

D A T A
S Y S

SPOLEHLIVĚ · NEJVÝHODNĚJI

KONEČNĚ PŘÁTELSKÝ BEZPEČNOSTNÍ DOHLED ANEB POHÁDKA O ELISE A EKRAHOVI

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
PŘÍSTUPUJÍ
NA FIREMNÍ WEB?



KDO PROVEDL
ZMĚNU
V DATABÁZI?



KTEŘÍ UŽIVATELE
STAHUJÍ NEJVÍCE
DAT Z INTERNETU?



KDO SMAZAL
SOUBORY
NA SDÍLENÉM DISKU?



K JAKÝM CHYBÁM
DOCHÁZÍ
V PODNIKOVÉM IS?



KDO SE SNAŽÍ
UHÁDNOUT
PŘÍSTUPOVÉ HESLO?



§22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

**Zaznamenávat určité činnosti
Ukládat logy pro vyhledávání
Zajistit jejich ochranu**

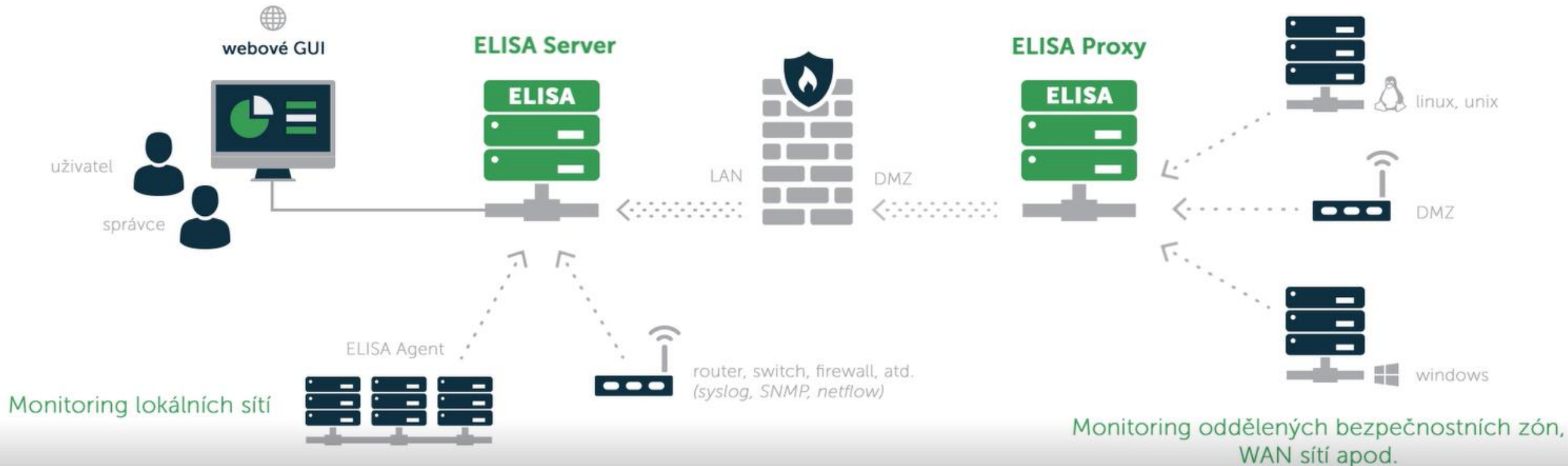
D A T A.....
S Y S

**PŘÁTELSKÝ
LOG MANAGEMENT**

ELISA LM/SIEM

ZÍSKÁTE CENTRÁLNÍ KONZOLI BEZPEČNOSTNÍHO DOHLEDU

Je to vcelku jednoduchá disciplína 😊



KLÍČOVÉ VLASTNOSTI



DETEKCE BEZPEČNOSTNÍCH RIZIK

- Soulad se ZKB, GDPR, ISO, PCI
- Rychlé odezvy
- Snadno nastavitelné filtry
- Horizontální škálovatelnost



NÍZKÉ NÁKLADY

- Integrace s OpenVAS a GSM
- Integrace s Flowmon ADS
- Fyzické i virtuální appliance
- Vysoký výkon (až 10 000 EPS)



PŘEHLEDNÉ UŽIVATELSKÉ PROSTŘEDÍ

ZDROJE LOGŮ

PODPORA PRAKTICKY VŠECH ZDROJŮ DAT ...



ZABUDOVANÝ ZABBIX

K TOMU JEŠTĚ NĚCO NAVÍC! PROVOZNÍ MONITORING!

Nejpopulárnější nástroj! Nadupaný a svobodný!



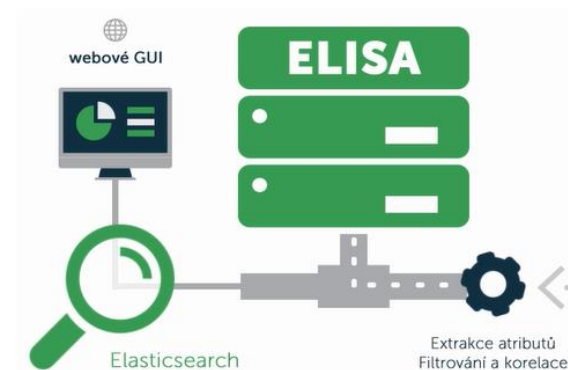
D A T A.....
S Y S

**OD LOG MANAGEMENTU
K NÁSTROJI TYPU SIEM**

OD LOG MANAGEMENTU K NÁSTROJI TYPU SIEM

- Automatizované vyhodnocování
- Korelace – nalézání vzájemných vztahů
- Zabudovaný „Change Auditor”
- Propracovanější alarmy a notifikace
- Centrální správa agentů
- Distribuovaný sběr logů

- Výpočet míry rizika
- Zjišťování zranitelností
- Normalizace logů a systematizace dat
- Agregace logů



ELISA SECURITY MANAGER

Robustní nástroj pro sběr a analýzu bezpečnostních událostí

Získáváte chytřejší konzoli bezpečnostního dohledu

Využijte na maximum i naše bezpečnostní specialisty!



KORELOVANÉ UDÁLOSTI - VZOR

Typ události	Závažnost	Obvyklý účel vyhodnocování a upřesnění	Třída a typ incidentu	ESM Id	<u>Dashboardy</u> Filtry (v GUI)
Privilegované přihlášení	NOTICE	Přehled úspěšných přihlášení privilegovanými účty s rozlišením servisních a dávkových úloh. Pro přihlášení do Windows detekováno z přiřazení privilegii, pro ostatní zdroje dle seznamu účtů.	Other <i>Authentication</i>	0111	Alarmy: Privilegovaná přihlášení
Hádání hesla	WARN	Detekce pokusů o zneužití cizí identity. Rozlišováno několik úrovní dle počtu opakování.	Intrusion attempt <i>Login attempts</i>	4211	Alarmy: Neúspěšná přihlášení
Hádání hesla hrubou silou	MAJOR	Detekce automatizovaných pokusů o zneužití cizí identity. Rozlišováno několik úrovní dle počtu.	Intrusion attempt <i>Login attempts</i>	4212	Alarmy: Neúspěšná přihlášení
Úspěšné přihlášení po hádání hesla	CRIT	Detekce úspěšných pokusů o uhádnutí hesla. Rozlišováno několik úrovní časové souslednosti.	Intrusion <i>Account compromise</i>	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 <i>Login attempts</i>	4221	Alarmy: Neobvyklá přihlášení
Přihlášení uživatele nového	NOTICE	Detekce prvního přihlášení k účtu. Zohledňuje přihlašování k danému účtu v posledním roce.	Intrusion attempt <i>Login attempts</i>	4222	Alarmy: Neobvyklá přihlášení
Přihlášení uživatele k nepoužívanému systému	WARN	Detekce přihlášení k uživateli k danému systému po několika týdnech. Zohledňuje v několika úrovních přihlašování k účtu v posledním roce.	Intrusion attempt <i>Login attempts</i>	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 <i>Login attempts</i>	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 <i>Login attempts</i>	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 <i>Login attempts</i>	4251	Alarmy: Neobvyklá přihlášení

VIZUÁLNÍ EDITOR PRAVIDEL

ELISA XLOG UPDATE: NO CONFIG CHANGE

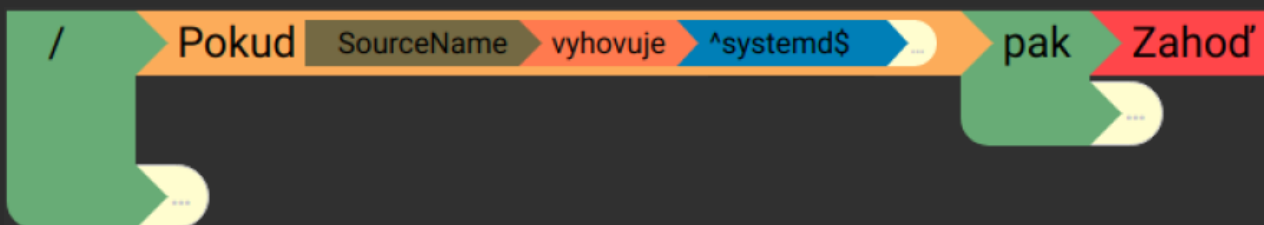
@timestamp: 2019-06-26T23:59:22.240100+02:00
AEFN.Category.1: Event
AEFN.Category.2: Generic
AEFN.Category.3: Other
.....

Pravidla

Priorita pravidla

Jméno pravidla

500



GENEROVANÝ KÓD

```
Exec \  
if ($) {  
}
```

TEST

SMAZAT

ULOŽIT

ZRUŠIT

POKUD

ZAHOD

PŘÍRAĎ

ODEBRAT

ZÁVAŽNOST

TAG

ALARM

E-MAIL

PŘEPOSLAT

ÚLOŽIŠTĚ DAT

DNS

GEOIP

MAC

ČÍSELNÍK

URL

KORELACE

VYTVOŘIT
KONTEXT

SMAZAT
KONTEXT

ZÍSKAT
KONTEXT

OVĚŘIT
KONTEXT

ZVÝŠIT POČET

ZÍSKAT POČET

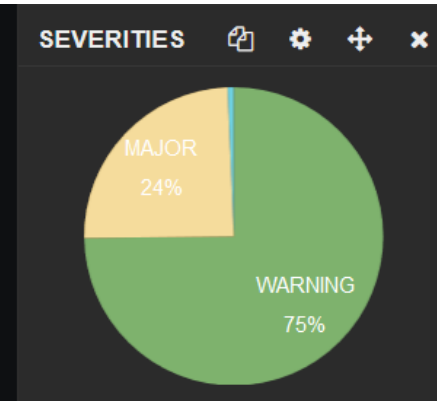
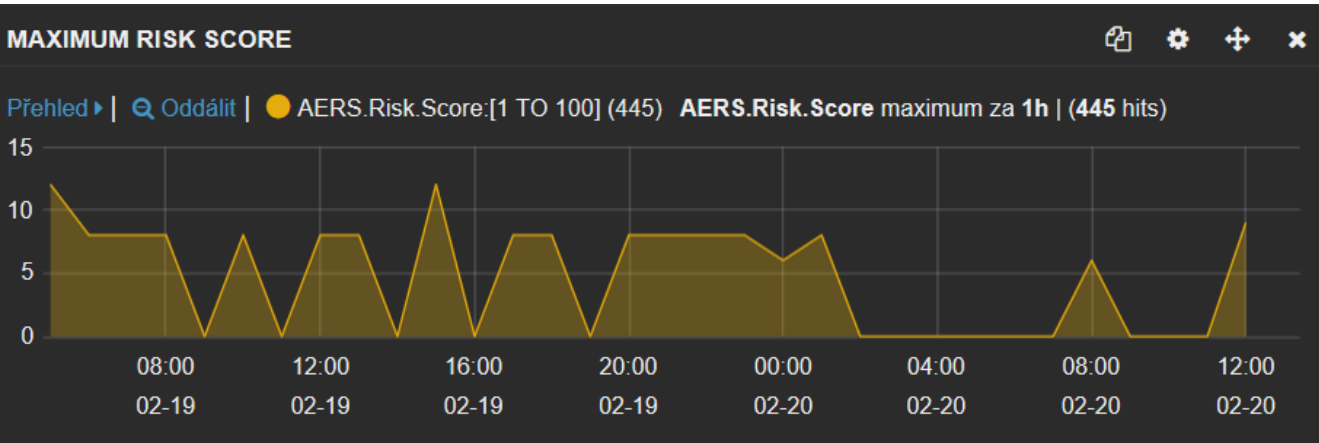
ZVÝŠIT
UNIKÁTNÍ
POČET

ZÍSKAT
UNIKÁTNÍ
POČET

VYTVOŘIT
UDÁLOST

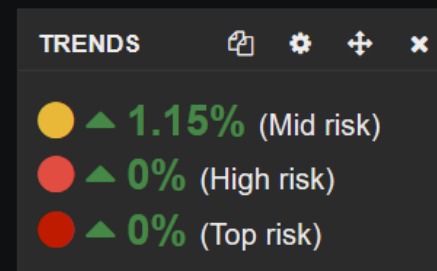
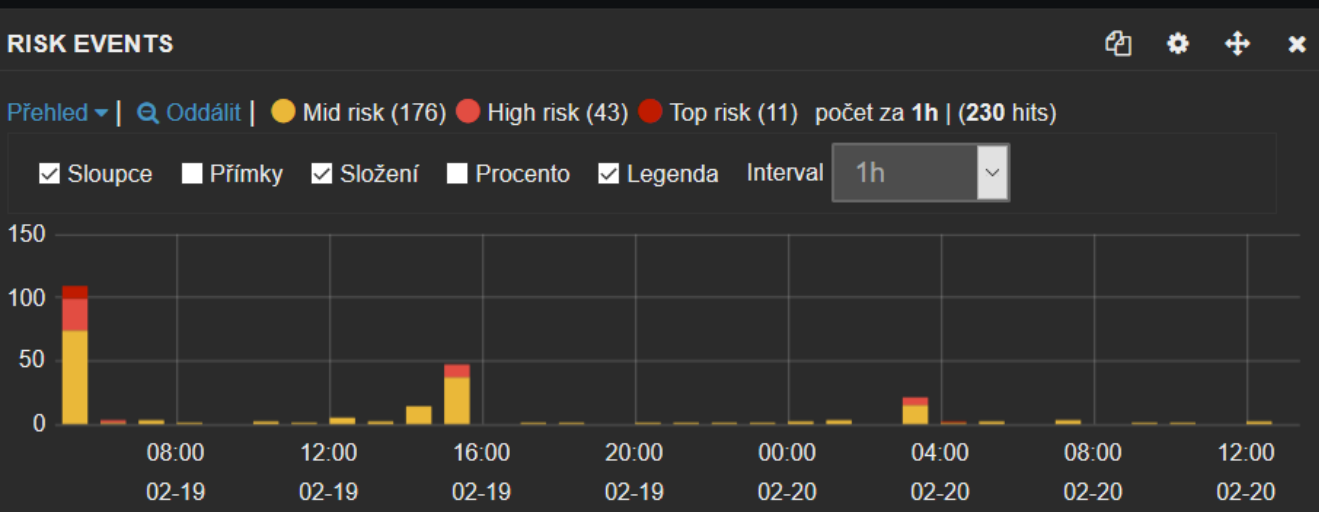
SKÓRE RIZIKA

$$\text{RISK_SCORE} = \text{ASSET_VALUE} * \text{SEVERITY} * \text{RELIABILITY}$$



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

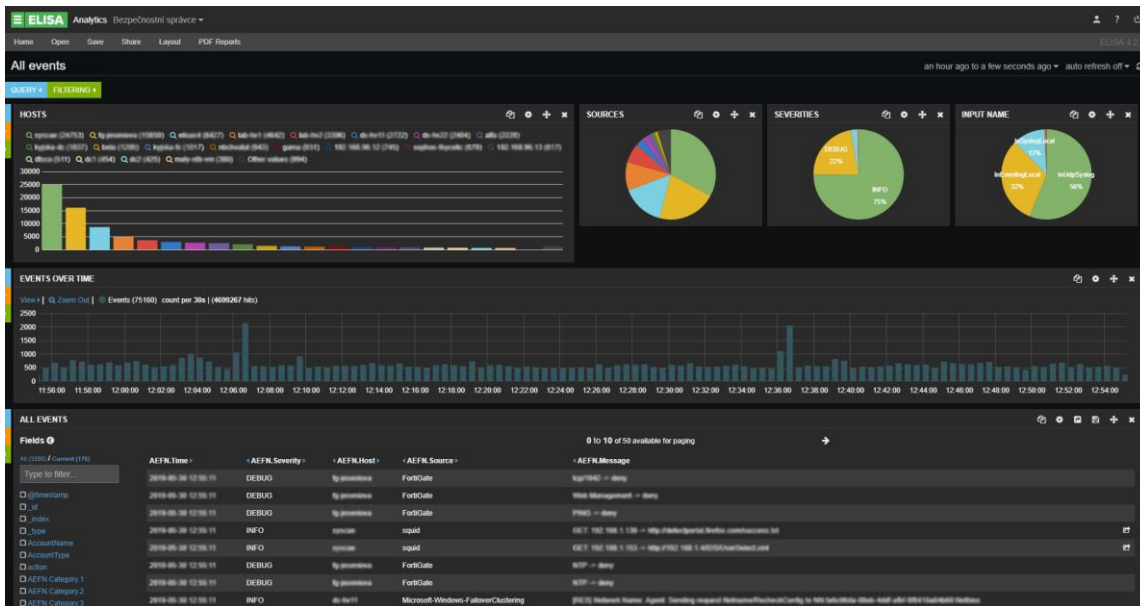
SKÓRE RIZIKA

- **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	

Odhalte a odstraňte problémy v aplikacích nebo infrastruktuře dříve, než negativně ovlivní chod vaší organizace.

Čas jsou peníze aneb kolik stojí váš čas?



PROČ POTŘEBUJETE ELISA SECURITY MANAGER

- Viditelnost a analýza problému
- Koordinace řešení a proaktivita
- Průběžný bezpečnostní dohled
- Efektivní řešení IT incidentů
- Soulad se zákony a regulacemi

D A T A
S Y S

EKRAN & ELISA

Privilegované přístupy dodavatelů

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

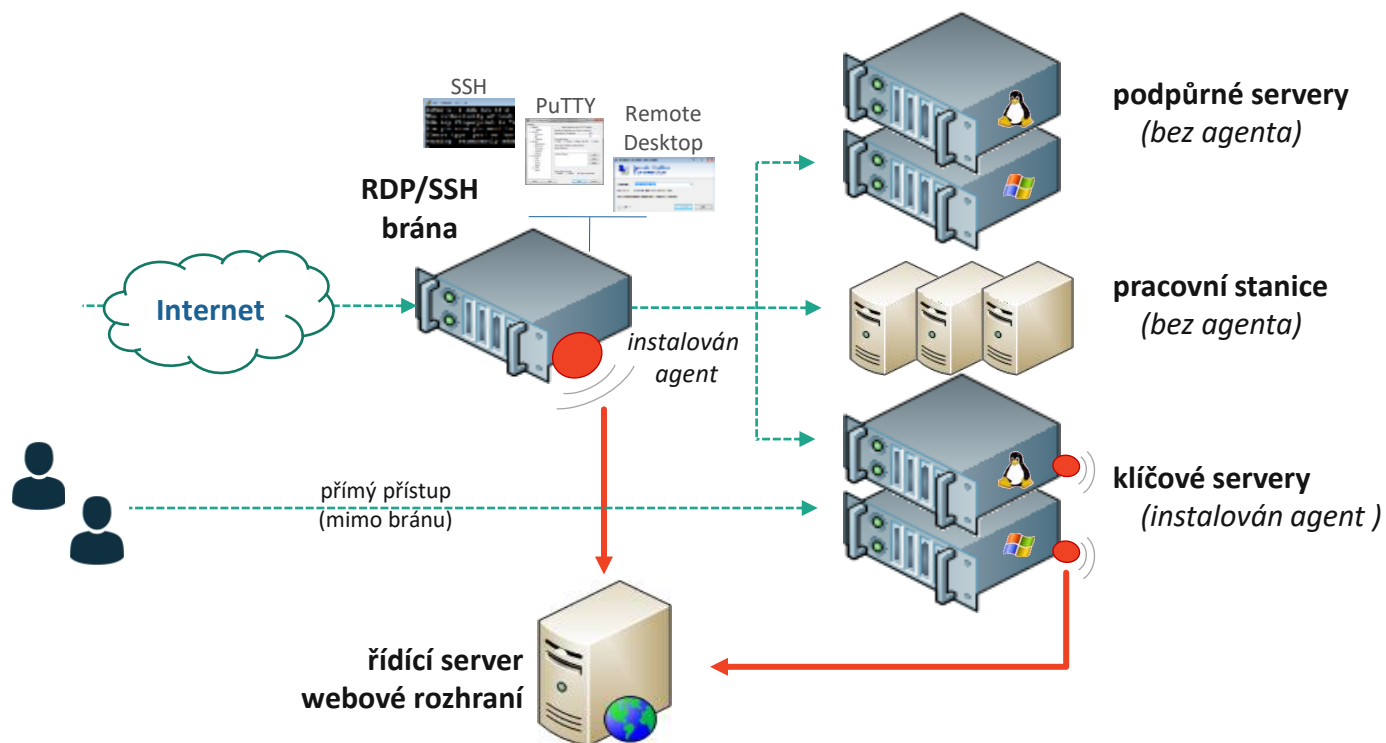
Řízení přístupů privilegovanými účty

- **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

QUICK WIN



D A T A.....
S Y S

**MÁME
ZVUČNÉ
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

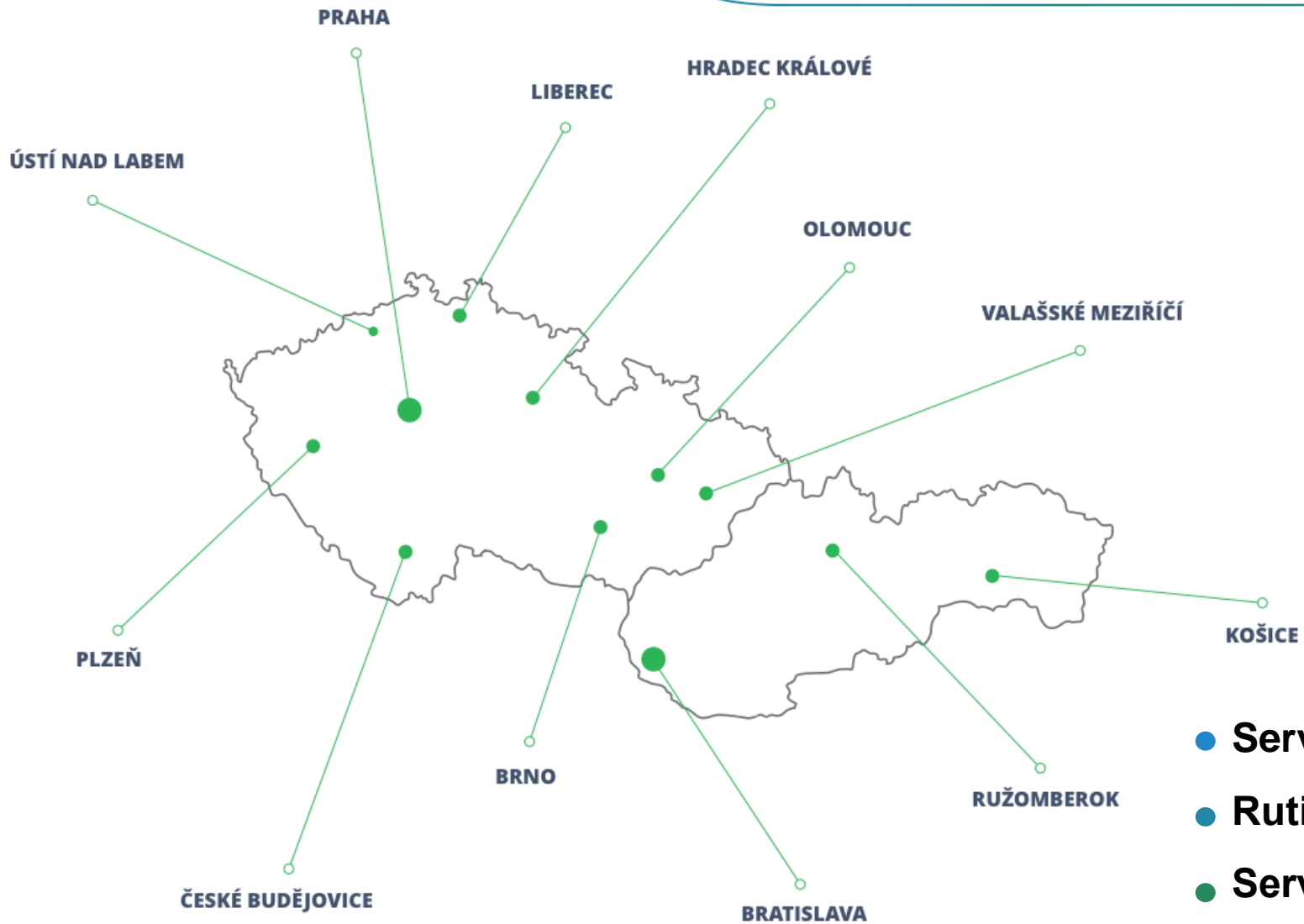


ČSN ISO 27001, PCI

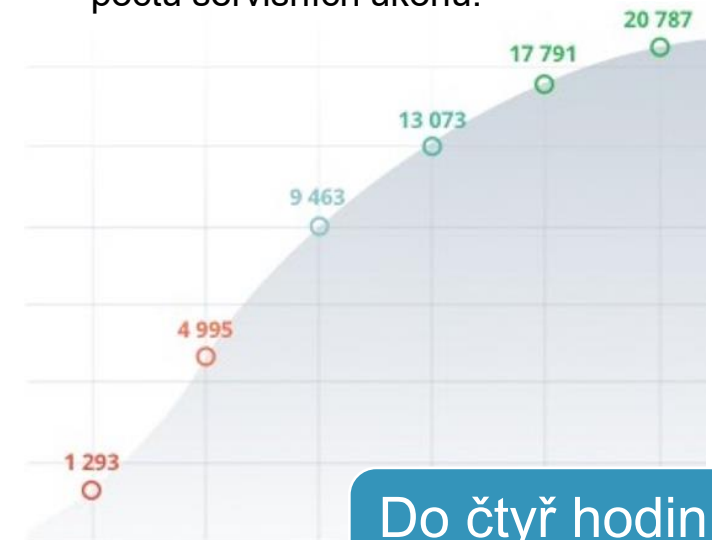
Specifika

- 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

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



Integrovaný bezpečnostní a provozní dohled

D A T A
S Y S

spolehlivě · nejvýhodněji