
SOCURITY
WE PROTECT. YOUR DATA. YOUR USERS. YOUR BUSINESS.

A Socurity IT Kft múltja és jövője

2020

A SOCURITY IT Kft. megalapítása

- Első ügyfelek megszerzése
- Szolgáltatási portfólió meghatározása
- Az első munkatársak megérkezése
- Az első hálózati projektek megvalósítása

2021

ÜZLETFEJLESZTÉS

- Üzletfejlesztési tevékenységek elindítása
- Értékesítés a COVID-időszak kihívásai között
- Az első partnerkapcsolatok kialakítása (Cisco, Palo Alto Networks, Clico)

2022

KÖZÖS ÉRTÉKESÍTÉSI TEVÉKENYSÉG VEZETŐ GYÁRTÓPARTNEREKKEL

IBM Gold Partnerség forgalom és előrejelzés alapján – Software LOB

2023

KÖZÖS ÉRTÉKESÍTÉSI TEVÉKENYSÉG TOVÁBBI TOP GYÁRTÓ PARTNEREKKEL

DELL Gold Partnerség forgalom és előrejelzés alapján – Enterprise HW és kliens LOB

2024

A NAPI MŰKÖDÉS STABILIZÁLÁSA

- 95% távoli+5% közösségi irodai munkavégzés
- A legjobb senior szakértők beválogatása a csapatunkba

AZ ELSŐ AI-ALAPÚ CISCO UCS PROJECT MAGYARORSZÁGON A SOCURITY IT-VAL VALÓSUL MEG

Ügyfelünk, egy biztosítótársaság átfogó Cisco UCS rendszerbeszerzést és a kapcsolódó implementációs szolgáltatásokat rendelte meg a Socuritytől. A projekt Magyarországon az első Cisco AI-ready rendszer bevezetése lesz.

2025

A SOC SZOLGÁLTATÁSAIN KÖVETKEZŐ MÉRFÖLDKÖVE

- 2026. január 1-jétől: állandó Security Operations Center (SOC) helyszín létrehozása – a 7/24 SOC szolgáltatás biztosításának elengedhetetlen feltétele
- NIS2 / DORA integrációs projektek elindítása

2026

SECURITY AS A SERVICE

SECURITY AS A SERVICE

Előfizetéses konstrukcióban elérhető megoldás, amely folyamatos, vállalati szintű kiberbiztonságot biztosít integrált képességeken keresztül, mint a SOC, SIEM, EDR/XDR, SOAR, fenyegetésszimuláció és proaktív tesztelés.
Kiszámítható havi költségeket nyújt, miközben csökkenti a kiberkockázatokat, támogatja a szabályozói megfelelést, és védi az üzletmenetet – mindezt jelentős kezdeti beruházás nélkül.

DNSSEC – Domain Name System Security Extensions

Biztosítja a DNS-válaszok hitelességét és sértetlenségét. Megvédi a felhasználókat a csalárd weboldalakra történő átirányítástól, ezáltal csökkentve a pénzügyi és reputációs kockázatokat.

BAS – Breach and Attack Simulation

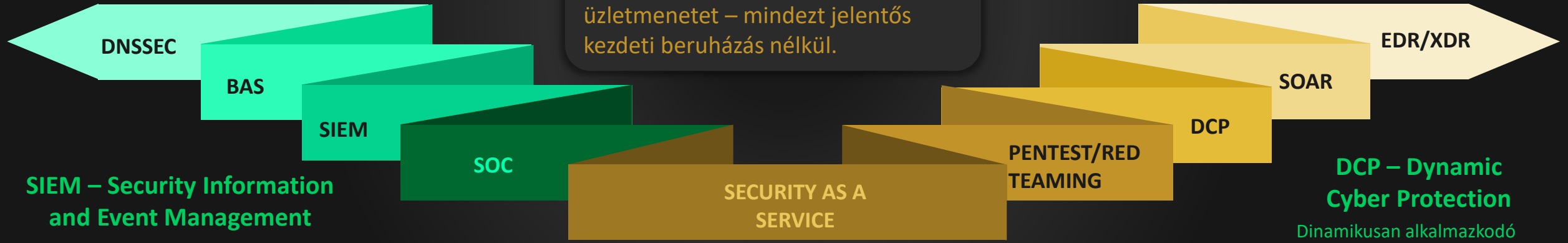
Automatizált technológia, amely kibertámadásokat szimulál a környezet ellen. Biztosítja, hogy a meglévő biztonsági kontrollok valós körülmények között is hatékonyan működnek.

SOAR – Security Orchestration, Automation and Response

Egy platform, amely összehangolja és automatizálja a biztonsági üzemeltetési és incidenskezelési folyamatokat. Csökkenti az üzemeltetési költségeket, és a manuális beavatkozások mérséklésével felgyorsítja az incidenskezelést.

EDR / XDR – Endpoint Detection and Response / Extended Detection and Response

Megoldás a végpontokon és több biztonsági rétegen átívelő fenyegetések észlelésére és kezelésére. Megakadályozza, hogy az incidensek üzletmenet-kieséssé vagy adatvesztéssé súlyosbodjanak.



SIEM – Security Information and Event Management

Központosított platform a biztonsági események gyűjtésére, korrelálására és elemzésére. Támogatja a szabályozói megfelelést, és lehetővé teszi a biztonsági kockázatok korai azonosítását.

SOC – Security Operations Center

Egy központosított szervezet, amely a biztonsági események monitorozásáért és kezeléséért felel. Folyamatos felügyeletet biztosít, lehetővé téve a gyorsabb incidenskezelést, valamint csökkentve az üzemkiesés és a szabályozói szankciók kockázatát.

Penetration Testing vs. Red Teaming

A penetrációs tesztelés konkrét technikai sérülékenységek azonosítására fókuszál, míg a red teaming valósághű, végponttól végpontig tartó támadásokat szimulál. Együttesen segítenek megítélni, hogy a biztonsági beruházások valóban hatékonyan csökkentik-e az üzleti kockázatokat.

DCP – Dynamic Cyber Protection

Dinamikusan alkalmazkodó kiberbiztonsági megközelítés, amely a fenyegetési környezet változásaira reagál. Az aktuális kockázatokhoz igazodva automatikusan módosítja a védelmi intézkedéseket, ezáltal csökkentve az üzemeltetési és pénzügyi kockázatokat.

TANÚSÍTVÁNYAINK

Minőségbiztosítási tanúsítványaink

- ISO/IEC 27001:2022

- EcoVadis Silver Badge, (90% for Ethics)

- CyberVadis Platinum Badge, (986/1000)

Gyártói tanúsítványaink

- 68 egyéni gyártói tanúsítvány 20 különböző vendortól
- 7 egyéni szakértői tanúsítvány (BTL, CompTIA, ISTQB, LetsDefend, LPIC, OSCP+)

SOCURITY

WE PROTECT. YOUR DATA. YOUR USERS. YOUR BUSINESS.

NIS2 AUDIT A GYAKORLATBAN

Hogyan mutasd meg, hogy

- *tudod mit védesz,*
- *miért,*
- *hogyan,*
- *és hogy a védelmed tényleg működik.*

Paulheim Alfonz - Senior cybersecurity mérnök - sales@socurity.hu

10 gyakorlati pont

01 **Scope: Mi tartozik bele?**
(Tudod mit védesz?)

02 **Adat- és üzleti hatás alapú gondolkodás**
(Tudod miért fontos?)

03 **Biztonsági osztályba sorolás**
(Tudod mennyire kell védeni?)

04 **Kontrollok tényleges megvalósítása**
(Tényleg véded?)

05 **Incident Response**
(Tudsz reagálni?)

06 **Business Continuity & Disaster Recovery**
(Üzleti folytonosság)

07 **Beszállítói és cloud kockázat**
(Külső kockázat)

08 **Governance és felelősség**
(Tudod ki a felelős?)

09 **Dokumentáció + evidence**
(Tudod bizonyítani?)

10 **Folyamatos működés**
(Elég érett vagy?)

1. Scope: Mi tartozik bele? (EIR-alapú gondolkodás)

Mit várhat az auditor?

- EIR lista (nem asset lista!)
- Szolgáltatás térkép
- Függőségek (pl. AD, network, cloud, vendor)

Gyakorlatban:

- “Bérszámfejtés” = 1 EIR
- “M365 tenant” = támogató rendszer
- “Gyártásirányítás” = külön EIR, akár OT kapcsolattal

Miért fontos?

HA ROSSZ A SCOPE:

- rossz helyre rakod a kontrollokat
- kritikus rendszerek kimaradnak
- auditon azonnali finding

2. Adat- és üzleti hatás alapú gondolkodás

Mit várhat az auditor?

- Adatosztályozás
- CIA (Confidentiality, Integrity, Availability) értékelés
- üzleti hatás (pl. leállás, reputáció, pénzügyi)

Gyakorlatban:

- Payroll ≠ marketing weboldal
- Termelés leállás = magas availability impact

Miért fontos?

A NIS2 nem azt mondja, hogy “mindenhol MFA kell”, hanem:
“oda tedd, ahol kockázat van”

3. Biztonsági osztályba sorolás (classification)

Mit várhat az auditor?

- EIR → biztonsági osztályozás (alacsony/jelentős/magas)
- dokumentált módszertan
- indokolás

Gyakorlatban:

- SAP → magas
- intranet → alacsony
- AD → mindig magas

Miért fontos?

- Ez az egész rendszer “gerince”, minden kontroll ebből következik
- Ha ez gyenge: az egész compliance “összedől”

4. Kontrollok tényleges megvalósítása (nem papíron)

Mit várhat az auditor?

- Access control (IAM, MFA, PAM)
- Logging / monitoring (SIEM, EDR)
- Patch / vuln management
- Backup + restore teszt
- Network szegmetnáció

Gyakorlatban:

- Nem az számít, hogy “van EDR”
- hanem hogy: Minden kritikus gépen fut? Alertel? Reagál rá valaki?

Miért fontos?

- NIS2 = működő védelem, nem policy
- Auditor itt kérhet: screenshot, log, config export

5. Incident Response (SOC működés)

Mit várhat az auditor?

- Incident process
- jegyek / ticketek
- bizonyíték: történt már IR?

Gyakorlatban:

- SIEM alert → SOC → escalation → IR
- RCA (root cause analysis)
- Containment / eradication / recovery

Miért fontos?

- A hatóságot nem érdekli, hogy “volt támadás”, azt nézi: mit csináltál?

6. Business Continuity & Disaster Recovery

Mit várhat az auditor?

- BCP / DR terv
- restore tesztek
- RTO / RPO

Gyakorlatban:

- backup van → de restore nincs tesztelve
- DR plan van → de senki nem ismeri

Miért fontos?

- Ransomware esetén ez a túlélés

7. Beszállítói és cloud kockázat (supply chain)

Mit várhat az auditor?

- vendor lista
- security követelmények szerződésben
- cloud risk assessment
- exit strategy

Gyakorlatban:

- M365, AWS, SAP vendor = kritikus
- outsourcing SOC → ugyanúgy scope-ban van

Miért fontos?

- A támadások nagy része itt jön be

8. Governance és felelősség (nem csak IT)

Mit várhat az auditor?

- kijelölt EIR Biztonsági felelős (IBF)
- vezetői jóváhagyás
- szerepkörök (RACI mátrix)

Gyakorlatban:

- CISO + IT + business együtt
- Nem lehet “IT problémának” eltolni

Miért fontos?

- NIS2 = vezetői felelősség
- Ez jogi, pénzügyi, reputációs kérdés

9. Dokumentáció + evidence (a legfontosabb)

Mit várhat az auditor?

Mindenre bizonyíték! Tipikus bizonyítékok:

- asset/EIR lista
- risk assessment
- policy
- SIEM dashboard
- patch report
- backup log
- incident ticket

Gyakorlatban:

- Ami nincs dokumentálva = nem létezik

Miért fontos?

- Ez különbözteti meg: a “jó SOC”-ot, az “auditált SOC”-tól

10. Folyamatos működés (nem projekt)

Mit várhat az auditor?

- rendszeres review
- javító intézkedések
- maturity fejlődés

Gyakorlatban:

- yearly review
- lessons learned
- tabletop exercise

Miért fontos?

- NIS2 nem egyszeri megfelelés, hanem egy **működési modell**

Források

- https://www.egve.hu/downloads/utmutato_nis_2_kiberbiztonsagi_iranyelv_2024.pdf
- https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32021R0887
- https://njt.hu/jogszabaly/2024-69-00-00
- https://njt.hu/jogszabaly/2024-418-20-22
- NIS2: ki legyen az információs rendszerek biztonságáért felelős személy? – Jogászvilág
- IBF Képzések listája - Nemzeti Koordinációs Központ

Magyarország vonatkozó jogszabályai:

- 2024. évi LXIX. törvény *Magyarország kiberbiztonságáról:* https://njt.hu/jogszabaly/2024-69-00-00
- 418/2024. (XII. 23.) Korm. rendelet *Magyarország kiberbiztonságáról szóló törvény végrehajtásáról:* https://njt.hu/jogszabaly/2024-418-20-22
- 7/2024. (VI. 24.) MK rendelet *A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről*: https://njt.hu/jogszabaly/2024-7-20-7G
- *1/2025 SZTFH* rendelet *a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról*: https://njt.hu/jogszabaly/2025-1-20-8K
- 2/2025 SZTFH rendelet *a kiberbiztonsági felügyeleti díjról*: https://njt.hu/jogszabaly/2025-2-20-8K
- 17/2025. (VII. 24.) EM rendelet a *Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelményekről*: https://njt.hu/jogszabaly/2025-17-20-8Y
- 2024. évi LXXXIV. törvény *a kritikus szervezetek ellenálló képességéről*: https://njt.hu/jogszabaly/2024-84-00-00
- 474/2024. (XII. 31.) Korm. rendelet *a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról*: https://njt.hu/jogszabaly/2024-474-20-22

NIS2 irányelv jogszabályi hivatkozások

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az *(EU) 2016/1148 irányelv* hatályon kívül helyezéséről (NIS 2 irányelv): https://jogkodex.hu/doc/2549655

Köszönöm a figyelmet!

Lépjen velünk kapcsolatba:

sales@socurity.hu
+36 70 375 2623