SIEM A SOC, DVA PILIERE KYBERNETICKEJ BEZPEČNOSTI OD SPOLOČNOSTI ARICOMA

ARICOMA

Proč je řešení spojující produkty IBM SIEM QRadar a know-how ARICOMA úspěšnou kombinací pro naplnění bezpečnostních cílů našich zákazníků.

Leoš Stránský / Head of IBM Department

21. 03. 2024

IBM Security

Stojíme na pevných základech

ARICOMA

Od roku 2017 budujeme značku Aricoma na základech firem s bohatou historií.

AUTOCONT
Založeno 1990

AEC
Založeno 1991

C-E-S-E-A
Založeno 2019

KOMIX
Založeno 1992

DataSpring
Založeno 2010

internet projekt
Založeno 2001

Cloud4com
Založeno 2010

sabris consulting
Založeno 1994

4U CONSULTING
Založeno 2000

SYSCOM SOFTWARE
Založeno 1994

EUR +400M
tržeb v roce 2023

EUR 23m
EBITDA v roce 2023

> 1 500
profesionálů

> 30
lokalit

> 6 000
klientů

3 500
certifikací

Qinshift

Sesterská společnost věnující se vývoji softwaru na zakázku pro komerční sféru.

28 lokalit
+200 mil EUR tržeb
+300 klientů
+3500 profesionálů

Cleverlance

seavus

MusalaSoft

STRATITEC

CLEARCODE

PROČ se zabývat SIEM a SOC - Legislativní rámec

- EU legislativa - směrnice EU, č. 2016/679 – GDPR
  - GDPR (General Data Protection Regulation). Účinné od 25. 5. 2018. Subjekty musí zajistit
    - průkaznou evidenci přístupu a práce (manipulace) pro systémy s osobními údaji
    - Řízený proces detekce a hlášení bezpečnostních incidentů
  - NIS2 (Network and Information Security 2). Účinné od 18. 10. 2024. Subjekty musí zajistit
    - Řízený proces detekce a hlášení bezpečnostních incidentů

- Regutaltorní požadavky pro nadnárodní společnosti
  - Reportovací standardy: ISO 27000, SOX, BASELII

- Národní legislativa – ZÁKON 69/2018 o kybernetickej bezpečnosti
  - § 20 – nástroj pro detekciu kybernetických bezpečnostných incidentov
- Národní legislativa – Vyhláška 362/2018 Z. z.
  - § 14 a § 15 – nástroj pro monitorování kybernetických bezpečnostných

Nasazujeme silný produkt - QRadar a jeho pozice na trhu

- 10 let trvale umístěný v leader kvadrantu
- 100+ implementací v CZ/SK
- Existuje rozsáhlá partnerská síť
- ARICOMA má významný tržní podíl na tomto trhu

Figure 1: Magic Quadrant for Security Information and Event Management

Udržujeme nejvyšší úroveň kompetence

- K dispozici je kompletní dedikovaný realizační a dohledový tým na QRadar:
  - Presale specialisté
  - Projektový vedoucí
  - Specialisté pro nasazení
  - Vývoj aplikací
  - Specialisté pro SOC dohled
- Dohledové centrum 7 x 24
- Certifikace (QRadar MIX, CompTIA, RedHat)
- Pracovníci s prověrkou NBÚ

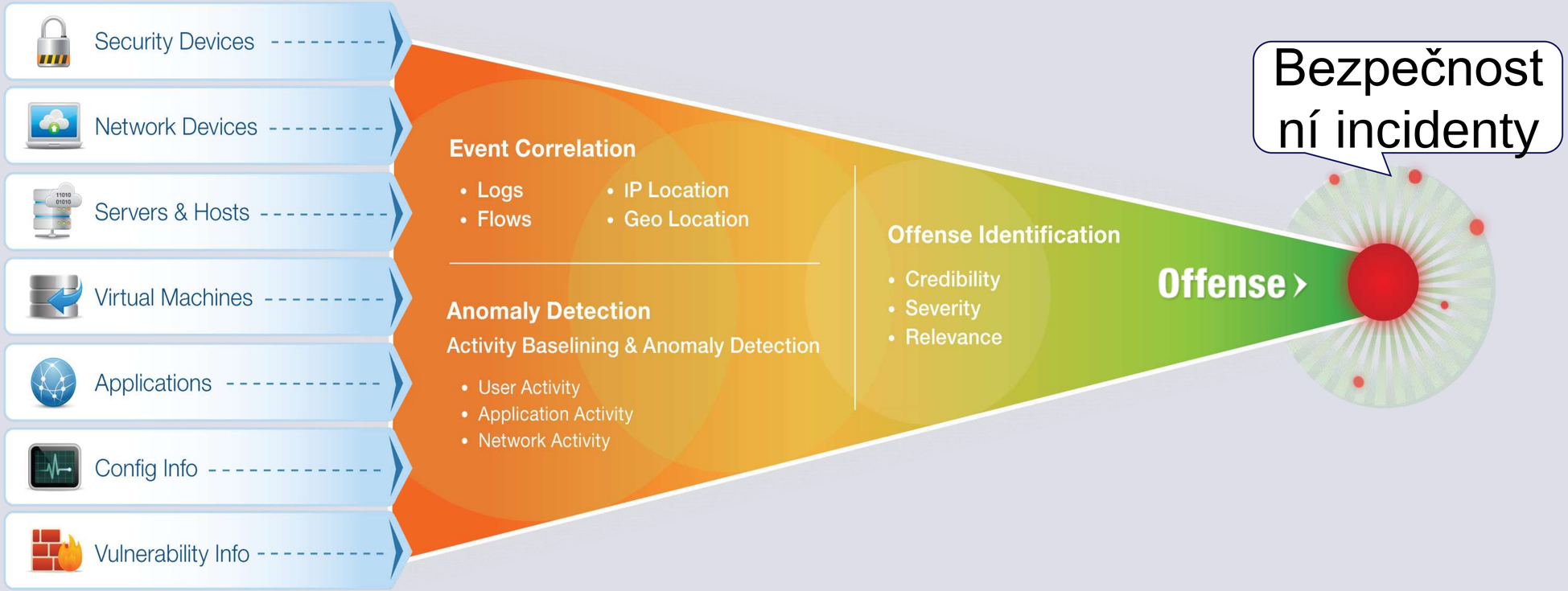
Společnost IBM Česká republika, spol. s r.o., sídlem V Parku 2294/4, 148 00 Praha 4-Chodov potvrzuje, že společnost Aricoma Systems, splňuje požadovaná kritéra a požadavky programu IBM Partner Plus™ a je pro rok 2024 **IBM GOLD BUSINESS PARTNER**.

Společnost Aricoma Systems a.s. disponuje k dnešnímu dni těmito certifikacemi:

PG00010 – Cloud Pak for Business Automation – Decision Management and FileNet
PG00038 – Power Systems Infrastructure
PG00039 – Power Systems Solution
PG00042 – Guardium Insights
PG00046 – Xforce Threat Intelligence
PG00047 – Security Orchestration and Response (SOAR)
PG00048 – QRadar EDR & XDR
PG00051 – Verify Governance
PG00055 – Storage for Hybrid Cloud
PG00057 – Storage for IBM Z
PG00058 – Storage for Data Resilience
PG00075 – IBM Cloud Pak for Security – Qradar XDR
PG00076 – IBM FlashSystem
PG00077 – QRadar Security Information and Event Management (SIEM)

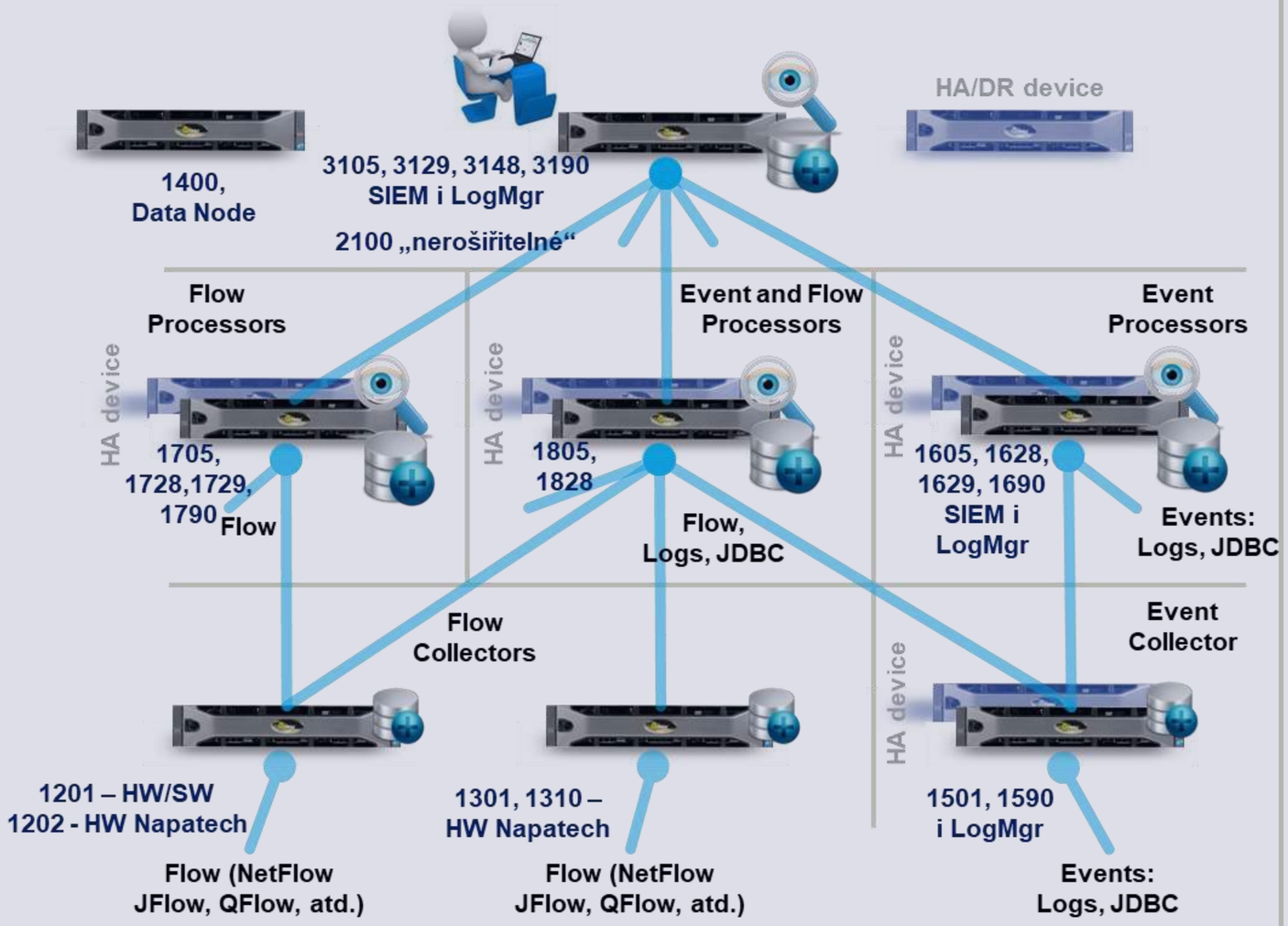
Princip SIEM

Produkt v reálném čase analyzuje (agreguje, koreluje) bezpečnostní události a toky generované zařízeními a aplikacemi v síti.



Extrémní množství dat + Pokročilá technologie = Vysoká úroveň viditelnosti a přesnosti detekce

All-in-one a distribuovaná infrastruktura



Existuje jako **All-in-One zařízení nebo pouze konzole** pro distiribuovanou architekturu. Je možný plynulý přechod z A-i-O na distribuovanou architekturu.
Pozn.: HA zařízení mají synchronní data i konfigurace.

Processor: Zvládá funkci Collectoru + provádí vyhodnocení dat dle pravidel a zajistí i jejich dlouhodobé ukládání.

Collector: provádí sběr a normalizaci dat. Data hromadí po kratší dobu, obecně max. po dobu výpadku spojení nebo při nastavení dávkového přenosu.

QRadar SIEM – klíčové vlastnosti

- QRadar, to je SIEM, Logmanagement a Flow sonda v jednom produktu, v jedné konzoli a pod jedním know-how.
- Není třeba kupovat samostatný Log Management ani Flow sondy.
- Není třeba se rozhodovat mezi velkým a malým boxem. Výkon QRadaru Vám stanovíme na míru a tedy za optimální náklady.
- QRadar nasadíme na Vašem HW nebo ve virtualizaci.
- QRadar je napojený na IBM X-Force. Obsahuje algoritmy strojového učení a komunikuje s umělou inteligencí.

QRadar má dva způsoby licencování

QRadar je možné licencovat na „Kapacitu“ nebo na „Enterprise“.
QRadar licence jsou začleněny do těchto balíků:

QRadar legacy

Licencuje se infrastruktura SIEM
- INSTALL, NODE, HA licence

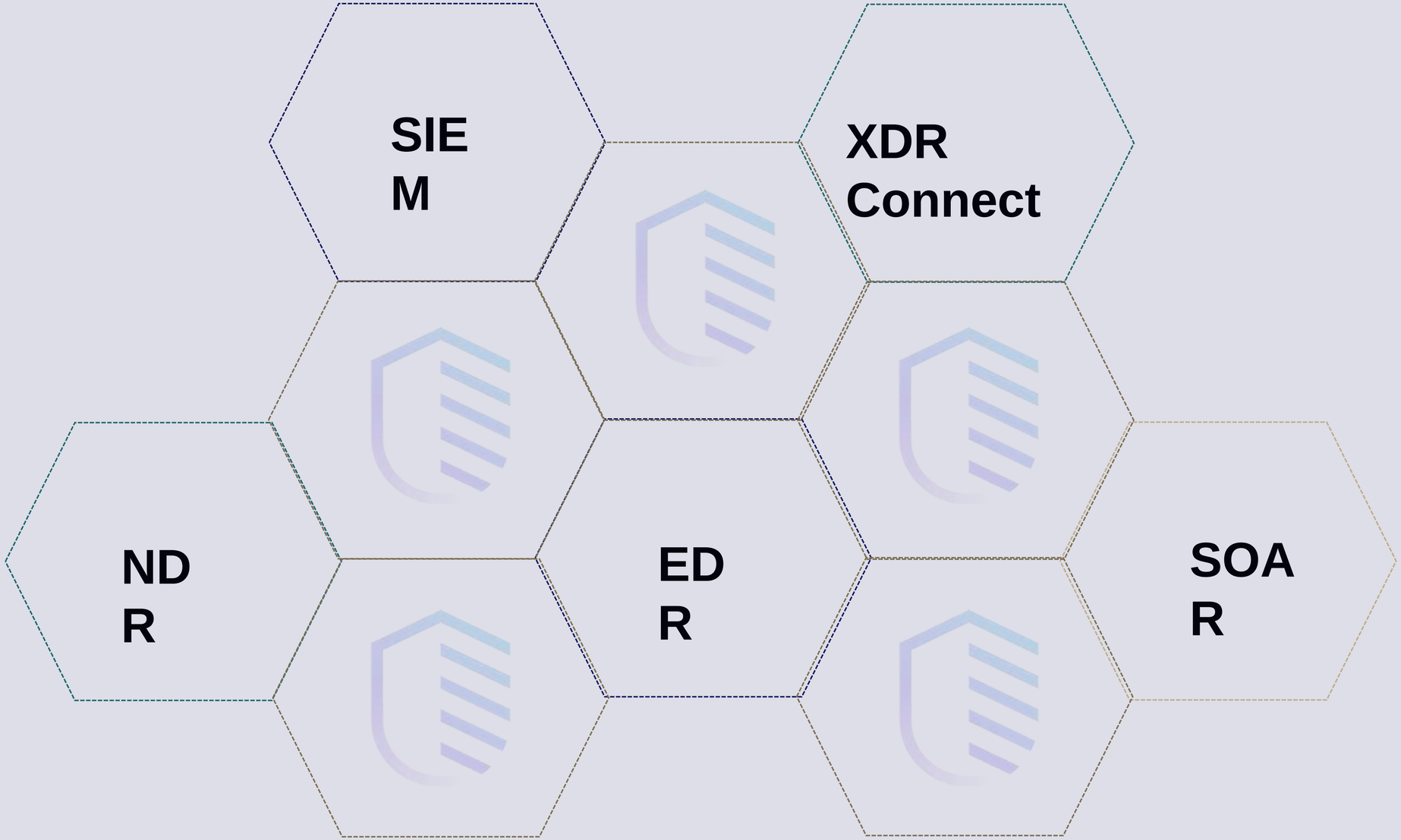
Licencuje se kapacita
- EPS, FPM, DataStore licence

QRadar Suite

„Enterprise“ - licencuje se podle počtu MVs (serverů)
- EPS a FPM vždy dostatečné
- Neomezená QRadar infrastruktura

„Usage“ - licencuje se kapacita
- EPS a FPM
- Neomezená QRadar infrastruktura

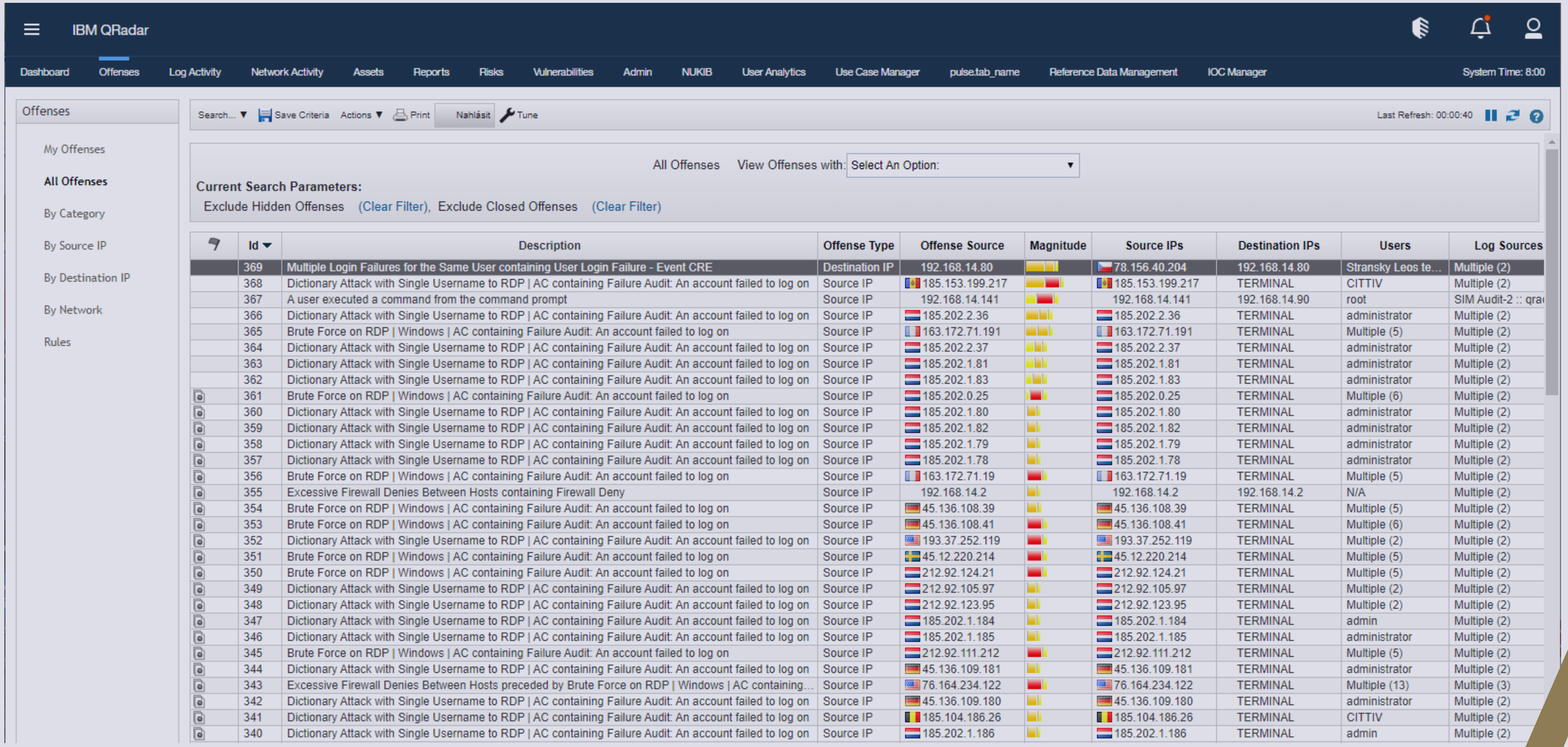
QRadar SUITE – moderní licenční program



QRadar SIEM – Dashboard

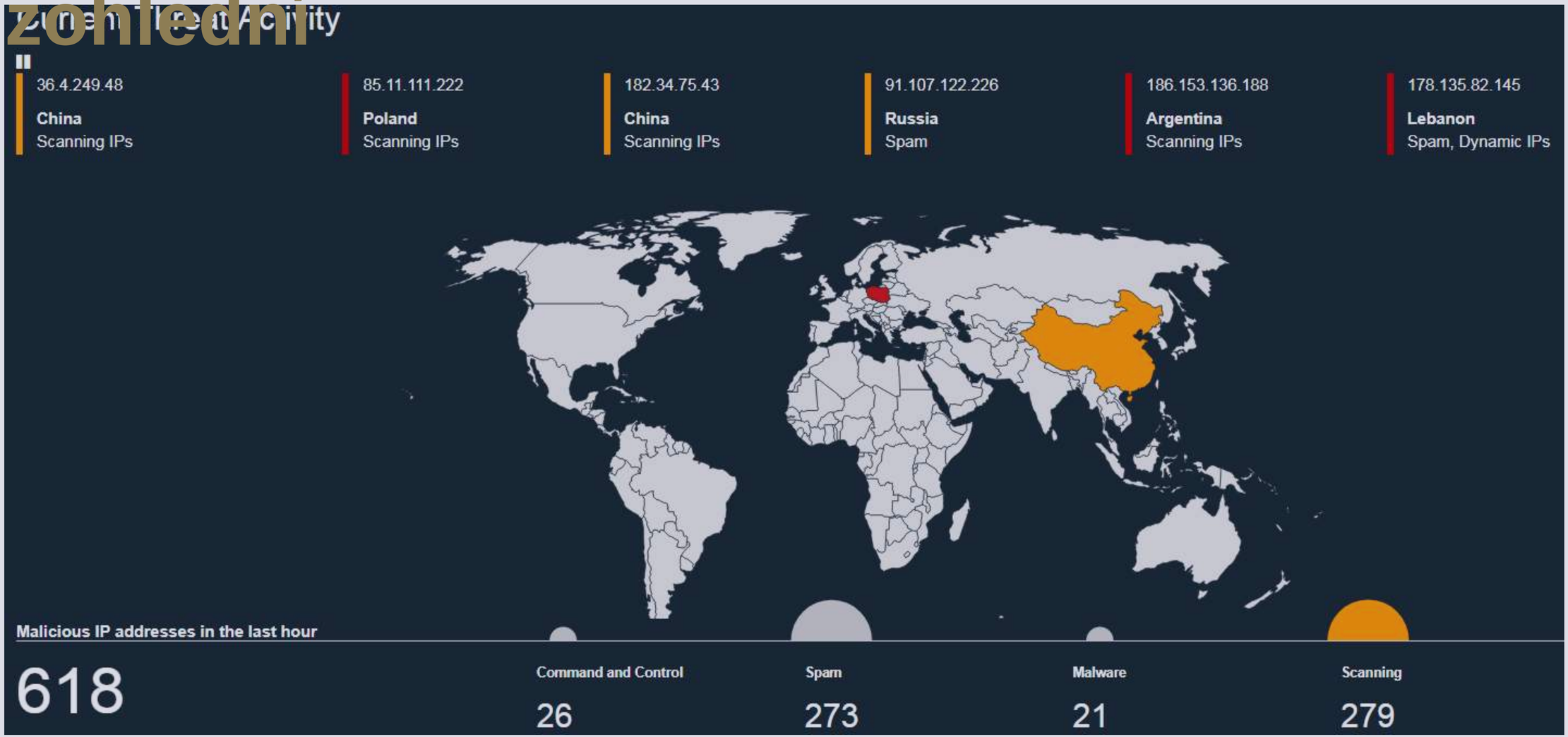
ARICOMA

QRadar SIEM – Dashboard - KBU

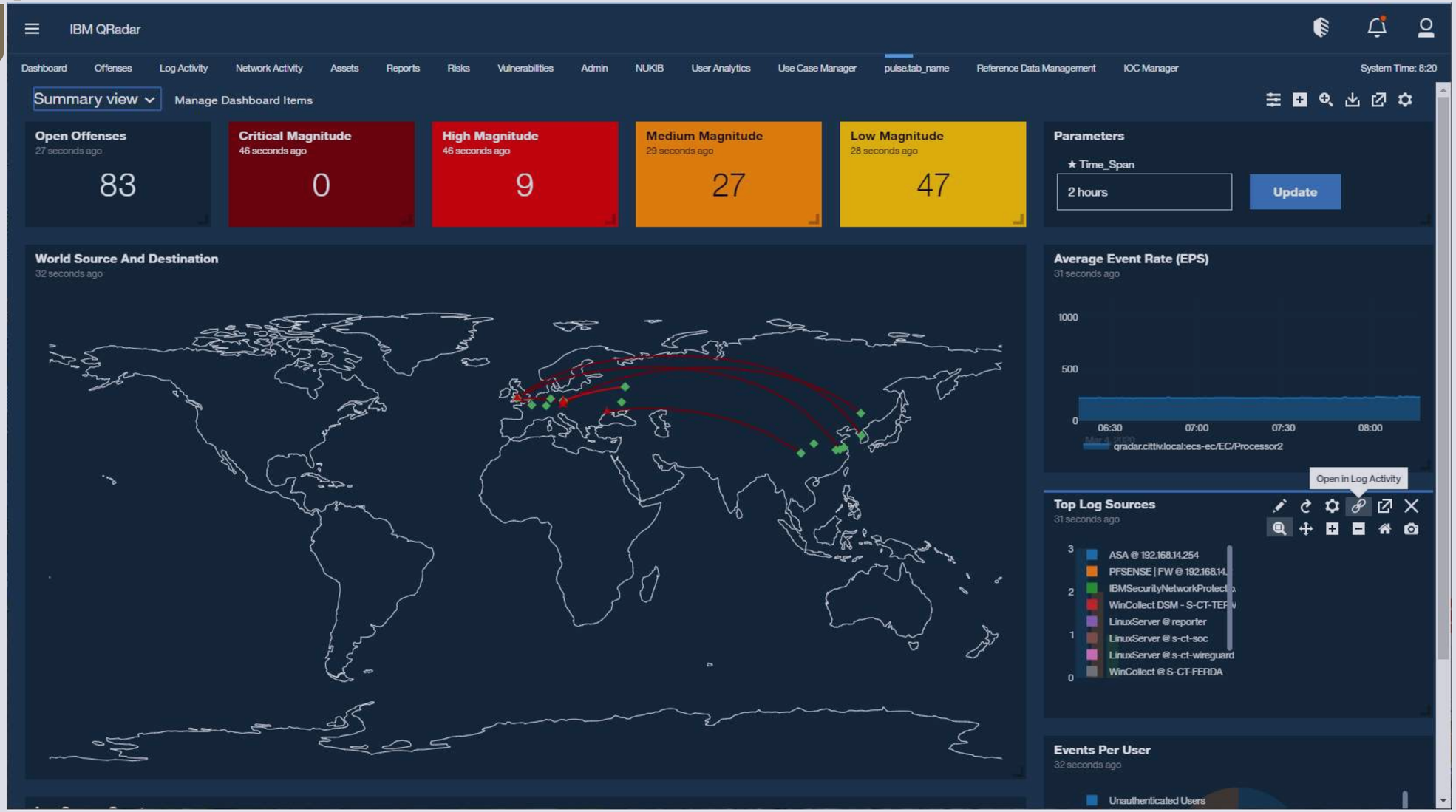


Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
369	Multiple Login Failures for the Same User containing User Login Failure - Event CRE	Destination IP	192.168.14.80		78.156.40.204	192.168.14.80	Stransky Leos te...	Multiple (2)
368	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.153.199.217		185.153.199.217	TERMINAL	CITTIV	Multiple (2)
367	A user executed a command from the command prompt	Source IP	192.168.14.141		192.168.14.141	192.168.14.90	root	SIM Audit-2 :: qra
366	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.2.36		185.202.2.36	TERMINAL	administrator	Multiple (2)
365	Brute Force on RDP | Windows | AC containing Failure Audit: An account failed to log on	Source IP	163.172.71.191		163.172.71.191	TERMINAL	Multiple (5)	Multiple (2)
364	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.2.37		185.202.2.37	TERMINAL	administrator	Multiple (2)
363	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.1.81		185.202.1.81	TERMINAL	administrator	Multiple (2)
362	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.1.83		185.202.1.83	TERMINAL	administrator	Multiple (2)
361	Brute Force on RDP | Windows | AC containing Failure Audit: An account failed to log on	Source IP	185.202.0.25		185.202.0.25	TERMINAL	Multiple (6)	Multiple (2)
360	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.1.80		185.202.1.80	TERMINAL	administrator	Multiple (2)
359	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.1.82		185.202.1.82	TERMINAL	administrator	Multiple (2)
358	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.1.79		185.202.1.79	TERMINAL	administrator	Multiple (2)
357	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.1.78		185.202.1.78	TERMINAL	administrator	Multiple (2)
356	Brute Force on RDP | Windows | AC containing Failure Audit: An account failed to log on	Source IP	163.172.71.19		163.172.71.19	TERMINAL	Multiple (5)	Multiple (2)
355	Excessive Firewall Denies Between Hosts containing Firewall Deny	Source IP	192.168.14.2		192.168.14.2	192.168.14.2	N/A	Multiple (2)
354	Brute Force on RDP | Windows | AC containing Failure Audit: An account failed to log on	Source IP	45.136.108.39		45.136.108.39	TERMINAL	Multiple (5)	Multiple (2)
353	Brute Force on RDP | Windows | AC containing Failure Audit: An account failed to log on	Source IP	45.136.108.41		45.136.108.41	TERMINAL	Multiple (6)	Multiple (2)
352	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	193.37.252.119		193.37.252.119	TERMINAL	Multiple (2)	Multiple (2)
351	Brute Force on RDP | Windows | AC containing Failure Audit: An account failed to log on	Source IP	45.12.220.214		45.12.220.214	TERMINAL	Multiple (5)	Multiple (2)
350	Brute Force on RDP | Windows | AC containing Failure Audit: An account failed to log on	Source IP	212.92.124.21		212.92.124.21	TERMINAL	Multiple (5)	Multiple (2)
349	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	212.92.105.97		212.92.105.97	TERMINAL	Multiple (2)	Multiple (2)
348	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	212.92.123.95		212.92.123.95	TERMINAL	Multiple (2)	Multiple (2)
347	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.1.184		185.202.1.184	TERMINAL	admin	Multiple (2)
346	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.1.185		185.202.1.185	TERMINAL	administrator	Multiple (2)
345	Brute Force on RDP | Windows | AC containing Failure Audit: An account failed to log on	Source IP	212.92.111.212		212.92.111.212	TERMINAL	Multiple (5)	Multiple (2)
344	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	45.136.109.181		45.136.109.181	TERMINAL	administrator	Multiple (2)
343	Excessive Firewall Denies Between Hosts preceded by Brute Force on RDP | Windows | AC containing...	Source IP	76.164.234.122		76.164.234.122	TERMINAL	Multiple (13)	Multiple (3)
342	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	45.136.109.180		45.136.109.180	TERMINAL	administrator	Multiple (2)
341	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.104.186.26		185.104.186.26	TERMINAL	CITTIV	Multiple (2)
340	Dictionary Attack with Single Username to RDP | AC containing Failure Audit: An account failed to log on	Source IP	185.202.1.186		185.202.1.186	TERMINAL	admin	Multiple (2)

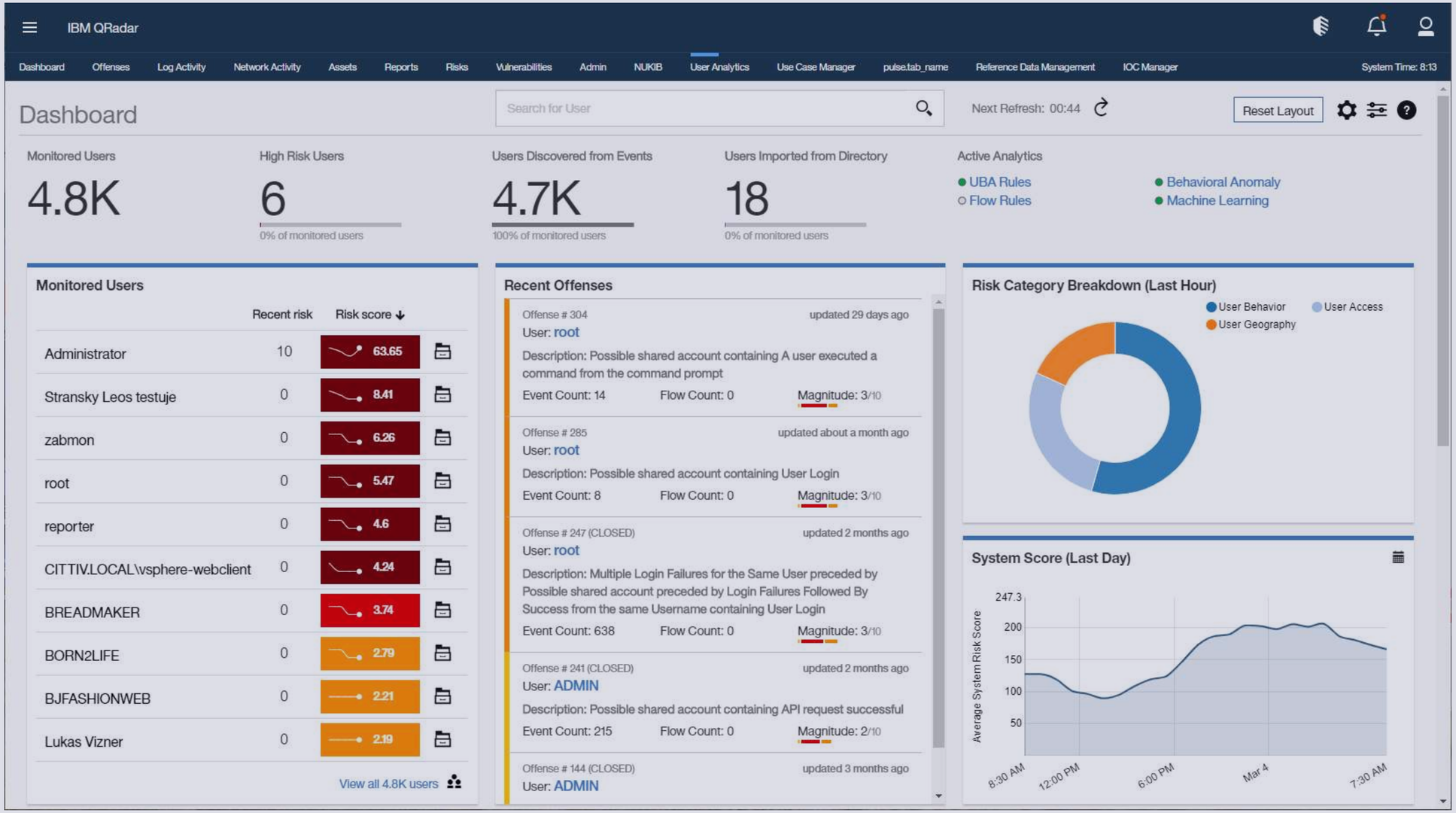
QRadar SIEM – aktuální hrozby, které SIEM zohlední



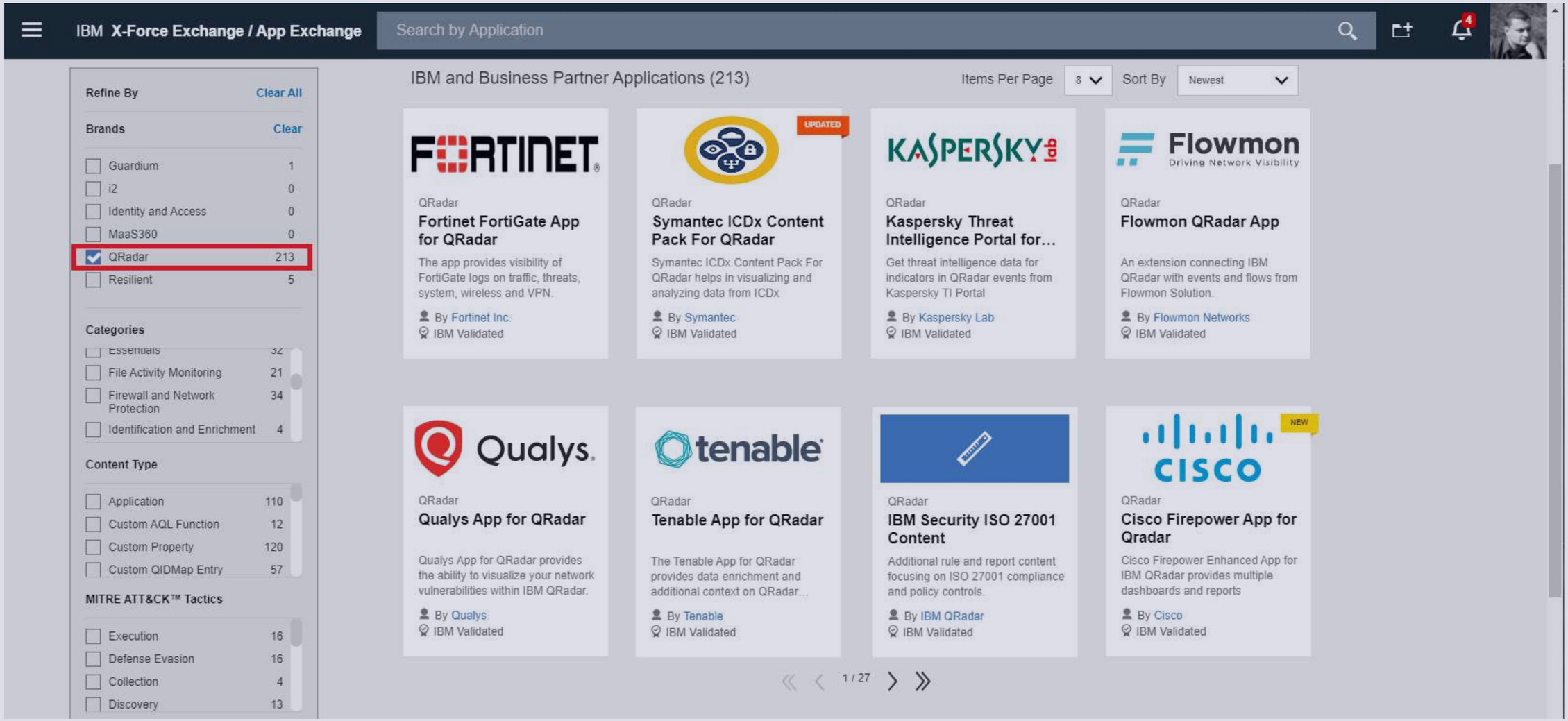
QRadar SIEM – aktuální hrozby které se Vás týkají



QRadar SIEM – analýza chování uživatelů s využitím strojového učení



QRadar SIEM – X-Force APP market




Efektivnější
bezpečnostní dohled
s QRadar
Zjistit více
ARICOMA

Pokrýváme celý životní cyklus provozování SIEM

Implementace

- analýza
- vlastní nasazení
- testovací provoz
- dokumentace
- školení

Servisní podpora

- health-check
- aktualizace
- administrace
- nové zdroje logů
- úpravy pravidel
- metodická podpora

Bezpečnostní dohled

- dohled s SLA
- vyhodnocování
- notifikace
- měsíční zprávy
- projektové vedení

QRadar SIEM, servisní a SOC program

Servisní a SOC program ARICOMA je pouze pro zákazníky
u kterých implementujeme nebo převezmeme QRadar.

Na servisním programu se stále podílejí kolegové, kteří systém implementovali.
ARICOMA má vlastní dohledové centrum na QRadar.

Servisní program obsahuje:

- Služby technické podpory a rozvoje – poskytují primárně kolegové s certifikaci QRadar Deployment Professional + doplňující certifikace RedHat, Tenable

- Služby kybernetického dohledu (SOC) – poskytují primárně kolegové s certifikacemi QRadar Administrator, CompTIA Security+ a s doplňujícími certifikacemi

Služby servisní podpory a rozvoje

- Poskytuje se v režimu 5 x 8 a sjednává se na objem MD nebo hodin měsíčně. Trvání minimálně rok.

- Obsahuje služby podpory a drobného rozvoje:
  - Health-check a administrace
  - Aktualizace log sources,
  - Úpravy pravidel, plnění referenčních setů, apod.
  - Konzultace k řešení problémových stavů
  - Konzultace k Offenses (na žádost zákazníka, pokud nemá SOC)

- Obsahuje služby aktualizace:
  - Pravidelné major-updates

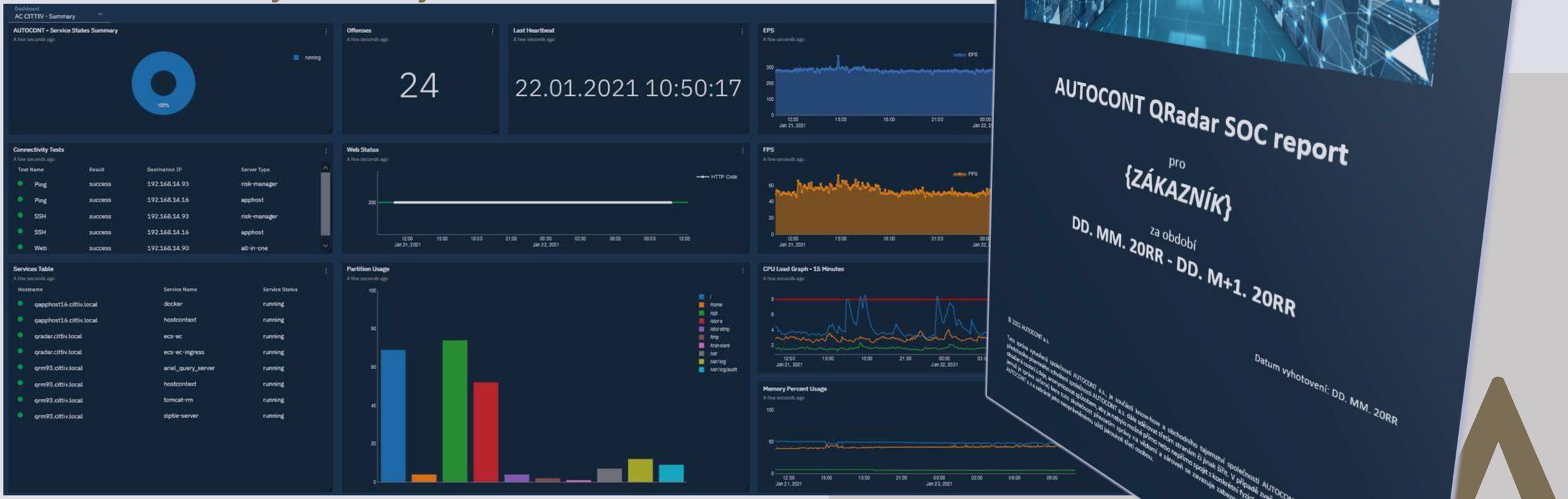
Služba kybernetického dohledu (SOC)

- Služba SOC je poskytována v režimu 5 x 8 (varianta „Basic“
  a „Standard“), nebo 7 x 24 „Nonstop“. Minimálně na rok.
- Obsahuje část zavedení služby (součást měsíční ceny):
  - Napojení QRadar na SOC
  - Sestavení komunikační matice kontaktů specialistů

- a část provozování služby:
  - Přistupování na zákazníkův QRadar. Řeší se všechny Offenses.
  - Řeší se ve dvou úrovních závažnosti – Analytik a Expert.
  - Za každý měsíc je vyhotovena zpráva o SOC službě.
  - Šetření probíhá přímo v prostředí QRadar SIEM
  - Žádná citlivá data nejsou uložena u poskytovatele služby
  - Služba je poskytována z CZ/SK tedy v rámci EU

Servis a SOC

- V rámci servisního programu je každý QRadar napojený zabezpečeným kanálem na centrální dohled
- SOC služby realizuje ARICOMA SOC Slovensko



QRadar SIEM – co projekt implementace obnáší?

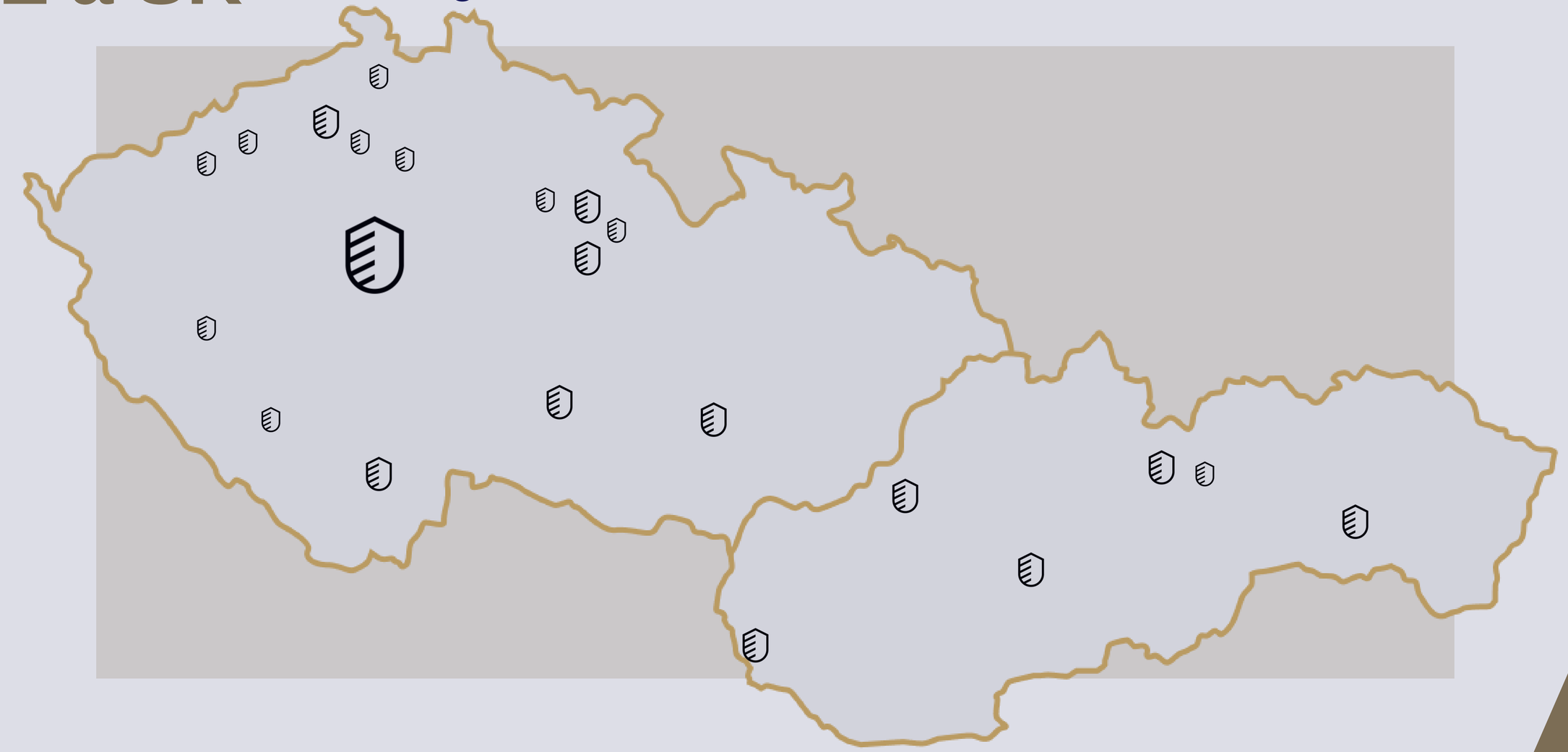
- Dobře poznat svoji síť, své uživatele, logy a jejich kvalitu ve Vašich systémech a aplikacích
- Vždy je potřeba začít analýzou
- Bude potřeba pořídit HW, SW, implementaci, servis a služby SOC na několik let
- Rozsah od 50.000 EUR do 500.000 EUR
- Implementace 3 až 9 měsíců (analýza, nasazení, testy, dokumentace, zaškolení)
- Služby servisní podpory a rozvoje. SOC služby 5 x 8 nebo 7 x 24

QRadar SIEM – ARICOMA reference

- Vzhledem k bezpečnostní strategii již neuvádíme konkrétní zákaznické REFERENCE
- Zákazníci jsou z CZ a SK
- Segmenty Finančnictví a pojišťovnictví, Státní správa, Zdravotnictví, Industry a Utility
- 90% zákazníků má servis, zbytek si objednává ad-hoc služby
- 100% zákazníků obnovuje licenční maintenance

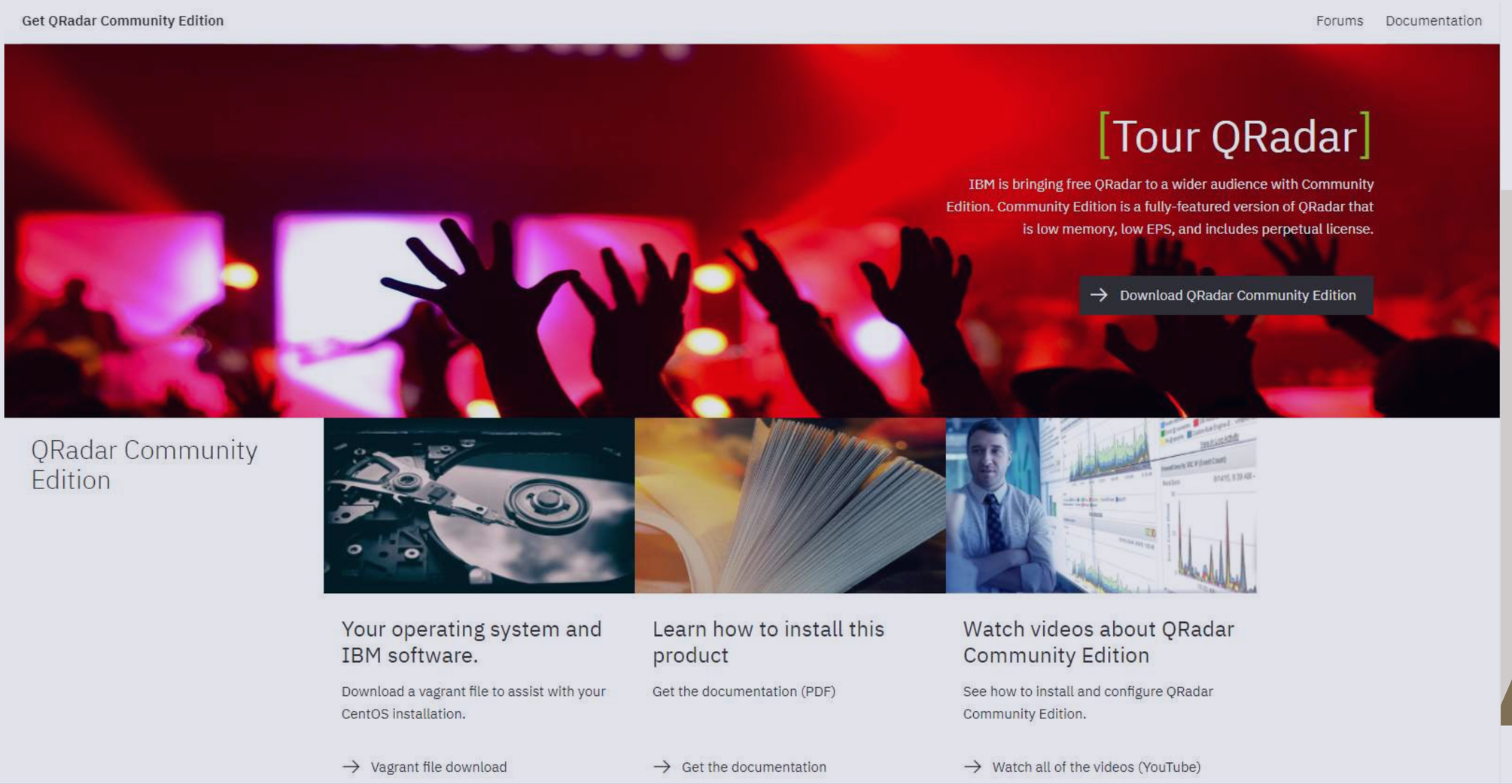
QRadar jsme nasadili na mnoha místech v CZ a SK

Reference ve všech segmentech



Vyzkoušejte zdarma

- https://exchange.xforce.ibmcloud.com/
- https://developer.ibm.com/qradar/ce/



ARICOMA

Leoš Stránský

Head of IBM Department
IBM Champion

ARICOMA