LOGmanager

> Důvody, proč se věnovat správě logů

4.dubna 2017

ISSS Konference v Hradci Králové

Miroslav Knapovský CISSP, CEH, CCSK
Security Solution Architect
knapovsky@logmanager.cz

Nějak se nám to tady množí…

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

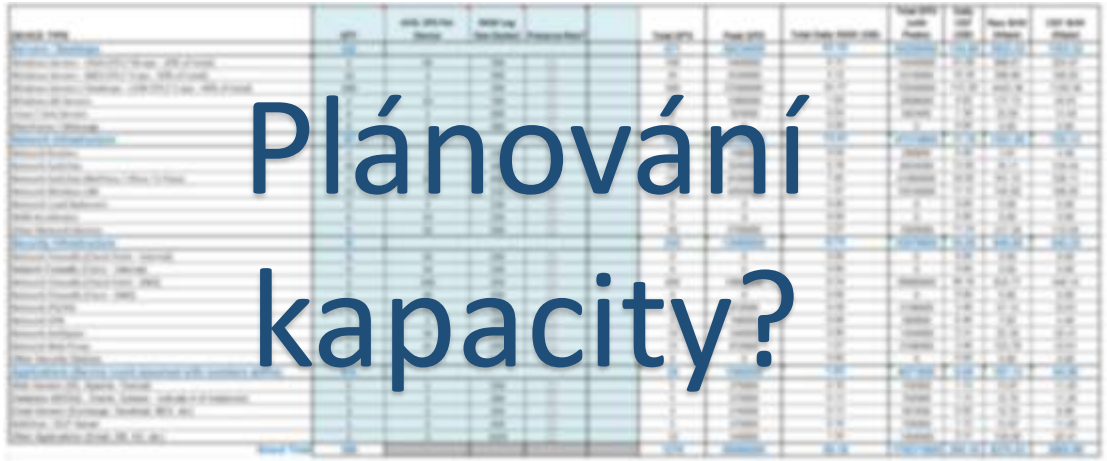
Zdroj: wikipedia.org

Current World Population

7,495,311,492

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



Plánování kapacity?

- ~ 2910 zaměstnanců
- ~ 1200 zdrojů / 3500+ EPS / 95-300 GB logů denně
- ~ Miliarda logů za týden

Zdroj: ČT 02/17

Proč se sběrem/pochopením logů zabývat ?

- **Praktické / provozní důvody**
  - Logy uložené na různých zařízeních nebo vůbec
  - Velikost jednotlivých log souborů a jejich rotace
  - Nejde centrálně vyhledávat / Kritický IT incident
- **Bezpečnostní důvody**
  - Korelace – statistické, bezpečnostní
  - Nebezpečí modifikace logů
  - Přehled o anomáliích, incidentech
- **Zákonné důvody**
  - Zákon o kybernetické bezpečnosti - § 23
  - General Data Protection Regulation od května 2018

Whitepaper na logmanager.cz


LOGmanager
> SIEM
> Centrální úložiště logů

Nasazení a provoz centrálního systému na správu a analýzu logů

Důvodová zpráva s argumenty pro nasazení SEM-SIEM řešení včetně uživatelských příkladů

Existují tři základní důvody, pro které organizace zvažují nasazení systému pro centralizovanou správu a analýzu logů. Jsou z těchto oblastí a každá může mít v organizaci dle jejího zaměření rozdílnou váhu:

- Provozní a operační
- Bezpečnostní
- Dodržení souladu s regulacemi a audit

V následujícím popisu jsou rozvedeny jednotlivé oblasti s konkrétními případy možného praktického použití LOGmanageru pro danou agendu. Možnosti použití jsou samozřejmě podstatně širší, vzorek uživatelských případů je pouze ilustrativní pro vytvoření základní představy.

Provozní a operační oblast

Kritický IT incident je středobodem dnešního IT světa, je nevyhnutelný stejně jako daně a smrt, protože dříve či později přijde. První, co znamená kritický IT incident – je to stav, kdy je nefunkční business aplikace nebo infrastruktura, na které je kritická aplikace navázaná. Taková situaci vyžaduje okamžité řešení, při kterém členové IT teamu organizace dle charakteru incidentu spolupracují na urychleném odstranění závady. V této souvislosti se zažily dva pojmy – MTTR a RCA (Mean Time To Repair a Root Cause Analysis; volně přeloženo to znamená Střední doba k nápravě a Analýza příčin problému). Snahou IT oddělení je najít co nejdříve příčinu výpadku a odstranit ji, poté analyzovat proč k výpadku došlo včetně souvislostí, zhodnotit celý incident a určit opravné mechanismy, aby ke stejné nebo podobné závadě příště nedošlo.

***Příklad použití LOGmanageru z praxe pro Kritický IT incident**: Známe přibližný čas počátku výpadku, aktuálně nic vyjma broadcast domén nekomunikuje. V LOGmanageru – dashboardu „All Event*

LOGmanagement a Kritický IT Incident

KRITICKÝ IT INCIDENT – VĚTŠINA ORGANIZACÍ ZAŽIJE 1-3 MĚSÍČNĚ

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

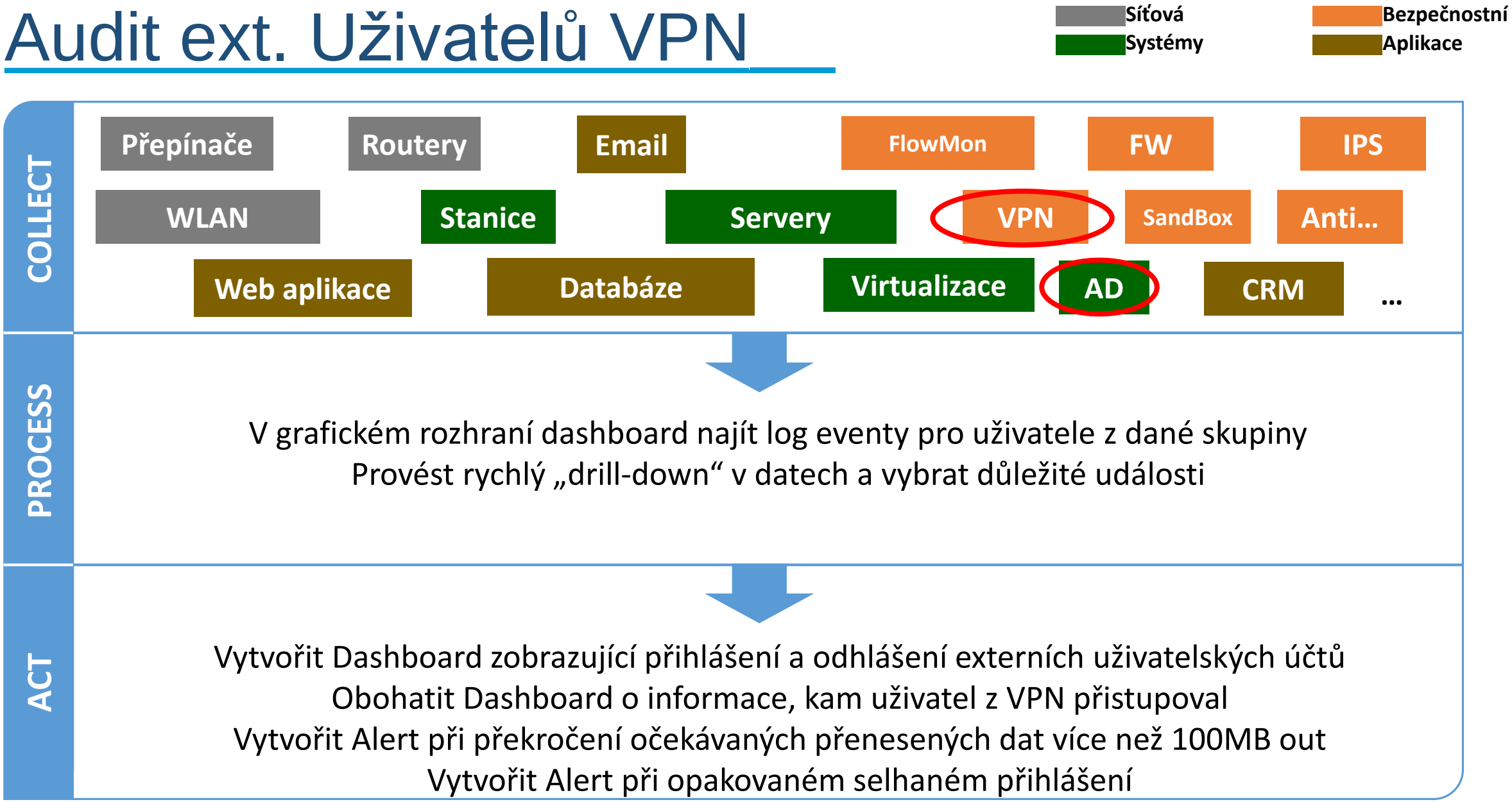
Dva důležité pojmy – **MTTR a RCA** – pro CIO: „*čas jsou peníze*“

Snížit MTTR/RCA umožňuje IT Operation Intelligence

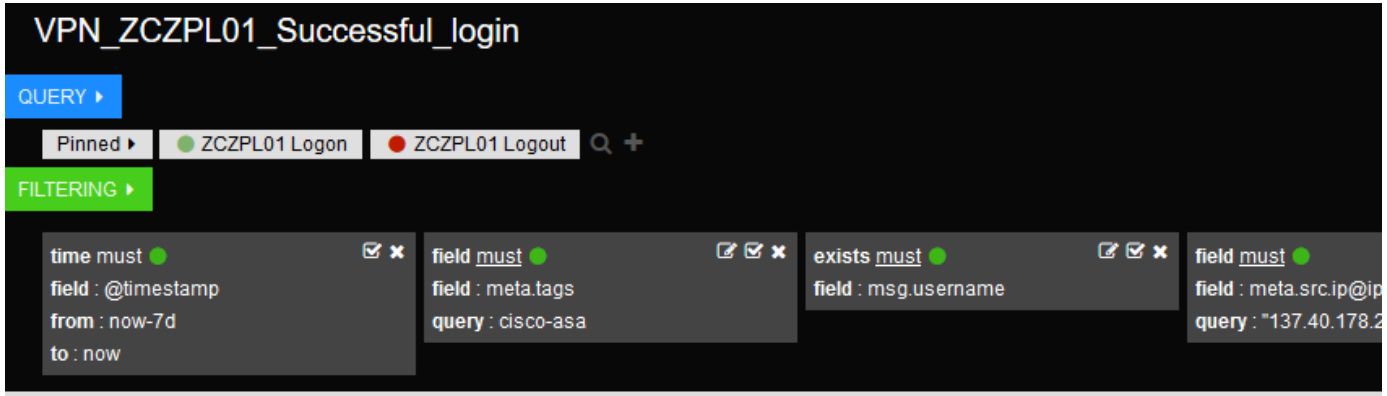
Základem IT OPS je vhodný nástroj na sběr logů

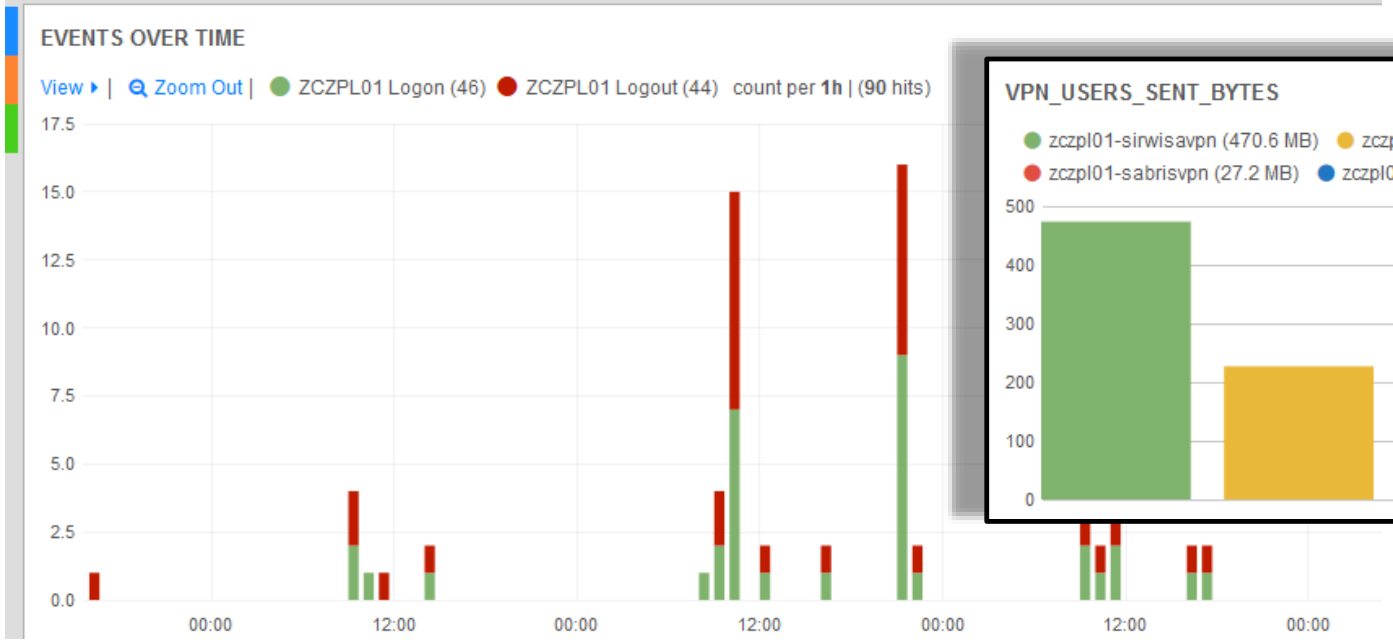
- Viditelnost
- Koordinace
- Produktivita při řešení incidentu

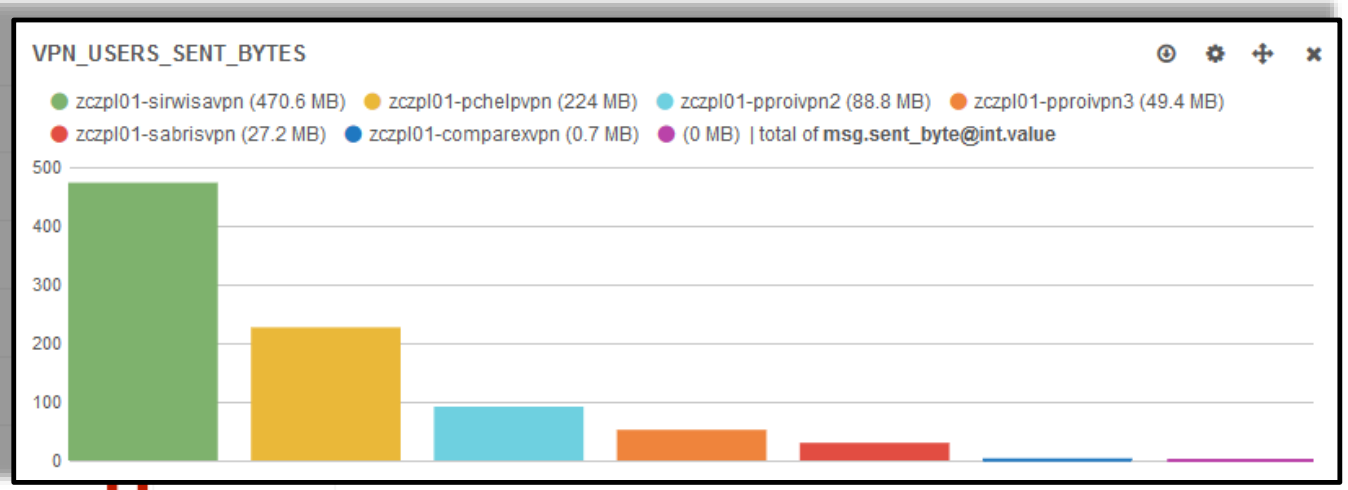
Audit ext. Uživatelů VPN



Snímek obrazovky z akce

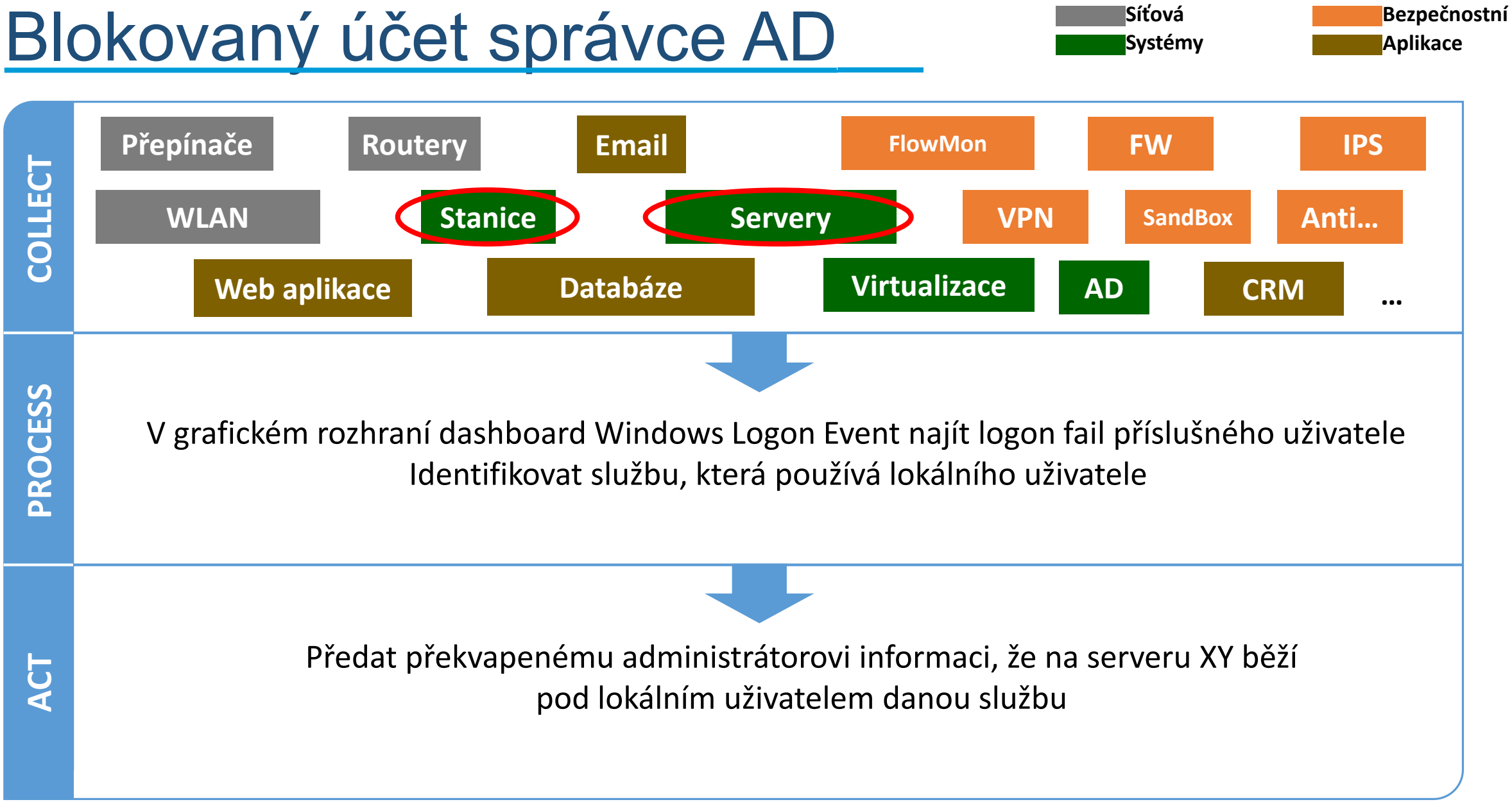




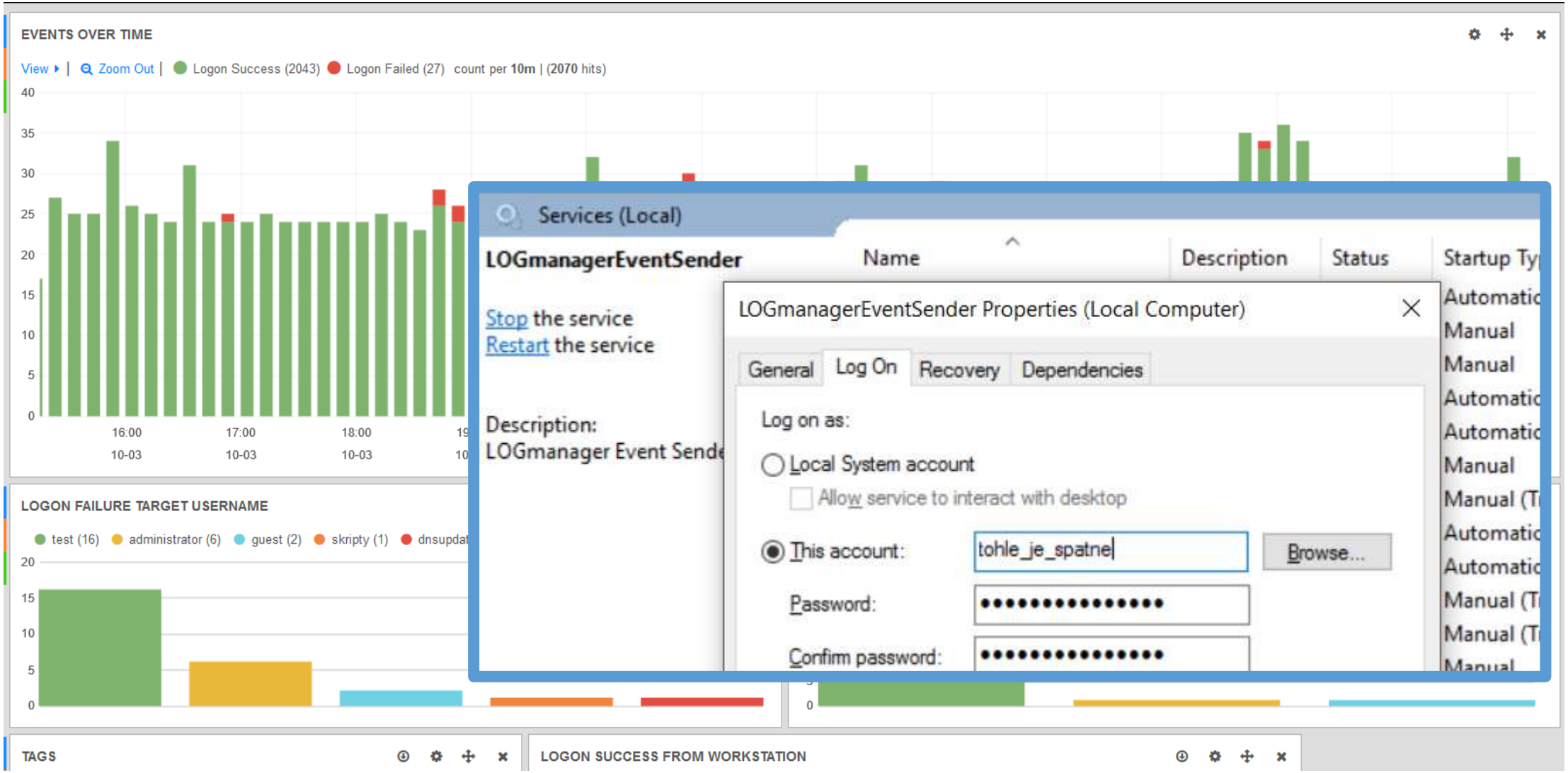


Zobrazí přihlášení a odhlášení
Identifikuje cíle komunikace z VPN
Zobrazí týdenní data za uživatele
Provede Audit všech přihlášení do CSV
Provede Alert při uzamknutí účtu
Zobrazí IP adresu a Geolokaci v mapě

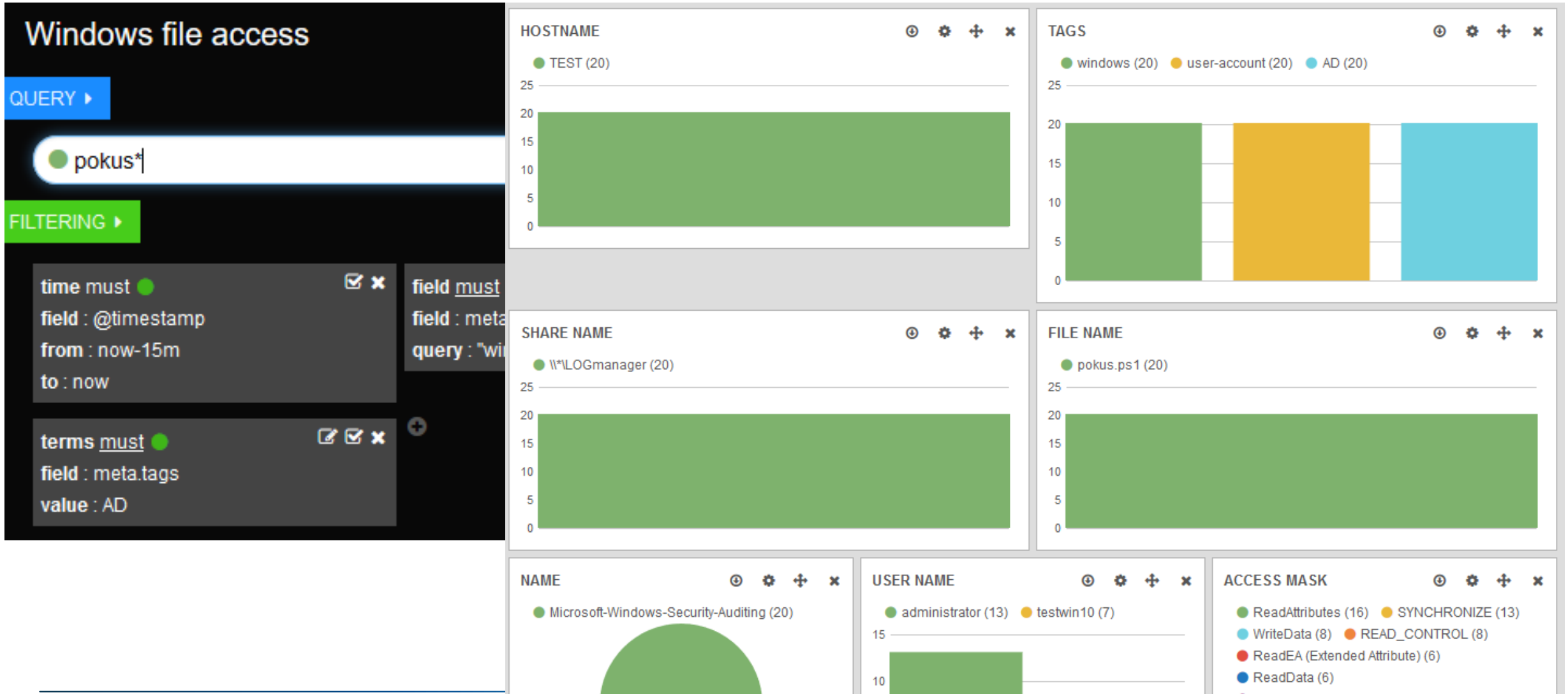
Blokovaný účet správce AD



Snímek obrazovky z akce



Pokročilý audit přístupu k souborům



LOGmanager

LOGmanager
představení

Schéma LOGmanager

Malý LOGmanager
nebo Forwarder

IPSEC
IPSEC

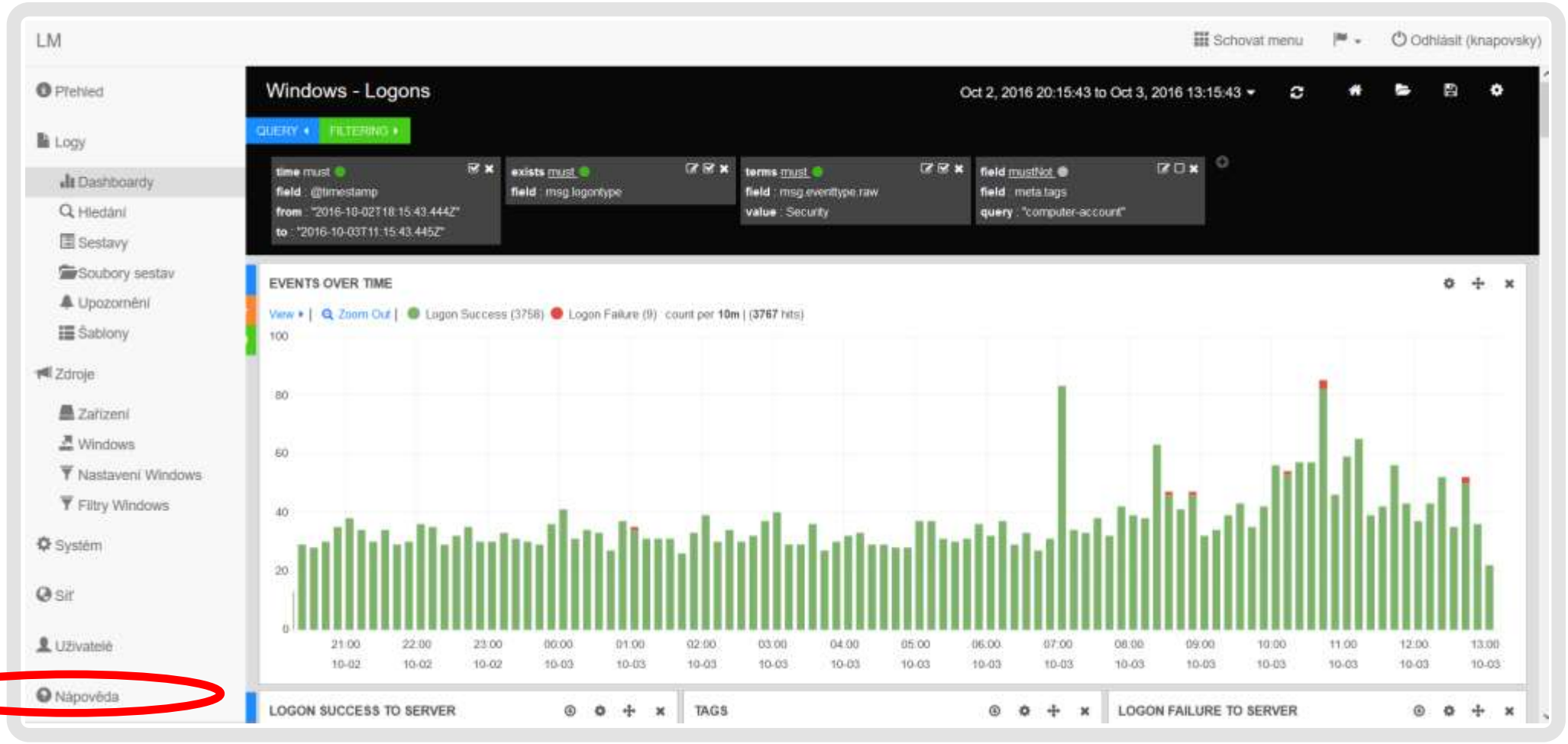
WAN vzdálený sběr s šifrováním, QoS a bufferem
LAN přímý sběr

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
12/40TB Database
LOGmanager

LOGmanager rozhraní



Podporovaná zařízení

HARDWARE:

Brocade SAN, Cisco (ASA, WLC), FortiNet (FG, FML, FA), H3C, HP (ComWare i ProCurve), CheckPoint, Juniper SRX, Kernun, Trapeze wifi, UBNT (Rocket, Unifi), PaloAlto Networks, …

SOFTWARE:

Apache web server, Cisco IOS, CEF, CEF TippingPoint SMS, Novell eDirectory, CompuNet GAMA, HP iLo 4, HP iMC, Kerio Connect, SAP, AV (Eset, Avast, AVG), Vmware,…

WINDOWS:

ESET Remote Administrator, Microsoft Windows IIS, Microsoft Windows firewall, Windows Avast Antivirus, Windows 7, 8, Server 2008, 2012 audit log (WES), Windows – any logs from Event Viewer, Windows – any text log from file

LINUX:

Freeradius, ISC Bind, ISC DHCP, SSH

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

Reference

Česká televize – možnost návštěvy
Česká zemědělská univerzita
Ostravská univerzita
Městská část Praha 3
Státní zemědělský intervenční fond
Krajská zdravotní a.s.
Vojenské lesy a.s.
Panasonic AVC Plzeň
ČEZ

LOGmanager – poslední slide ;-)

- **Řešení Kritických IT Incidentů**
- **Plní požadavky Zákona o kybernetické bezpečnosti, GDPR a ISO/IEC 27001.**
- **Uschování logů pro předložení organizacím zabývajících se bezpečností nebo Policii ČR.**

- Centrální přehled s grafickou prezentací
- Intuitivní a rychlé vyhledávání
- Forenzní analýza
- Alerty, reporty
- Sjednocení formátu logů
- Dlouhodobé uložení se zálohováním do NFS
- Podpora clusteru v základu
- Centrální úložiště logů s obrovskou kapacitou

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

Vývojář: Sirwisa a. s. www.sirwisa.cz
Distribuce: Veracomp s. r. o. www.veracomp.cz

www.logmanager.cz