Konečně přátelský bezpečnostní dohled aneb pohádka o ELISE a EKRANOVI

DATA SYS

spolehlivě · nejvýhodněji

AGENDA

MOTIVACE A PARAGRAFY

AUTOMATIZACE A KORELACE

ZVUČNÉ REFERENCE

LOG MANAGEMENT

POHÁDKA O ELISE A EKRANOVI

PŘIROVNÁNÍ

INTERNET
obsahuje množství informací.

Internetové vyhledávače
je sbírají a indexují.

Využíváte je pro
rychlé nalezení odpovědí **!!!**

INFORMAČNÍ SYSTÉMY
generují množství informací

Log management nástroje
je sbírají a indexují.

Využíváte je pro
rychlé nalezení odpovědí **???**

CO ZJISTÍTE?

Z JAKÝCH MÍST LIDÉ PŘISTUPUJÍ NA FIREMNÍ WEB?

KDO PROVEDL ZMĚNU V DATABÁZI?

KTEŘÍ UŽIVATELÉ STAHUJÍ NEJVÍCE DAT Z INTERNETU?

KDO SMAZAL SOUBORY NA SDÍLENÉM DISKU?

K JAKÝM CHYBÁM DOCHÁZÍ V PODNIKOVÉM IS?

KDO SE SNAŽÍ UHÁDNOUT PŘÍSTUPOVÉ HESLO?

POŽADAVKY ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI: §22

§22 - Zaznamenávání událostí informačního a k u, jeho uživatelů a administrátorů

Povinná osoba

- ✓ **zaznamen** ch aktiv
- ✓ **vodce** a sběr informací
- **ktiva a účtu a (ne)úspěšnost činnosti**
- dací **před neoprávněným čtením a změnou**
- ✓ **konkrétních typů činností**

Zaznamenávat určité činnosti
Ukládat logy pro vyhledávání
Zajistit jejich ochranu

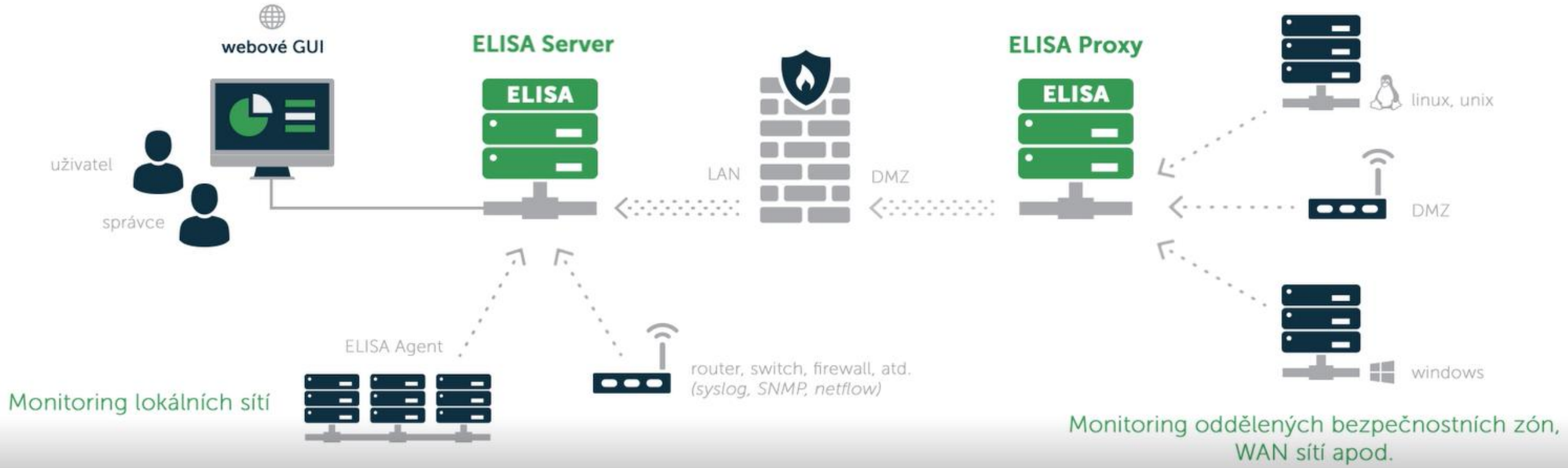
DATA SYS

PŘÁTELSKÝ LOG MANAGEMENT

ELISA LM/SIEM

ZÍSKÁTE CENTRÁLNÍ KONZOLI BEZPEČNOSTNÍHO DOHLEDU

Je to vcelku jednoduchá disciplína ☺

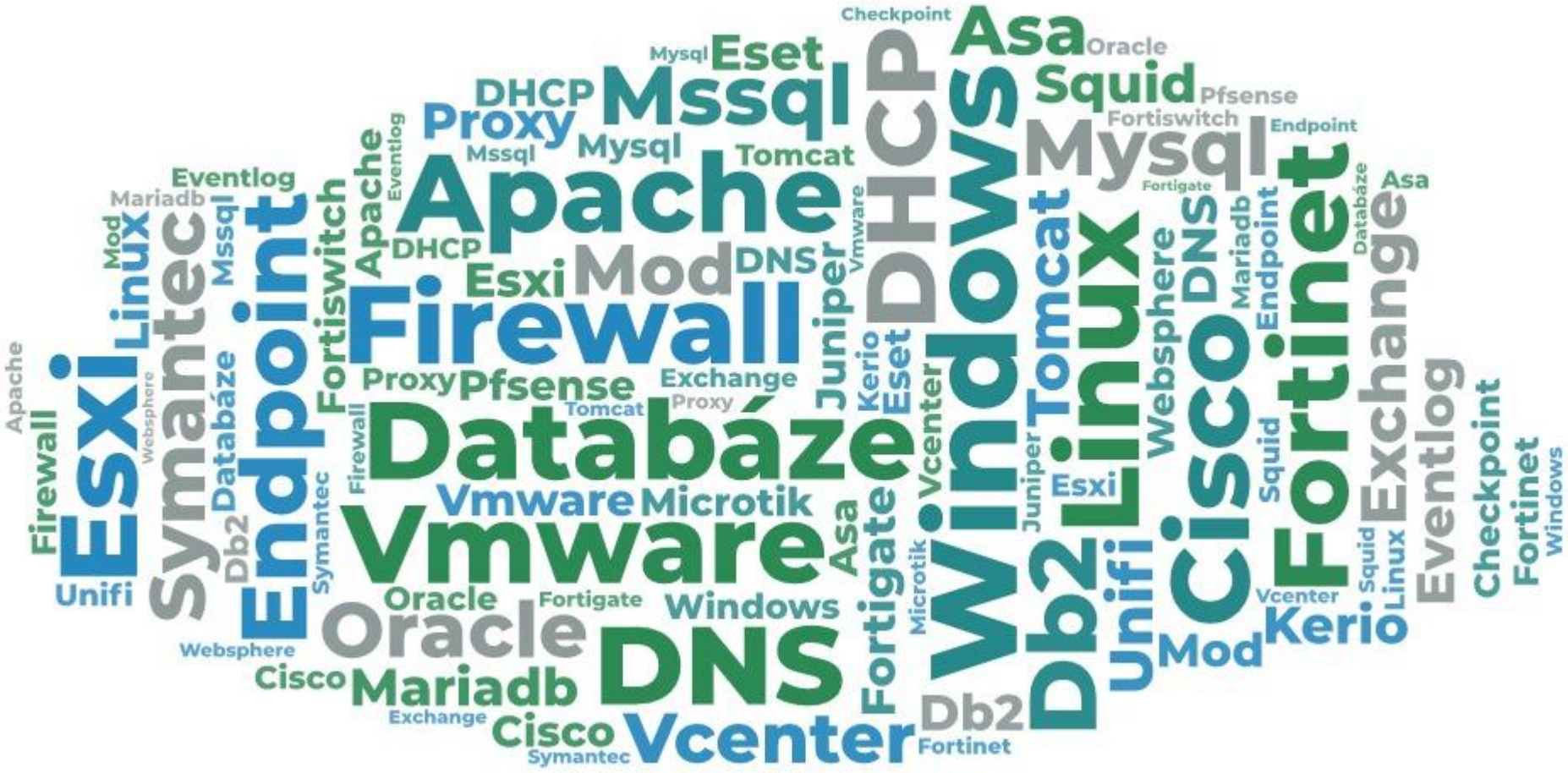


CO OD ELISA ČEKAT ?

- Rychlé odezvy
- Snadno nastavitelné filtry
- Distribuovaný sběr logů
- Centrální správa agentů

ZDROJE LOGŮ

PODPORA PRAKTICKY VŠECH ZDROJŮ DAT …



ZABUDOVANÝ ZABBIX

K TOMU JEŠTĚ NĚCO NAVÍC! PROVOZNÍ MONITORING!

Nejpopulárnější nástroj! Nadupaný a svobodný!

DATA SYS

AUTOMATIZACE KORELAČNÍMI PRAVIDLY

OD LOG MANAGEMENTU K NÁSTROJI TYPU SIEM

- Automatizované vyhodnocování
  - ✓ Normalizace a systematizace dat
  - ✓ Propracovanější alarmy a notifikace
  - ✓ Korelace – nalézání vzájemných vztahů

- Výpočet míry rizika
  - ✓ Různě hodnotná aktiva
  - ✓ Zabudovaný „Change Auditor”
  - ✓ Zjišťování a řízení zranitelností

ELISA SECURITY MANAGER

Robustní nástroj pro sběr a analýzu bezpečnostních událostí

Získáváte chytřejší konzoli bezpečnostního dohledu

Využijte na maximum i naše bezpečnostní specialisty!

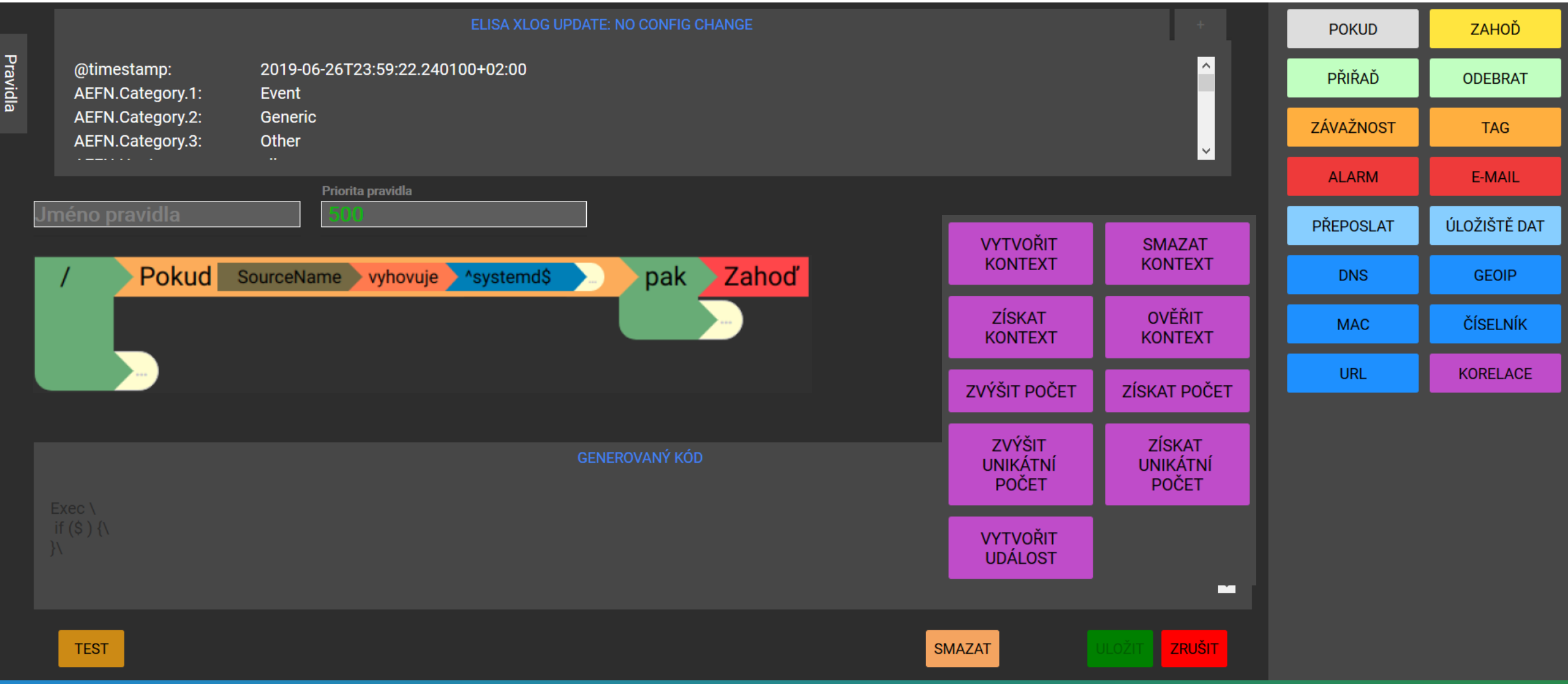
ELISA SECURITY MANAGER

DATA SYS

KORELOVANÉ UDÁLOSTI - VZOR

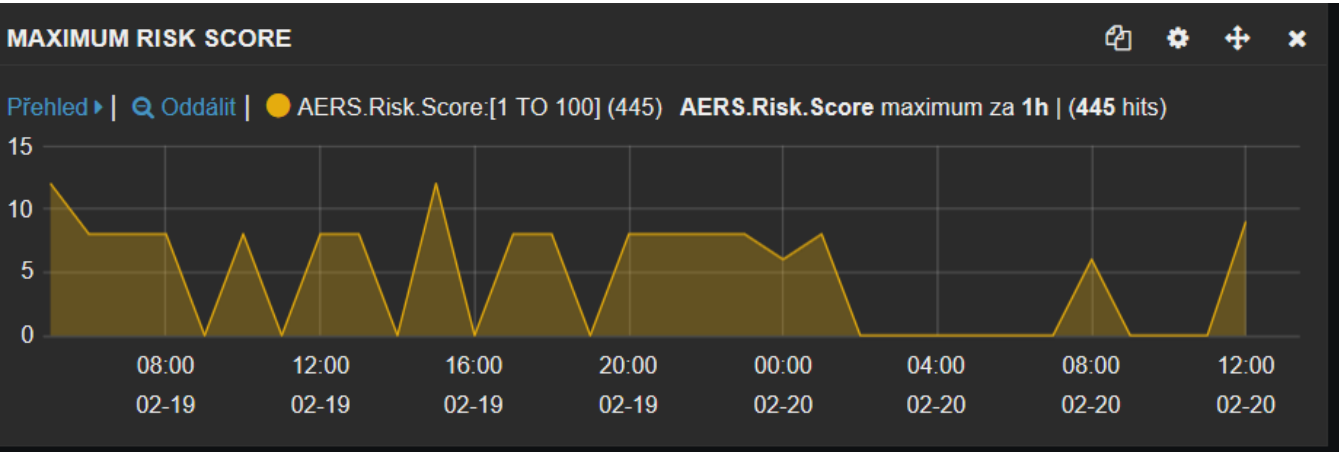
Typ události	Závažnost	Obvyklý účel vyhodnocovaní a upřesnění	Třída a typ incidentu	ESM Id	Dashboardy | Filtry (v GUI)
Privilegované přihlášení	**NOTICE**	Přehled úspěšných přihlášení privilegovanými účty s rozlišením servisních a dávkových úloh. Pro přihlášení do Windows detekováno z přiřazení privilegií, pro ostatní zdroje dle seznamu účtů.	Other *Authentication*	0111	Alarmy: Privilegovaná přihlášení
Hádání hesla	**WARN**	Detekce pokusů o zneužití cizí identity. Rozlišováno několik úrovní dle počtu opakování.	Intrusion attempt *Login attempts*	4211	Alarmy: Neúspěšná přihlášení
Hádání hesla hrubou silou	**MAJOR**	Detekce automatizovaných pokusů o zneužití cizí identity. Rozlišováno několik úrovní dle počtu.	Intrusion attempt *Login attempts*	4212	Alarmy: Neúspěšná přihlášení
Úspěšné přihlášení po hádání hesla	**CRIT**	Detekce úspěšných pokusů o uhádnutí hesla. Rozlišováno několik úrovní časové souslednosti.	Intrusion *Account compromise*	5211	Alarmy: Neúspěšná přihlášení
Přihlášení uživatele neaktivního	**WARN**	Detekce přihlášení k účtu po několika týdnech. Korelace zohledňuje v několika úrovních přihlašování k danému účtu v posledním roce.	Intrusion attempt *Login attempts*	4221	Alarmy: Neobvyklá přihlášení
Přihlášení uživatele nového	**NOTICE**	Detekce prvního přihlášení k účtu. Zohledňuje přihlašování k danému účtu v posledním roce.	Intrusion attempt *Login attempts*	4222	Alarmy: Neobvyklá přihlášení
Přihlášení uživatele k nepoužívanému systému	**WARN**	Detekce přihlášení k uživatele k danému systému po několika týdnech. Zohledňuje v několika úrovních přihlašování k účtu v posledním roce.	Intrusion attempt *Login attempts*	4223	Alarmy: Neobvyklá přihlášení
Přihlášení uživatele k novému systému	**NOTICE**	Detekce prvního přihlášení k systému. Zohledňuje přihlašování k danému účtu v posledním roce.	Intrusion attempt *Login attempts*	4224	Alarmy: Neobvyklá přihlášení
Přihlášení mimo běžnou dobu	**WARN**	Detekce přihlášení mimo běžnou pracovní dobu organizace pro detekci potenciálně kompromitovaných účtů. Korelace zohledňuje přihlašování k danému účtu v posledních 4 týdnech.	Intrusion attempt *Login attempts*	4225	Alarmy: Neobvyklá přihlášení
Pokus o přihlášení k zakázanému účtu	**WARN**	Přehled neúspěšných pokusů o přihlášení, které mohou být se zvýšenou pravděpodobností pokusem o neautorizovaný přístup. Podporováno pro:	Intrusion attempt *Login attempts*	4251	Alarmy: Neobvyklá přihlášení

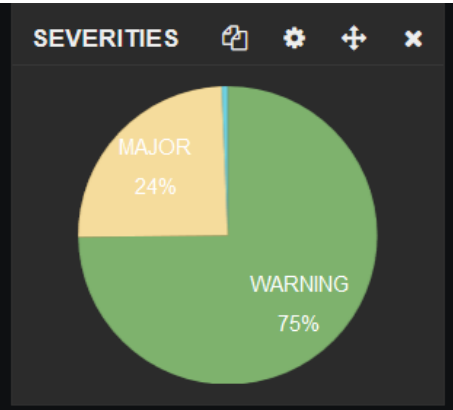
VIZUÁLNÍ EDITOR PRAVIDEL



SKÓRE RIZIKA

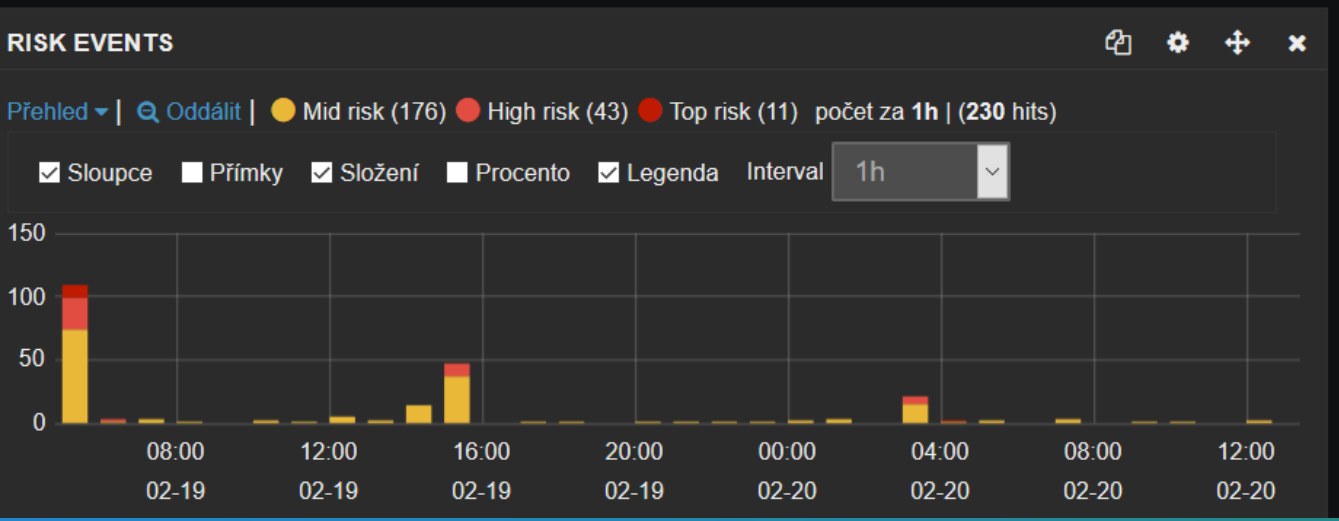
- **RISK_SCORE = ASSET_VALUE * SEVERITY * RELIABILITY**

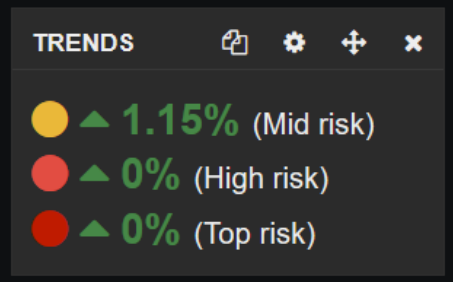




CORRELATED EVENTS - MAX RISK TOP 5

Term	maximum
Logon of new user	40
New target of user logon	40
Special privileges assigned to new logon	8





CORRELATED EVENTS - MAX COUNT TOP 5

Term	Počet
New target of user logon	6
Special privileges assigned to new logon	5
Logon of new user	4

SKÓRE RIZIKA

- **Indikátor hodnoty dotčeného aktiva a „teploměr” skóre rizika**
  - Barevné vlajky v každém záznamu

	AEFN.Severity	AEFN.Source	AEFN.Message	AEFN.Username
12:50:58	MAJOR	Xlog	subprocess '/usr/bin/curl' was terminated by a signal	NA
12:31:47	WARNING	Microsoft-Windows-Security-Auditing	Special privileges assigned to new logon.	SIEM-W2K12$
10:44:46	WARNING	Microsoft-Windows-Security-Auditing	Special privileges assigned to new logon.	SIEM-W2K12$
09:09:45	WARNING	Microsoft-Windows-Security-Auditing	Special privileges assigned to new logon.	SIEM-W2K12$
07:31:43	WARNING	Microsoft-Windows-Security-Auditing	Special privileges assigned to new logon.	SIEM-W2K12$
07:31:43	WARNING	Microsoft-Windows-GroupPolicy	This machine is configured to retrieve Group Policy files from a file share in an insecure way.	SYSTEM
07:31:43	WARNING	Microsoft-Windows-GroupPolicy	This machine is configured to retrieve Group Policy files from a file share in an insecure way.	SYSTEM
05:39:43	WARNING	Microsoft-Windows-Security-Auditing	Special privileges assigned to new logon.	SIEM-W2K12$
05:27:17	WARNING	Microsoft-Windows-Security-Auditing	Special privileges assigned to new logon.	SIEM-W2K12$
04:00:02	WARNING	WindowsHotfix	Last update 'KB4054566' was installed on '6.2.2019', 379 days ago	NA

DATA SYS

EKRAN a ELISA

Privilegované přístupy dodavatelů >>> video logy

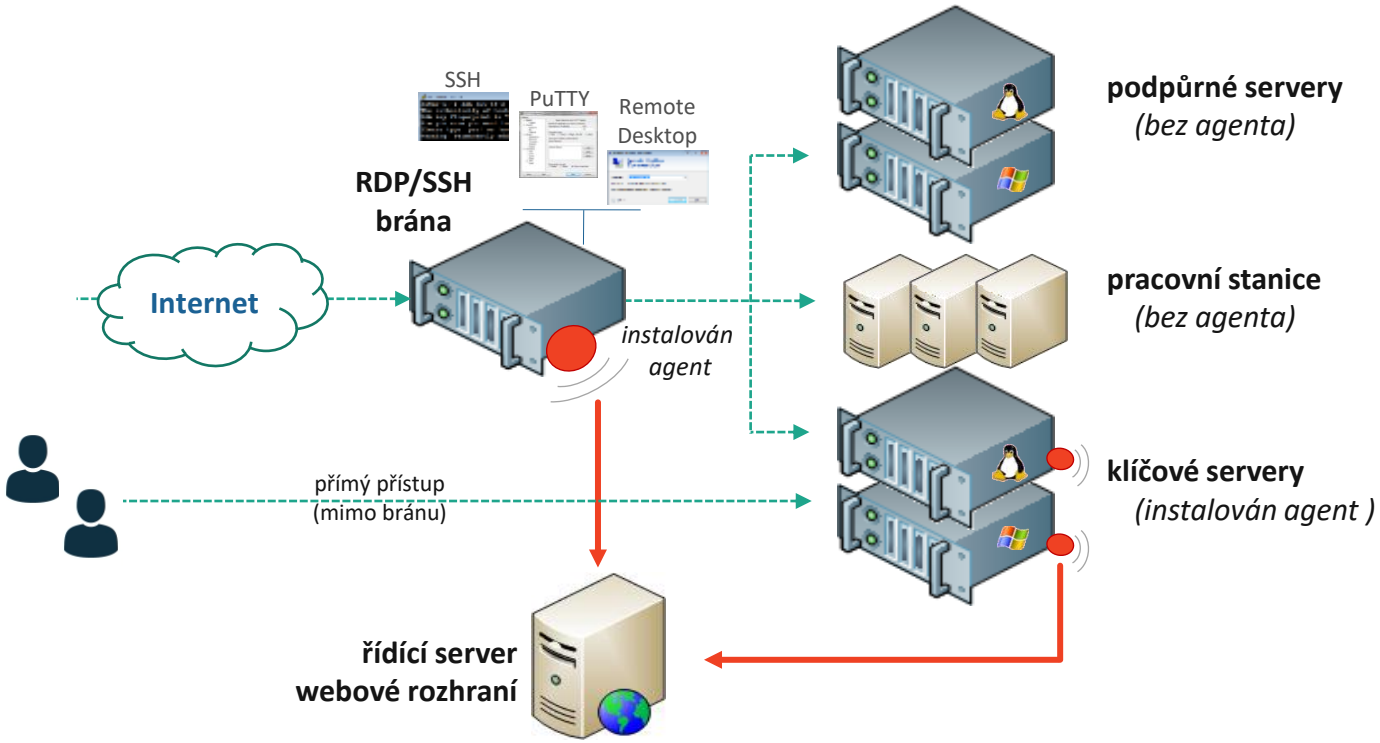
Vědět je fajn, ale co je lepšího, než vše VIDĚT?

Řízení přístupů privilegovanými účty

- **Video logy uživatelských relací**
- Indexované snímky obrazovek
- Podpora doplňkové autentizace
- Chráněný běh agenta

OBVYKLÝ PRINCIP NASAZENÍ

Nahrávání na „jump“ serveru a na klíčových serverech.



DALŠÍ BENEFITY

Jeden z mála bezpečnostních nástrojů se zřetelným ROI

- Optimalizace servisních smluv

- Přenos znalostí na juniorní správce
- Automaticky vznikající provozní deník
- Snazší budování zástupnosti v týmu

DATA SYS

MÁME ZVUČNÉ REFERENCE

REFERENCE

- **Ministerstvo spravedlnosti** (2018/05 – dosud)
  - Log management pro 1000+ monitorovaných serverů a zařízení
  - Zaznamenávání událostí i z významných informačních systémů dle ZKB
  - Průběžná analýza kybernetických bezpečnostních událostí s reportingem měsíčně

- **Komerční pojišťovna KB** (2016/11 – dosud)
  - Plošné pokrytí, korelační pravidla pro 19 „top“ scénářů z analýzy rizik
  - Provedena integrace auditních logů z databází a webových aplikačních serverů
  - Analýza událostí a incidentů naším specialistou 2x týdně s reportingem měsíčně

- **Lagardere Travel Retail** (2016/02 – dosud)
  - Plošné pokrytí, centrála i 1000+ maloobchodních míst
  - Analýza naším specialistou 1x týdně s reportingem měsíčně

Statutární město Kladno

-10%

pořizovací náklady proti konkurenci

- 30+ monitorované servery
- 150+ monitorovaná zařízení

Událostí za sekundu

průměrně	nárazově	maximum
300	800	4000

„Log management systém je pro nás opravdu bohatým zdrojem informací."

Pavel Rous, IT manažer

soulad: ČSN ISO 27001

Specifika

- statistiky provozu webové proxy
- vyhodnocování řízení přístupu dle IEEE 802.1x
- plus ELISA Security Manager

Ministerstvo zahraničních věcí ČR

-70%

pořizovací náklady proti konkurenci

- 600+ monitorované servery
- 150+ monitorovaná zařízení

Událostí za sekundu

průměrně	nárazově	maximum
300	500	5000

„ELISA se nám osvědčila v kombinaci s netflow monitoringem, kdy v log managementu dohledáváme detaily bezpečnostních událostí."

Luboš Pilař, IT manažer

soulad: ČSN ISO 27001

Specifika

- integrace Lotus Domino infrastruktury a aplikací
- auditování databází MSSQL, MySQL
- integrace se ZABBIX provozním monitoringem

Artesa, spořitelní družstvo

260 000 Kč

pořizovací náklady

- 50+ monitorované servery
- 20+ monitorovaná zařízení

Událostí za sekundu

průměrně	nárazově	maximum
30	100	2000

„ELISA nám pomáhá naplnit bezpečnostní požadavky bankovního dohledu ČNB."

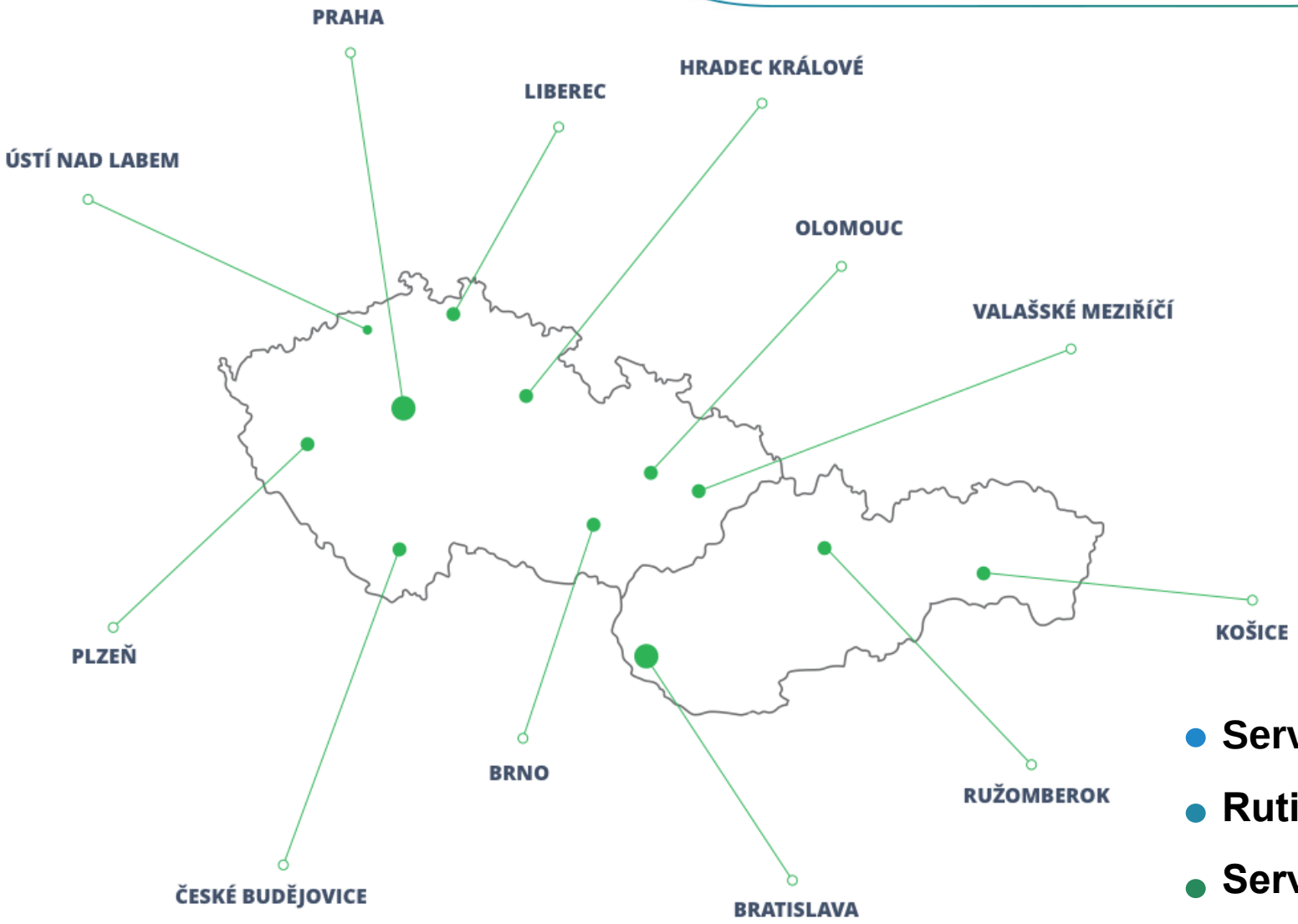
Miroslav Rudolf, , IT manažer

ČSN ISO 27001, PCI

Specifika

- auditování Oracle databáze
- méně obvyklý souborový server (NAS)
- integrace se ZABBIX provozním monitoringem

STŘEDISKA PODPORY



Náběh celkového ročního počtu servisních úkonů:

Do čtyř hodin i u Vás

- **ServiceDesk a HelpDesk v režimu 24 / 7**
- **Rutinní zásahy i specializovaná L3 podpora**
- **Servisní zásah do 4 hodin kdekoli v ČR i SR**

PRAGMATICKÝ PŘÍSTUP K BEZPEČNOSTI

Využití již pořízených prostředků „naplno“

Řízení přístupu, řízení konfigurací, ..

Invence

Nízkonákladová fungující řešení

Kombinace procesů a technologií

Nejkvalitnější technologie

Nástroje pro segmentování sítě

Nástroje pro detekci malwaru

Invence kombinovaná s kvalitou, důsledností a zkušenostmi

Nezbytné nápravné prostředky v nouzi - fázování

Rychlá opatření a testy

- Propojení IT s byznysem
- Skenování zlořádů v síti
- Praktické testy odolnosti

Malé stovky tisíc Kč

Malé desítky dnů

Rychlá ochrana (automatizovaná)

- NG ochrana endpointů
- NG segmentační firewall
- Webový či DB firewall

Už nákladnější

Malé desítky dnů

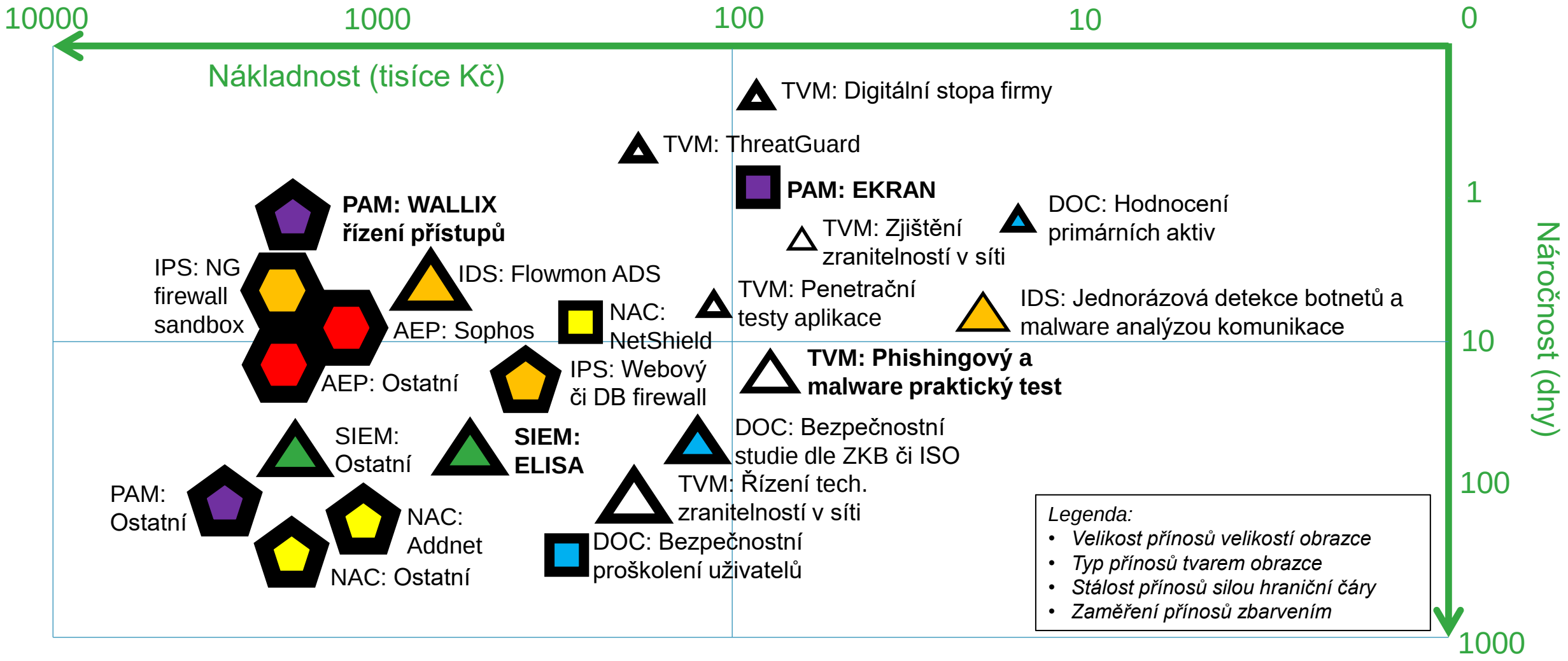
Průběžný dohled (udržovaný)

- Centrální bezp. dohled
- Řízení privileg. účtů
- Řízení přístupů do sítě

Už nákladnější

Několik měsíců

MAGICKÝ KVADRANT – NÁKLADNOST, NÁROČNOST, PŘÍNOSY



Integrovaný bezpečnostní a provozní dohled

DATA SYS

spolehlivě · nejvýhodněji