Dynatrace Application Security

Bezpečne a plynulo

Július Loman

SECURITY JE TÍMOVÁ PRÁCA

Alanata
Technology Meets Business

POTREBUJEME INÝ PRÍSTUP

Alanata
Technology Meets Business

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

Alanata
Technology Meets Business

Zameranie na podstatné zraniteľnosti

Runtime Vulnerability Analytics

Ochrana pred zero-day a neopravenými zraniteľnosťami

Runtime Application Protection

Automatizácia

Security Automation

Proaktívna investigácia útokov a incidentov

Security Analytics

PRÍKLAD LOG4SHELL ZRANITEĽNOSTI

Alanata
Technology Meets Business

Live feed

Assessment

Zraniteľnosť publikovaná na GitHub

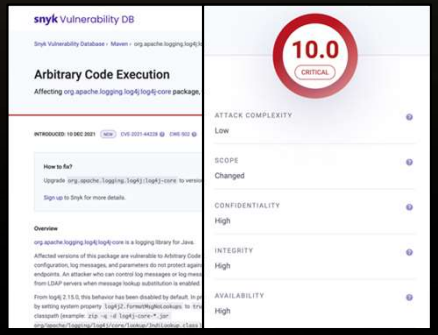
Dec 10, 00:40am*

Zraniteľnosť v zozname NVD

Dec 10, 10:15am

Zraniteľnosť v zozname Snyk

Dec 10, 10:45am



AppSec vulnerability catalog aktualizovaný

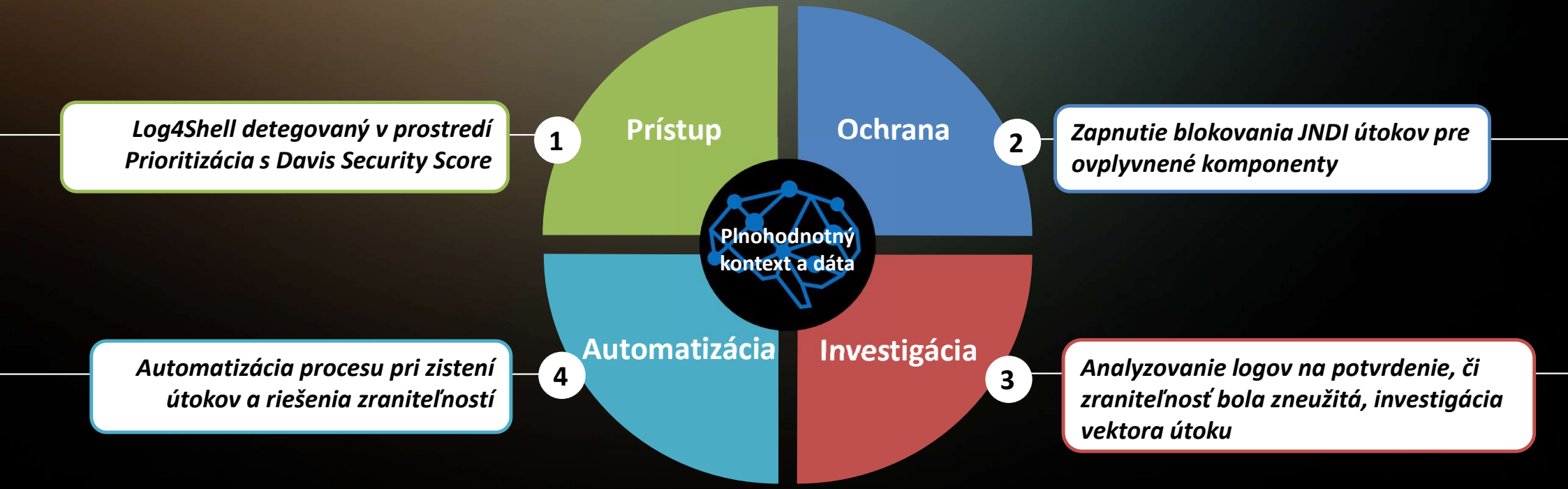
Dec 10, 10:50am

Zraniteľnosti zistená a okamžite vyhodnotené s Davis Security Score

Dec 10, 11:05am

PRÍKLAD LOG4SHELL ZRANITEĽNOSTI

Alanata
Technology Meets Business



1 *Log4Shell detegovaný v prostredí Prioritizácia s Davis Security Score*

2 *Zapnutie blokovania JNDI útokov pre ovplyvnené komponenty*

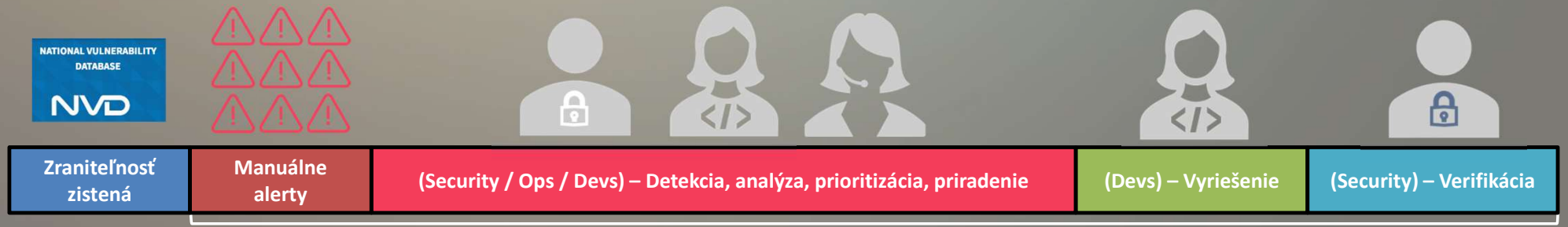
3 *Analyzovanie logov na potvrdenie, či zraniteľnosť bola zneužitá, investigácia vektora útoku*

4 *Automatizácia procesu pri zistení útokov a riešenia zraniteľností*

PRÍKLAD PROCESU RIEŠENIA ZRANITEĽNOSTI

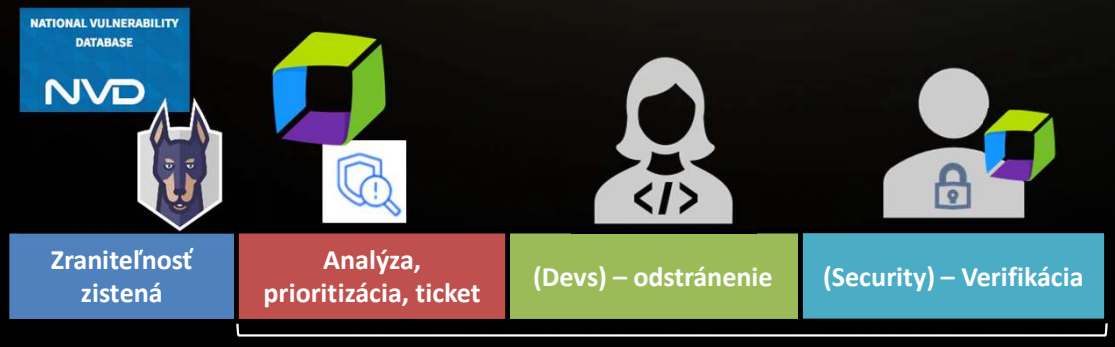
Alanata
Technology Meets Business

Predtým



> 96 hodín

S Dynatrace



4 hodiny

Skrátenie času o 95%

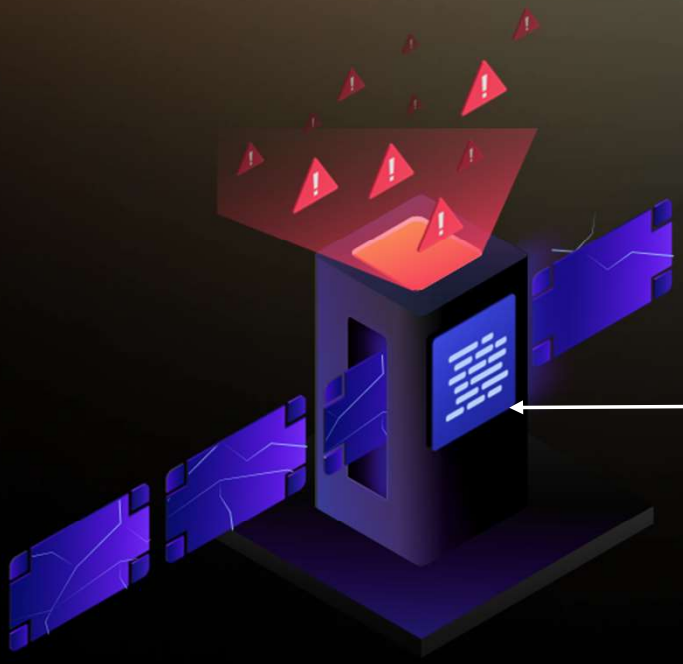
RUNTIME VULNERABILITY ANALYTICS

Alanata

Technology Meets Business

RIEŠENIE ZRANITEĽNOSTÍ MUSÍ ŠKÁLOVAŤ S KOMPLEXNOSŤOU APLIKÁCIÍ A PROSTREDÍ

Alanata
Technology Meets Business



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

Alanata
Technology Meets Business

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?

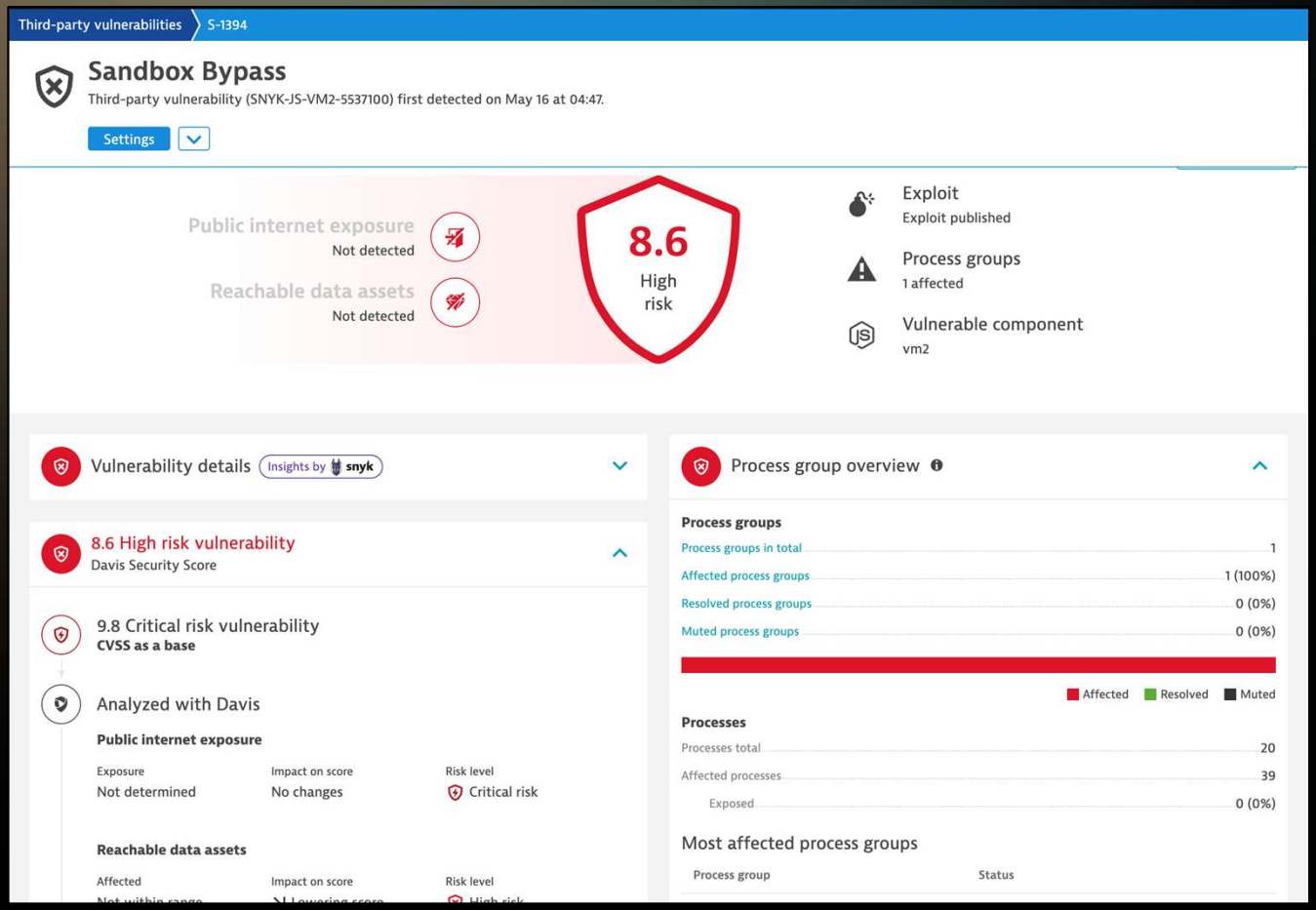
PRIORITIZÁCIA PODĽA DÔLEŽITOSTI A DOPADU

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



Prehľadne môžeme vidieť a vyriešiť zraniteľnosti v ľubovoľnom prostredí

SECURITY PROTECTION

Alanata

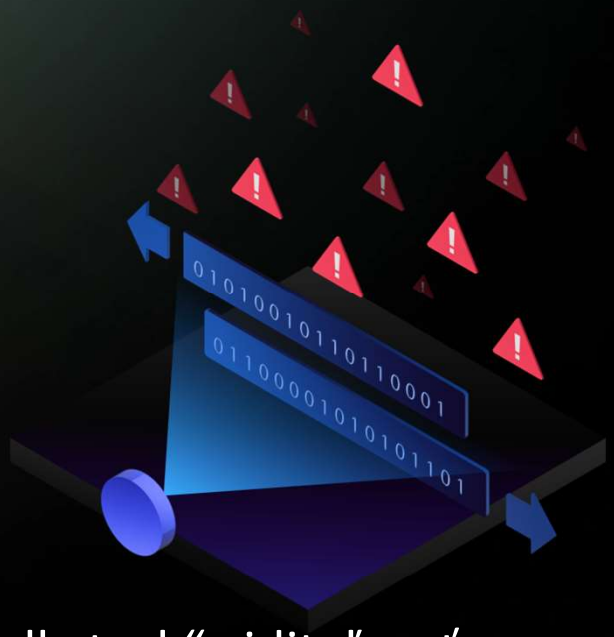
Technology Meets Business

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

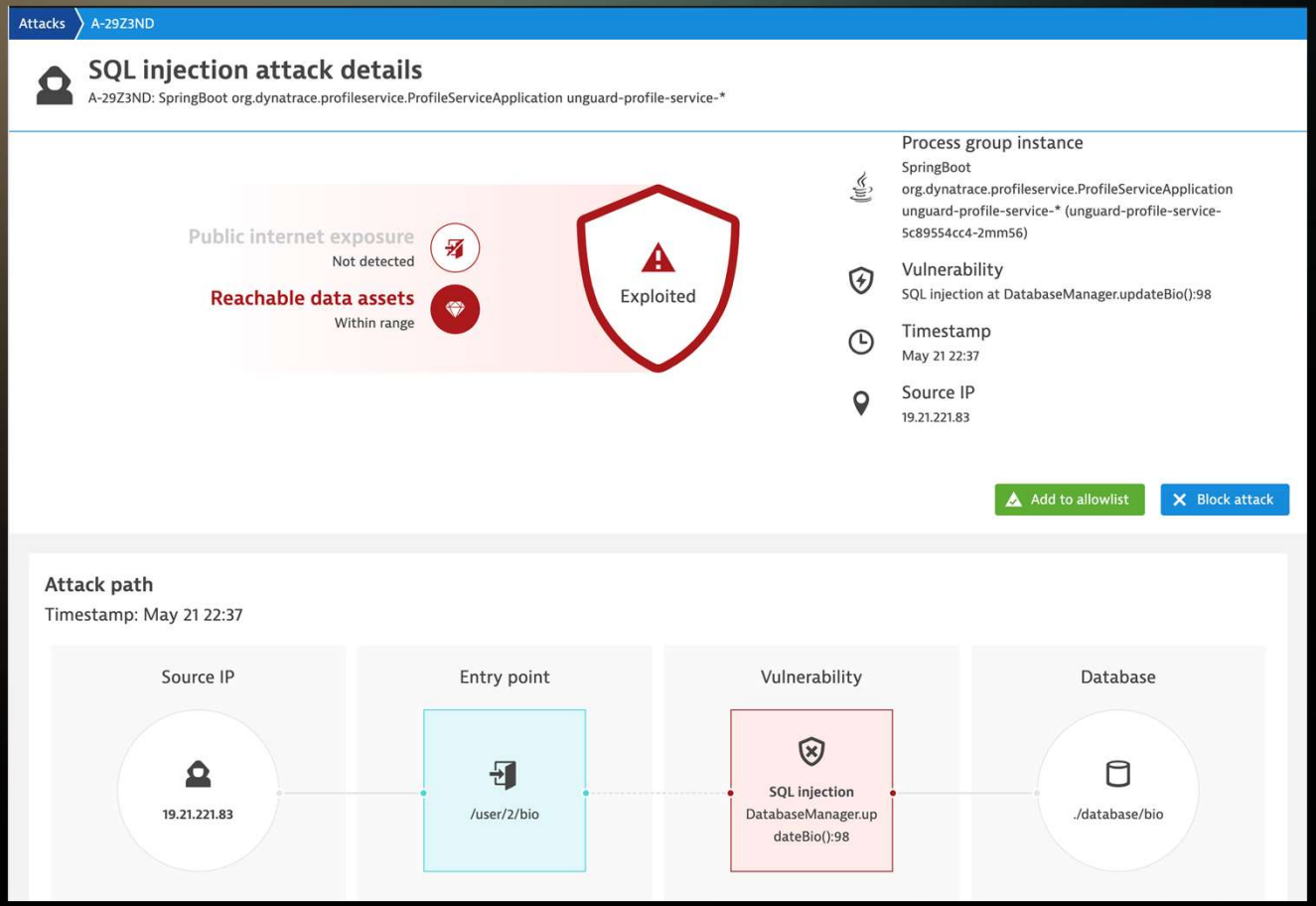
RUNTIME APPLICATION PROTECTION

Alanata
Technology Meets Business

Detekcia a blokovanie injection útokov

Vysoko presné, bez alert storm, minimum false positives

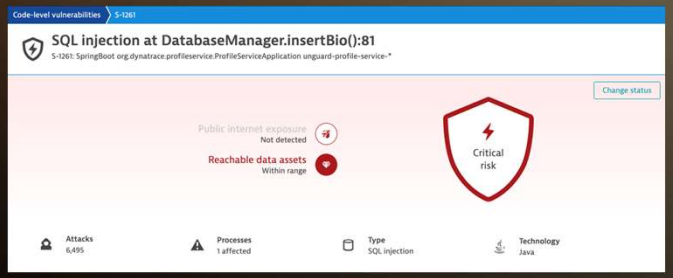
Bez dopadu na používateľskú skúsenosť alebo prevádzku



Minimalizácia rizika z prehliadnutých a zero-day zraniteľností

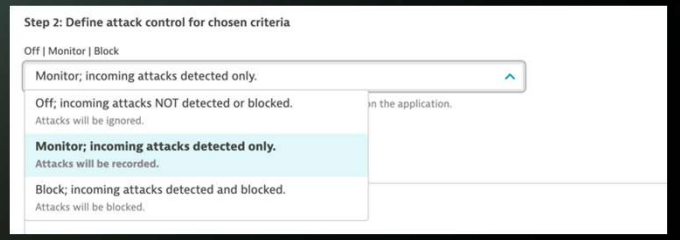
OCHRANA PRIAMO V APLIKÁCII

Alanata
Technology Meets Business



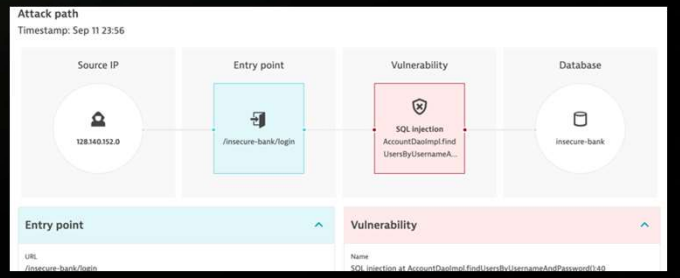
Detekcia Code Level zraniteľnosti

Detekcia a blokovanie útokov



Odstránenie zraniteľnosti

Investigácia útokov, nápravné aktivity



SECURITY ANALYTICS

Alanata

Technology Meets Business

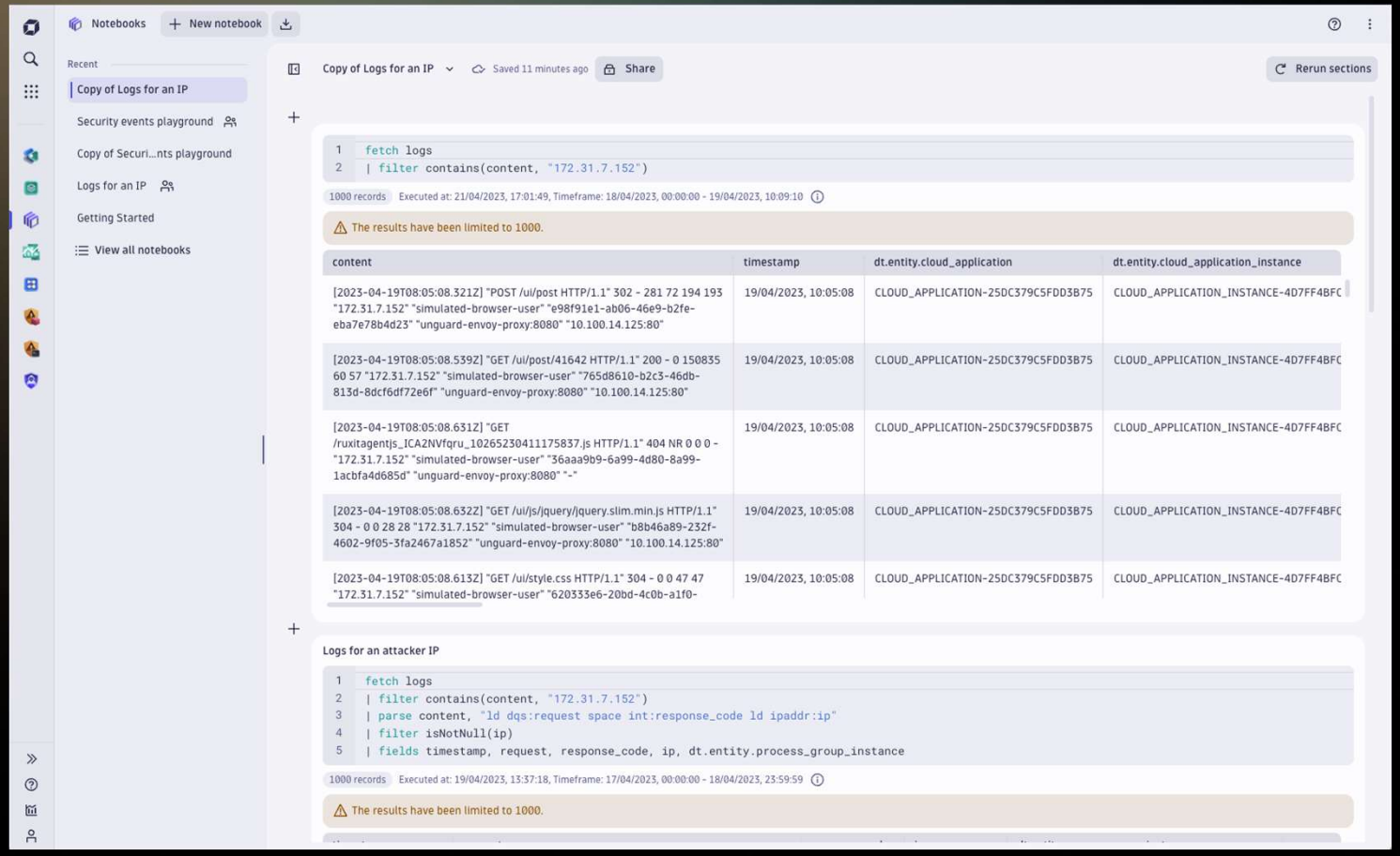
OBSERVABILITY DÁTA
= RÝCHLA A PRESNÁ INVESTIGÁCIA

Alanata
Technology Meets Business

Odfiltrovanie „šumu“ využitím observability, topológie a kontextu

Rýchla investigácia hrozieb a incidentov, jednoducho aj zo starších dát

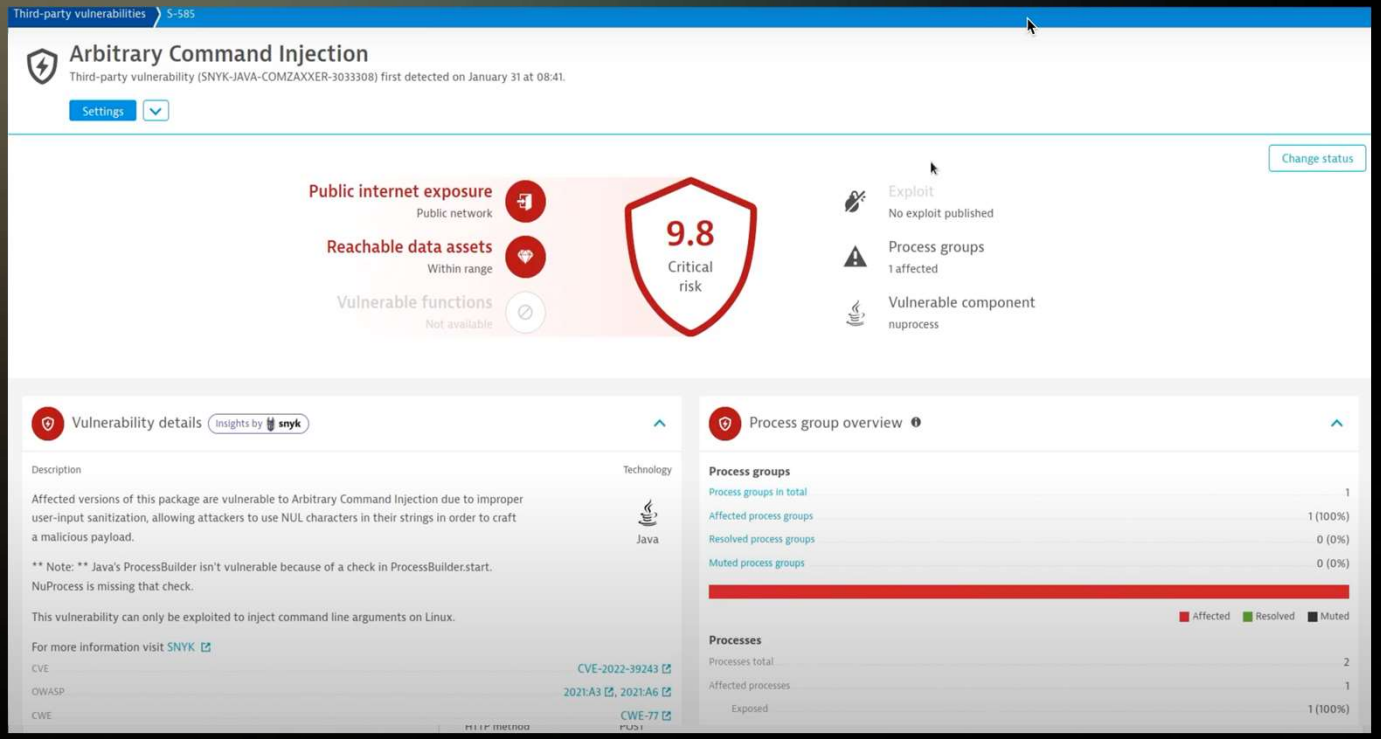
Tímová kolaborácia a produktivita



PRÍKLAD - FORENZNÁ ANALÝZA ÚTOKU COMMAND INJECTION

Alanata
Technology Meets Business

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



SECURITY AUTOMATION

Alanata

Technology Meets Business

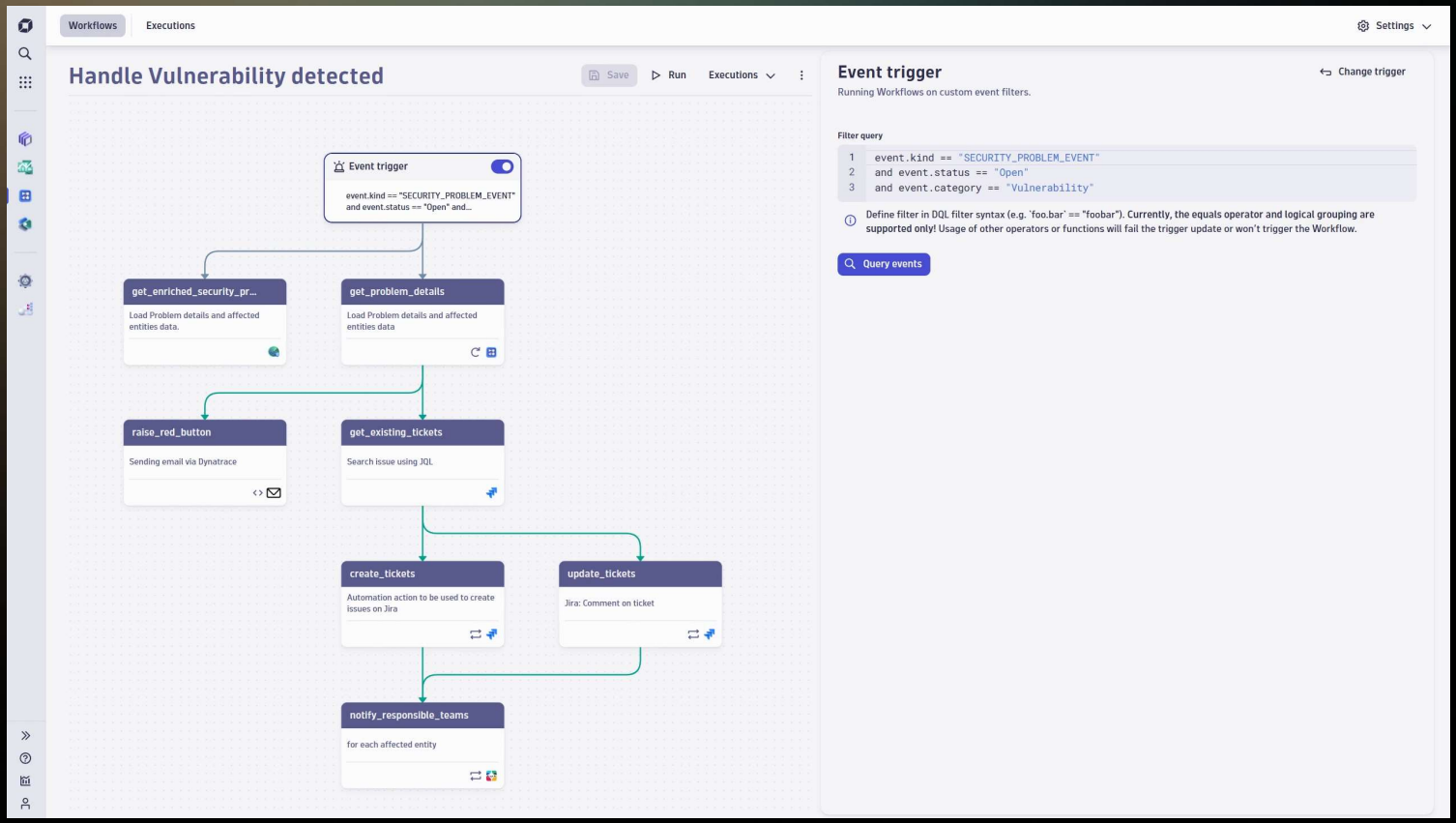
PLYNULO S DYNATRACE AUTOMATION ENGINE

Alanata
Technology Meets Business

Prehľadne a jednoducho môžeme vytvoriť workflow automatizácie

Akonáhle Davis AI zistí zraniteľnosti je možné automaticky spustiť workflow

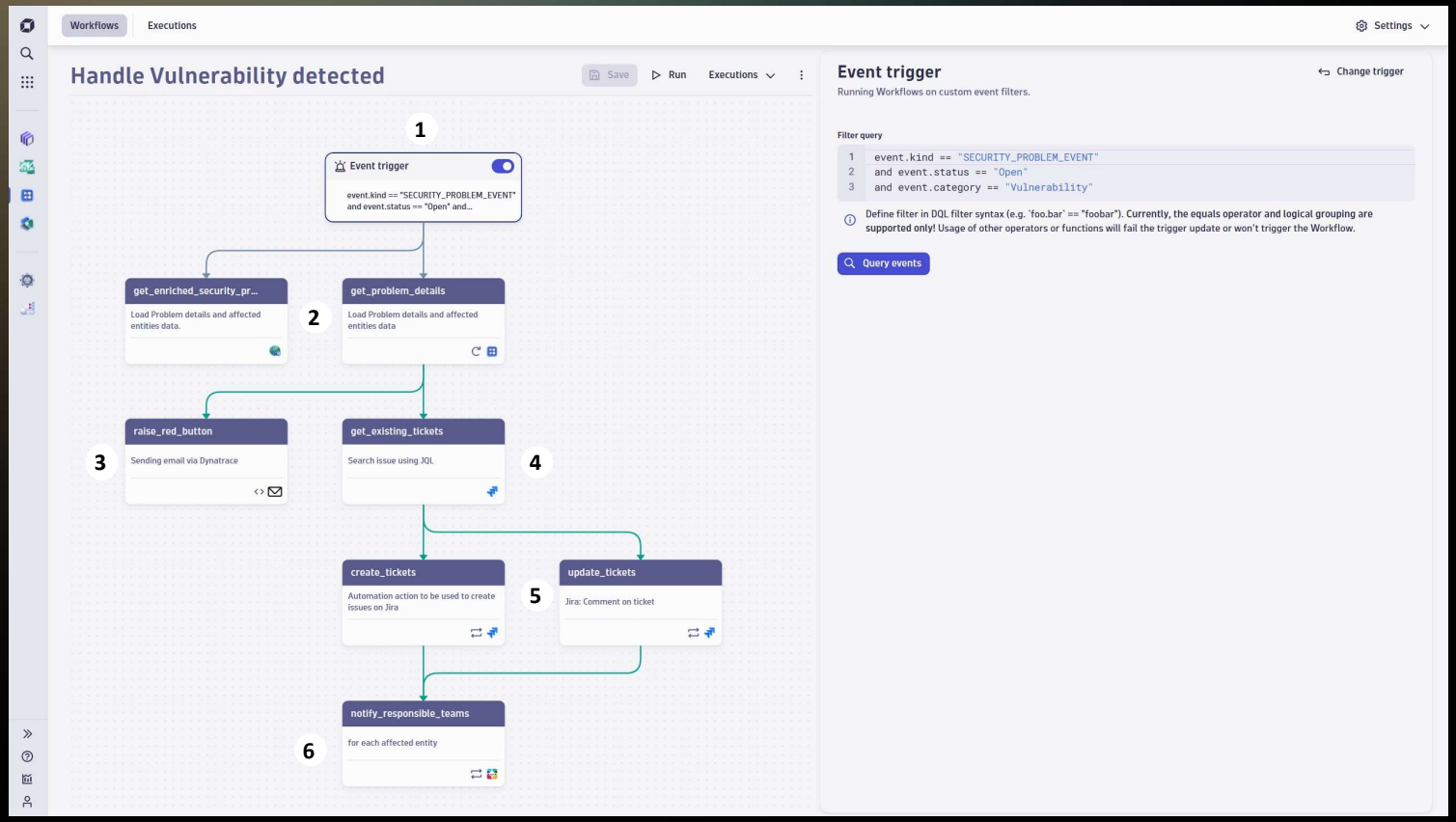
Možné ďalšie vyhodnocovanie, dotazy na iné systémy a dáta, notifikácie, ...



PRÍKLAD – AUTOMATIZOVANÝ PROCES NA ZISTENIE A RIEŠENIE ZRANITEĽNOSTI

Alanata
Technology Meets Business

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



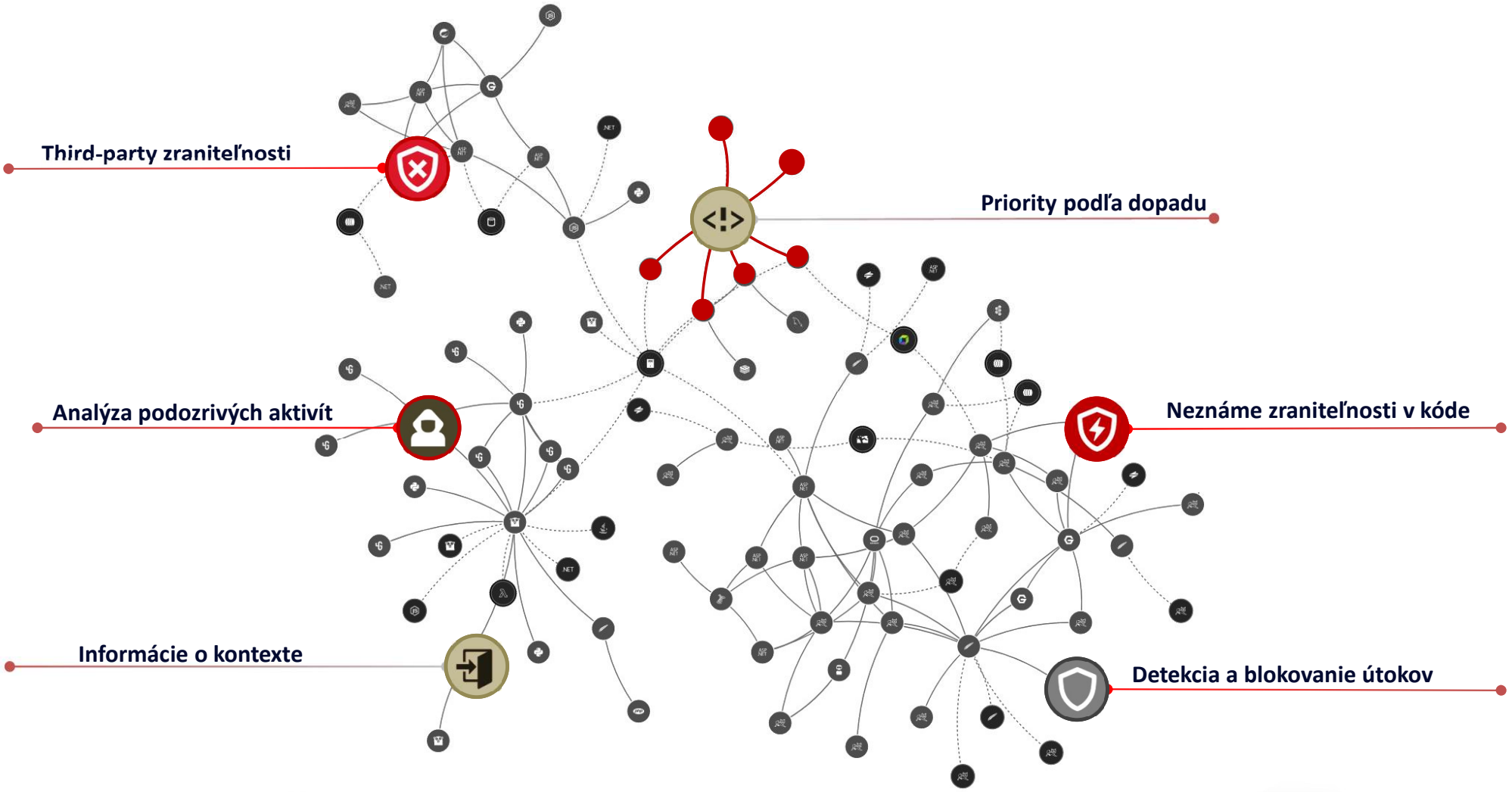
AKO TO FUNGUJE SPOLU?

Alanata

Technology Meets Business

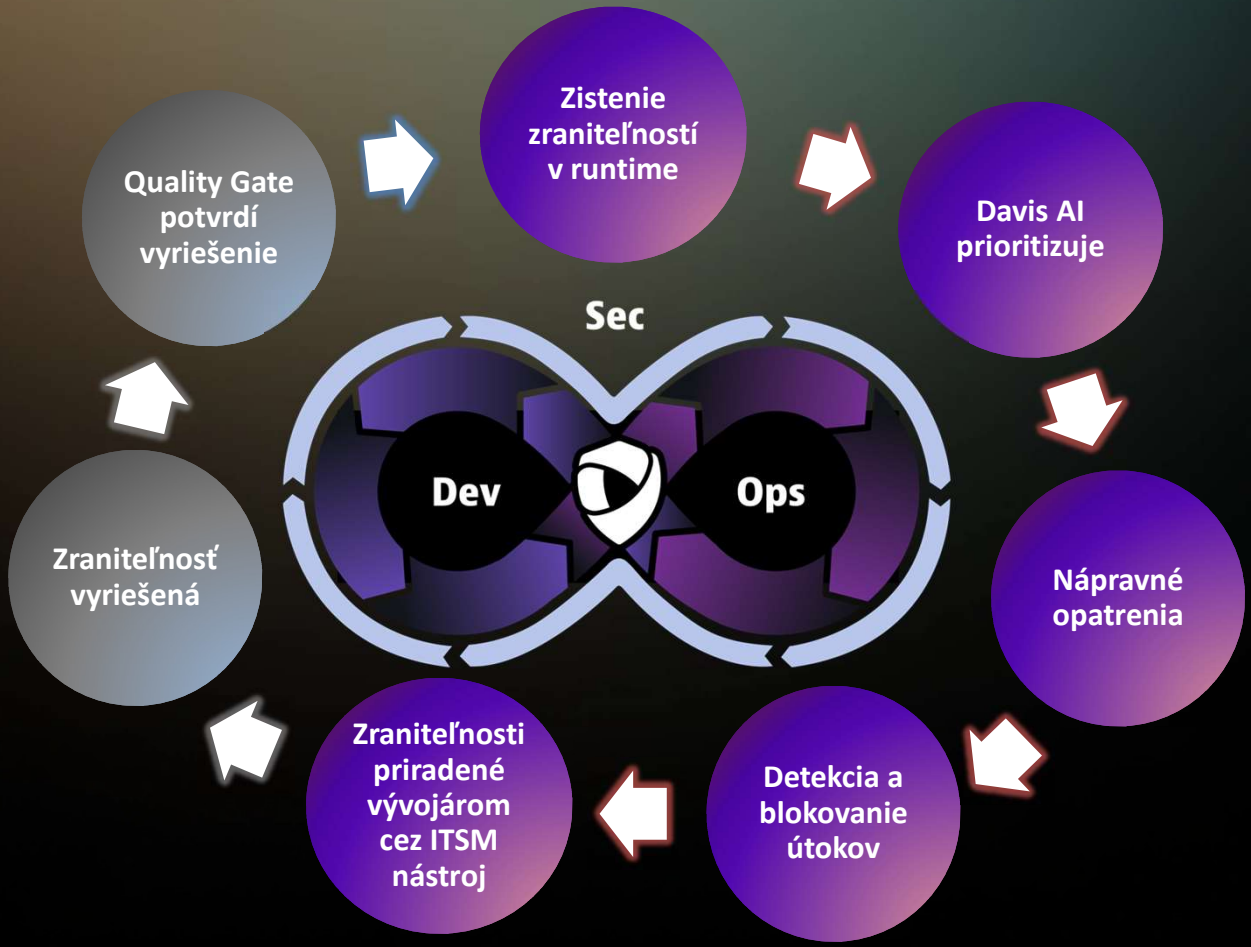
OBSERVABILITY + SECURITY

Alanata



SECURITY A OBSERVABILITY V DEVSECOPS

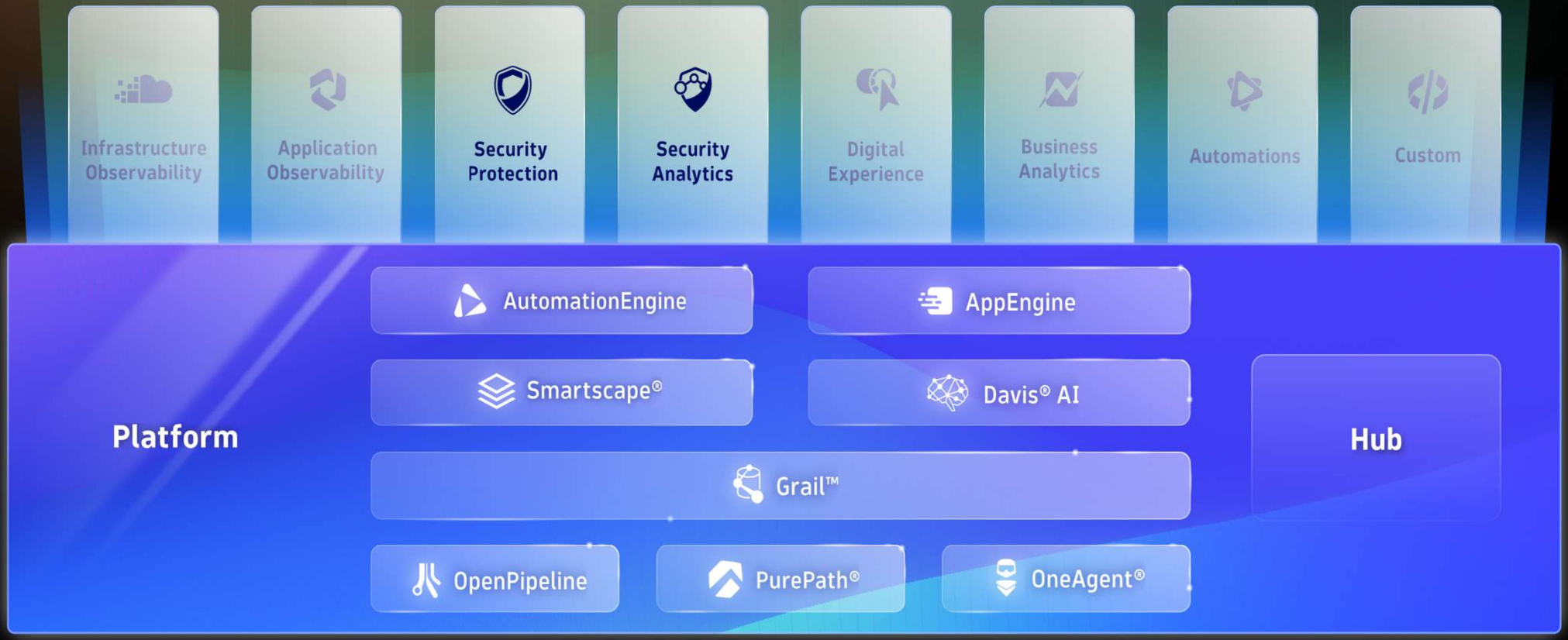
Alanata
Technology Meets Business



POSTAČÍ IBA ZAPNÚŤ

Alanata
Technology Meets Business

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