



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

ADAPTÁCIÓ HELYETT ELŐRELÁTÁS – NIS2 ÉS THREAT INTELLIGENCE A GYAKORLATBAN

Paulheim Alfonz

Senior cybersecurity mérnök
sales@socurity.hu

MKET konferencia, 2026.03.10. , Mátraháza



Adaptáció helyett
előrelátás:
*Threat Intelligence a
gyakorlatban*

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



NIS2 megfelelés magyar
vállalatoknak

*Vezetői nézőpont
erőművek és kritikus infrastruktúrák
számára*



Rólunk röviden

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



Cégünk széles körű tapasztalattal rendelkezik a kiberbiztonsági és hálózati megoldások teljes spektrumában. Az iparág meghatározó gyártóival szoros partneri kapcsolatot építettünk ki, többségükkel silver vagy gold szintű partnerségi státusszal. Ennek köszönhetően ügyfeleink számára magas színvonalú, testre szabott megoldásokat és szolgáltatásokat tudunk biztosítani, amelyek pontosan illeszkednek egyedi biztonsági igényeikhez.



Kiberbiztonsági fókusz, niche technológiák, senior szintű szakértelem a csapatban, folyamatos növekedés, iparági specializációk

SECURITY AS A SERVICE



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.

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.

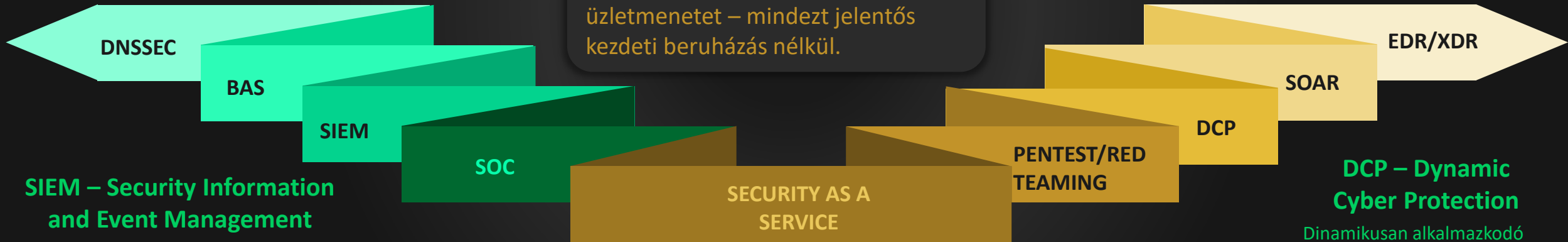
Kiszámítható havi költségeket nyújt, miközben csökkenti a kiberkockázatokat, támogatja a szabályozói megfelelést, és védi az üzletmenetet – mindezt jelentős kezdeti beruházás nélkül.

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 valóság-hű, végponttól végpontig tartó támadásokat szimulál. Együttesen segítenek megítélni, hogy a biztonsági beruházások valóban hatékonyan csökkentik-e az üzleti kockázatokat.

DCP – Dynamic Cyber Protection

Dinamikus 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.

Mi a NIS2 irányelv?

Szabályozás

01

EU-s kiberbiztonsági szabályozás kritikus szolgáltatóknak

Kötelezettség

02

Kötelező kockázatkezelés és incidensjelentés

Felelősség

03

Vezetői felelősség és auditálhatóság

Magyarországi NIS2 elvárások

01 Folyamatos
kockázatelemzés

03 Dokumentált és
bizonyítható kontrollok

02 24 órán belüli
incidensértesítés

04 Hatósági ellenőrzések
lehetősége

Szükséges képessegek

NIS2-re felkészült szervezet számára

01

Folyamatos monitoring és észlelés

02

Threat Intelligence

03

Incidenskezelés és reporting

04

**Sebezhetőség kezelés és beszállítói
kockázatkezelés**

01

Fenyegetésintelligencia és reporting
- QuoIntelligence

02

SIEM/XDR – technikai észlelés és
válasz- IBM Qradar

03

GRC – governance és
dokumentáció

Megoldási kategóriák

NIS2 felkészültséghez

Fő értékajánlat



- A Quointelligence egy európai fejlesztésű cyber threat intelligence platform.
- **Nyílt, zárt és dark web forrásokból gyűjt és elemez** fenyegetettségi információkat.
- **Segít korán azonosítani** a szervezetet érintő kibertámadási kockázatokat.
- **Vezetői dashboardokon** mutatja a releváns kockázatokat és trendeket.
- Támogatja a **NIS2 szerinti** kockázatmonitorozást és döntéshozatalt.



CTI – Cyber Threat Intelligence

Külső és belső forrásokból származó fenyegetési információk gyűjtése és elemzése annak érdekében, hogy a szervezet előre felismerje a releváns támadási mintákat és fenyegető szereplőket.

SIEM / XDR – fő értékajánlat



Mély technikai átláthatóság



Automatikus riasztás és válasz



Központosított logkezelés



Komplex infrastruktúrákhoz ideális

- **SIEM – Security Information and Event Management**
Központi rendszer, amely az IT infrastruktúra naplóadatait gyűjti, elemzi és korrelálja, hogy azonosítsa a biztonsági eseményeket és potenciális támadásokat.
- **EDR – Endpoint Detection and Response**
Végpontvédelmi technológia, amely folyamatosan monitorozza a végpontokon zajló tevékenységeket, és képes észlelni és kezelni a gyanús vagy rosszindulatú aktivitásokat.
- **XDR – Extended Detection and Response**
Kiterjesztett észlelési és válaszplatform, amely több biztonsági réteg (endpoint, hálózat, cloud, email) adatait integrálja az összetettebb támadások hatékonyabb felismeréséhez.

GRC rendszerek szerepe

GRC – Governance, Risk & Compliance

- **Governance:** a szervezet irányítási és döntéshozatali keretrendszere, amely meghatározza a felelősségeket, szabályokat és kontrollokat.
- **Risk:** üzleti, IT- és kiberkockázatok azonosítása, értékelése és kezelése strukturált módszertan alapján.
- **Compliance:** a szervezet működésének biztosítása a jogszabályi, szabványi és belső szabályzati követelményeknek megfelelően.
- **Cél:** a kockázatok átlátható kezelése, a megfelelés biztosítása és a vezetői döntéshozatal támogatása integrált keretrendszerben.



Működési kockázat csökkentése

A digitalizáció az üzemi kockázatokat is átalakítja

Digitális működés és ellátásbiztonság az erőművekben

A kiberkockázat ma már működési kockázat

Vezetői szemlélet

Intelligence + Detection + Governance

Ajánlott kombinált megközelítés

Technológia és folyamat együtt

Teljes NIS2 megfelelés



Digitális működés és ellátásbiztonság az erőművekben – vezetői nézőpontból

Mi változott meg az erőművek működésében?

RÉGEN

- helyi, emberi döntések
- elszigetelt vezérlés
- a problémák fizikai formában jelentkeztek

MA

- szoftverek hoznak döntéseket
- automatizált működés
- rendszerek össze vannak kötve

KÖVETKEZMÉNYEK

a digitális rendszerek:

- teljesítményt szabályoznak
- leállítanak / átkapcsolnak,
- vészhelyzetre reagálnak
- Az IT közvetlenül hat a fizikai termelésre

Digitális működés és ellátásbiztonság az erőművekben – vezetői nézőpontból

Nem azért történik üzemzavar, mert:

- eszközhiba történik

Hanem mert:

- hibás adat érkezett
- külső beavatkozás történt
- a rendszer nem a valóságot „látta”

Mit jelent, ha egy „digitális döntés” rossz?



A kockázat nem a számítógépen, hanem a szolgáltatásban jelentkezik. –
Üzemzavar lesz a következmény

Következmények

- indokolatlan leállítás
- ellátási zavar
- lakossági panasz
- reputációs kár

A NIS2 lényege vezetői nyelven

01

Nem paragrafusokról és
technikai részletekről szól

02

A digitális kockázatok a
kritikus szolgáltatásokat
veszélyeztetik

03

A kiesés nem elfogadható

04

A NIS2 a
felkészületlenséget
bünteti, nem a hibát

Miért vezetői felelősség?

Mert incidensnél vezetői döntések születnek

Például:

- leállítjuk-e a termelést?
- mikor indítjuk újra?
- ki kommunikál a hatósággal?
- mit mondunk a lakosságnak?

” Ezek nem IT-döntések, hanem vezetői döntések ”

Mit vizsgálnak egy incidens után?

- milyen vírus volt?
- milyen tűzfal futott?

Nem azt, hogy

Hanem azt, hogy

- fel voltunk-e készülve?
- időben felismertük-e?
- tiszták voltak-e a felelősségi körök?
- megfelelő volt-e a reakció?

A kiberincidens vezetői kérdésekkel kezdődik, de nem a technikaiakkal végződik.

Erőmű-specifikus vezetői kockázatok

Beszállítói hozzáférések

- karbantartók
- rendszerintegrátorok
- külső szakértők

Tudjuk, ki, mikor, mihez fér hozzá?

Régi vezérlőrendszerek

- nem mai környezetre tervezve
- működnek, de sérülékenyek

Meddig vállalható ez a kockázat?

Új digitális fejlesztések

- optimalizálás
- távfelügyelet
- Hatékonyságnövelés

A kockázat is nő velük együtt

Mit vár el a NIS2 ezekre a kérdésekre válaszul?

ne fejlesszünk

Nem azt, hogy

Hanem azt, hogy

- értsük a kockázatokat
- tudatosan kezeljük őket
- vállaljuk a döntések következményeit

Nem technikai feladatlista, hanem kérdések

Mit jelent ez vezetőként a gyakorlatban?

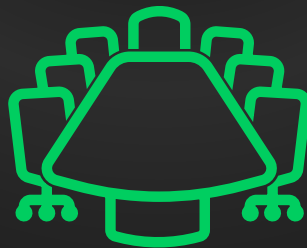


- Van-e átfogó képünk a digitális kockázatokról?
- Tudjuk-e, mi kritikus?
- Van-e incidens-forgatókönyv?
- Tudjuk-e, ki dönt vészhelyzetben?
- Gyakoroltuk-e ezt valaha?

„A felkészültség nem a hibátlanságot, hanem a kezelhetőséget jelenti.”

Záró üzenetek

- A kiberbiztonság az üzemi kockázatkezelés része lett
- A felkészültség kezelhetőséget és kontrollt jelent
- Az erőművek kiberbiztonsága ma már vezetői felelősség



Köszönöm a figyelmet!

Lépjen velünk kapcsolatba:

sales@security.hu

+36 70 375 2623