks ago

94%

JWT: name1

Low

Not Active

1 month ago

88%

JWT: name2

Low

Not Active

1 month ago

81%

IP: 172.31.26.160

Info

Not Active

Attacker Information						Block		Allow List		Unidentified	Search	
Confidence ⓘ	Risk ⓘ	Country	IPs	IP Reputation ⓘ	User Agents							
88%	Low	None	172.31.17.121	N/A	noname							
Last Activity ↓	Incident	Severity	Triggered On		Actions							
2024-08-12 08:32	API Input Validation Attack Inconclusive	Info	/users/v1/<alphanumeric>{5}/email PUT vampi.demos.commercesolutions.com:5000		Evidence							
2024-08-12 08:32	API Input Validation Attack Inconclusive	Info	/books/v1 POST vampi.demos.commercesolutions.com:5000		Evidence							
2024-08-12 08:31	API Access Attempt With Missin Attempted	Low	/users/v1/<alphanumeric>{5}/email PUT vampi.demos.commercesolutions.com:5000		Evidence							
2024-08-12 08:31	API Access Attempt With Missin Attempted	Low	/books/v1/<alphanumeric>{6} GET vampi.demos.commercesolutions.com:5000		Evidence							
2024-08-12 08:31	API Access Attempt With Missin Attempted	Low	/books/v1 POST vampi.demos.commercesolutions.com:5000		Evidence							
2024-08-12 08:31	API Access Attempt With Missin Attempted	Low	/users/v1/<alphanumeric>{5}/password PUT vampi.demos.commercesolutions.com:5000		Evidence							

Processes

DoD DevSecOps Security Strategy

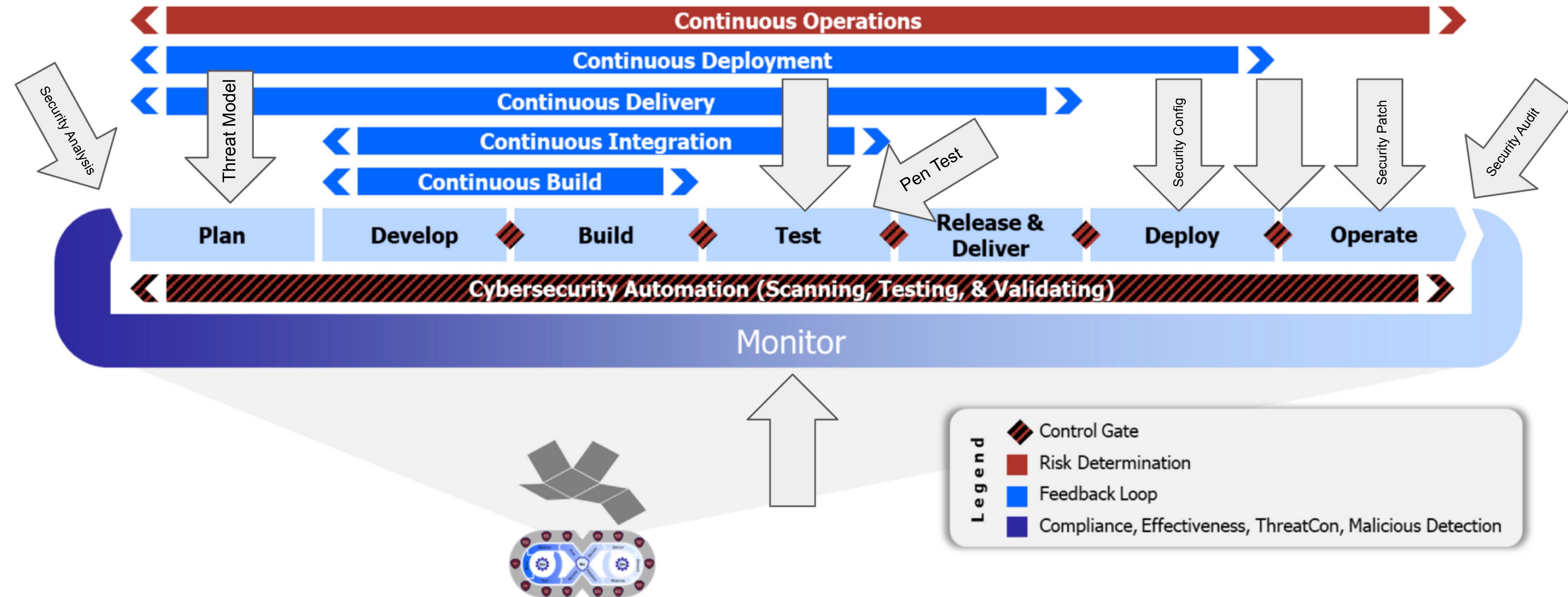


Figure 6 DevSecOps Lifecycle Phases, Continuous Feedback Loops, & Control Gates

People

- Break down silos
- DevSecOps Center of Excellence
- Share best practices
- Technical trainings
- Social events
- **Cross-Incentivize**



Q&A

Thank you!

Contact me at
sbly@sisinc.com

LinkedIn
<https://linkedin.com/in/blyscott>



Talent · Technology · Partners