GALILEUM

AZ ELSŐ 100 NAP

avagy SOC bevezetés lépései

Security Operations Center
by Andrews IT Engineering

AZ ELSŐ 100 NAP

100

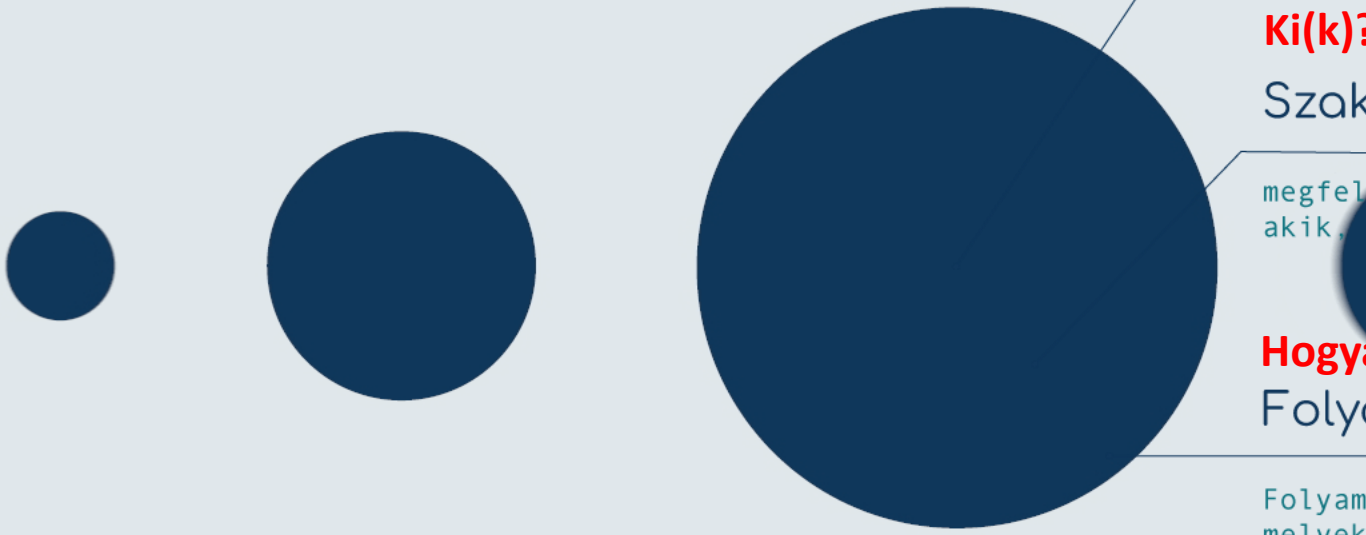
A 100 nap fogalmának gyökerei Franciaországból származnak, ahol a “Cent Jours” (száz nap) fogalma az 1815-ös időszakra utal **Bonaparte Napóleon**nak az Elba szigeti száműzetéséből Párizsba való visszatérése és a szigeten elszenvedett végső veresége között. Waterloo-i csata, amely után XVIII. Lajos király visszaszerezte a francia trónt.

Az **"első 100 nap**" kifejezést először **Franklin D. Roosevelt** használta fel beszédeiben, amikor 1933-ban hivatalba lépett. Az Egyesült Államokban addig senki sem beszélt annyit egy elnök első 100 napjának fontosságáról. Roosevelt gyors intézkedéseket hozott a nemzetet sújtó pénzügyi pánik enyhítése érdekében, Roosevelt rendkívüli termelékenysége hatalmas népszerűséget eredményezett, és ő állította fel az első 100 napos szabványt, amellyel minden jövőbeli amerikai elnököt (talán igazságtalanul) mérnek.

Tekintsük át mi fér bele az első 100 napba …

A SOC egy szervezeti egység, melynek feladata az információbiztonsággal kapcsolatos rendszerek, események kezelése.

MIBŐL TEVŐDIK ÖSSZE A SOC?



Mivel?

Szakalkalmazások és infrastruktúra

Speciális információ biztonsági eszközök, támadások feltérképezésére elemzésére és elhárítására

Ki(k)?

Szakértők

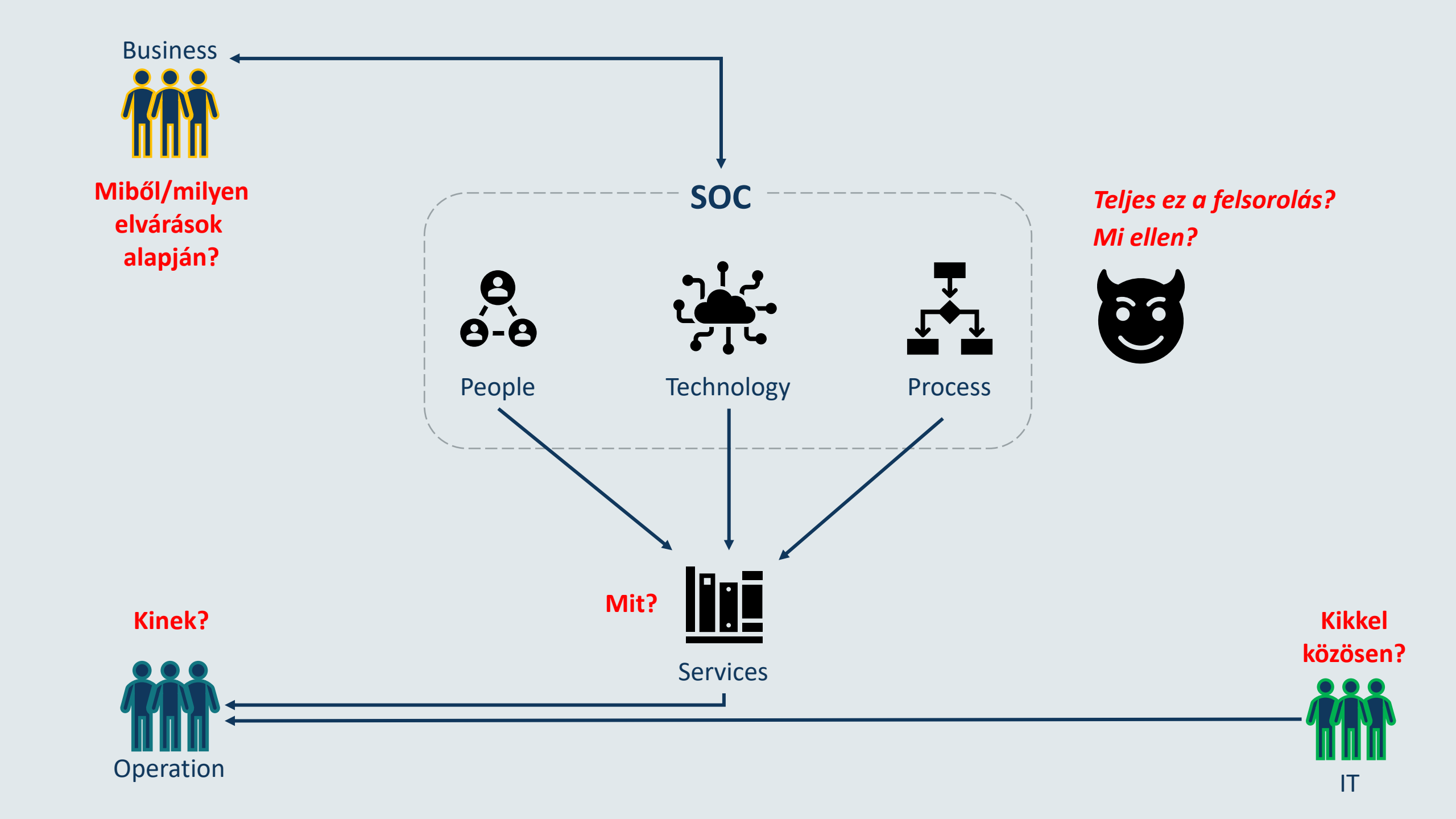
megfelelő tudású és létszámú szakértői csapat, akik rendelkezésre állnak szükség esetén

Hogyan?

Folyamatok, eljárások

Folyamatok, ellenőrző listák és eljárásrendek melyek biztosítják a folyamatos és megfelelő minőségű szakmai tevékenységet.

Teljes ez a felsorolás?


Business
Miből/milyen elvárások alapján?
SOC
People
Technology
Process
Teljes ez a felsorolás?
Mi ellen?
Mit?
Services
Kinek?
Operation
Kikkel közösen?
IT

MIT KELL ÁTGONDOLNI MIELŐTT KEZDÜNK?

BUSINESS ENABLEMENT

MERGER/AQUISITION
- Acquision risk management
- Integration cost
- Identity management

MOBILE TECHNOLOGY
- Policy
- Technology
- Lost/stolen devices
- BYOD
- Mobile apps inventory

CLOUD COMPUTING
- Cloud architecture
- Strategy and guidelines
- Cloud risk evaluation
- Compilance
- Ownership/Liability/Incidents
- SaaS strategy
- Log integration
- Virtualized security appliances

PROCESS
- HR on boarding/termination
- Business partnerships

SELLING INFOSEC
- Aligning with corporate objective
- Continuos MGMT updates
- Innovation and value creation

SECURITY OPERATIONS
THREAT PREVENTION
- Vulnerability management
- Application security
- IPS
- Identity management
- Information Security policy
- DLP
- Anti malware, anti-spam
- Proxy/content filtering
- Patching
- DDoS protection
- Hardening guidelines
- Desktop secutity
- Encryption SSL
- PKI

THREAT DETECTION
- Alerting (IDS/IPS, FIM, WAF, antivirus, etc)
- NetFlow analysis
- DLP
- Threat hunting
- MSSP integration
- SOC Operations

INCIDENT MANAGEMENT
- Media relations
- Incident readiness
- Forensic investigation
- Data breach preparation

PROJECT DELIVERY LIFECYCLE
- Requirements
- Design
- Security testing
- Certification and accreditation

SOC

IDENTITY MANAGEMENT
- Credentialing
- Account creation/deletions
- Single sign on (SSO simplified sign on)
- Repository (LDAP/Active directory)
- Federation
- 2-factor authentication
- Role-based access control
- Ecommerce and mobile apps
- Password resets/self service
- HR process integration
- Integrating cloud based identities

RISK MANAGEMENT
- Physical security
- Vulnerability management
- Ongoing risk assessments/ pam testing
- Integration to project delivery (PMD)
- Code reviews
- Risk assesment methodology
- Policies and procedures
- Associate awareness
- Data centric approach
- IoT technologies
- Operational technologies

BUDGET
- Security projects
- Business case developement
- ROSI
- Alignment with IT projects
- FTE and contractors
- Balancing budget for people. Trainings and tools/ technology

SECURITY ARCHITECTURE
- Network segmantation
- Application protection
- Defense-in-depth
- Remote access
- Encryption technologies
- Backup/replication/ multiple sites
- Cloud/hybrid/ multiple cloud vendors

COMPILANCE AND AUDITS
- PCI
- SOX
- HPAA
- Regular audits
- SSAE 16
- Other compilance needs

+NIS2

LEGAL & HUMAN RESOURCES
- Data discovery
- Vendor contracts
- Investigations/forensics
- Integrating into IDM processes

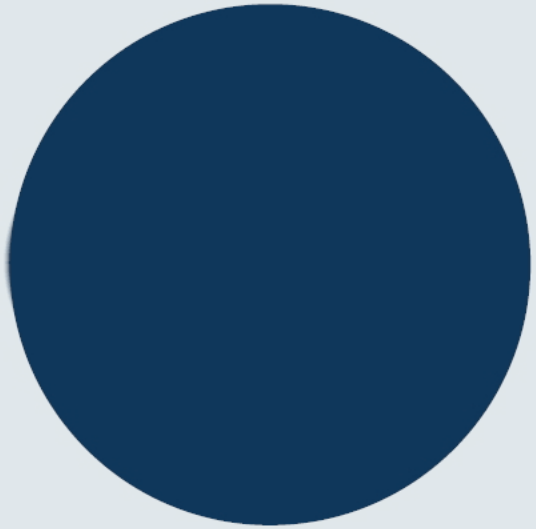
ÍGY TESZI A SOC LÁTHATÓVÁ A LÁTHATATLANT

Támogatás: biztonsági szint megőrzése, javítása

\ a naplókban található objektív bizonytékok alapján feltárt hiányosságokra adunk szakmai megoldási javaslatokat

Elhárítás: folyamatos biztonsági felügyelet

\ Naplók elemzése, riasztások kiértékelése
\ Incidensek elhárítása



Felmérés: Kockázatelemzés és értékelés

\ Üzleti folyamatok, értékek azonosítása
\ Jelenlegi állapot felmérése, kockázatok azonosítása, értékelése

Felkészülés: lehetséges incidensek kezelésének kidolgozása

\ Megelőzés, megerősítés
\ Hogyan észlelhető?
\ Teendők az adott esetben

Business

Igény azonosítása

Szükség van erre a szervezetnek?

Projekt

Célok meghatározása

Tagok kijelölése

Projekt indítása, követése

Döntés előkészítő anyag

Üzleti terv, finianszírozás

Projekt indítása, követése

Üzleti döntés

Reporting igények meghatározása /feldolgozása

Egyéb területekkel való együttműködés kialakítása a SOC kapcsán

Irányítás

Emberek

Induló csapat

SOC architekt keresése/kiválasztása (mi alapján)?

SOC vezető kiválasztása

Csapat felvétele

Csapattagok interjuzása

Belső/külső képzések

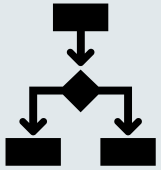
Szerepkör szerinti bevezető oktatások

Szükséges létszám /tudás?

Milyen szerepkörök / Shifting kialakítása?

Milyen rendelkezésreállásban, milyen reagálási idővel?

Csapat tervezése



Folyamatok

Folyamat katalógus/tervezés

Milyen külső és belső folyamatok szükségesek

Milyen elvárások vannak a folyamatokkal kapcsolatban

Milyen folyamat támogató eszközök szükségesek?

Folyamatok működtetése

Életcilkus kezelése, Minőségbiztosítás, mérés

"Mit tanultunk" visszavezetése

Folyamatok belső oktatása, mérése

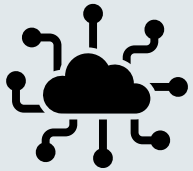
Ki írja meg ezeket? (techwriter?)

Mi alapján? (szabványok?)

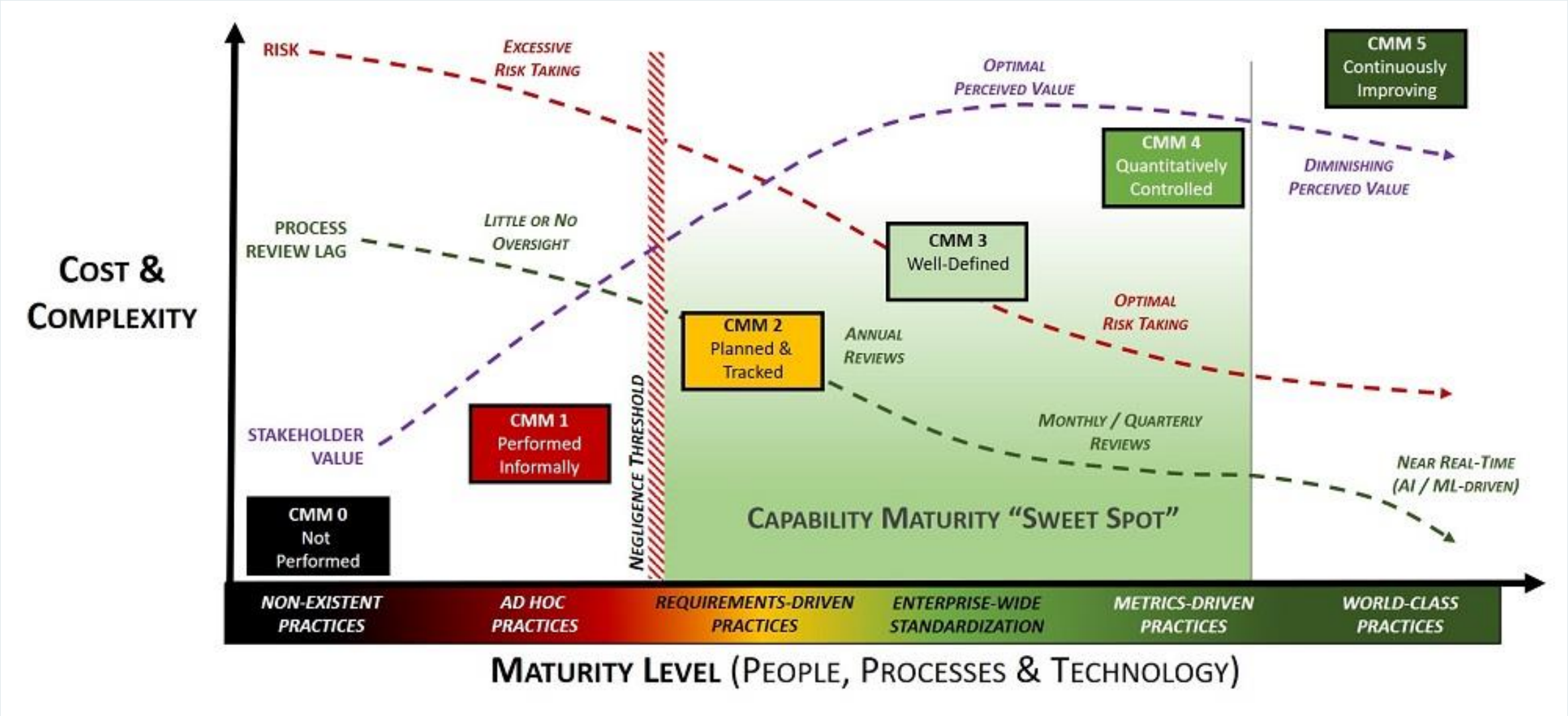
Folyamatok ellenőrzése, teljesség vizsgálat

Folyamat kialakítása

Eszközök ...



És ha ide eljutottunk akkor bejön a képbe még ez is …



forrás: https://securecontrolsframework.com/capability-maturity-model/

SOC BEVEZETÉS LÉPÉSEI

1.

Felmérés:
Meglevő infrastruktúra felmérése, védendő rendszerek & kockázatok azonosítása

2.

Telepítés, konfiguráció:
SOC appliance telepítése az ügyfélhez, naplóforrások bekötése, konfigurációja.

3.

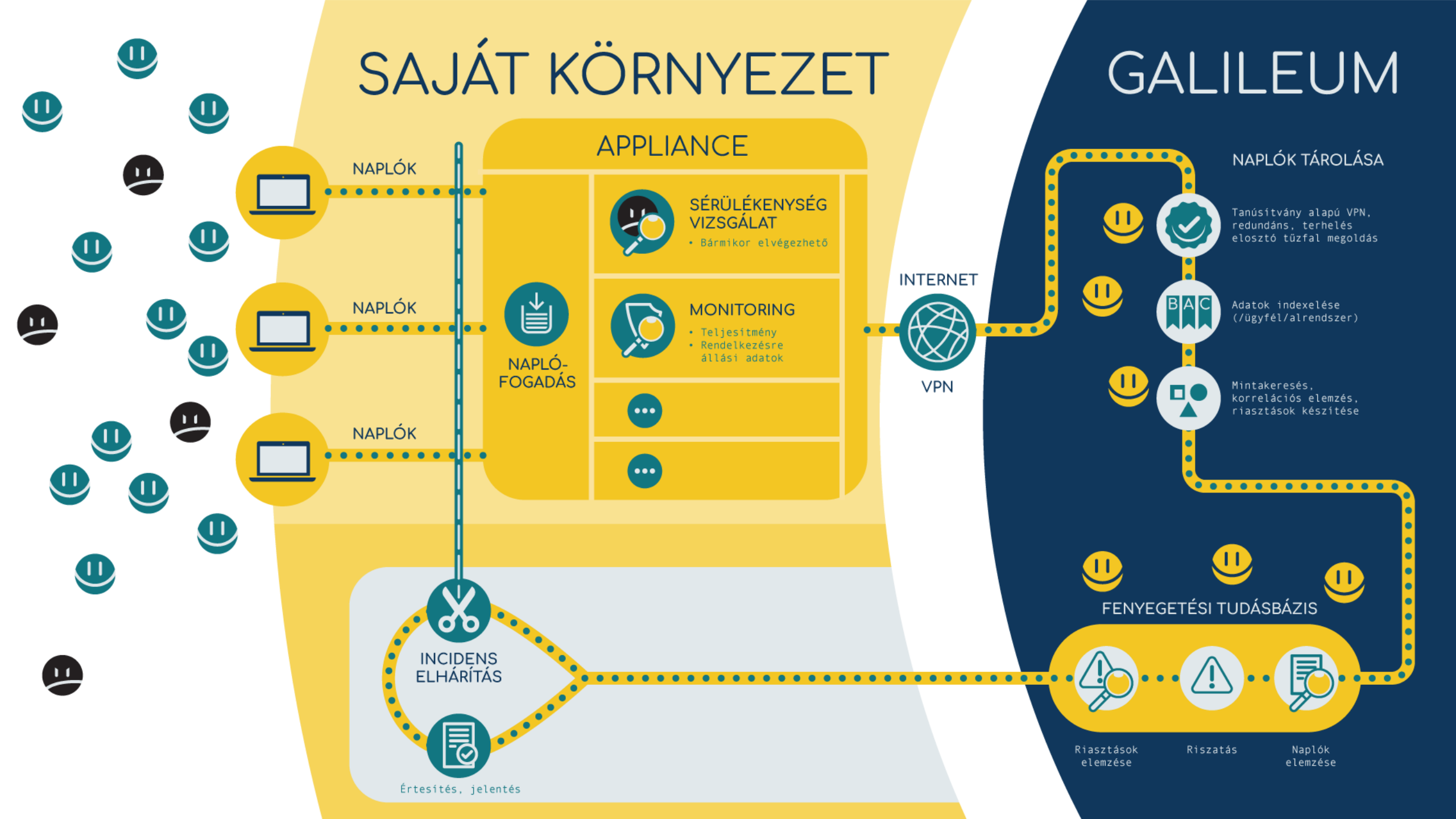
Bevezetés támogatás:
Naplók, riasztások elemzése, false+ riasztások szűrése, jelentés sablonok tesztreszabása

4.

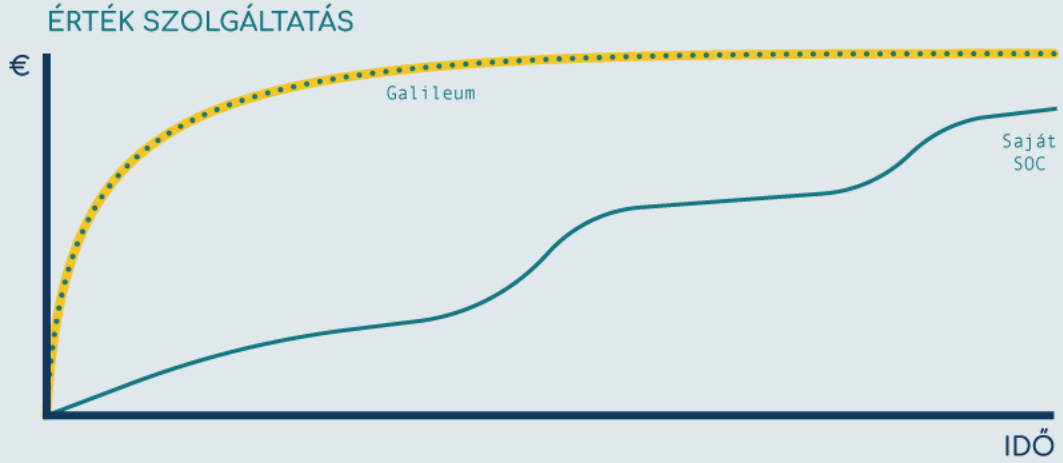
Védelmi intézkedések:
Bevezetés tapasztalatai alapján védett rendszerek megerősítése, szükséges védelem kialakítása

5.

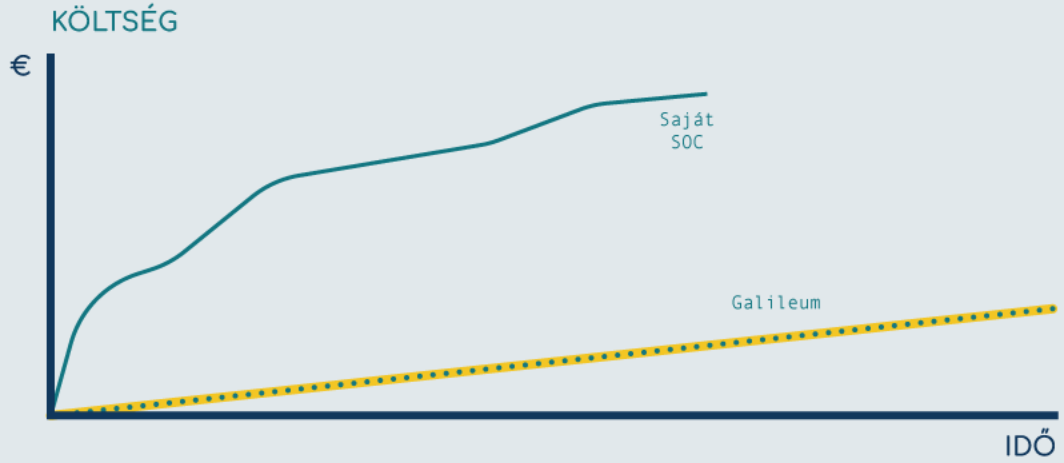
SOC szolgáltatás:
Éles üzemű SOC szolgáltatás az elvárt rendelkezésre állási szint keretében.


SAJÁT KÖRNYEZET
APPLIANCE
NAPLÓK
NAPLÓK
NAPLÓK
NAPLÓ-
FOGADÁS
SÉRÜLÉKENYSÉG
VIZSGÁLAT
• Bármikor elvégezhető
MONITORING
• Teljesítmény
• Rendelkezésre
állási adatok
INTERNET
VPN
GALILEUM
NAPLÓK TÁROLÁSA
Tanúsítvány alapú VPN,
redundáns, terhelés
elosztó tűzfal megoldás
Adatok indexelése
(/ügyfél/alrendszer)
Mintakeresés,
korrelációs elemzés,
riasztások készítése
FENYEGETÉSI TUDÁSBÁZIS
Riasztások
elemzése
Riszatás
Naplók
elemzése
INCIDENS
ELHÁRÍTÁS
Értesítés, jelentés

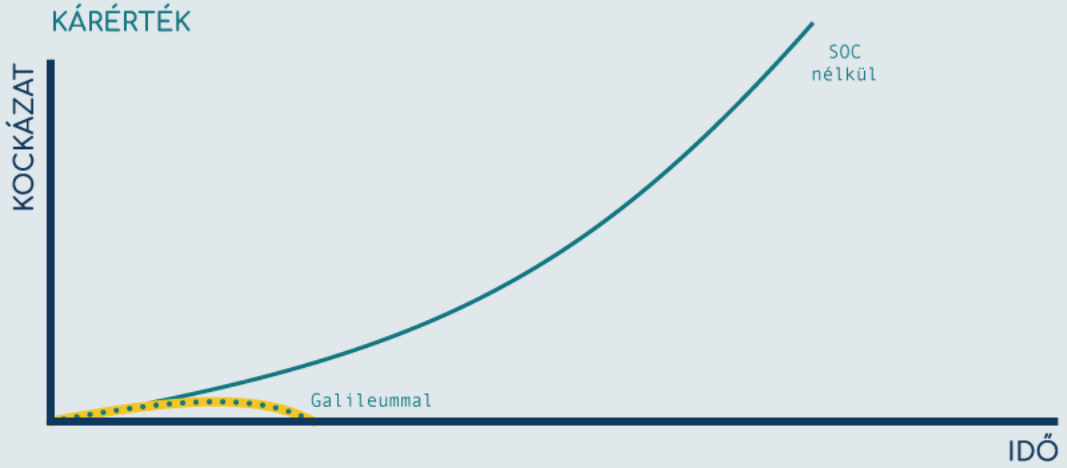
SAJÁT SOC VS KÜLSŐ



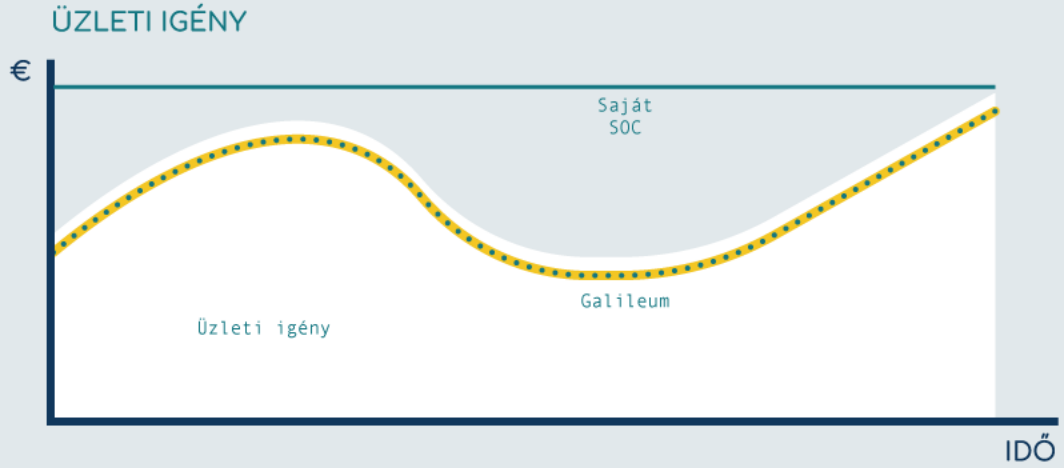
A saját SOC lassan kezd értéket termelni, mert kiépítése gyakran évekig húzódik.



A Galuleum olcsóbb, mint egy saját SOC, hisz zéró kezdeti befektetéssel jár.

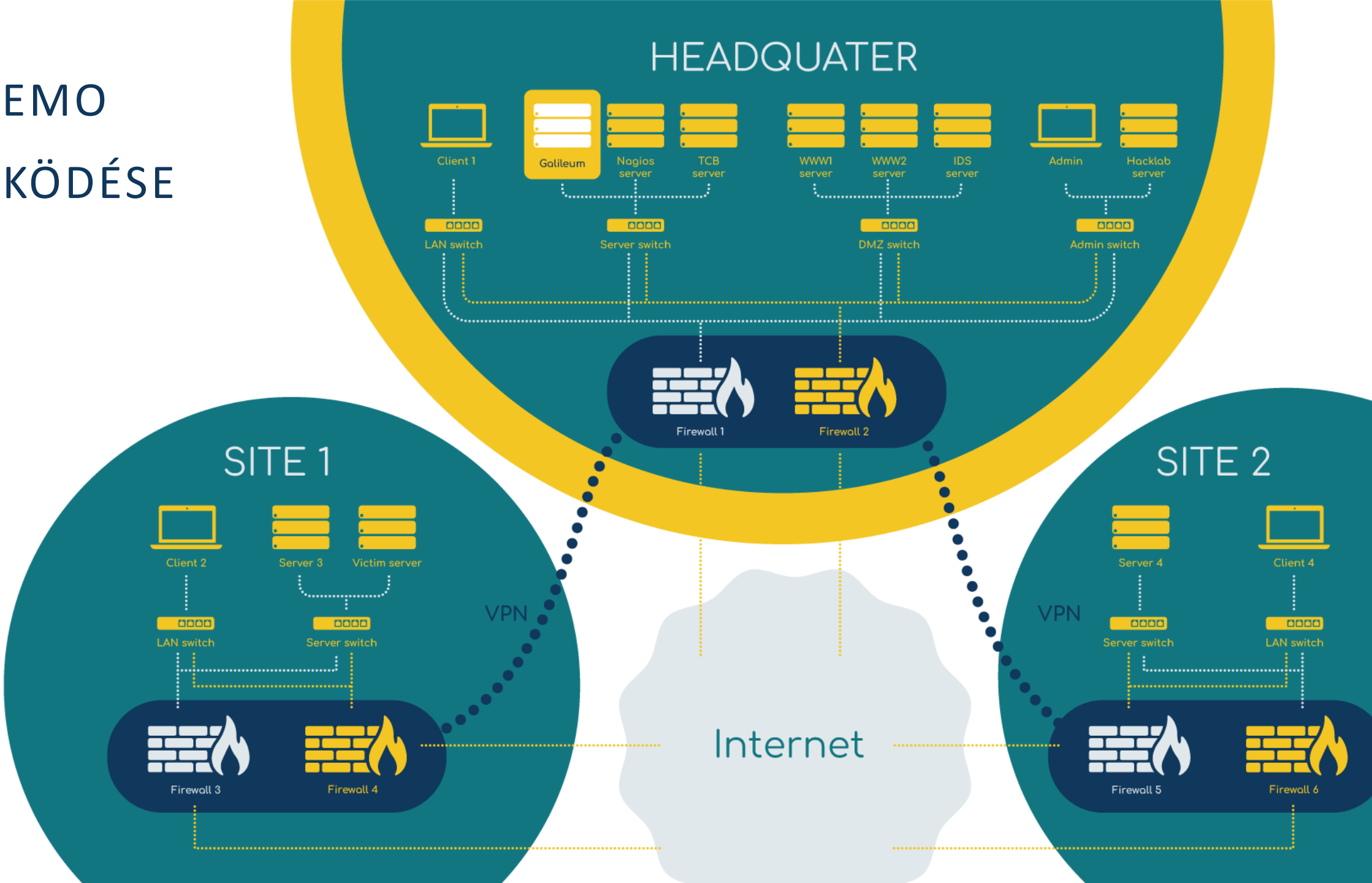


Egy sérülékenységből adódó incidens kockázata idővel folyamatosan nő. A SOC segíti ezek feltárását és támogatja az elhárításukat.



A saját SOC fenntartása költségesebb, hisz nem tud rugalmasan alkalmazkodni pillanatnyi üzleti igényeihez.

A DEMO MŰKÖDÉSE



DEMO ELŐNYÖK

Azonnal kipróbál-ható

A támadások egyszerűen szimulálhatók

PILOT ELŐNYÖK

Nincs induló költség

Elégedettség esetén a rendszer már készen áll az éles használatra

Saját adatokkal kipróbál-ható a rendszer

GALILEUM

ANDREWS
IT ENGINEERING KFT.

1138 Budapest,
Tomori utca 32.
2. emelet

+36 1 428 0600
www.andrews.hu