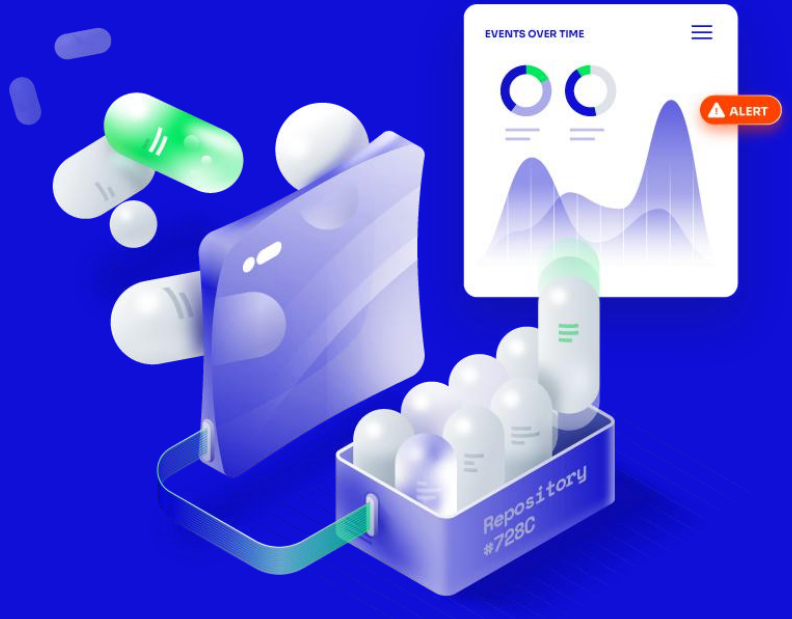
NAVIGACE SVĚTEM LOGŮ

Úloha Logmanageru v řešení IT bezpečnosti a infrastruktury



Ing. Jan Kalabus
Channel Sales Manager, Central Europe
jan.kalabus@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

Vysoká škola ekonomická v Praze VŠE

Cargo

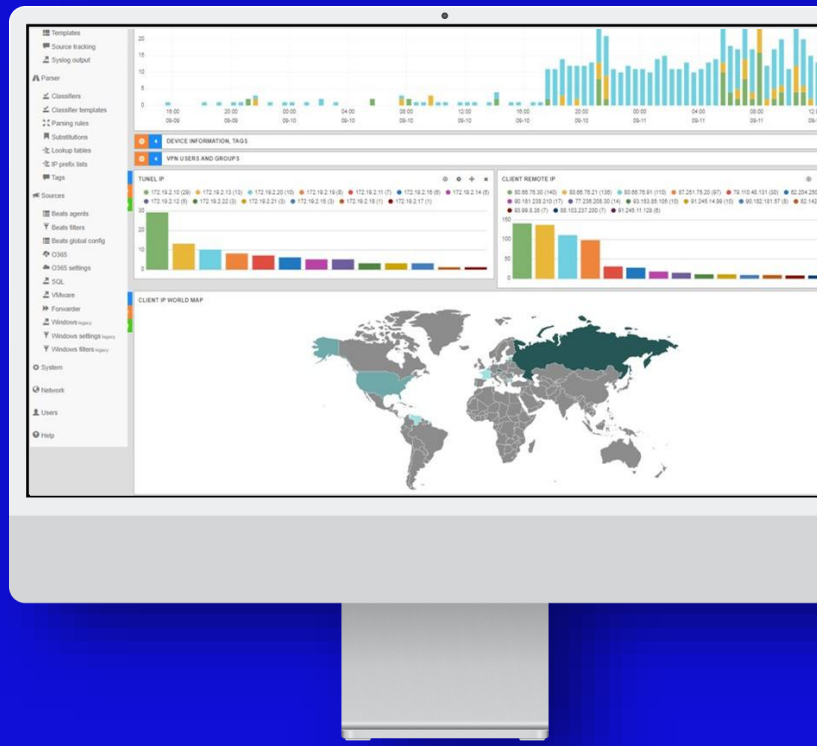
Dr.Max

O2

DPMB Dopravní podnik města Brna a.s.

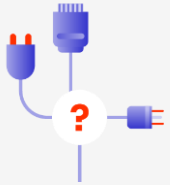
LOGMANAGER

Log management



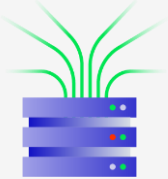
ÚLOHA LOGMANAGERU V IT BEZPEČNOSTI

Výzvy v log managementu



Chybějící standard

Nejednotné získávání různých typů událostí



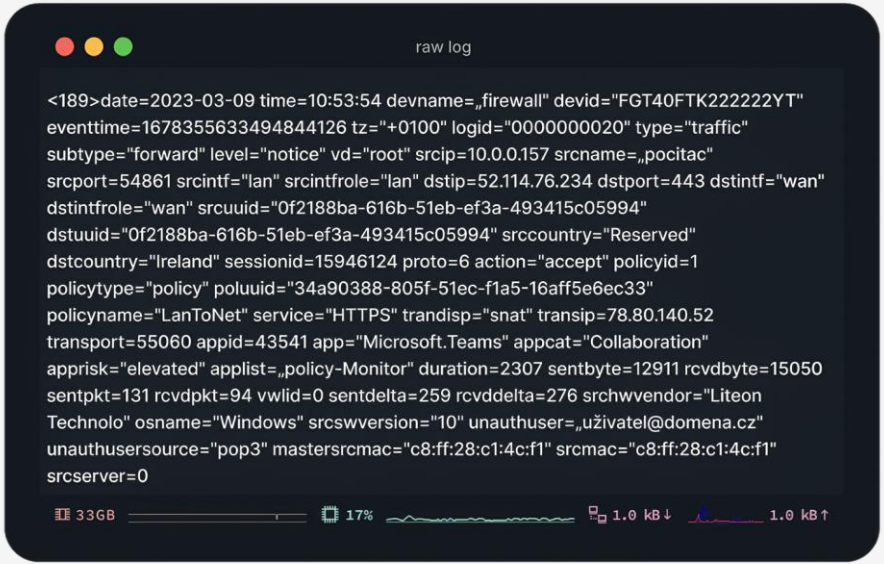
Centrální ukládání dat z různých systémů

Velký objem dat

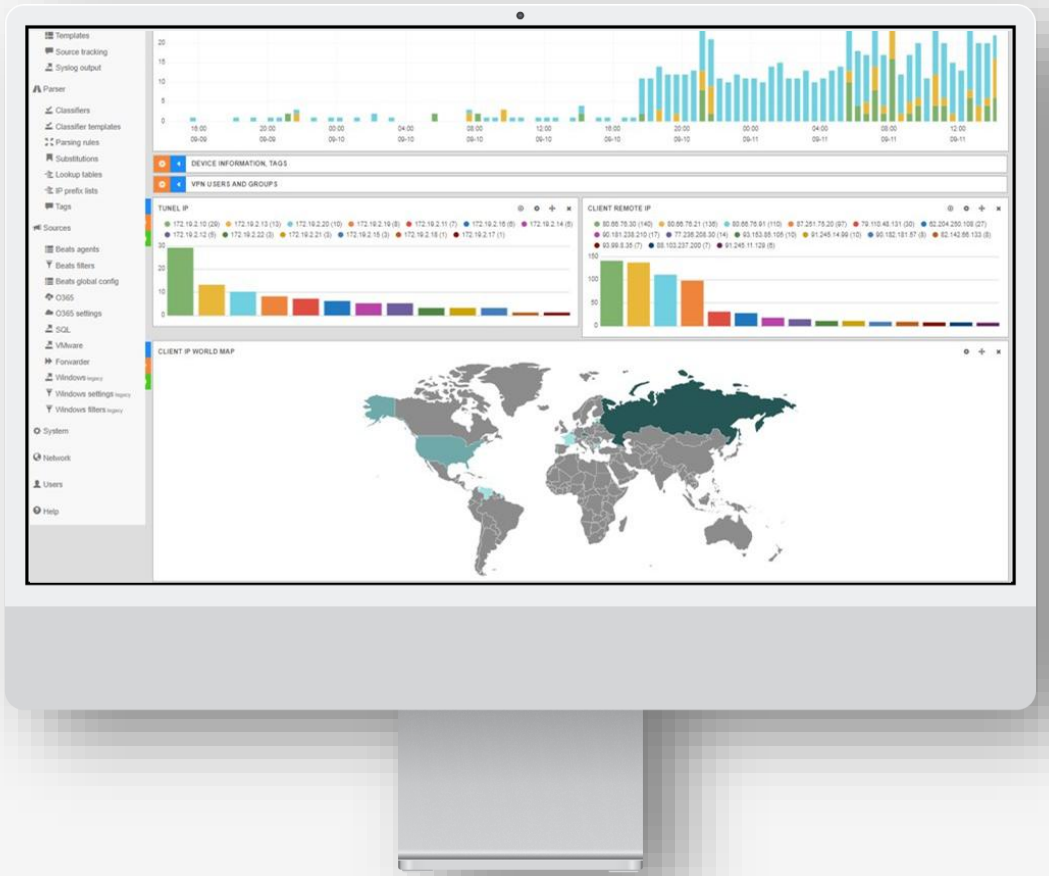
Legislativní požadavky

Velké množství šumu

Toto je log

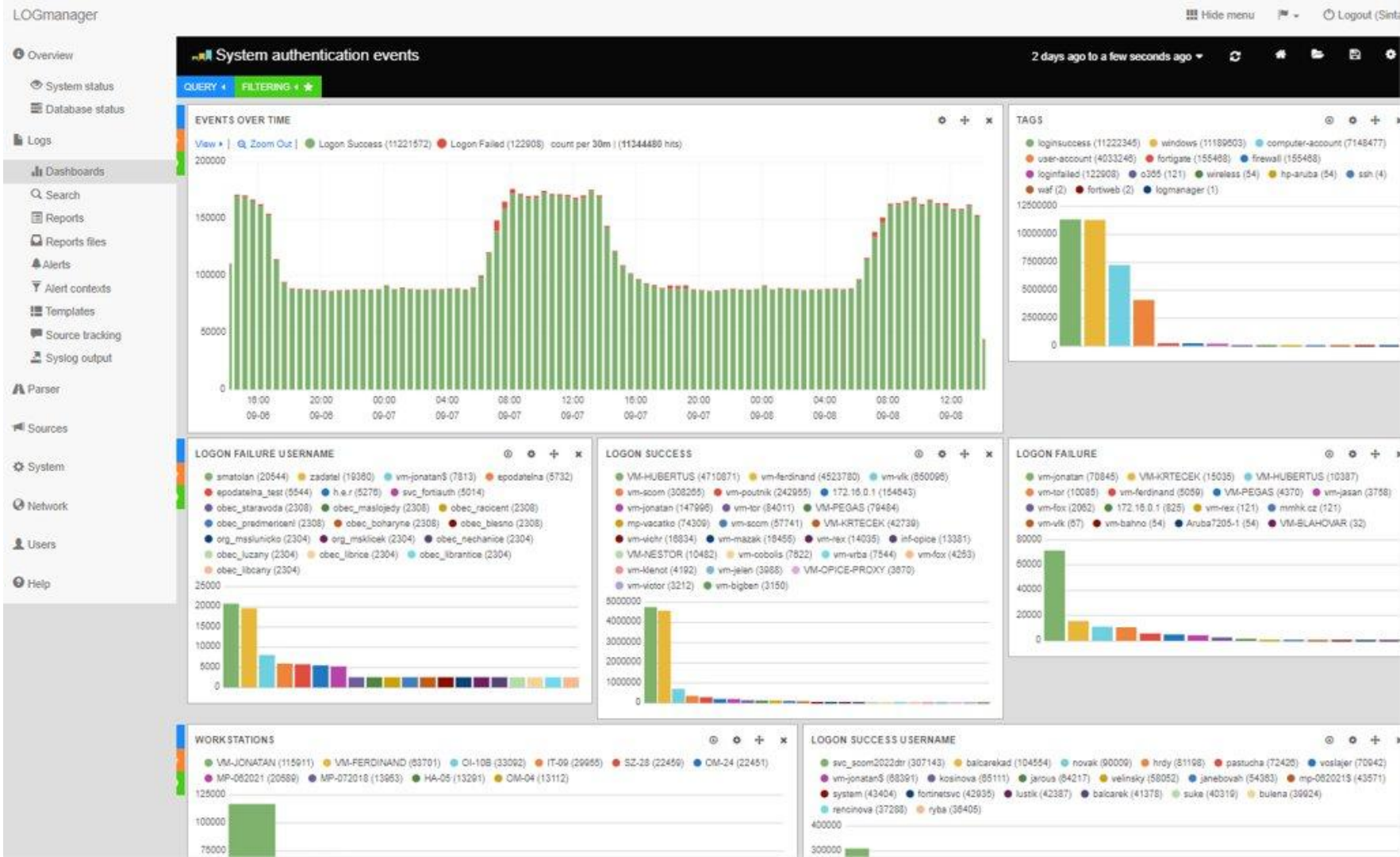

raw log
<189>date=2023-03-09 time=10:53:54 devname=„firewall" devid="FGT40FTK222222YT"
eventtime=1678355633494844126 tz="+0100" logid="0000000020" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.0.0.157 srcname=„pocitac"
srcport=54861 srcintf="lan" srcintfrole="lan" dstip=52.114.76.234 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↑

Takhle vidíme log my



LOGMANAGER

ÚLOHA LOGMANAGERU V IT BEZPEČNOSTI




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
Windows settings
Windows filters
System
Network
Users
Help
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

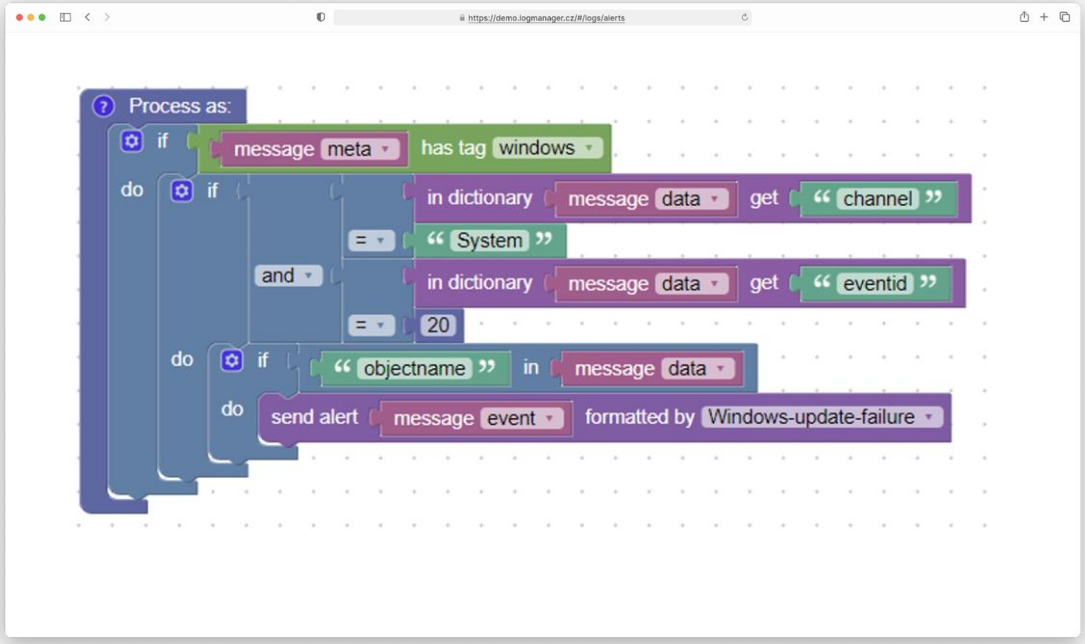
Konzistentní programování business logiky pomocí Google Blockly

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



Je Logmanager SIEM?

Srovnání SIEM vs log management

- **Implementace a údržba**
- **Zpracování dat v reálném čase pro reakce na incidenty**
- **Uživatelské rozhraní s rychlou křivkou učení**
- **Bezpečnostní notifikace a reportování**
- **Investigace incidentů**
- **IT compliance**

Potřebujete SIEM?

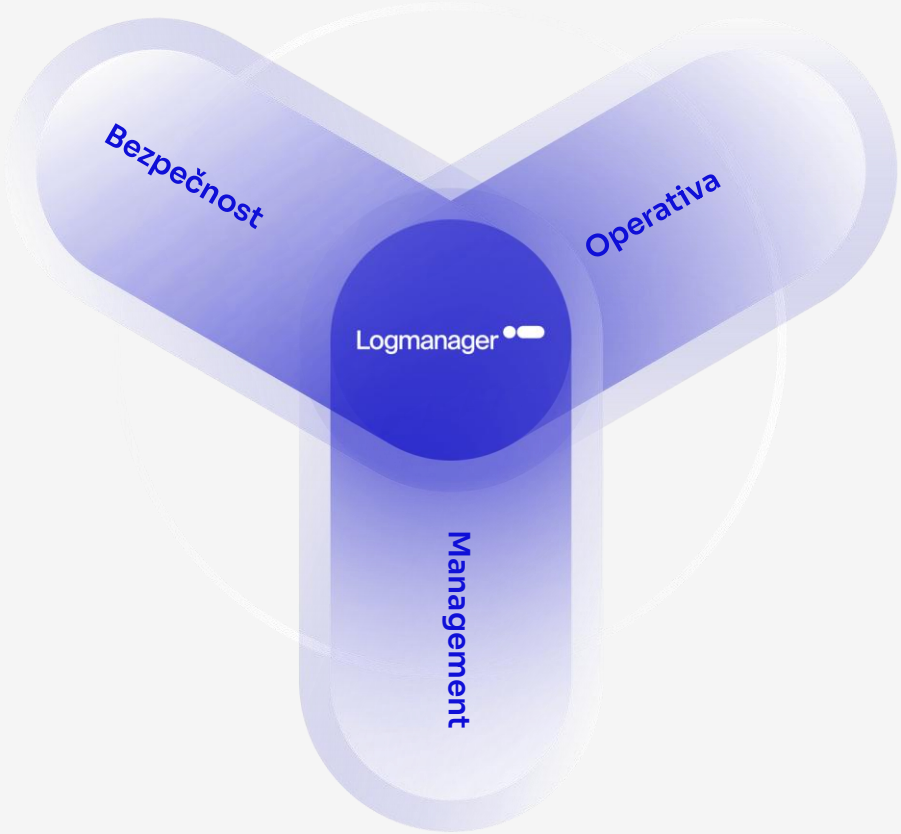
SIEM Use-cases

FIGURE 2

Top Reported Use Cases for the Security Information and Event Management

Source: IDC's Security Operations Center Survey, December 2022

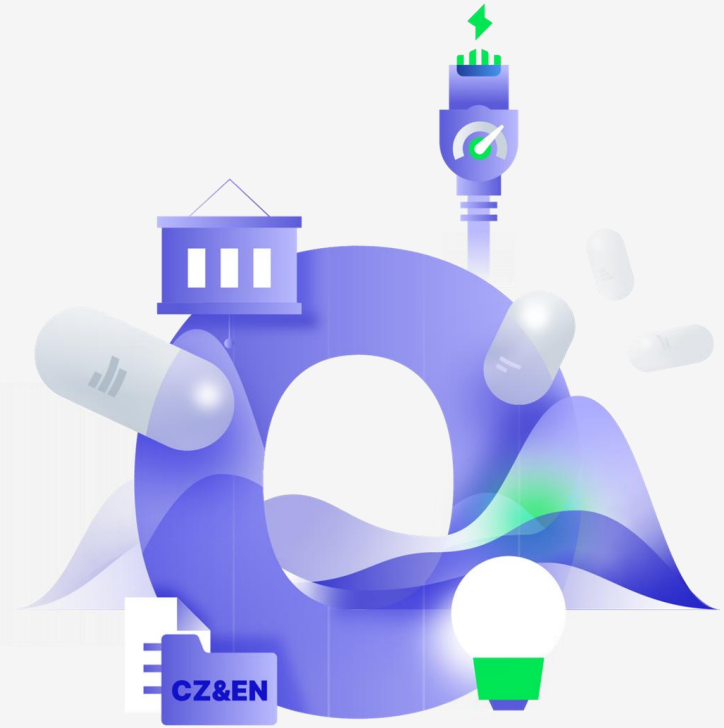
Pro koho je logmanager?



Pro koho je logmanager?

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

LOGMANAGER

ÚLOHA LOGMANAGERU V IT BEZPEČNOSTI

Role log managementu v NIS2

Přehled technických požadavků ZoKB

- Fyzická bezpečnost
- Bezpečnost komunikačních sítí
- Správa a ověřování identit
- Řízení přístupových oprávnění
- **Detekce kybernetických bezpečnostních událostí**
- **Zaznamenávání bezpečnostních a relevantních provozních událostí**
- **Vyhodnocování kybernetických bezpečnostních událostí**
- Aplikační bezpečnost
- Kryptografické algoritmy
- Zajišťování dostupnosti regulované služby
- Zabezpečení průmyslových, řídicích a obd. spec. technických aktiv

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

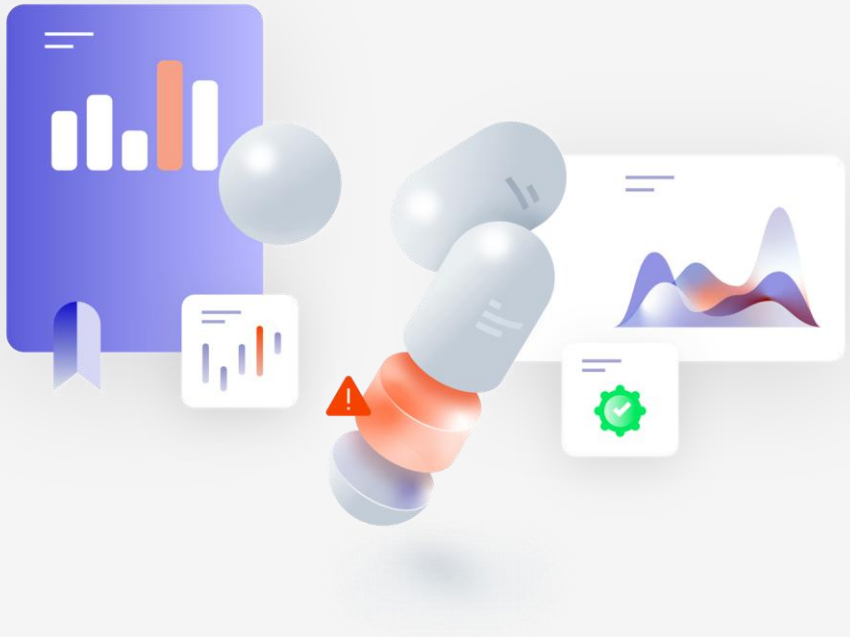
b) typ činnosti,

c) jednoznačnou identifikaci technického aktiva a identifikaci účtu a

d) úspěšnost nebo neúspěšnost činnosti.

NIS2 + 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.

→ GO

Děkuji za pozornost

Luboš Lunter

lubos.lunter@logmanager.com

www.logmanager.com