NIS2 irányelvről, annak bevezetéséről és a megfeleléshez szükséges megoldásokról

PRIANTO

LOGPOINT

Intelligible, secure digital transformation

Leading global software distributor focusing on enterprise IT solutions

NIS2

AZ ÚJ BIZTONSÁGI IRÁNYELVRŐL DIÓHÉJBAN

A NIS (Network and Information Systems) EU belső piaci működésének javítása érdekében létrehozott kiberbiztonsági irányelv. A hálózati és információs rendszerek biztonságának magas szintjét biztosítja egységesen, az EU teljes területén.

Az irányelv célja biztosítani a tagállamok számára, hogy nagyobb rugalmassággal reagálhassanak a kiberbiztonsági incidensekre, és magasabb szintű védelemmel láthassák el a kritikus infrastruktúrákat, különös tekintettel az ellátási láncok integritására. Szabályozza az érintett szervezeteknél szükséges kiberbiztonsági intézkedéseket és a jelentéstételi kötelezettségeket.

A szervezetek **minden jelentős eseményt 24 órán belül kötelesek bejelenteni** a biztonsági eseményekre reagáló csoportoknak (CSIRT) vagy a nemzeti hatóságnak.

Egy esemény akkor tekintendő jelentősnek, ha:

- súlyos működési zavart okozott vagy képes okozni a szolgáltatásokban
- pénzügyi veszteséget okozott az érintett szervezetnek
- az esemény jelentős vagyoni vagy nem vagyoni kárt okoz (képes okozni) természetes vagy jogi személyek számára

NIS2

BEVEZETENDŐ KIBERBIZTONSÁGI INTÉZKEDÉSEK

A hatály alá tartozó szervezeteknek további kiberbiztonsági kockázattal arányos biztonsági intézkedéseket kell bevezetniük amely kiterjed:

- a kockázatelemzési és információbiztonsági szabályzatokra
- üzletmenet folytonosságra
- katasztrófa utáni helyreállításra
- ellátási láncok biztonságának biztosítására
- kiberhigiéniai gyakorlatokra és kiberbiztonsági képzésekre
- titkosításra, kriptográfiai megoldások használatára vonatkozó szabályzatok és eljárások alkalmazására
- HR biztonságra
- hitelesítési megoldásokra
- biztonságos hang-, video- és szöveges kommunikációra
- illetve biztonságos vészhelyzeti kommunikációs rendszerek használatára

LOGPOINT

SIEM+SOAR: KIBERBIZTONSÁG EGYSZERŰSÍTVE

KOMPLEX BIZTONSÁGI PLATFORM - NIS2 SZEMÜVEGEN KERESZTÜL

2023 OKTÓBER

NIS2 | Szervezeti követelmények

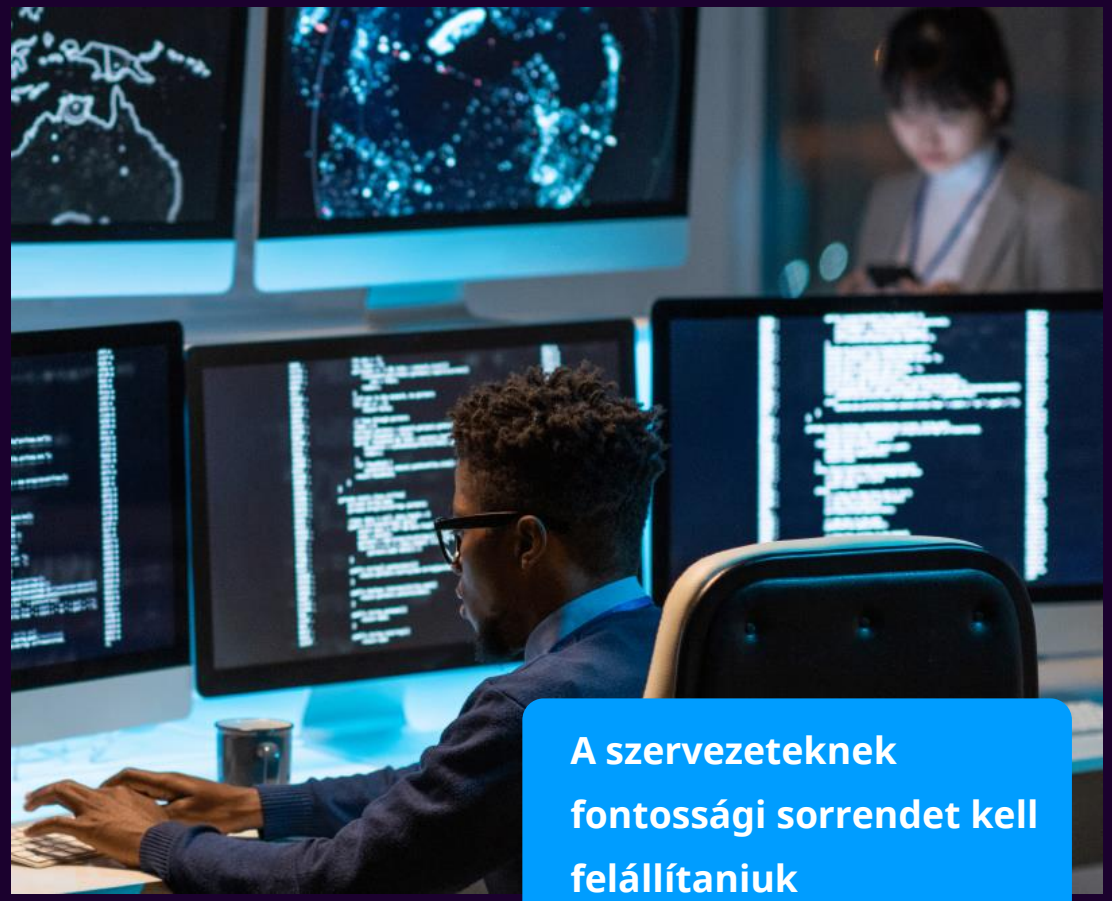
NIS2 | Szükséges Intézkedések

- Kockázatértékelések és biztonsági szabályzatok az információs rendszerek számára
- A biztonsági intézkedések hatékonyságának értékelésére szolgáló irányelvek és eljárások
- A kriptográfia és a titkosítás használatára vonatkozó eljárások
- Biztonsági események kezelése
- Biztonságos rendszerbeszerzési szabályzatok a sebezhetőségek kezelésére és jelentésére
- Kiberbiztonsági képzés
- Az érzékeny vagy fontos adatokhoz való hozzáférés figyelése és érvényesítése
- Üzleti folytonosság (katasztrófa utáni helyreállítási tervek)
- Többtényezős hitelesítés használata
- Az ellátási láncok körüli biztonság

KIHÍVÁSOK

Az informatikai vezetők nehezen tudják eldönteni, hol kell összpontosítaniuk a technológiákra, szolgáltatásokra és megoldásokra

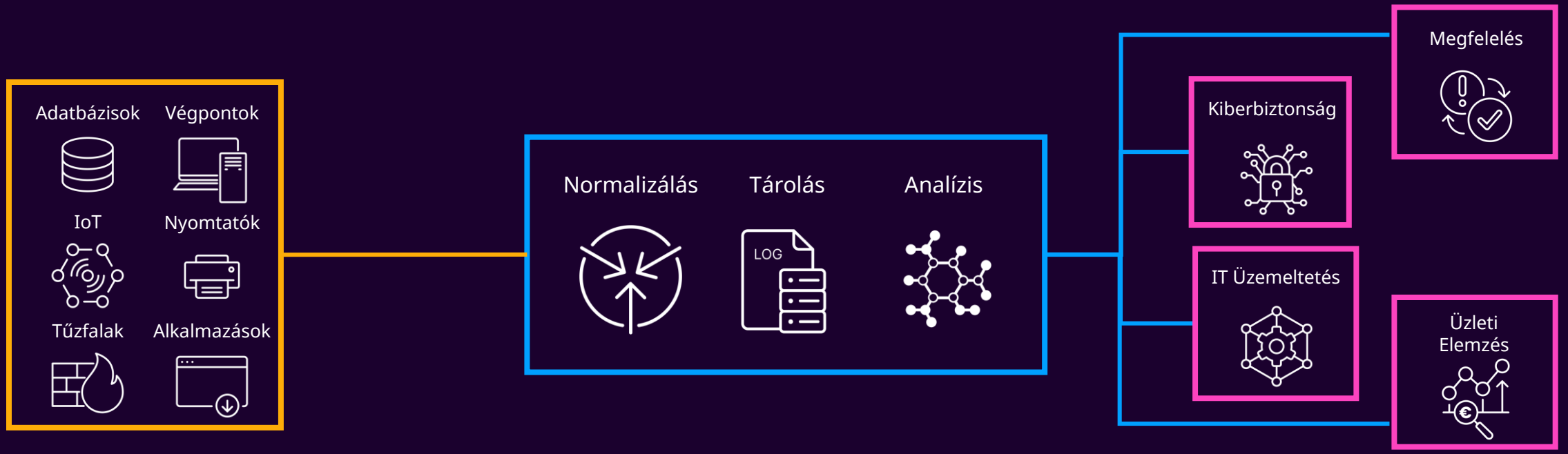
- Bővülő támadási felület a digitalizációnak köszönhetően
- Az adatok és az infrastruktúra felhőbe költözése
- Kiberbiztonsági szakemberek felvétele, képzése és megtartása
- Túl sok olyan eszköz, amely nem integrálható
- Fokozott nyomás a kiberbiztonság megfelelővé tételére



A szervezeteknek fontossági sorrendet kell felállítaniuk

- Adatszivárgás
- Ransomware
- Fenyegetés vadászat
- Az incidensre adott válasz

SIEM RÖVIDEN



A vállalati adatmennyiség exponenciálisan növekszik

A nyers formában lévő adatokat az IT-szakemberek többsége nem tudja hatékonyan feldolgozni

A SIEM szabványosítások és használati esetek révén a nyers adatokat gyakorlatias betekintésekké alakítja át

Az információ ezután három fő területen használható fel:
Biztonság: Optimálisan biztonságos a cég?
Megfelelőség: Hogyan lehet igazolni a megfelelőséget?
Műveletek: Maximális a hatékonyság?

NAGYOBB ÁTLÁTHATÓSÁG | TÖBB ESZKÖZ | KÁOSZ (?)

	Védelem	Észlelés	Válaszadás
Felhasználók	Security awareness training, MFA	Insider threat, UEBA, SIEM	SOAR
Eszközök	AV, EPP, FIM, HIPS, Allowlisting, Patch management, Email security	EPP, UEBA, SIEM, Email security	EP response (EDR, MDR), EP forensics, SOAR
Hálózat	FW, IPS, UTM, Microsegmentation, ESG, SWG, SASE, ZTNA, DNS, VPN	DDoS detection, Net traffic analysis, UEBA, SIEM, DNS	DDoS response, SOAR, NW forensics, SASE
Alkalmazások	RASP, WAF, ZT app access, CASB, SSPM	Source code compromise, App IDS, SIEM, CASB, SSPM	SSPM, SOAR
Adatok	Encryption, Tokenization, DLP, DRM, DBAM, Email security	Dark web scanning, Data behavior analytics, SIEM	DRM, SOAR, breach response

A SIKERES ÉSZLELÉS TITKA NEM A SOK ESZKÖZ…

Integráció

Bővített képességek

Eszközpark egyszerűsítése

Méretgazdaságosság növelése

Fenyegetések észlelése és keresése

A biztonsági pozíció javítása

Biztonsági elemzés

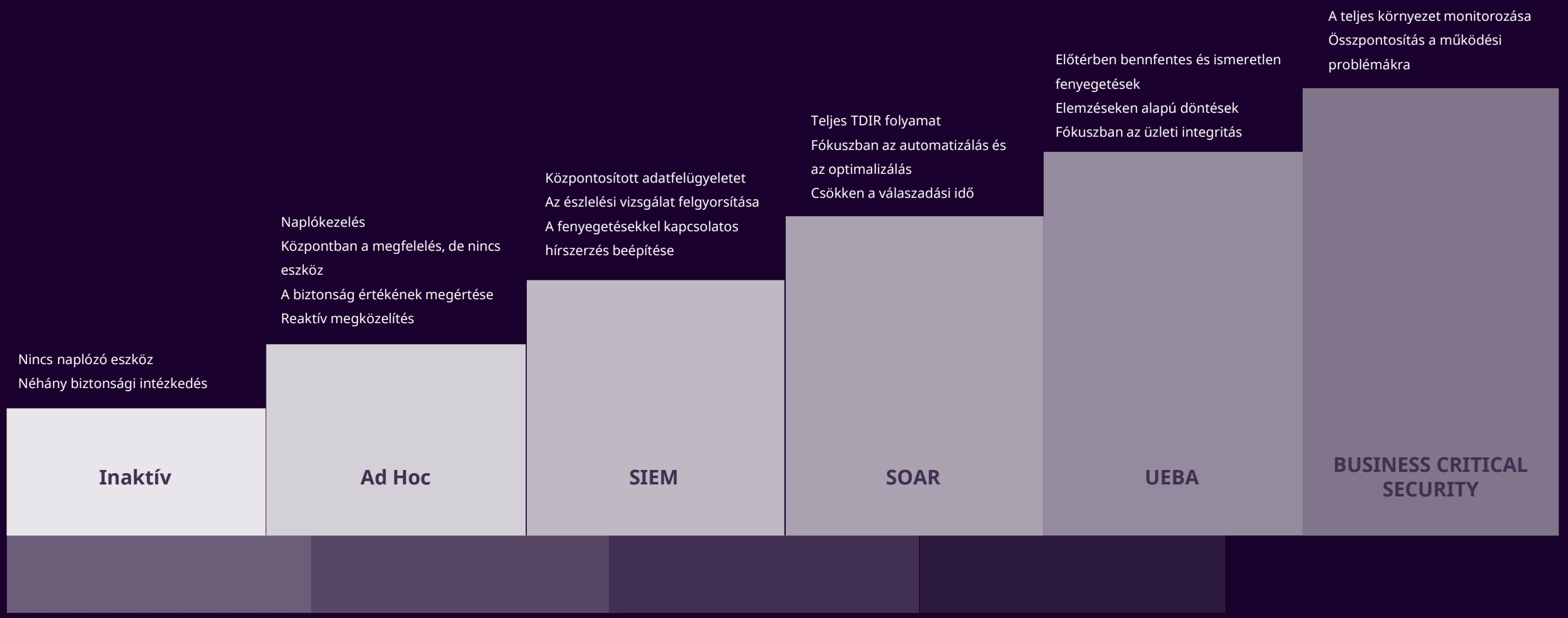
Egyszerű tartalom-szolgáltatás

Validáció

Ismételhetőség, következetesség

A NAGY KIBERÉRETTSÉGI UTAZÁS

Akár el kell kezdenie, akár optimalizálnia kell a folyamatokat



A megoldás:

CONVERGEDSIEM

Integrált biztonsági műveleti platform

A MEGOLDÁS: CONVERGED SIEM

Integrált biztonsági műveleti platform

- **Teljes körű biztonsági platform:**
  Felgyorsítja a fenyegetés észlelését, kivizsgálását és reagálást
- **Jó átláthatóság és helyzetfelismerés:**
  A biztonsági problémák észlelése és javítása az adatvesztés előtt
- **Időigényes feladatok automatizálása:**
  Az elemzőt konzisztens és optimális folyamatokhoz irányítja
- **Könnyű jelentéskészítés és megfelelőség:**
  GDPR, NIS2, PCI DSS, stb.
- **Szigorú biztonság- és minőségbiztosítás:**
  EAL 3+ certification
- **Gyors és rugalmas telepítés**
  On-prem, SaaS, és private cloud

SIEM	SOAR	AgentX	UEBA	BCS	Integrációk
A naplók és a telemetria felvétele	Összehangolt automatizáció	Végpontfigyelés és válaszadás	Viselkedési anomáliák és kockázatpontozás	Kritikus alkalmazások biztonsági elemzése	Fenyegetés-észlelés kiterjesztése

Logpoint Converged SIEM Platform

BIZTONSÁGI MENEDZSMENT KIHÍVÁSAINAK MEGOLDÁSA

ADATGYŰJTÉS	ÉSZLELÉS	VIZSGÁLAT	VÁLASZADÁS
Log-gyűjtés	Converged SIEM	Riasztás	Bizonyítékok elemzése	Idővonalak felállítása	Válaszadás
PROBLÉMA	Nehéz lefedni a teljes támadási felületet	Ismeretlen fenyegetéseket nem lehet észlelni	Nehéz az adatok összeegyeztetése	Manuális elemzés	Kézi, nem teljes válasz
MEGOLDÁS	Integráció bármilyen adatforrással	Viselkedés analízis (UEBA)	Adat normalizálás	Automatizált elemzés	Forgatókönyvek válaszadáshoz (SOAR)

LOGPOINT ARCHITEKTÚRA ÉS ÖKOSZISZTÉMA

Log források

- Adatbázisok
- Tűzfalak
- Alkalmazások
- Végpontok
- Nyomtatók
- IoT
- Egyéni források

1000+ adatforrás

Core product – Converged SIEM + SOAR + EDR képességek

Collector

- Gyűjtés
- Normalizálás
- Gazdagítás
- Threat intel

Tárolás

Több szintű Repositorik

Analízis

- Keresés
- Korreláció
- Detektálás
- Vizsgálat
- Válaszadás

75+ playbook (forgatókönyv)

800+ integráció

Rugalmas telepítés

Director

Multi Tenancy

Business-critical security

ERP Security

UEBA

Viselkedéselemzés

Szolgáltatások

Operations Monitoring

Playbook tervezési szolgáltatás

Global Support

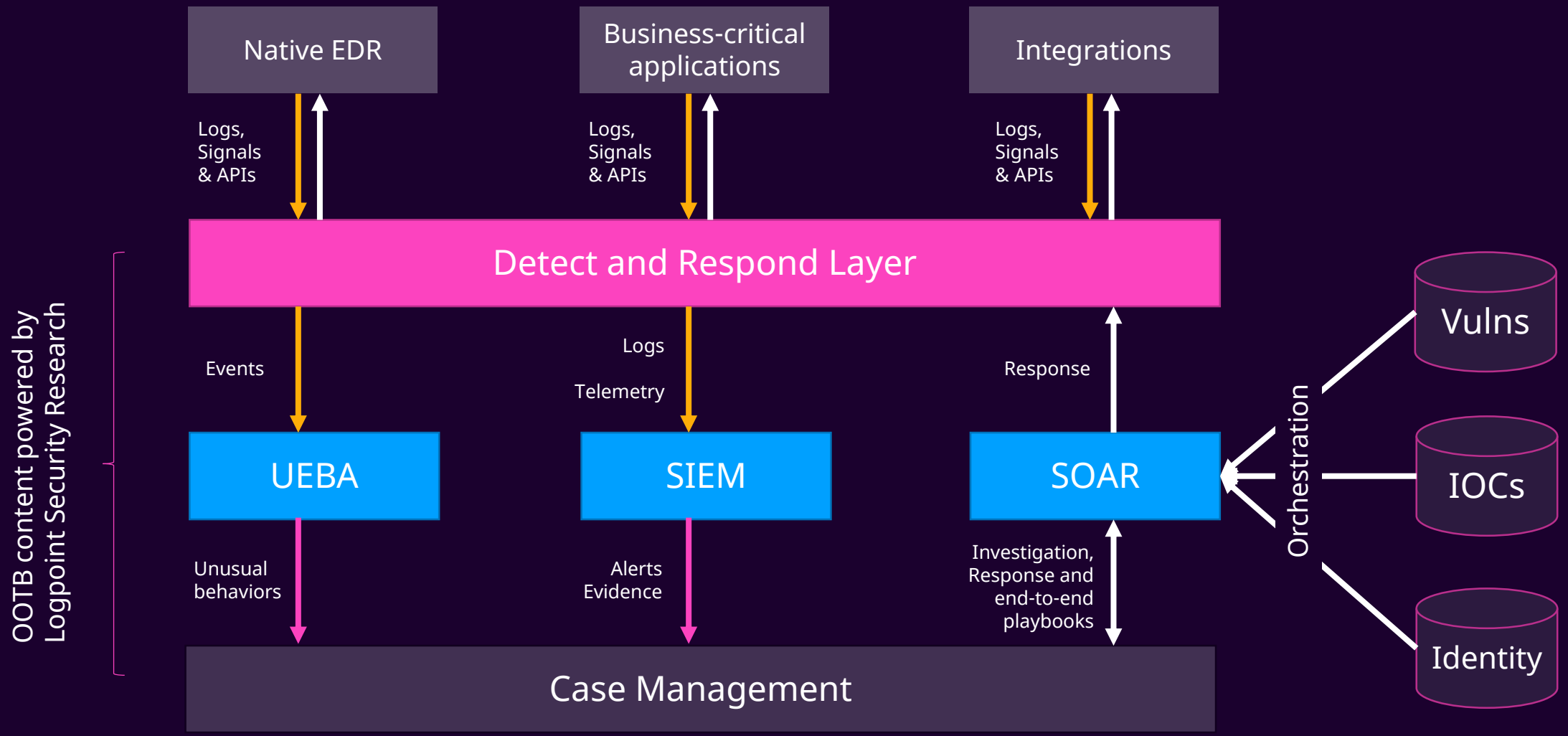
Use case-ek

- Naplókezelés
- Megfelelőségi menedzsment
- Bennfentes fenyegetés észlelése
- Műveletek figyelése
- Riasztási osztályozás
- Adathalászat kivizsgálása és válaszadás
- Ransomware enyhítése

Security content

- Logpoint Marketplace
- Logpoint Community
- Logpoint Doc Portal

LOGPOINT *KONVERGÁLT* SIEM PLATFORM



FELHASZNÁLÓK ÉS IDENTITÁSOK

Anomália/viselkedés észlelése

- Bennfentes fenyegetés észlelése
- Rendellenes kezdeti hozzáférés
- Belső felderítés
- Feltört fiók

Megfelelőség / TDIR

- Szabályozási ellenőrzés és válaszadás
- Szabályzatfigyelés: SoD és engedélyezési riasztások
- Fenyegetés vadászat

ÜZLETMENET-KRITIKUS ALKALMAZÁSOK

Felhő / SaaS

- Adathalászat és e-mail TDIR
- Ellenőrzési szabályok módosítása
- Változások az engedélyekben
- Adatvesztés

ERP

- Csalás és kockázatfigyelés
- Szabályzatfigyelés: SoD és üzleti integritás
- Szellemi tulajdon ellopása
- Csapatokon átívelő átláthatóság

VÉGPONTOK

Észlelés

- Automatizált nyomozás
- Naplógyűjtés és bizonyítékgyűjtés
- Helyzetfelismerés: osquery
- Az eszközök biztonsági pozíciójának mérése

Válaszadás

- Összehangolt válasz
- Ransomware-csökkentés
- Automatizált nyomozás és osztályozás
- Hatások visszaszorítása

INFRASTRUKTÚRA

Hálózat

- Hálózati hozzáférés: Távoli hozzáférés és oldalirányú mozgás
- Rendellenes forgalom
- A hálózati forgalom korlátozása, elkülönítése és leállítása
- Kontextus tudatosság

Szerverek

- Behatolási jelek (IoC)
- Sebezhetőség kezelése
- Az erőforrásokhoz való hozzáférés figyelése: eszköz és felhasználó
- Automatizált válaszadás

NIS2 Szükséges Intézkedések

1. **Kockázatértékelések és biztonsági szabályzatok az információs rendszerek számára**
   - CIS Controls Version 8, MITRE ATT&CK
2. **A biztonsági intézkedések hatékonyságának értékelésére szolgáló irányelvek és eljárások**
   - E2E Biztonsági megfigyelés és jelentéskészítés
3. **A kriptográfia és a titkosítás használatára vonatkozó eljárások**
   - Eljárások és beállítások figyelése
4. **Biztonsági események kezelése**
   - Automatikus validálás és jelentéskészítés (24h / 72h)
5. **Biztonságos rendszerbeszerzési szabályzatok a sebezhetőségek kezelésére és jelentésére**
   - Sebezhetőségi vizsgálat és jelentés

NIS2 Szükséges Intézkedések

6. **Kiberbiztonsági képzés**
    - A viselkedés megfigyelése és jelentéskészítés
7. **Az érzékeny vagy fontos adatokhoz való hozzáférés figyelése és érvényesítése**
    - PII monitoring
8. **Üzleti folytonosság (katasztrófa utáni helyreállítási tervek)**
    - Bizonsági mentések monitorozása
9. **Multi-faktoros hitelesítés használata**
    - MFA használat monitoring, audit és kényszerítés
10. **Az ellátási láncok körüli biztonság**
    - SAP Budget Control System és ellátási lánc monitoring, audit

PRIANTO

Prianto Hungary / Prianto GmbH
Róbert Károly Krt. 47/a.
1134 Budapest, Hungary

Tel:+36 1 769 6371
Mob: +36 70 418 7177
Email: contact@prianto.hu
Web: www.prianto.hu

LinkedIn: https://www.linkedin.com/company/prianto-hungary-cee
Facebook: https://www.facebook.com/priantohungary

Sales

- Mario Kosztik (mario.kosztik@prianto.com)
- Mariann Blaskó (mariann.blako@prianto.com)
- Eszter Baté (eszter.bate@prianto.com)

Country Manager

- Olivér Urzica (oliver.urzica@prianto.com)

Marketing

- Anna Birinyi (anna.birinyi@prianto.com)

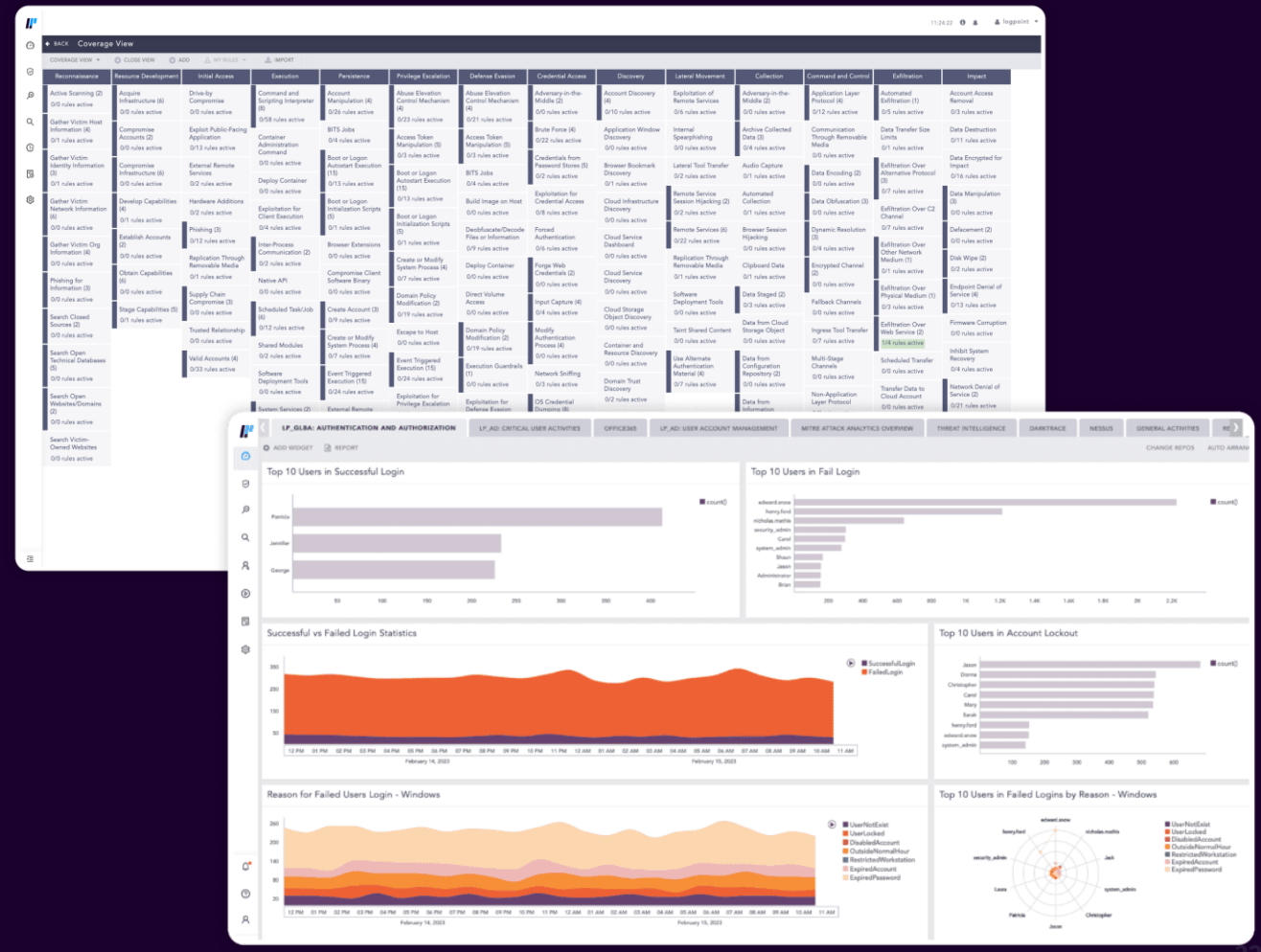
Presales

- Krisztián Donner (krisztian.donner@prianto.com)

LOG COLLECTION

Converged SIEM allows you to efficiently manage storage and lifecycle management

- Collect:
  Log and telemetry from devices, applications or endpoints in your infrastructure
- Normalize:
  Single taxonomy
- Enrich:
  Users, assets, threats, vulnerabilities, compliance
- Add threat intelligence:
  MITRE ATT&CK mapping



LOG STORAGE

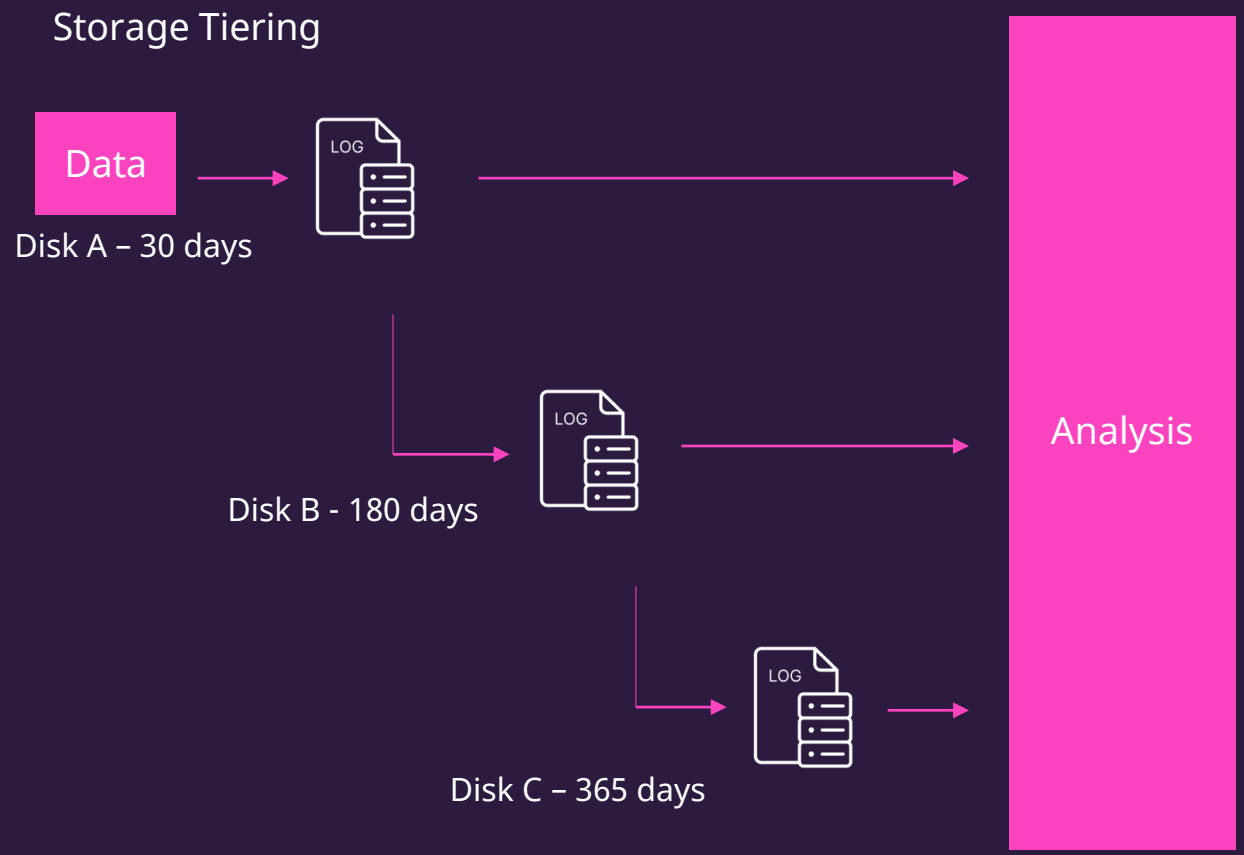
Flexible option, retention decided by the customers

Store different logs for different amount of times and automatic storage tiers management.

Use of different repositories to:

- Keep the same type of data grouped together for faster analysis
- RBAC-based data access control
- Data Privacy Mode
- Secure storage of sensitive data
- Possibility of hardware-agnostic data prioritization

SaaS: includes 30 days of hot storage and 60 days of warm storage

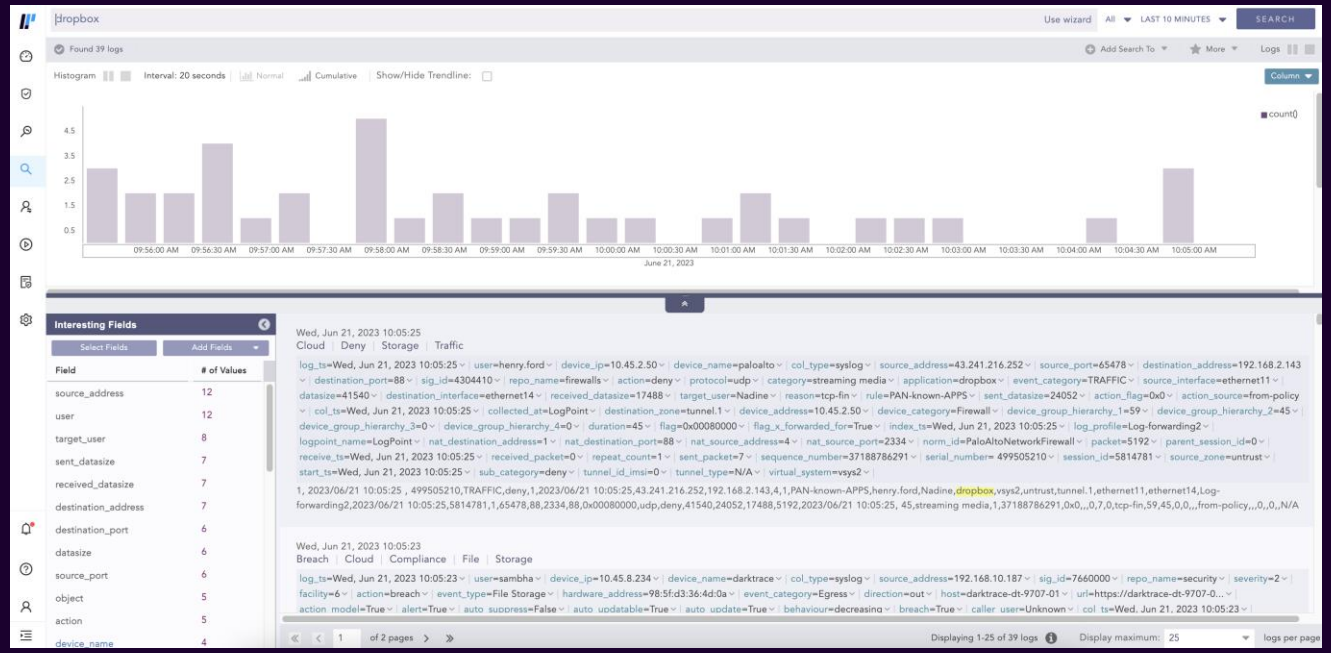


NORMALIZATION (COMMON TAXONOMY)

Wed, Jun 21, 2023 10:05:25
Cloud | Deny | Storage | Traffic

log_ts=Wed, Jun 21, 2023 10:05:25 | user=henry.ford | device_ip=10.45.2.50 | device_name=paloalto | col_type=syslog | source_address=43.241.216.252 | source_port=65478 | destination_address=192.168.2.143 | destination_port=88 | sig_id=4304410 | repo_name=firewalls | action=deny | protocol=udp | category=streaming media | application=dropbox | event_category=TRAFFIC | source_interface=ethernet11 | datasize=41540 | destination_interface=ethernet14 | received_datasize=17488 | target_user=Nadine | reason=tcp-fin | rule=PAN-known-APPS | sent_datasize=24052 | action_flag=0x0 | action_source=from-policy | col_ts=Wed, Jun 21, 2023 10:05:25 | collected_at=LogPoint | destination_zone=tunnel.1 | device_address=10.45.2.50 | device_category=Firewall | device_group_hierarchy_1=59 | device_group_hierarchy_2=45 | device_group_hierarchy_3=0 | device_group_hierarchy_4=0 | duration=45 | flag=0x00080000 | flag_x_forwarded_for=True | index_ts=Wed, Jun 21, 2023 10:05:25 | log_profile=Log-forwarding2 | logpoint_name=LogPoint | nat_destination_address=1 | nat_destination_port=88 | nat_source_address=4 | nat_source_port=2334 | norm_id=PaloAltoNetworkFirewall | packet=5192 | parent_session_id=0 | receive_ts=Wed, Jun 21, 2023 10:05:25 | received_packet=0 | repeat_count=1 | sent_packet=7 | sequence_number=37188786291 | serial_number= 499505210 | session_id=5814781 | source_zone=untrust | start_ts=Wed, Jun 21, 2023 10:05:25 | sub_category=deny | tunnel_id_imsi=0 | tunnel_type=N/A | virtual_system=vsys2 |

1, 2023/06/21 10:05:25 , 499505210,TRAFFIC,deny,1,2023/06/21 10:05:25,43.241.216.252,192.168.2.143,4,1,PAN-known-APPS,henry.ford,Nadine,dropbox,vsys2,untrust,tunnel.1,ethernet11,ethernet14,Log-forwarding2,2023/06/21 10:05:25,5814781,1,65478,88,2334,88,0x00080000,udp,deny,41540,24052,17488,5192,2023/06/21 10:05:25, 45,streaming media,1,37188786291,0x0,,,0,7,0,tcp-fin,59,45,0,0,,,from-policy,,,0,,0,,N/A



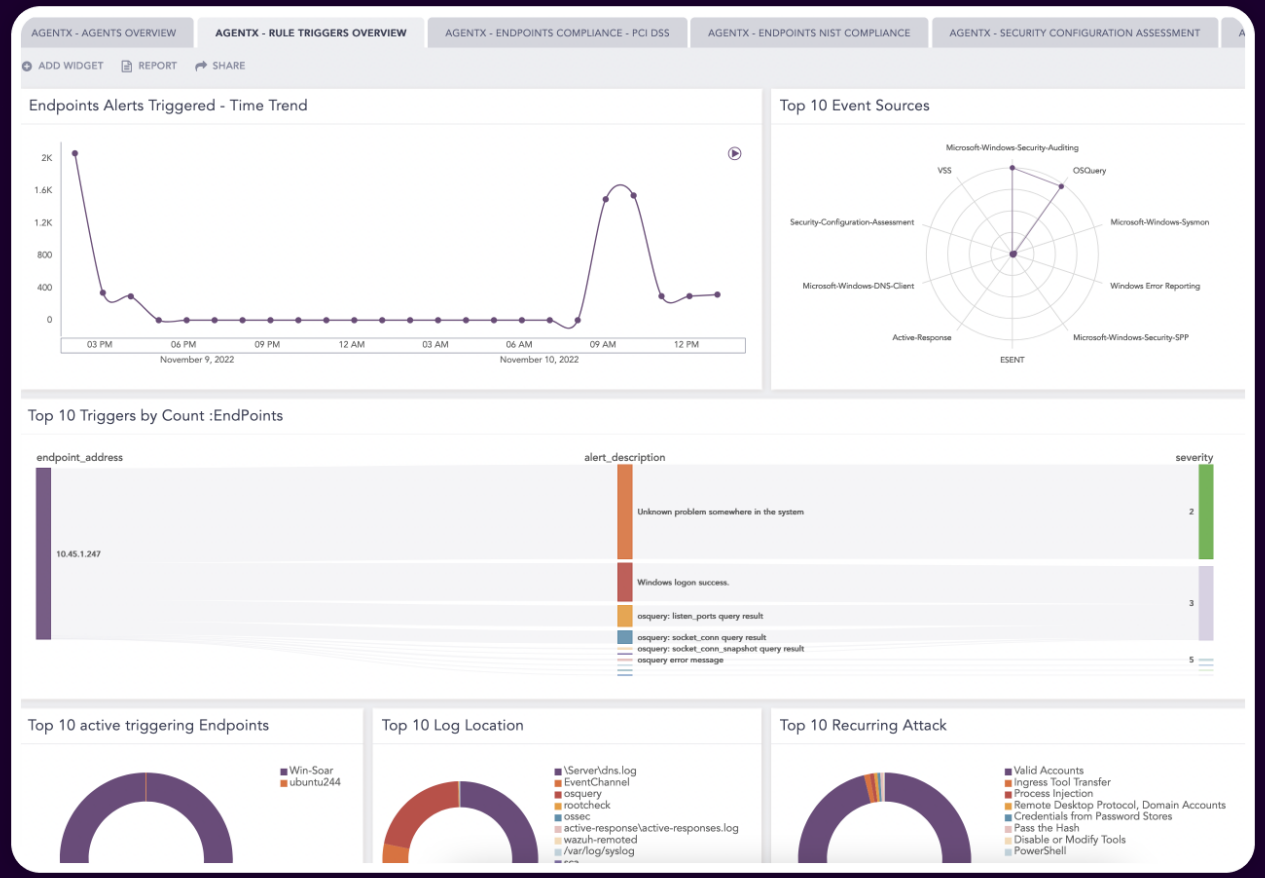
LOG ANALYSIS

- Easy and fast analysis:
  Single taxonomy and MITRE ATT&CK framework

- Correlate data from all applications within your infrastructure

- Fuse weak signals into meaningful alerts by automatically adding:
  - Operational context
  - Threat intelligence

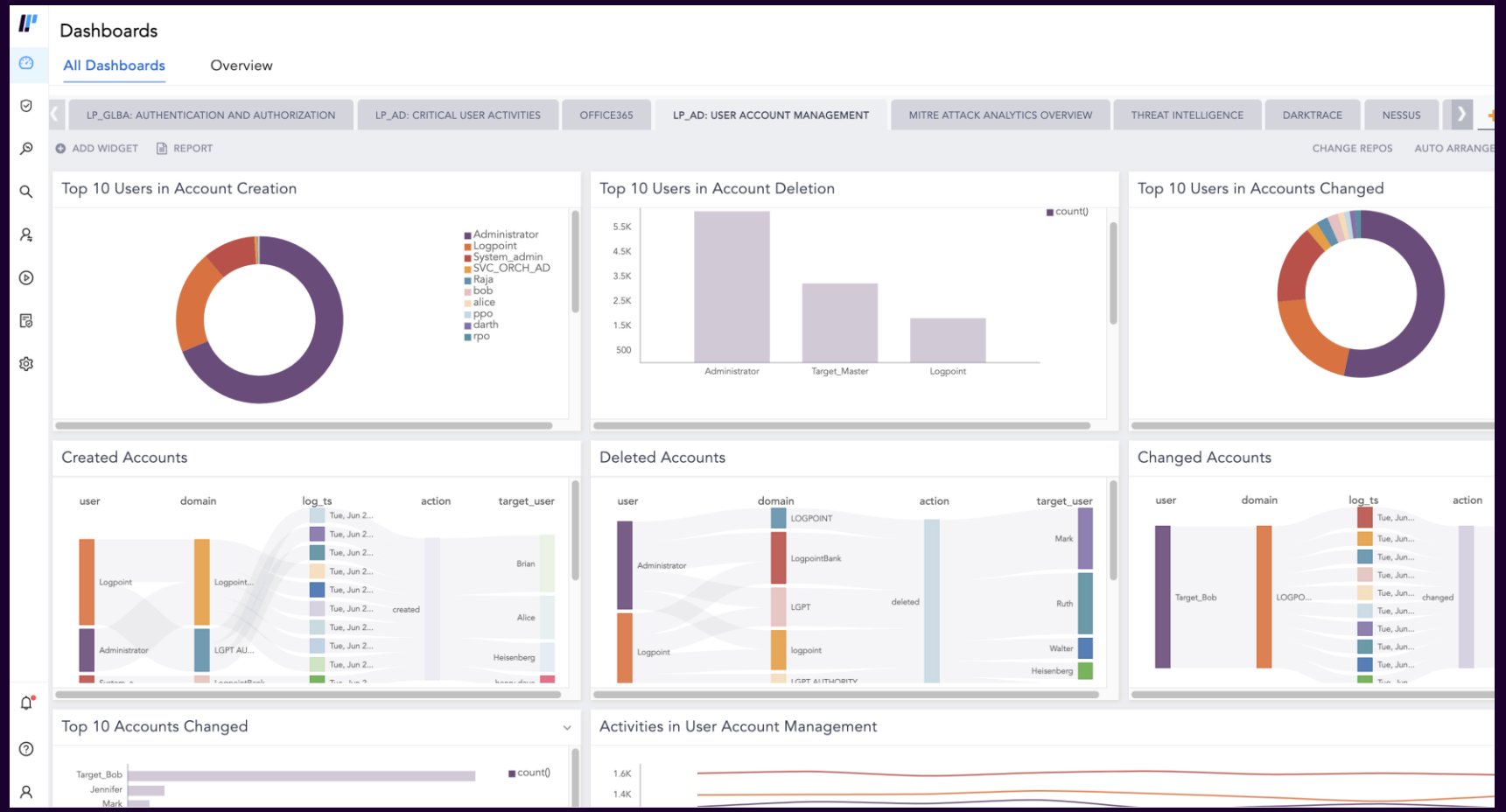
- Quickly create alert rules, dashboards, and reports:
  Clear visualization to reduce MTTR



THREAT INTELLIGENCE

Enrich events with threat indicators for external IP addresses

Show on-demand threat intelligence, giving analysts contextual information



SOAR

Reduce cybersecurity risk

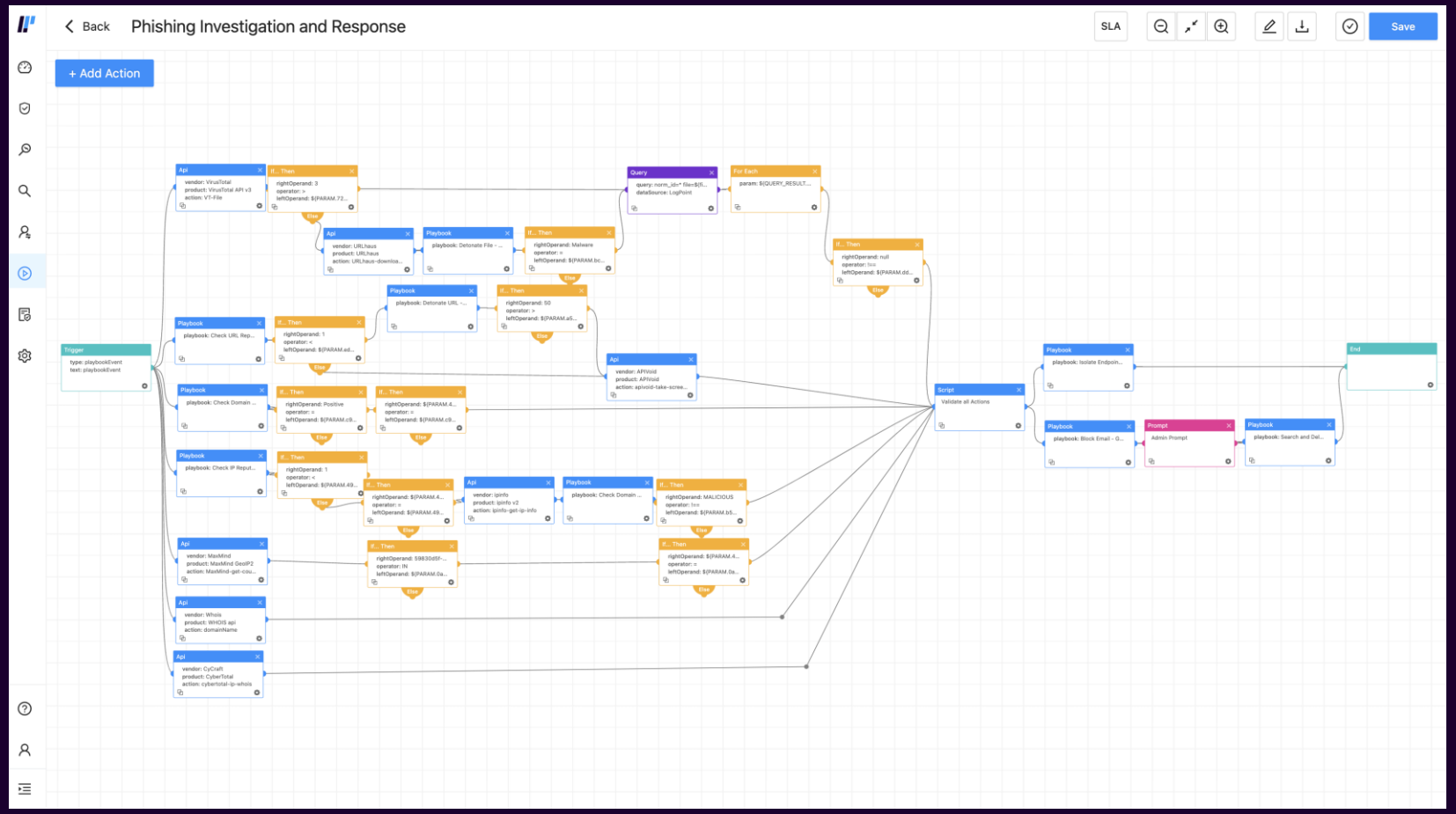
Automated playbooks help rapidly investigate, contain and remove cyber threats

Increase sec ops efficiency

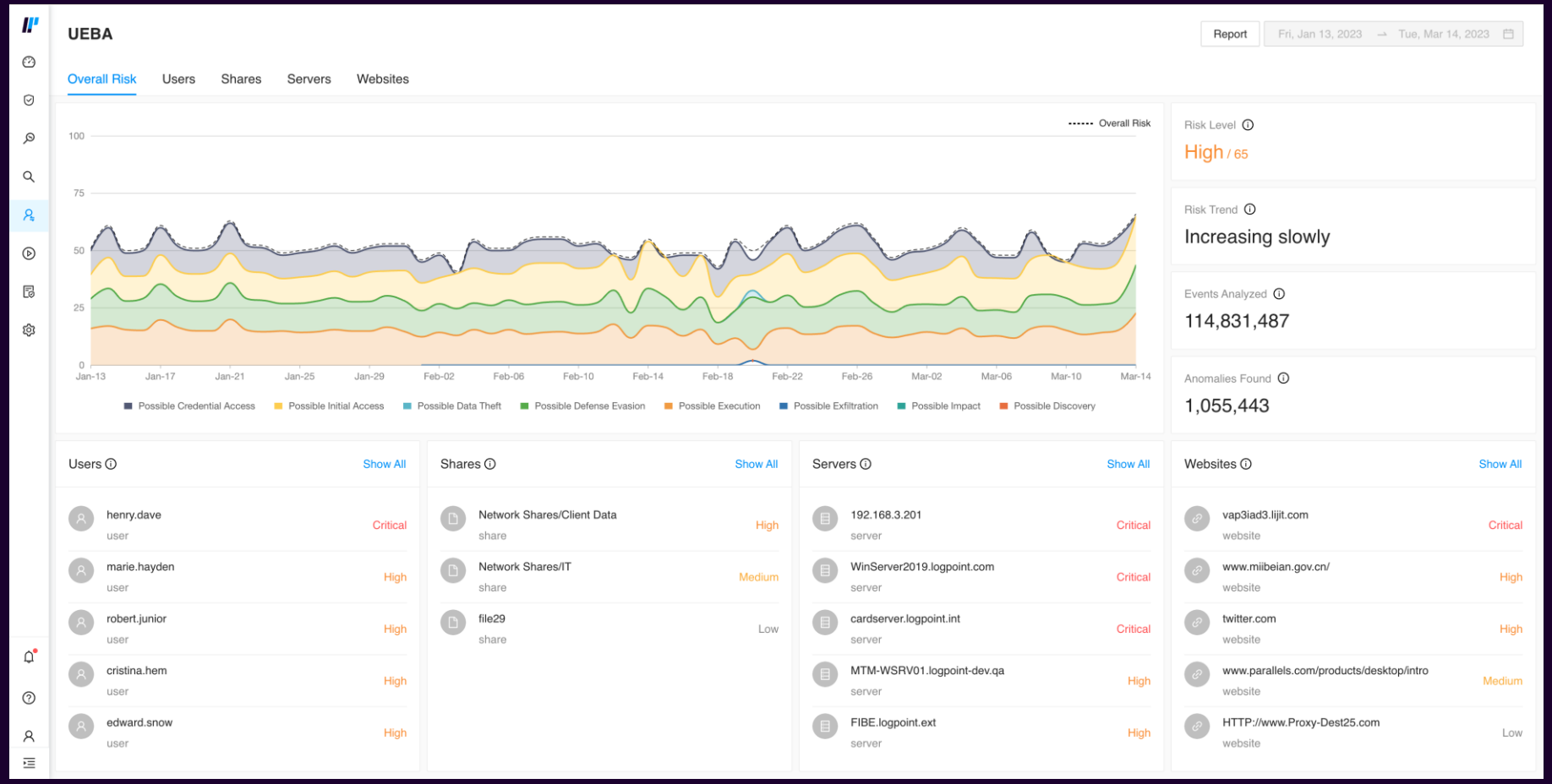
SOAR guides analysts to correct and consistent decisions by providing context enrichment and prioritizing alerts

Improve cyber intelligence

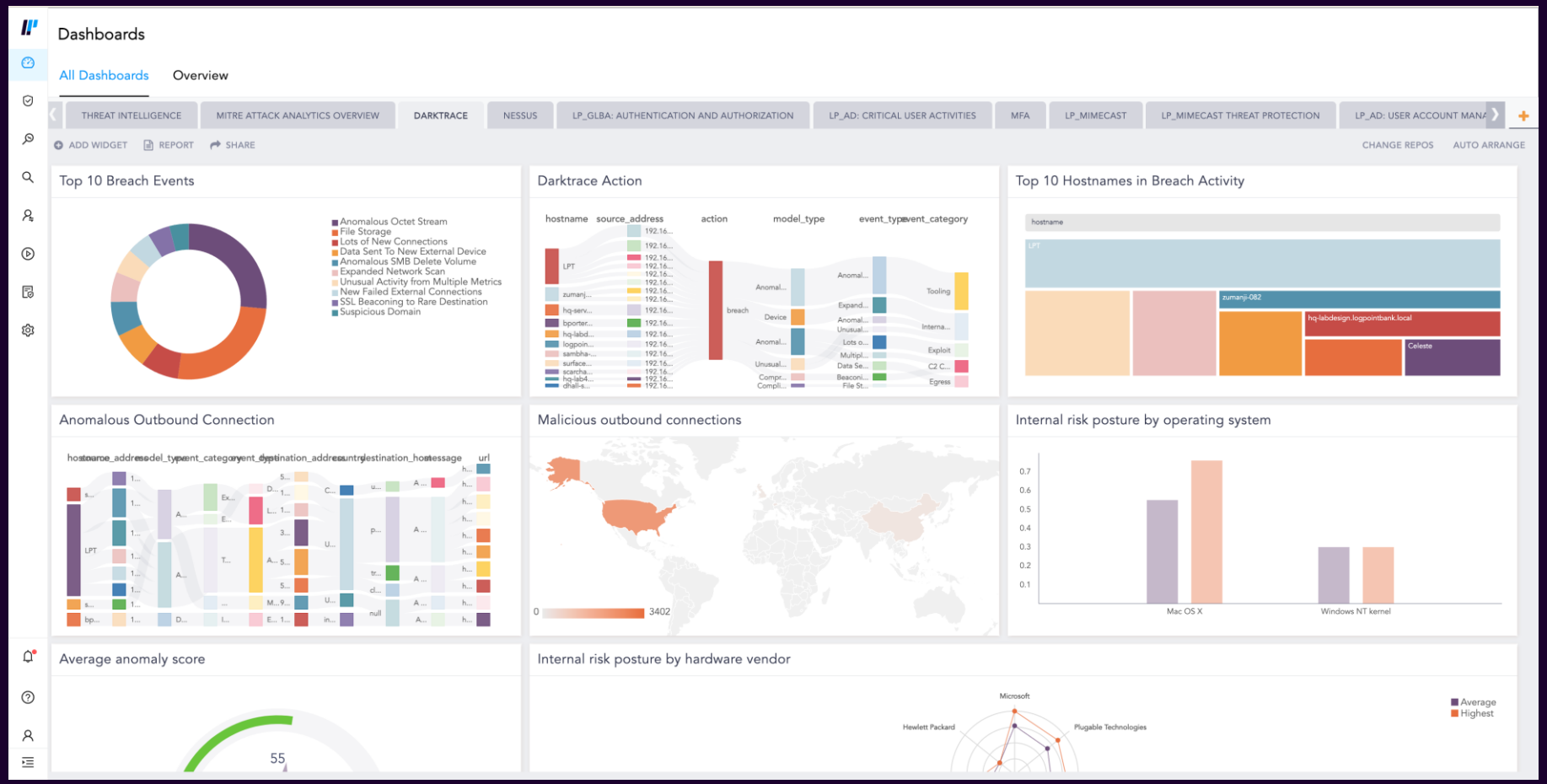
Orchestrate and prioritize alerts and security data from many sources and systems to always have the right information.



INSIDER THREAT DETECTION

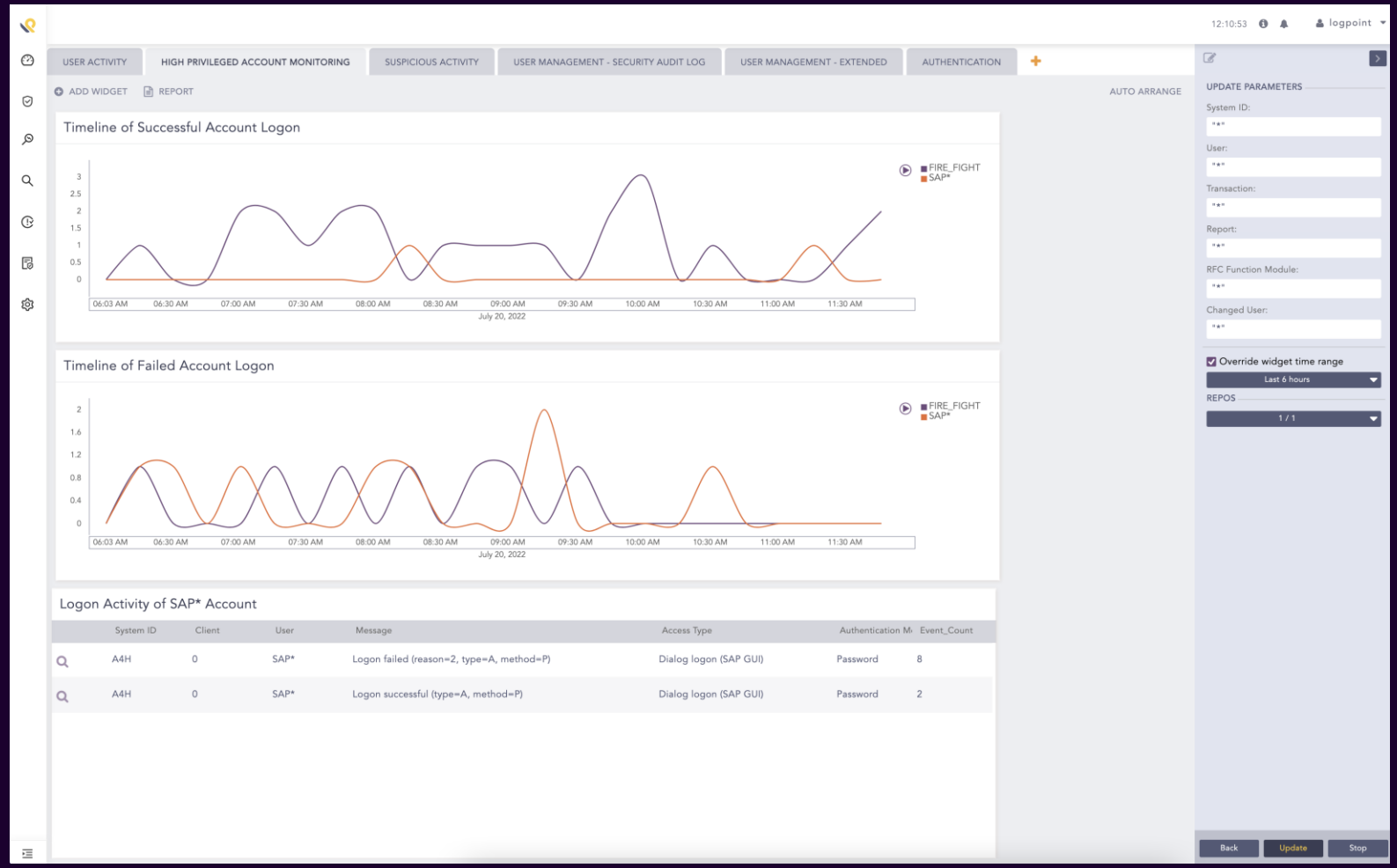


THREAT DETECTION



SECURITY OPERATIONS

SAP SECURITY



ABOUT LOGPOINT

Protecting the digital heart of organizations since 2012

Headquartered in Copenhagen, Denmark

The only EAL3+ Certified SIEM in the world

Recognized in Gartner Magic Quadrant for 4 years

300+ employees globally

Privately held by European investors

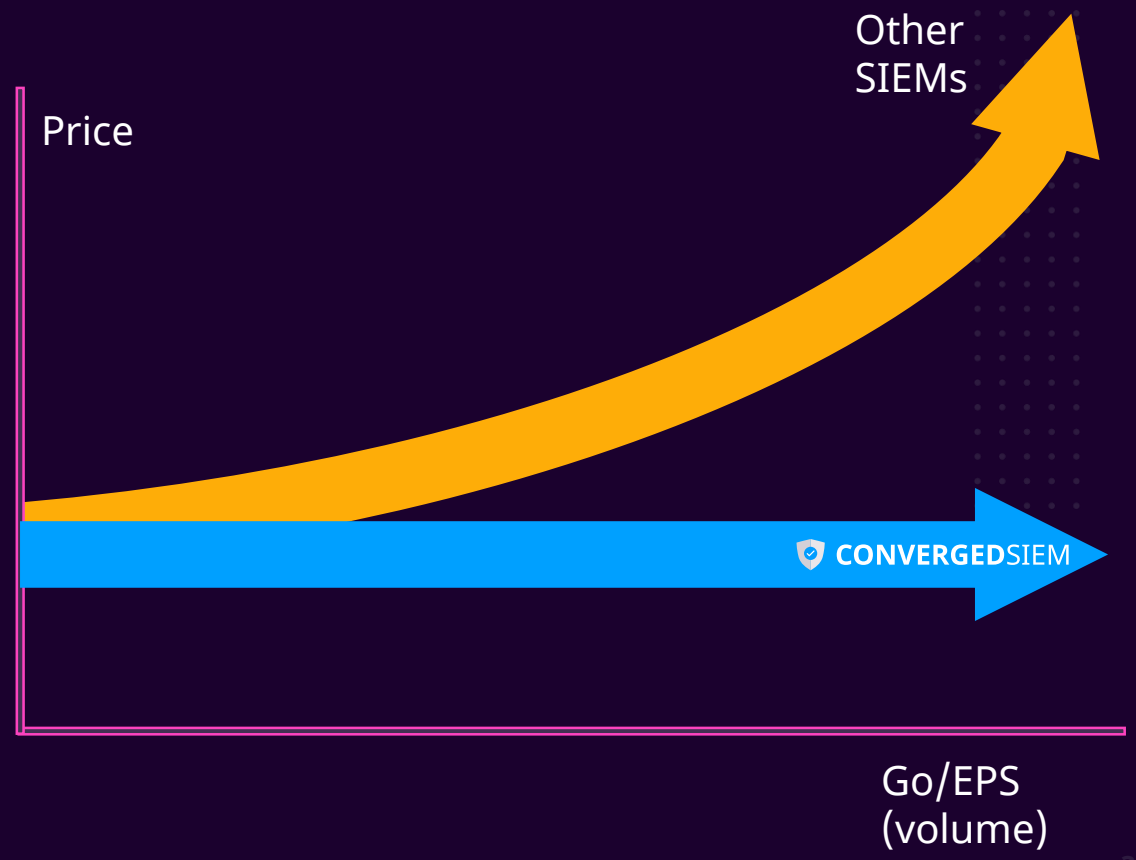
Trusted by Thousands, Guarding Millions

Product Recognitions

LICENSING

Fair, predictable, accessible and transparent

- Predictable cost model within customer's control and not based on data volume
- Licensing based on
  - Nodes for on-prem
  - Users for SaaS
- One SOAR seat for free – concurrent license
- Easy to plan and scale for future business growth



WHY ARE WE DIFFERENT

Why Customers Choose Logpoint

- A single platform for foundational security operations
- Native automation capabilities for instant response
- Machine learning identifies risky and suspicious activity
- Quick deployment: Fully operational in ~5 days
- 800+ Log sources with prebuilt controls, incl. 75+ playbooks
- Unmatched technical support and customer success
- Integration with the existing security tech stack
- Flexible deployment options – On-prem, SaaS, or private cloud
- Transparent and predictable licensing

G2:
Quality of support
9.1/10

Gartner Peer Insights:
Service & support
4.6/5

Software Reviews:
Vendor Support
86%

Evidence: How Logpoint Stacks Up

Customers rank Logpoint at the top in nearly category for product capabilities and support

	LOGPOINT	Splunk	Microsoft	Securonix	IBM	LogRhythm
Overall rating	**9.1**	8.5	8.9	8.6	8.5	8.5
Support	**9.3**	8.3	8.0	9.2	8.1	8.4
Flexible Pricing	**9.3**	8.2	7.3	9.2	7.6	8.5
Product Capabilities to meet customer needs	**8.9**	8.6	8.8	9.4	8.3	8.5
Easy to deploy	**8.8**	8.1	8.6	8.7	8.2	8.0
Analytics	**8.7**	8.5	8.0	9.1	8.1	8.3
Automated response	**8.7**	8.0	8.7	8.2	7.8	7.6
Threat intelligence	**8.6**	8.4	8.7	8.0	8.3	8.3
Out-of-the-box integrations	**8.5**	8.2	8.2	8.1	8.1	8.4

The above ratings are an evaluation of numeric scores available in the public customer rating platforms: Gartner Peer Insights, G2 and SoftwareReviews

WHAT INDUSTRY ANALYSTS SAY ABOUT LOGPOINT

Logpoint is the ONLY European SIEM recognized by:

Gartner®

Magic Quadrant for SIEM, 2022

FORRESTER®

Wave, Security Analytics Platform, 2022

IDC

SIEM Market Study, 2022

Mitchell Schneider
Sr. Principal Analyst, Gartner

Clear and concise TDIR message … **strong integration through the Logpoint ecosystem**

Pricing is easy to understand and consume – **especially SaaS**

Having security coverage for **SAP is a differentiator** – I don't see any vendors doing what you're doing

Allie Mellen
Senior Analyst, Forrester

Logpoint has a vision to create the **lowest TCO converged SIEM for midsize enterprises**, and thus far, it is delivering

Customers highlight that [Logpoint] is **straightforward and easy to use**

Customers appreciate that [Logpoint] is from the EU and has **local, on-the-ground teams for support**

PRIANTO

Prianto Hungary / Prianto GmbH
Róbert Károly Krt. 47/a.
1134 Budapest, Hungary

Tel:+36 1 769 6371
Mob: +36 70 418 7177
Email: contact@prianto.hu
Web: www.prianto.hu

LinkedIn: https://www.linkedin.com/company/prianto-hungary-cee
Facebook: https://www.facebook.com/priantohungary

Sales

- Mario Kosztik (mario.kosztik@prianto.com)
- Mariann Blaskó (mariann.blako@prianto.com)
- Eszter Baté (eszter.bate@prianto.com)

Country Manager

- Olivér Urzica (oliver.urzica@prianto.com)

Marketing

- Anna Birinyi (anna.birinyi@prianto.com)

Presales

- Krisztián Donner (krisztian.donner@prianto.com)