Bezpečnost dat a řešení IT incidentů pomocí SIEM

Luboš Lunter
CPO

lubos.lunter@logmanager.com
www.logmanager.com

Představení

- Nástroj pro správu a uchovávání logů s funkcemi SIEM
- Více než **10 let** na trhu
- Aktuálně přes **300 zákazníků** ve střední a východní Evropě
- Radically simple log management

Reference

Česká televize

O2

Dr.Max

Cargo

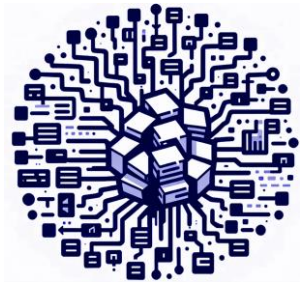
Vysoká škola ekonomická v Praze

Dopravní podnik města Brna a.s.

Log management

Výzvy v log managementu

Chybějící standard



Nejednotné získávání různých typů událostí

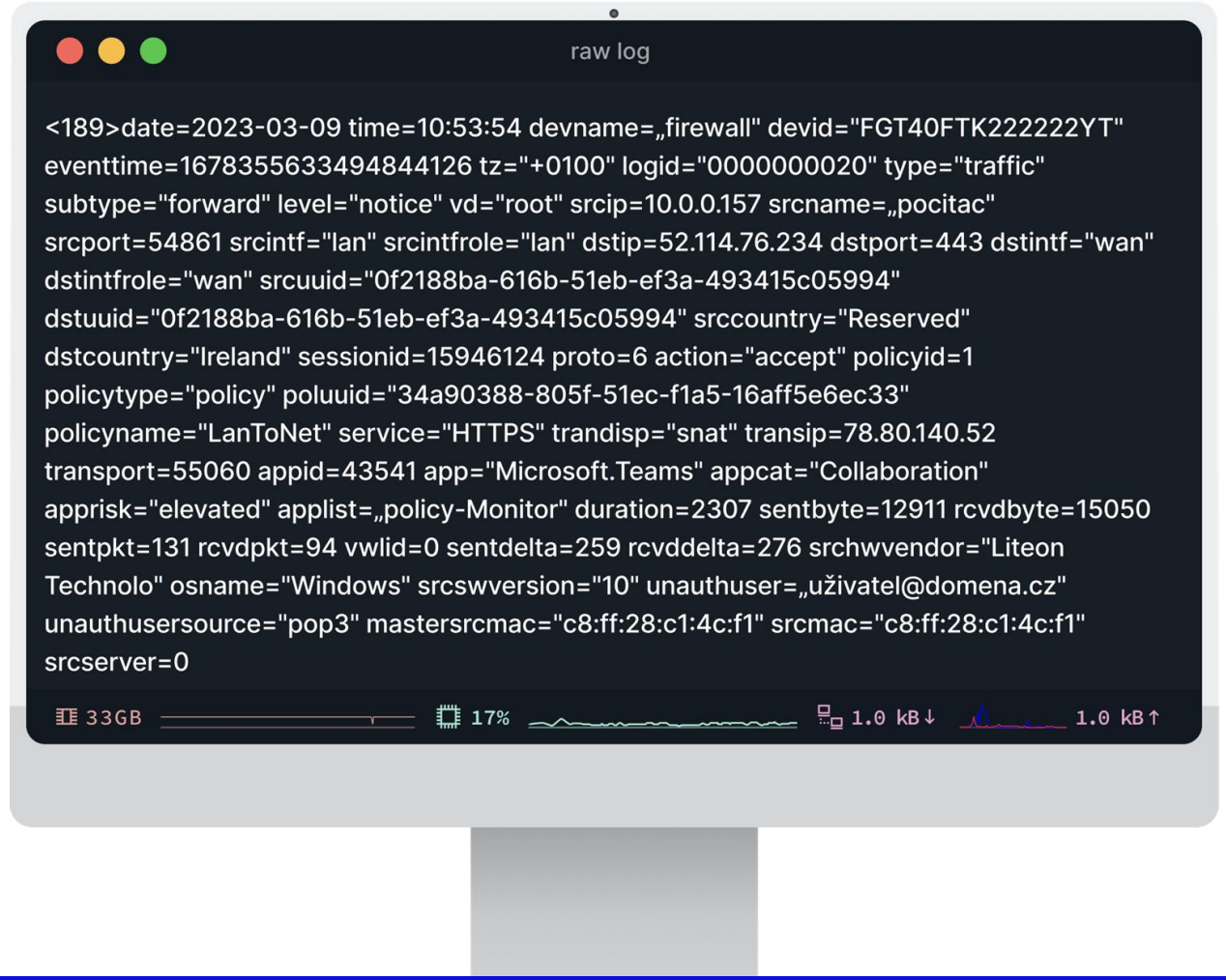
Centrální ukládání dat z různých systémů

Velký objem dat

Legislativní požadavky

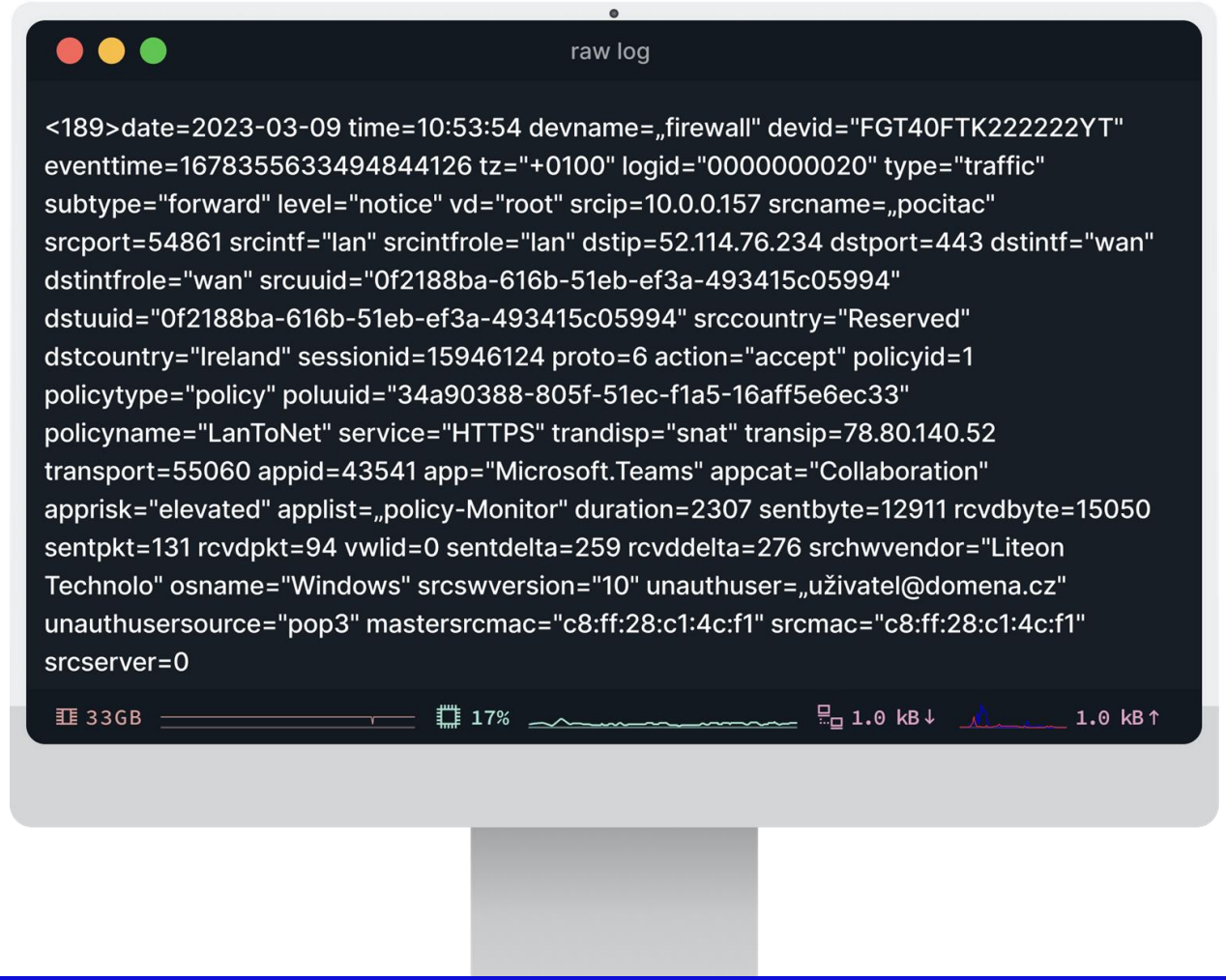
Velké množství šumu

Log z blízka


raw log
<189>date=2023-03-09 time=10:53:54 devname=„firewall" devid="FGT40FTK222222YT"
eventtime=1678355633494844126 tz="+0100" logid="0000000020" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.0.0.157 srcname=„pocitac"
srcport=54861 srcintf="lan" srcintfrole="lan" dstip=52.114.76.234 dstport=443 dstintf="wan"
dstintfrole="wan" srcuuid="0f2188ba-616b-51eb-ef3a-493415c05994"
dstuuid="0f2188ba-616b-51eb-ef3a-493415c05994" srccountry="Reserved"
dstcountry="Ireland" sessionid=15946124 proto=6 action="accept" policyid=1
policytype="policy" poluuid="34a90388-805f-51ec-f1a5-16aff5e6ec33"
policyname="LanToNet" service="HTTPS" trandisp="snat" transip=78.80.140.52
transport=55060 appid=43541 app="Microsoft.Teams" appcat="Collaboration"
apprisk="elevated" applist=„policy-Monitor" duration=2307 sentbyte=12911 rcvdbyte=15050
sentpkt=131 rcvdpkt=94 vwlid=0 sentdelta=259 rcvddelta=276 srchwvendor="Liteon
Technolo" osname="Windows" srcswversion="10" unauthuser=„uživatel@domena.cz"
unauthusersource="pop3" mastersrcmac="c8:ff:28:c1:4c:f1" srcmac="c8:ff:28:c1:4c:f1"
srcserver=0
33GB
17%
1.0 kB↓
1.0 kB↑

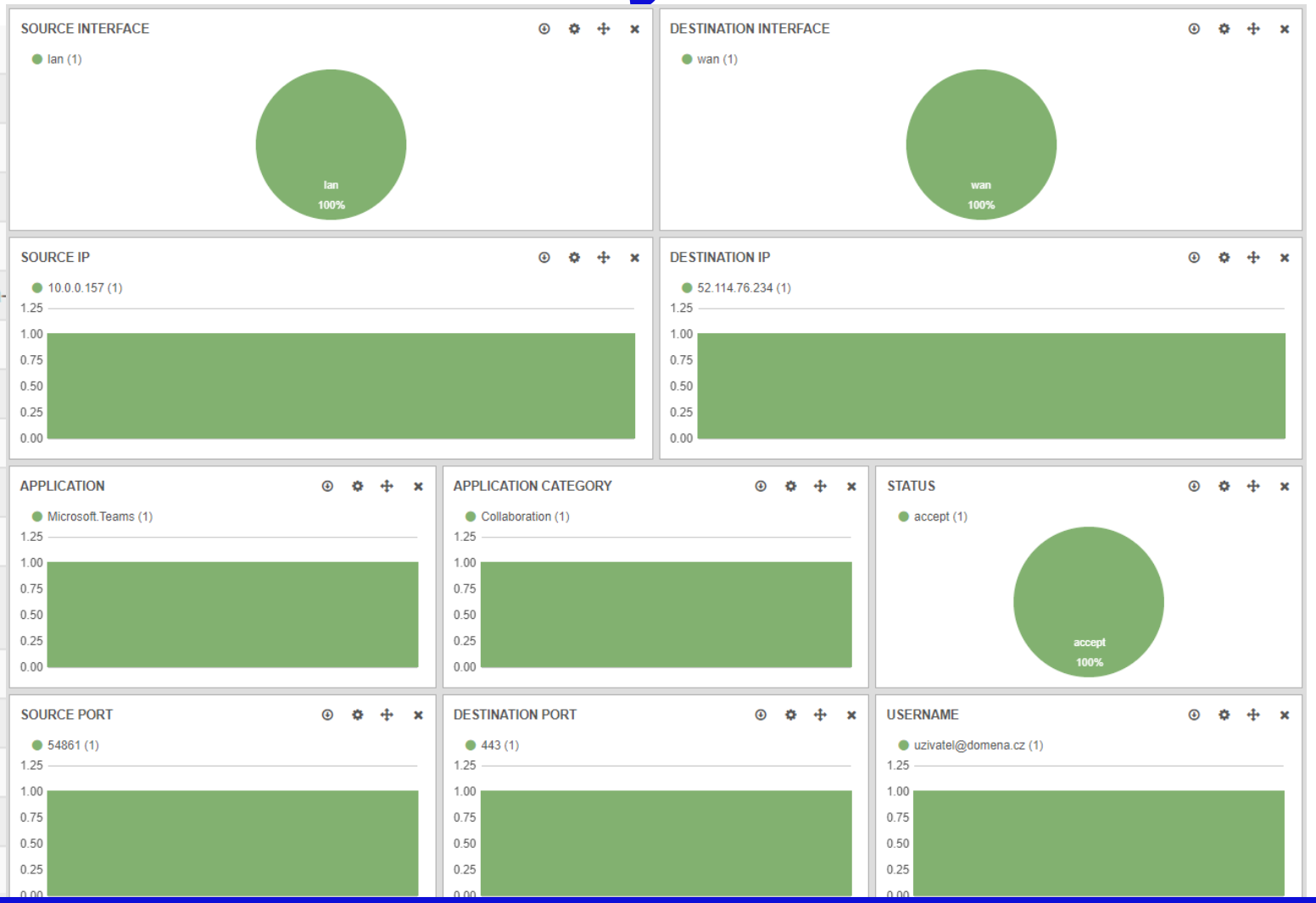
Logmanager

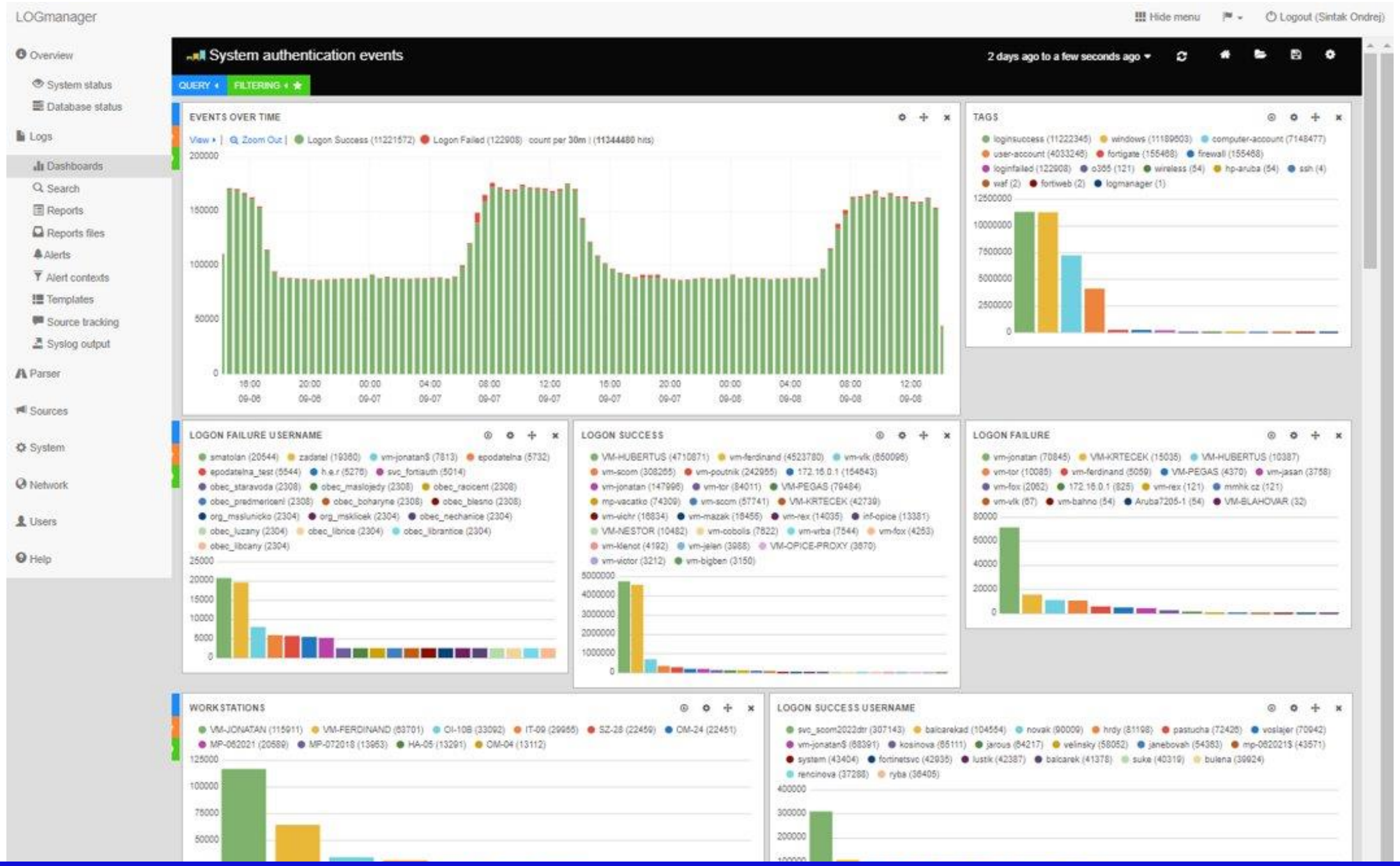
Takhle to vidíme my

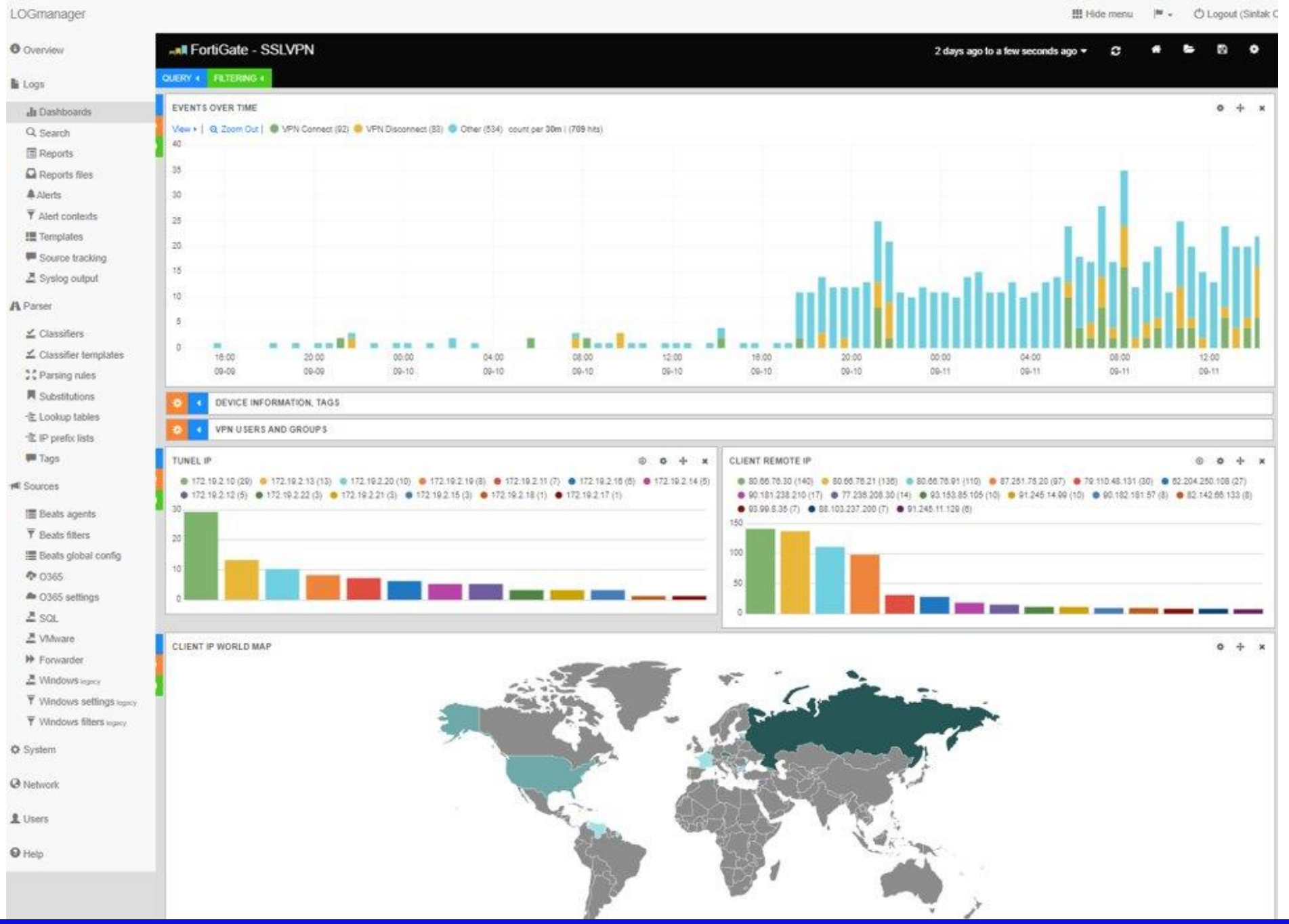


Takhle to vidíme my

msg.srchwvendor		Liteon Technolo
msg.srcintfrole		lan
msg.srcname		pocitac
msg.srcserver		0
msg.srcswversion		10
msg.srcuuid		0f2188ba-616b-51eb-ef3a-
msg.status		accept
msg.subtype		forward
msg.transposition_disposition		snat
msg.transposition_src_ip		78.80.140.52
msg.transposition_src_port		55060
msg.transposition_src_port@int.value		55060
msg.type		traffic
msg.tz		+0100
msg.unauthuser		uzivatel@domena.cz
msg.unauthusersource		pop3
msg.vd		root




LOGmanager
Hide menu
Logout (Sintak Ondrej)
Overview
System status
Database status
Logs
Dashboards
Search
Reports
Reports files
Alerts
Alert contexts
Templates
Source tracking
Syslog output
Parser
Sources
System
Network
Users
Help
System authentication events
2 days ago to a few seconds ago
QUERY
FILTERING
EVENTS OVER TIME
View | Zoom Out | Logon Success (11221572) Logon Failed (122908) count per 30m | (11344480 hits)
200000
150000
100000
50000
0
16:00 09-06
20:00 09-06
00:00 09-07
04:00 09-07
08:00 09-07
12:00 09-07
16:00 09-07
20:00 09-07
00:00 09-08
04:00 09-08
08:00 09-08
12:00 09-08
TAGS
loginsuccess (11222345) windows (11189503) computer-account (7148477)
user-account (4033248) fortigate (155468) firewall (155468)
loginfailed (122908) o365 (121) wireless (54) hp-aruba (54) ssh (4)
waf (2) fortiweb (2) logmanager (1)
12500000
10000000
7500000
5000000
2500000
0
LOGON FAILURE USERNAME
smatolan (20544) zadatel (19360) vm-jonatan$ (7813) epodatelna (5732)
epodatelna_test (5544) h.e.r (5276) svc_fortiauth (5014)
obec_staravoda (2308) obec_maslojedy (2308) obec_racicent (2308)
obec_predmericenI (2308) obec_boharyne (2308) obec_blesno (2308)
org_msslunicko (2304) org_msklicek (2304) obec_nechanice (2304)
obec_luzany (2304) obec_librice (2304) obec_librantice (2304)
obec_libcany (2304)
25000
20000
15000
10000
5000
0
LOGON SUCCESS
VM-HUBERTUS (4710871) vm-ferdinand (4523780) vm-vlk (850096)
vm-scom (308265) vm-poutnik (242955) 172.16.0.1 (154543)
vm-jonatan (147996) vm-tor (84011) VM-PEGAS (79484)
mp-vacatko (74309) vm-scom (57741) VM-KRTECEK (42739)
vm-vichr (16834) vm-mazak (16455) vm-rex (14035) inf-opice (13381)
VM-NESTOR (10482) vm-cobolis (7822) vm-wrba (7544) vm-fox (4253)
vm-klenot (4192) vm-jelen (3988) VM-OPICE-PROXY (3870)
vm-victor (3212) vm-bigben (3150)
5000000
4000000
3000000
2000000
1000000
0
LOGON FAILURE
vm-jonatan (70845) VM-KRTECEK (15035) VM-HUBERTUS (10387)
vm-tor (10085) vm-ferdinand (5059) VM-PEGAS (4370) vm-jasan (3758)
vm-fox (2062) 172.16.0.1 (825) vm-rex (121) mmhk.cz (121)
vm-vlk (87) vm-bahno (54) Aruba7205-1 (54) VM-BLAHOVAR (32)
80000
60000
40000
20000
0
WORKSTATIONS
VM-JONATAN (115911) VM-FERDINAND (63701) OI-10B (33092) IT-09 (29955) SZ-28 (22459) OM-24 (22451)
MP-062021 (20589) MP-072018 (13953) HA-05 (13291) OM-04 (13112)
125000
100000
75000
50000
LOGON SUCCESS USERNAME
svc_scom2022dtr (307143) balcarekad (104554) novak (90009) hrdy (81198) pastucha (72428) voslajer (70942)
vm-jonatan$ (68391) kosinova (65111) janous (64217) velinsky (58052) janebovah (54383) mp-062021$ (43571)
system (43404) fortinetsvc (42935) lustik (42387) balcarek (41378) suke (40319) bulena (39924)
rencinova (37268) ryba (36405)
400000
300000
200000


LOGmanager
Hide menu
Logout (Sinlak C
Overview
Logs
Dashboards
Search
Reports
Reports files
Alerts
Alert contexts
Templates
Source tracking
Syslog output
Parser
Classifiers
Classifier templates
Parsing rules
Substitutions
Lookup tables
IP prefix lists
Tags
Sources
Beats agents
Beats filters
Beats global config
O365
O365 settings
SQL
VMware
Forwarder
Windows legacy
Windows settings legacy
Windows filters legacy
System
Network
Users
Help
FortiGate - SSLVPN
2 days ago to a few seconds ago
QUERY
FILTERING
EVENTS OVER TIME
View
Zoom Out
VPN Connect (92)
VPN Disconnect (83)
Other (534)
count per 30m (709 hits)
DEVICE INFORMATION, TAGS
VPN USERS AND GROUPS
TUNEL IP
CLIENT REMOTE IP
CLIENT IP WORLD MAP

Unikátní vlastnosti

Záznamy nelze upravit ani smazat (ani superuser)

Jednoduché vyhledávání bez znalostí SQL

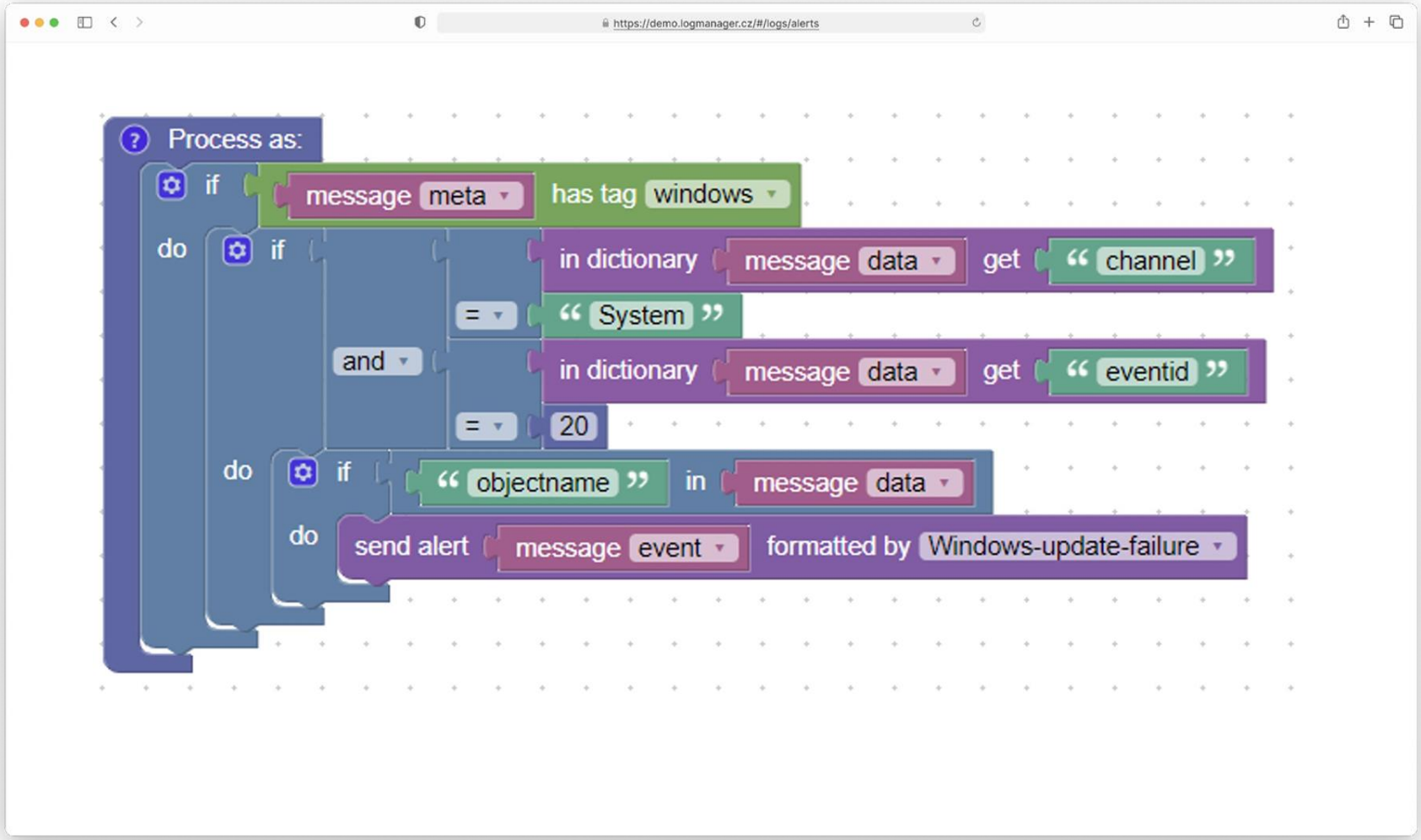
Konzistentní programování business logiky pomocí Google Blockly

Jednoduchá správa celé platformy – komplet přes web GUI

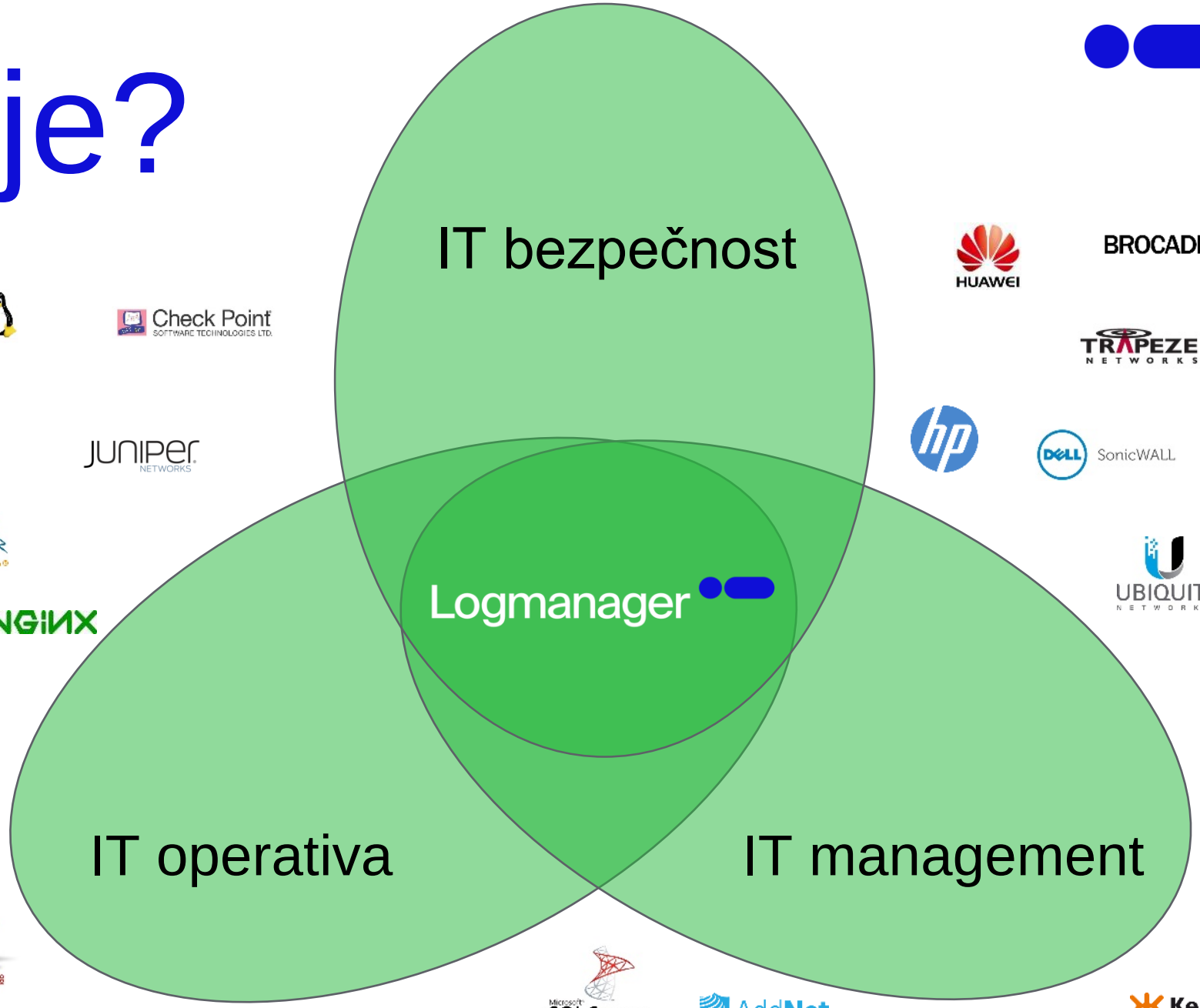
Centrální správa Forwarderů, Windows Agentů a jejich politik

Jednoduché licencování bez omezení počtu uživatelů nebo agentů

Editace Alertu v Blockly



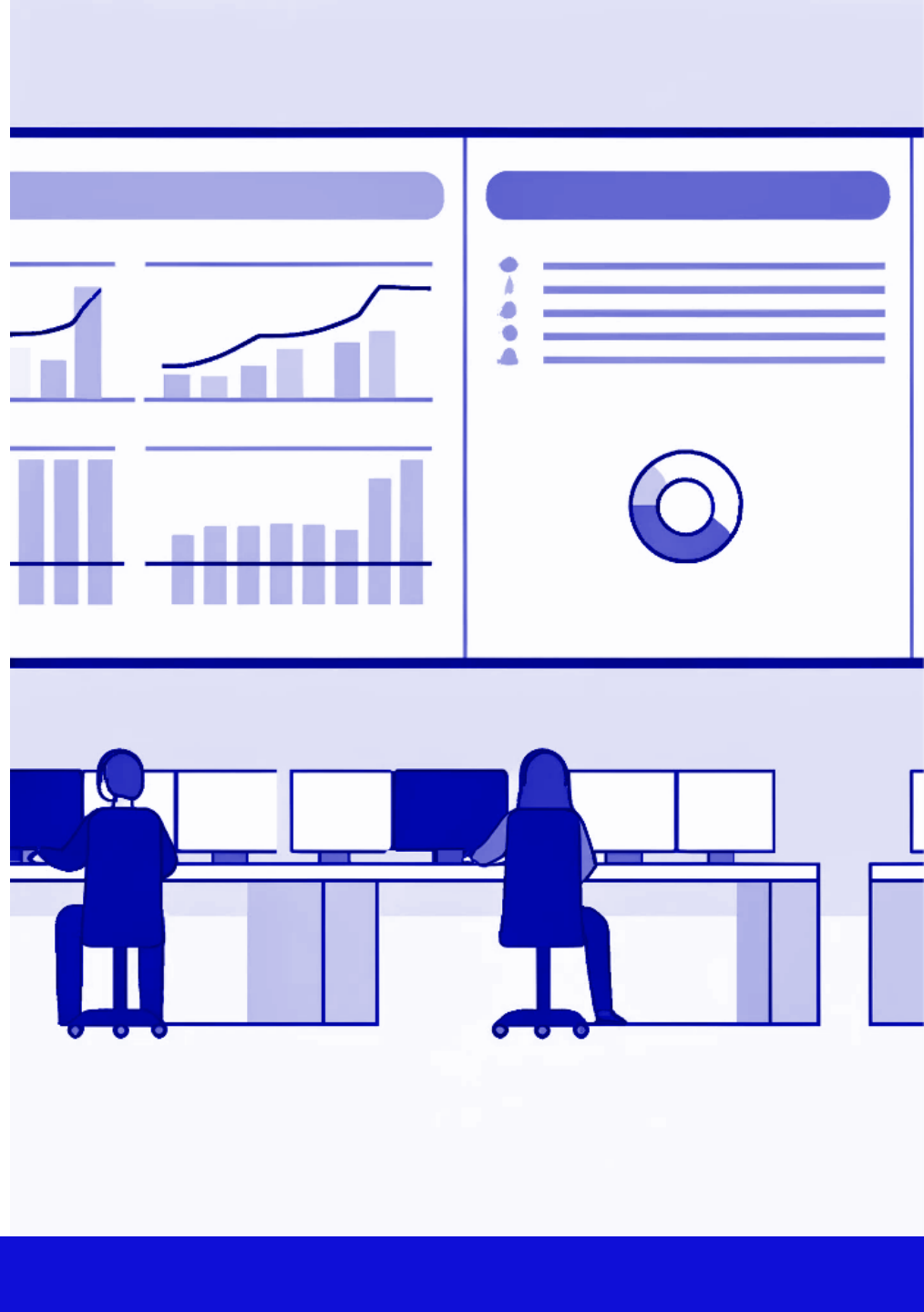
Pro koho je?



Flowmon
Driving Network Visibility
Linux
Check Point
SOFTWARE TECHNOLOGIES LTD.
Windows Server
ISS
DELL
H3C
FORTINET
JUNIPER
NETWORKS
vmware
MySQL
APACHE
TOMCAT
NGINX
DHCP
Novell
eDirectory
ORACLE
aruba
NETWORKS
GAMA
networksolutions
cisco
eset
Active Directory
KASPERSKY
ANTIVIRUS
HUAWEI
BROCADE
TRAPEZE
NETWORKS
hp
DELL
SonicWALL
UBIQUITI
NETWORKS
Microsoft
SQL Server
AddNet
Kernun

Přínos pro IT operativu

- data + analytika pro IT Operace
- dostupnost dat s minimálním zpožděním
- jednotná viditelnost dat ze všech zdrojů
- snadné zpracování textových logů
- fulltext vyhledávání
- centrálně řízený Windows agent
- návod na nastavení Windows auditních politik
- podrobná dokumentace česky a anglicky



Přínos pro IT bezpečnost

- viditelnost do bezpečnostních událostí
- granulární RBAC pro logy a správu platformy
- audit a forenzní analýza
- nesmazatelné uložení dat
- nezpochybnitelné časové razítko
- neztratí se ani jeden log, co záznam to unikátní ID
- obohacování dat
- detekce a alerting bezpečnostních událostí včetně korelace
- přeposílání logů na SIEM / UBA / SOC

Přínos pro IT management

- plnění požadavků regulací i standardů
- funkční produkt pro libovolná strojová data
- predikovatelná cena vlastnictví
- minimalizace nákladů na správu platformy
- flexibilita adaptace na změny prostředí
- naučí se obsluhovat každý z teamu
- znalosti výrobce a partnera
- shoda nejen s ISO 27001:2013

Role SIEM a log managementu v NIS2

NIS2

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu **nižších povinností**

§ 4 – Zajišťování kybernetické bezpečnosti

(1) Povinná osoba v rámci zajišťování kybernetické bezpečnosti zavede a provádí přiměřená bezpečnostní opatření zohledňující bezpečnostní potřeby organizace. Povinná osoba vždy zavede a provádí alespoň bezpečnostní opatření podle § 4 až 6 a § 11.

§ 5 – Povinnosti vrcholového vedení

§ 6 – Bezpečnost lidských zdrojů

§ 11 - Řešení kybernetických bezpečnostních incidentů

(2) Povinná osoba zajistí detekci kybernetických bezpečnostních událostí a dále při jejich

detekci používá nástroje podle § 10.

NIS2

§ 10 - Detekce a zaznamenávání kybernetických bezpečnostních událostí

(1) Povinná osoba v rámci detekce kybernetických bezpečnostních událostí zajistí

a) ověření a kontrolu přenášených dat na perimetru komunikační sítě, včetně blokování nežádoucí komunikace,

b) nástroj pro nepřetržitou a automatickou ochranu před škodlivým kódem na jednotlivých relevantních technických aktivech, zejména na 1. serverech, 2. koncových stanicích,

c) pravidelnou aktualizaci detekčních nástrojů a jejich pravidel,

d) řízení automatického spouštění obsahu a

e) nepřetržité poskytování informací o relevantních detekovaných kybernetických bezpečnostních událostech a včasné varování relevantních osob.

(2) **Povinná osoba zaznamenává kybernetické bezpečnostní události a relevantní provozní události** v souladu s odstavcem 1 a u těchto událostí zaznamenává zejména následující

a) datum a čas včetně specifikace časového pásma

b) typ činnosti,

c) jednoznačnou identifikaci technického aktiva a identifikaci účtu a

d) úspěšnost nebo neúspěšnost činnosti.

NIS2 a ZoKB

Detekce a reakce na incidenty

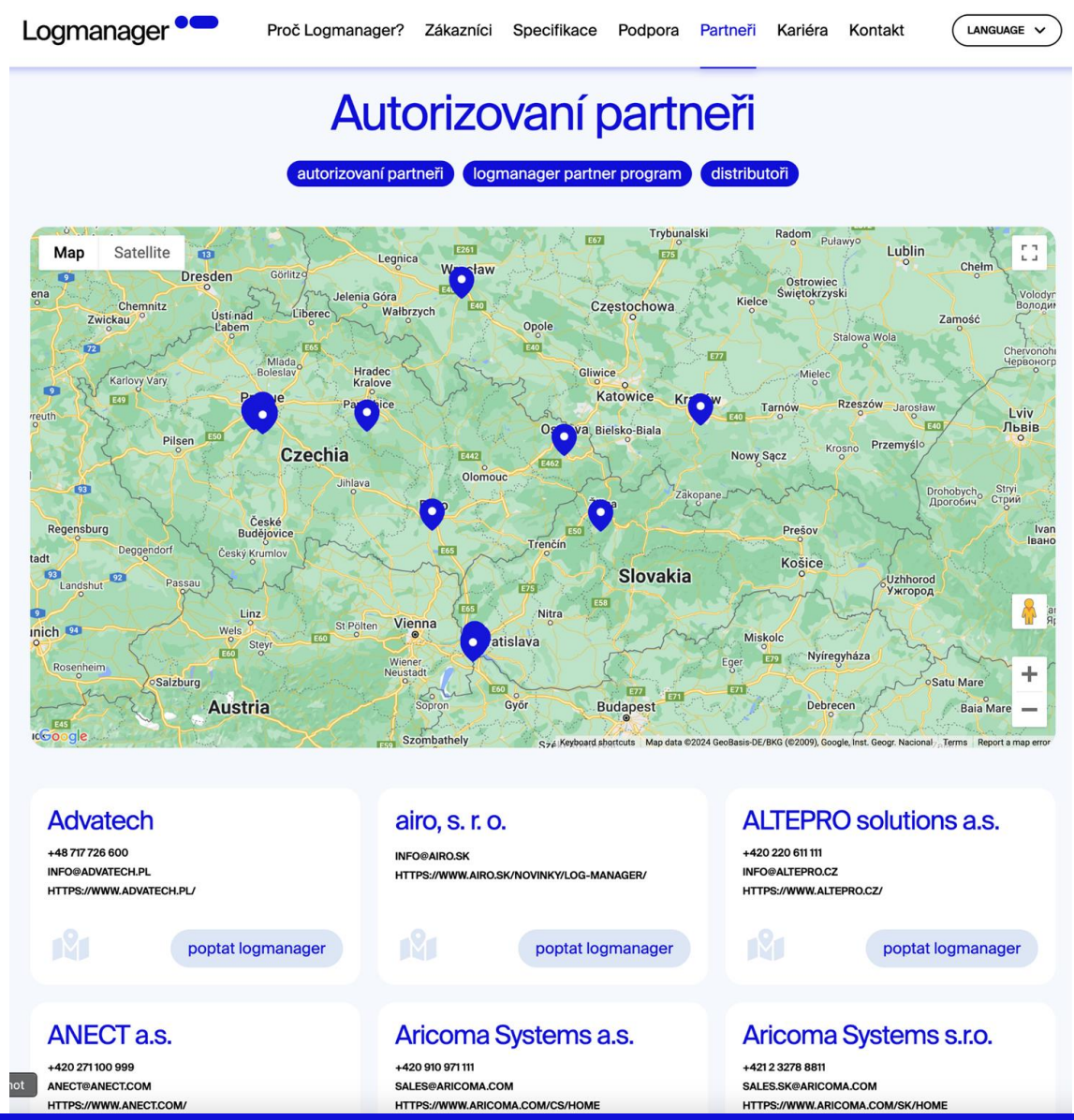
Forenzní analýza

Zlepšení bezpečnostních praxí

Dokumentace a shoda s regulacemi

Jak začít?

1. Inventura IT infrastruktury
2. Poptávka PoC u Vašeho dodavatele IT security nebo služeb
3. Sizing + rozpočet
4. Výběr a nasazení vybrané platformy, školení obsluhy
5. Nastavení zdrojů - politiky a destinace odesílání událostí
6. Implementace logiky na klíč s partnerem - custom parsery, alerty, reporty atp.
7. **Konzumace benefitů**



Děkuji za pozornost

Luboš Lunter
lubos.lunter@logmanager.com

www.logmanager.com