JAK ROZUMĚT SVÉMU IT

Miroslav Knapovský CISSP, CEH, CCSK
Security Solution Architect

knapovsky@logmanager.cz

Co jsou logy, události, strojová data?

Velká data

Zákaznická data

- Click stream data
- Shopping cart data
- Online transaction data

Mimo datacentrum

- Manufacturing, Logistics
- CDRs & IPDRs
- Power consumption
- RFID Data
- GPS Data
- IoT

Windows

- Registry
- Event logs
- File system
- Sysinternals

Linux/Unix

- Configurations
- Syslog
- File system
- Ps,iostat,top

Virtualizace & Cloud

- Hypervisor
- Guest OS, Apps
- Cloud

Aplikace

- Web logs
- Log4J, JMS, JMX
- .Net Events
- Code and scripts

Databáze

- Configurations
- Audit
- Tables
- Schemas

Networking

- Configurations
- Syslog
- SNMP
- Netflow

Nějak se nám to tady množí

Current World Population

7,530,945,842

Světová populace		
Roků k další miliardě	Rok	Miliard obyvatel
-	1800	1
127	1927	2
33	1960	3
14	1974	4
13	1987	5
12	1999	6
12	2011	7
14	*2025**	8

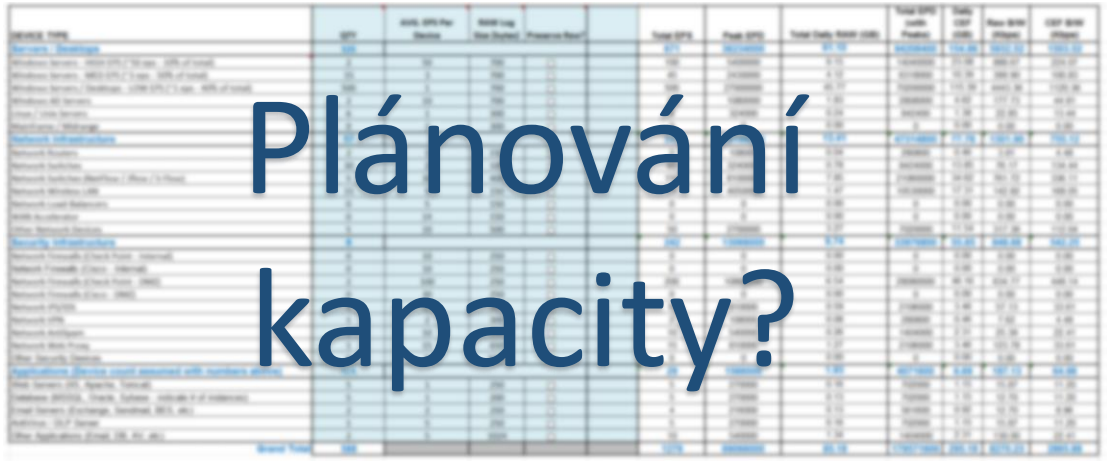
*optimistický výhled

Zdroj: wikipedia.org

Nějak se nám to tady množí

Konzervativní odhad logů ve firmě		
Zaměstnanců	EPS	Dní do Miliardy logů
250	200	125
500	500	50
1000	700	35
3000	1500	15

Czech TV



Plánování kapacity?

- 2910 zaměstnanců
- 1200 zdrojů / 3500+ EPS / 200-500 GB logů denně
- Miliarda logů za týden

Proč se pochopením logů zabývat ?

Praktické / provozní důvody

- ❑ Nejde centrálně vyhledávat
- ❑ Jazyk zdroje – nerozumíme?
- ❑ Rotace LOG souboru

Bezpečnostní důvody

- ❑ Nebezpečí modifikace logů
- ❑ Analýzy – statistické, bezpečnostní
- ❑ Přehled o anomáliích, incidentech

Zákonné důvody

- ❑ Zákon o kybernetické bezpečnosti - § 5
- ❑ General Data Protection Regulation od května 2018

Nasazení a provoz centrálního systému na správu a analýzu logů

LOGmanager a soulad s požadavky
Zákona o kybernetické bezpečnosti

LOGmanager a soulad s požadavky GDPR

Whitepaper ilustrující, jak nasazení platformy LOGmanager napomáhá zajistit dodržování

PDF na www.logmanager.cz

LOGmanager

Příklady použití

LOG management a Kritický IT Incident

Kritický IT Incident zažije občas většina organizací

Nastane, když je nefunkční business aplikace nebo infrastruktura.
Obvyklý čas vyřešení +-6 hodin.

Dva důležité pojmy – **MTTR a RCA** – pro CIO: *„čas jsou peníze“*

Snížit MTTR/RCA umožňuje IT Operations Intelligence

Základem IT OPS je vhodný nástroj na sběr logů

- Viditelnost
- Koordinace
- Produktivita při řešení incidentu

LOG management – další možné příklady

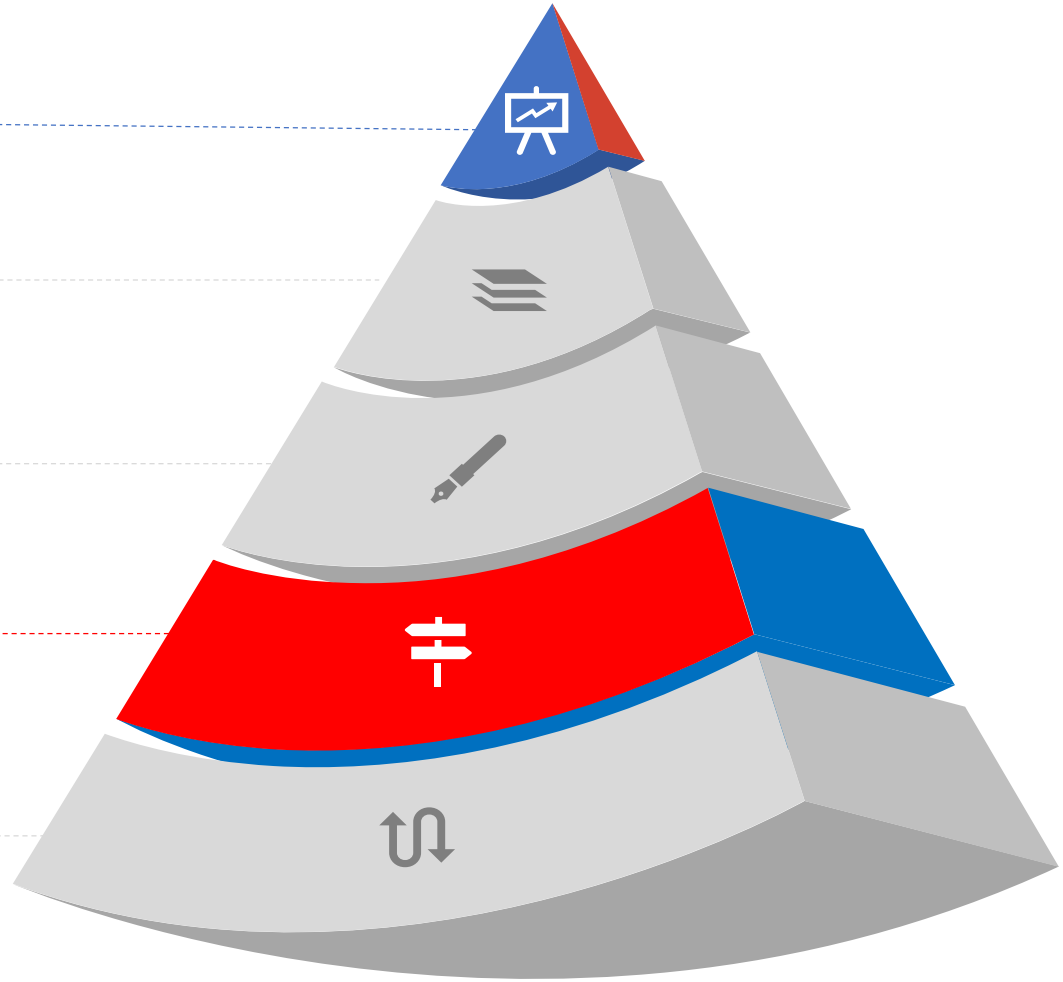
Drill-down v událostech

Sledování přístupu ke službám (adresářovým / db / souborovým)

Analýzy, reporty, dohled, monitoring, audit

IoT – Dohled, analýza událostí, statistiky, Alarm

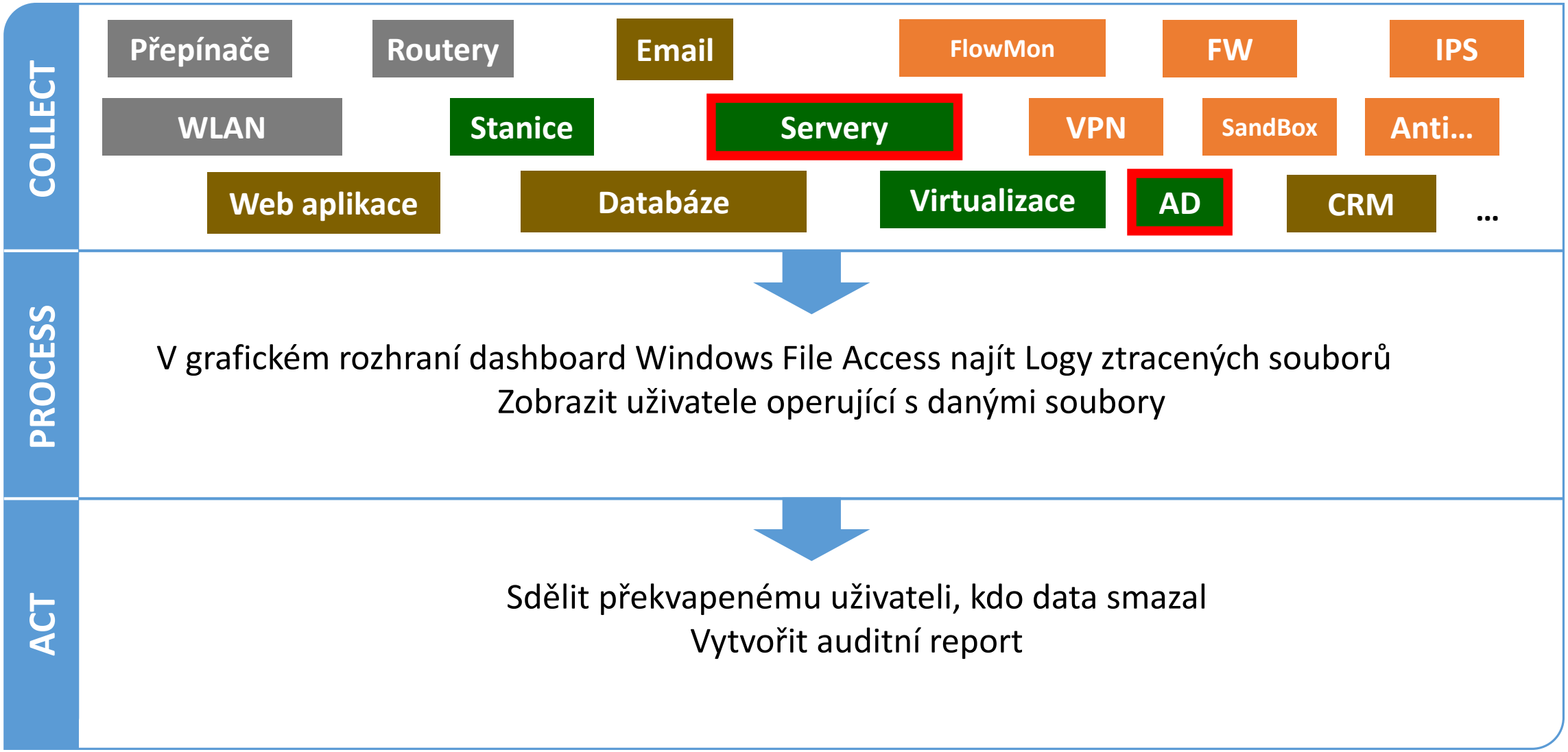
GDPR – Kdo, kdy a jakým způsobem přistupoval k systémům s osobními daty



LOGmanager

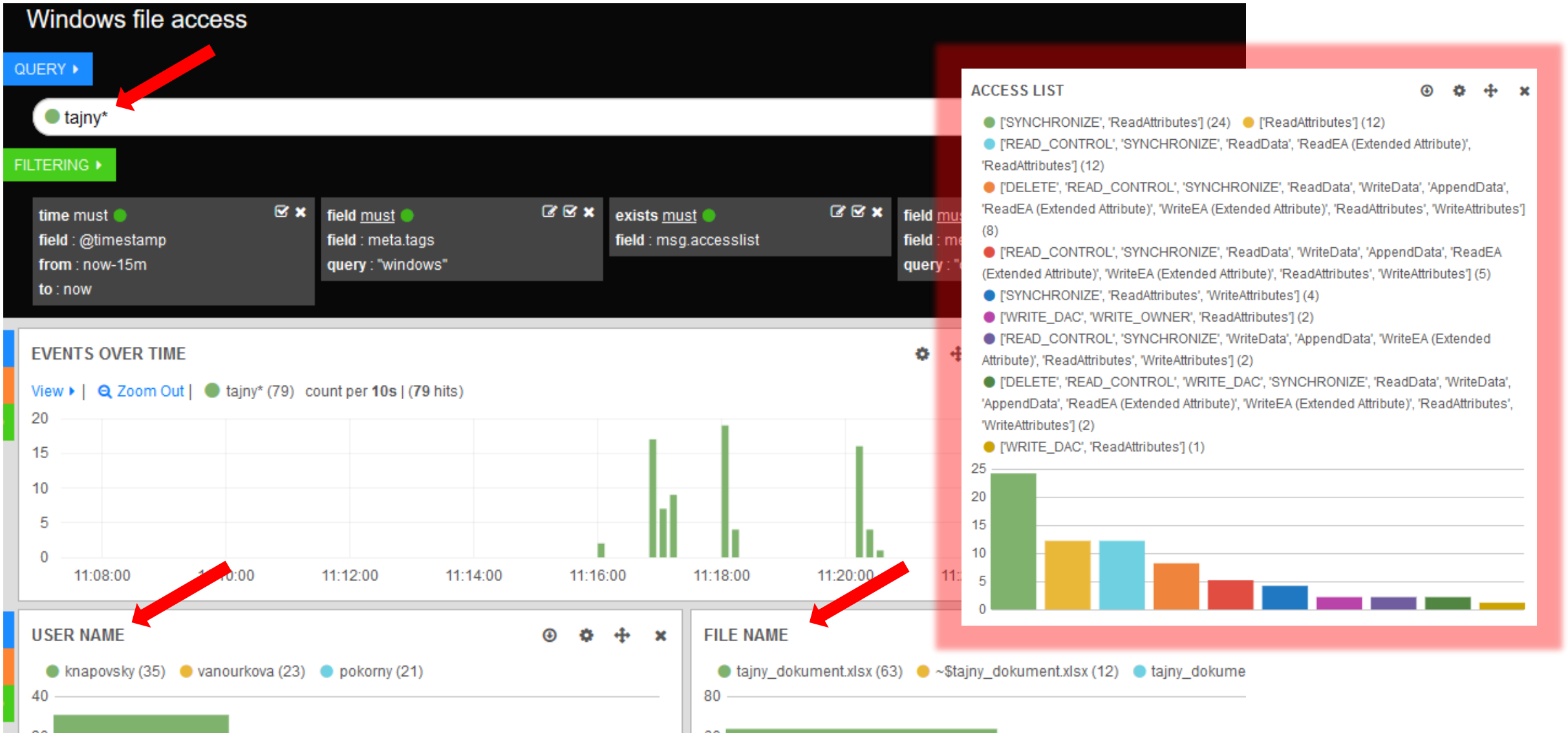
Kdo smazal data?

Síťová | Bezpečnostní | Systémy | Aplikace

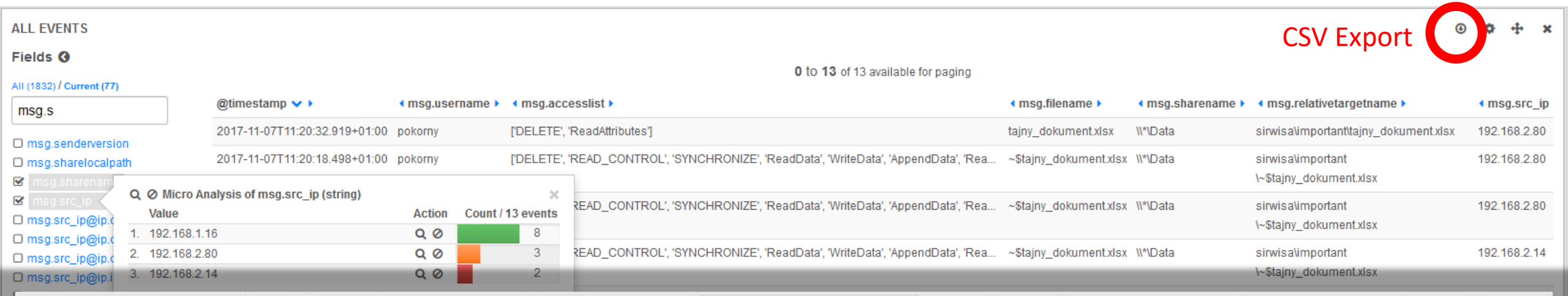


LOGmanager

Vyhledávání jako v Google



Generování auditu na vyžádání

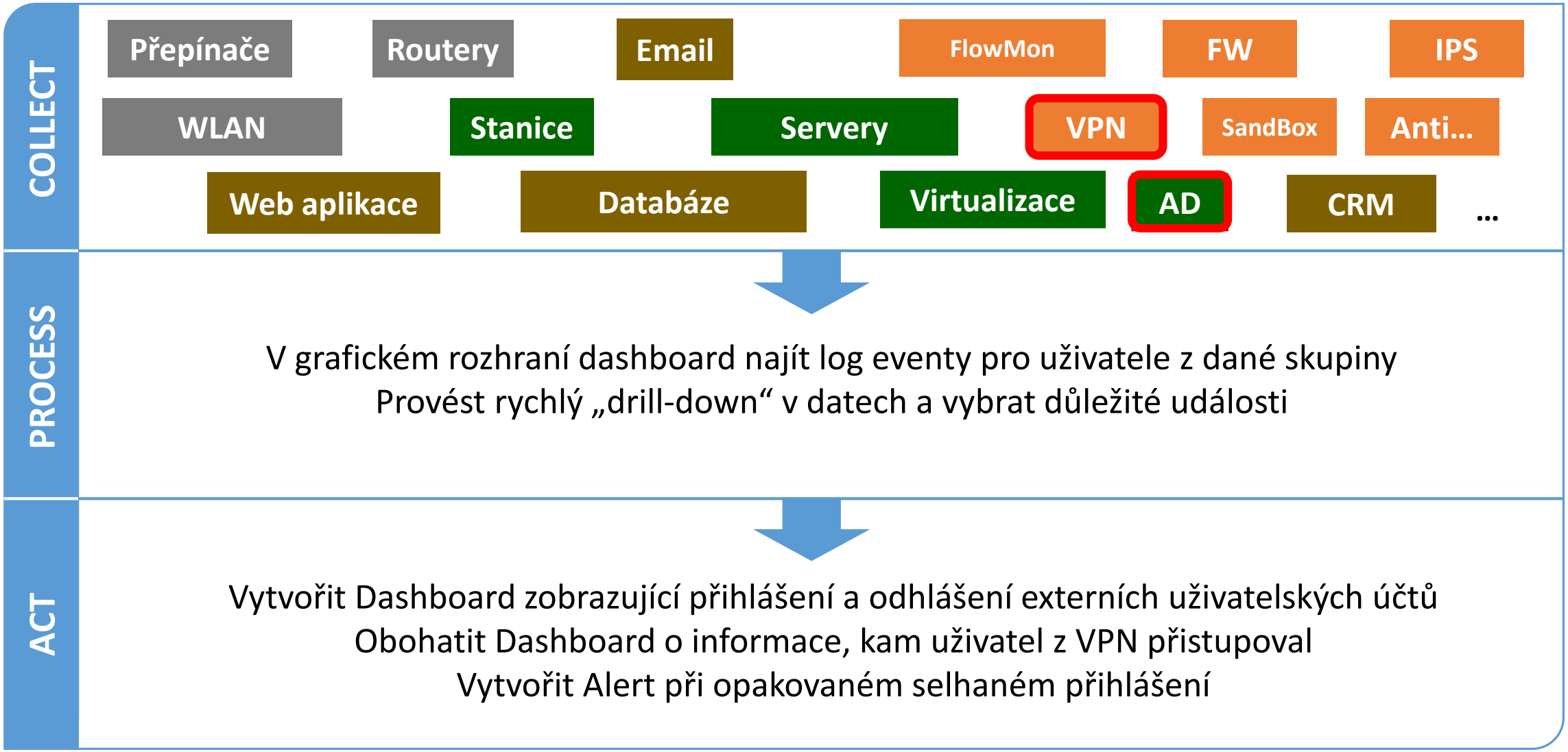


	A	B	C	D	E	F	G
1	@timestamp	msg.username	msg.accesslist	msg.filename	msg.sharename	msg.relativetargetname	msg.src_ip
2	2017-11-07T10:20:32	pokorny	['DELETE', 'ReadAttributes']	tajny_dokument.xlsx	*\Data	sirwisa\important\tajny_dokument.xlsx	192.168.2.80
3	2017-11-07T10:20:18	pokorny	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	~$tajny_dokument.xlsx	*\Data	sirwisa\important\~$tajny_dokument.xlsx	192.168.2.80
4	2017-11-07T10:20:18	pokorny	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	~$tajny_dokument.xlsx	*\Data	sirwisa\important\~$tajny_dokument.xlsx	192.168.2.80
5	2017-11-07T10:18:05	vanourkova	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	~$tajny_dokument.xlsx	*\Data	sirwisa\important\~$tajny_dokument.xlsx	192.168.2.14
6	2017-11-07T10:18:05	vanourkova	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	~$tajny_dokument.xlsx	*\Data	sirwisa\important\~$tajny_dokument.xlsx	192.168.2.14
7	2017-11-07T10:17:12	knapovsky	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	tajny_dokument.xlsx	*\Data	sirwisa\important\tajny_dokument.xlsx	192.168.1.16
8	2017-11-07T10:17:12	knapovsky	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	tajny_dokument.xlsx	*\Data	sirwisa\important\tajny_dokument.xlsx	192.168.1.16
9	2017-11-07T10:17:00	knapovsky	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	~$tajny_dokument.xlsx	*\Data	sirwisa\important\~$tajny_dokument.xlsx	192.168.1.16
10	2017-11-07T10:17:00	knapovsky	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	~$tajny_dokument.xlsx	*\Data	sirwisa\important\~$tajny_dokument.xlsx	192.168.1.16
11	2017-11-07T10:16:5	knapovsky	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	~$tajny_dokument.xlsx	*\Data	sirwisa\important\~$tajny_dokument.xlsx	192.168.1.16
12	2017-11-07T10:16:56	knapovsky	['DELETE', 'READ_CONTROL', 'SYNCHRONIZE',	~$tajny_dokument.xlsx	*\Data	sirwisa\important\~$tajny_dokument.xlsx	192.168.1.16
13	2017-11-07T10:16:02	knapovsky	['DELETE', 'READ_CONTROL', 'WRITE_DAC', 'S	tajny_dokument.xlsx	*\Data	sirwisa\important\tajny_dokument.xlsx	192.168.1.16
14	2017-11-07T10:16:02	knapovsky	['DELETE', 'READ_CONTROL', 'WRITE_DAC', 'S	tajny_dokument.xlsx	*\Data	sirwisa\important\tajny_dokument.xlsx	192.168.1.16

LOGmanager

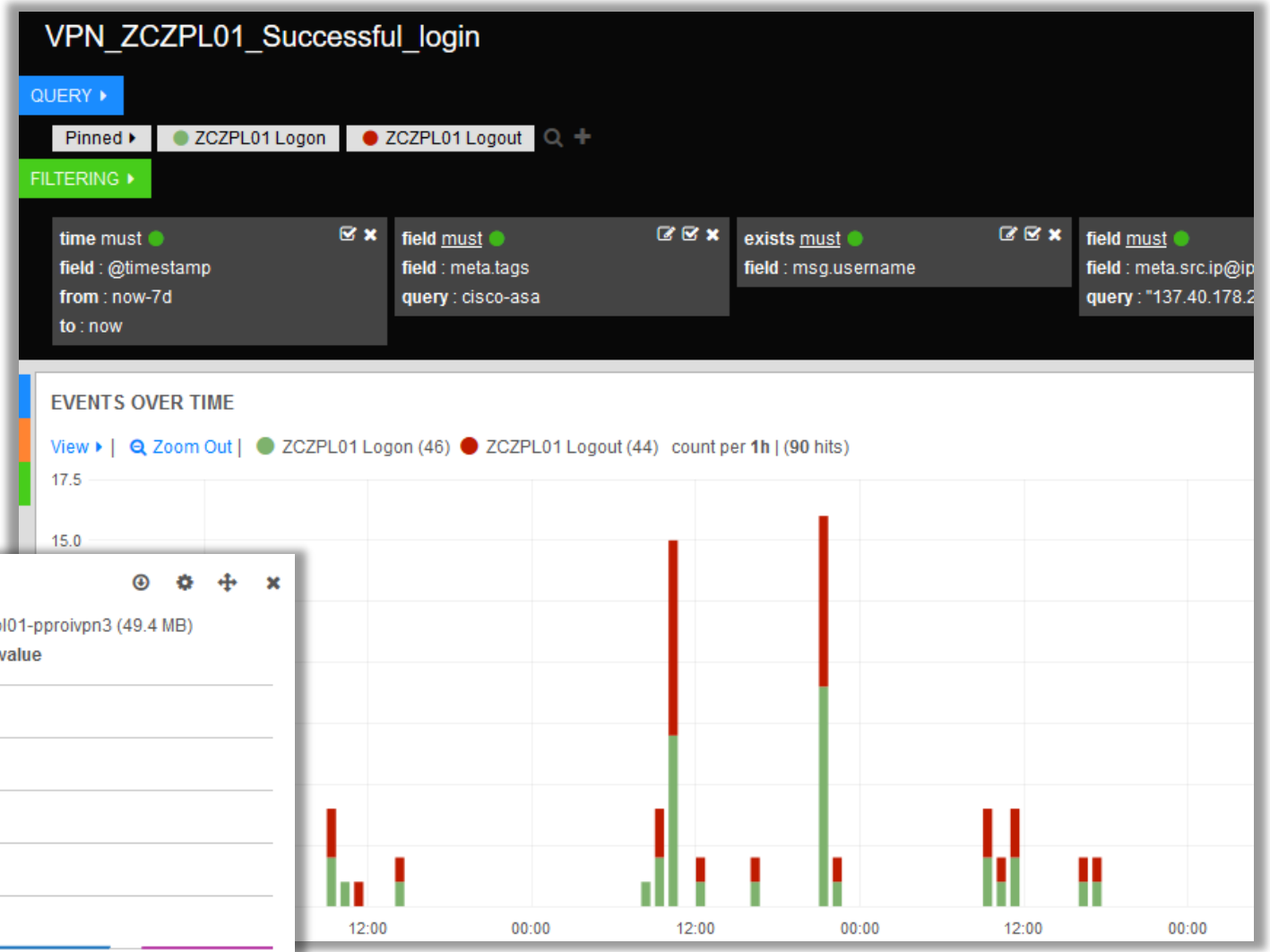
Audit ext. uživatelů VPN

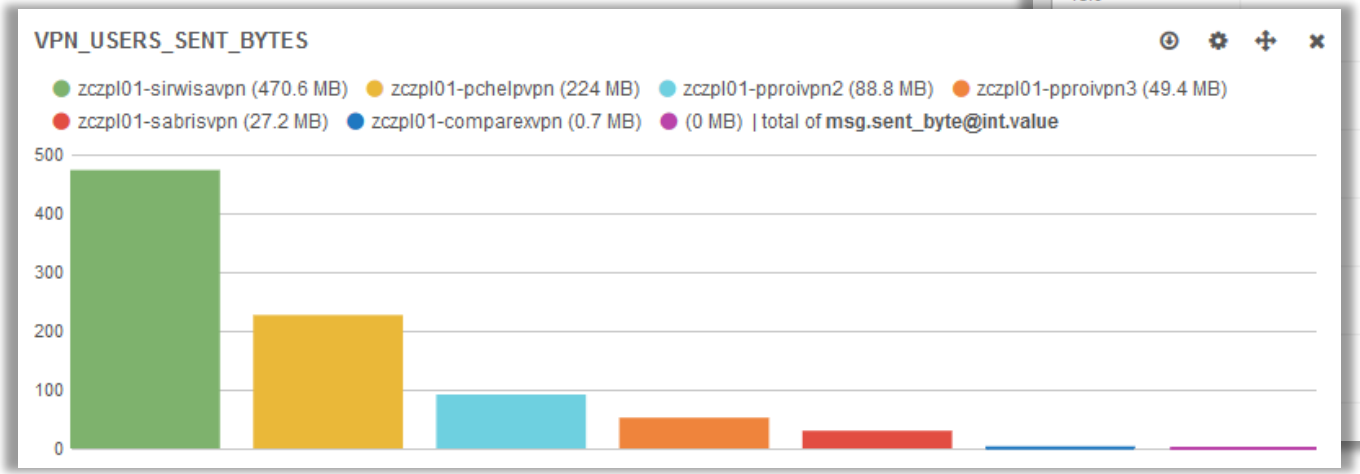
Síťová | Bezpečnostní | Systémy | Aplikace



Snímek obrazovky z akce

- Zobrazí přihlášení a odhlášení
- Identifikuje cíle komunikace z VPN
- Zobrazí týdenní data za uživatele
- Provede Audit všech přihlášení do CSV
- Provede Alert při uzamknutí účtu
- Zobrazí IP adresu a Geolokaci v mapě





LOGmanager

Představení

Schéma LOG manager

Malý LOGmanager
nebo Forwarder

WAN vzdálený sběr s šifrováním, QoS a bufferem

LAN přímý sběr

IPSEC

IPSEC

Syslog

Syslog NG

WES

Windows
Event Sender

DB

Log4j/XML

CheckPoint, VMWARE, SQL

UDP

CEF

TCP

JSON

File

Prot

Prot

REST-API
Syslog -out

Prezentační rozhraní

Aplikační engine

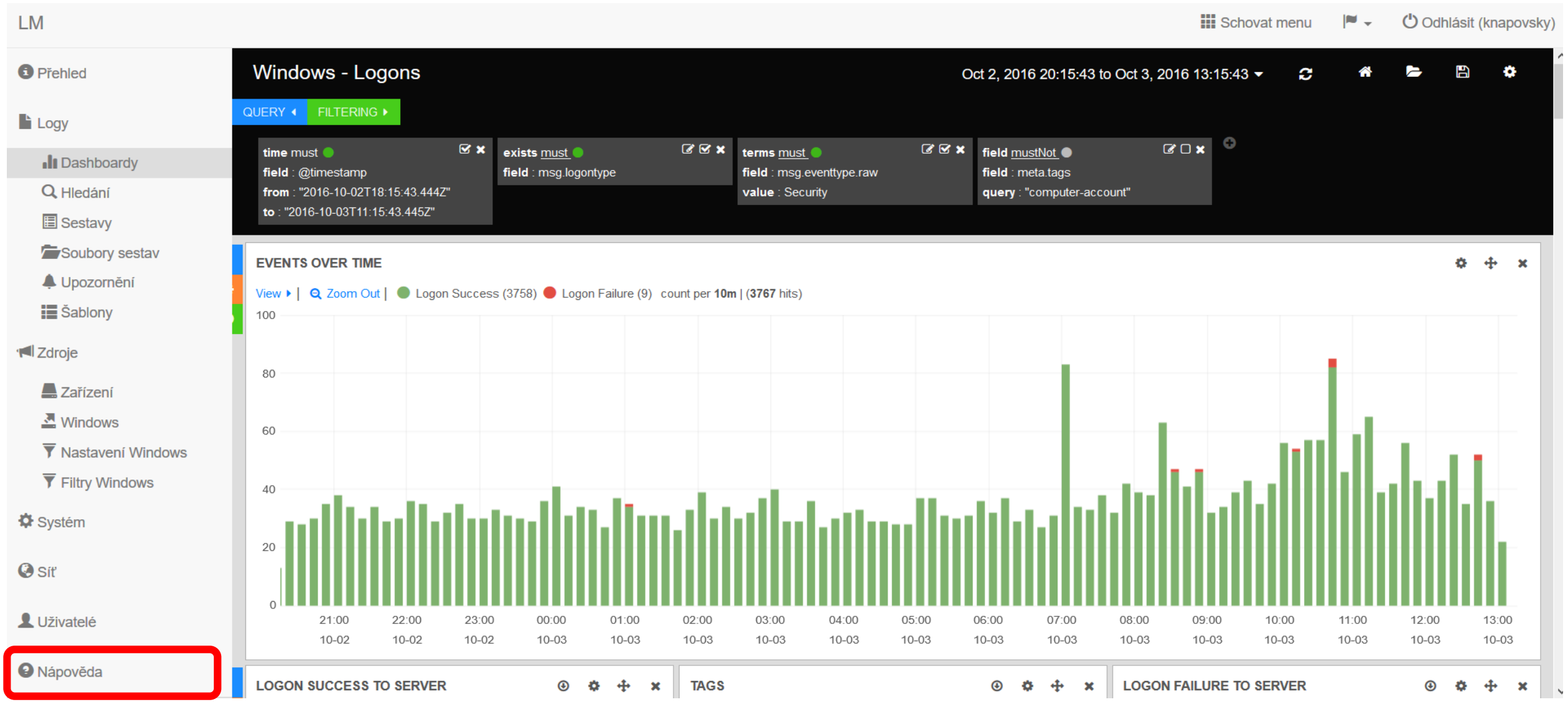
Buffer

Parser

12/40/100TB db

LOGmanager

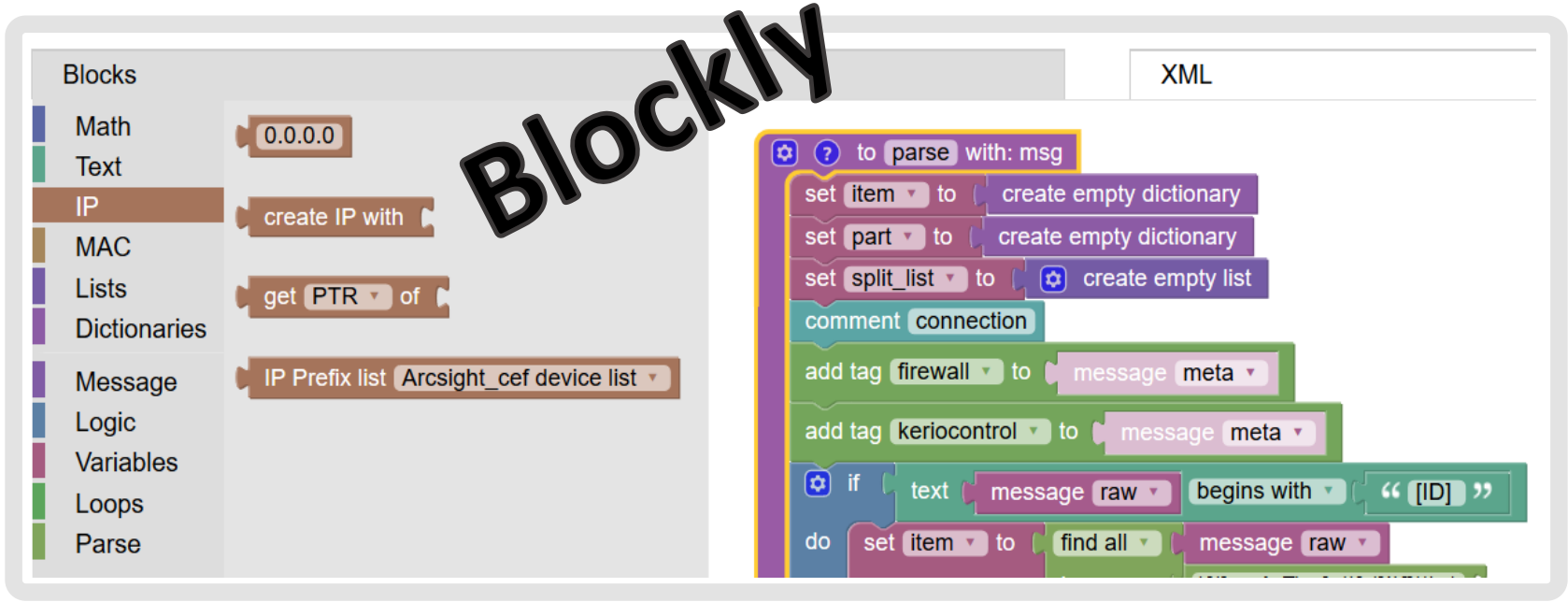
LOGmanager rozhraní



LOGmanager

Radikální jednoduchost

- Dashboardy
- Alerty
- Reporty
- Databáze zařízení
- Systém oprávnění



- Vestavěné i zákaznicky vytvářené parsery logů
- Metadata, integrace (např. MS AD, Turris Greylist)
- Uživatelské fórum

PROJECT:TURRIS

LOGmanager

Parametry a Roadmapa, Reference

LOGmanager

Podporované systémy

Víc než 100 zdrojů v základu

- **Infrastruktura:**
  Brocade SAN, Cisco (IOS, ASA, WLC), Dell
  FortiNet (FG, FML, FA), FlowMon
  Huawei, H3C, HPE, CheckPoint, Juniper
  Kernun, Trapeze UBNT (Rocket, Unifi)
  PaloAlto Networks Mikrotik, Extreme
  Sophos, Trend Micro…

- **Software:**
  AV (Eset, Avast, Kaspersky, AVG)
  Apache web server, Tomcat
  Novell eDirectory, CompuNet GAMA
  HPE iMC, Kerio Connect, SAP
  SQL (MySQL, MSSQL, Oracle, Postgres)
  Vmware,…

- **Microsoft:**
  Windows Vista, 7, 8, 10
  Server 2008, 2012, 2016
  Sharepoint, Exchange, MS-SQL
  Microsoft Windows IIS, Windows firewall
  Windows – any text logs…

- **Linux/Unix:**
  Amavis, Freeradius
  ISC Bind, ISC DHCP
  NGiNX
  Postfix
  SSH & DropBear…

a všechny systémy, co používají JSON, CEF a LEEF formát logů

Parametry

01 **Trvalý příjem až 7.000 logů za sekundu**

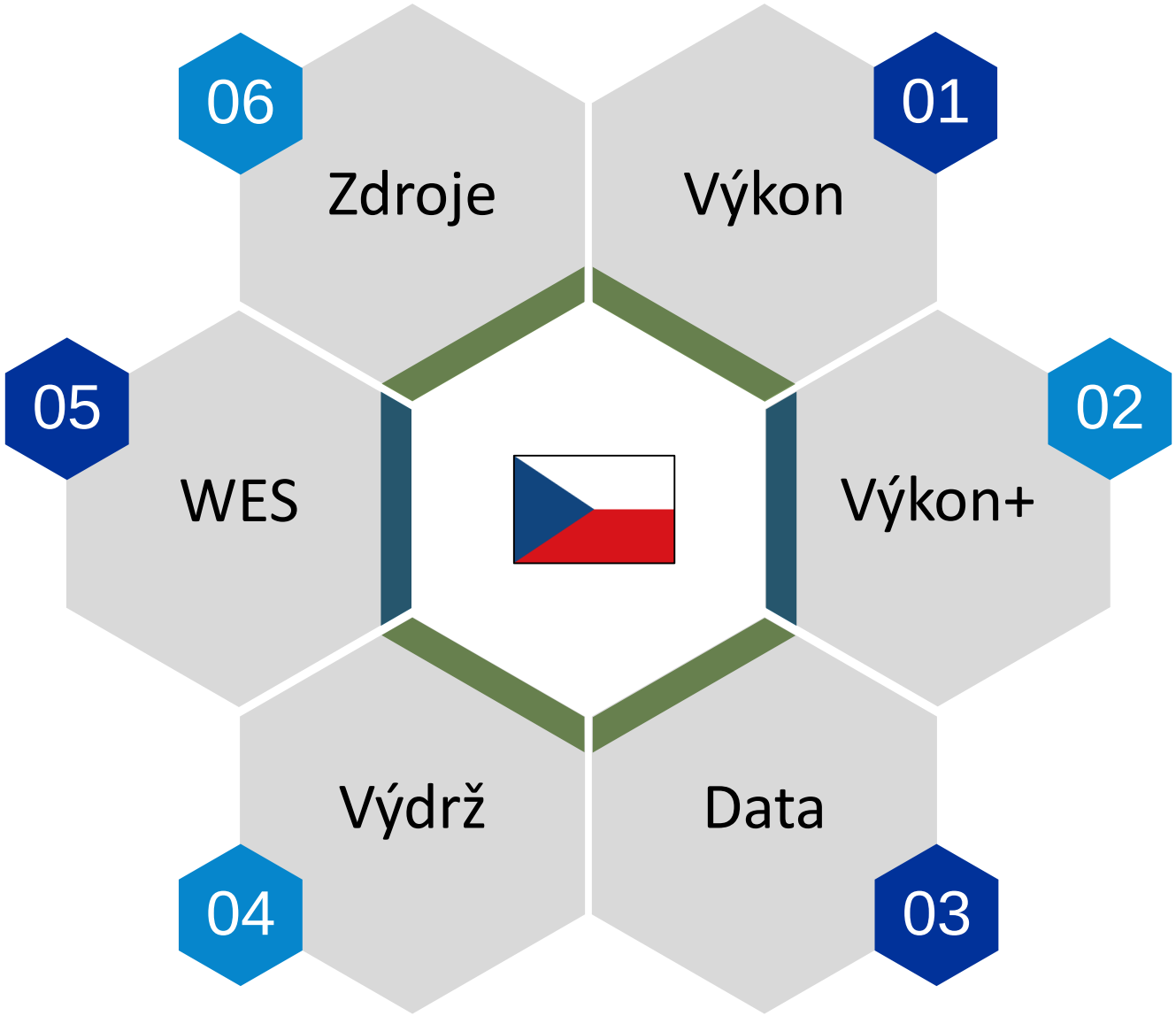
02 **Workload akcelerátor pro Velký a XL LOGmanager**

03 **V základu uložení až 100TB logů**

04 **Nativní podpora clusteringu**

05 **Vlastní centrálně řízený klient pro Windows**

06 **Neomezený počet zdrojů**



Parametry

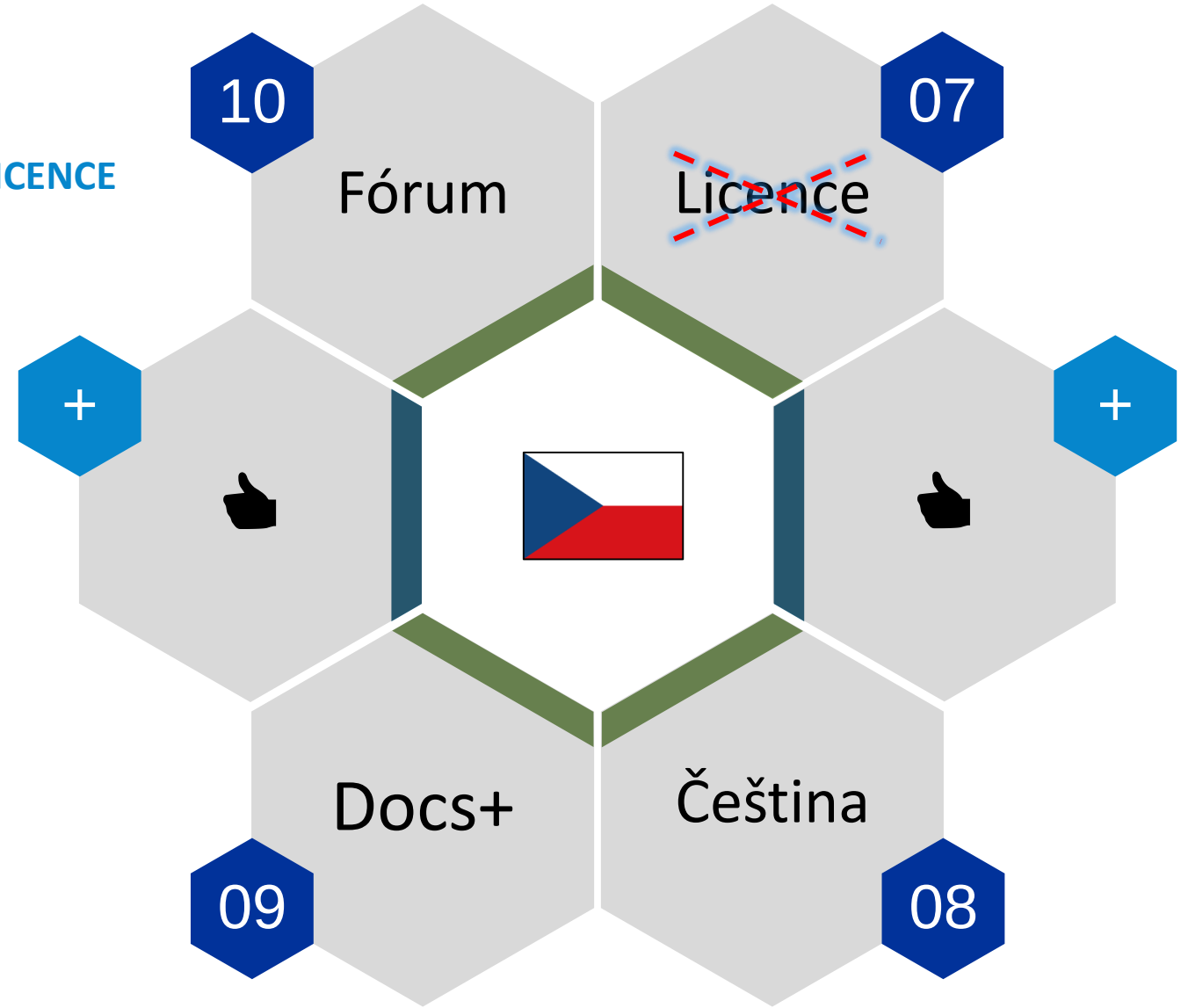
07 **Snadný a přehledný systém licencování. – ŽÁDNÉ LICENCE**

08 **Přímá technická podpora výrobcem v českém jazyce**

09 **Dokumentace a rozhraní v češtině, angličtině a pokud bude zájem tak i v jakémkoliv jiném**

10 **Moderované uživatelské fórum**

\+ **Nové funkce - naslouchámeme zákazníkům**



Vývoj LOGmanageru

Máme tah na branku

Databázový stroj Parser engine Databáze zařízení	Podpora CEF WES – Windows Event Sender s filtrací irelevantních událostí DNS Resolver Alerty Reporty	Podpora LEEF Přístupová práva Kategorizace zařízení Kategorizace událostí Šifrování disků	Event correlator v reálném čase Uživatelské parsery Archivace na externí úložiště Export událostí v JSON Forwarder	Podpora LEEF Retence dat + Rozšíření Event Correlator Příjem SNMP událostí Virtuální konektory Workload Akcelerátor	IPv4/IPv6 Dual Stack Nový design Nové API Spouštění skriptů Thresholdy Sjednocování identit Statistiky ...

PARSERY – průběžné aktualizace a doplňování

SYSTÉM – zvyšování výkonu a optimalizace

Security Event Management → SIEM

2014 | 2015 | 2016 | 2017 | 2018

Více než 80 zákazníků

Česká televize – možnost návštěvy

Slovensko: 4 zákazníci

Česká zemědělská univerzita

Ostravská univerzita

Magistrát Hlavního Města Prahy

Státní zemědělský intervenční fond

ZZS Olomouckého kraje

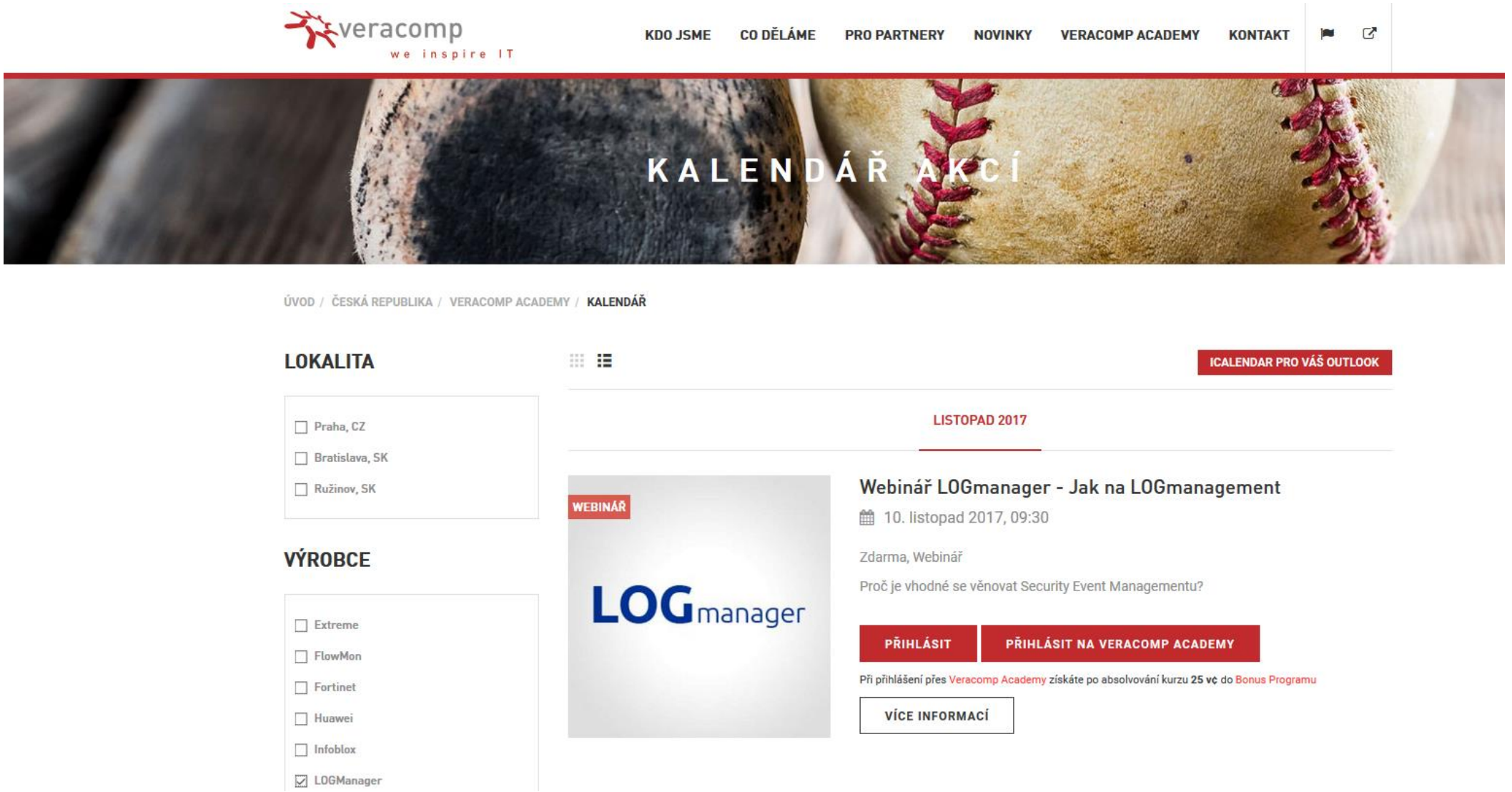
Ministerstva (Zdravotnictví, Kultury, Dopravy)

Vojenské lesy a.s.

Panasonic AVC Plzeň

ČEZ

Další akce online



https://www.veracomp.cz/cz/kalendar-akci

LOGmanager – Souhrn

- Centrální přehled s grafickou prezentací
- Intuitivní a rychlé vyhledávání
- Audit a forenzní analýza
- Inteligentní alerty a snadné reporty
- Sjednocení formátu a retence logů
- Dlouhodobé online uložení dat
- Podpora clusteru
- Centrální úložiště logů s obrovskou kapacitou

Řešení Kritických IT Incidentů

Plní požadavky Zákona o kybernetické bezpečnosti, GDPR ISO/IEC 27001 a PCI-DSS.

Uschování logů pro předložení organizacím zabývajících se bezpečností nebo Policii ČR.

A to vše bez licencí, v češtině a na výkonném hardware s výměnou do příštího pracovního dne.

LOGmanager

Děkuji za pozornost

Miroslav Knapovský CISSP, CEH, CCSK
Security Solution Architect

knapovsky@logmanager.cz