

Dynatrace Application Security

Bezpečne a plynulo

Július Loman



SECURITY JE TÍMOVÁ PRÁČA

Kde, ako a
čím sme
ovplyvnení?



Dev

Sme
zraniteľní?



Sec

Aký je
dopad?



Ops

POTREBUJEME INÝ PRÍSTUP

Komplexnosť aplikácií

“68% tvrdí, že komplexnosť software robí správu zraniteľností zložitou”¹

“58% z “kritických” zraniteľností sú false positive”¹

Neošetrené zraniteľnosti

“Vyriešenie zraniteľnosti priemerne trvá 96 dní”²

“Vypli sme blokovanie na WAF pre **priveľa false positive** hlásení”

Manuálne riešenia

“33% tímov používa automatizáciu pri vzájomnej kolaborácii”¹

“28% času stráveného pri riešení zraniteľností sa dá automatizovať”¹

Komplikovaná investigácia

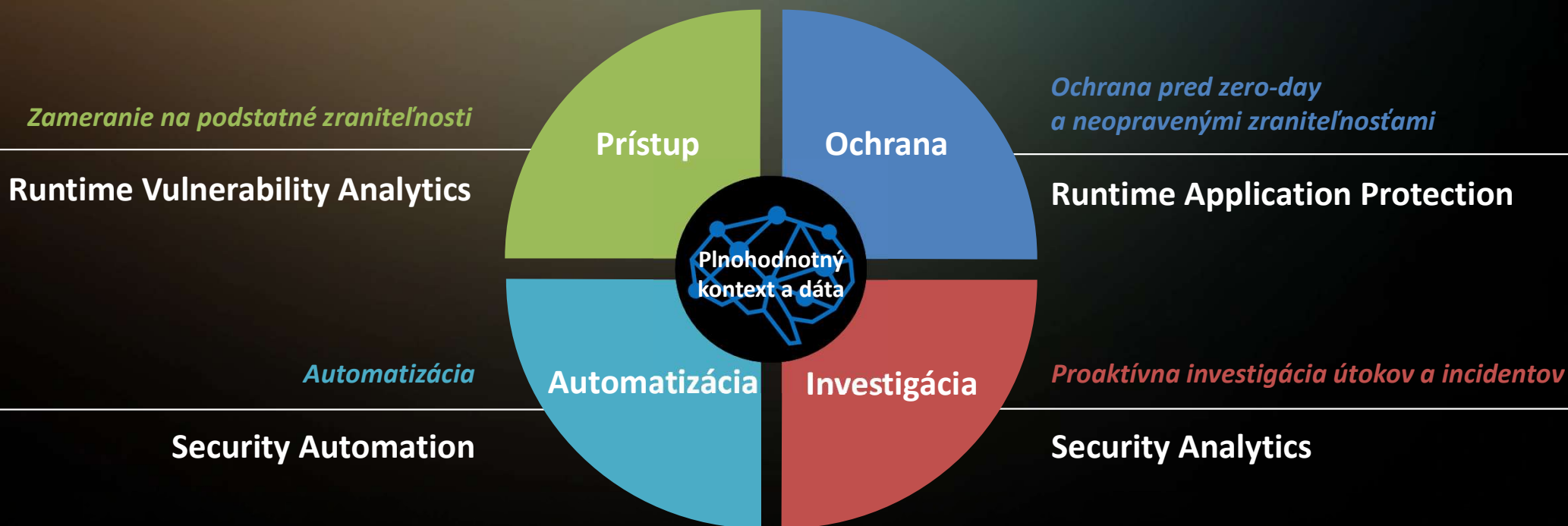
“55% tvrdí, že security dáta pre vyhodnocovanie sú naprieč systémami bez previazanosti kontextu”¹

“70% alertov nie je nikdy prešetrených”¹

1: Dynatrace 2023 CISO Research Report

2: Snyk 2022 State of Open source

PRÍSTUP OBSERVABILITY + SECURITY



PRÍKLAD LOG4SHELL ZRANITEĽNOSTI



Zraniteľnosť publikovaná na GitHub



Zraniteľnosť v zozname NVD



Zraniteľnosť v zozname Snyk

Live feed



AppSec vulnerability catalog aktualizovaný

Assessment



Zraniteľnosti zistená a okamžite vyhodnotená s Davis Security Score

Dec 10, 00:40am*

Dec 10, 10:15am

Dec 10, 10:45am

Dec 10, 10:50am

Dec 10, 11:05am

CVE-2021-44228 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. The information provided.

Current Description

Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages and other JNDI related endpoints. An attacker who can control log messages from LDAP servers when message lookup substitution is enabled. From Log4j2 releases (>2.10) this behavior can be mitigated by setting system property log4j2.formatMsgNoLookups to true. From Log4j2 releases (<2.10) by removing the JndiLookup class from the classpath org.apache.logging.log4j/core/lookup/JndiLookup.class).

snyk Vulnerability DB

Arbitrary Code Execution

Affecting org.apache.logging.log4j:log4j-core package.

10.0 CRITICAL

ATTACK COMPLEXITY: Low

SCOPE: Changed

CONFIDENTIALITY: High

INTEGRITY: High

AVAILABILITY: High

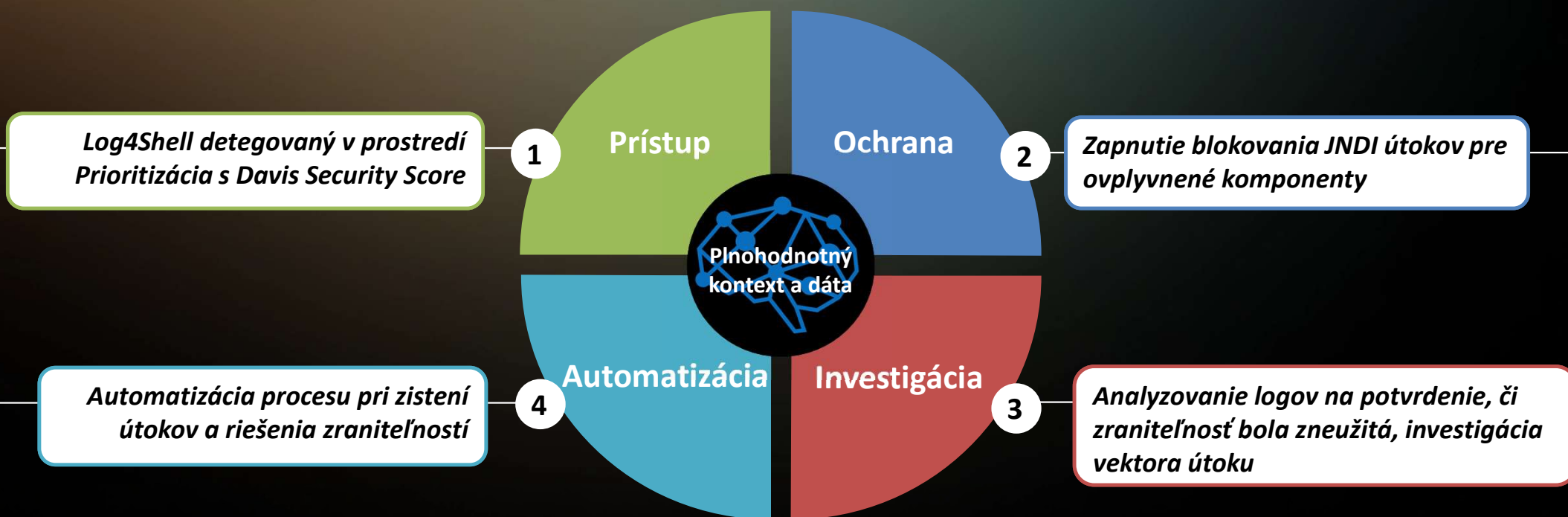
Public internet exposure
Exposure: Public network

Sensitive data assets
Affected: within range

Vulnerable functions
Not available

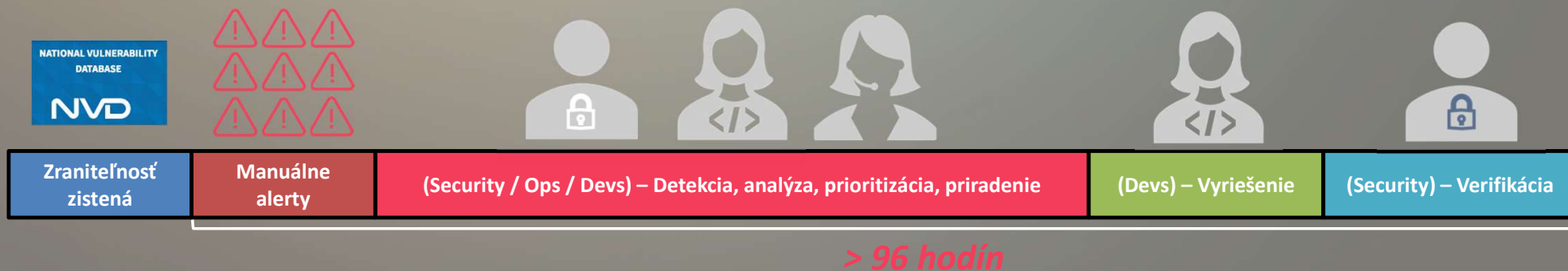
10 Critical risk

PRÍKLAD LOG4SHELL ZRANITEĽNOSTI

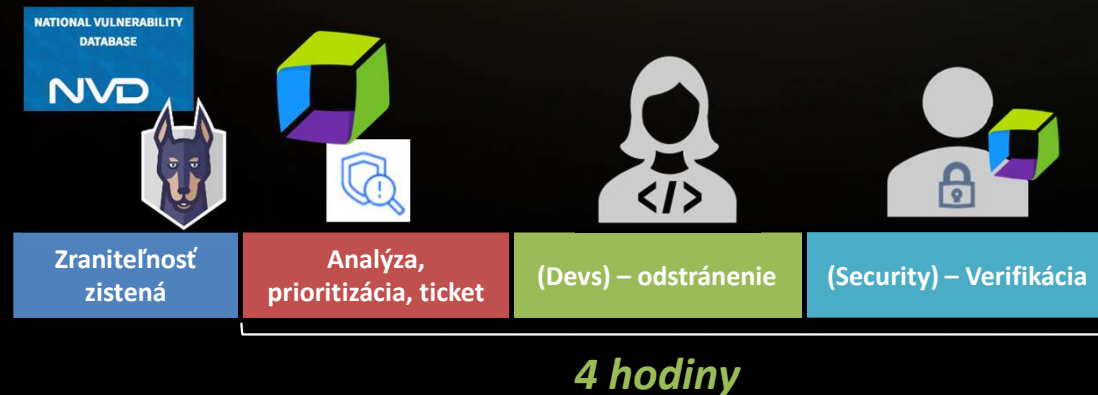


PRÍKLAD PROCESU RIEŠENIA ZRANITEĽNOSTI

Predtým



S Dynatrace



Skrátenie času o 95%

RUNTIME VULNERABILITY ANALYTICS

Alanata

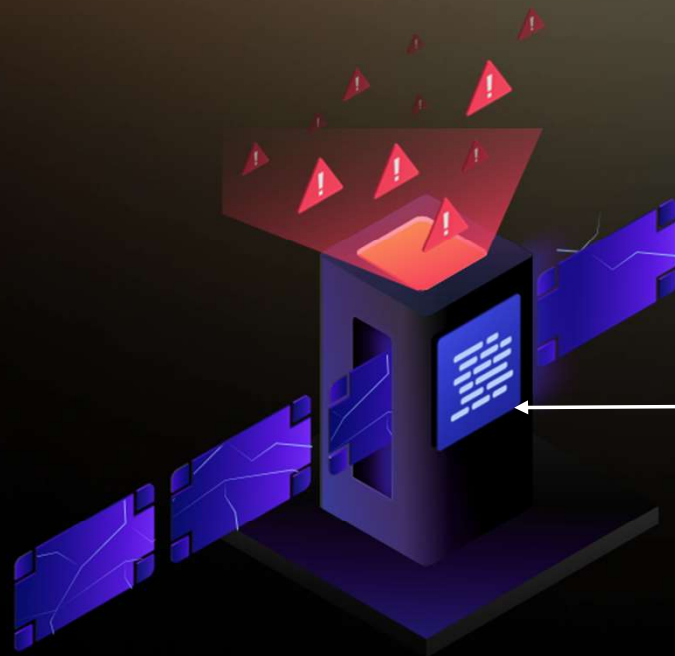
Technology Meets Business



RIEŠENIE ZRANITEĽNOSTÍ MUSÍ ŠKÁLOVAŤ S KOMPLEXNOSŤOU APLIKÁCIÍ A PROSTREDÍ

Code skenery

- Sú dobré v počiatočných fázach životného cyklu
- Priveľa alertov ako aj false positive
- Bez kontextu sa nedá prioritizovať



Zraniteľnosti sa môžu stále dostať do produkcie

Neprodukčné prostredia

Produkcia

Perimeter

ANALÝZA ZRANITEĽNOSTI POTREBUJE DÁTA

Sme vystavení zraniteľnosti?



Vo vnútri bežiacej aplikácie

- Používa sa kód so zraniteľnosťami?
- Aké aplikácie sú ovplyvnené?



Kontext prostredia

- Je aplikácia dostupná z internetu?
- Aplikácia komunikuje s inými rizikovými aplikáciami?



Hrozby

- Existuje verejne dostupný exploit?



Potenciálny dopad

- Aké entity v prostredí sú ovplyvnené?
- Sú ovplyvnené aj citlivé dáta? Z akých zdrojov?



Davis AI

Áno!
Aké je pre mňa
riziko a aké
zraniteľnosti mám
odstrániť najskôr?

PRIORITIZÁCIA PODĽA DÔLEŽITOSTI A DOPADU

Alanata
Technology Meets Business

Automaticky zanalyzuje runtime kontext využitím SmartScape topológie a dát

Prioritizuje pomocou Davis AI a security intelligence s využitím observability dát

Jednoducho môžeme odstrániť zraniteľnosť a urobiť ďalšie opatrenia

Third-party vulnerabilities 5-1394

Sandbox Bypass

Third-party vulnerability (SNYK-JS-VM2-5537100) first detected on May 16 at 04:47.

Settings

Public internet exposure Not detected

Reachable data assets Not detected

8.6 High risk

Exploit Exploit published

Process groups 1 affected

Vulnerable component vm2

Vulnerability details

Insights by snyk

8.6 High risk vulnerability
Davis Security Score

9.8 Critical risk vulnerability
CVSS as a base

Analyzed with Davis

Public internet exposure

Exposure	Impact on score	Risk level
Not determined	No changes	Critical risk

Reachable data assets

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

Process group overview

Process groups

Process groups in total	1
Affected process groups	1 (100%)
Resolved process groups	0 (0%)
Muted process groups	0 (0%)

Processes

Processes total	20
Affected processes	39
Exposed	0 (0%)

Most affected process groups

Process group	Status
---------------	--------

Prehľadne môžeme vidieť a vyriešiť zraniteľnosti v ľubovoľnom prostredí

SECURITY PROTECTION

Alanata
Technology Meets Business

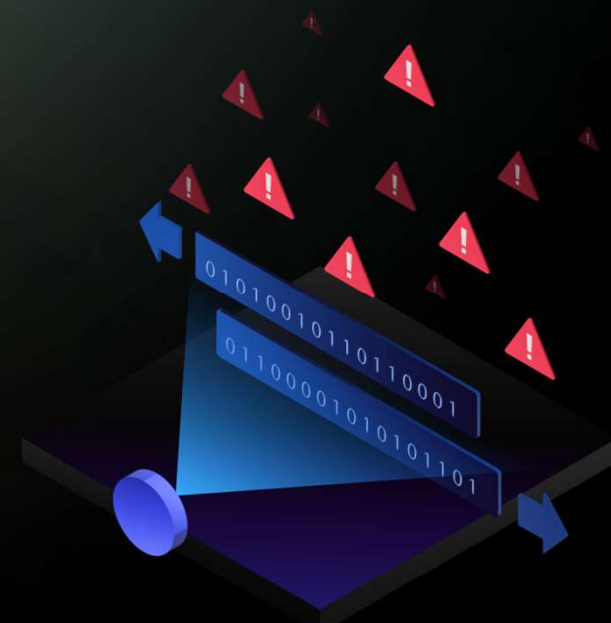


DETEKCIA ÚTOKOV

Alanata

Sieťové skenery

- Priveľa alertov a „false positives“
- Sú vhodné pre útoky na perimetri
- Pravidlá je potrebné často aktualizovať
- Nepoznajú kontext aplikácie



Spoľahlivá detekcia útokov a podozrivých aktivít potrebuje „full-stack“ viditeľnosť

Neprodukčné prostredia

Produkcia

Perimeter

RUNTIME APPLICATION PROTECTION

Detekcia a blokovanie
injection útokov

Vysoko presné,
bez alert storm,
minimum false positives

Bez dopadu na
používateľskú skúsenosť
alebo prevádzku

The screenshot displays the 'SQL injection attack details' page for attack A-29Z3ND. The interface includes a status summary, a detailed metadata section, and an attack path diagram.

Attack Summary:

- Public internet exposure: Not detected
- Reachable data assets: Within range
- Status: Exploited

Metadata:

- Process group instance: SpringBoot org.dynatrace.profileservice.ProfileServiceApplication unguard-profile-service-* (unguard-profile-service-5c89554cc4-2mm56)
- Vulnerability: SQL injection at DatabaseManager.updateBio():98
- Timestamp: May 21 22:37
- Source IP: 19.21.221.83

Attack path: Timestamp: May 21 22:37

The attack path diagram shows the following sequence:

- Source IP: 19.21.221.83
- Entry point: /user/2/bio
- Vulnerability: SQL injection DatabaseManager.updateBio():98
- Database: ./database/bio

Minimalizácia rizika z prehliadnutých a zero-day zraniteľností

OCHRANA PRIAMO V APLIKÁCI

Code-level vulnerabilities 5/1261

SQL injection at DatabaseManager.insertBio():81

5-1261: SpringBoot.org.dynatrace.profileservice.ProfileServiceApplication.unguard-profile-service-*

Public internet exposure: Not detected

Reachable data assets: Within range

Critical risk

Attacks: 6,095 | Processes affected: 1 | Type: SQL injection | Technology: Java

Detekcia
Code Level
zraniteľnosti

Detekcia a
blokovanie
útokov

Step 2: Define attack control for chosen criteria

Off | Monitor | Block

Monitor; incoming attacks detected only.

Off; incoming attacks NOT detected or blocked. Attacks will be ignored.

Monitor; incoming attacks detected only. Attacks will be recorded.

Block; incoming attacks detected and blocked. Attacks will be blocked.

```
Name
SQL injection at AccountDaoImpl.findUsersByUsernameAndPassword():40

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

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

SQL statement
select * from account where username='' or 1=1 -- 0' AND password=''
```

Odstránenie
zraniteľnosti

Investigácia
útokov,
nápravné
aktivity

Attack path

Timestamp: Sep 11 23:56

Source IP: 128.140.152.0

Entry point: /insecure-bank/login

Vulnerability: SQL Injection AccountDaoImpl.findUsersByUsernameAnd...

Database: Insecure-bank

Entry point details: URL: /insecure-bank/login

Vulnerability details: Name: SQL injection at AccountDaoImpl.findUsersByUsernameAndPassword():40

SECURITY ANALYTICS

Alanata
Technology Meets Business



OBSERVABILITY DÁTA = RÝCHLA A PRESNÁ INVESTIGÁCIA

Alanata
Technology Meets Business

Odfiltrovanie „šumu“
využitím observability,
topológie a kontextu

Rýchla investigácia hrozieb a
incidentov, jednoducho aj zo
starších dát

Tímová kolaborácia a
produktivita

The screenshot displays the Alanata observability platform interface. The main window shows a notebook titled "Copy of Logs for an IP" with a code editor containing the following query:

```
1 fetch logs
2 | filter contains(content, "172.31.7.152")
```

The results are displayed in a table with the following columns: content, timestamp, dt.entity.cloud_application, and dt.entity.cloud_application_instance. The table shows several log entries for the IP address 172.31.7.152, including requests for HTTP/1.1, simulated-browser-user, and unguard-envoy-proxy.

Below the first table, there is a section titled "Logs for an attacker IP" with a code editor containing the following query:

```
1 fetch logs
2 | filter contains(content, "172.31.7.152")
3 | parse content, "ld dqs:request space int:response_code ld ipaddr:ip"
4 | filter isNotNull(ip)
5 | fields timestamp, request, response_code, ip, dt.entity.process_group_instance
```

The results are displayed in a table with the same columns as the first table. The table shows several log entries for the IP address 172.31.7.152, including requests for HTTP/1.1, simulated-browser-user, and unguard-envoy-proxy.

PRÍKLAD - FORENZNÁ ANALÝZA ÚTOKU COMMAND INJECTION

- 1 Detekcia útoku typu command injection
- 2 Začneme s logmi z času útoku
- 3 Analýza logov zo súvisiacich entít
- 4 Preverenie trace dát s podozrivými logmi
- 5 Analýza volaní z podozrivých IP adries

Third-party vulnerabilities 5-985

Arbitrary Command Injection

Third-party vulnerability (SNYK-JAVA-COMZAXXER-3033308) first detected on January 31 at 08:41.

Settings

Public internet exposure
Public network

Reachable data assets
Within range

Vulnerable functions
Not available

9.8
Critical risk

Exploit
No exploit published

Process groups
1 affected

Vulnerable component
nuprocess

Change status

Vulnerability details

Insights by snyk

Description

Affected versions of this package are vulnerable to Arbitrary Command Injection due to improper user-input sanitization, allowing attackers to use NUL characters in their strings in order to craft a malicious payload.

** Note: ** Java's ProcessBuilder isn't vulnerable because of a check in ProcessBuilder.start. NuProcess is missing that check.

This vulnerability can only be exploited to inject command line arguments on Linux.

For more information visit [SNYK](#)

CVE [CVE-2022-39243](#)

OWASP [2021-A3](#), [2021-A6](#)

CWE [CWE-77](#)

Technology

Java

Process group overview

Process groups

Process groups in total	1
Affected process groups	1 (100%)
Resolved process groups	0 (0%)
Muted process groups	0 (0%)

Processes

Processes total	2
Affected processes	1
Exposed	1 (100%)

Legend: Affected (red), Resolved (green), Muted (grey)

SECURITY AUTOMATION

Alanata
Technology Meets Business



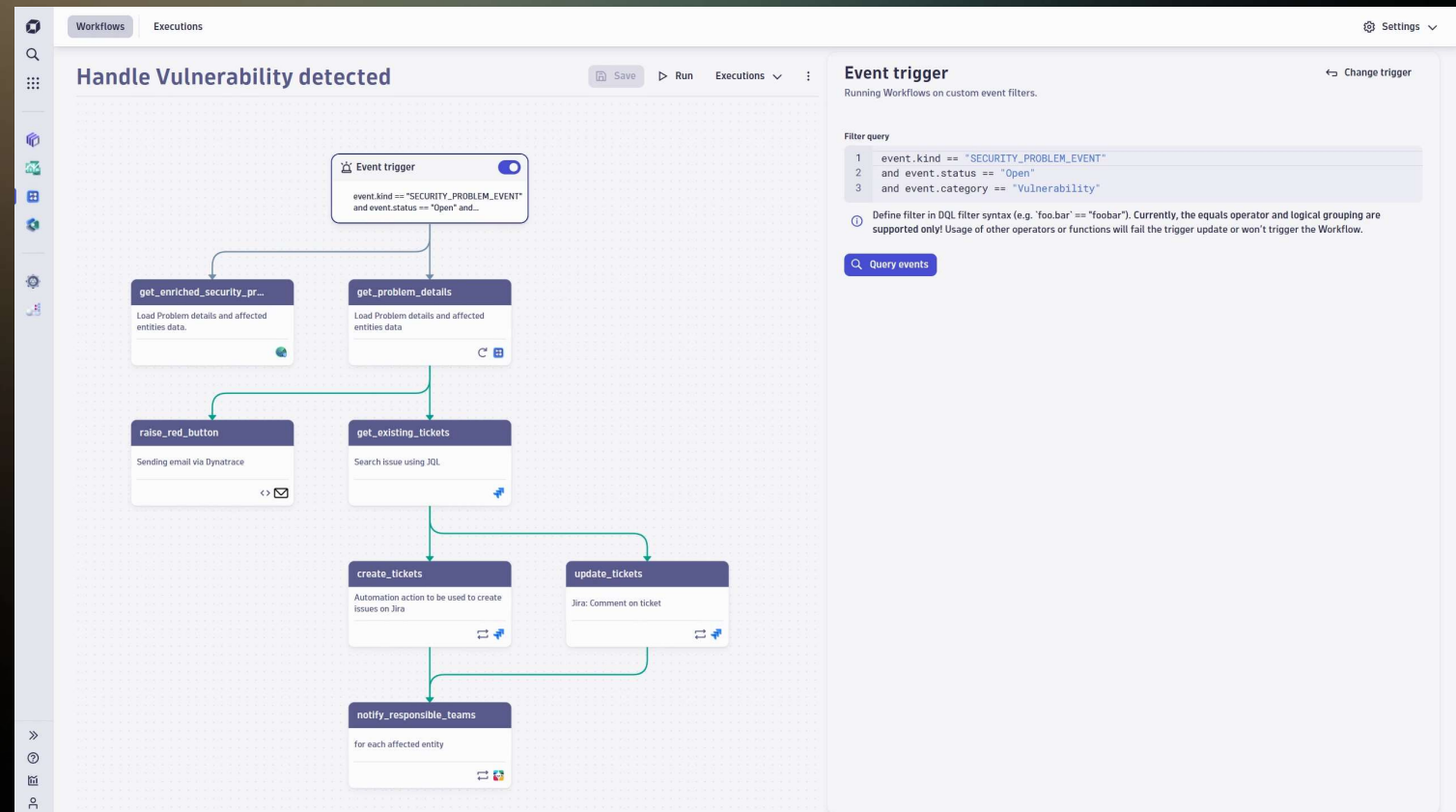
PLYNULO S DYNATRACE AUTOMATION ENGINE

Alanata
Technology Meets Business

Prehľadne a jednoducho
môžeme vytvoriť
workflow automatizácie

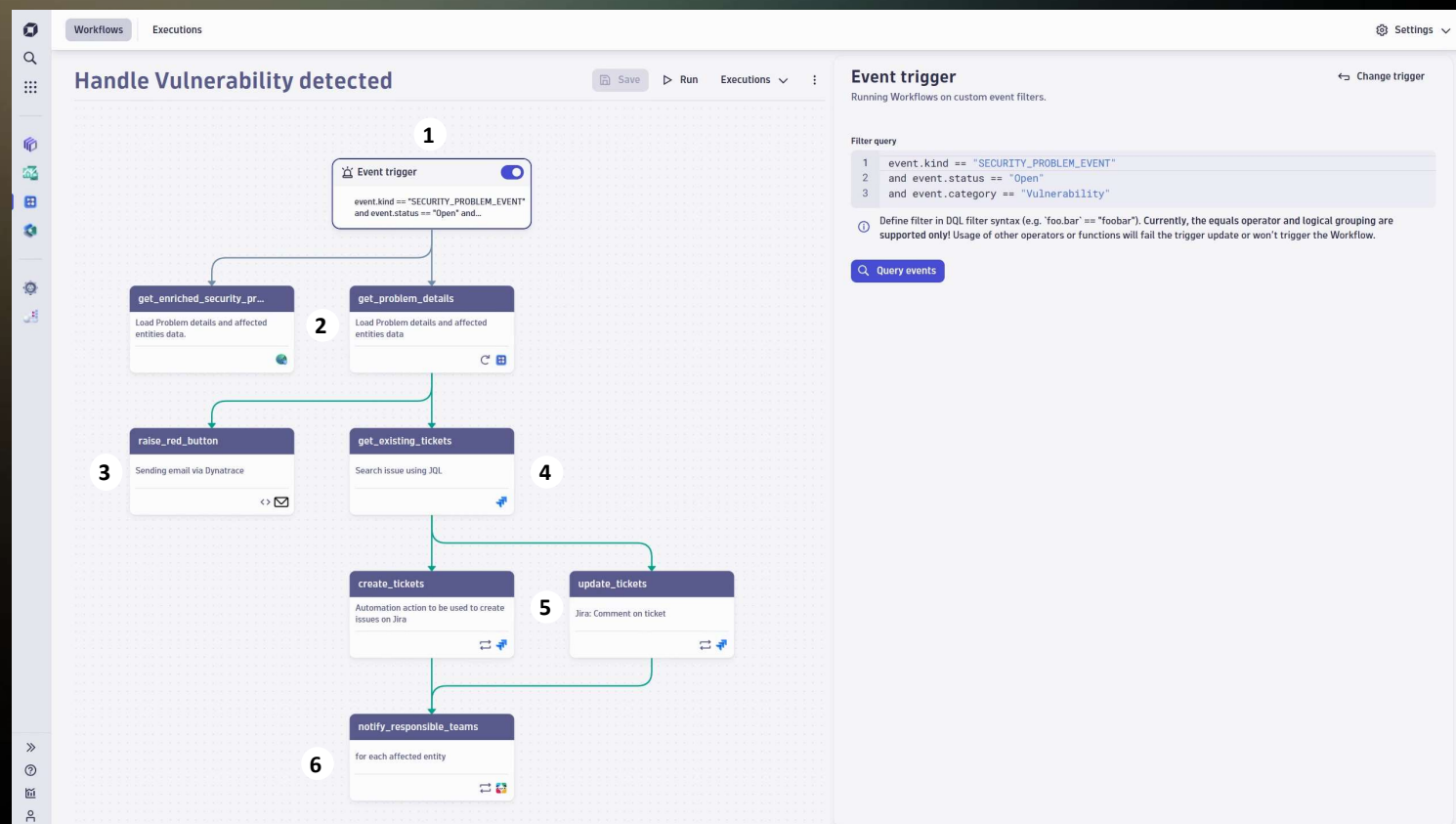
Akonáhle Davis AI zistí
zraniteľnosti je možné
automaticky spustiť
workflow

Možné ďalšie
vyhodnocovanie, dotazy
na iné systémy a dáta,
notifikácie, ...



PRÍKLAD – AUTOMATIZOVANÝ PROCES NA ZISTENIE A RIEŠENIE ZRANITEĽNOSTI

- 1 Workflow spustený keď Davis zistí zraniteľnosť - “Security Problem Event” - “vulnerability”
- 2 Zistí detaily problému, informácie o zraniteľnosti a ovplyvnených entitách
- 3 Okamžite notifikuje CISO ak ide o kritickú zraniteľnosť
- 4 Vyhľadá existujúce JIRA tickety súvisiace s problémom
- 5 Vytvorí (alebo aktualizuje) JIRA ticket s detailmi problému
- 6 Notifikuje zodpovedné tímy



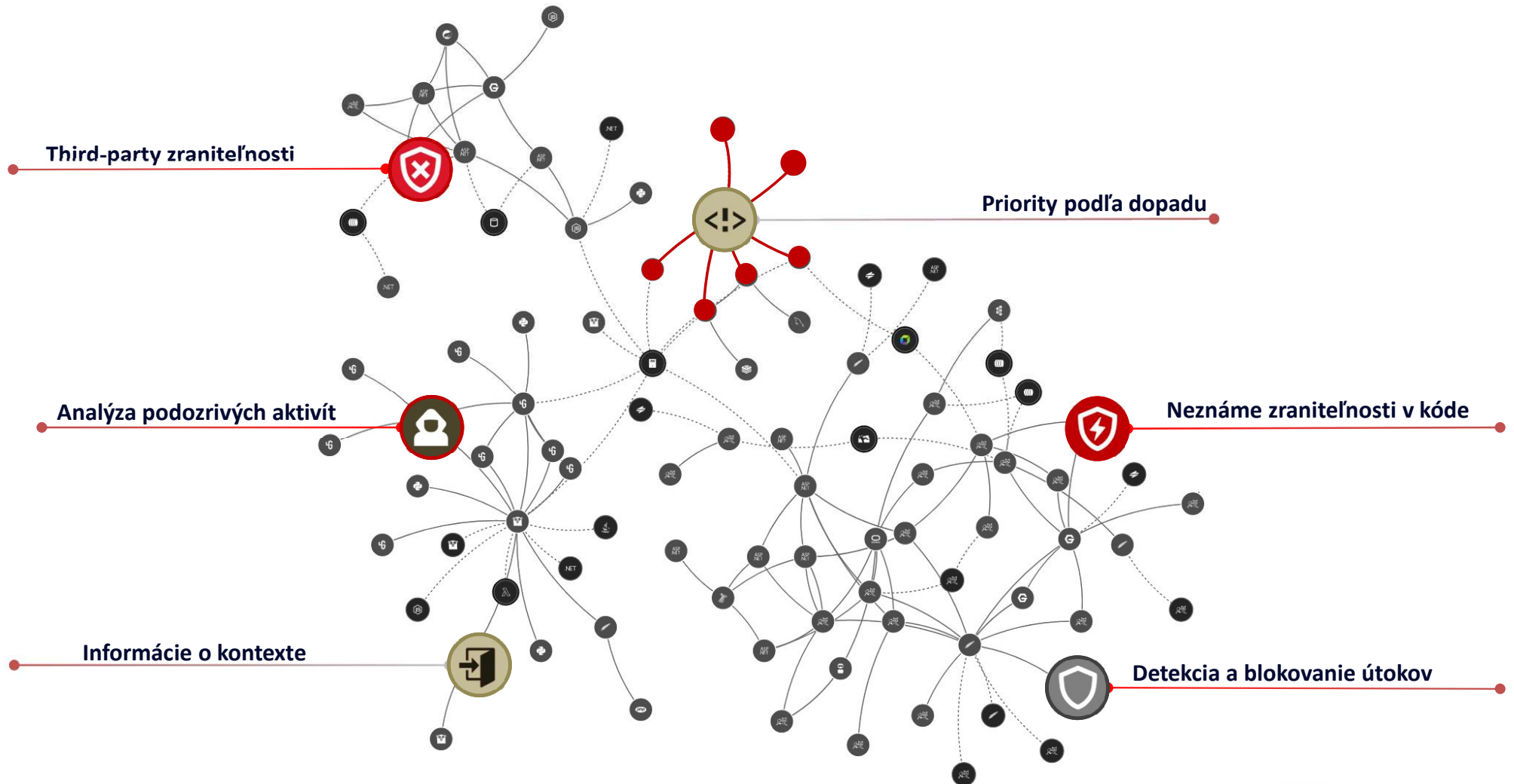
AKO TO FUNGUJE SPOLU?

Alanata
Technology Meets Business

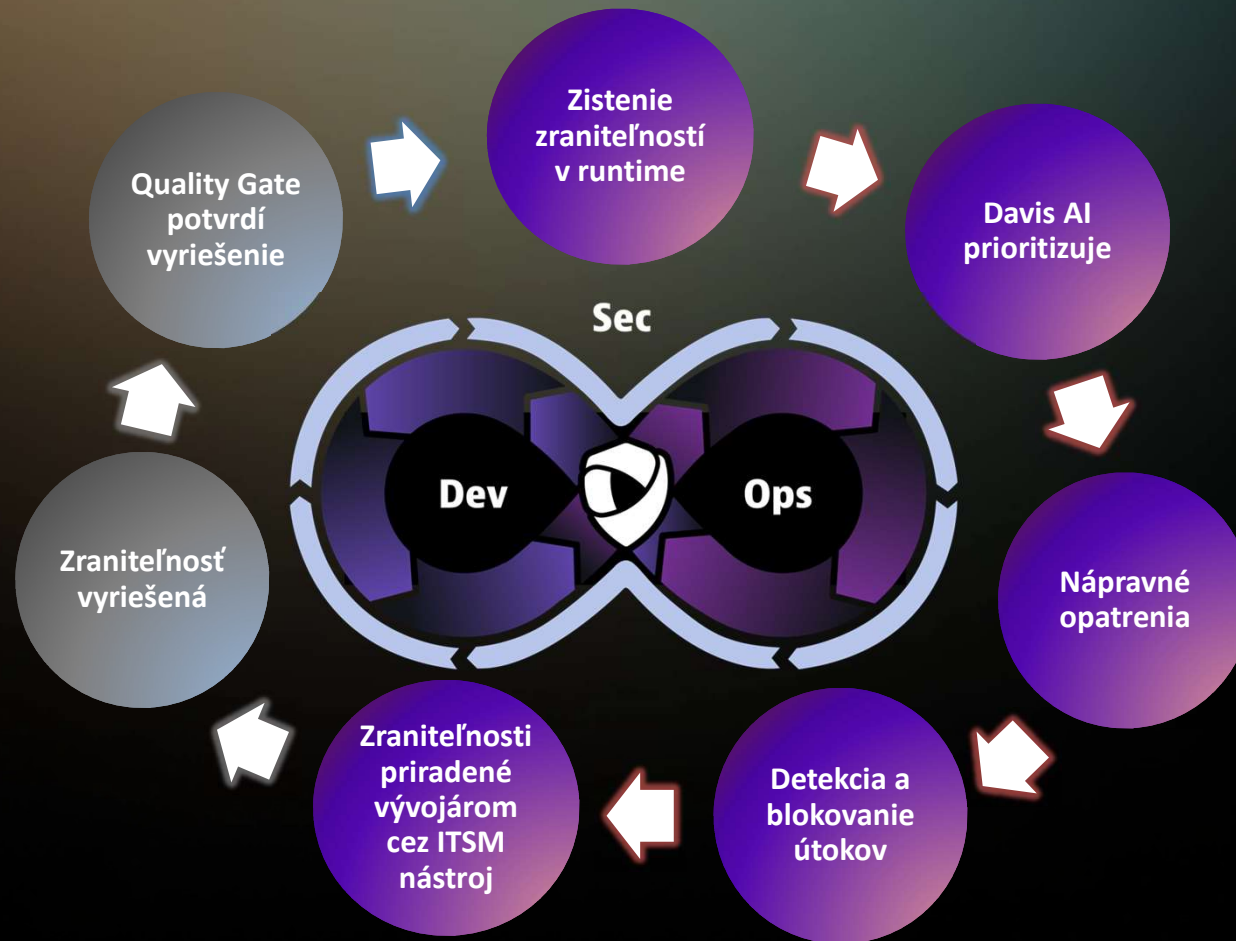


OBSERVABILITY + SECURITY

Alanata

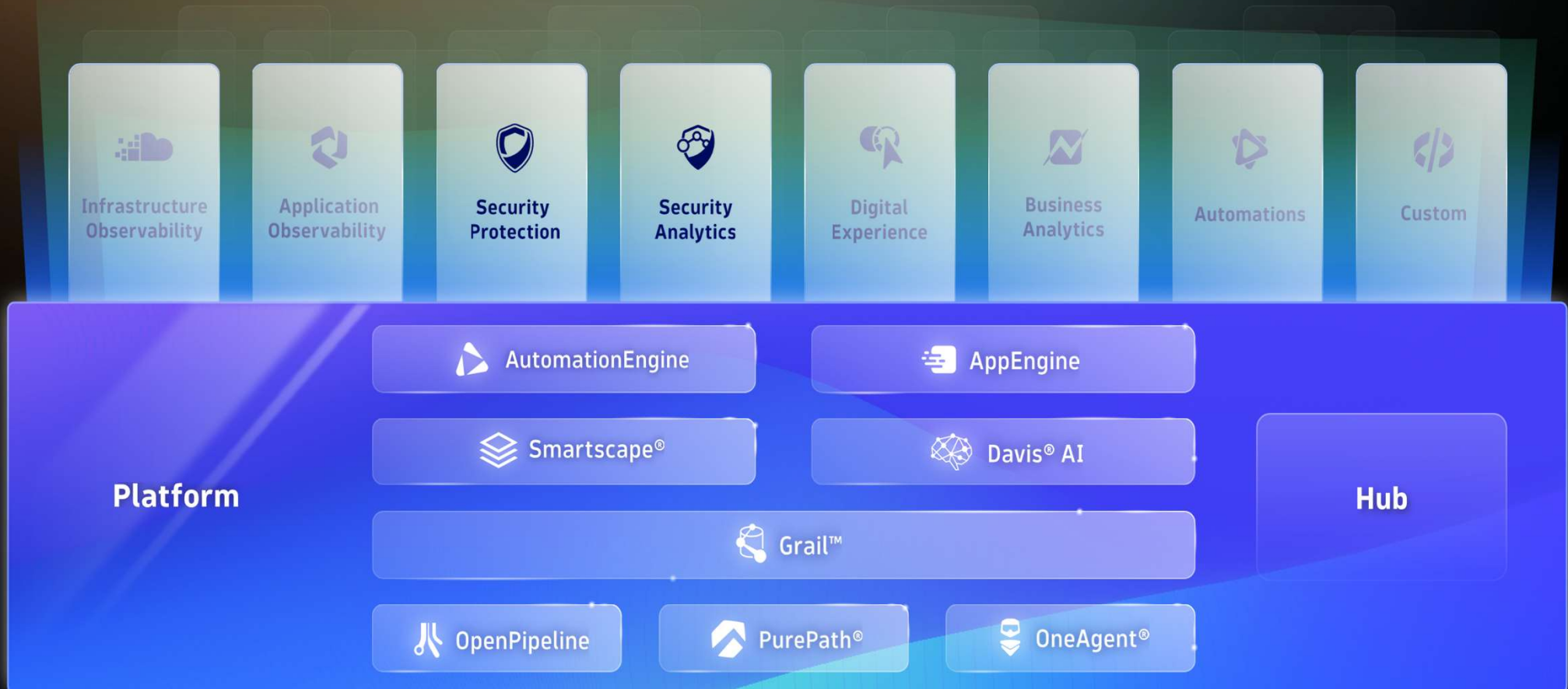


SECURITY A OBSERVABILITY V DEVSECOPS



POSTAČÍ IBA ZAPNŮŤ

Application security moduly sú priamo súčasťou Dynatrace platformy





CLOUD DONE RIGHT

Alanata

Technology Meets Business

Alanata a.s.

Einsteinova Business Center

Krasovského 14

851 01 Bratislava 5

Slovenská republika

www.alanata.sk