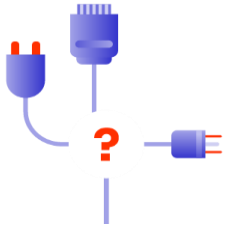
GAPP
SYSTEM

Technická opatření vyplývající z NIS2 v praxi (2)

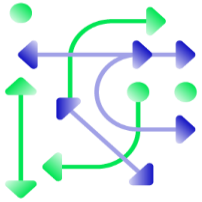
David Gottvald

Hotel Jalta, Praha
1. 4. 2025

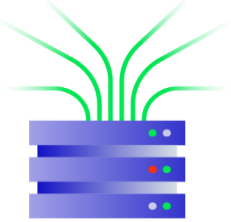
Výzvy v log managementu



Chybějící standard



Nejednotné získávání různých typů událostí



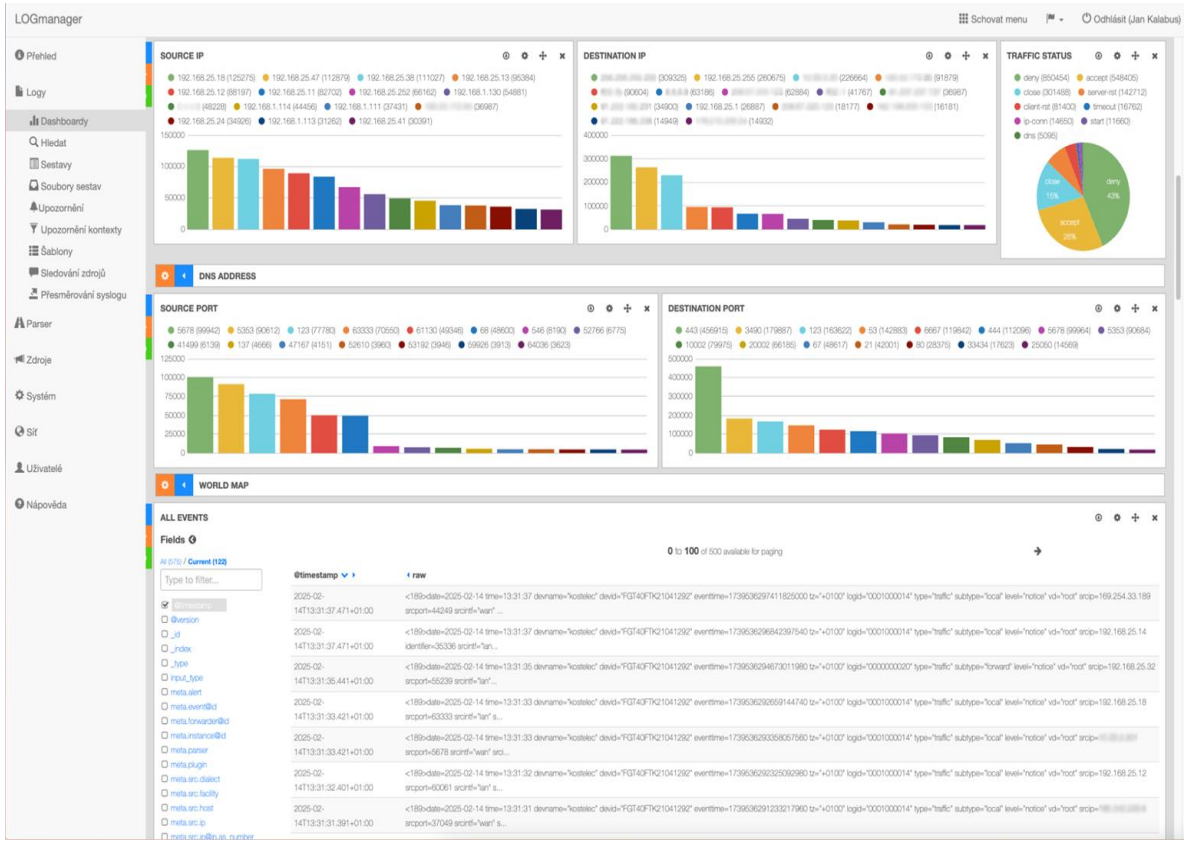
Centrální ukládání dat z různých systémů

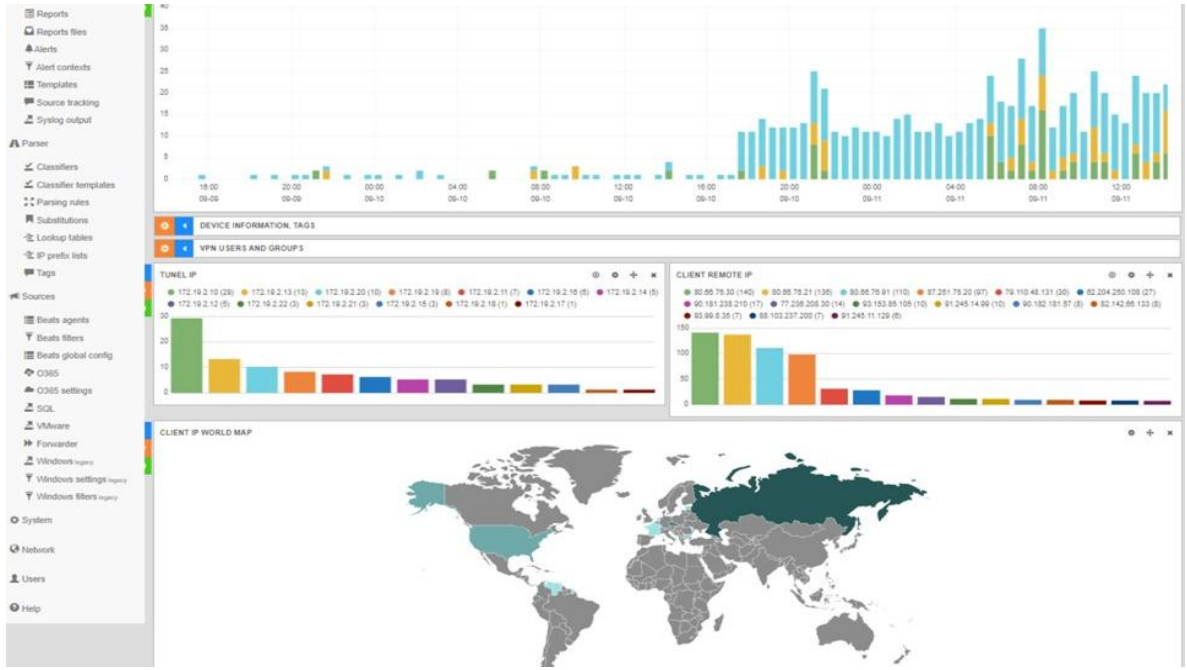
Velký objem dat

Legislativní požadavky

Velké množství šumu

LOG Manager


LOGmanager
Schovat menu
Odhlásit (Jan Kalabus)
Přehled
Logy
Dashboardy
Hledat
Sestavy
Soubory sestav
Upozornění
Upozornění kontexty
Šablony
Sledování zdrojů
Přesměrování syslogu
Parser
Zdroje
Systém
Síť
Uživatelé
Nápověda
SOURCE IP
DESTINATION IP
TRAFFIC STATUS
DNS ADDRESS
SOURCE PORT
DESTINATION PORT
WORLD MAP
ALL EVENTS
Fields
0 to 100 of 500 available for paging
@timestamp
raw


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

LOG Manager - 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

Cargo

Dr.Max

O2

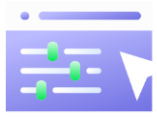
Dopravní podnik města Brna a.s.

Unikátní vlastnosti

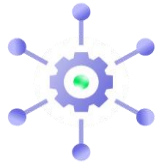
Záznamy nelze upravit ani smazat (ani superuser)

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

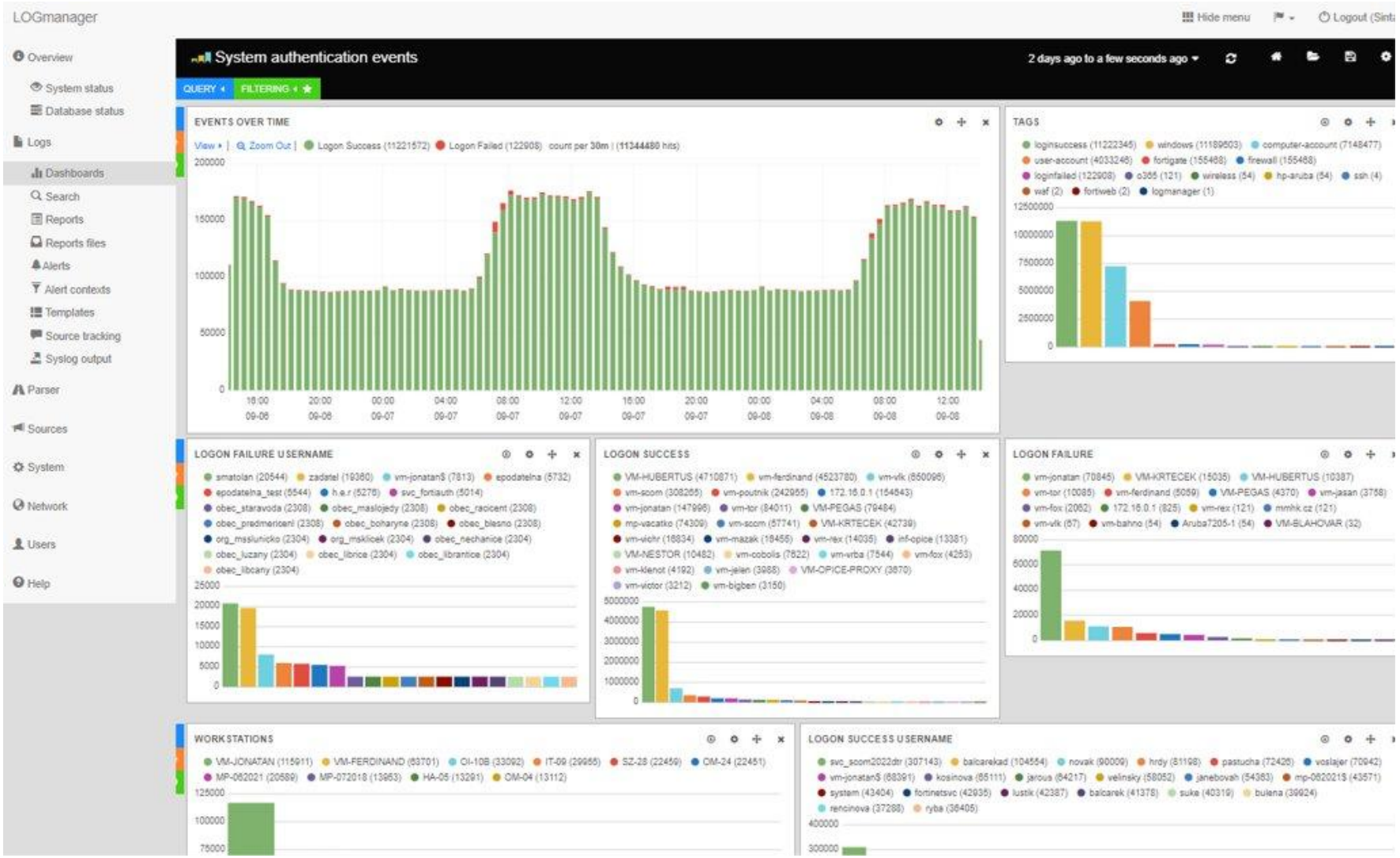
Standardní formát LOGu

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

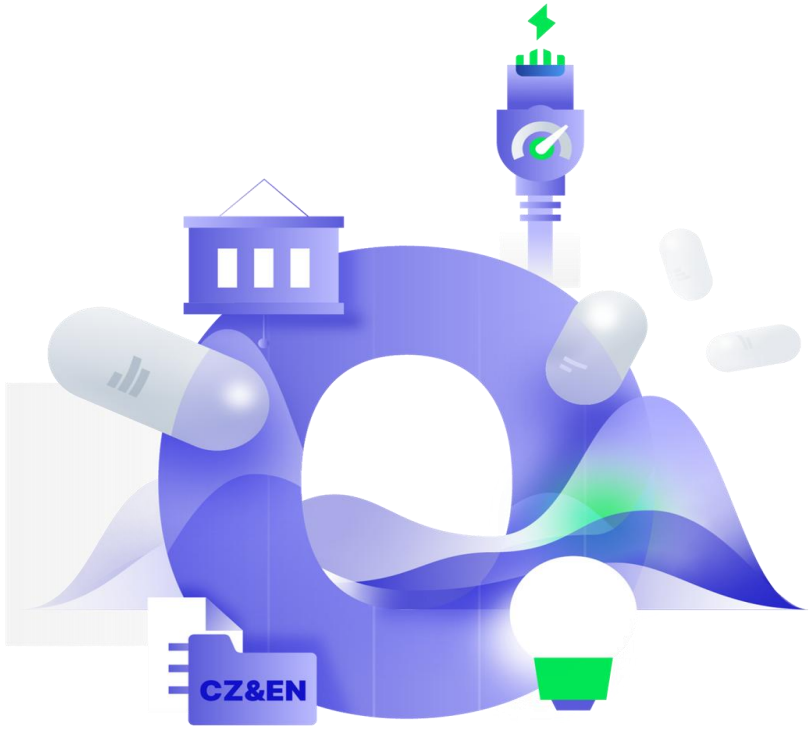
33GB 17% 1.0 kB↓ 1.0 kB↑

LOGy v LOG Manageru - Authentication



Přínosy LOG Manageru - operativa

- 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



Přínosy LOG Manageru - bezpečnost

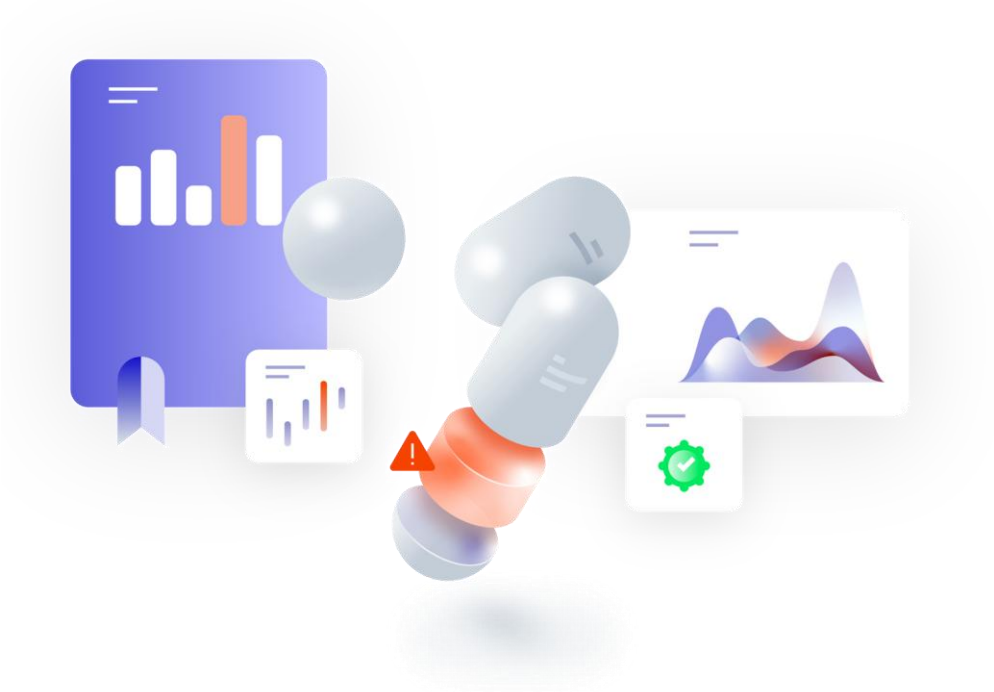
- viditelnost do bezpečnostních událostí
- granulární RBAC pro logy a správu platformy
- audit a forenzní analýza
- nesmazatelné uložení dat
- nezpochybnitelné časové razítko
- neztratí se ani jeden log, co záznam to unikátní ID
- obohacování dat
- detekce a alerting bezpečnostních událostí včetně korelace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

Přínosy LOG Manageru - 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

NIS2 a ZoKB

- Detekce a reakce na incidenty
- Forenzní analýza
- Zlepšení bezpečnostních praxí
- Dokumentace a shoda s regulacemi



Soulad s 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.

LOG Manager HW Appliance / Cluster

Model	MAX Constant EPS[1]	Data Retency in Days	DB Capacity	Memory	RAID
Logmanager-XL	10000	~440 - 800	120 - 220 TB	128GB	RAID 6
Logmanager-L	5000	~275/550	40/80 TB	128GB	RAID 6
Logmanager-M	2000	~230	12TB	64GB	RAID 5
Logmanager-S	1000	~150	4TB	64GB	RAID 0
Logmanager Forwarder	9000	N/A; acts as remote buffer	250GB	8GB	N/A

Model	MAX Constant EPS	DB Capacity	RAID
3 x XL 120TB	15800	180 TB	RAID 6
4 x XL 120TB	21000	240 TB	RAID 6
4 x XL 160TB	21000	320 TB	RAID 6
5 x XL 160TB	26000	400 TB	RAID 6

Opatření související s NIS2 a ZoKB - shrnutí

Technická opatření:

- Zálohování a Disaster Recovery lokalita (Datový trezor) včetně pravidelného testování.
- Vysoká dostupnost IT infrastruktury a redundance
- Zabezpečení IT infrastruktury
  - Perimetrový Firewall
  - Segmentace sítě (mikrosegmentace)
  - Multifaktorové přihlašování
- Monitoring IT infrastruktury
  - Stavový monitoring
  - Centrální správa a vyhodnocování LOGů
  - Řešení PIM/PAM a DLP
- Mobile Device Management

Organizační opatření opatření:

- Stanovení jasných pravidel pro práci s firemními daty.
- Pravidelné školení zaměstnanců včetně vrcholového managementu.
- Pravidelné ověřování a testování DR plánů a redundancí.
- Zpracované bezpečnostní směrnice.
- Kontrola a ověřování souladu opatření a zabezpečení s platnými normami.

Děkuji za pozornost

David Gottvald
+420 724 954 105
david.gottvald@gapp.cz