# Zákonné požadavky na sběr logů v organizacích státní správy

DATA SYS

spolehlivě · nejvýhodněji

# AGENDA

PARAGRAFY ZÁKONA

AUTOMATIZACE A KORELACE

BEZP. DOHLED JAKO SLUŽBA

LOG MANAGEMENT

PŘÍPADOVÁ STUDIE

# Požadavky zákona o kybernetické bezpečnosti: §

## §22 - Zaznamenávání událostí informačn
## systému, jeho uživatelů a admini

Povinná osoba

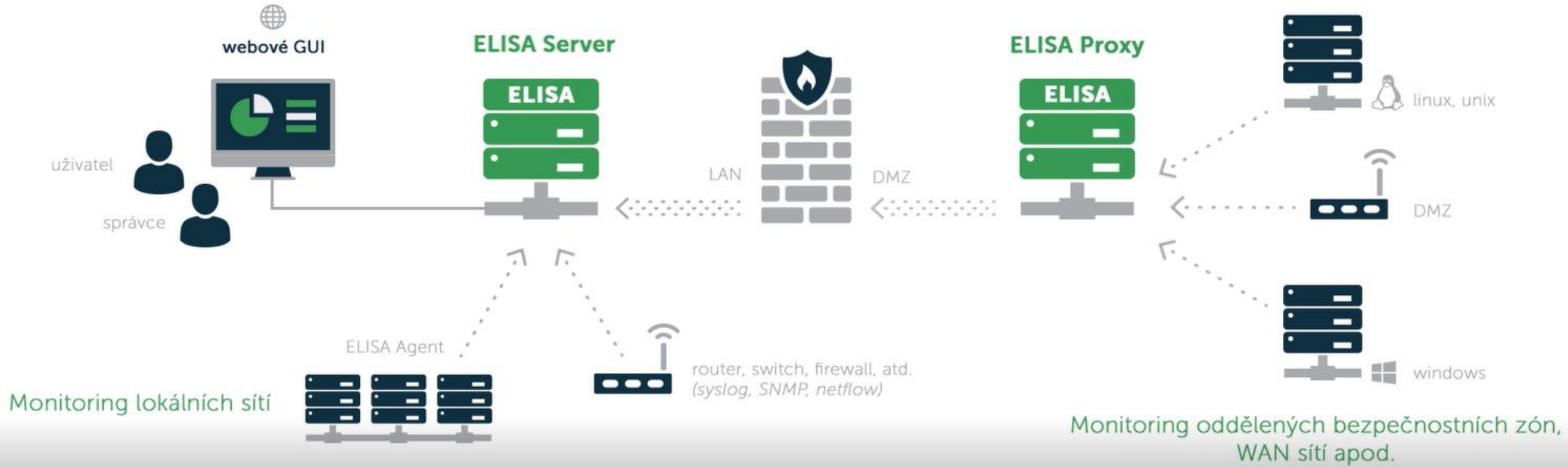
- ✓ **zaznam** **důležitých aktiv**
- ✓ **původce** a sběr informací
- **aktiva a účtu a (ne)úspěšnost činnosti**
- ✓ ormací **před neoprávněným čtením a změnou**
- ✓ **ní konkrétních typů činností**

Zaznamenávat určité činnosti
Ukládat logy pro vyhledávání
Zajistit jejich ochranu

# Odpověď – LM/SIEM

*Log management … je vcelku jednoduchá disciplína ☺*

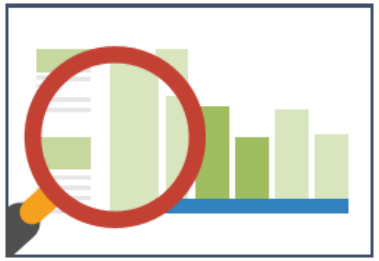
- **Získáte centrální konzoli bezpečnostního dohledu**



# PŘIROVNÁNÍ

**Internet** obsahuje množství užitečných informací.

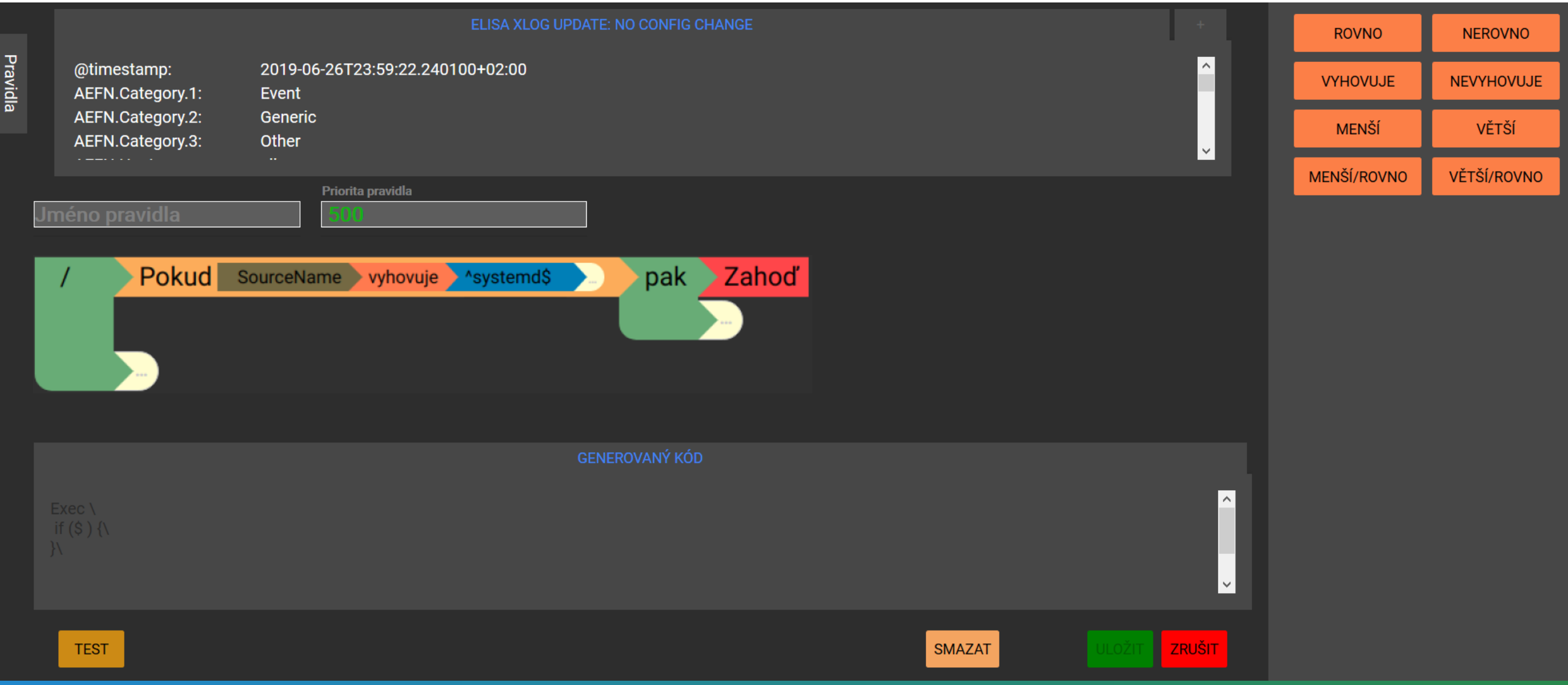
- Internetové vyhledávače je sbírají a indexují.
  - ✓ Využíváte je pro rychlé nalezení odpovědí !!!



**Informační systémy** generují množství užitečných informací.

- Log management nástroje je sbírají a indexují.
  - ✓ Využíváte je pro rychlé nalezení odpovědí **???**

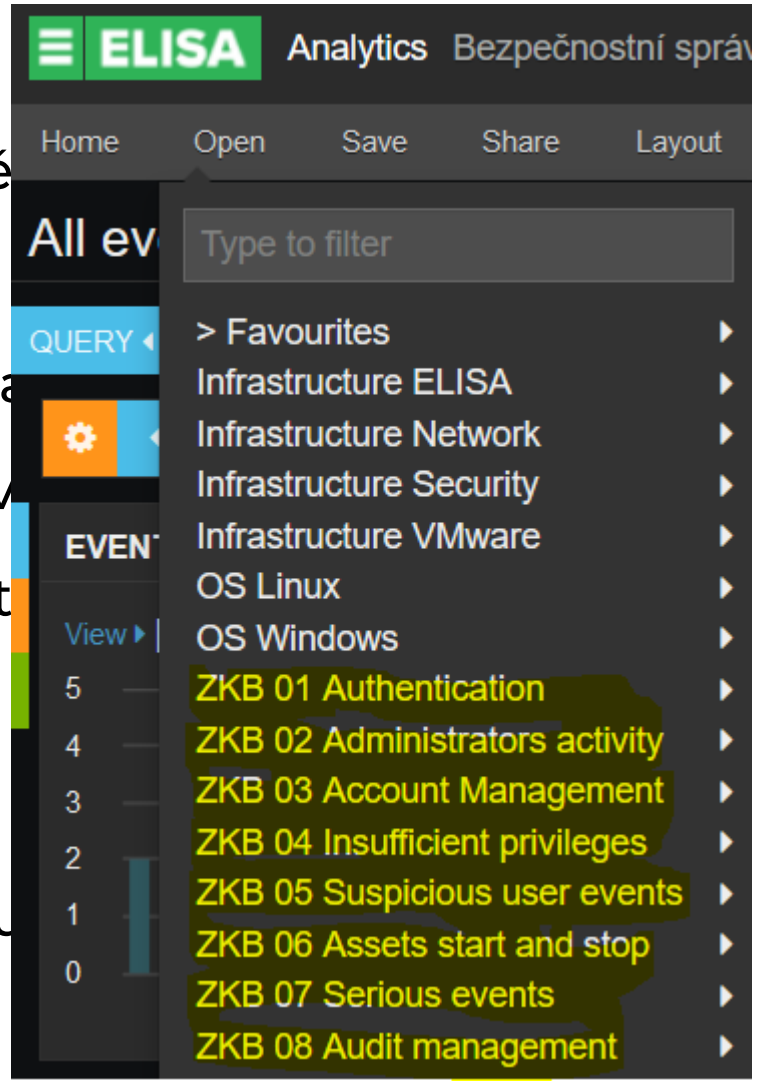
# VIZUÁLNÍ EDITOR PRAVIDEL



# Požadavky zákona o kybernetické bezpečnosti: §22

## §22 – Zaznamenávání konkrétních typů činností

1. přihlašování a odhlašování ke všem účtům, a to včetně
2. činností provedených administrátory,
3. úspěšné i neúspěšné manipulace s účty, oprávněními a
4. neprovedení činností v důsledku nedostatku přístupov
5. činností uživatelů, které mohou mít vliv na bezpečnost
6. zahájení a ukončení činností technických aktiv,
7. kritických i chybových hlášení technických aktiv a
8. přístupů k záznamům o událostech a pokusy o manipu



# Požadavky zákona o kybernetické bezpečnosti - §23

## §23 - Detekce kybernetických bezpečnostních událo

Povinná osoba zajistí detekci KBÚ přiměřeně s ohledem … v rámci

- ✓ koncových stanic,
- ✓ mobilních zařízení,
- ✓ serverů,
- ✓ datových úlož… datových nosičů,
- ✓ síťov… ků
- … aktiv

Integrovat množství technologií

# ZDROJE LOGŮ

Nejen tyto zdroje!

**Podpora prakticky všech zdrojů dat ...**

| Id | Název zdroje logů | Stručný popis vyhodnocovaných událostí |
|---|---|---|
| 291 | VMware ESXi | Události z lokálního syslogu se zaměřením na události o autentizaci uživatelů přistupujících na SSH, VIClient rozhraní. |
| 295 | VMware vCenter eventlog | Sběr událostí z vCenter eventlogu, Alarmy, změny stavu komponent VMware (host, cluster), detailní události podchycující změny konfigurací VM. |
| 311 | Oracle databáze | Sběr auditních záznamů o přístupu k DB serveru |
| 321 | MySQL databáze | Sběr auc |
| 322 | MariaDB databáze | Sběr auc |
| 331 | DB2 databáze | Sběr auc |
| 411 | Apache HTTPd | Sběr uda<br>Všechny |
| 415 | Mod Security | Sběr auc |
| 421 | Apache Tomcat | Sběr uda |
| 431 | WebSphere | Sběr uda |
| 451 | Squid proxy | Evidenc |
| 511 | Cisco ASA firewall | Evidenc |
| 515 | Cisco switch | Sběr uda |
| 521 | Fortinet FortiGate firewall | Evidenc<br>(webfilt |
| 522 | Fortinet FortiSwitch | Sběr uda |
| 531 | CheckPoint firewall | Evidenc<br>(webfilt |
| 541 | Juniper firewall | Evidenc |
| 551 | MicroTik | Sběr uda |
| 561 | UniFi | Sběr uda |
| 591 | Kerio firewall | Evidenc |
| 595 | pfSense firewall | Evidenc |
| 611 | ESET – Endpoint Security | Sběr uda |
| 621 | Symantec – Endpoint Security | Sběr uda |
| 625 | Symantec Management Server | Sběr uda |

| Id | Název zdroje logů | Stručný popis vyhodnocovaných událostí |
|---|---|---|
| 101 | Windows – systémový log | Všechny záznamy z eventlogu vyjma explicitně odfiltrovaných. Automatický parser všech atributů události obsažených v eventlogu. Zaznamenávání systémových událostí a chyb, evidence provedených změn konfigurace účtů a politik včetně lokálního firewallu. Deduplikace událostí o změnách přístupových práv k objektům. |
| 102 | Windows – doménový řadič | Evidence provedených změn konfigurace v Active Directory, události kategorie „Directory management“. |
| 103 | Windows – souborový server | Sběr auditních událostí o přístupech uživatelů k souborům, o změnách souborů, o vytváření a mazání souborů a složek. Detekce úniku dat excesivním kopírováním dokumentů, detekce podezřelého excesivního mazání nebo velkého počtu měněných souborů. |
| 104 | Windows – tiskový server | Evidence vytisknutých dokumentů pomocí Windows PrintServer |
| 105 | Windows – webový server | Sběr událostí o přístupu k webových stránkách, resp. všem zdrojům poskytovaným webovým serverem.<br>Všechny události z error logu IIS. |
| 106 | Windows – DHCP | Evidence událostí o přiřazení IP adrese stanicím. |
| 107 | Windows – DNS | Záznamy z DNS debug logu o úspěšném či neúspěšném překladu IP adres |
| 108 | Windows – RADIUS | Evidence úspěšných či odmítnutých žádostí o autentizaci. |
| 121 | Exchange server | Sběr událostí z logů Exchange Serveru umožňující sledovat Antispam funkcionalitu (agentlog), odchozí spojení, message tracking i detailní záznam komunikace na úrovni SMTP protokolu. |
| 151 | MSSQL server | Sběr auditních záznamů o přístupu k DB serveru |
| 211 | Linux server – systémový log | Všechny záznamy z lokálního systémového logu s důrazem na události týkající se autentizace uživatelů, evidence provedených změn konfigurace apod. |
| 212 | Linux server – auditní log | Sběr událostí z auditního modulu pro detailnější sledování prováděných operací nad OS. |
| 221 | AIX server – systémový log | Všechny záznamy z lokálního systémového logu s důrazem na události týkající se autentizace uživatelů, evidence provedených |

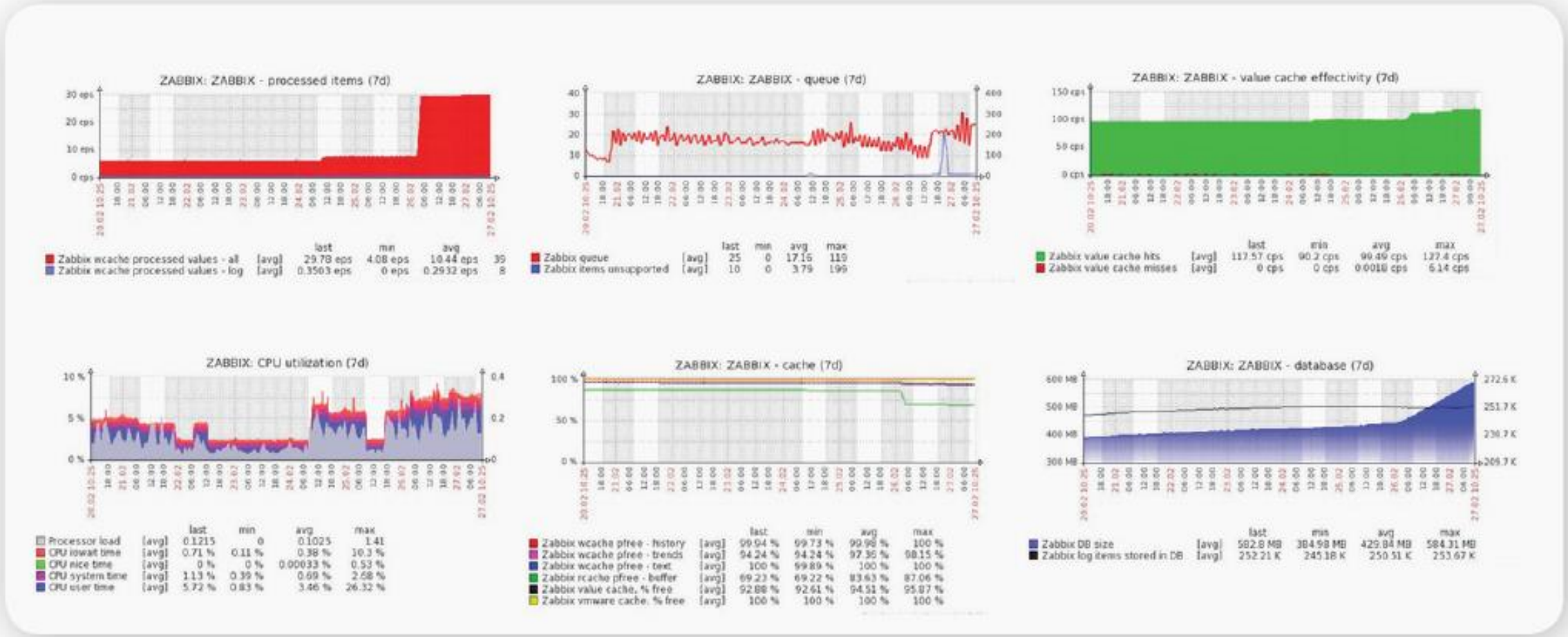
# ZABUDOVANÝ ZABBIX

K tomu ještě něco navíc!

**Provozní monitoring!**

Nejpopulárnější nástroj!

**Nadupaný a svobodný!**



# Požadavky zákona o kybernetické bezpečnosti: §24

## §24 - Nástroj pro sběr a vyhodnocování KBU

- ✓ vyhledávání a seskupování souvisejících zá
- ✓ poskytování informací o detekova ských bezp. událostech
- ✓ vyhodnocování KBU s cíl kybernetických bezpečnostních incidentů, včetn ování
- ✓ omeze avného vyhodnocení **pravidelnou aktualizací pravidel**

Optimalizovat vyhodnocování

DATA SYS

automatizace

# korelačními pravidly

# Od log managementu k nástroji typu SIEM

➢ Automatizované vyhodnocování bezpečnostních událostí

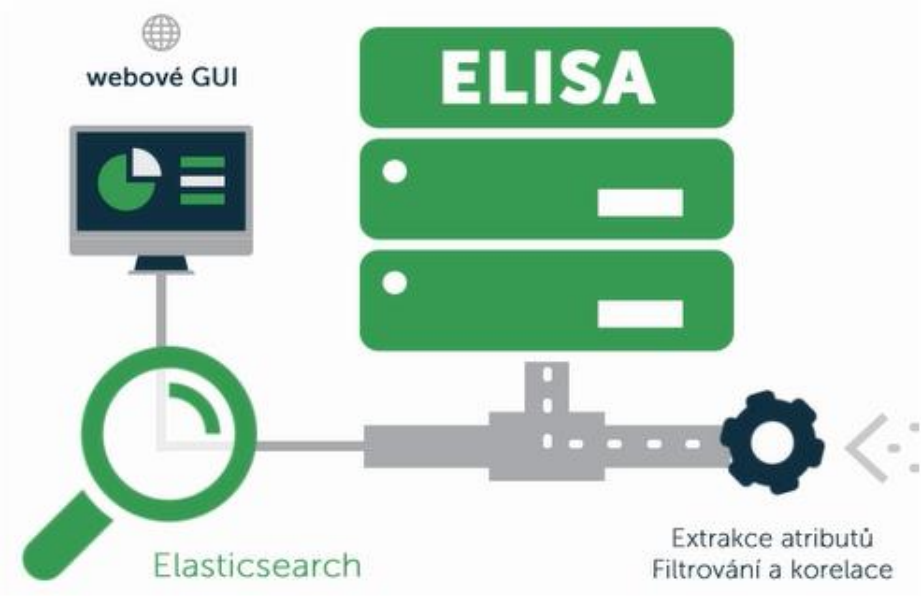
- Normalizace logů a systematizace dat
- Agregace logů – přehlednější prezentace
- Korelace – nalézání vzájemných vztahů
- Propracovanější alarmy a notifikace

## Robustní nástroj pro sběr a analýzu bezpečnostních událostí

Získáte chytřejší konzoli bezpečnostního dohledu

*Náš tip:* ***Získejte i našeho bezpečnostního specialistu!***

- Široká sada podporovaných zdrojů
- Integrace s FM pro detekci anomálií
- Zabudovaný „Change Auditor“ modul
- Škálovatelnost a nízké náklady



Rozšíření funkcionality ELISA Security Manager

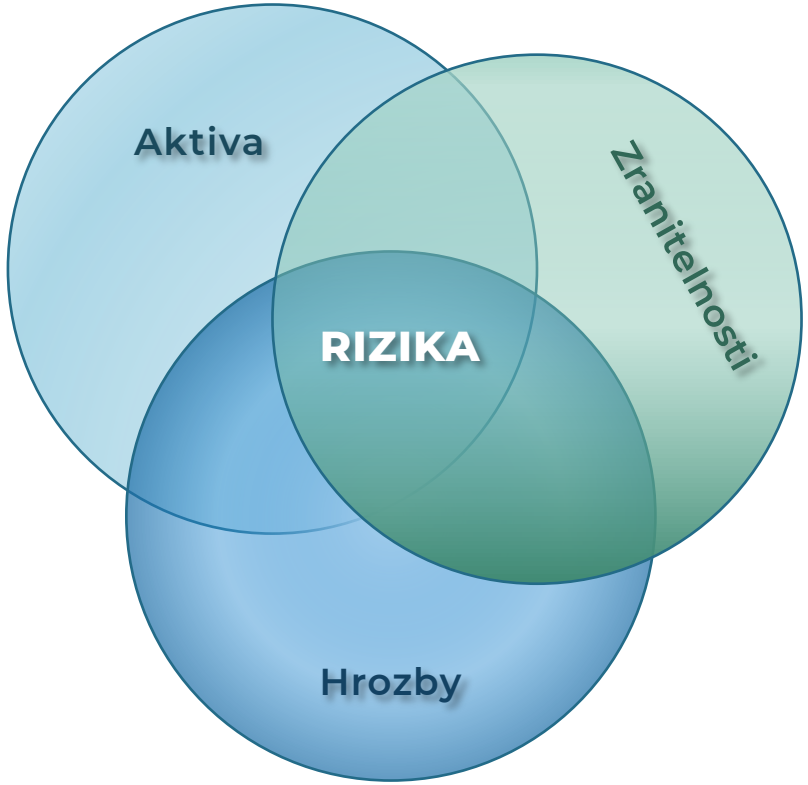
- **Detekce a protokolování změn v konfiguracích**

  - File Integrity Monitoring
  - Registry Integrity Monitoring
  - Protokolování rozdílů v různých exportech konfigurací
  - Protokolování změn provedených ve VMware vCenter

# VÝPOČET MÍRY RIZIKA, ZJIŠŤOVÁNÍ ZRANITELNOSTÍ

## Volitelné rozšíření o „vulnerability management“

- RISC_SCORE = ASSET_VALUE * SEVERITY * RELIABILITY




- Auto-registrace hostů
- Automatické spouštění skenů
- Alarmování zjištěných zranitelností
- Evidence v inventarizační databázi

# 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<br>*Authentication* | 0111 | Alarmy: Privilegovaná přihlášení |
| Hádání hesla | **WARN** | Detekce pokusů o zneužití cizí identity. Rozlišováno několik úrovní dle počtu opakování. | Intrusion attempt<br>*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<br>*Login attempts* | 4212 | Alarmy: Neúspěšná přihlášení |
| Úspěšné přihlášení po hádání hesla | **CRIT** | Detekce úspěšných pokusů o uhádnutí hesla. Rozlišováno několik úrovní časové souslednosti. | Intrusion<br>*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<br>*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<br>*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<br>*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<br>*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<br>*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<br>*Login attempts* | 4251 | Alarmy: Neobvyklá přihlášení |

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

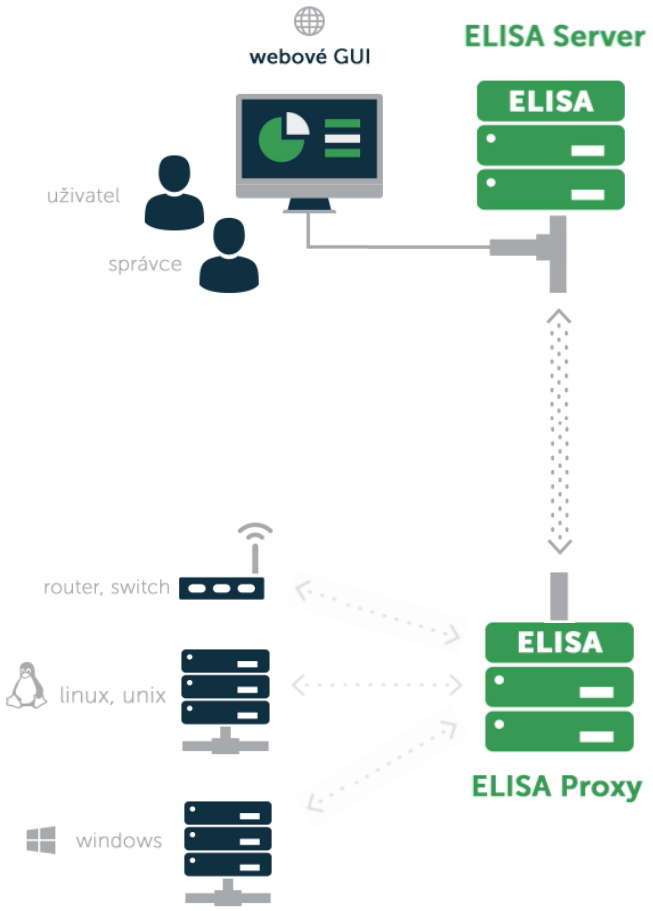
- auditování Oracle databáze
- méně obvyklý souborový server (NAS)
- integrace se ZABBIX provozním monitoringem

# Ministerstvo spravedlnosti

- ❑ Log management pro 1000+ monitorovaných serverů a zařízení
- ❑ Zaznamenávání událostí i z významných informačních systémů dle ZKB
- ❑ Průběžná analýza KBÚ s reportingem měsíčně

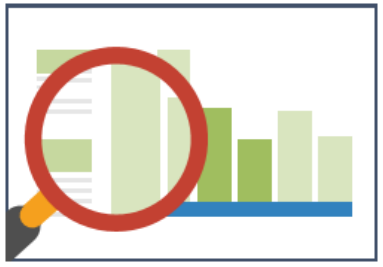
- ✓ Kompletní implementace během dvou měsíců
- ✓ 2000 událostí za sekundu, uchování po dobu 18-ti měsíců
- ✓ Hodnotné reporty - výsledek práce analytika DATASYSu

# LOGICKÁ ARCHITEKTURA – MS ČR




**Centrální server** (1x)

- Webové uživatelské rozhraní
- Úložiště konfigurací
- Úložiště dat



**Kolektor server** (9x)

- Komunikační brána pro:
  - agenty instalované na serverech
  - syslog a SNMP zařízení
  - VMware API

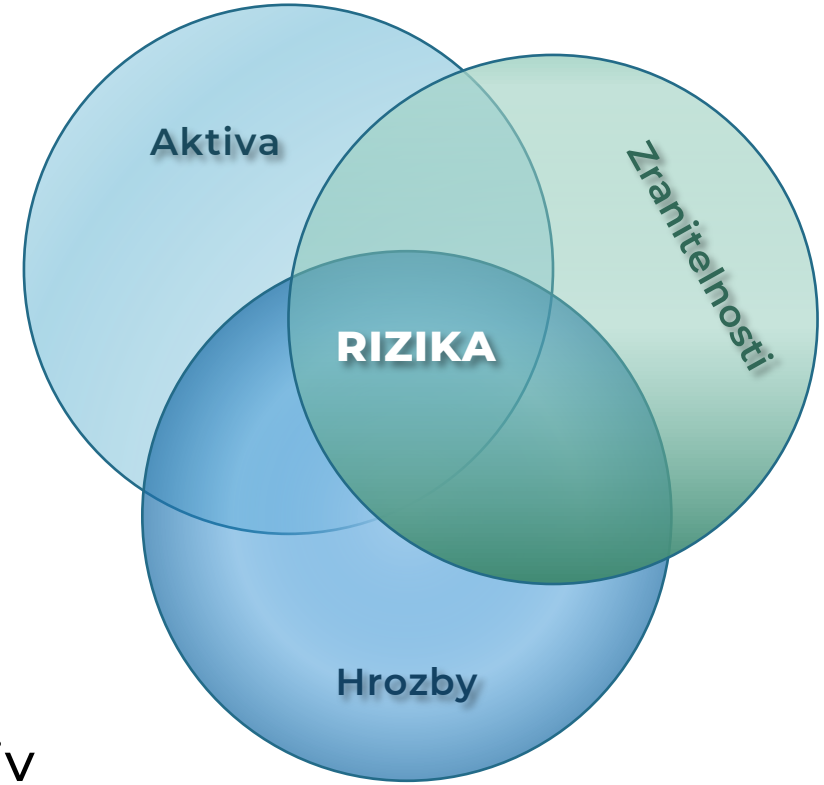
NXLog ENTERPRISE EDITION

DATA SYS

bezpečnostní
dohled
**jako služba**

# SOC = veškerá operativa kybernetické bezpečnosti

- **Řízení aktiv**
  - Evidence primárních i podpůrných aktiv
  - Vazba na proces identifikace a hodnocení aktiv
- **Řízení zranitelností**
  - Automatizovaná detekce nástrojem
  - Nad stejnou evidencí aktiv
- **Řízení hrozeb**
  - Automatizovaná detekce, nad stejnou evidencí aktiv
  - Centrální přehledová konzole, integrované analytické nástroje



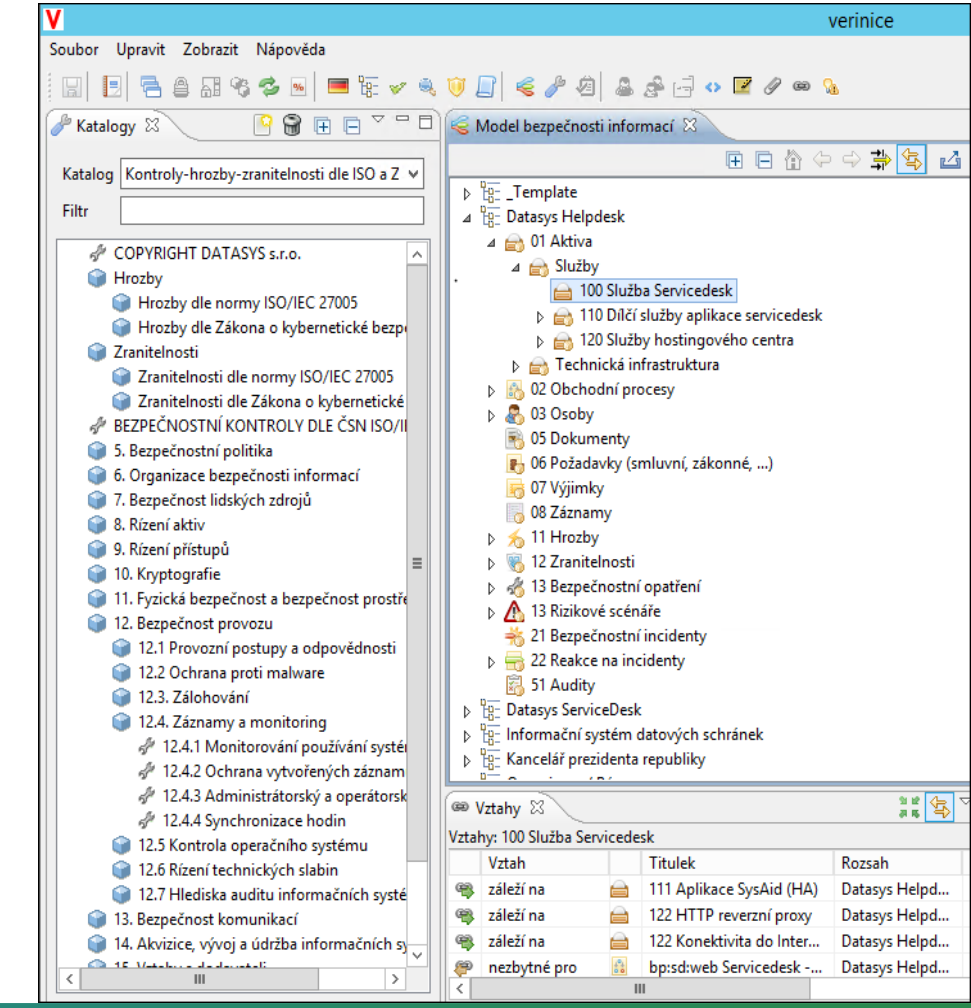
# CÍLE? KOMPLEXNÍ.

**Komplexní centralizace řízení kybernetických bezpečnostních událostí a incidentů**

- Systematizace zvládání KBÚ a KBI
- Konsolidace znalostí kyberbezpečnosti
- Snížení reakční doby a zmírnění dopadů
- Snížení nákladů na zvládání KBÚ a KBI

# Řízení aktiv - ve vazbě na řízení ISMS jako celku

- **Nástroj pro podporu systému řízení bezpečnosti informací**
- Pro české právní prostředí
- Snadné modelování scénářů rizika
- Garanty aktiv nominuje klient



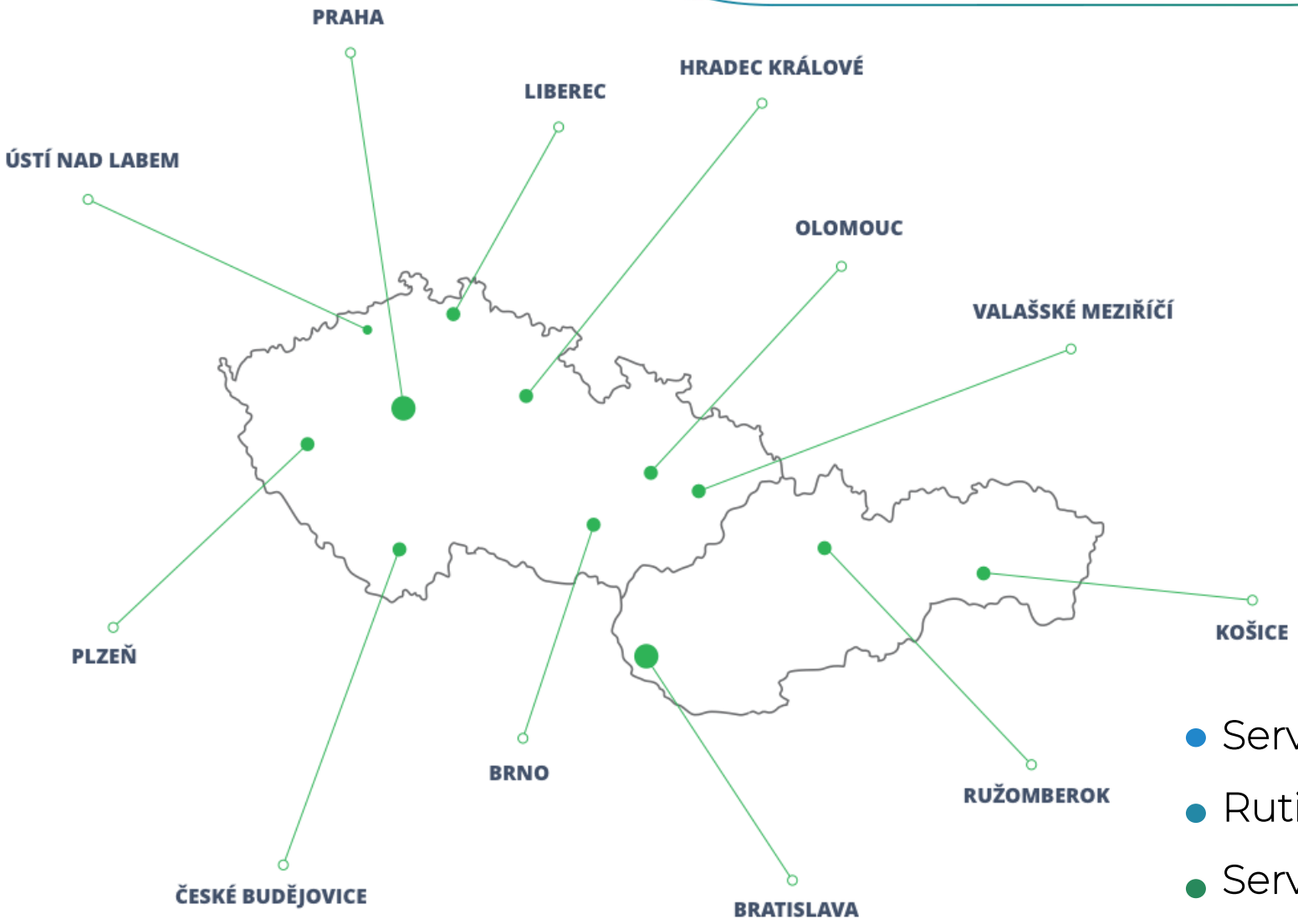
# Řízení zranitelností není nástroj, je to proces !


- ❑ Příprava
  - ✓ Definice cílů, harmonogramu apod.
- ❑ Identifikace, klasifikace a prioritizace
  - ✓ Získání přehledu o tom, co je důležité řešit
- ❑ Přiřazení a zvládnutí – **zajišťuje klient**
  - ✓ Realizace opatření kompetentními osobami
- ❑ Prověření a zlepšení
  - ✓ Kontrola, automatizace, rozšíření do dalších oblastí

# Máme silnou kompetenci, a to i produktově neutrální!

- Bezpečnostní dohled – SIEM nástroj
  - Invenční nízkonákladové nástroje
  - Průběžný bezpečnostní monitoring
  - Pravidelná datová analýza specialistou
- Auditování aktivit privilegovaných účtů

# 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

# Integrovaný bezpečnostní a provozní dohled

DATA SYS

spolehlivě · nejvýhodněji