Adding API Security to your DevSecOps Toolbelt

Location
Date

iSOA | GROUP

Building the Foundation for Digital Innovation

Agenda

- Introduction
- Why API Security
- DevOps vs DevSecOps
- Technology
- Processes
- People
- Contact

Introduction

iSOA Group API Security

Scott Bly

Director, API Security Practice

sbly@isoagroup.com

IBM Silver Partner

Noname/Akamai Partner

Background

Noname Security

AWS

CyberSecurity Solutions Architect

Director IT, Cyber

IT/Cyber Consultant 15+ years

Why API Security

- DevOps success
- Increased vulnerability
- Data is the new GOLD
- 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
- Infra as Code
- Predictable results

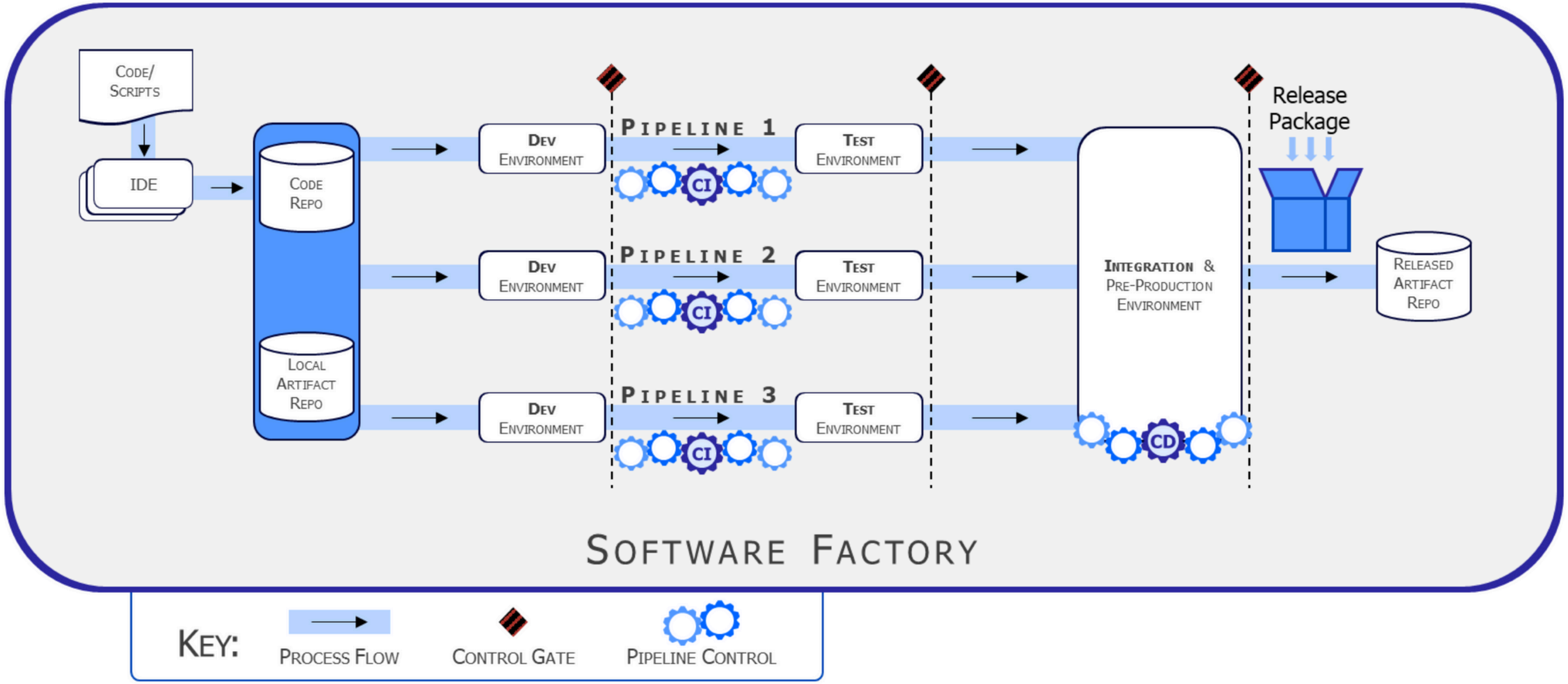


Figure 5 Normative Software Factory Construct

DevSecOps

DevSecOps Software Factory

- Shift Left
- Testing built into stages
- Not enough

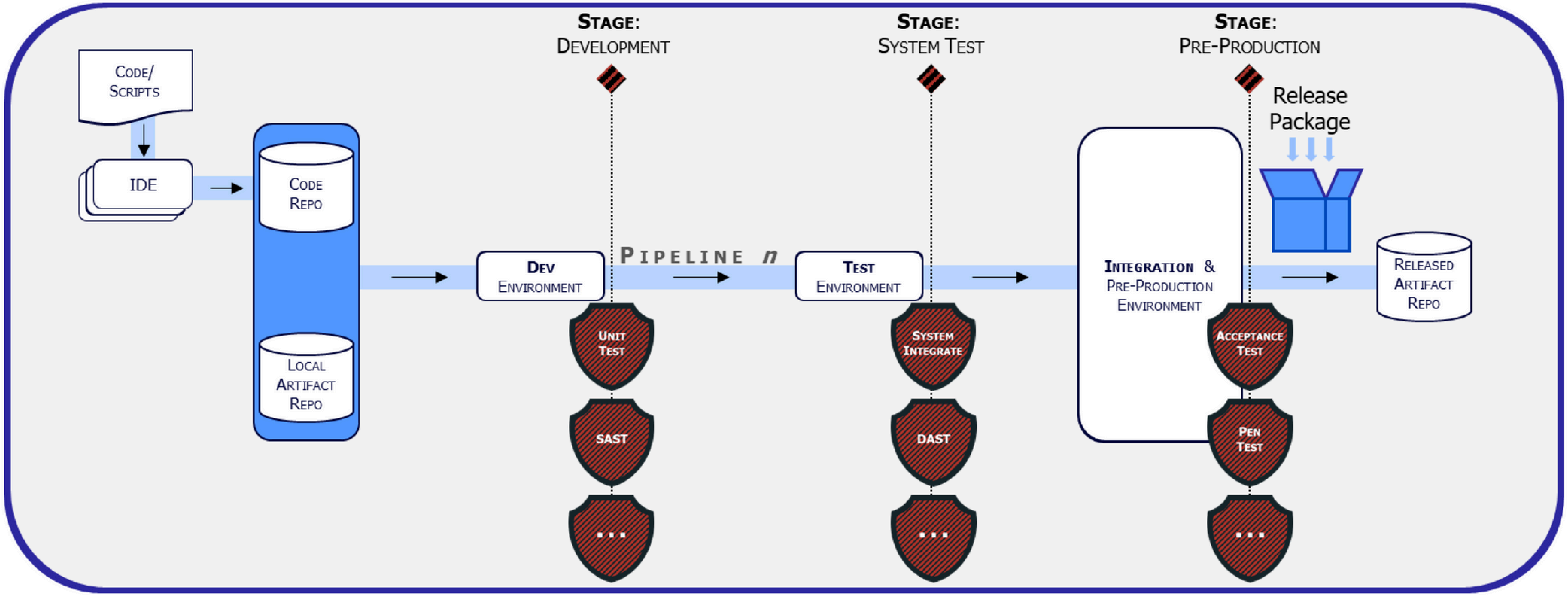


Figure 7 Notional expansion of a single DevSecOps software factory Pipeline

DevSecOps

DevSecOps Lifecycle

- DoD model
- Security at every stage
- Compre-hensive code lifecycle

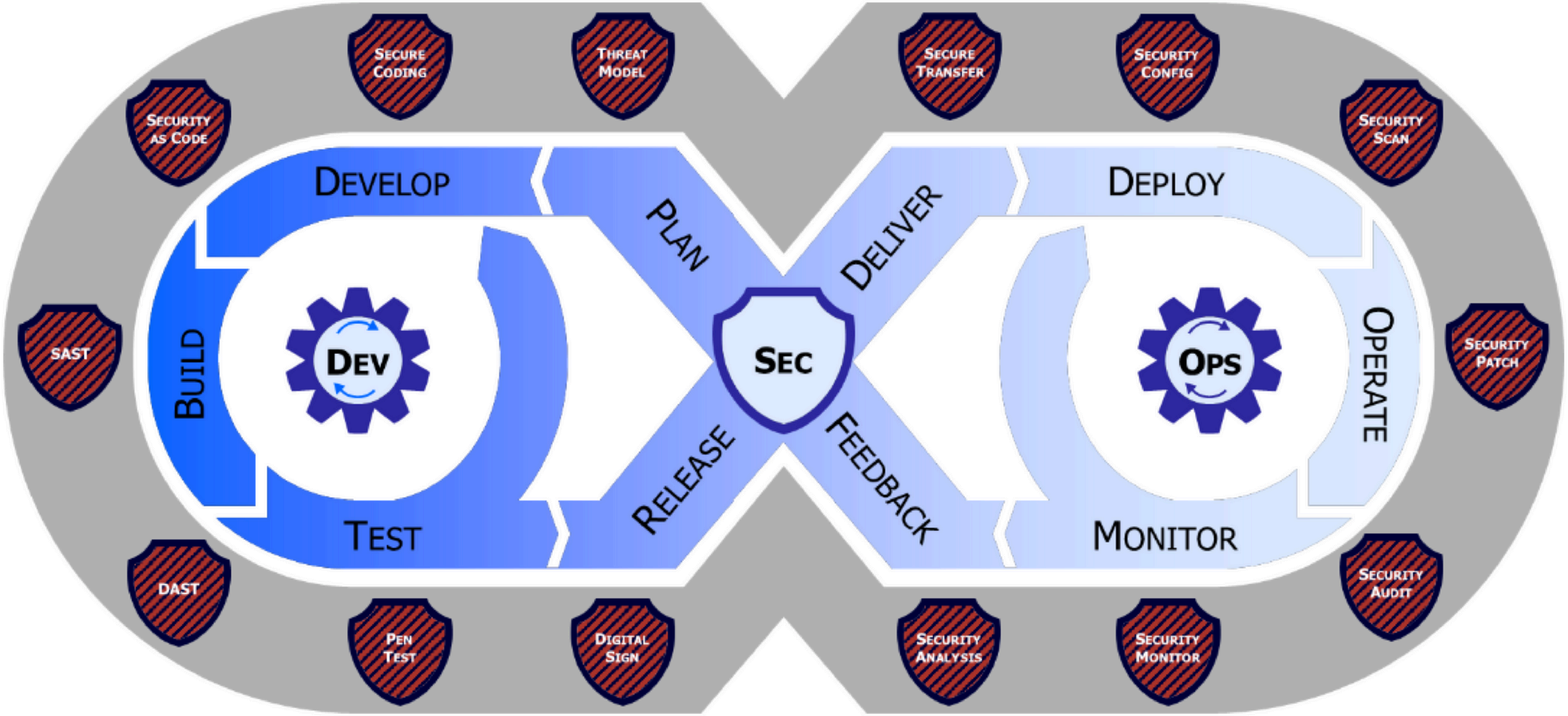


Figure 3 DevSecOps Distinct Lifecycle Phases and Philosophies

API Sec at arrows

DoD DevSecOps Security Strategy

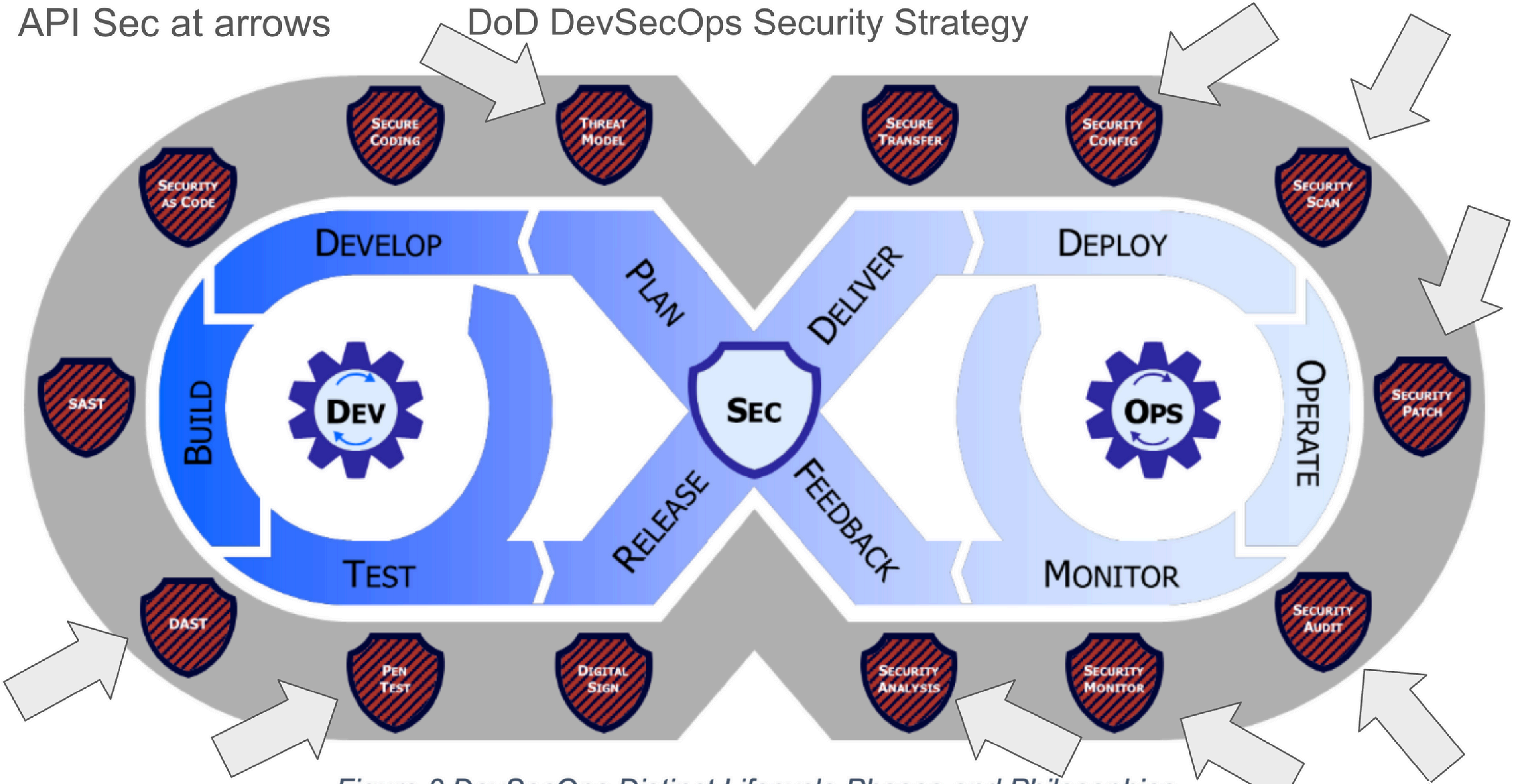


Figure 3 DevSecOps Distinct Lifecycle Phases and Philosophies

Technology

DoD DevSecOps Security Strategy

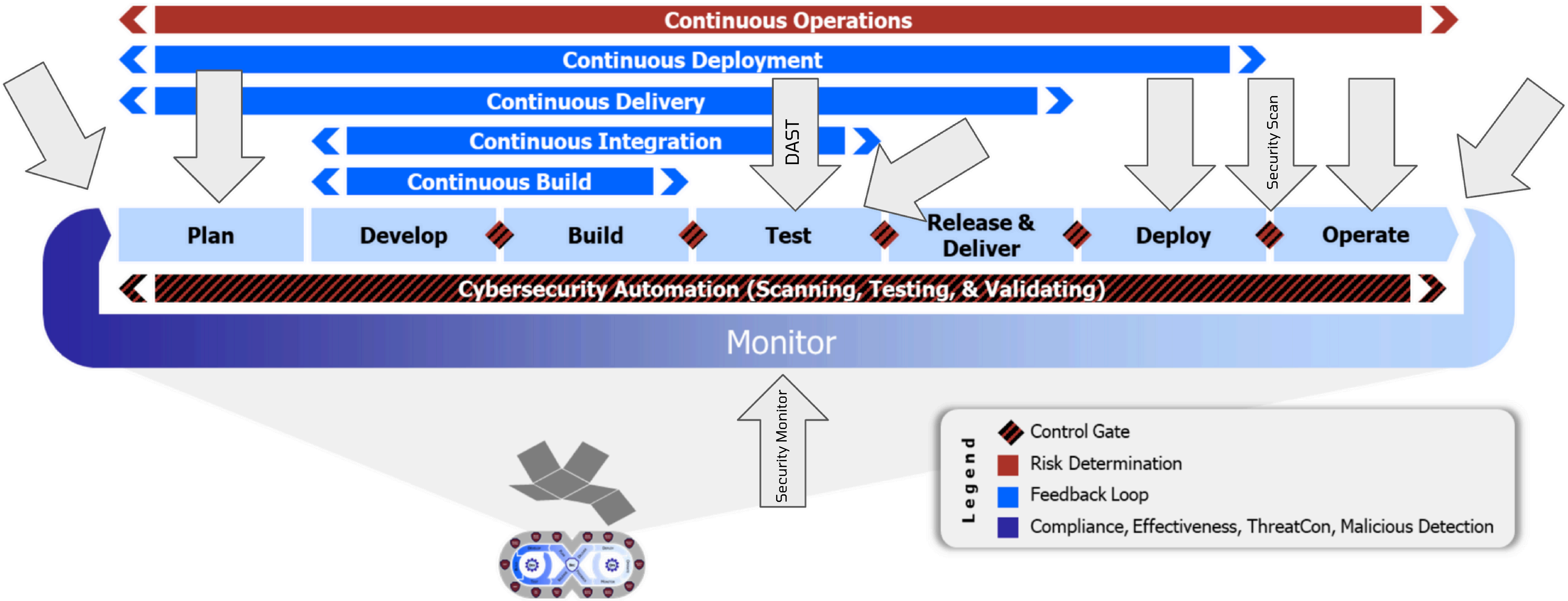
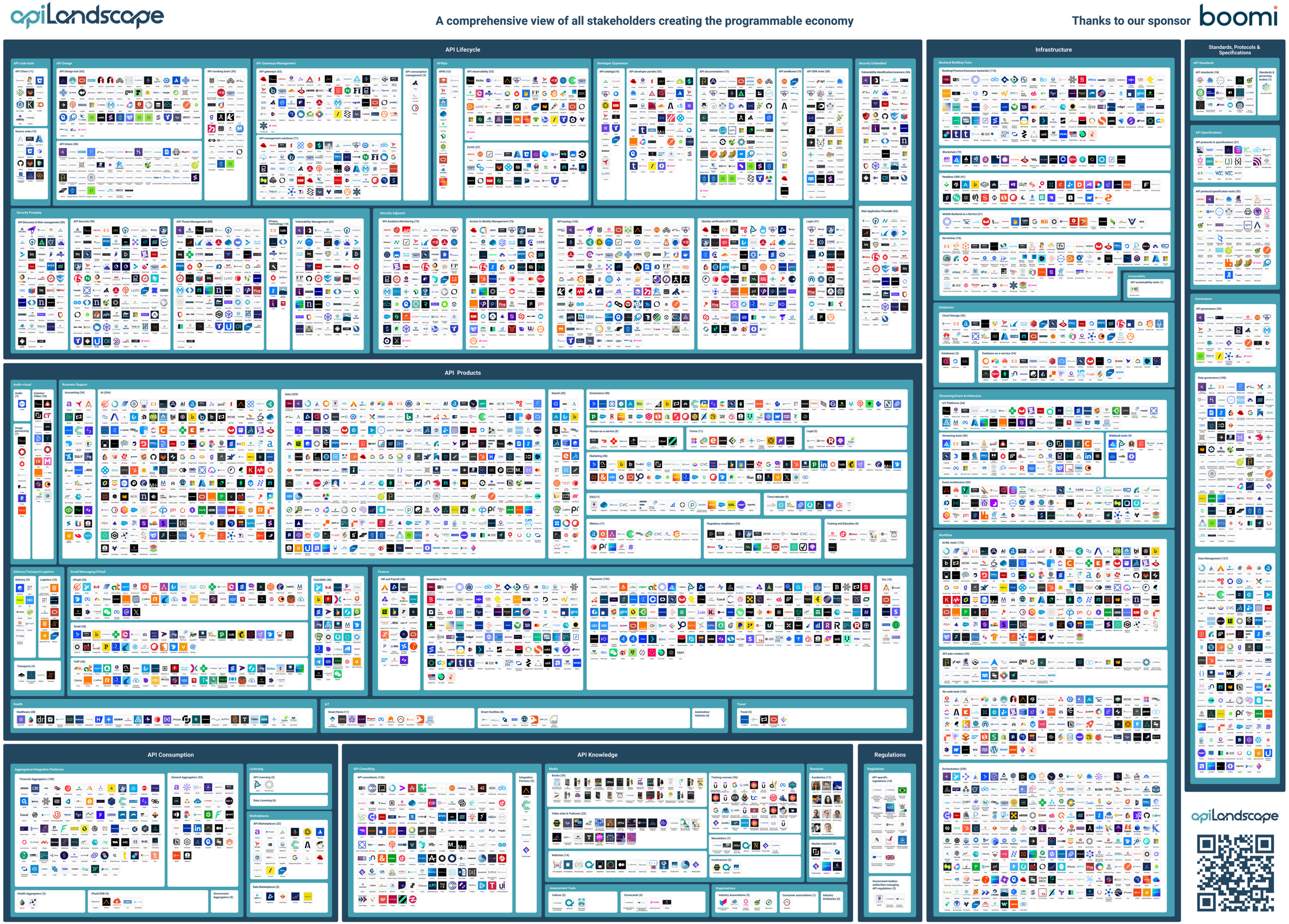


Figure 6 DevSecOps Lifecycle Phases, Continuous Feedback Loops, & Control Gates

Technology

Behold the API Landscape


apiLandscape
A comprehensive view of all stakeholders creating the programmable economy
Thanks to our sponsor boomi
API Lifecycle
Infrastructure
Standards, Protocols & Specifications
API Products
API Consumption
API Knowledge
Regulations
apiLandscape

Security Pureplay ?

API Discovery & Risk management (49) ?

- Aiculus
- Akto
- Ammune.ai
- APICheck
- apinity
- APISec
- Archium
- Armory
- Bearer.sh
- Cequence A
- Cloud Vect
- Contrast S
- Cyral
- Dapr
- Data Theor
- Digia
- digitalML
- Enfo
- eSynergy
- FireTail
- GitGuardia
- gotestwaf
- Graylog
- HostedScan
- IBM
- ImmuniWeb
- Imperva
- Indusface
- kiterunner
- Levo.ai
- LexisNexis
- Micro Focu
- Neosec
- Noname Sec
- OpenText
- PolyAPI
- Prisma Clo
- Radware
- Resurface
- Salt Secur
- ScanRepeat
- Sematext
- StackHawk
- TeejLab
- Thales Gro
- Traceable.
- Truffle Se
- wadl-dumpe
- Wib

API Security (98) ?

- Aiculus
- Akamai Tec
- Akana
- Akto
- Alibaba Cl
- APIable
- APISec
- Apozy
- Approov
- Auth0
- Authlete
- Axway
- Balasys
- Bearer.sh
- BLST Secur
- BLST Secur
- Cequence A
- Check Poin
- Clearlake
- Cloudflare
- CloudVecto
- Confluent
- Contrast S
- Crosscheck
- Cyral
- Dashlane
- Data Theor
- Datadog
- Digia
- digitalML
- Dome9
- Edgescan
- Endava CAT
- Enfo
- Entersoft
- EPAM Syste
- Equixly
- Escape
- eSynergy
- eXate
- F5
- F5 NGINX
- FireTail
- Fortinet
- Forum Syst
- GitGuardia
- Gravitee.i
- Graylog
- Huntress
- Idera
- Integrella
- Ippon Tech
- Keycloak
- Kong
- Layer7 by
- Les Tilleu
- Levo.ai
- Mesh7
- Metlo
- Moss Adams
- Naoplay
- Neosec
- Noname Sec
- oas-tools
- Okta
- Open Legac
- openapi-ba
- openapi-fu
- OpenAPI3 F
- Partners G
- Perforce S
- Progress
- Protegrity
- Pynt
- Radware
- Reblaze
- RESTler
- Resurface
- SAASPASS
- Salt Secur
- Shape Secu
- Smartbear
- Solo.io
- Sqreen
- StackHawk
- Synack
- TeejLab
- Tego Cyber
- ThreatX
- Traceable.
- Treblle
- Truffle Se
- Upstream S
- Veracode
- Vulscan
- Wallarm
- Wib
- Zuplo

API Threat Management (83) ?

- 42crunch
- Aiculus
- Akamai Tec
- Amazon AWS
- Ammune.ai
- APISec
- Apozy
- Approov
- Astra
- Auth0
- Azion
- Barracuda
- Bearer.sh
- Broadcom
- Capgemini
- Castle
- Cequence A
- Cisco
- Cloud Vect
- Cloverleaf
- Core Secur
- Crosscheck
- Data Theor
- Deepfence
- Distil Net
- DNSFilter
- Dyn
- Enfo
- Fastly
- FireTail
- Fortinet
- Fortra
- Forum Syst
- GitGuardia
- Google Clo
- gotestwaf
- Graylog
- HGGC
- ImmuniWeb
- Imperva
- Indusface
- Levo.ai
- LexisNexis
- MetaCert
- Micro Focu
- MuleSoft
- Neosec
- NetApp
- Nokia
- Noname Sec
- OpenText
- OPSWAT
- Pangea
- Ping Ident
- Primer.ai
- Prisma Clo
- Protego
- Radware
- Reblaze
- Resurface
- RingCaptch
- Rubrik
- Salt Secur
- ScanRepeat
- Shape Secu
- Signal Sci
- Smyte
- Spherical
- Sqreen
- StackHawk
- Tego Cyber
- Thales Gro
- Thoma Brav
- Threat Sta
- ThreatX
- Traceable.
- Treblle
- Upstream S
- Veracode
- VMware
- Wallarm
- Web Shrink
- Wib

Privacy Technology (14) ?

- Alibaba Cl
- CyberArk
- Dapr
- EnvKey
- Fastly
- Fivetran
- Invicti Se
- Lob
- Neosec
- Olympe Leg
- Salt Secur
- Skyflow
- Summit Par
- Tanla

Vulnerability Management (63) ?

- 42crunch
- Acunetix
- Ammune.ai
- API Critiq
- APIFuzzer
- APISec
- Apozy
- AppCheck
- Arjun
- Astra
- Azion
- Beagle Sec
- Bearer.sh
- Cequence A
- Cisco
- Cloud Vect
- Contrast S
- Crashtest
- CyberAnt W
- Cyral
- Dashlane
- Data Theor
- Deepfence
- Digia
- Dome9
- Edgescan
- Ethnos IT
- Fastly
- Francisco
- GitHub
- Graylog
- HostedScan
- ImmuniWeb
- Imperva
- Indusface
- Invicti Se
- K2 Cyber S
- Micro Focu
- Microsoft
- Neosec
- Netsparker
- New Relic
- Nokia
- Noname Sec
- OpenText
- OPSWAT
- Prisma Clo
- Probely
- Radware
- Resurface
- ScanRepeat
- Signal Sci
- Sqreen
- StackHawk
- Summit Par
- Synack
- Thales Gro
- TnT-Fuzzer
- TPG
- Traceable.
- Truffle Se
- Wib
- Zed Attack

Technology

OWASP API Security Tools List
https://owasp.org/www-community/api_security_tools

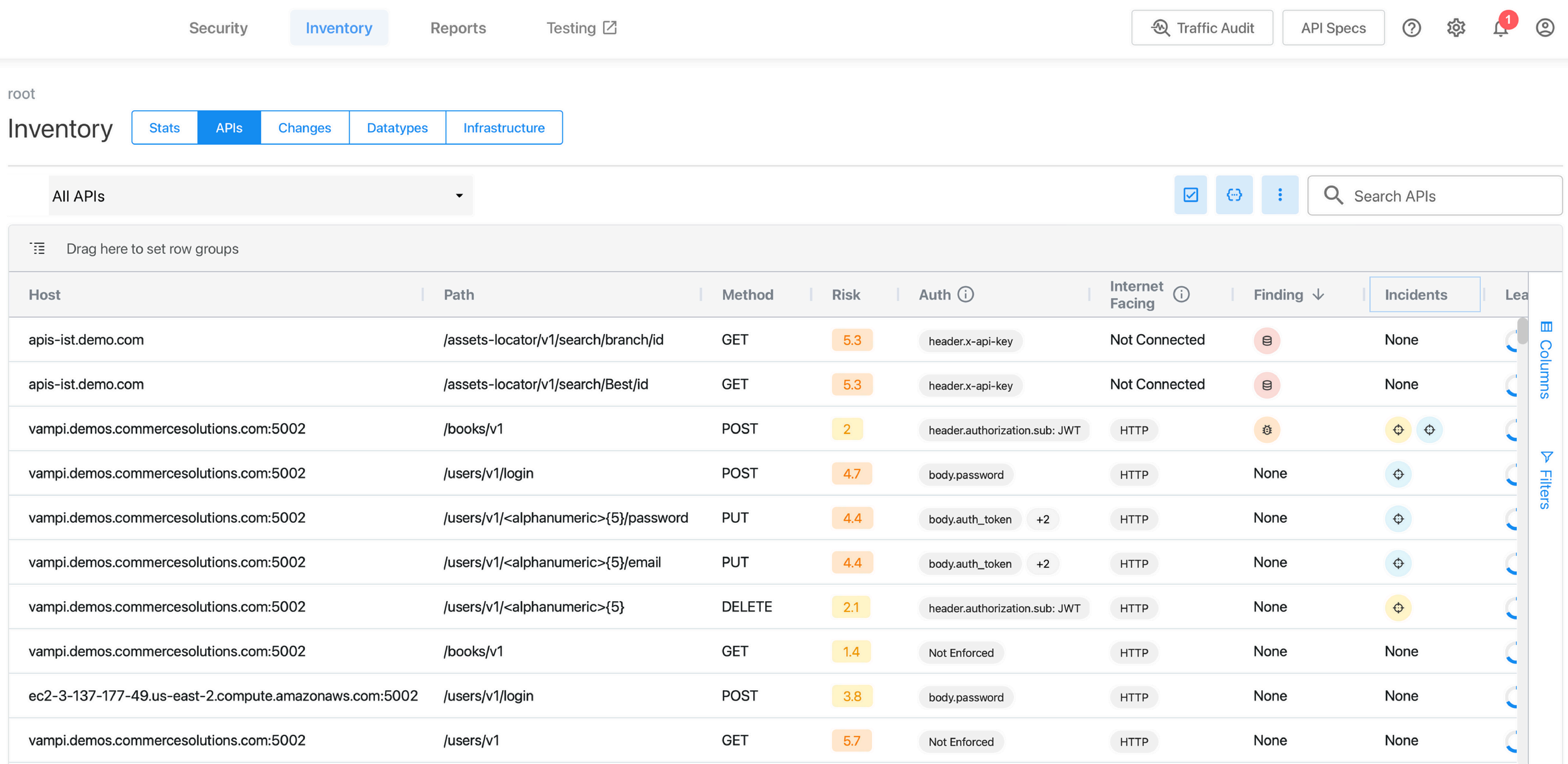
Summary

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



Security | Inventory | Reports | Testing

Traffic Audit | API Specs

root

Inventory

Stats | APIs | Changes | Datatypes | Infrastructure

All APIs

Search APIs

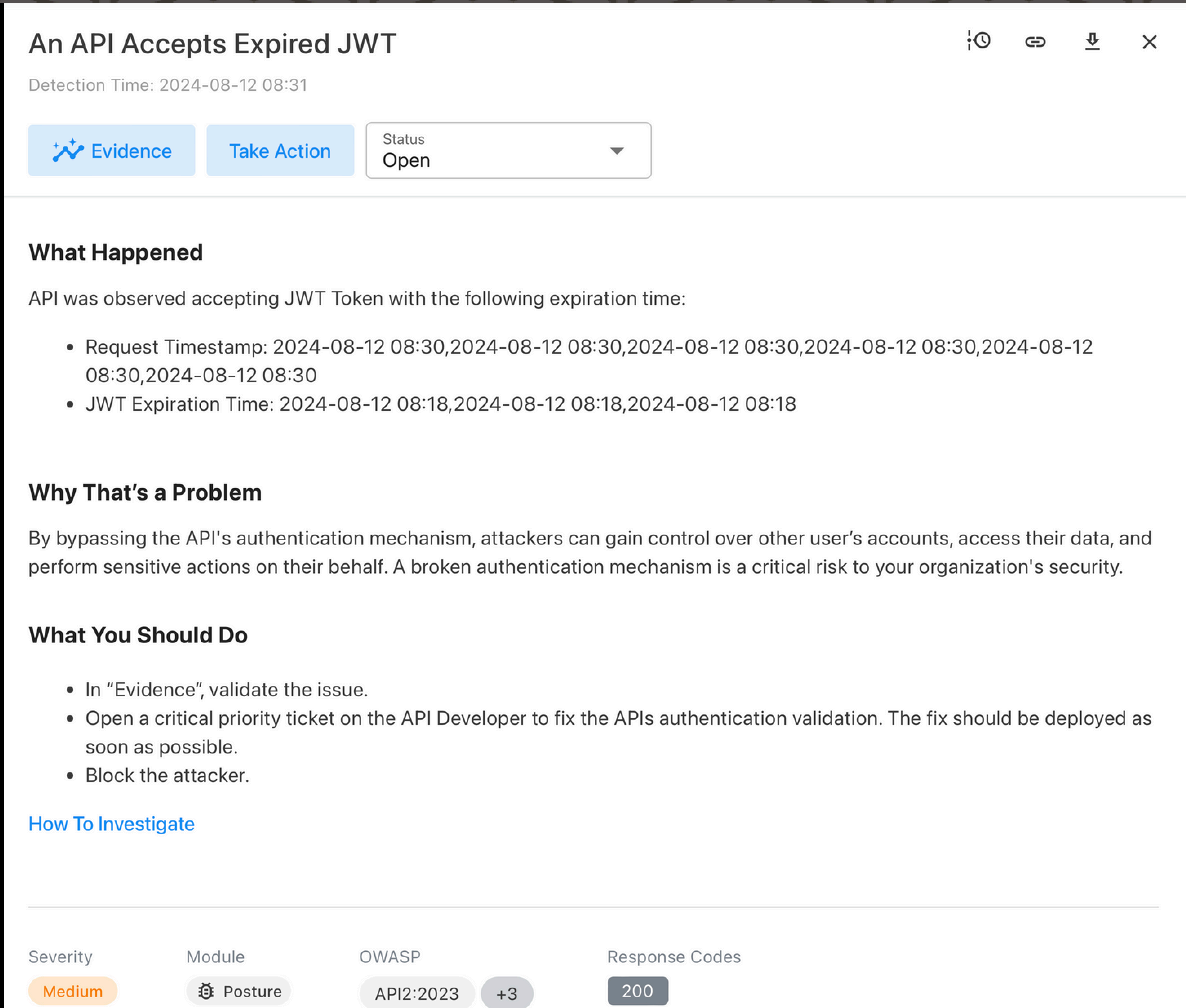
Drag here to set row groups

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

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.

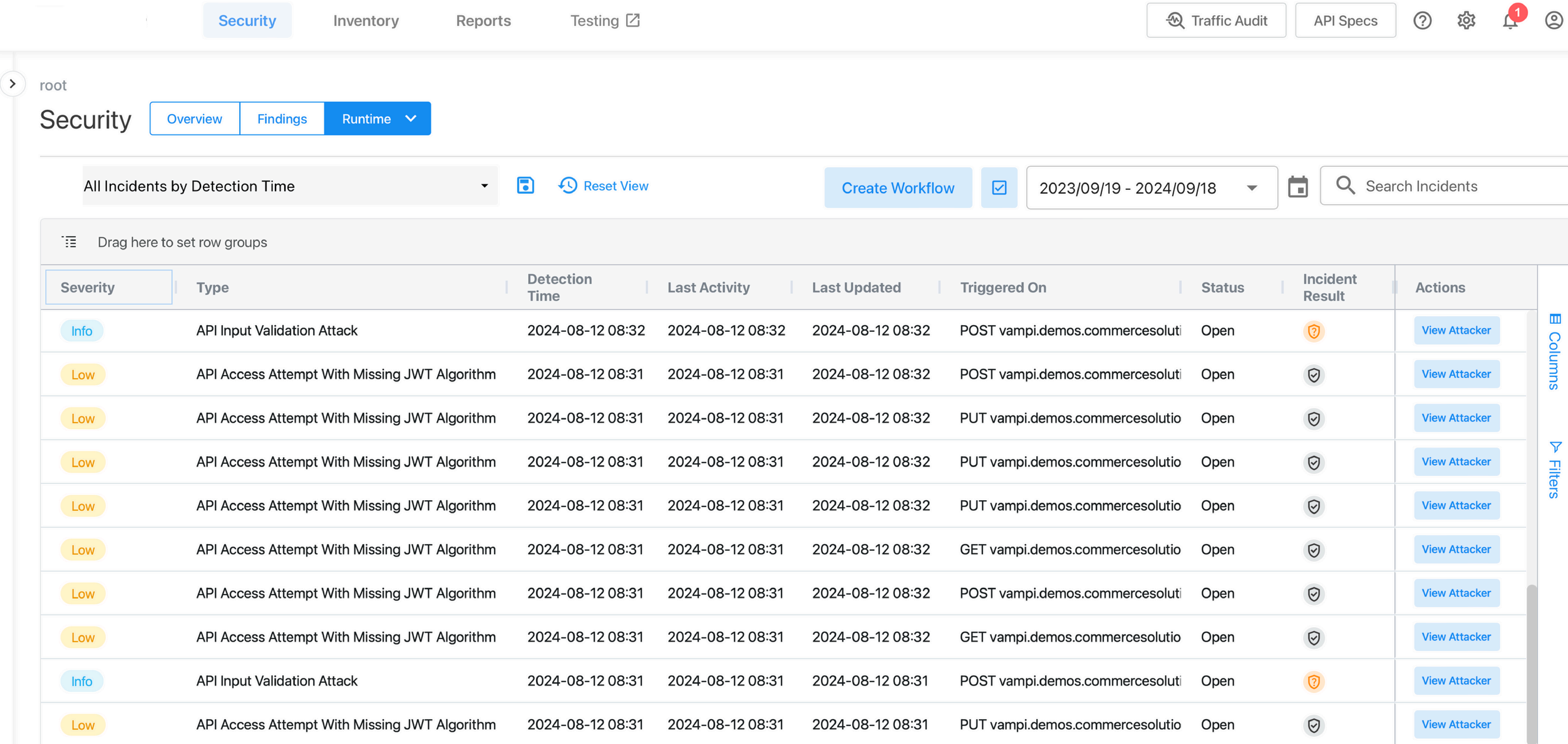
What You Should Do

- 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	Module	OWASP	Response Codes
Medium	Posture	API2:2023 +3	200

Technology

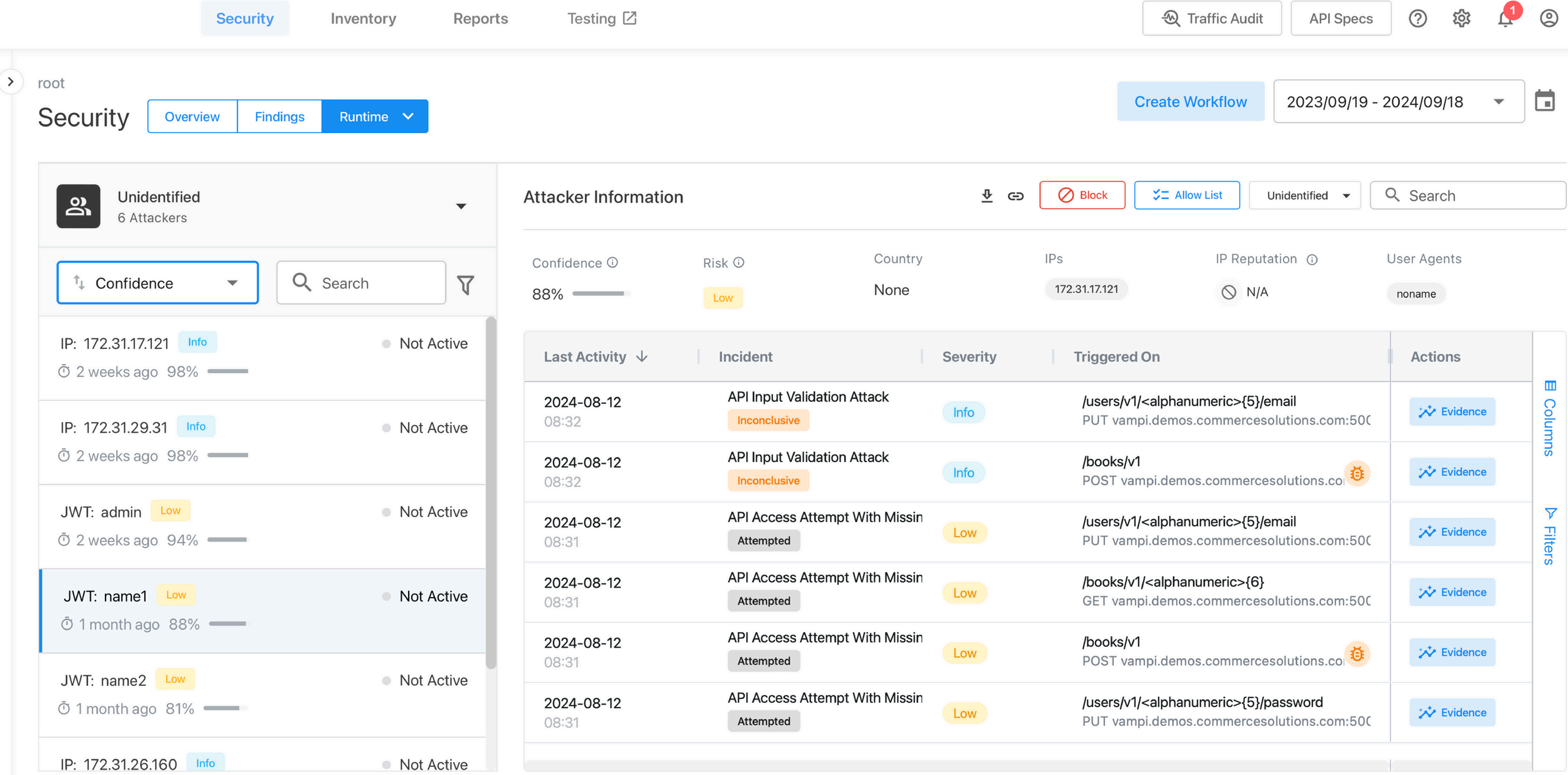


All Incidents by Detection Time

2023/09/19 - 2024/09/18

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

Technology



Security | Inventory | Reports | Testing | Traffic Audit | API Specs

root

Security

Overview | Findings | Runtime

Create Workflow

2023/09/19 - 2024/09/18

Unidentified
6 Attackers

Confidence | Search

IP: 172.31.17.121 Info	2 weeks ago 98%	Not Active
IP: 172.31.29.31 Info	2 weeks ago 98%	Not Active
JWT: admin Low	2 weeks ago 94%	Not Active
JWT: name1 Low	1 month ago 88%	Not Active
JWT: name2 Low	1 month ago 81%	Not Active
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:50(	Evidence
2024-08-12 08:32	API Input Validation Attack Inconclusive	Info	/books/v1 POST vampi.demos.commercesolutions.co	Evidence
2024-08-12 08:31	API Access Attempt With Missin Attempted	Low	/users/v1/<alphanumeric>{5}/email PUT vampi.demos.commercesolutions.com:50(	Evidence
2024-08-12 08:31	API Access Attempt With Missin Attempted	Low	/books/v1/<alphanumeric>{6} GET vampi.demos.commercesolutions.com:50(	Evidence
2024-08-12 08:31	API Access Attempt With Missin Attempted	Low	/books/v1 POST vampi.demos.commercesolutions.co	Evidence
2024-08-12 08:31	API Access Attempt With Missin Attempted	Low	/users/v1/<alphanumeric>{5}/password PUT vampi.demos.commercesolutions.com:50(	Evidence

Processes

DoD DevSecOps Security Strategy

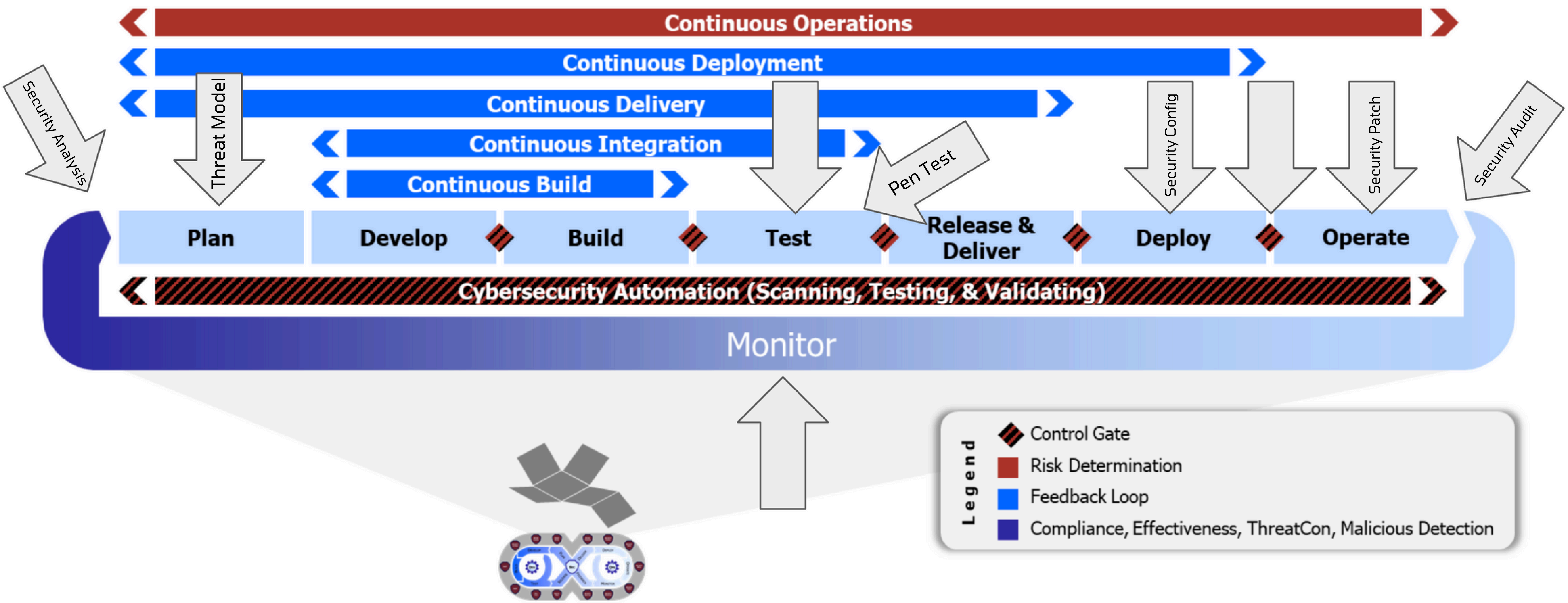


Figure 6 DevSecOps Lifecycle Phases, Continuous Feedback Loops, & Control Gates

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@isoagroup.com

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

iSOA | GROUP

Building the Foundation for Digital Innovation