

Releasing secure software at the speed of DevOps

Mid-Atlantic CIO Forum
November 2022



Jason Ostroski
Principal Solutions Engineer





What am I going to learn?

- How DevOps and cloud-native trends are affecting security practices
- What observability is and how we can leverage observability data for application security and risk prioritization
- How runtime application security reduces vulnerability blindspots, even in production
- How to track and speed up the remediation of vulnerabilities
- How to increase DevSecOps collaboration

Every business is undergoing a digital transformation



RETAIL

GOVERNMENT

MANUFACTURING

TRAVEL

HEALTHCARE

FINANCE

DevOps practices and cloud native platforms enable releasing software at remarkable speeds



Securing cloud-native applications has never been harder

75%

CISOs worried about application vulnerabilities leak into production

67%

CISOs that say dev does not have time to scan and fix vulnerabilities

50

Open-source vulnerabilities in average Java application

80

Average number of days to fix a high-risk application vulnerability



Cloud applications face evolving runtime security threats



Constant new threats

- New code vulnerabilities constantly being discovered and exploited
- Critical OSS and custom code vulnerabilities frequently escape into production



Dev, Sec, Ops in silos

- Security and Development teams lack collaboration, with practices and tooling
- Unreliable prioritization using different datasets that lack runtime context

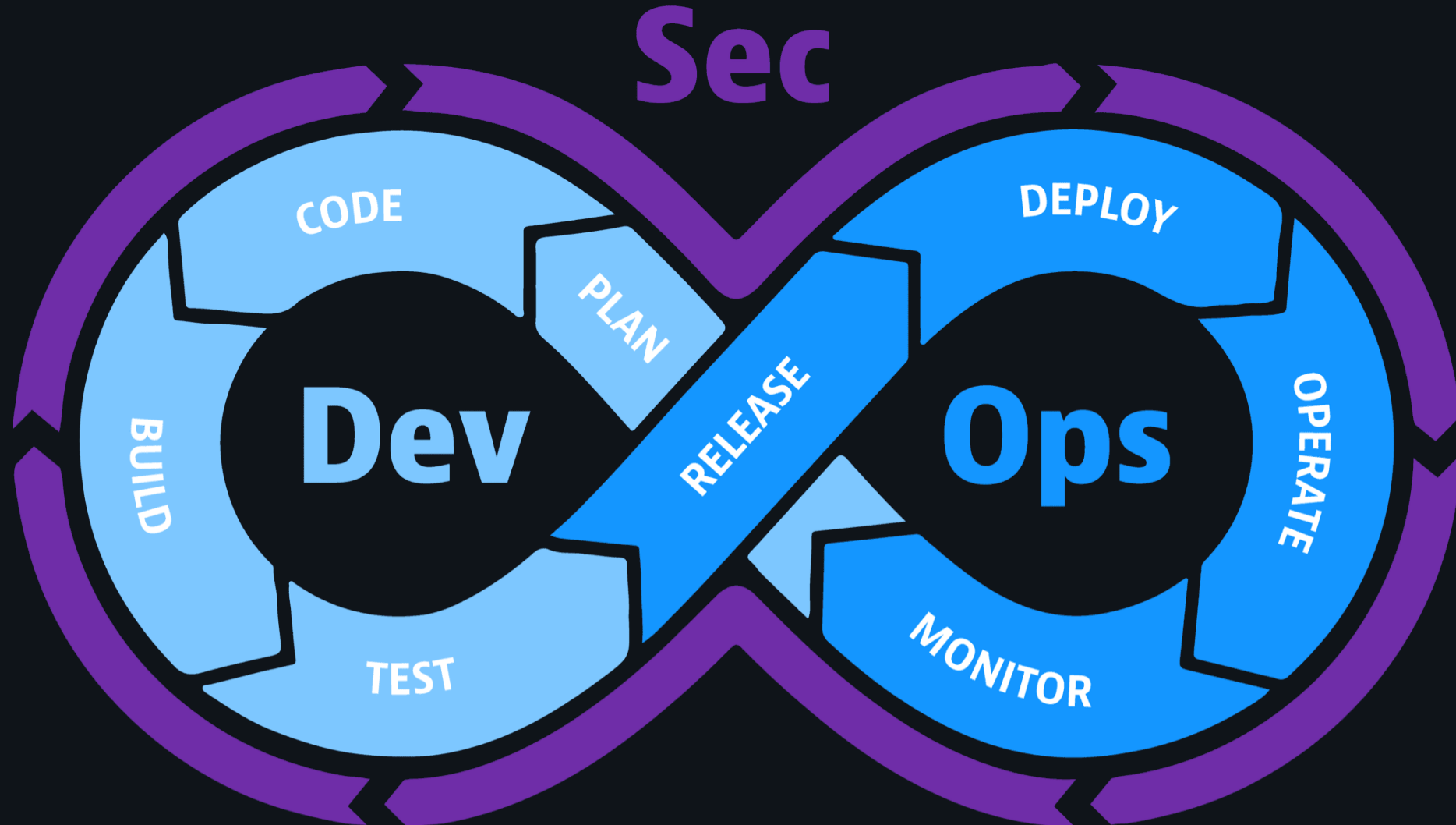


Tools not up to task

- Traditional security tools not designed for cloud-native applications
- Teams take hours/days to identify where they are vulnerable, leaving application exposed



Security needs to span the entire SDLC





What if...

- We had something already deeply monitoring our applications
- That had code level visibility and could see the loaded libraries
- That could trace transactions and knew the topology of our environment
- That runs with low overhead, continuously, across all environments, including production
- And could leverage an AI engine to make sense of that data



Observability and Security Converge



Traces



Metrics



Logs



Topology



Behaviour



Code



Metadata



Network





Cloud done right.



Traces Metrics Logs



Topology Behaviour Code Metadata Network



API OpenTelemetry keptn

600+

Supported technologies

Kubernetes OpenShift AWS Azure GCP Tanzu Enterprise Hybrid cloud

Automatic and intelligent observability

Broadest multicloud and technology support



Cloud done right.



Attack blocking and protection



Vulnerability runtime analytics



Risk-based remediation

- ✓ Automatically detect vulnerabilities in any of your production apps
- ✓ Automatically prioritize biggest risks and identify remediation actions
- ✓ Automated developer workflow to mitigate affected apps

Infrastructure Monitoring

Applications & Microservices

Application Security

Digital Experience

Business Analytics

Cloud Automation

Dynatrace Hub

dynatrace Software Intelligence Platform



OneAgent®



PurePath®



Smartscape®



Grail™



Davis® AI



Traces



Metrics



Logs



Topology



Behaviour



Code



Metadata



Network



API



OpenTelemetry



keptn

600+

Supported technologies



Kubernetes



OpenShift



AWS



Azure



GCP



Tanzu



Enterprise



Hybrid cloud

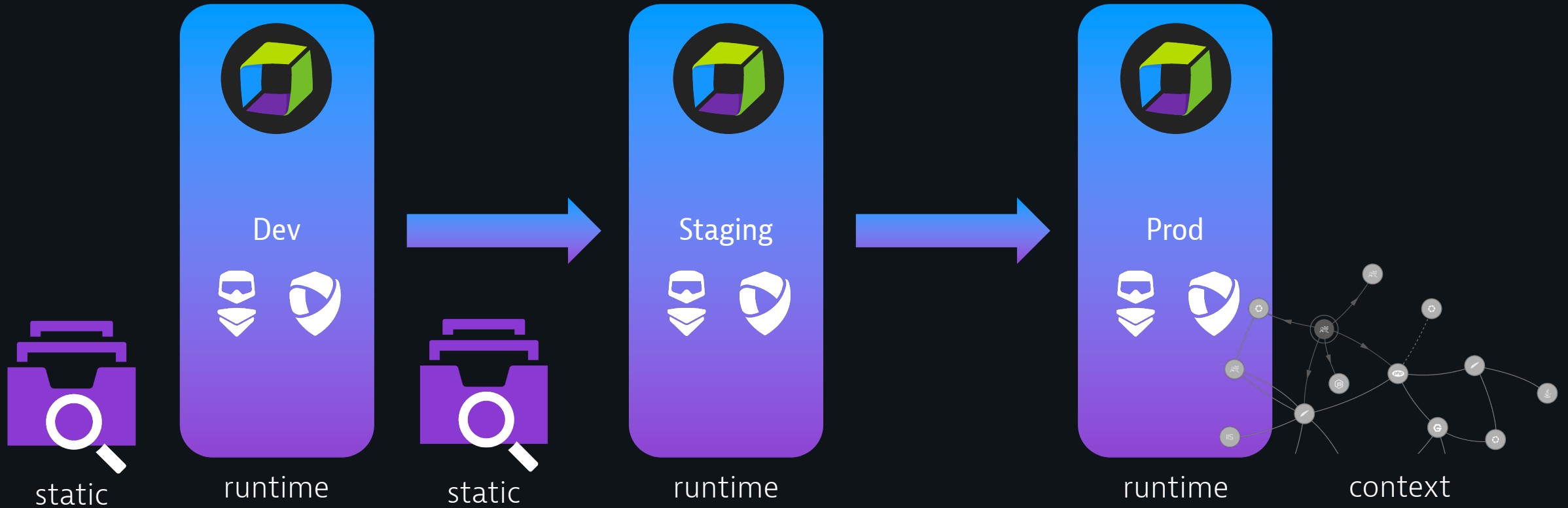
Automatic and intelligent observability

Broadest multicloud and technology support



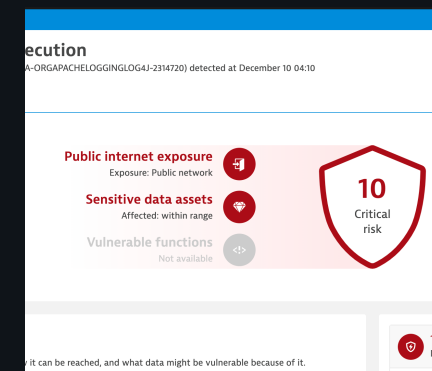
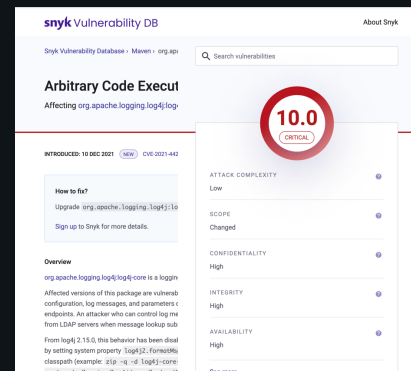
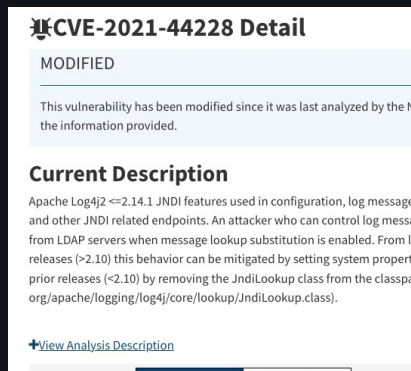
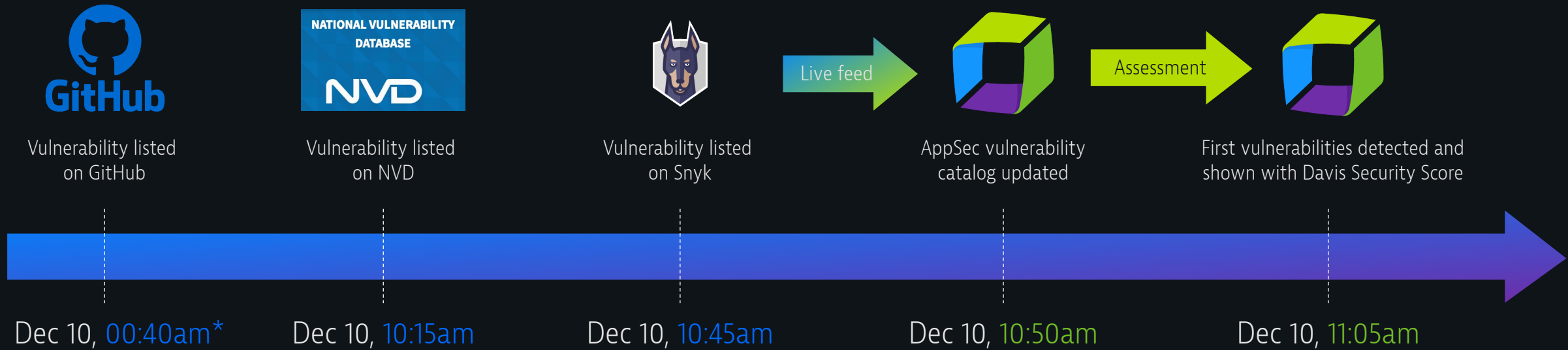
Dynatrace Application Security — Automated visibility across the SDLC

Continually Observing – Not Scanning





Dynatrace identified Log4Shell in production apps minutes after it became known



*All times in UTC



*David Catanoso
Acting Director of Infrastructure
Operations*

"We take a layered, defense-in-depth approach to security, and Dynatrace is one of the solutions we use because it identifies vulnerabilities fast for monitored applications across our clouds.

As an example, with the Log4shell vulnerability, its platform delivered and instantly identified exactly where we were affected, prioritized the systems and runtime environments that required immediate attention, and kept us from wasting time in war rooms and chasing false positives."





Automatically detect vulnerabilities across your environment

Remote Code Execution

Third-party vulnerability (SNYK-JAVA-ORGSPRINGFRAMEWORK-2436751) first detected on March 30 at 19:24.

[Settings](#)

Public internet exposure
Public network

Reachable data assets
Within range

Vulnerable functions
Not available

9.8

Critical risk

Exploit
Exploit published

Process groups
8 affected

Vulnerable component
spring-beans

Vulnerability details

Insights by snyk

Description

Technology

Java

[org.springframework:spring-beans](#) is a package that is the basis for Spring Framework's IoC container. The BeanFactory interface provides an advanced configuration mechanism capable of managing any type of object.

Affected versions of this package are vulnerable to Remote Code Execution via manipulation of ClassLoader that is achievable with a POST HTTP request. This could allow an attacker to execute a webshell on a victim's application (TomCat), or download arbitrary files from the server (Payara/Glassfish).

Note:

- Current public exploits require victim applications to be built with JRE version 9 (or above) and to be deployed on either Tomcat, Payara, or Glassfish.
- However, we have confirmed that it is technically possible for additional exploits to work under additional application configurations as well.

Process group overview

Process groups

Process groups in total	9
Affected process groups	8 (89%)
Resolved process groups	1 (11%)
Muted process groups	0 (0%)

Affected Resolved Muted

Processes

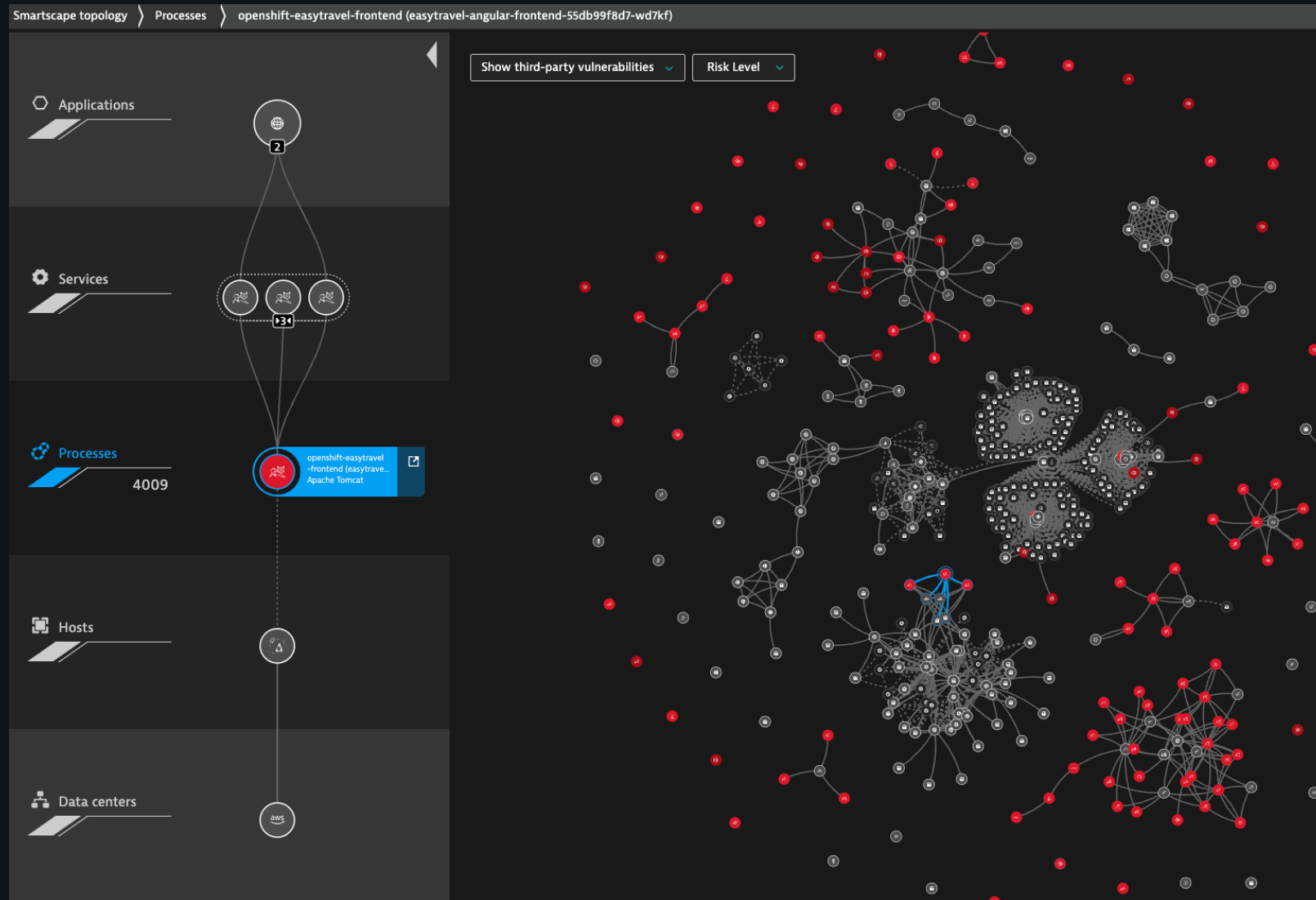
Processes total	9
Affected processes	8
Exposed	4 (50%)

Most affected process groups

Process group	Status	
SpringBoot api-gateway-*	Affected	
1/1 process affected		



Leverage topology for automatic risk prioritization





Leverage topology for automatic risk prioritization

9.8 Critical risk problem
Davis Security Score

9.8 Critical risk problem
CVSS as a base

Analyzed with Davis

Public internet exposure

Exposure	Impact on score	Risk level
Public network	No changes	Critical risk

Reachable data assets

Affected	Impact on score	Risk level
Within range	No changes	Critical risk

9.8 Critical risk problem
Davis Security Score

1 reachable data asset ⓘ
Directly connected to an affected entity.

Data asset	Database and host
service_instance_db	service_instance_db on gke-keptn-demo1-cos-bd5b5ae9-806f.c.dynatrace-demoability.internal

8.6 High risk problem
Davis Security Score

9.8 Critical risk problem
CVSS as a base

Analyzed with Davis

Public internet exposure

Exposure	Impact on score	Risk level
Public network	No changes	Critical risk

Reachable data assets

Affected	Impact on score	Risk level
Not within range	Lowering score	High risk

8.6 High risk problem
Davis Security Score

Davis Security Score rated this problem down by 12%.



Remediation Tips and Automatic Remediation Tracking

snyk Vulnerability DB

Snyk Vulnerability Database > Maven > org.springframework:spring-beans

Remote Code Execution

Affecting `org.springframework:spring-beans` package, versions [,5.2.20) [5.3.0, 5.3.18)

INTRODUCED: 30 MAR 2022 [CVE-2022-22965](#) [?](#) [CWE-94](#) [?](#)

How to fix?

Upgrade `org.springframework:spring-beans` to version 5.2.20, 5.3.18 or higher.

SpringBoot visits-service-*	1/1 process affected		Affected
SpringBoot api-gateway-*	1/1 process affected		Affected
SpringBoot org.dynatrace.ssrfservice.Application unguard-proxy-service-*	1/1 process affected		Affected
tomcat	0/1 processes affected		Resolved

Details	Status
Process group name.....tomcat	Vulnerability resolved
Processes.....0/1 processes affected	215 d 17 h ago (2022-04-12)
Status.....Resolved	Change status
First detected.....228 d 1 h ago	
Last update.....215 d 17 h ago	



Remediation Tips and Automatic Remediation Tracking

6 related container images ⓘ

Find out which container images are used by the affected processes.

Image name	Image ID	Affected processes
246186168471.dkr.ecr.us-east-1.amazonaws.com/unguard-microblog-service:v0.3.3	sha256:18a00b1790ccc38e4d227731472e2dcd8cb65ffcea71fb1f36d780cc27a16d23	1
246186168471.dkr.ecr.us-east-1.amazonaws.com/unguard-proxy-service:v0.5.1	sha256:0368d3cc7785f2017f98757cce21fa4b3ee94e2eda44e60ae8d519e7a8d926f4	1

Hosts 5

Related Hosts Affected processes

gke-keptn-demo1-cos-bd5b5ae9-dj74.c.dynatrace-demoability.internal	3
i-040585ffc09e5c519	2
credhub/711d53a1-9a2c-40b9-b1e9-78245d907a7c	1
diego_cell/7fdfae37-2489-4244-9835-376b5a052df1	1
gke-keptn-demo1-cos-bd5b5ae9-qlcr.c.dynatrace-demoability.internal	1

[View all related hosts](#)

Databases 2

Kubernetes workloads 6

Kubernetes clusters 2

Related Kubernetes clusters Affected nodes

gke	4
EKS	2





Remediation Tips and Automatic Remediation Tracking


Davis® Security Advisor

Top recommended fixes

These are the most impactful actions you can take right now to improve the security of your environment.

 Upgrade log4j-core
Solves 1 critical (4 vulnerabilities total)
[Add as filter](#)

 Upgrade commons-fileupload
Solves 1 critical (3 vulnerabilities total)
[Add as filter](#)

 Upgrade vm2
Solves 1 critical (2 vulnerabilities total)
[Add as filter](#)









< 1 2 3 ... 40 41 42 >

Filtered by: Risk assessment: [Public internet exposure](#) X Risk level: [Critical](#) X

4 vulnerabilities detected

Powered by [Davis® Security Score](#)

[Public exposure](#) [Reachable data](#) [Vulnerable functions](#) [Public exploit](#)

Vulnerability	Davis Security Score	Status	Affected entities	First detected	Last update	Details
S-353: Remote Code Execution org.springframework:spring-beans	 Critical 9.8 Public exposure Reachable data Public exploit	Open	Process groups: 8	228 d 2 h ago	13 min 56 s ago	
S-468: Arbitrary Code Execution commons-fileupload:commons-fileupload	 Critical 9.8 Public exposure Reachable data Vulnerable functions Public exploit	Open	Process groups: 1	354 d 10 h ago	2 h 1 min ago	
S-889: HTTP Request/Response Smug... Node.js runtime	 Critical 9.1 Public exposure Reachable data Public exploit	Open	Process groups: 17	6 d 15 h ago	3 d 4 h ago	
S-318: Remote Code Execution (RCE) org.apache.logging.log4j:log4j-core	 Critical 9.0 Public exposure Reachable data Public exploit	Open	Process groups: 3	334 d 6 h ago	6 d 9 h ago	



Effortlessly detect, prioritize, and protect against app vulnerabilities

Dynatrace secures applications at run time, filling a critical visibility gap and enabling DevSecOps to scale as complexity grows



Vulnerabilities 5-314

Arbitrary Code Execution

Third-party vulnerability (SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720) detected at December 10 04:10

Settings

Mute

- Public internet exposure**
Exposure: Public network
- Sensitive data assets**
Affected: within range
- Vulnerable functions**
Not available

10
Critical risk

- Exploit
Public exploit available
- Process groups
8 affected
- Vulnerable component
log4j-core

Context and details
Find out more about this vulnerability, how it can be reached, and what data might be vulnerable because of it.

- 1 exposed process**
to the public internet, within 1 process group. Forward user-controlled input
tomcat within 1 process group
[View all exposed process groups](#)
- 8 affected processes**

10.0 Critical risk problem
Davis Security Score

10.0 Critical risk problem
CVSS as a base

Analyzed with Davis

Public internet exposure

Exposure	Impact on score	Risk level
Public network	No changes	Critical risk



Takeaways

- Get visibility into production app runtime vulnerabilities
- Empower your Dev teams with risk prioritization so they know what's important
 - Leverage observability data for risk assessment
 - Provide developers with remediation tips
- Integrate app security in every step of your pipeline
 - Catch early and often
 - Know exactly what and where in production

Thank you

