COMGUARD

cyber security masters

Problematika zranitel'ností v praxi

Ondrej Malík

20.09.2024

Teória zraniteľností

Zraniteľnosť vs. Miskonfigurácia

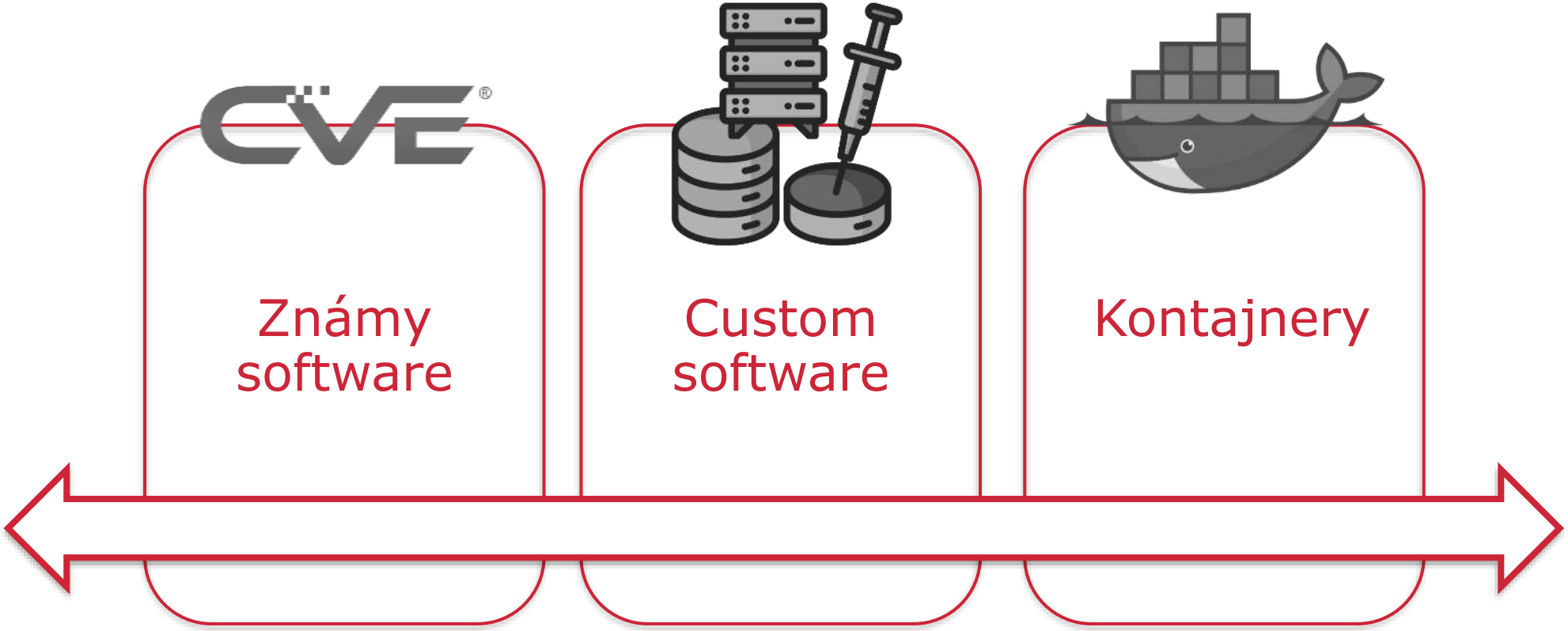
Zraniteľnosť je bezpečnostná chyba priamo v software

Oprava je priamo závislá na vendorovi

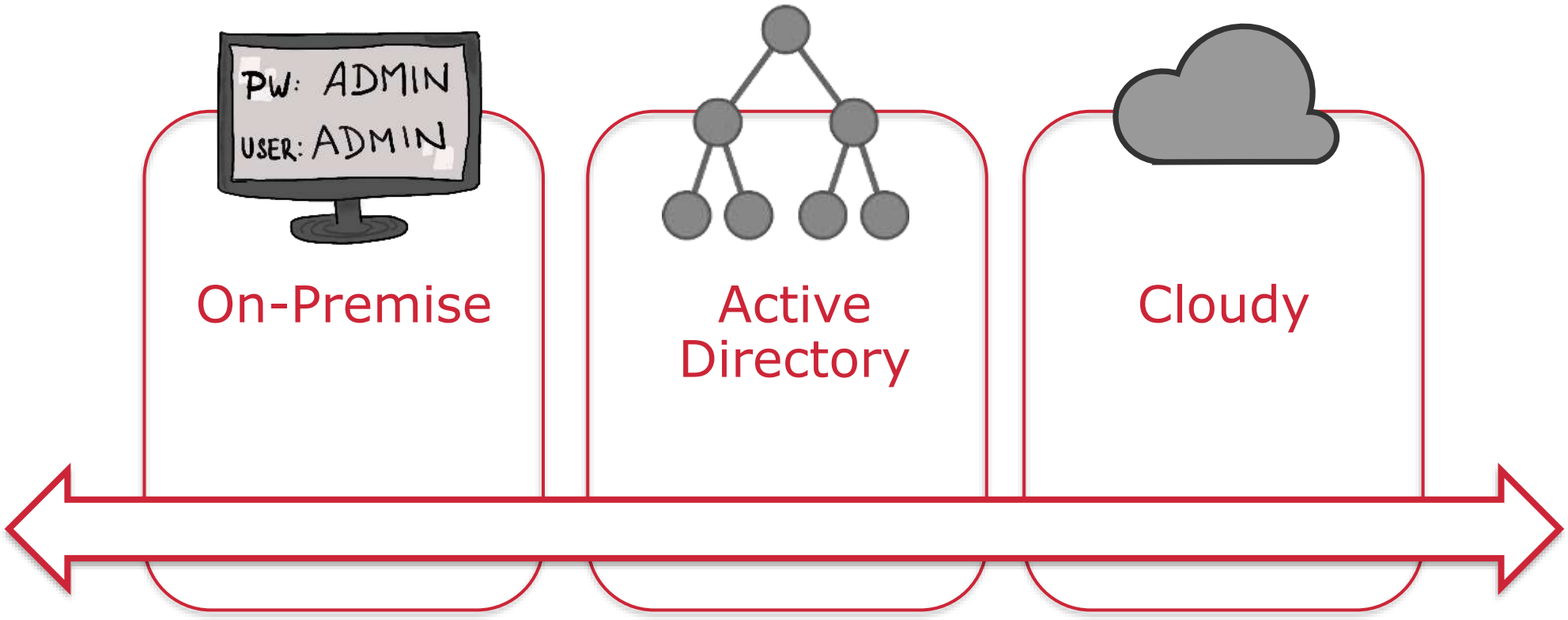
Miskonfigurácia je bezpečnostná chyba vytvorená konfiguráciou software

Oprava je závislá na operátorovi

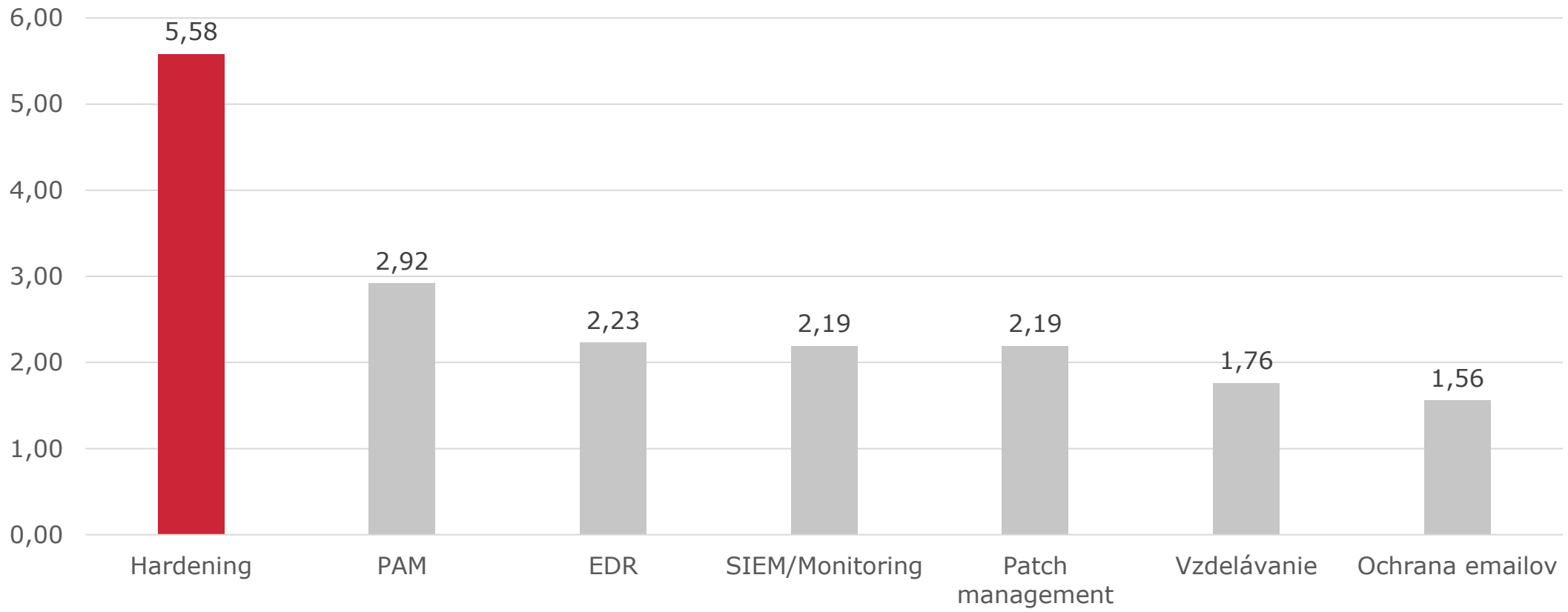
Typy zraniteľností



Typy miskonfigurácií



Hardening – doplnok alebo priorita?



Zdroj: Marsh McLennan

Detekcia zraniteľností

Ručne

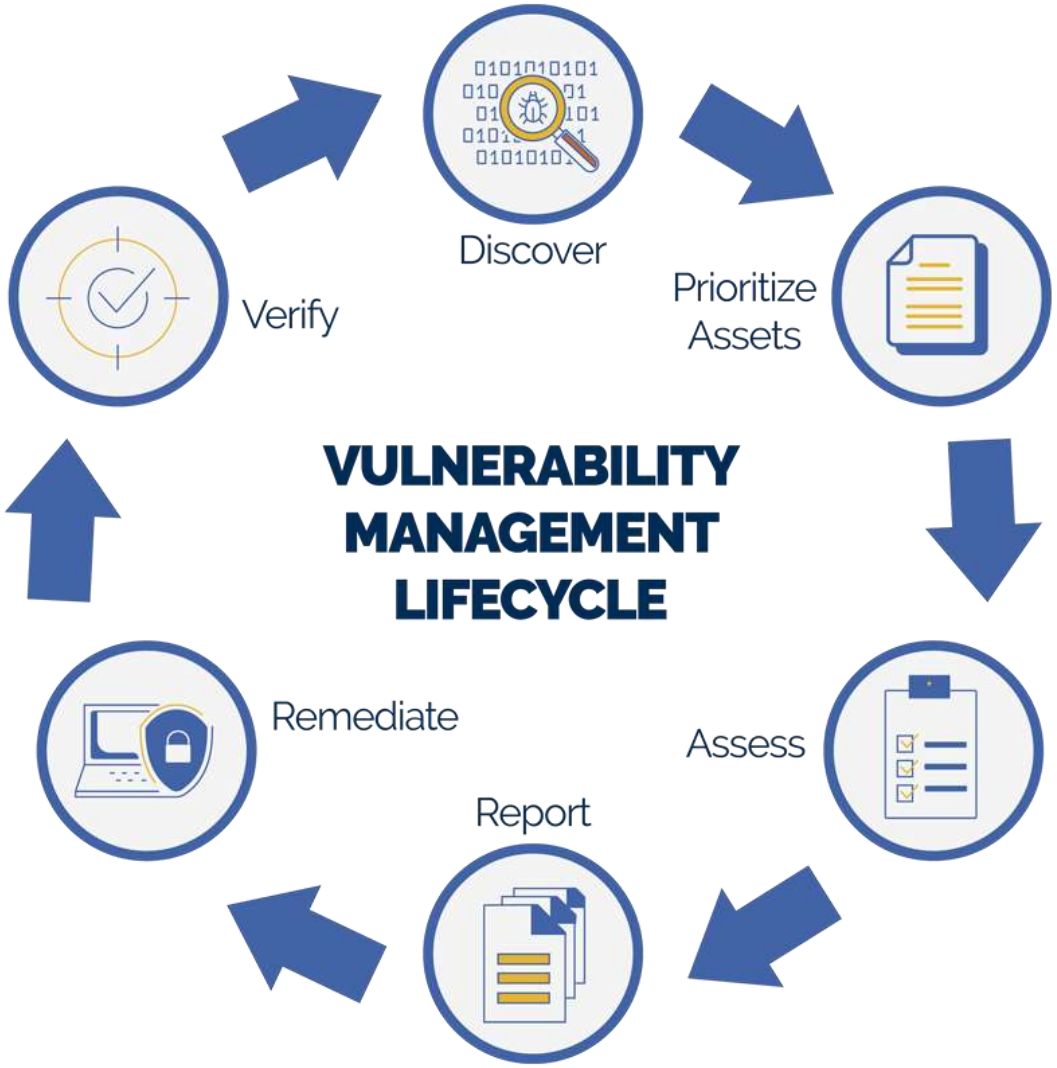
- Penetračné testy

- Pokrytie typov zraniteľností
  - Testy infraštruktúry (externé, interné, Wi-Fi, cloud)
  - Testy webových aplikácií (OWASP)
  - Red Teaming

Známy software

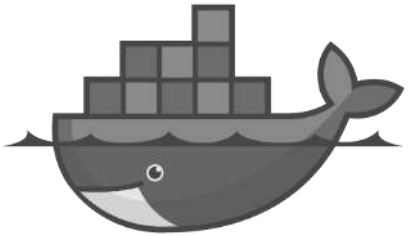
Detekcia zraniteľností v známom software

Známy software



On-Premise

Custom software



Kontajnery

Custom software

Detekcia zraniteľností v custom software

IDE

CI

CD

Developer Training

+

Secure code

Build

+

Unit testing
Code review

+

Integration testing

SAST

Review

+

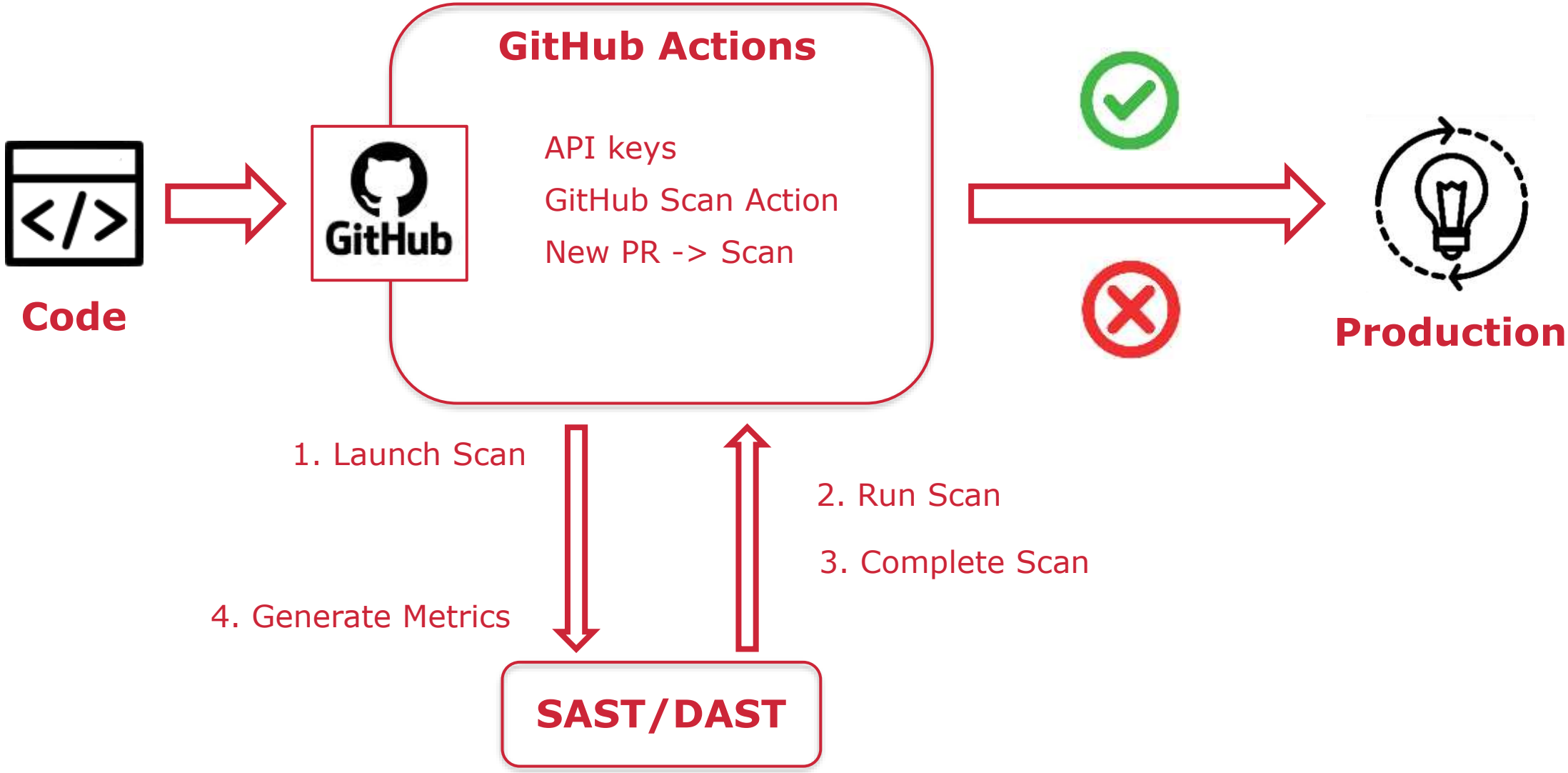
Pre-Production testing

+

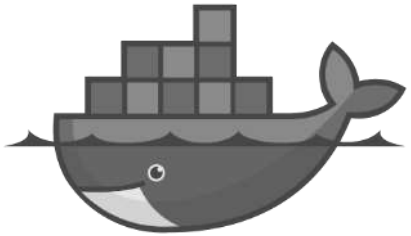
Production

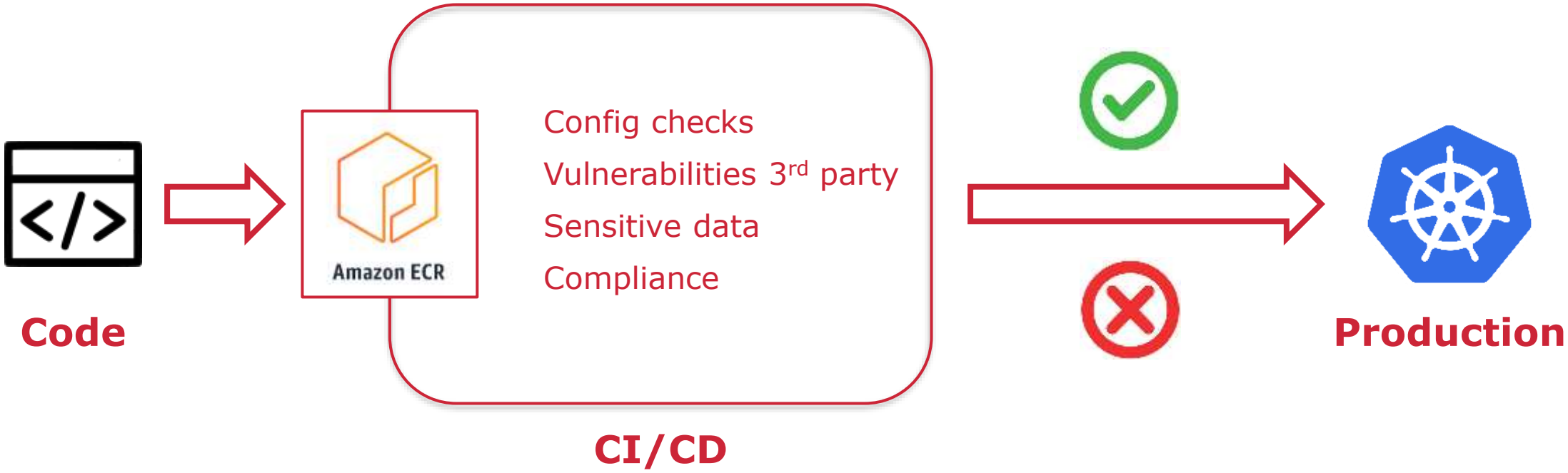
DAST

Detekcia zraniteľností v custom software



Kontajnery

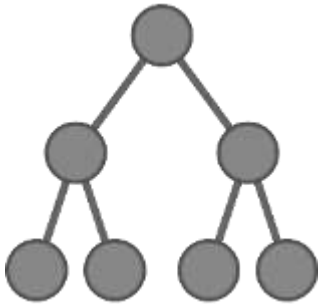



Amazon ECR
Config checks
Vulnerabilities 3rd party
Sensitive data
Compliance
Code
CI/CD
Production

Detekcia miskonfigurácií

On-Premise

Active Directory



Detekcia

- Detekčné nástroje – Komerčné aj OSS
  - Doména, koncové stanice, virtualizácia, cloudové prostredia
- Čo nám dajú?
  - Jednorázový report
  - Health score z kľúčových ukazateľov
  - Managovateľné množstvo nálezov
- Co viac chcieť?
  - Neustálý dohľad
  - Široký detekčný súbor

Mitigácia

- Ako napraviť?
  - Čo je ideálny stav? Google / dokumentácia / info od komunity

- Budeme fungovať? Miskonfigurácia ~ Feature
  - Kedy a ako zjistíme nefunkčnosť?

- Nefungujeme – Ako naspäť?

Cloudy

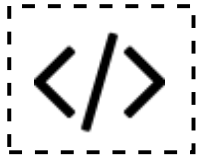
Detekcia miskonfigurácií v Cloude

Cloud Security Posture Management

Kubernetes Security

Cloud Workload Protection

CNAPP

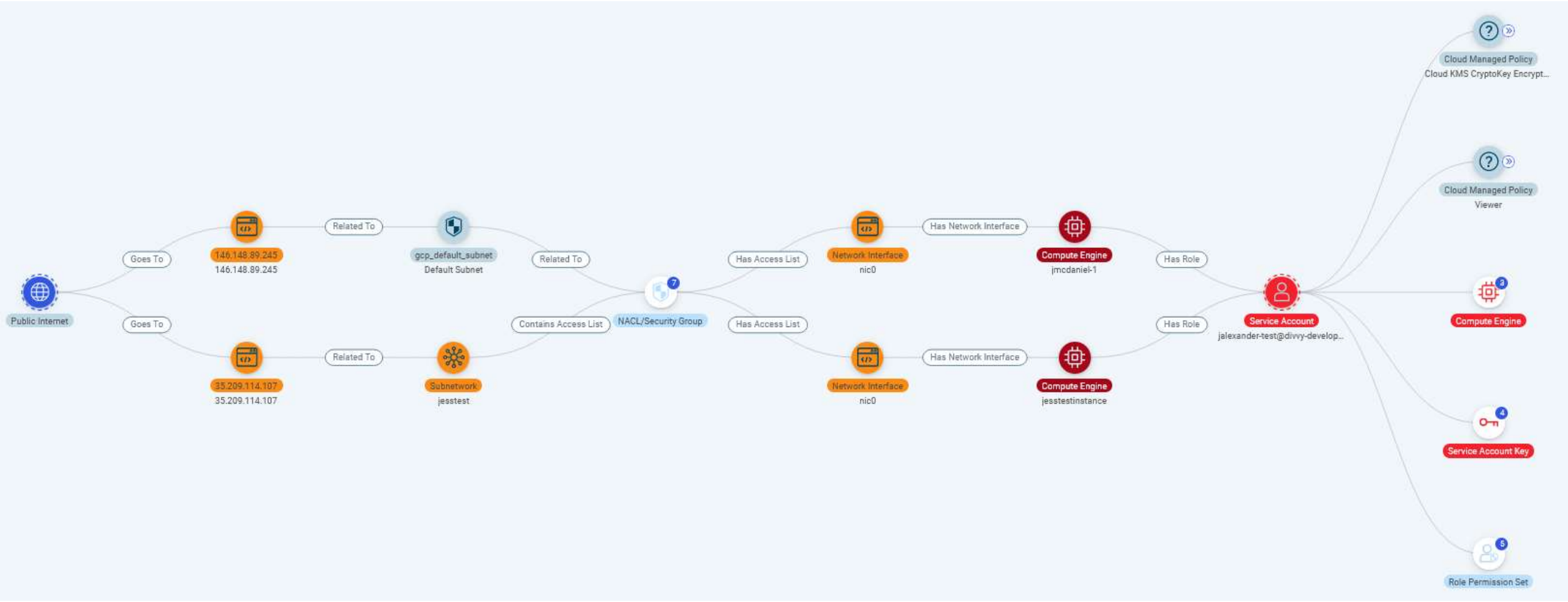


Infrastructure-as-Code Analysis

Cloud Identity and Access Management

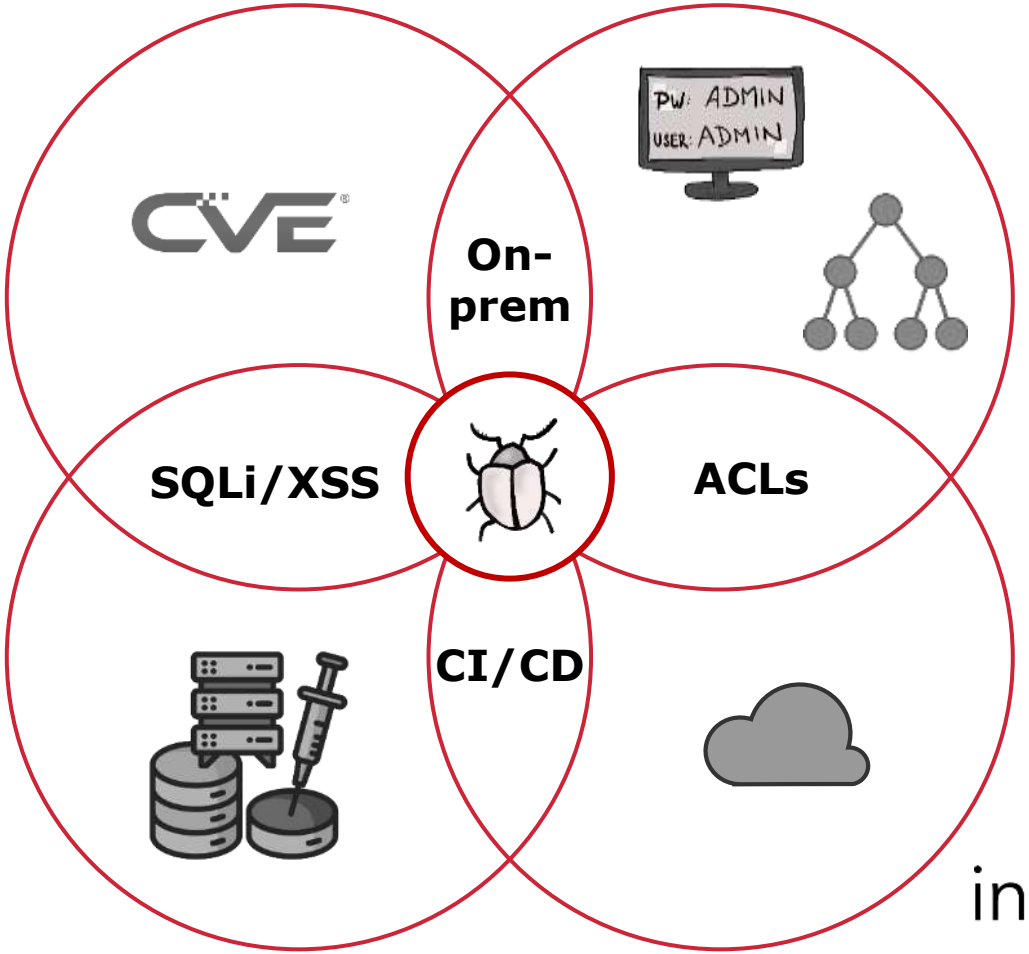
Customizable Reporting

Detekcia miskonfigurácií v Cloude



Vulnerability Management

insightVM
RAPID7



Validator

GYTPOL

DAST/SAST

insightAppSec
RAPID7

CNAPP

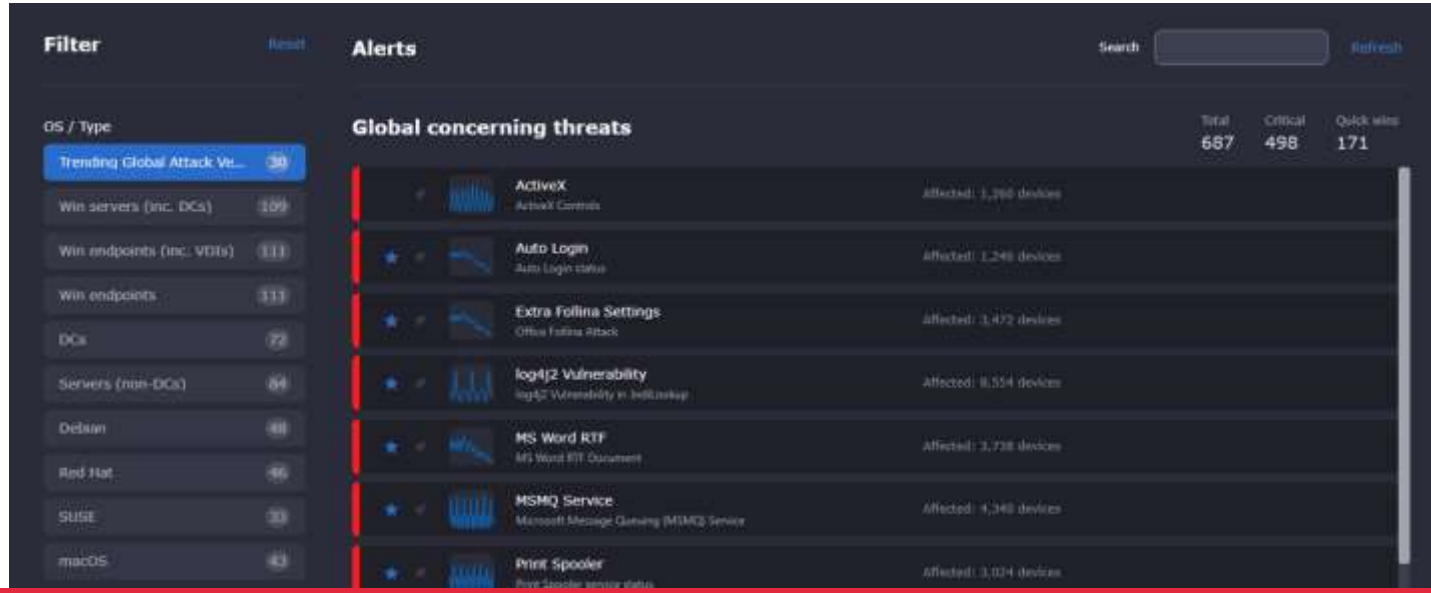
insightCloudSec
RAPID7

Gytpol Validator

- Nepřetržitý dohled nad stavem konfigurací AD, GPO, koncových bodů
- Pokročilá analytika využívání systémových funkcí

- Obsáhlá hardening databáze – Best practices, CIS, NIST,

- Nápravné procesy
  - Poskytnutí informací o nálezu
  - Doporučení postupů
  - Automatizace náprav

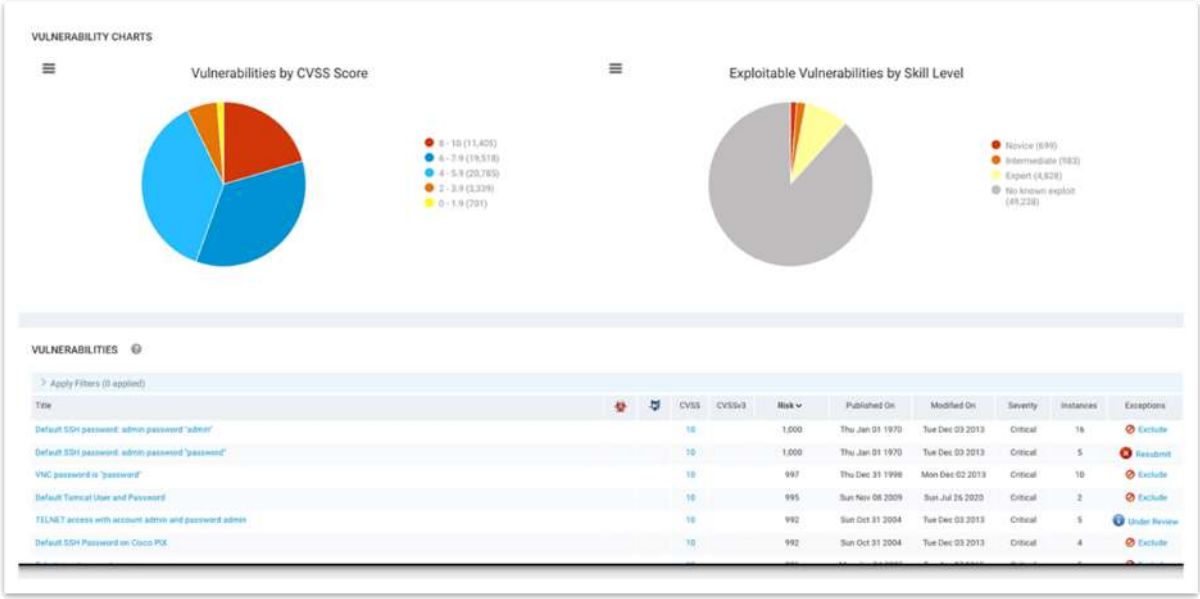


Rapid7 InsightVM

- Detekce zranitelností ve fyzických prostředích, virtualizaci, cloudu, kontejnerech

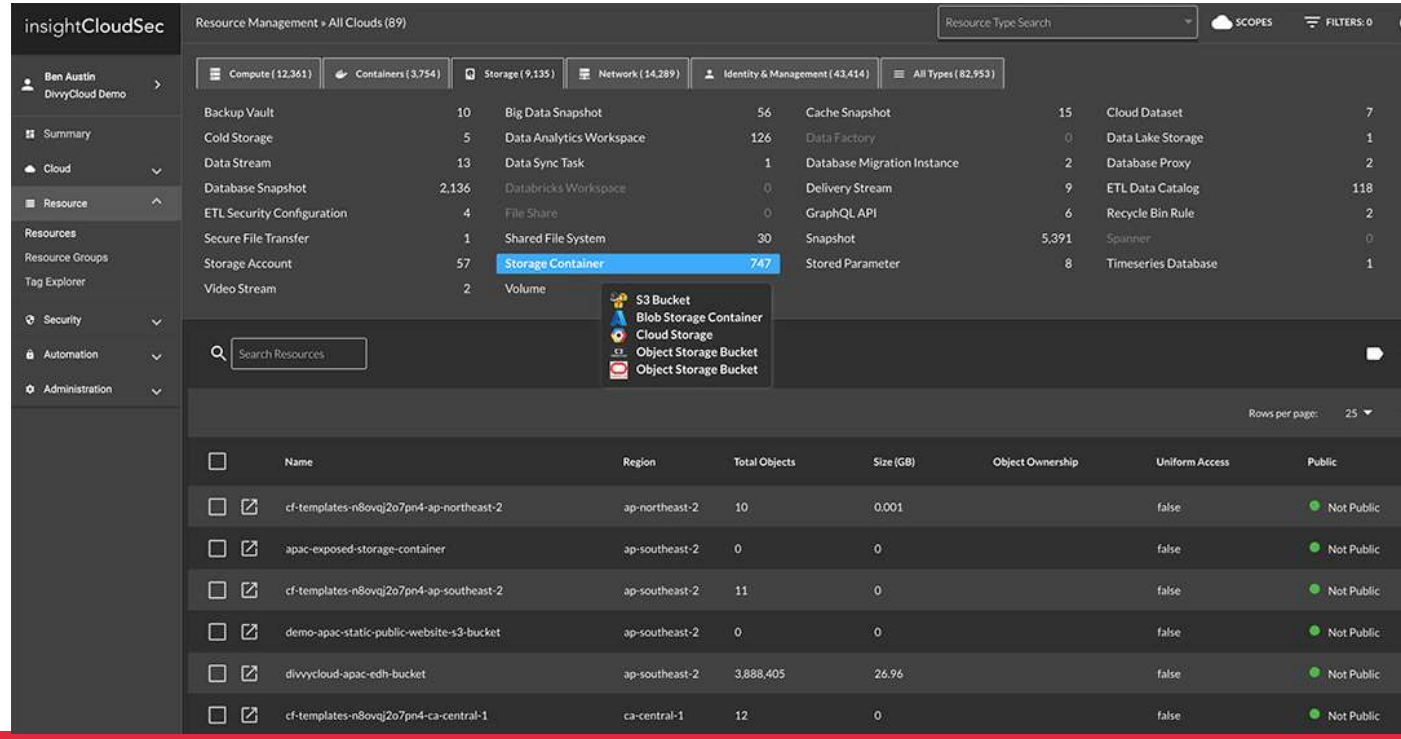
- Pokročilý scoring - Active Risk Score
  - Četnost a oblast výskytu
  - Obtížnost zneužití
  - Threat Intelligence

- Řízení nápravných procesů
  - Doporučení postupů
  - Project management, ticketing



Rapid7 CloudSec

- Centrální monitoring rizik v cloudových / multi-cloudových prostředích
  - AWS, Azure, GCP
- Okamžitá analýza změn konfigurací, nových assetů
  - Vulnerability management
  - Detekce miskonfigurací
  - Odhalení exponovaných identit



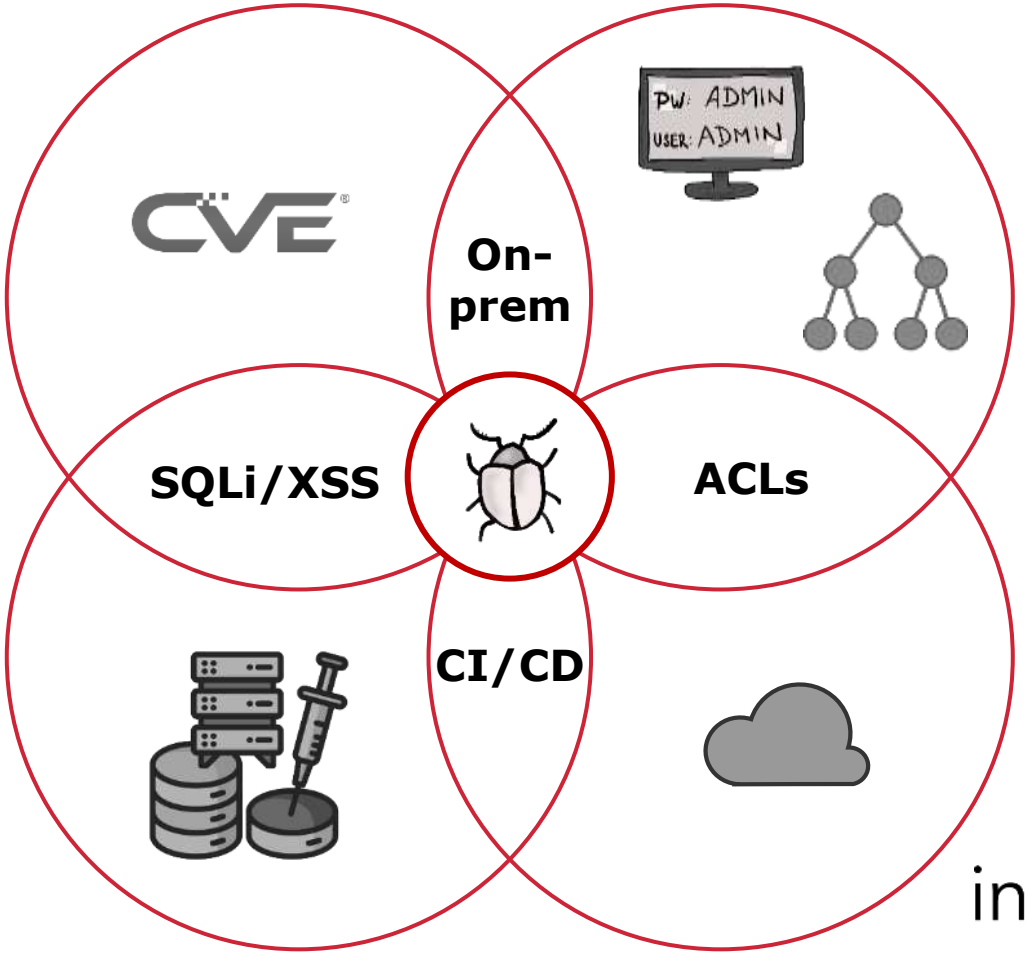
Rapid7 AppSec

- Automatizované black-box testování webových aplikací
- Checky proti OWASP Top Ten & aplikačním miskonfiguracím

- Integrace do DevSecOps procesů
  - Testování probíhá paralelně s vývojem
  - Attack replays v živém prostředí
  - Identifikace chyby až na rovinu řádku kódu
  - Snadný retesting v podání vývojáře

Vulnerability Management

insightVM
RAPID7



Validator

GYTPOL

DAST/SAST

insightAppSec
RAPID7

CNAPP

insightCloudSec
RAPID7

COMGUARD

cyber security masters

Ďakujem za pozornosť!