

comGUARD

cyber security masters

Problematika zranitelností v praxi

Ondřej Malík

20.09.2024

Teória zraniteľnosti

Zraniteľnosť vs. Miskonfigurácia



Zraniteľnosť je bezpečnostná chyba priamo v software

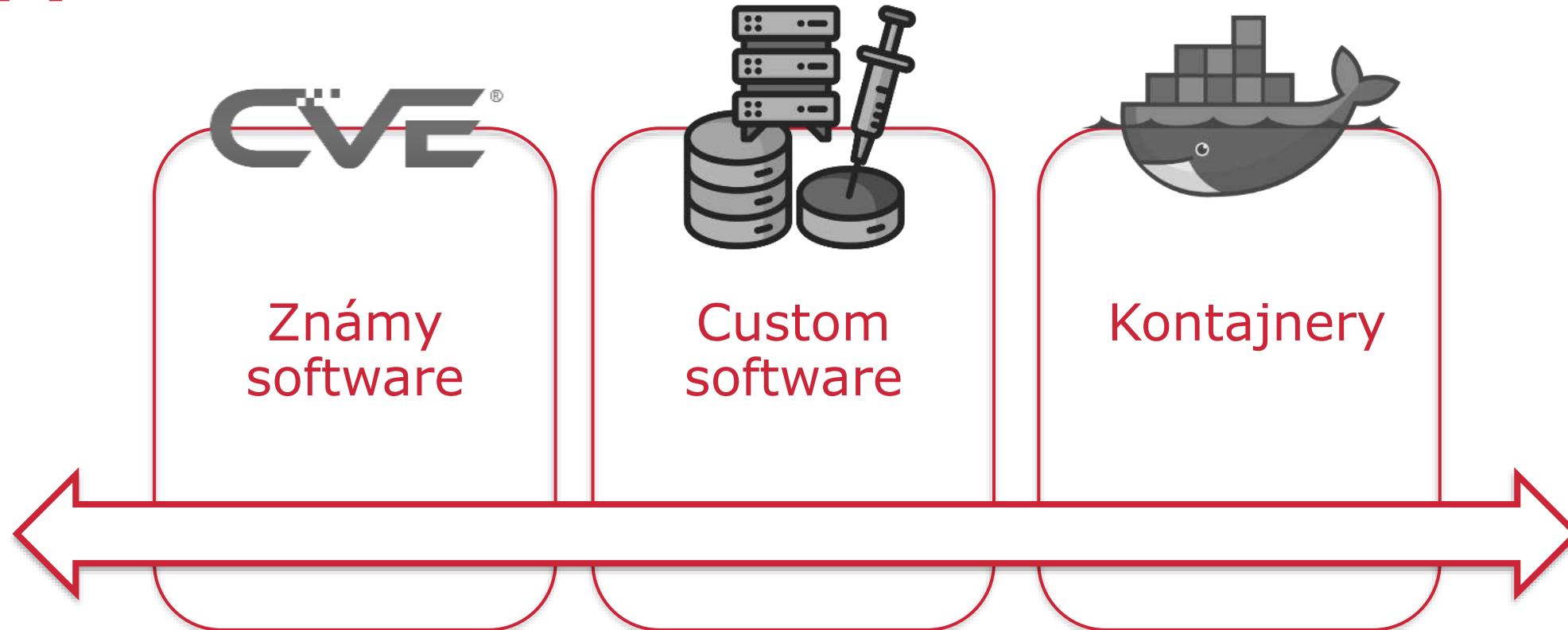
Oprava je priamo závislá na vendorovi



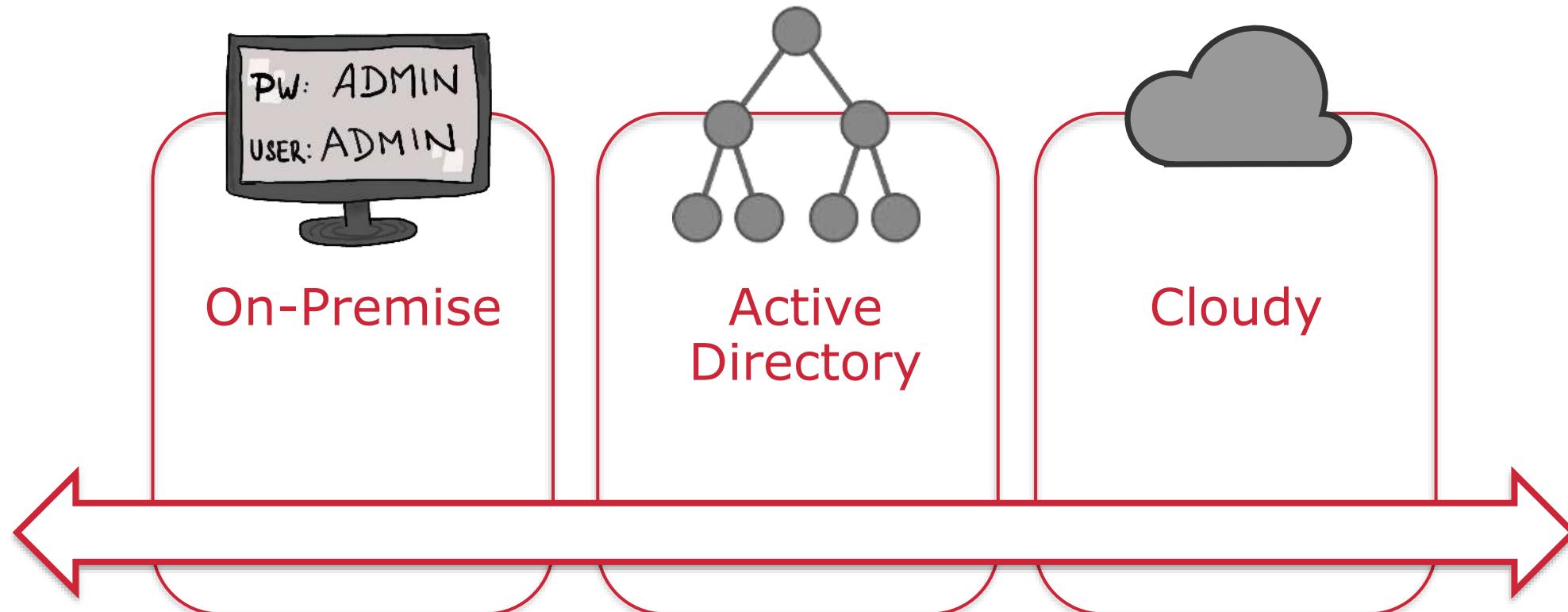
Miskonfigurácia je bezpečnostná chyba vytvorená konfiguráciou software

Oprava je závislá na operátorovi

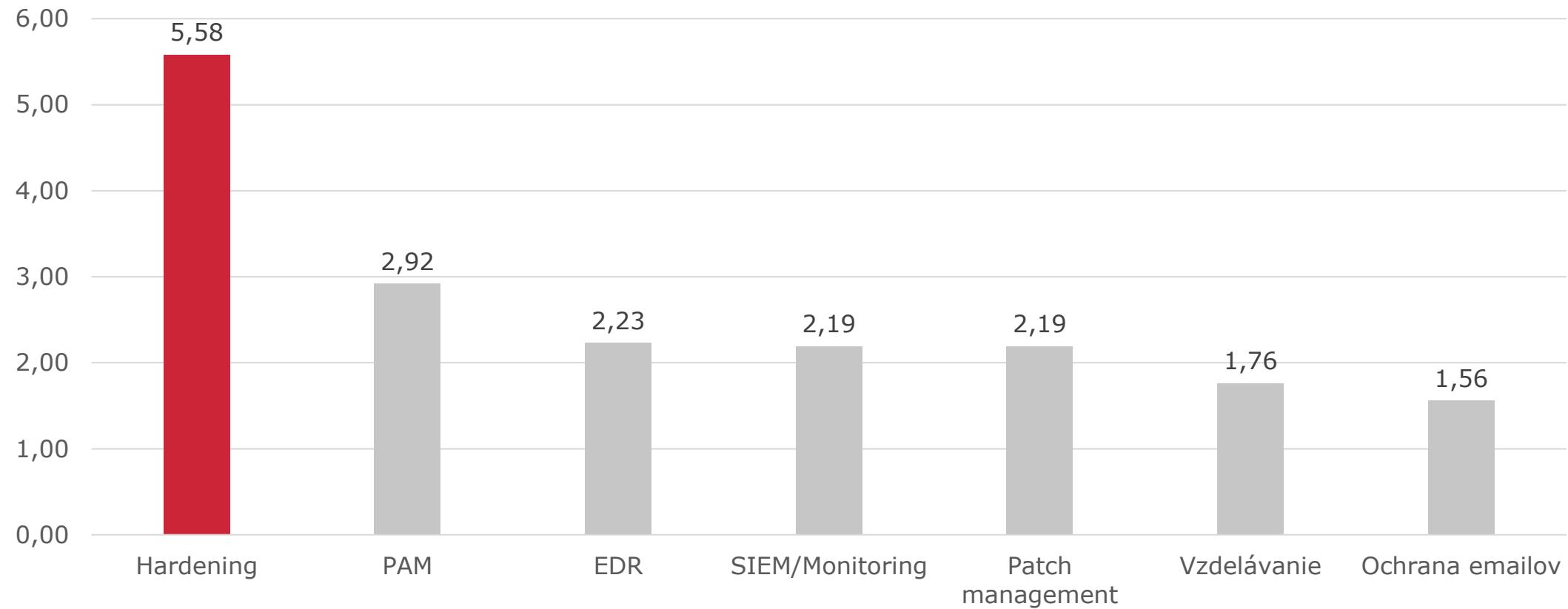
Typy zraniteľnosti



Typy miskonfigurácií



Hardening – doplnok alebo priorita?



Zdroj: Marsh McLennan

Detekcia zraniteľnosti

Ručne

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



Známy software





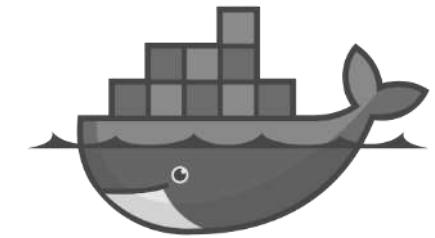
Známy software



Custom software



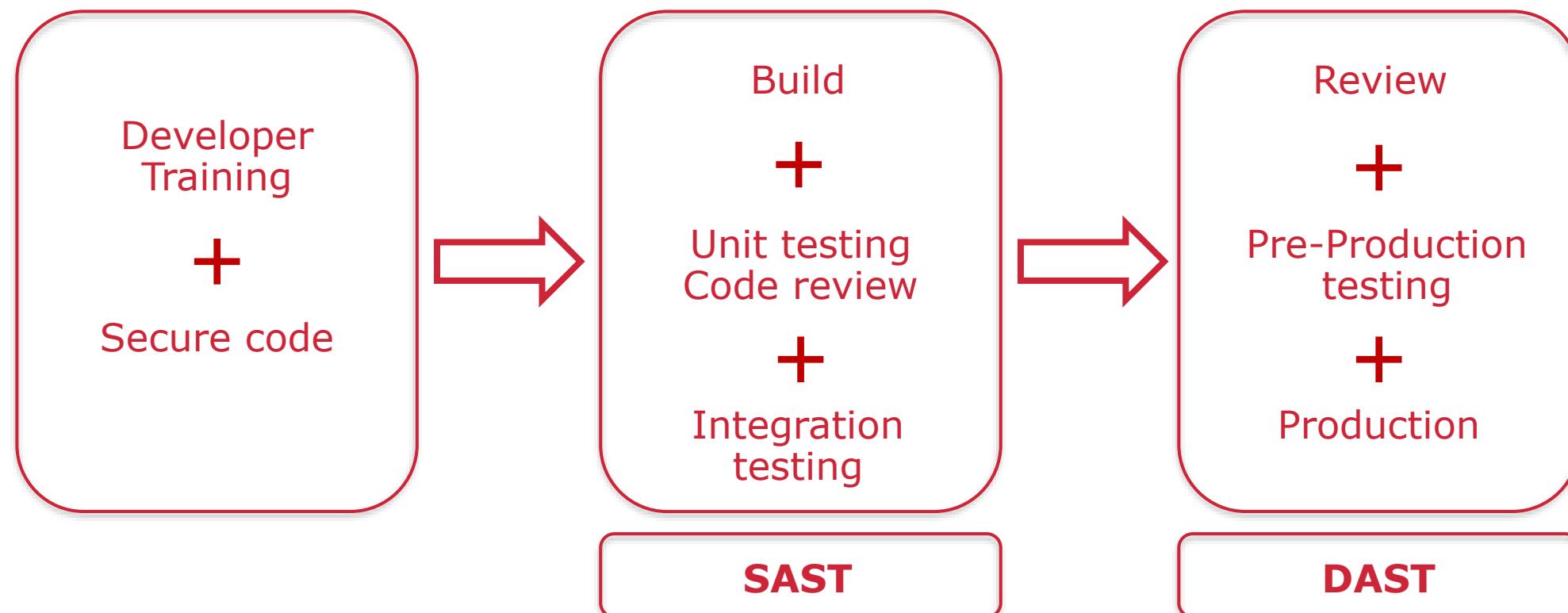
On-Premise

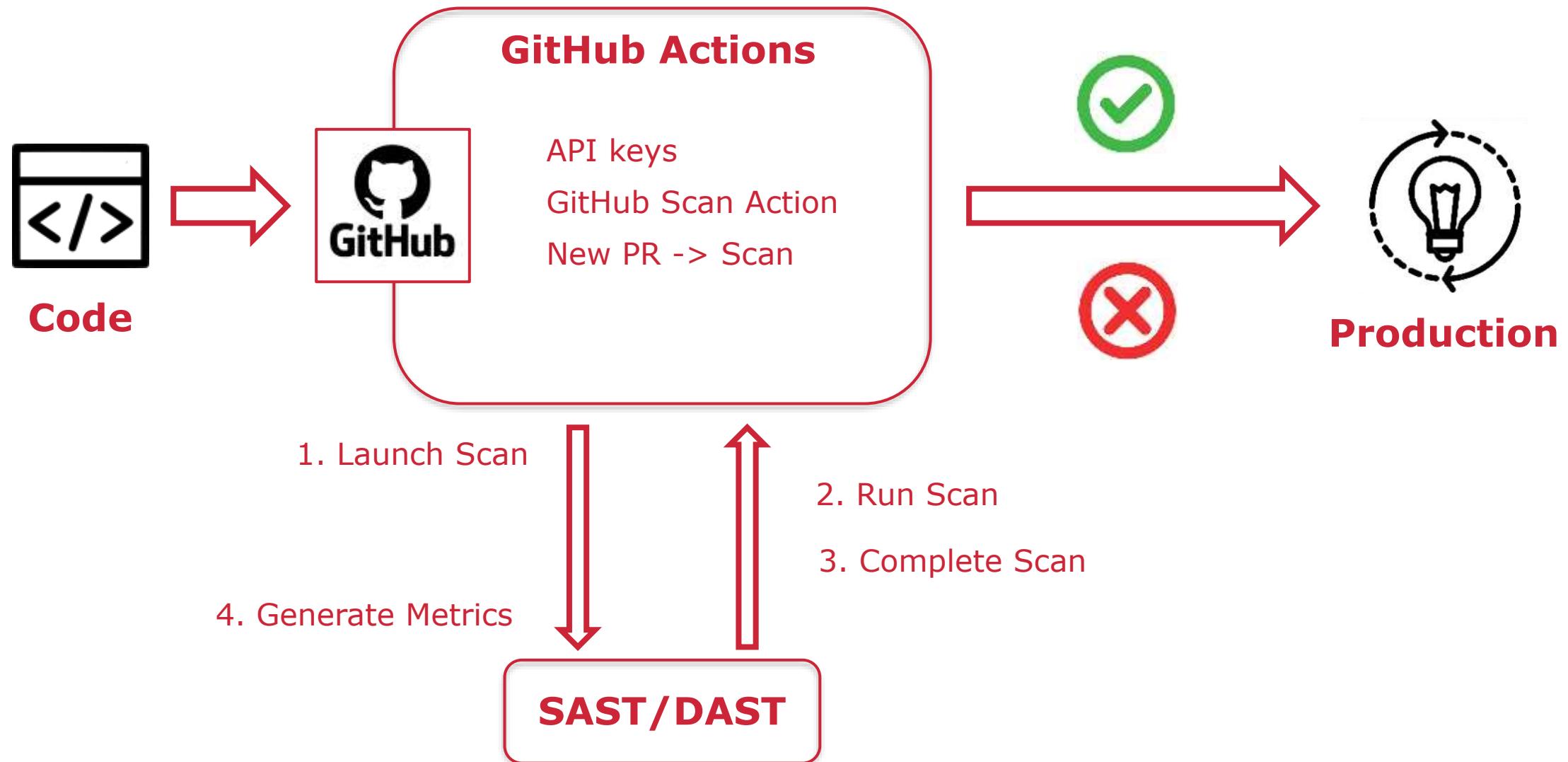


Kontajnery

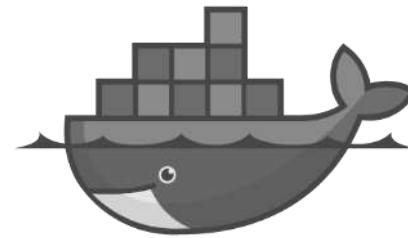
Custom software

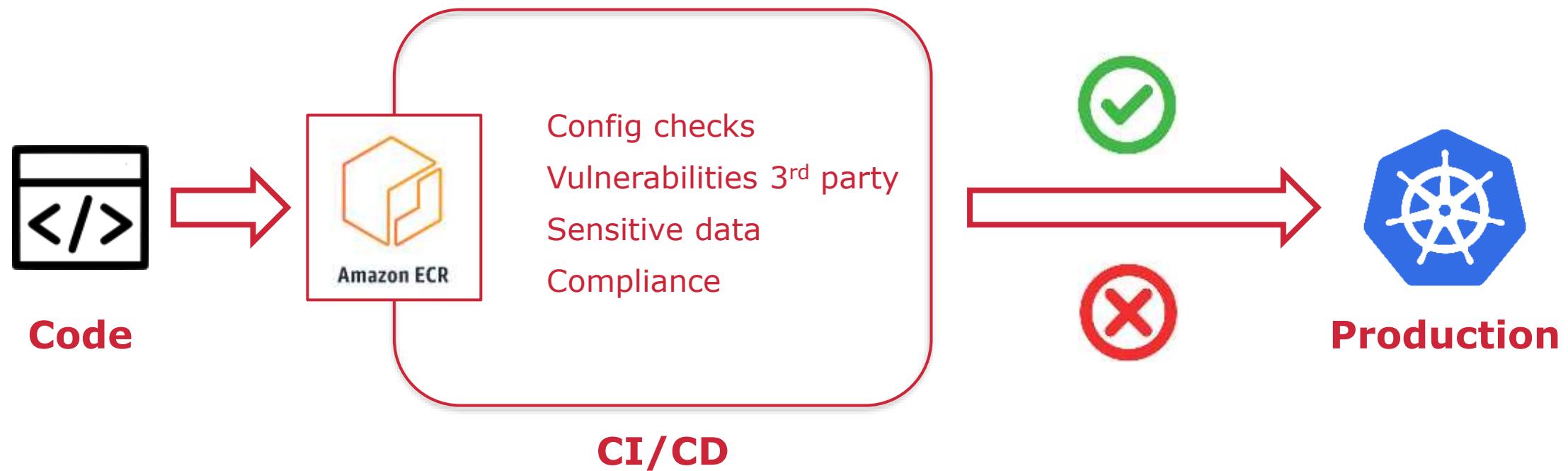


**IDE****CI****CD**



Kontajnery



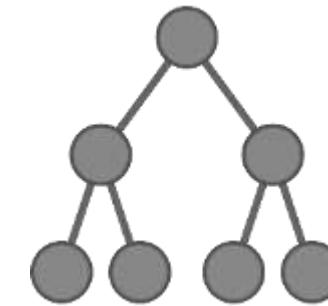


Detekcia miskonfigurácií

On-Premise



Active Directory



Detekcia

- Detekčné nástroje – Komerčné aj OSS
 - Doména, koncové stanice, virtualizácia, clouдовé prostredia
- Čo nám dajú?
 - Jednorázový report
 - Health score z kľúčových ukazateľov
 - Manažovateľné 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





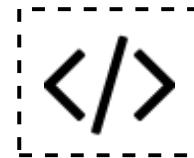
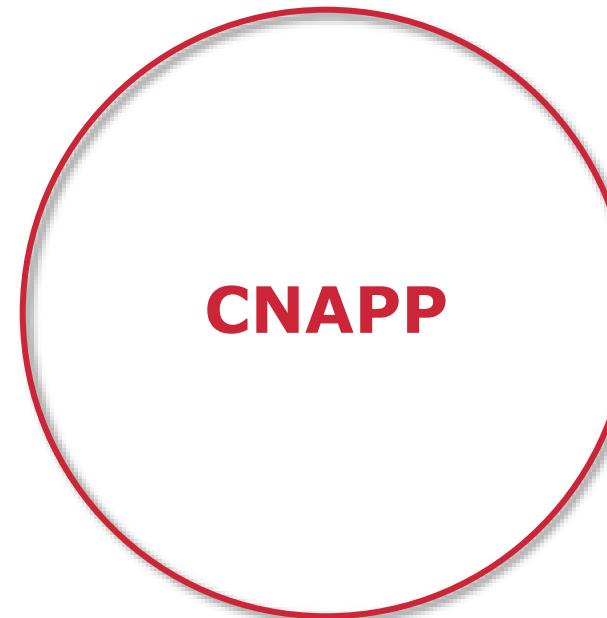
**Cloud Security
Posture Management**



Kubernetes Security



**Cloud Workload
Protection**



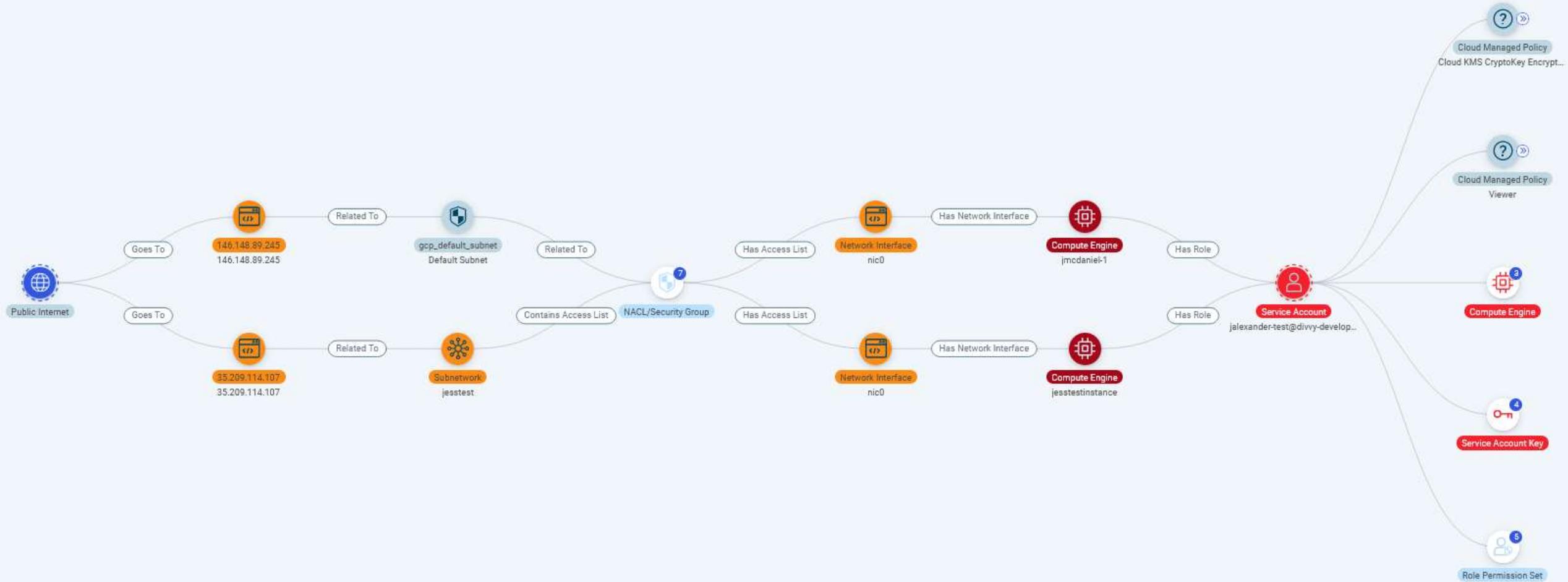
**Infrastructure-as-Code
Analysis**

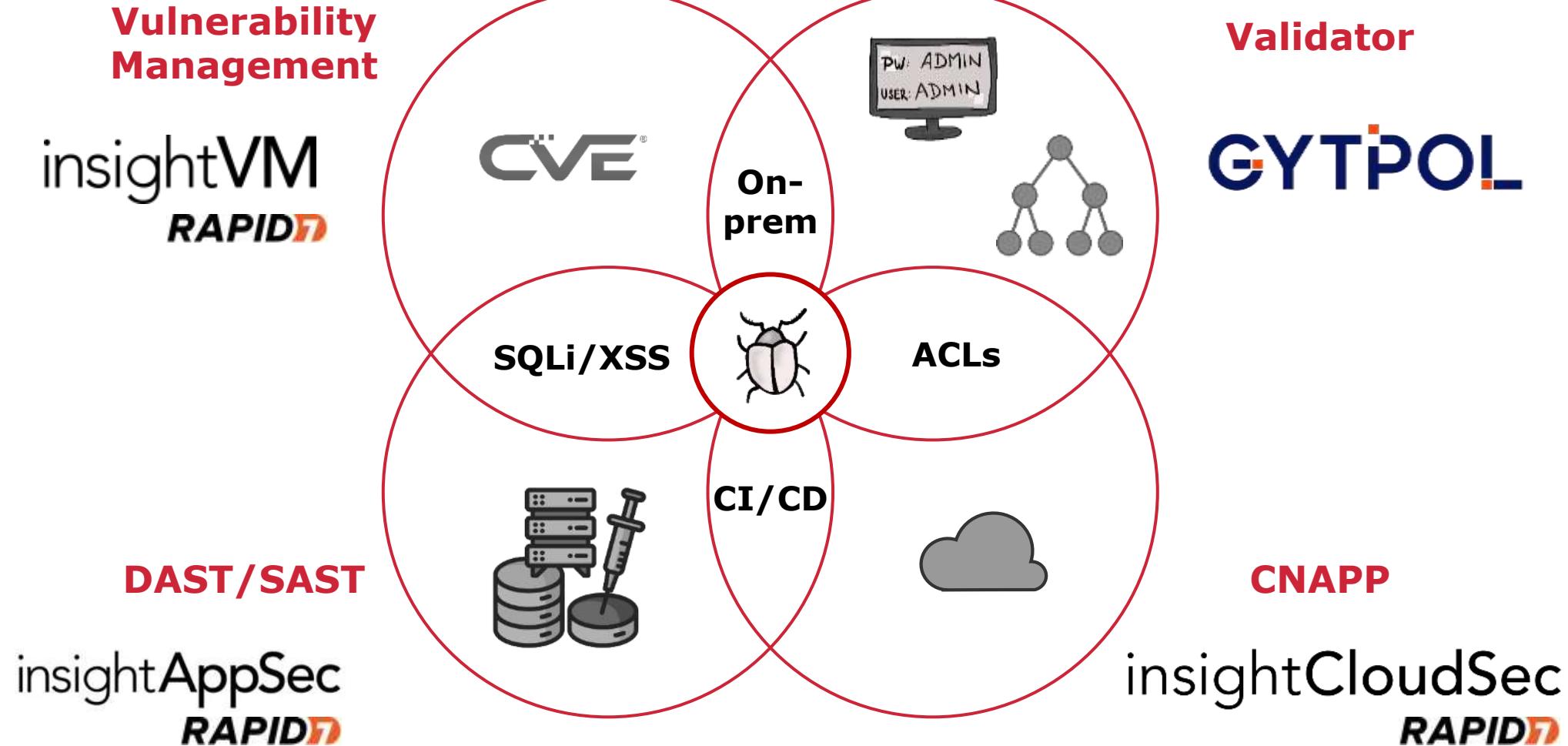


**Cloud Identity and
Access Management**



**Customizable
Reporting**





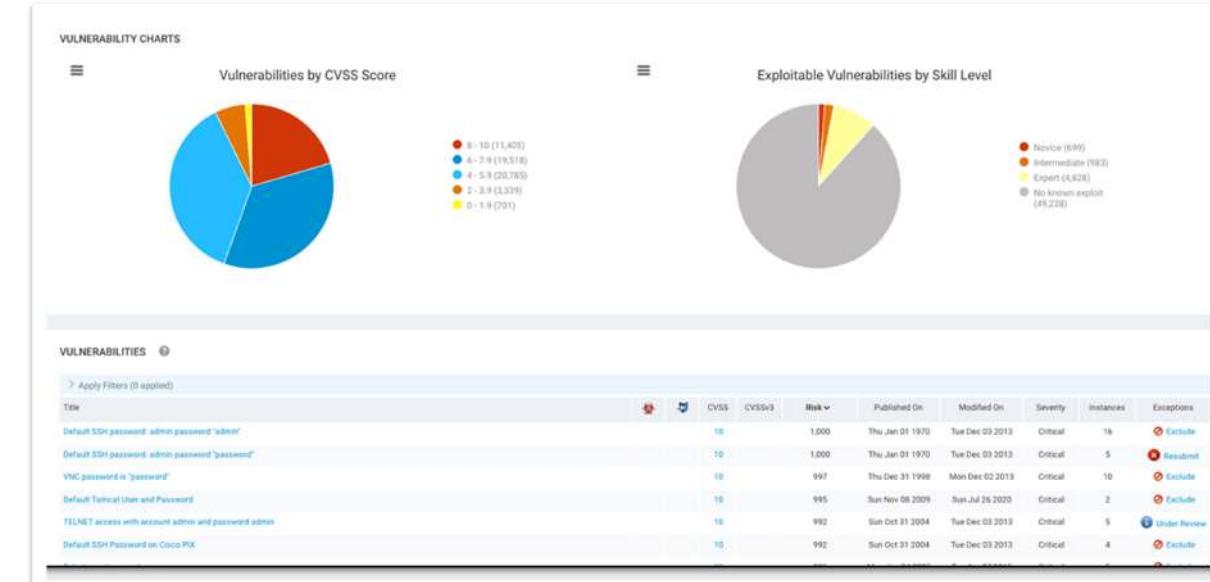
Gytpol Validator

- 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**

The screenshot shows a dashboard titled 'Global concerning threats' from the Gytpol Validator tool. On the left, there is a sidebar with a 'Filter' section containing a search bar and a 'Reset' button. Below the search bar is a list of OS / Type categories with their respective counts: Trending Global Attack: Vt... (30), Win servers (inc. DCs) (109), Win endpoints (inc. VHDs) (111), Win endpoints (111), DCs (72), Servers (non-DCs) (64), Debian (61), Red Hat (66), SUSE (30), and macOS (43). To the right of the sidebar, a main panel displays a list of threats with icons, names, and affected device counts. The threats listed are: ActiveX (ActiveX Controls, Affected: 1,296 devices), Auto Login (Auto Login config, Affected: 1,246 devices), Extra Follina Settings (Office Follina attack, Affected: 1,472 devices), log4j2 Vulnerability (log4j2 Vulnerability in Jenkins, Affected: 8,554 devices), MS Word RTF (MS Word RTF Document, Affected: 3,738 devices), MSMQ Service (Microsoft Message Queuing (MSMQ) Service, Affected: 4,346 devices), and Print Spooler (Print Spooler service status, Affected: 3,024 devices). At the top right of the main panel, there are buttons for 'Total' (687), 'Critical' (498), and 'Quick view' (171).

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

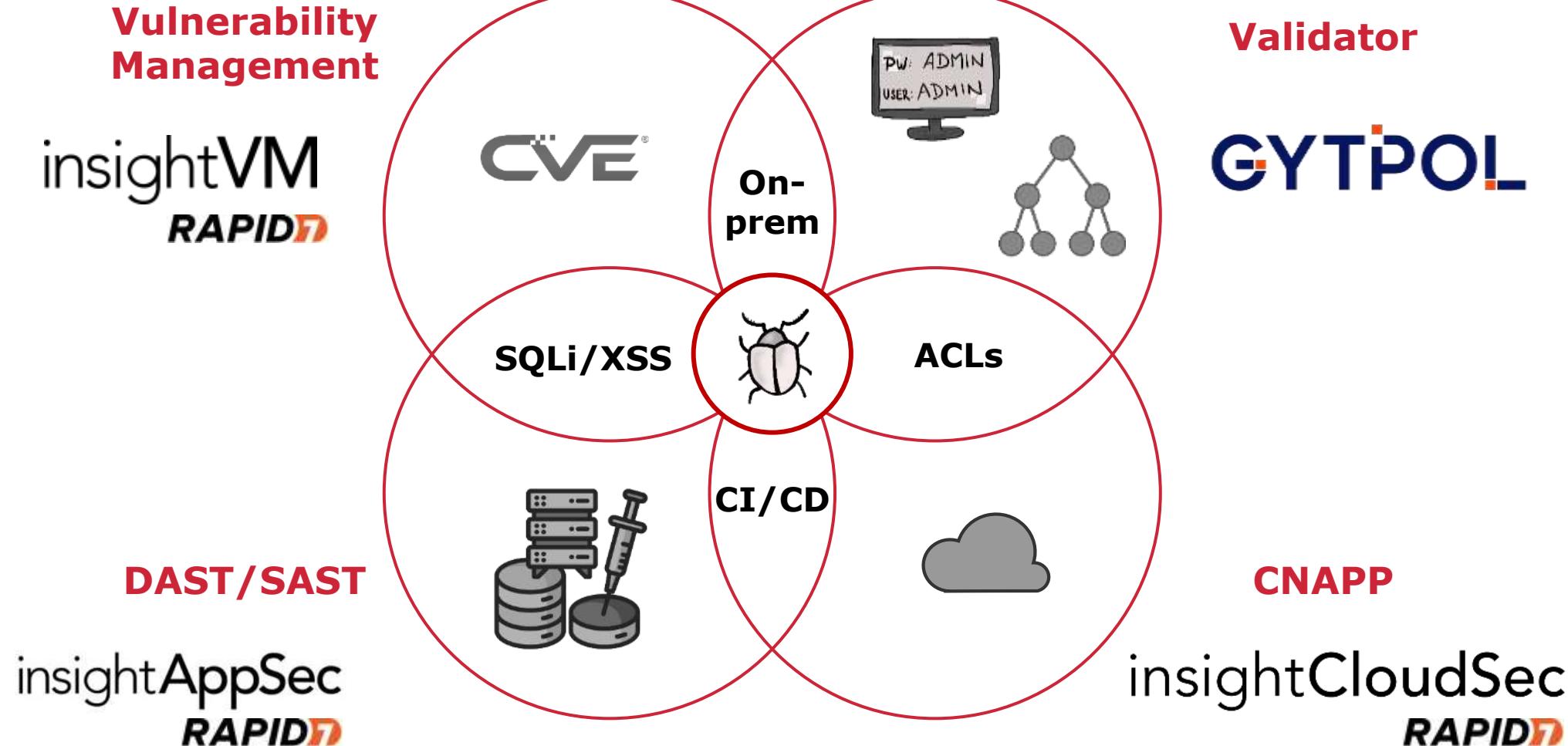
- Centrální monitoring rizik v cloudových / multi-cloudových prostředích
 - AWS, Azure, GCP
- Okamžitá analýza změn konfigurací, nových assetů
 - Vulnerability management
 - Detekce miskonfigurací
 - Odhalení exponovaných identit

The screenshot shows the insightCloudSec web application interface. On the left is a navigation sidebar with options like Ben Austin, DivvyCloud Demo, Summary, Cloud (selected), Resource (selected), Resources, Resource Groups, Tag Explorer, Security, Automation, and Administration. The main area is titled "Resource Management > All Clouds (89)". It displays a grid of resources categorized by type: Compute (12,361), Containers (3,754), Storage (9,135), Network (14,289), Identity & Management (43,414), and All Types (82,953). A specific "Storage Container" resource is highlighted with a blue border. Below the grid is a search bar labeled "Search Resources". At the bottom, there's a table with columns: Name, Region, Total Objects, Size (GB), Object Ownership, Uniform Access, and Public status. Several rows of storage buckets are listed, all marked as "Not Public".

Name	Region	Total Objects	Size (GB)	Object Ownership	Uniform Access	Public
cf-templates-n8ovqj2o7pn4-ap-northeast-2	ap-northeast-2	10	0.001		false	Not Public
apac-exposed-storage-container	ap-southeast-2	0	0		false	Not Public
cf-templates-n8ovqj2o7pn4-ap-southeast-2	ap-southeast-2	11	0		false	Not Public
demo-apac-static-public-website-s3-bucket	ap-southeast-2	0	0		false	Not Public
divvycloud-apac-edn-bucket	ap-southeast-2	3,888,405	26.96		false	Not Public
cf-templates-n8ovqj2o7pn4-ca-central-1	ca-central-1	12	0		false	Not Public

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



comGUARD

cyber security masters

Ďakujem
za pozornosť!