COMGUARD
communication security

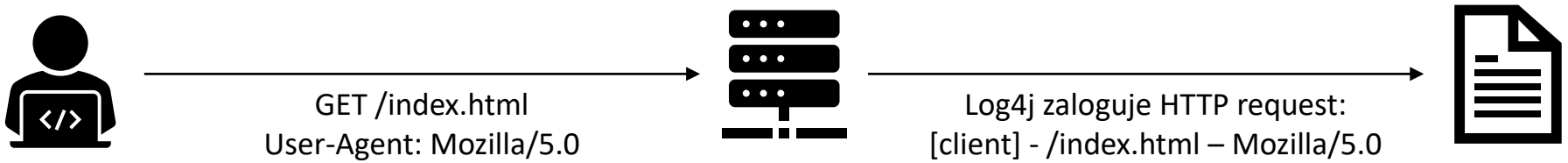
Nejzávažnější zranitelnosti pohledem Vulnerability Managementu

Ondrej Malík | Security Consultant

- Aké boli najzávažnejšie zraniteľnosti za posledný rok?
- Prečo mať a používať Vulnerability Management?
- Dá sa spoliehať na jednorázové skeny zraniteľností?

Apache Log4Shell – CVE-2021-44228

Normálny Log4j scenár



Exploit

Java Spring framework

- Vzdialené spustenie kódu v Spring Core (Spring4Shell) – CVE-2022-22963

VMware

- vCenter Server – CVE-2021-22005 (RCE)
- vCenter Client (Server plugin) – CVE-2021-21972 (RCE)
- Workspace ONE Access a Identity Manager – CVE-2022-22954 (RCE)

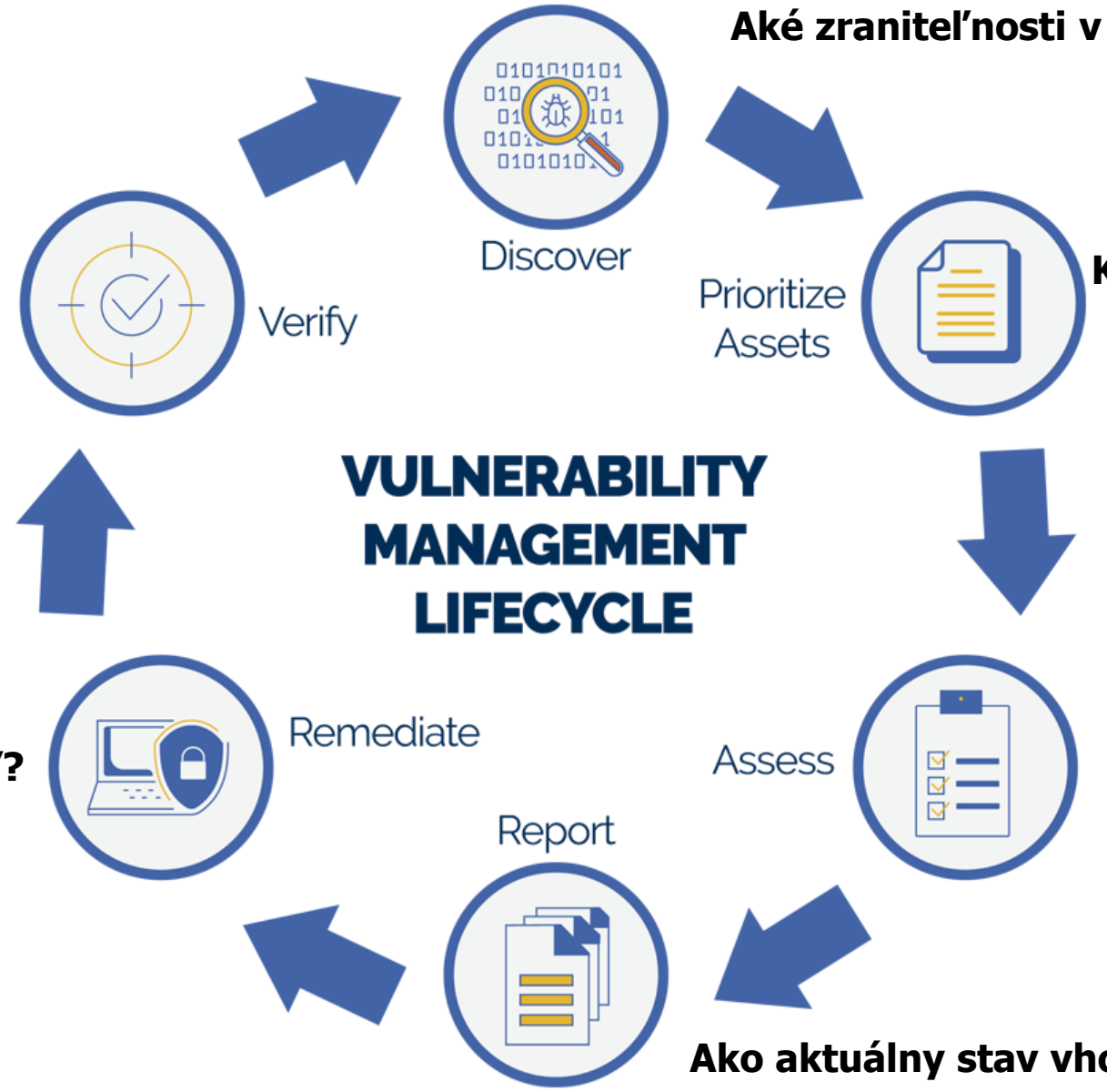
Attlasian Confluence

- Vzdialené spustenie kódu cez OGNL v Attlasian Confluence Server a Confluence Data Center – CVE-2022-26134
- Používané na Behinder web shell, China Chopper a vlastné shell skripty

Zyxel

- CVE-2022-0342
  - Obídenie autentizácie a získanie admin prístupu
- CVE-2022-30525
  - Modifikácia súborov a RCE v Zyxel firewalloch
  - Odhad zraniteľných zariadení bol 15 tisíc

Aké zraniteľnosti v sieti máme?



Ktoré assety sú najdôležitejšie?

Ktoré zraniteľnosti riešiť jako prvé?

Ako aktuálny stav vhodne interpretovať?

Ako zraniteľnosti odstrániť?

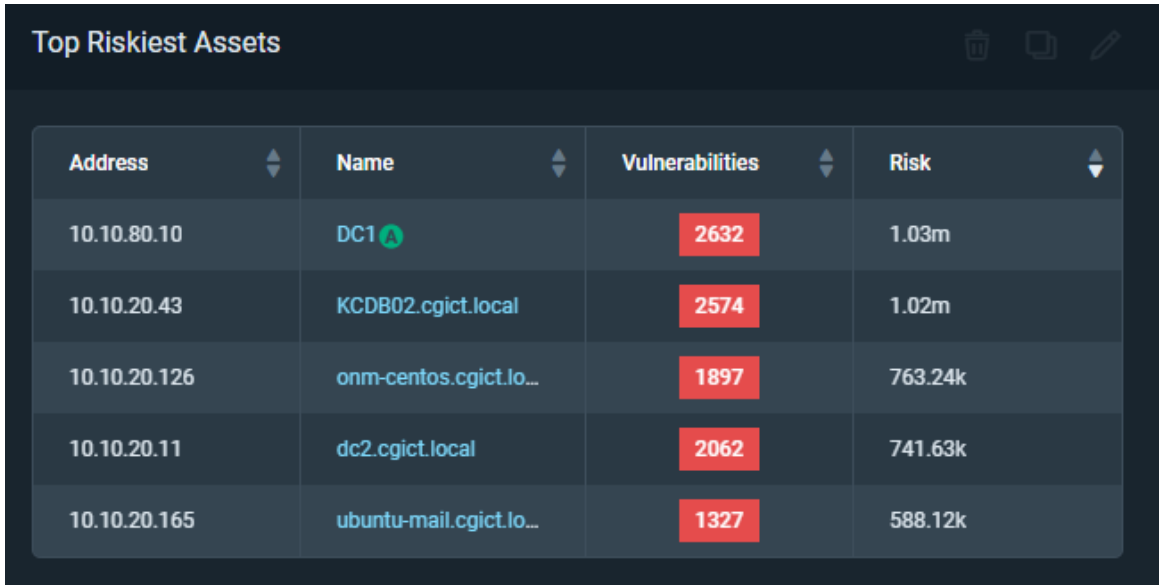
Sú zraniteľnosti naozaj odstránené?

Aké zraniteľnosti v sieti máme?

- Aktívne skenovanie zraniteľností
- Skenovanie zraniteľností pomocou agentov
- Web spidering
- Skenovanie politík
- Skeny autentizovanými účtami

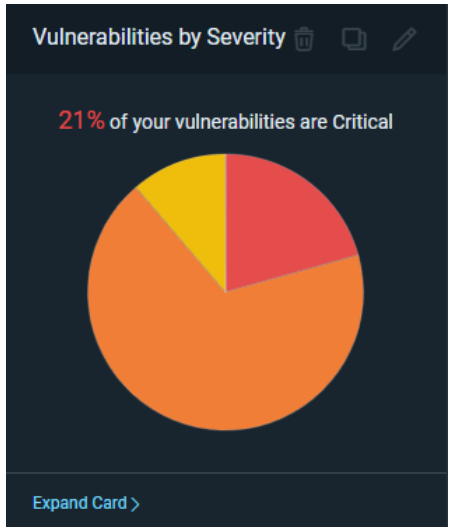
Ktoré assety sú najdôležitejšie?

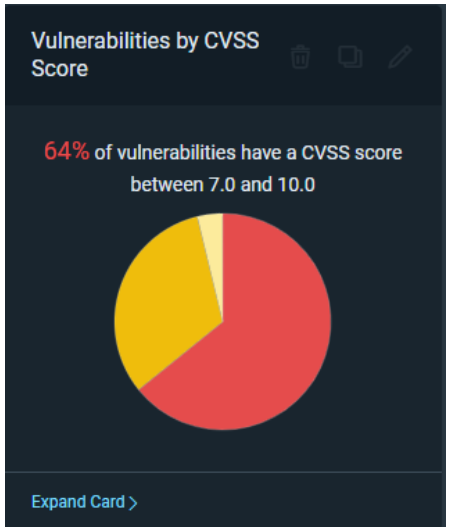
- Označenie assetov tagmi – domain controller, database server…
- Vytváranie statických/dynamických skupín assetov
- Prehľadné dashboardy o kritických assetoch

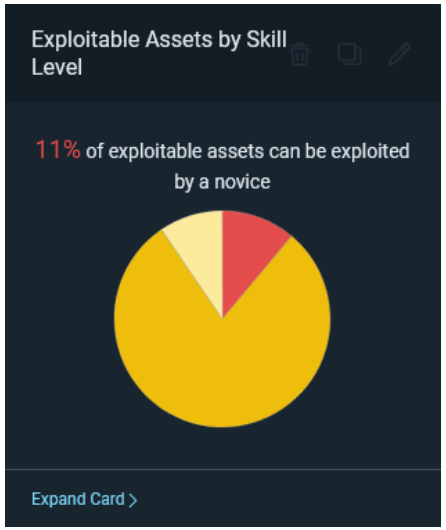


Ktoré zraniteľnosti riešiť jako prvé?

- Real Risk Score – pohľad zo strany útočníka:
  - Je dostupný exploit?
  - Ako zložité je zraniteľnosť zneužiť
  - Čo je ohrozené?
- CVSS score vs. RRS

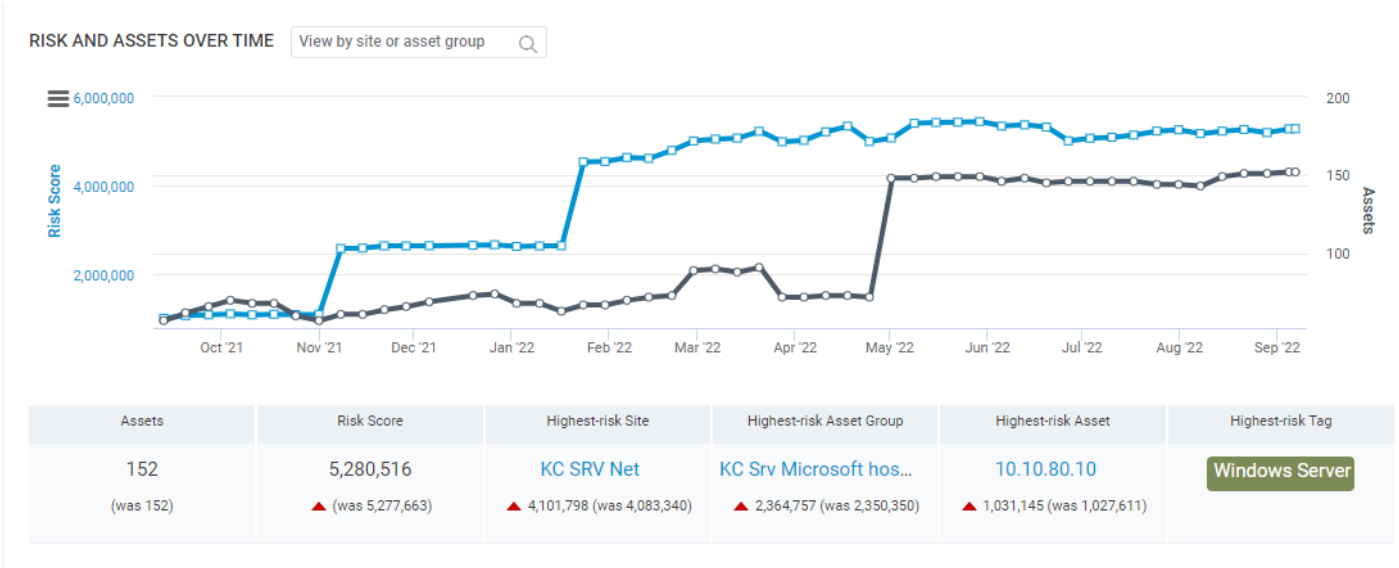


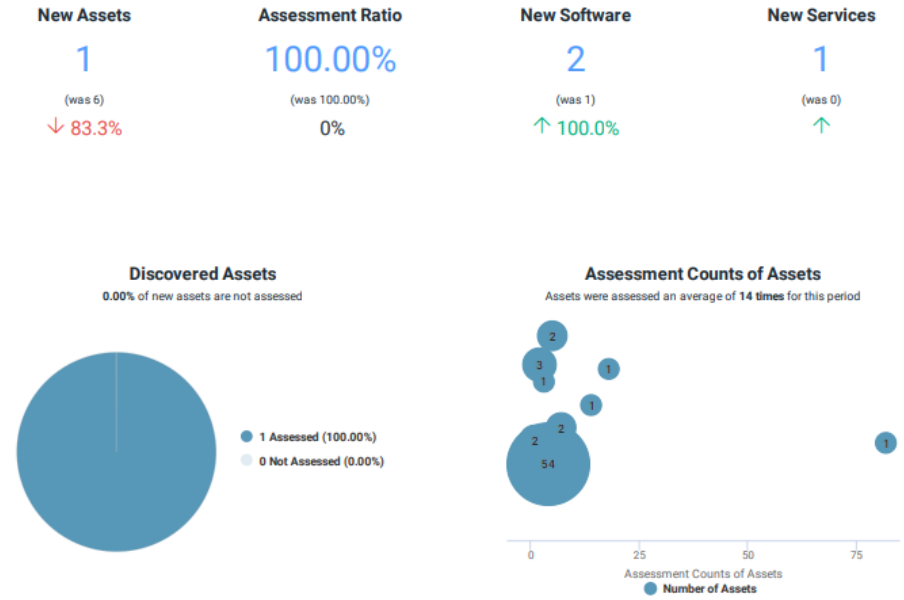




Ako aktuálny stav vhodne interpretovať?

- Využitie šablón automatických reportov
- Pravidelné zasielanie reportov na kľúčových ľudí





Ako zraniteľnosti odstrániť?

- Návrh opatrení na odstránenie zraniteľností
- Projekty zamerané na remediácie

Solution	Asset Co...	Vulnerabili...	Total Risk
2022-08 Cumulative Update for Windows Server ...	9	7,802	2.83m
2022-08 Cumulative Update for Windows Server ...	2	720	163.11k
Upgrade kernel	1	375	144.93k
Upgrade tcpdump	3	165	94.73k
Upgrade php5	1	142	75.21k

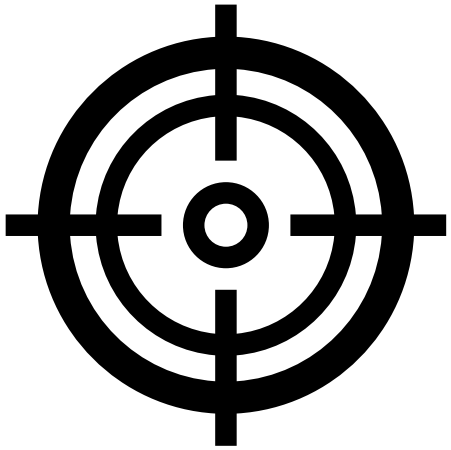
Project Name	Work Remaining
Remediate critical vulnerabilities	94%
Skoleni Windows Servery	86%
SRV Net DC	83%

Sú zraniteľnosti naozaj odstránené?

- Skeny po odstránení zraniteľností
- Kontrola správnosti nasadenia patchov

Sken zraniteľností

- Jednorázový
- Chýbajúci progres
- Cena



Vulnerability Management

- Reakcia na Zero-Day
- Prioritizácia assetov
- Riadenie remediácií
- Neustály prehľad
- Pravidelné skeny
- Cena

Apache Log4Shell – CVE-2021-44228

2021-11-24
Zraniteľnosť objavená a nahlásená vendorovi

2021-12-01
Prvý známy pokus o exploit

2021-12-06
Vydaná verzia Log4j 2.15.0

2021-12-09
Prvá publikácia na Twitteri

2021-12-10
CVE publikované
Začiatok patchovania

2021-12-13
Vydaná verzia Log4j 2.16.0
Opravená CVE-2021-45046 (DoS)

2021-12-17
CVE-2021-45046 povýšená na **kritickú** (RCE)

2021-12-17
Vydaná verzia Log4j 2.17.0
Opravená CVE-2021-45105 (DoS)

2021-12-28
Vydaná verzia Log4j 2.17.1
Opravená CVE-2021-44832 (RCE)

2022-01-18
Publikované ďalšie Log4j zraniteľnosti (CVE-2022-23307, CVE-2022-23305, CVE-2022-23302)

Výber vulnerability managementu

- Background vendora:
  - Vlastný security researcher tím
  - Robustná databáza
  - Komunitné projekty
- Prehľadnosť a user-friendly GUI
- Integrácie s tretími stranami
- Platforma

RAPID7 insightVM

- Background vendora:
  - Vlastný security researcher tím
  - Robustná databáza
  - Komunitné projekty – **Metasploit Framework**

Apache Log4Shell – CVE-2021-44228

2021-11-24
Zraniteľnosť objavená a nahlásená vendorovi

2021-12-01
Prvý známy pokus o exploit

2021-12-06
Vydaná verzia Log4j 2.15.0

2021-12-09
Prvá publikácia na Twitteri

2021-12-10
CVE publikované
Začiatok patchovania

2021-12-13
Vydaná verzia Log4j 2.16.0
Opravená CVE-2021-45046 (DoS)

2021-12-17
CVE-2021-45046 povýšená na **kritickú** (RCE)

2021-12-17
Vydaná verzia Log4j 2.17.0
Opravená CVE-2021-45105 (DoS)

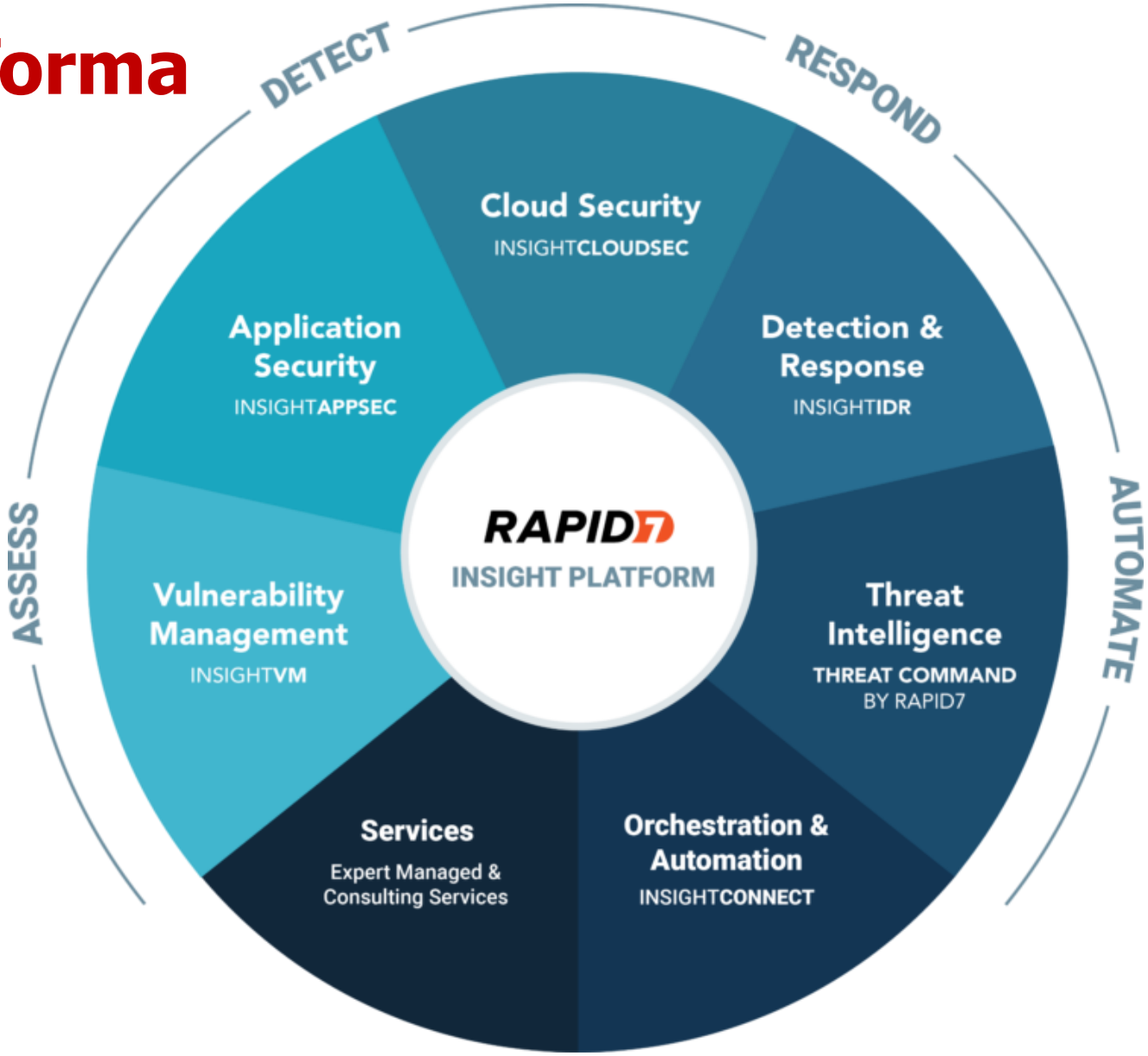
2021-12-28
Vydaná verzia Log4j 2.17.1
Opravená CVE-2021-44832 (RCE)

2022-01-18
Publikované ďalšie Log4j zraniteľnosti (CVE-2022-23307, CVE-2022-23305, CVE-2022-23302)

RAPID7 insightVM

- Background vendora:
  - Vlastný security researcher tím
  - Robustná databáza
  - Komunitné projekty – **Metasploit Framework**
- Prehľadnosť a user-friendly GUI
- Integrácie s tretími stranami:
  - **SIEM, Jira, ServiceNow, VMware, AWS, Trellix ePO**
- Insight Platforma

Insight platforma



COMGUARD
communication security

Ďakujem za pozornosť!

Ondrej Malík | ondrej.malik@comguard.cz