

PRIANTO



sumo logic

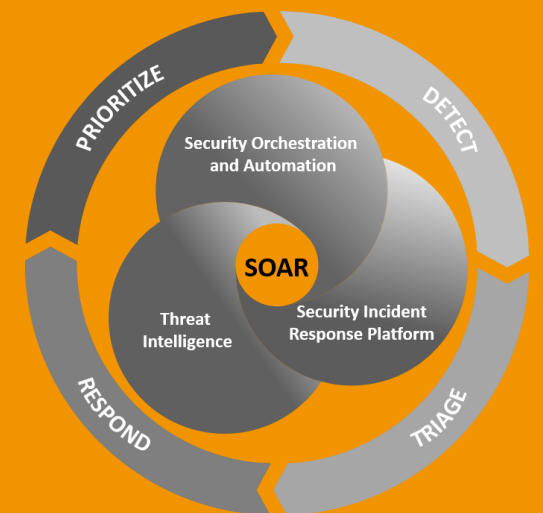
Kibertámadások kontroll alatt

Automatikus válaszadás biztonsági incidensekre
SOAR platform segítségével

Donner Krisztián | krisztian.donner@prianto.com | www.prianto.hu
Urzica Olivér | oliver.urzica@prianto.com | www.prianto.hu

Agenda

- Kibertámadási trendek
- SecOps kihívások
- Mikor van szükség SOAR-ra?
- A Sumo Logic (DFLLabs) SOAR-ról
- Mit nyújt az Sumo Logic SOAR?
- Mitől más az újgenerációs Sumo Logic SOAR?
- Licenszelés
- Összegzés



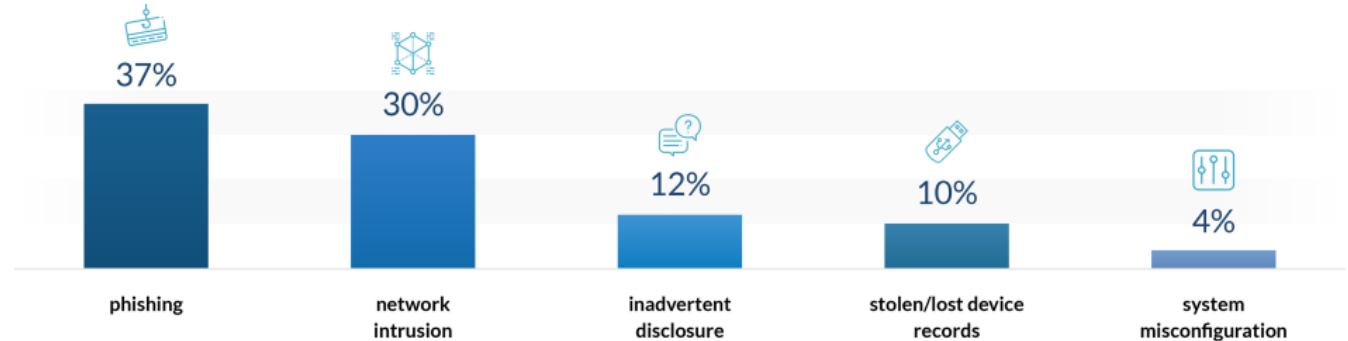


Top Security and Risk Trends

2021		2022
Cybersecurity mesh	1	Attack surface expansion
Cyber-savy boards	2	Identity system defense
Vendor consolidation	3	Digital supply chain risk
Identity-first security	4	Vendor consolidation
Managing machine identities becoming a critical security capability	5	Cybersecurity mesh
'Remote work' now just 'work'	6	Distributed decisions
Breach and attack simulation	7	Beyond awareness
Privacy-enhancing computation techniques	8	

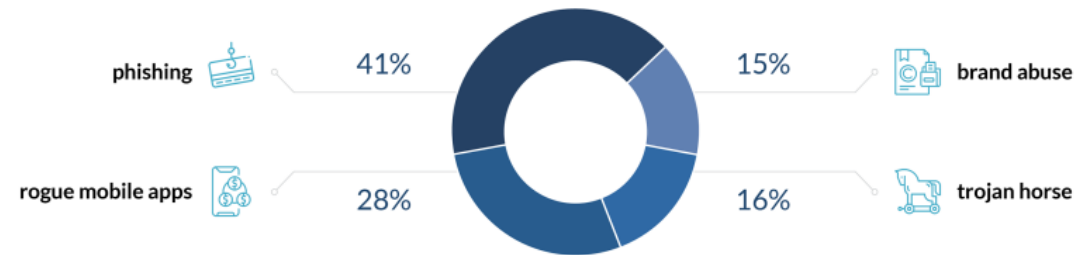
1 Most common cyber attacks experienced by companies

Source: Statista



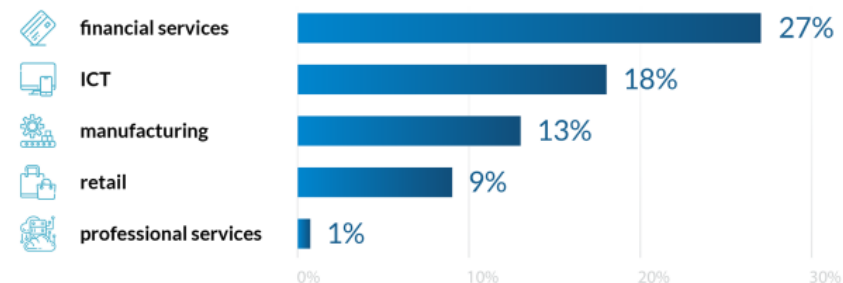
2 Top global fraud types

Source: Payments Source



3 Volume of cybersecurity incidents by sector

Source: CB Insights



SecOps kihívások

Nagyvállalati és MSSP problémák kezelése SOAR segítségével



A SUMO LOGIC (DFLABS) SOAR-ról

Security Orchestration, Automation & Response

IT-Biztonság Vezénylés, Automatizálás és Reagálás. 😊



sumo logic



A SOAR technológia úttörője.

- Alapítva 2004-ben / 2021-ben megvásárolta a SUMO LOGIC
- MILAN | LONDON | BOSTON | ABU DHABI | SKOPJE | MEXICO CITY
- Befektetők: Evolution Equity Partners
- A legtöbb szabadalommal rendelkező SOAR gyártó
- Több, mint 50 tudományos projektben való közreműködés
- ISO Editors. 3 ISO szabvány szerkesztése: Incident Response and Security Operations – IETF and OASIS Cooperation

Fortune 500 ügyfelek és MSSP.

- Az ügyfelek 60%-a Fortune 500, Global 2000 enterprise és kormányzati ügynökségek.

SUMO LOGIC SOAR Technológia.

- Nyílt Integrációs Keretrendszer (OIF)
- Magasan fejlett automatizáció
- Incidens rangsorolási képességek (Triage)
- Testre szabható Dashboardok és Reportok
- Incident Management
- MSSP-k számára is elérhető
- Kiváló támogatás

PRIANTO

Mit nyújt az SUMO LOGIC SOAR megoldás?

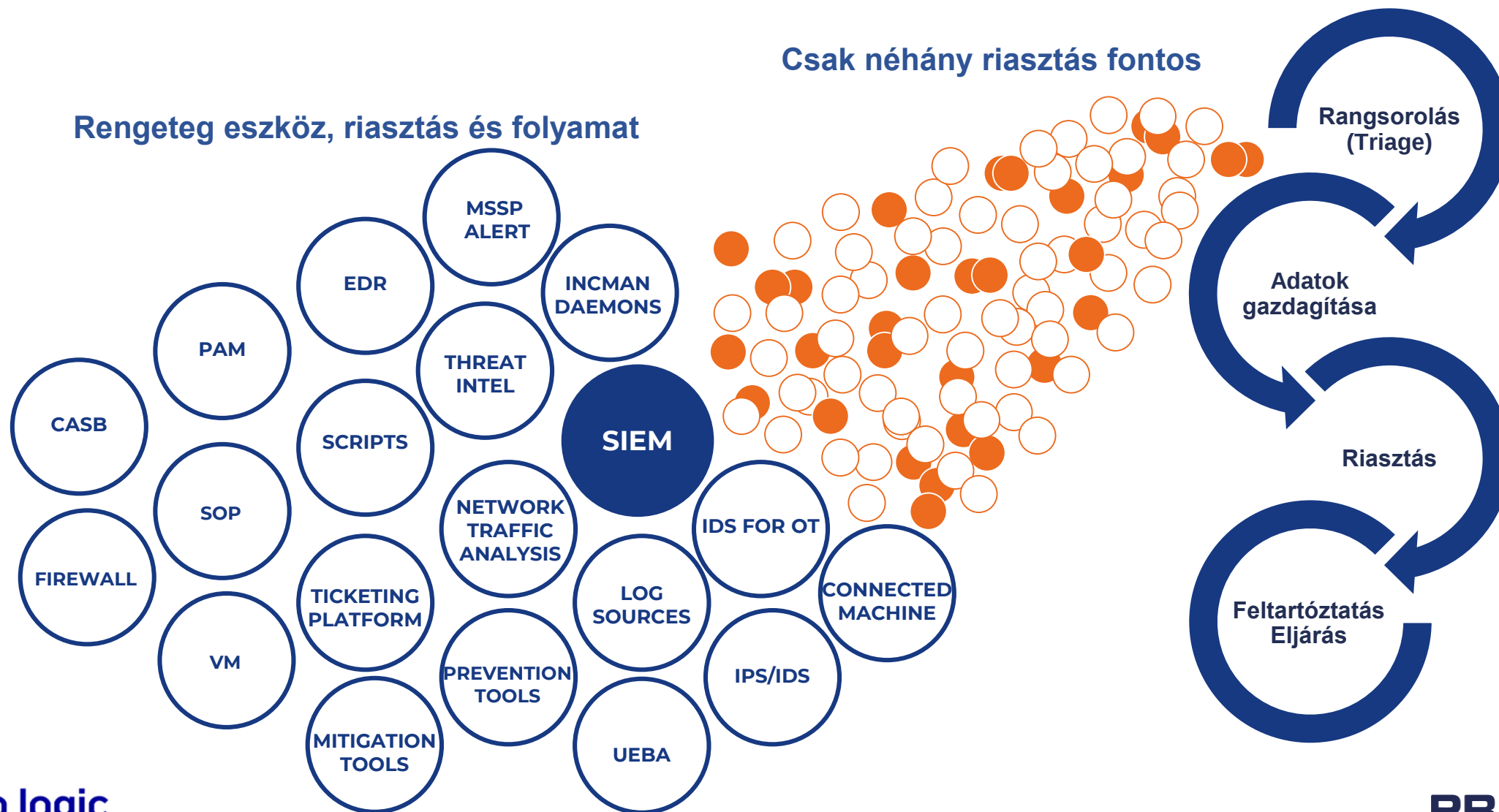
Hatékony és gyors válaszadás kibertámadásokra



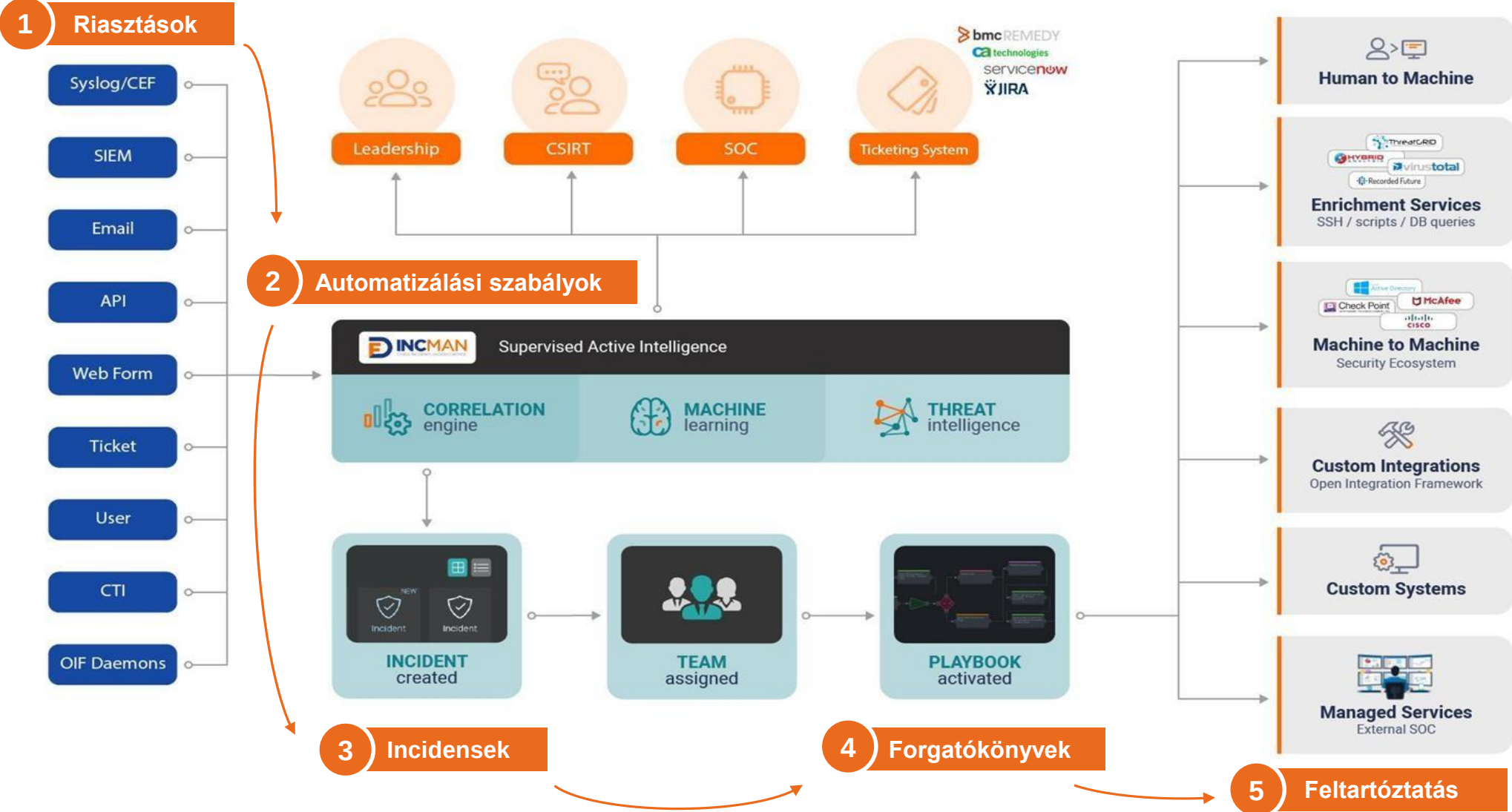
90%-os javulás az incidensekre adott válaszidőben	A fals-pozitív riasztások számát 90%-kal csökkenti	Minimalizálja a manuális műveletek számát és jobb munkaerő-megtartást eredményez
Fenyegetés-intelligencia 10x növeli a SOC termelékenységet	Számos „use case”-re felkészült meglévő forgatókönyvek alapján	Felügyelt aktív intelligencia-támogatás (SAI), amely segíti a SOC-csapatok megalapozott döntéshozatalát
Automatizált jelentések és könnyen nyomon követhető KPI-k	Eszközök egyszerű összehangolása és felügyelete az OIF segítségével	Egyszerű optimalizált fenyegetés-elemzési folyamatok és intelligencia
A riasztások osztályozása az incidensek létrehozása előtt	Nyílt, független integrációs keretrendszer, gyors integráció	Legtöbb technológiai szabadalom (machine learning, incident correlation, reporting, forensic case mgt.)

Mikor van szükség a SOAR-ra?

A SOAR ott kezdődik, ahol az észlelés befejeződik!!



SUMO LOGIC SOAR működési elve



Mitől más az Újgenerációs SUMO LOGIC SOAR?

1 Nyílt Integrációs Keretrendszer (OIF)

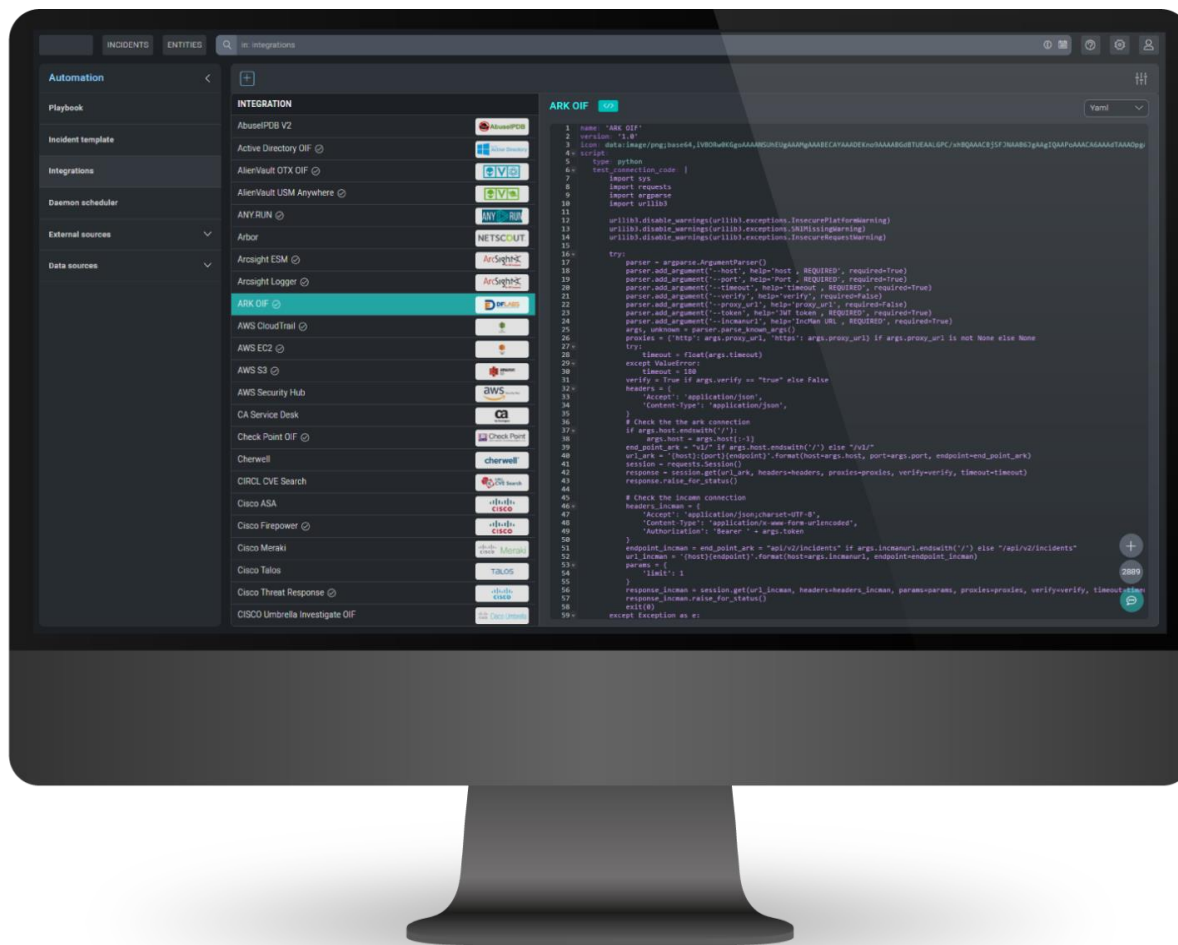
2 Incidenskezelés, forgatókönyvek és ügyek/esetek (case) menedzsmentje

3 SecOps Kezdőképernyő

4 Triázs, Gépi Tanulás és Felügyelt Aktív Intelligencia (SAI)

5 Részletesen testreszabható műszerfal

6 Incidensjelentések



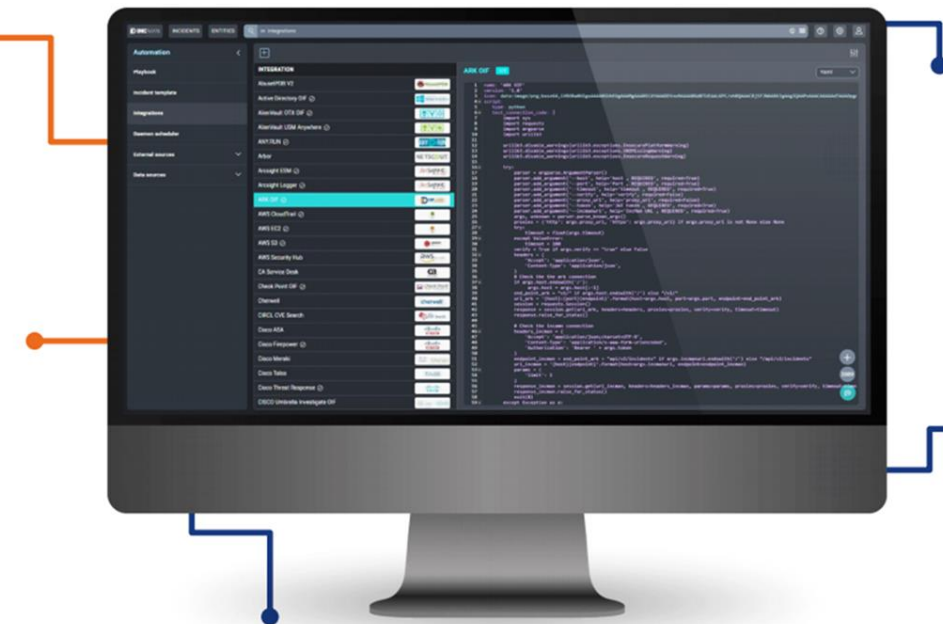
Nyílt Integrációs Keretrendszer (OIF)

Közösségi portál az integrációk, forgatókönyvek (playbook) és a frissítések megosztásához

A közösségi portálon keresztül érhető el a nyitott és együttműködő ökoszisztéma

Bárki fejleszthet API-integrációt

A konnektorok Python, Perl, PowerShell, Shell szkripteléssel vagy Yaml nyelvvél, így könnyen hozzáadhat műveleteket a meglévő integrációkhoz anélkül, hogy módosítani a meglévő kódot



Az integrációk módosítása menet közben

Az OIF az összes integrációt a cselekvési szinten, nem pedig egy monolitikus fájlként definiálja. Minden egyes integráció végrehajtása a egy egyedi Docker konténerben zajlik, így könnyen konfigurálható az integrációs fájlon keresztül.

Az első SOAR rendszer IT/OT esetekkel

Nincsenek korlátok a létrehozható integrációknak beleértve a saját szkriptet is - Cyber - Csalás elleni - Ipari - IoT és azon túl

Külön konténerekben futó daemonok a folyamatok ütemezéséhez

A démonok alkalmazási területe szinte korlátlan. Nem csak biztonsági tevékenységeket esetében, hanem IT incidenseknél vagy egyszerű napi felügyeleti folyamatoknál is alkalmazhatóak.

Nyílt Integrációs Keretrendszer (OIF)

SUMO LOGIC: A „legnyitottabb” SOAR platform

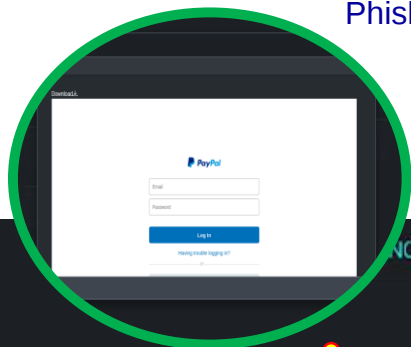


- **300+** konnektor és **1500+** akció-folyamat
- Standard nyelvopciók
- **Nagy szakértői közösség** tudás- és integrációk megosztására
- **Több száz** azonnal alkalmazható **playbook**
- **Számtalan** különböző iparági esettanulmány és referencia
- **Daemon**-ok & **Trigger**-ek

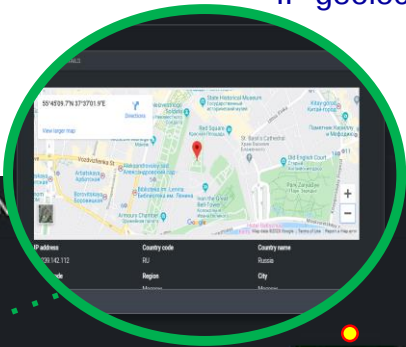
Incidents-, forgatókönyv- és esetkezelés

PÉLDA: Phishing forgatókönyv

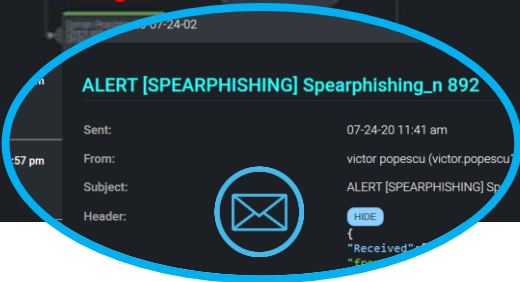
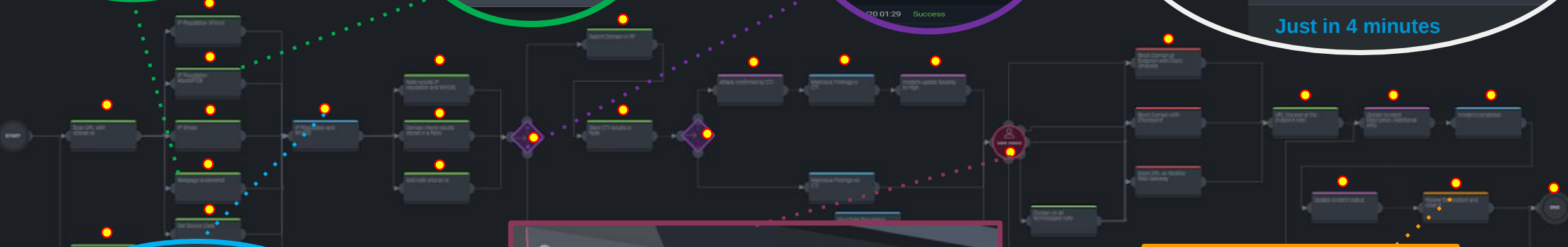
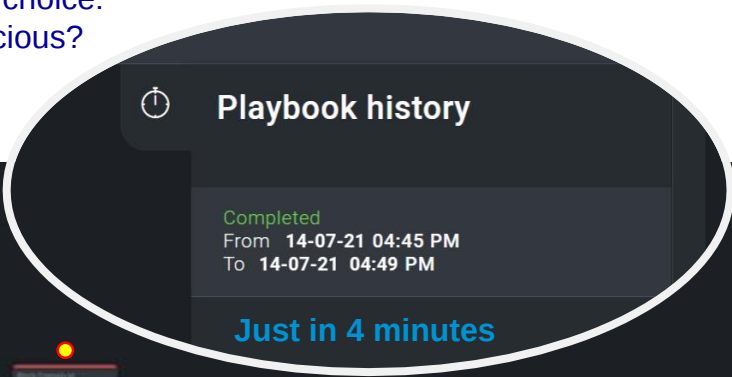
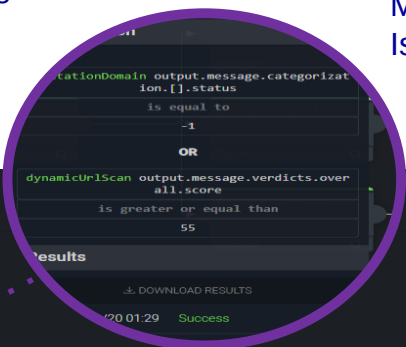
Phishing domain screenshot



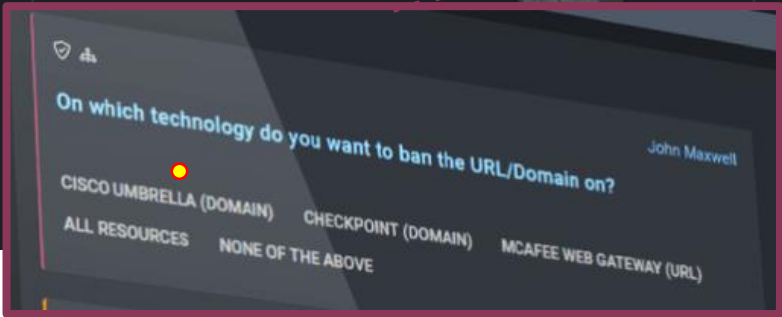
IP geolocation of phishing domain



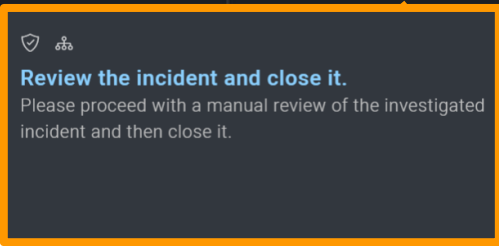
Machine choice:
Is it malicious?



Notification sent



Analyst Choice



Automatically assigned task

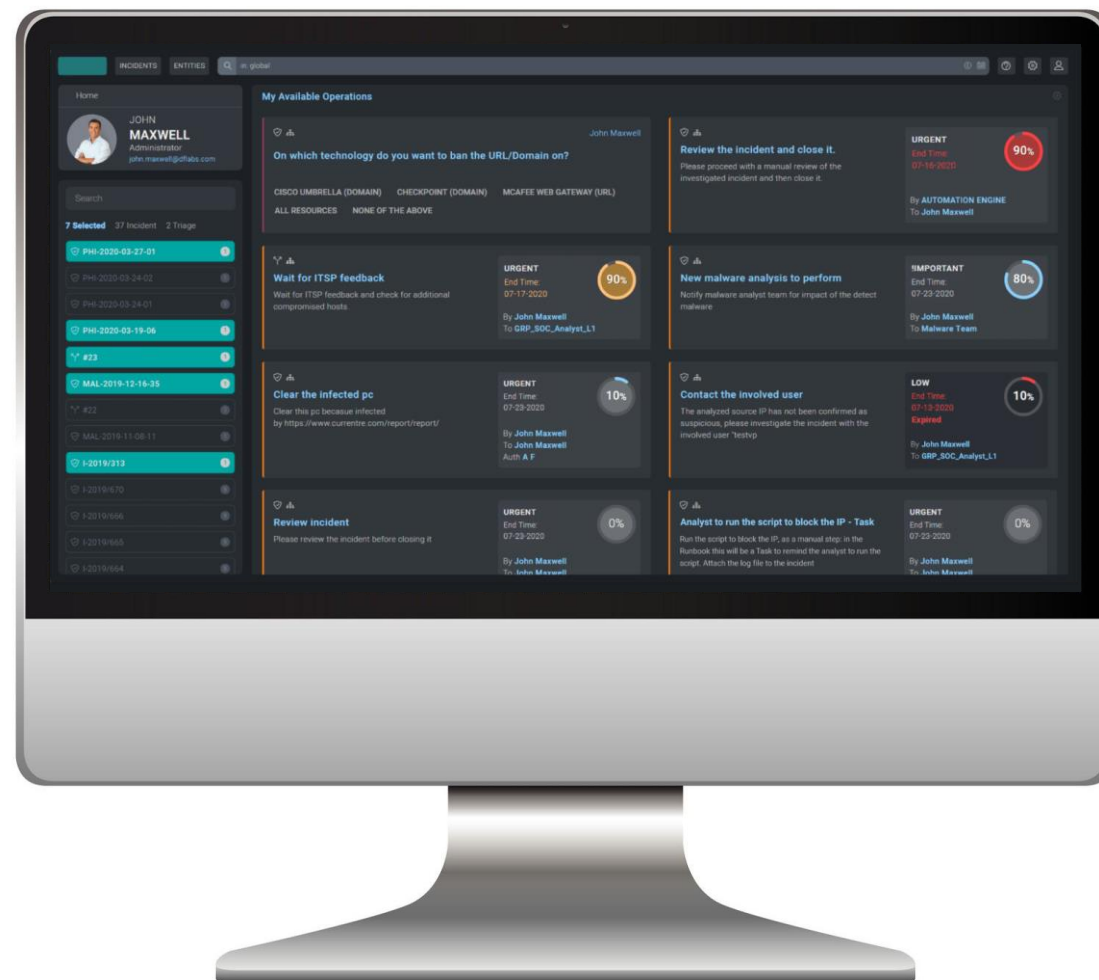
PÉLDA: DDOS forgatókönyv



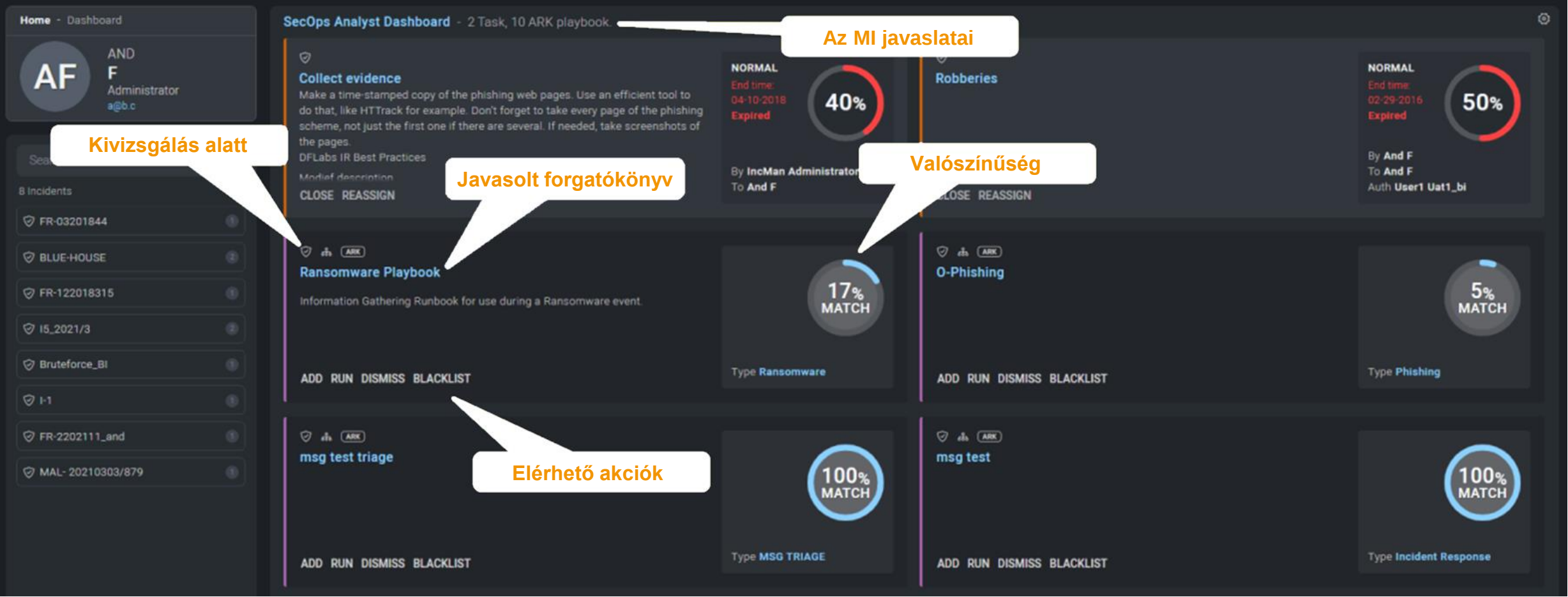
SecOps kezdőképernyő

Minden feladat egy helyen

- **Forgatókönyv műveletek kezelése:** felhasználói válaszadás, feladatok manuális futtatása
- **Incidensek kezelése:** befejezés, hozzárendelés, lezárás, átirányítás vagy elutasítás
- A **SecOps hatékonyságának javítása** a mesterséges intelligencia által javasolt forgatókönyvek segítségével
- Feladatkör-specifikus, **egyedi beállítások** a magasabb fokú felhasználói élmény érdekében



Mesterséges Intelligencia



Események kezelése és a hadműveleti szoba

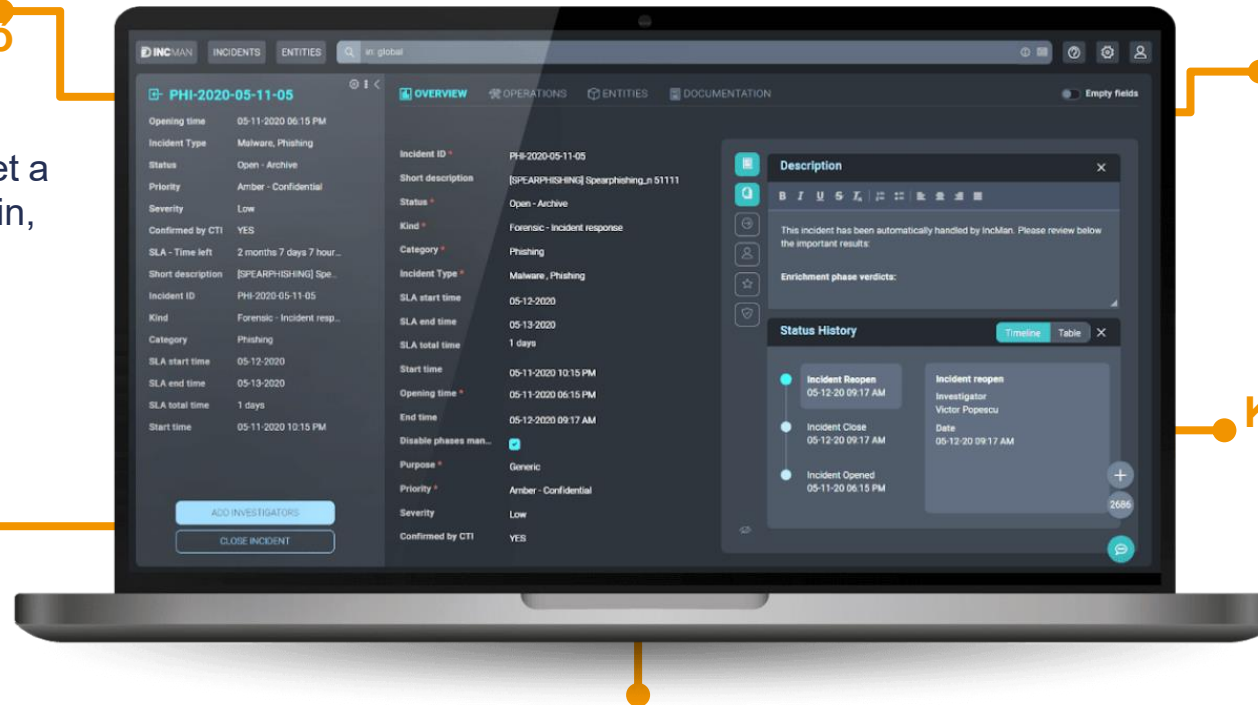
Az incidens minden aspektusának megjelenítése egy helyen

Több száz testreszabható mező

Tárolja strukturáltan a különböző eszközök által gyűjtött adatokat, és használjon egyéni mezőhelyettesítőket a választási opciókon, a feladatok címein, leírásain és az incidensjelentéseken belül.

Szerepkörök szegregálása, részletes RBAC-modell

Részletes szerepkör alapú hozzáférés-szabályozás (RBAC) a szükséges jogosultságok rendelkezésre állása érdekében.



Minden információ egy helyen

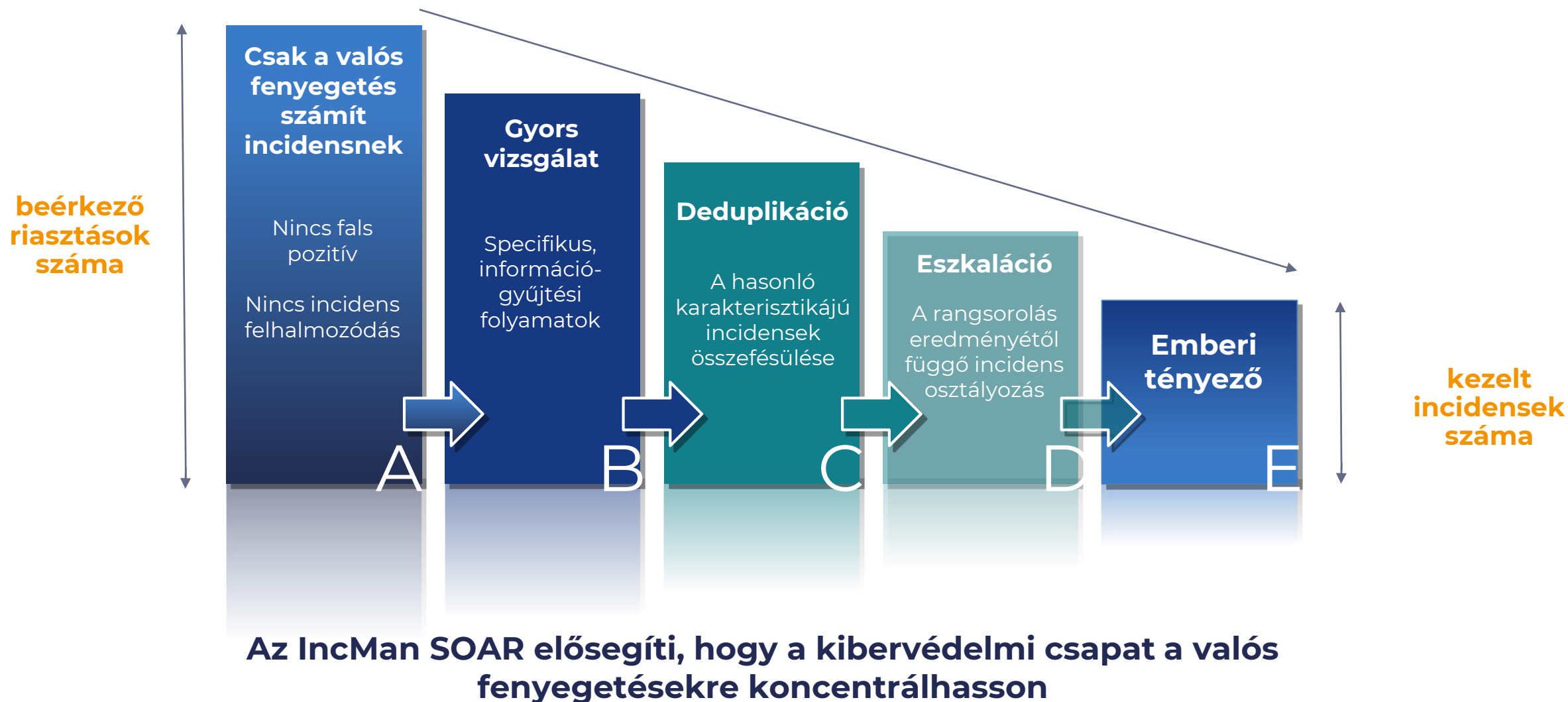
Hozzáférés egy adott incidens folyamatának teljes és részletes képéhez a war room-ban

Konfigurálható incidensfázisok

Annyi állapotípust adható az eseményhez, amennyit szükséges. A szakaszok színét ennek megfelelően változtatható az intuitív használat érdekében.

Ezen túlmenően a War room lehetővé teszi az elemzők számára, hogy az integrált csevegéseken keresztül többek között további információkat adjanak meg, ami sokkal hatékonyabb kommunikációt eredményez a SOC-csapat tagjai között.

Triázs, a riasztások osztályozása



Részletesen testreszabható műszerfal

Egyszerű és Mérhető

A módszer, amellyel az egyes KPI-okat mérjük, egyértelműen meghatározottnak és következetesnek kell lennie.

Döntéselőkészítés

A KPI-kat úgy kell használni, hogy segítsék a döntéseket



Releváns

A biztonsági programban minden egyes KPI egy, a vizsgált funkcióra vonatkozó mérés kell legyen

Időalapú

A hatékony KPI-nak összegyűjthetőnek, különböző időpontok és intervallumok alapján csoportosíthatónak kell lennie, hogy mutassa a változásokat és mintákat

Incidens jelentések

Azonnali jelentések

Azonnali és részletes jelentések készítése kevesebb, mint egy perc alatt



A kommunikáció javítása

Gyorsabb és hatékonyabb incidens kezelés és jelentés készítés



Könnyű információgyűjtés

Részletes incidens-jelentések a kapcsolódó IOC-kkel, az ütemezéssel és a végrehajtott korrekciós intézkedésekkel együtt.

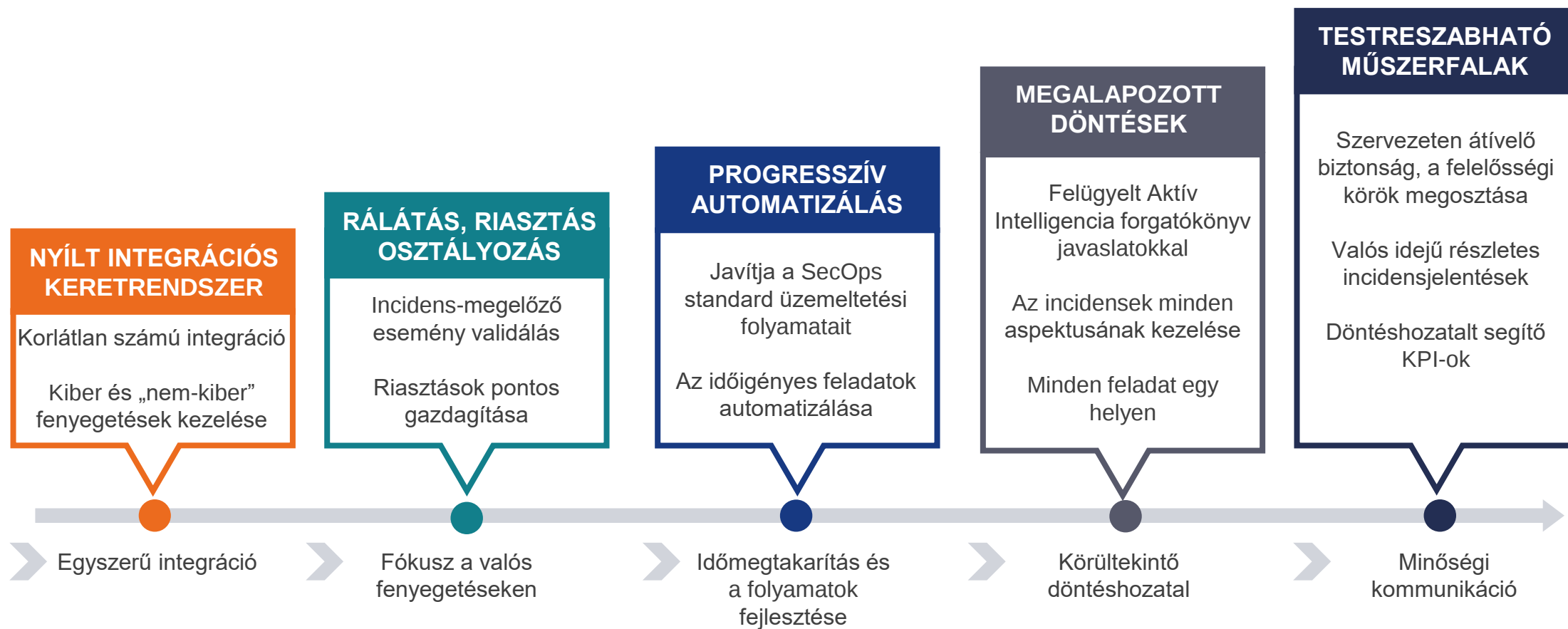


Nagyfokú testreszabhatóság

Testreszabható jelentések készítése saját sablonban és jelentések generálása különböző formátumban

Léptesse új szintre IT-biztonsági csapata eszköztárát

Csökkentse a válaszidőt automatizálással, vezénnyel és körültekintő döntéshozattal



Licenszelés – Előfizetési konstrukció

SOAR rendszert kezelő felhasználók száma alapján, korlátlan playbook-ok és rendszerek használata mellett – ON-PREM / FELHŐS / MSSP

INC MAN

HOME DASHBOARD INCIDENTS OPERATIONS DATA SOURCES TRIAGE

IncMan

Features

• Number of Authorized Users- Named Users

• Subscription License - yearly

• Multiyear discount available

• High level Support

• DFLabs Library of playbooks

• Number of Tenants (=customers)

• Unlimited tenants option available

Enterprises

Standalone

✓

✓

✓

✓

✓

MSSP

Multitenancy

✓

✓

✓

✓

✓

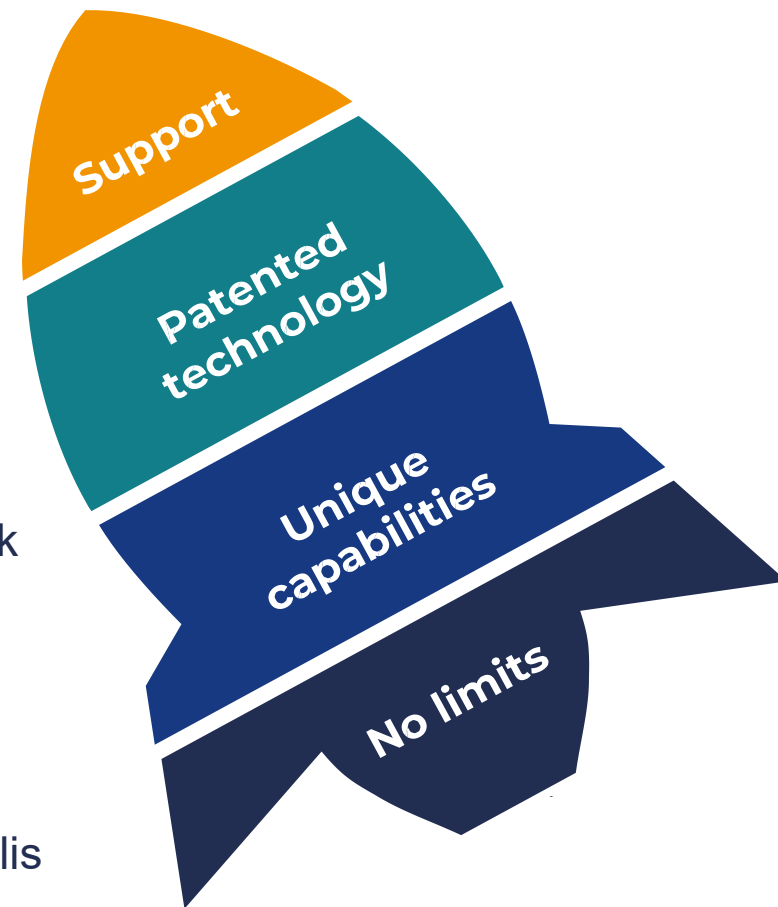
✓

✓

On Premise / Cloud / SaaS

Összegzésként

- **Valós idejű vizsgálatok:**
Napi több, mint 500 konszolidált riasztás rangsorolása az incidenssé alakítás előtt, átlag 55 másodperc alatt
- **Jobb reakcióidő:**
Több, mint napi 150 incidens automatikus feldolgozása
- **Növelt hatékonyság:**
Progresszív automatizált feltartóztatás és kezelés mindössze 2 perc alatt
- **Szabványosított és dokumentált munkafolyamatok** az iparági előírásoknak megfelelően (Hazai & nemzetközi szabványok-szabályozások)
- **Rugalmasan bővíthető integráció** a nyílt keretrendszernek köszönhetően
- **Optimalizált HR erőforrás-kihasználtság és -allokáció**, csökkentett manuális műveletek és jobb munkaerő-megtartás



Fejlett kibervédelmi triumvirátus – SIEM + SOAR + Threat Intel

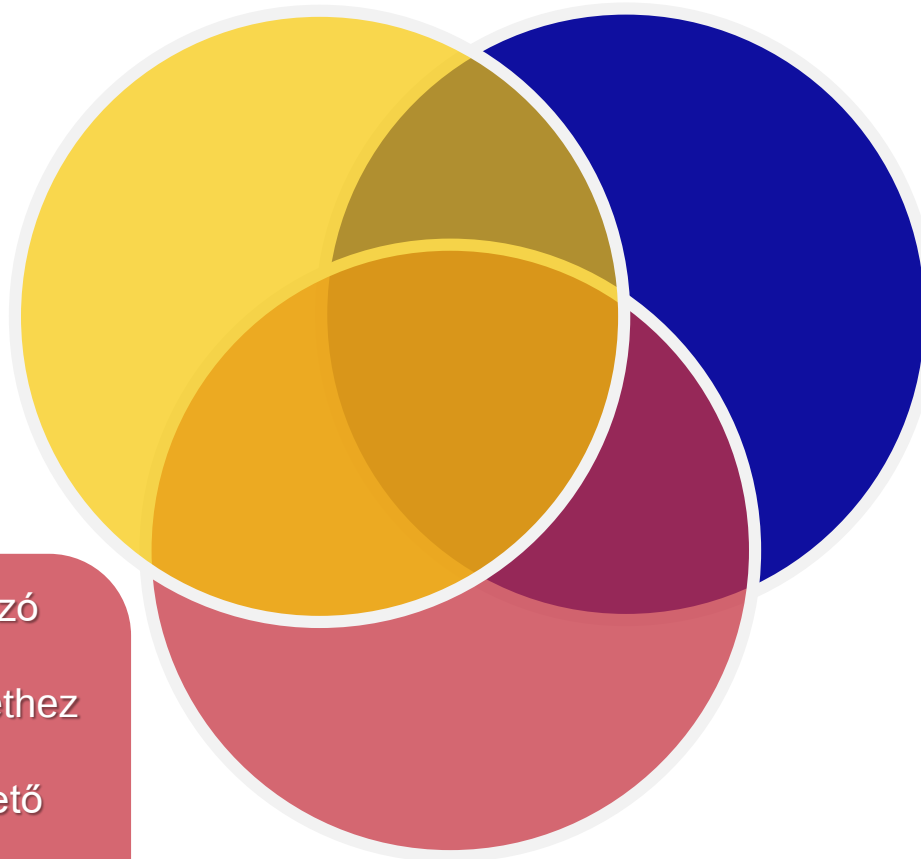
SIEM



- Licenzelés: végpont alapú On-prem/ SaaS / MSSP
- Gazdag API – natív konnektorok
- Újgenerációs, skálázható
- Felhasználóbarát kezelői felület
- Kiemelt gyártói támogatás
- Lokális szakértő partner
- Attraktív árazás

- Licenzelés: felhasználó-kulcsszó SaaS / MSSP
- Egyedi hozzáférés dark-deepnethez
- Speciális információ korrelálás
- Skálázható, rugalmasan bővíthető
- Gyors integráció, konfiguráció
- 6-az 1-ben látásmód
- Személyreszabott gyártói támogatás
- Attraktív árazás

sumo logic



Threat Intelligence



CYFIRMA

SOAR



sumo logic

- Licenzelés: felhasználó On-prem/ SaaS / MSSP
- Gazdag API – natív konnektorok
- Újgenerációs, skálázható, számos szabadalommal
- Azonnal alkalmazható forgatókönyvek
- Natív integráció más rendszerekkel
- Felhasználóbarát kezelői felület
- Gyors és egyszerű integráció
- Lokális szakértő partner
- Attraktív árazás

PRIANTO



Köszönjük! **Kérdések?**

Donner Krisztián | krisztian.donner@prianto.com | www.prianto.hu
Urzica Olivér | oliver.urzica@prianto.com | www.prianto.hu

PRIANTO sumo logic