Driving Transformation:

Unleashing AI & Automation Innovation

PRESENTER

ENRIC CHOO

LEAD, SOLUTION ENGINEER


…business expect IT to operate faster than before


…software development and delivery must match the speed of the customer

Complexity

Stakes are high

You have one of the hardest jobs in the world

Release frequency,
Digital Transformation

User
expectation


10:13
MySejahtera

Digital Services

IT Services

Google Cloud Platform

aws

Enterprise

Tanzu

Openshift

Azure

Hybrid Cloud

Kubernetes

3rd Party Services

- Other Enterprises
- Banks & Payments
- External Content
- Network & Gateways
- Data & Storage

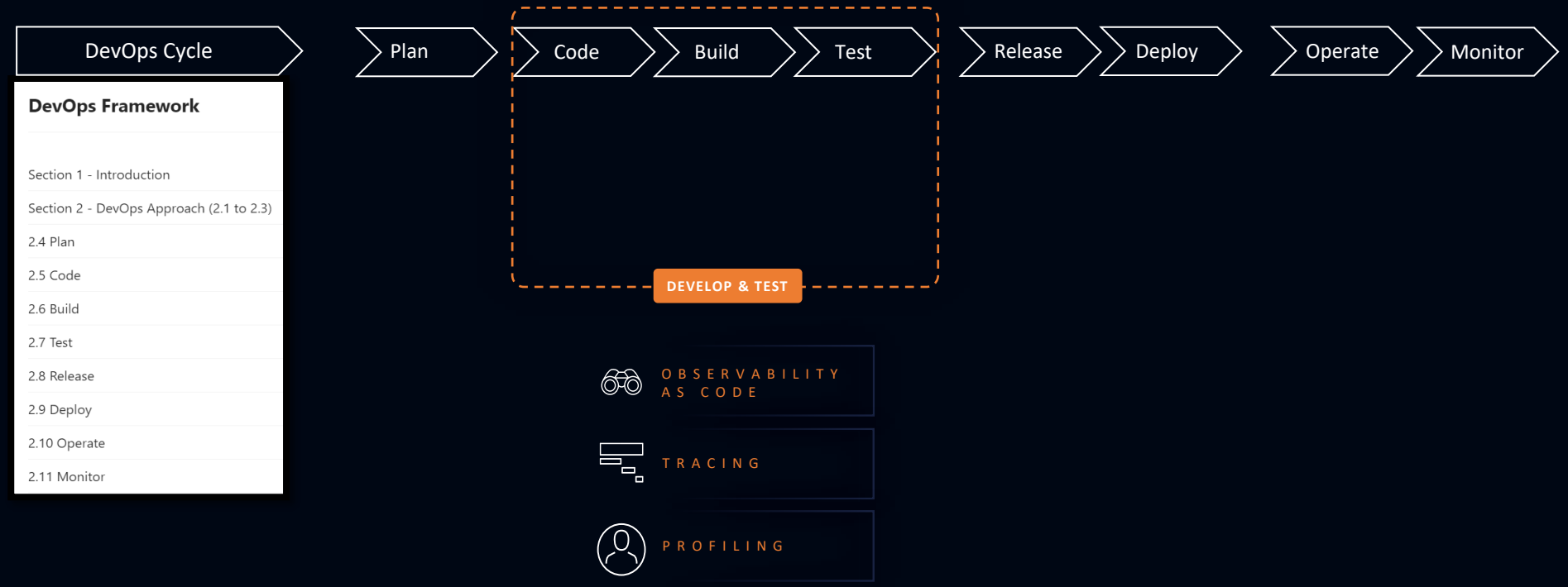
Requires **Automatic** Observability and **Application Security**

Business context | User Experience | **Contextual** Data Collection | Security | **Intelligent** Automation | Dev + Prod

On-Prem

SaaS + Data Lakehouse + Log Management + Business Events + Custom Apps + Automation Workflow

THE DEVOPS FRAMEWORK



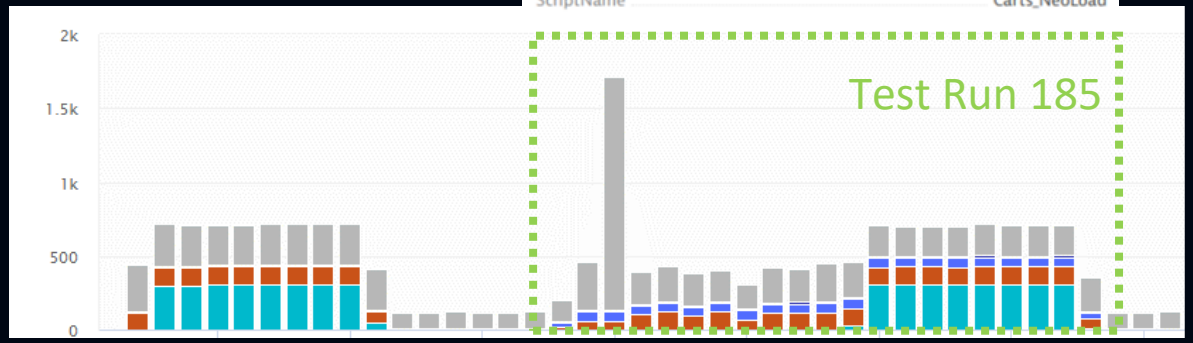
Source: *https://sqa.jdn.gov.my/index.php/ms/section-1-introduction*

SHIFT LEFT

Push Test Context

Start/Stop NeoLoad Test FuncChec... today, 16:06

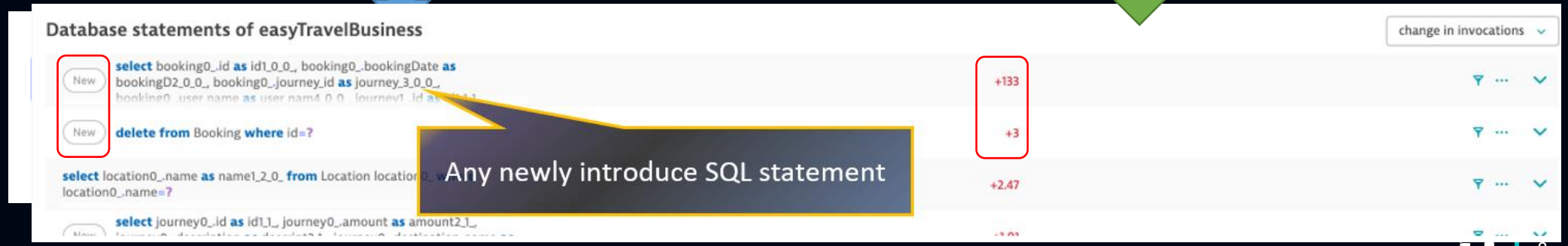
Entity	ItemsController
Time	today, 16:06 - 16:16 (10 min)
Source	NeoLoadWeb
Type	NeoLoad TestFuncCheck_carts_185
NeoLoad_Scenario	Cart_Load
NeoLoad_TestName	FuncCheck_carts_185
NeoLoad_URL	https://neoload.saas.neotys.com/#!result/2d74a94d-153b-409e-bd87-d6de52ff6703/overview
ScriptName	Carts_NeoLoad



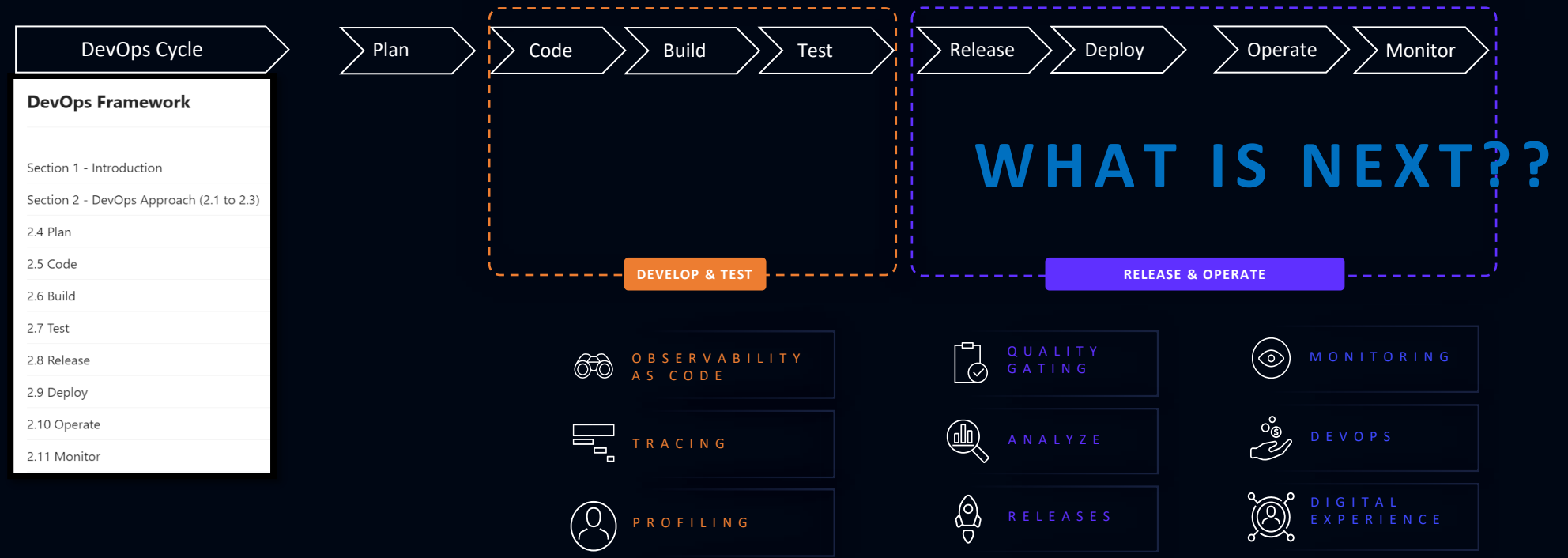
dynatrace

FullStack Hotspot Analysis

FullStack Hotspot Comparison



THE DEVOPS FRAMEWORK



Source: *https://sqa.jdn.gov.my/index.php/ms/section-1-introduction*

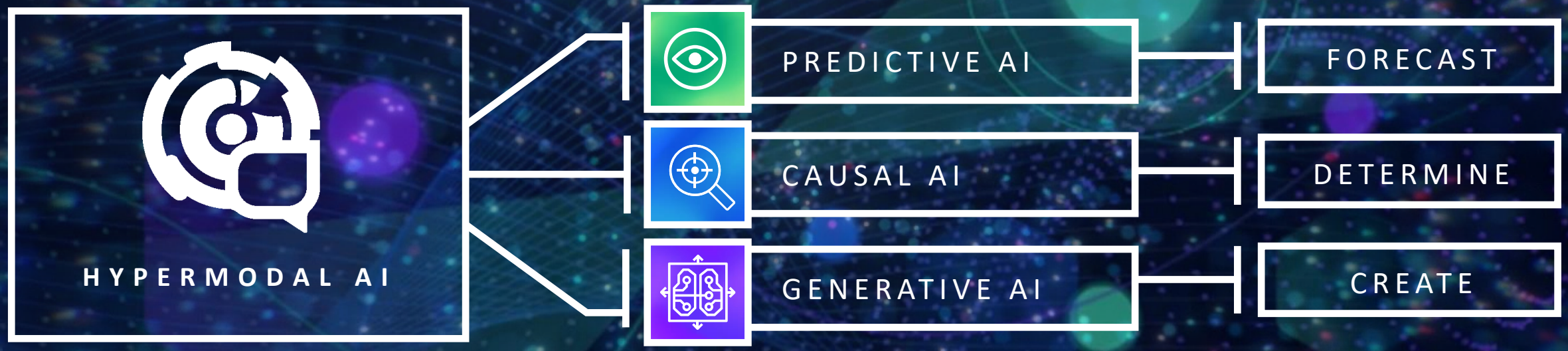

AI

LLMs

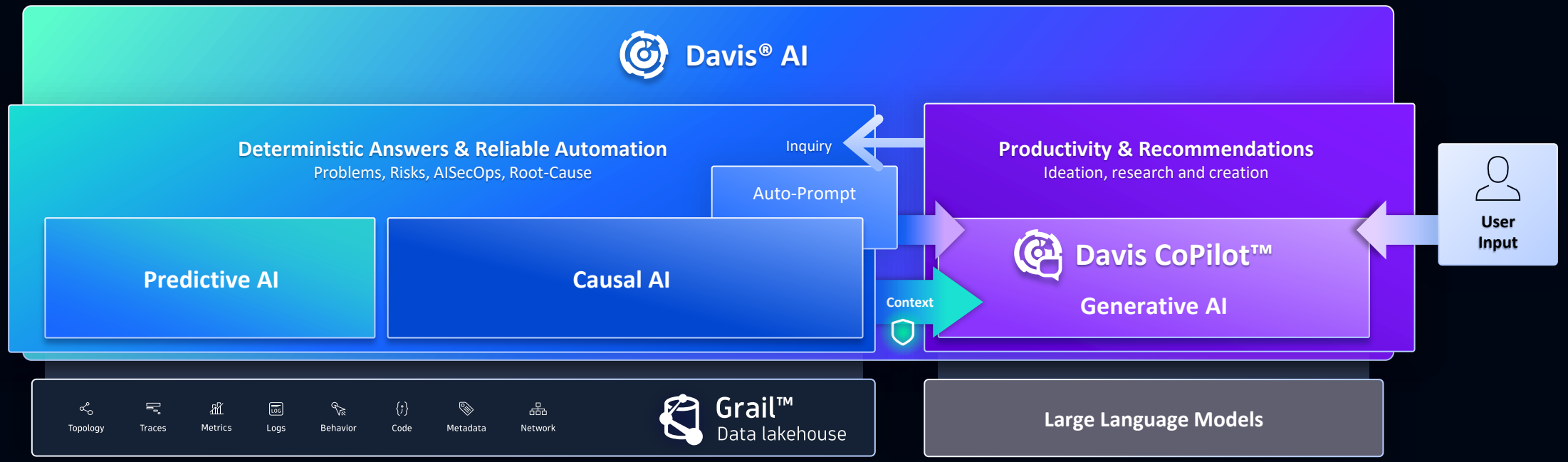
Early disease detection

Self-driving cars

Davis® AI – Industry‘s first hypermodal AI – The Power Of Three



Davis® AI – Industry‘s first hypermodal AI – The Power Of Three

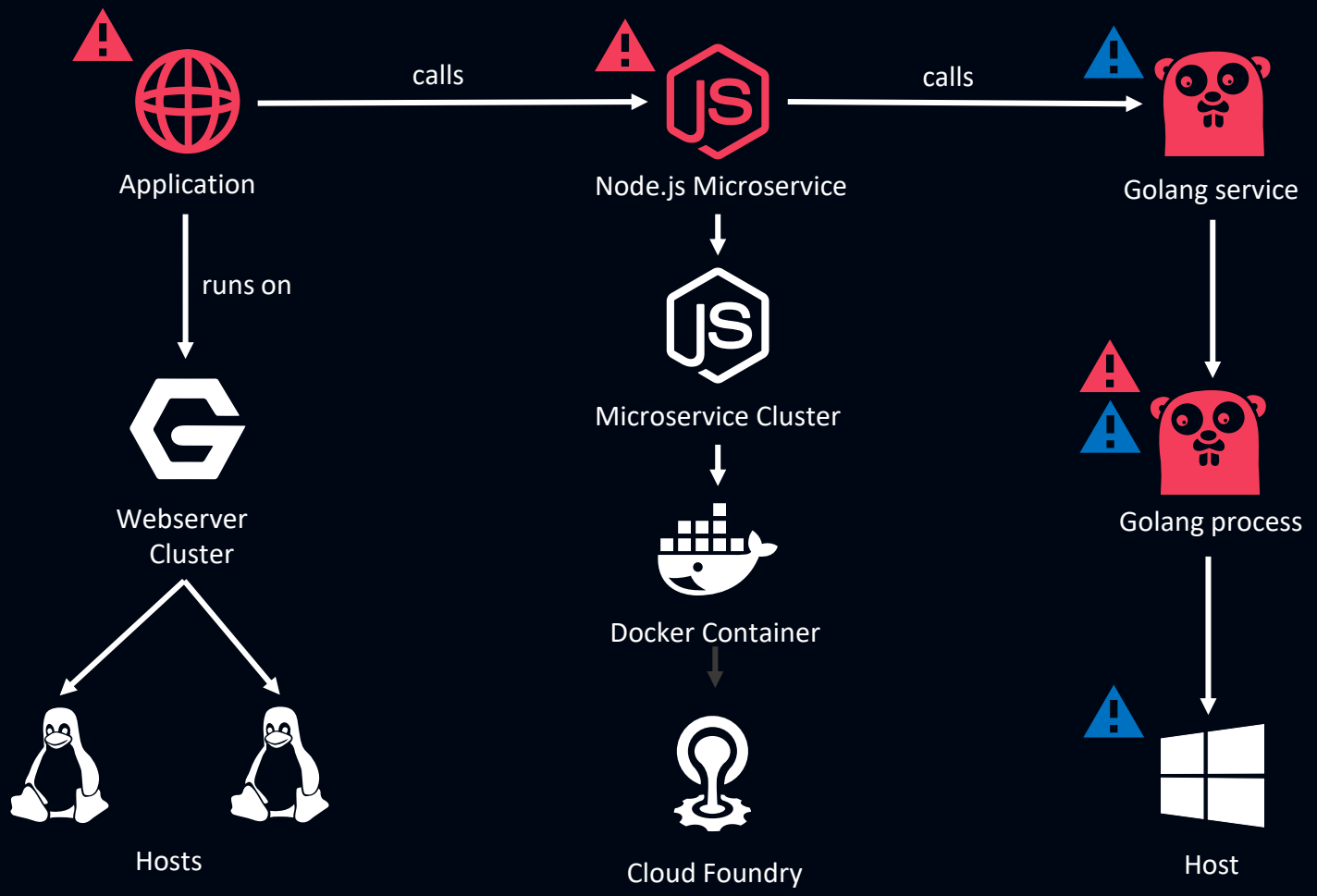


DAVIS AI

CAUSAL AI

AUTOMATIC ROOT-CAUSE ANALYSIS

DYNATRACE DAVIS AI DETECTS AND ANALYZES THE ROOT CAUSE OF PROBLEMS.



1. Real user experience
2. Topology
3. Transactions
4. Code-level insights
5. Metrics
6. Cloud platform
7. Events
8. Logs
9. Third-party events

DAVIS AI

PREDICTIVE AI

PREDICTIVE OPERATIONS

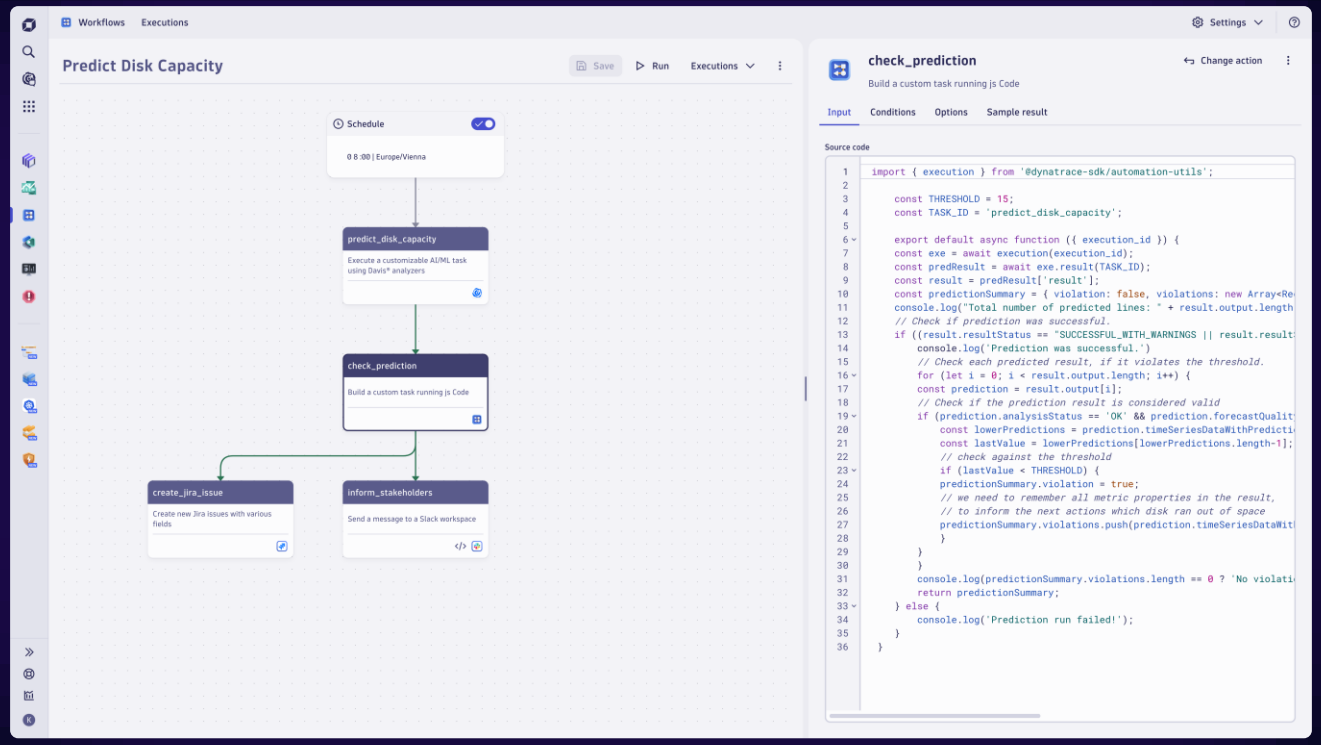
PROACTIVELY REACT

CHOOSE THE TRIGGER SCHEDULE
CHECK ONCE A DAY, HOUR, WEEK

FORECAST
ALL DISK FREE SPACE

GENERATES A REPORT OF ALL DISKS THAT WILL RUN OUT

CHOOSE A DELIVERY ACTION,
E.G.: SEND BY SLACK, EMAIL, ETC



DAVIS AI

GENERATIVE AI

Notebooks
Notebook
Perform 24
Share
Rerun sections
Run
Last 2 hours
Hide input
Options
Davis CoPilot Preview
Try "Today's error logs" or "Service instances and their hosts"

Notebooks | Notebook

Perform 24 | Share | Rerun sections

Run | Set in prompt | Hide input | Options

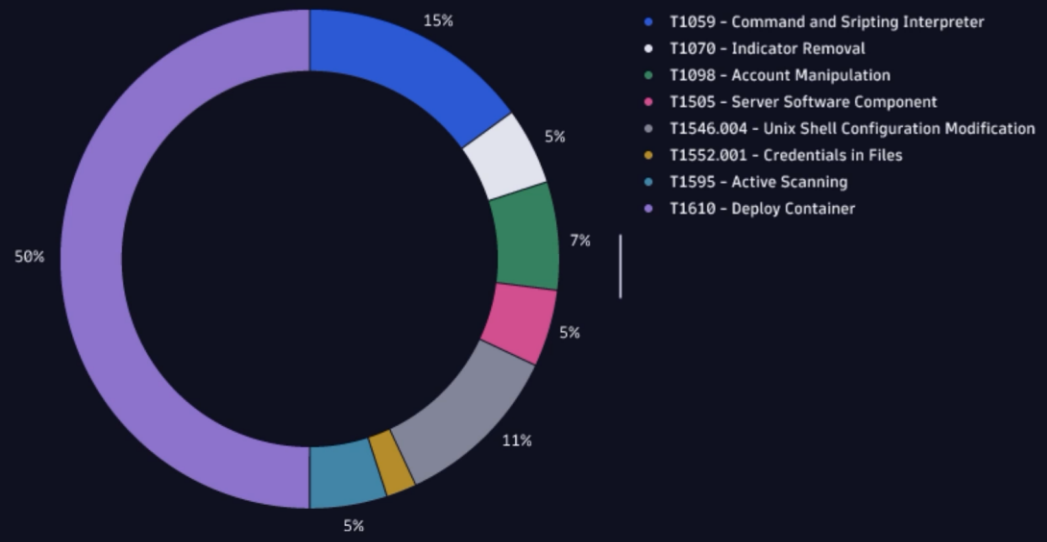
Davis CoPilot Preview

Summarize all mitre security events of the last 72 hours

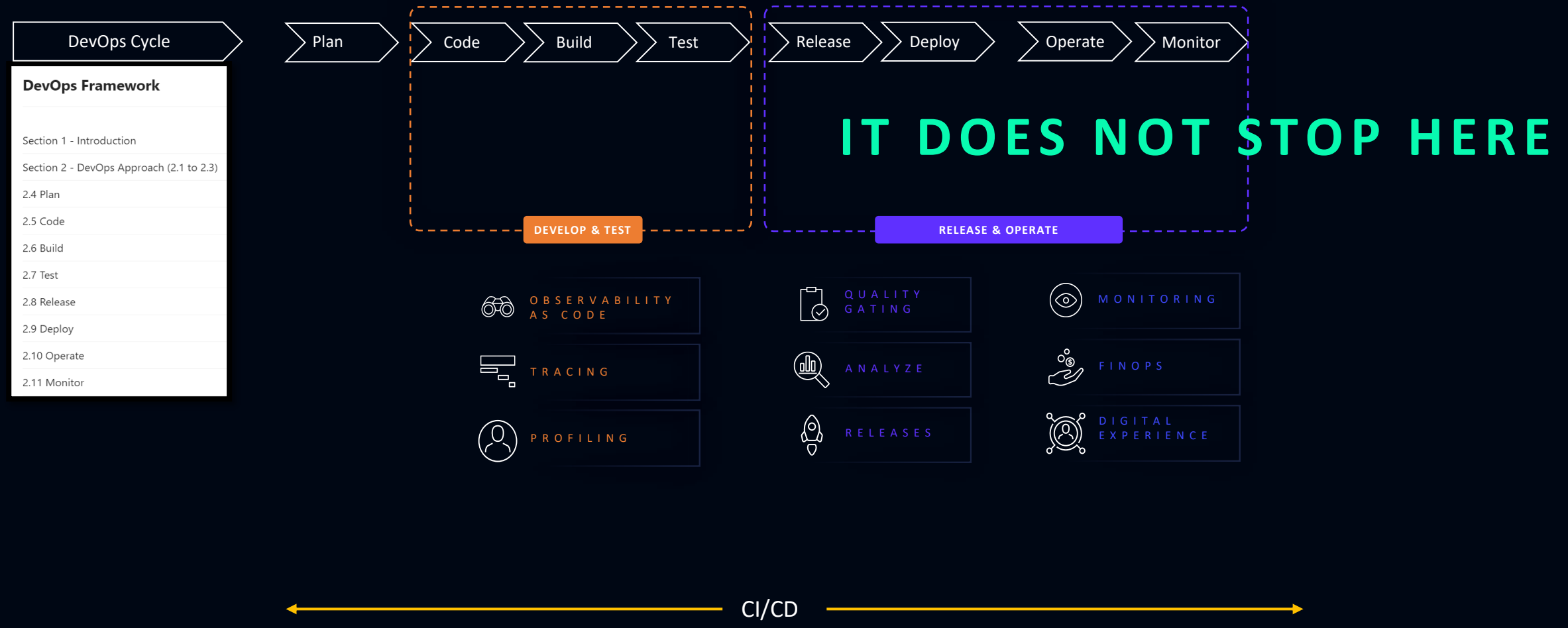
AI-generated results might be inaccurate. DQL

```
fetch events, from:now() - 72h
| filter event.kind == "MITRE_SECURITY"
| summarize by: {event.type}, count = count()
```

8 records Executed at: 13/01/2024, 10:03:56 Timeframe: 8:04:36 – 10:03:56

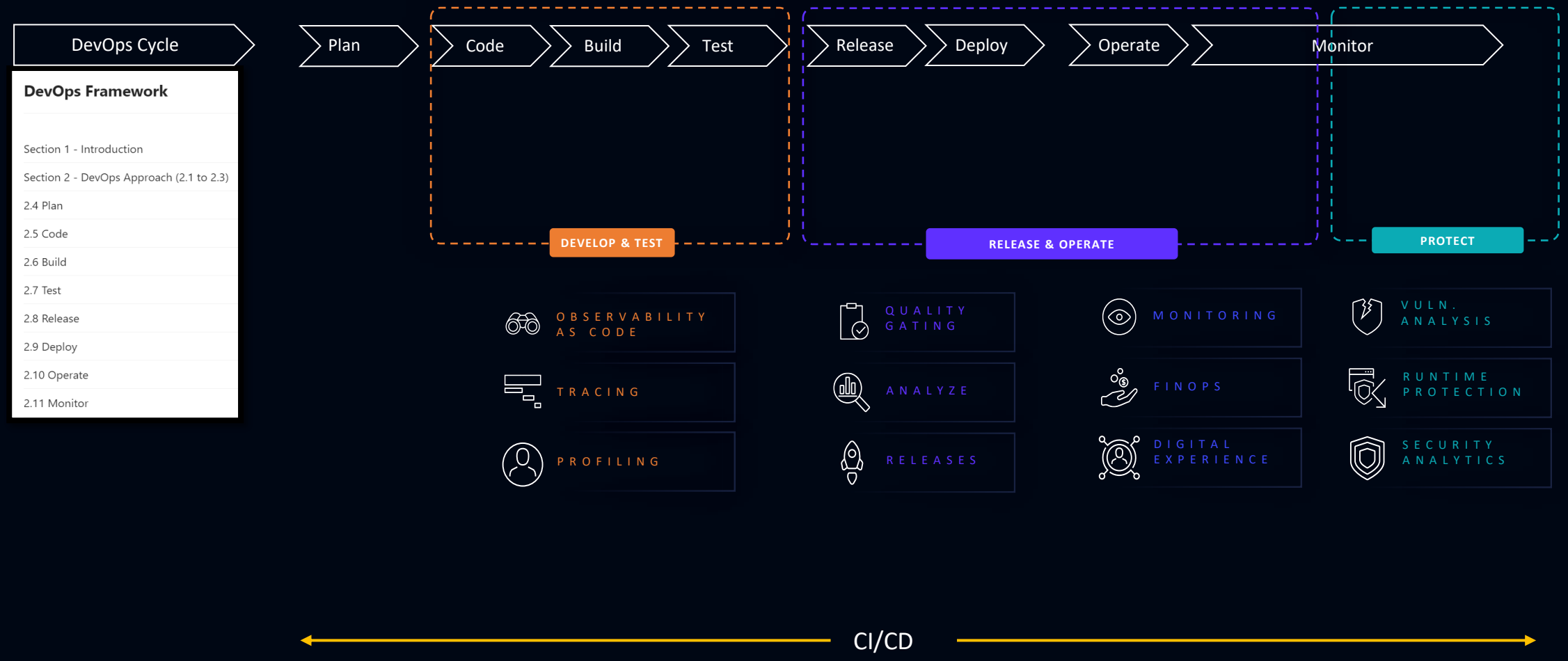


THE DEVOPS FRAMEWORK



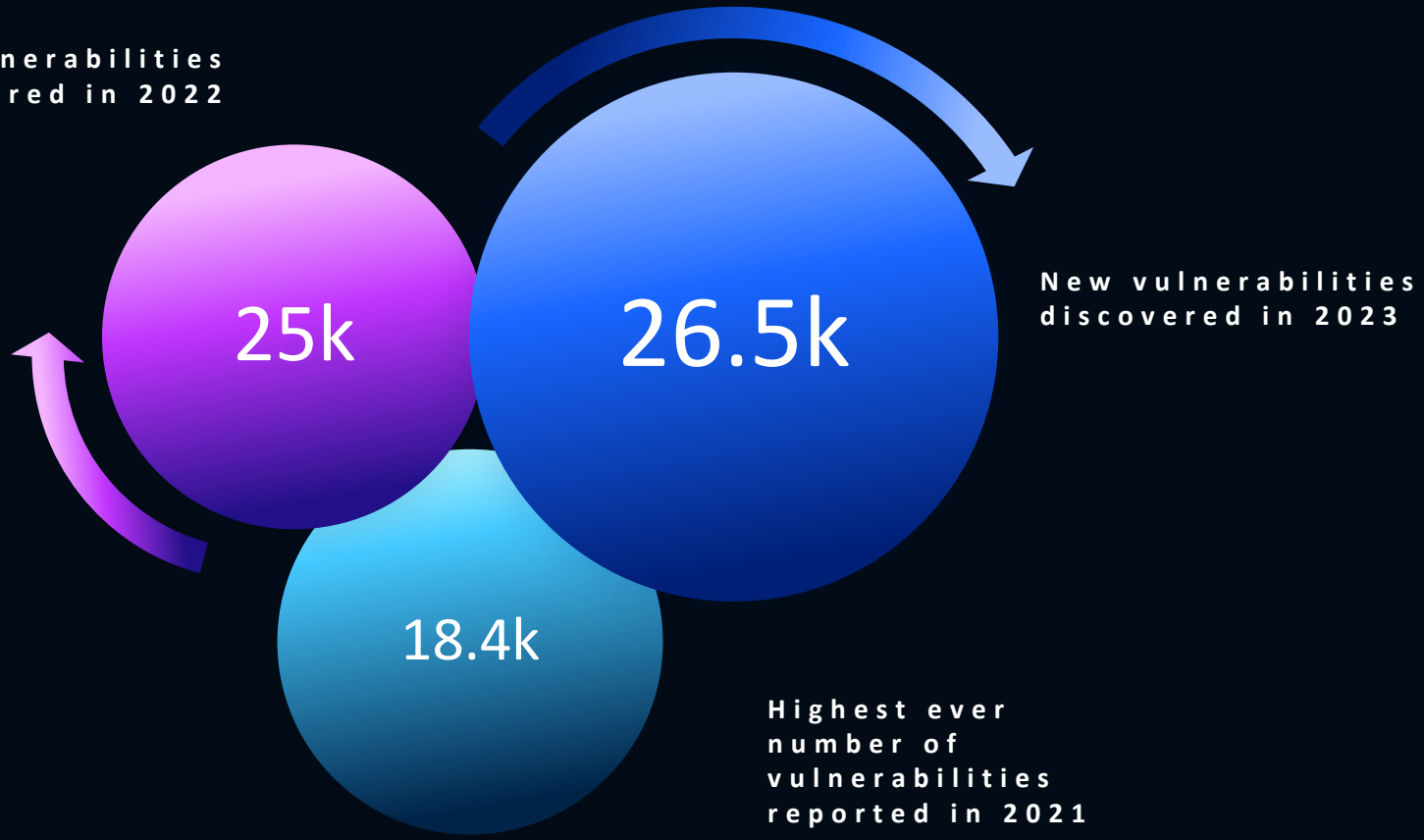
Source: *https://sqa.jdn.gov.my/index.php/ms/section-1-introduction*

THE DEVSECOPS FRAMEWORK

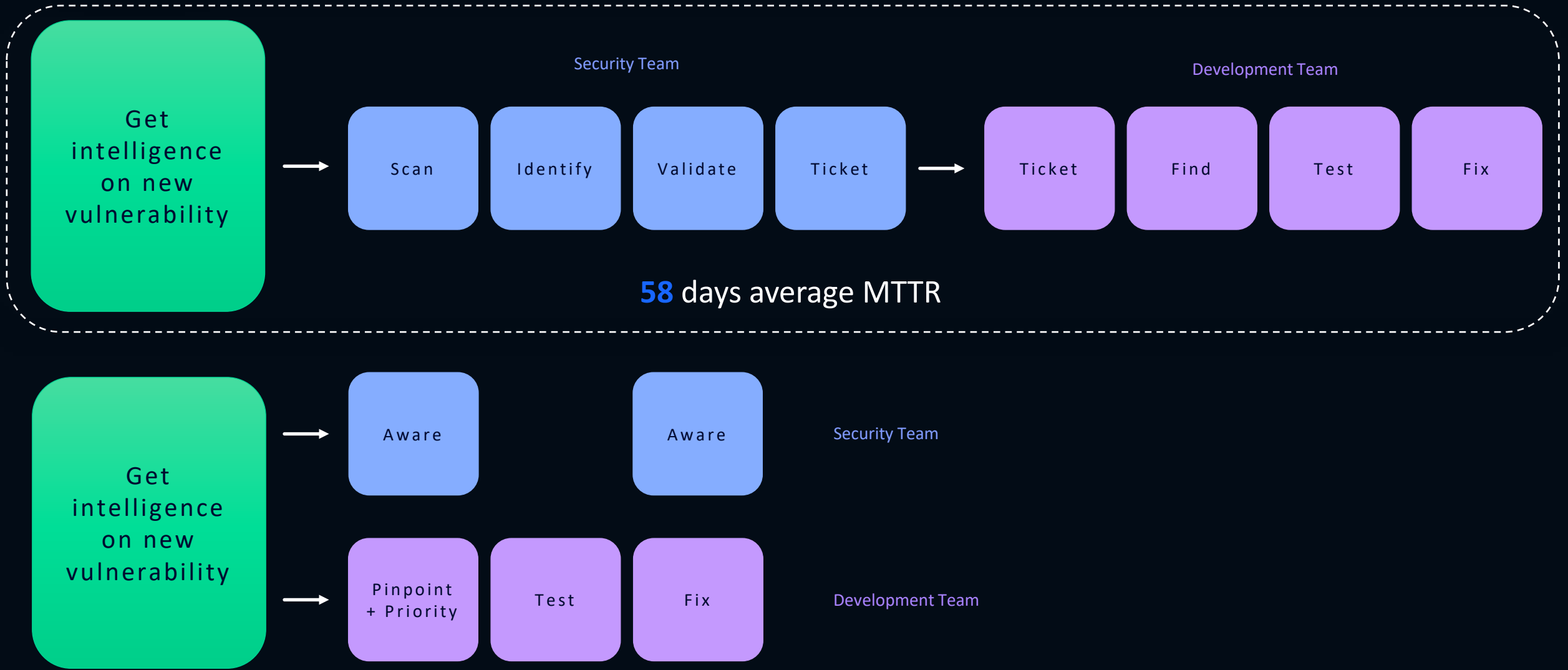


Source: *https://sqa.jdn.gov.my/index.php/ms/section-1-introduction*

Securing environments has never been harder



Actionable, prioritized and real time vulnerability risk mitigation



"The top assets impacted in breaches are web application and email servers" -*2022 Verizon DBIR*

Application Security overview

This environment's security posture.

Your environment is currently monitored.

Dynatrace brings immediate awareness to critical vulnerabilities that put your operations and business at risk

Easily identify the number of known vulnerabilities in your environment

Vulnerabilities

315 total (+5 muted)

5 118 150 42

5 Critical

55% of total

Host coverage

Application Security covered hosts: 61 (55% of total hosts)

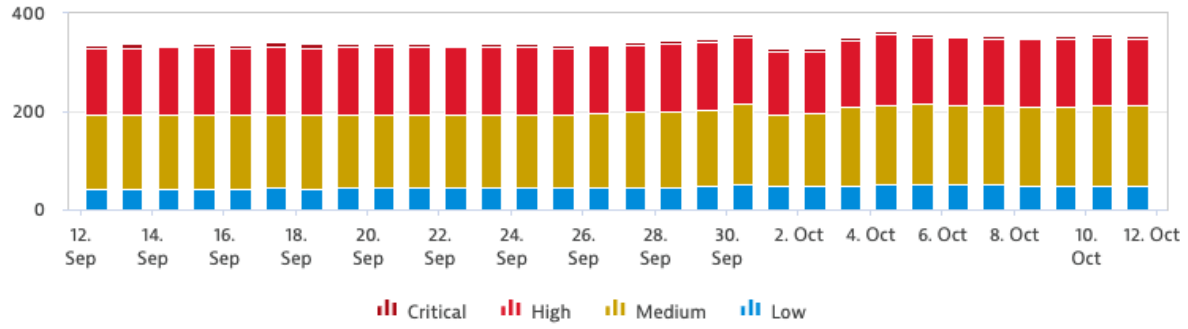
Increase coverage

Vulnerabilities are observed in real-time, without scheduled/static scanning

Risk level

Open vulnerabilities

5 Critical 118 High 150 Medium 42 Low

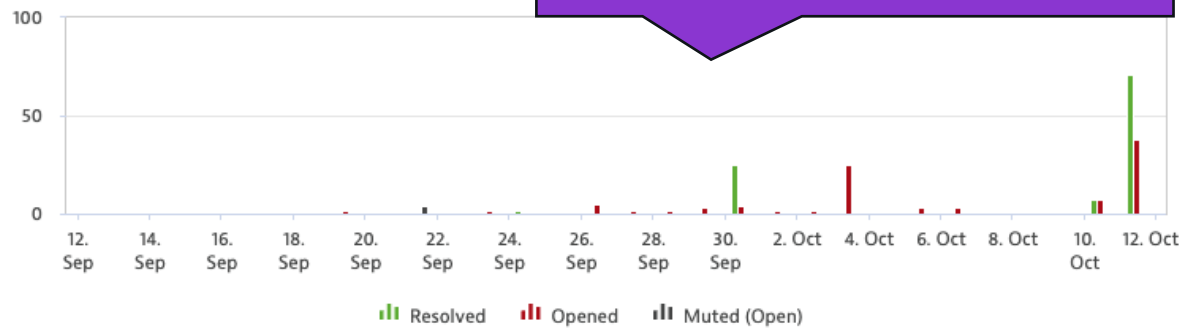


View all vulnerabilities

Track vulnerability trends over time as new vulnerabilities are discovered and existing ones are successfully remediated

Vulnerabilities

SNYK partner integration updates known vulnerabilities every 5 minutes



View all vulnerabilities

Affected process groups

Sorted by severity

Process group	Technology	Vulnerabilities
SpringBoot customers-service-*	Java	4 Critical (46 total)
SpringBoot visits-service-*	Java	3 Critical (44 total)

Demo data used in this slide

Remote Code Execution (RCE)

Third-party vulnerability (SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720) first detected on December 10 at 22:10.

Settings

Davis provides an easy to consume summary of the security problem (vulnerability) including the what, where, and why your environment is vulnerable

Mute

Public internet exposure
Public network

Reachable data assets
Within range

Vulnerable functions
Not available

10.0
Critical risk

Exploit
Exploit published

Process groups
3 affected

Vulnerable component
log4j-core

Immediately identify where the vulnerability exists – in real-time. Dynatrace doesn't rely on scheduled/static scans, instead providing real-time runtime vulnerability detection within the monitored process

Vulnerability details

Insights by snyk

Description

org.apache.logging.log4j:log4j-core is a logging library for Java.

Affected versions of this package are vulnerable to Remote Code Execution (RCE). Apache Log4j2 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

From log4j 2.15.0, JNDI LDAP endpoints are restricted to localhost by default.

For more information visit SNYK

Technology

Java

CVE	CVE-2021-44228
OWASP	2021:A3, 2021:A6
CWE	CWE-94

Process group ov

Process groups

Process groups in total	9
Vulnerable process groups	3 (33%)
Resolved process groups	5 (56%)
Muted process groups	1 (11%)

Vulnerable Resolved Muted

Processes

Processes total	10
Vulnerable processes	3
Affected processes	0 (0%)
Affected and exposed processes	3 (100%)

Affected Exposed Not affected

Demo data used in this slide

Vulnerable functions

Third-party vulnerability (SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720) first detected on December 10 at 22:10.

Settings

CWE CWE-94

Vulnerable functions

The following function has been identified to contain the vulnerability within the library.

PG: Process group

Class	Vulnerable function	Function usage	PGs
org.apache.logging.log4j.core.lookup.JndiLookup	lookup	In use	0
		Not in use	3
		Not available	0

Details on the specific vulnerable function and if it being used in their environment

10.0 Critical risk problem
Davis Security Score

10.0 Critical risk problem
CVSS as a base

Truly understand your actual level of risk through AI analysis of the vulnerability, where it exists, and how it can be exploited

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

10.0 Critical risk problem
Davis Security Score

Affected and exposed processes 3 (100%)

Affected Exposed Not affected

Most affected process groups

Process group	Status
SpringBoot customers-service-* 1/1 process affected	Vulnerable
SpringBoot org.dynatrace.ssrfservice.Application unguard-proxy-service-* 1/1 process affected	Vulnerable
SpringBoot vets-service-* 1/1 process affected	Vulnerable
SpringBoot visits-service-* 1/1 process affected	Muted
hipstershop.AdService adservice-* 0/2 processes affected	Resolved

Immediately identify where the vulnerability exists – in real-time. Dynatrace doesn't rely on scheduled/static scans, instead providing real-time runtime vulnerability detection within the monitored process

View all process groups

1 reachable data asset
Directly connected to an affected entity.

Data asset	Database and host
service_instance_db	service_instance_db

Demo data used in this slide

Attacks

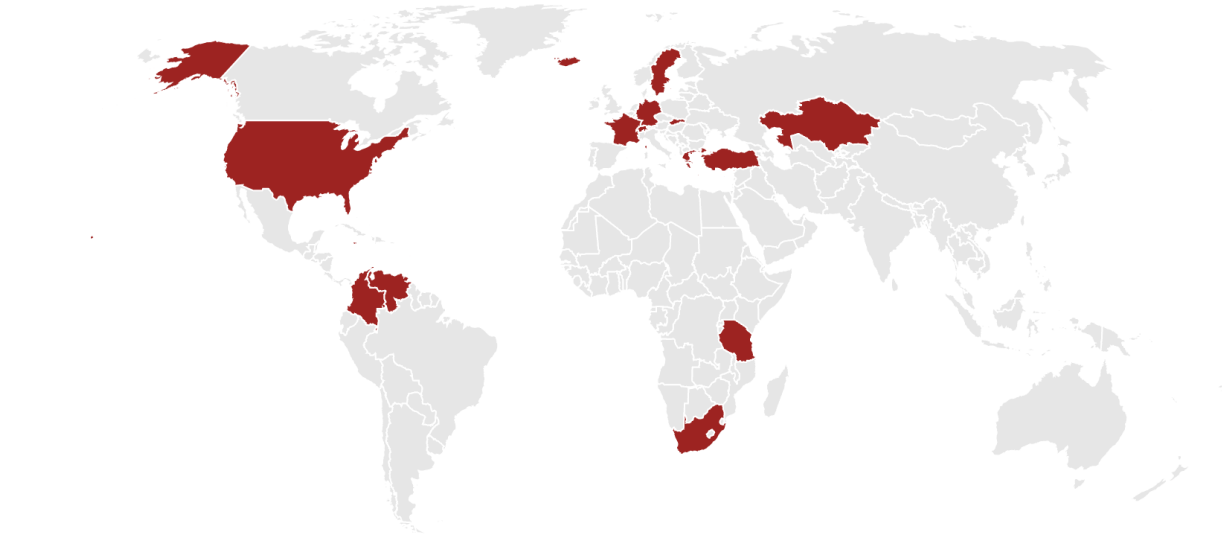
Overview of all attacks to your environment in real time.

Your environment is currently monitored.

1,501/2,393	892/2,393	0/2,393	Monitoring
Attacks exploited	Attacks blocked	Attacks allowlisted	Global attack control

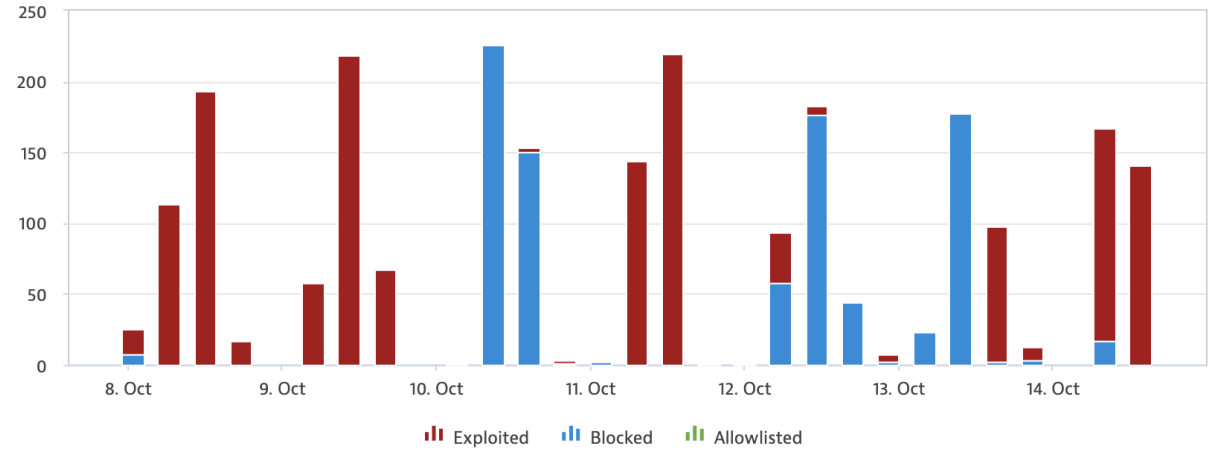
Attack source locations

>10 attacks 5 - 10 attacks <5 attacks



Attacks over time

Exploited: 1,501 Blocked: 892 Allowlisted: 0

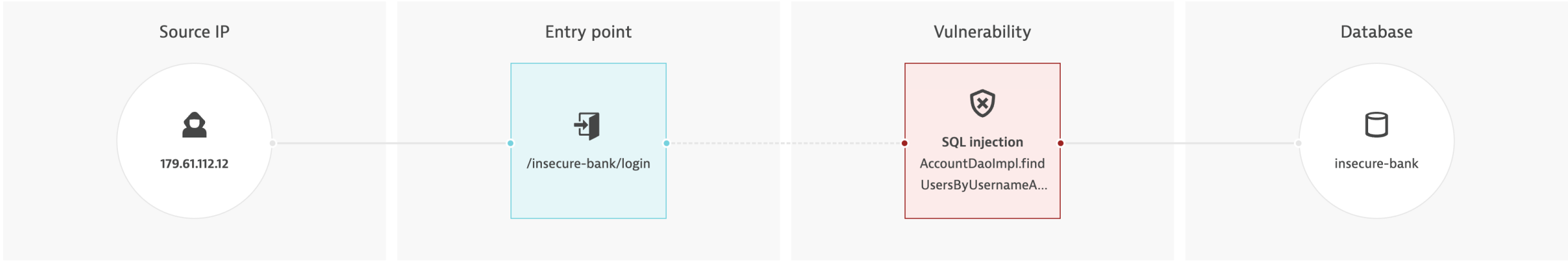


Demo data used in this slide

A-5MWPVN: insecure-bank (Tomcat)

Attack path

Timestamp: Oct 14 17:51



Entry point

URL
/insecure-bank/login

Code location
```
javax.servlet.ServletRequestWrapper.getParameter(String)
```

Entry point function
```
javax.servlet.ServletRequestWrapper.getParameter(String)
```

Payload

HTTP parameter	username
HTTP parameter value	admin') or ('1'='1

Vulnerability

Name
SQL injection at AccountDaoImpl.findUsersByUsernameAndPassword():40

Code location
```
org.vulnsamples.dao.AccountDaoImpl.findUsersByUsernameAndPassword(String, String):40
```

Vulnerable function
```
org.apache.commons.dbcp.DelegatingStatement.executeQuery(String)
```

SQL statement
```
select * from account where username='admin') or ('1'='1' AND password=''
```

View vulnerability

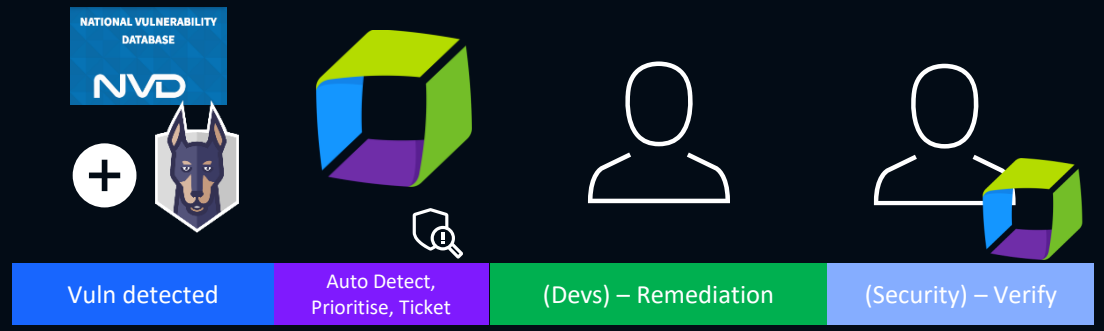
Demo data used in this slide

Large Insurance Customer **95%** reduction in vulnerability risk remediation time

Before AppSec

> 96 hours

After AppSec



4 hours

1. **Before** Dynatrace AppSec
   100 vulnerabilities
   400 days (96 x 100 = 9600hrs)
2. **After** Dynatrace AppSec
   20 vulnerabilities prioritised by impact
   3.3 days (4 x 20 = 80hrs)
   13.3 days (4 x 80 = 320hrs)
3. **Remediate 100 vulnerabilities**
   383.3 days saving (400 days –16.6 days)

HUGE developer time savings

OTHER USE CASES

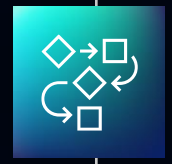
DEVELOP	RELEASE	OPERATE	PREDICT	PREVENT	RESOLVE	PROTECT	IMPROVE
 OBSERVABILITY-DRIVEN DEVELOPMENT	 PROGRESSIVE DELIVERY	 INFRASTRUCTURE OBSERVABILITY	 FORECASTING IN DATA ANALYTICS	 UNIFIED EXPOSURE PRIORITIZATION	 SLO ERROR BUDGET ALERTING	 PROTECT APPS FROM THE INSIDE	 KUBERNETES UTILIZATION IMPROVEMENT
 CONTINUOUS TESTING VALIDATION	 PIPELINE OBSERVABILITY	 KUBERNETES OBSERVABILITY	 FORECASTING IN WORKFLOWS	 CONTINUOUS SECURITY POSTURE AWARENESS	 AUTO-HEALING	 CONTEXTUALIZED THREAT DETECTION	 BUSINESS ALIGNMENT
 TEST PIPELINE OBSERVABILITY	 RELEASE VALIDATION	 CLOUD COST OPTIMIZATION	 PREDICTIVE OPERATIONS	 BUG PREVENTION	 INSTANT INTRUSION RESPONSE	 SOC NOISE REDUCTION	 ALWAYS-ON APP PROFILING
 AI MODEL VALIDATION	 ENGINEERING INTELLIGENCE	 AI RELIABILITY	 SRE AUTO PILOT	 ACCELERATED RESOLUTION	 INCIDENT AUTO-ROUTING	 SECURITY AS A SERVICE	 INCREASE SATISFACTION
 OBSERVABILITY AS A SERVICE	 BEHAVIOR VALIDATION	 KUBERNETES ORCHESTRATION	 AI COST MANAGEMENT	 DATA OBSERVABILITY	 ERROR INSPECTOR	 CENTRAL AUDIT LOGS	 SALESFORCE SPEED

OUR APPROACH IS RADICALLY DIFFERENT

THE DYNATRACE PLATFORM

CONTEXTUAL ANALYTICS

HYPERMODAL AI



AUTOMATION

61% less time analyzing service interruptions

Deutsche Telekom

Efficiency savings of 75% attributed to AIOps with Dynatrace

TD Bank

83% of engineers' time being productive versus 30% before

DELL Technologies

CONTEXTUAL ANALYTICS

HYPERMODAL AI

AUTOMATION

OBSERVABILITY PLAYS A VITAL ROLE IN SUPPORTING

YOUR BUSINESS TRANSFORMATION JOURNEY

THANK YOU