

informatikai osztályvezető

Székesfehérvári Épületfenntartó és Hőszolgáltató Zártkörűen Működő Részvénytársaság



SZÉPHŐ

- 24.000 fogyasztó
- 248 fős dolgozói létszám (KKV.)
- 6 fős informatikai csapat

Nem vagyunk egyformák, sem működésben, sem szervezetileg, sem lehetőségeink tekintetében, de leginkább az informatikai érettségünk lehet eltérő.

Megnézzük az utat amit bejártunk, a kihívásokat amivel szembesültünk, és néhány megoldást amivel válaszoltunk ezen kihívásokra!





SZEPHŐ

- 2023. **Augusztus** – Helyzet van ...
„Te jó ég mi ez már megint”, „Ez sokkal nagyobb falat lesz mint a GDPR”
- 2023. **Október** – GAP analízis elvégzése (41/2015 BM rendelet)
„Nem állunk valami fényesen, azért szakmailag jók az alapok de szükségünk lesz új képességekre, a szabályzatainkat pedig újra kell alkotnunk”, „Mennyibe fog ez kerülni?”, „Ki fogja ezt megcsinálni?”
- 2023. **November** – Cselekvési terv összeállítása, vezetői elköteleződés megteremtése, beruházás tervezés
- 2024. **Január** – Külsős tanácsadó cég megbízása az Információ Biztonság Irányítási Rendszer kialakítására
- 2024. **Február** – Megjelenik a vhr. normaszövege (2.sz. melléklet), 19. fejezetben csaknem 900 követelmény alap/jelentős/magas besorolással, ami alapján végre elkezdődhet a konkrét szakmai munka, a megfelelés biztosítása érdekében
- 2024. **Március** – IBF. pozíció betöltésre kerül, bejelentkezés az SZTFH.-hoz. - Form 420 - (EIR. nyilvántartás + osztályba sorolás, közreműködők, hírközlési szolgáltatók)
- 2024. **Április** – Nagyrészt befejeződnek a beruházási terv részeként beszerzendő szoftverek és megoldások kiválasztása, (ajánlatkérések, tesztelések, Proof of Concept telepítések, szerződéskötés) és elindulhatnak a bevezetések
- 2025. **Május** – Véget érnek a személyes interjúk (IT., HR., Beszerzés), a követelmények teljesítésének dokumentálása (excel tábla), elkezdődnek a kockázatkezelési és üzletmenet folytonossági felmérések a BCP.-hez
- 2024. **Június** – Elkezdődik a szabályzatok kiadása a követelmény csoportok alapján



SZEPHŐ

- **Komoly emberi erőforrás lekötöttséget jelent a felkészülés**
 - Belső projekt vezető, IBF., IT. vezető, HR. vezető, PD. vezető, OT. vezető, BCP.-hez az üzleti folyamatokért felelős vezető kollégák
 - IT. személyzetnek a normál megszokott üzemeltetési és támogatási feladatokon felül extra terhet jelent a megfelelőség biztosítása, az alkalmazandó megoldások bevezetése
- **Nem statikus az elérendő állapot, folyamatos utógondozást és rendszeres felülvizsgálatot igényel a kialakított szabályozási környezet**
- **Sok még a bizonytalanság**
 - Mi történik ha változik a bejelentkezéskor megadott állapot (EIR, közreműködők, IBF)
 - Nincs véglegesítve a követelményrendszer, még mindig a februári társadalmi egyeztetésre kiadott tervezet alapján lehet csak dolgozni, hiányoznak a „beígért” szakmai segédletek
<https://kormany.hu/dokumentumtar/biztonsagi-osztalyba-sorolas-es-alkalmazando-vedelmi-intezkedesek-min-rendelet>
 - Az egyes követelmények mögötti szakmai tartalom sok esetben homályos (tükörfordítás, de segít a NIST SP 800-53 szabvány
<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>)
 - Nincs meghatározva az incidenskezelés folyamata (az ismert elvárás a 24 órán belüli incidens jelzése, majd a 72 órán belüli kivizsgálása), a kijelölt hatóság (CSIRT)
 - A megfelelőségértékelési szervezetek jegyzéke jelenleg 2 engedélyest számlál!

Fizikai és környezeti védelem

- Beléptető rendszer
- Kulcs nyilvántartás, kulcsfelvétel rendje, vendégek nyilvántartása (GDPR)
- Vagyonvédelmi rendszerek alkalmazása átjelzéssel (tűzvédelem, riasztó)
- Klimatizálás biztosítása, hőmérséklet – és páratartalom riasztás, elárasztás elleni védekezés
- Követelmény a szünetmentes táplálás (UPS), de nem követelmény az aggregátoros üzem
- Vészvilágítás kiépítése



SZÉPHŐ

Határvédelem



STORMSHIELD



SOPHOS



FORTINET

- **NextGen Firewall (NGFW) tűzfal**
 - Antivirus Engine, Spamfilter, Geolocation, Application Control, Web filter, Intrusion Detection System (IDS), Virtual Private Network (VPN)
 - Szabályok rendszeres felülvizsgálata, változások követése, megjegyzések használata, idő limitált kivételek
 - Közösségi média (Facebook, Tiktok), webmail (Freemail, Gmail), tárhely szolgáltatások (Google, Onedrive) tiltása amennyiben üzletileg nem indokolt a használatuk!
- Levélszemét szűrő megoldás
- **Webes alkalmazás tűzfal (WAF)** – magas kitettségű webalkalmazások védelmére pl.: ügyfélszolgálat, Outlook Web Access

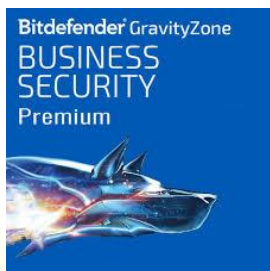
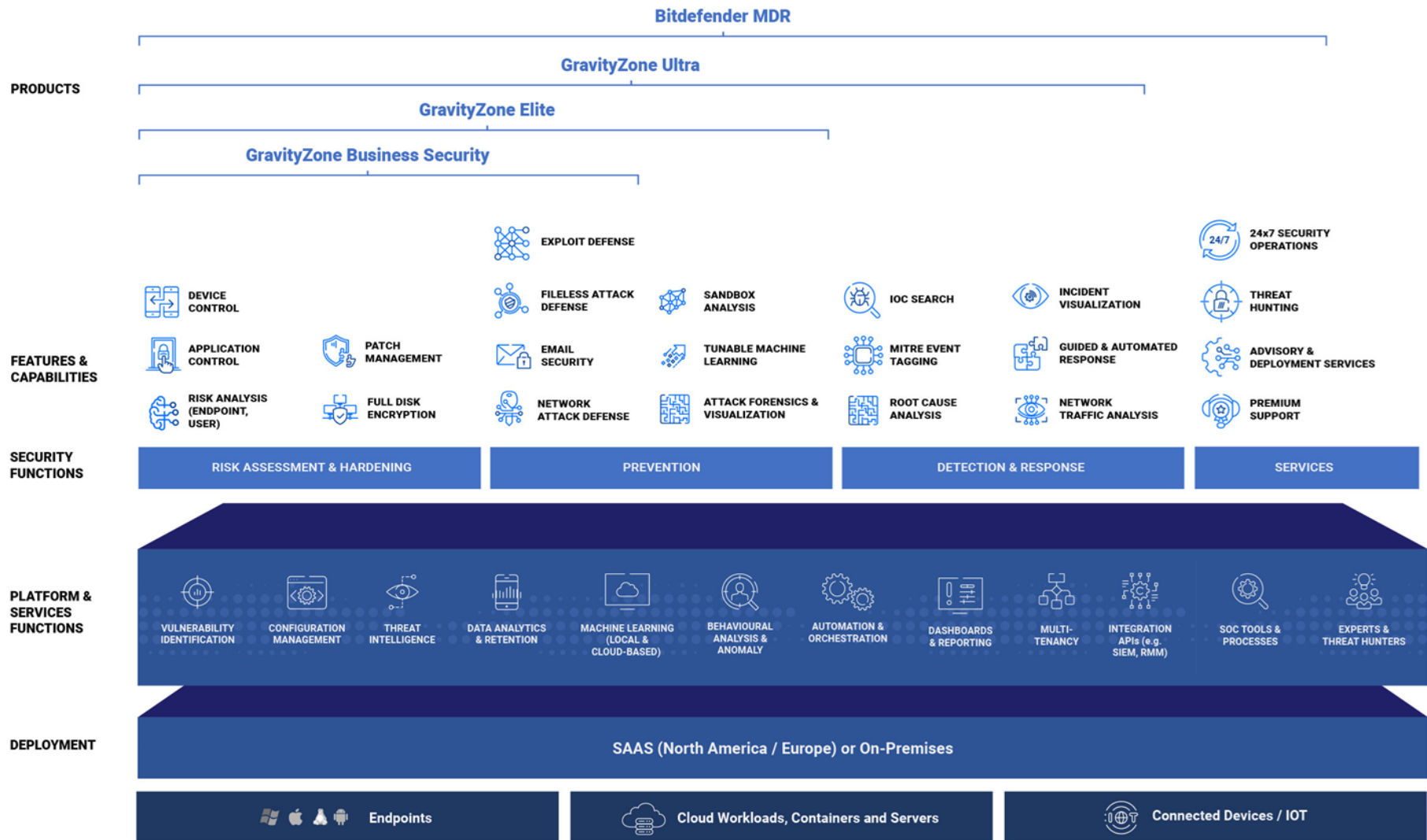


Végpont védelem

- **Endpoint protection (EPP)**
 - Nevezük „hagyományos” vírusvédelemnek helyi tűzfallal kiegészítve
- **Endpoint Detection and Response (EDR)**
 - Viselkedés elemzés, fenyegetések észlelése, átfogó rálátás a végpontokra
- **Extended Detection and Response (XDR)**
 - Fokozott védelem a több vektoros támadásokkal szemben a biztonsági adatforrások összekapcsolásával (Network, Identity), *automatizált válaszadás képességével az incidensekre, az IT. biztonsági személyzet terheinek csökkentése mellett*
- **Managed Detection and Response (MDR)**
 - Szolgáltatásként kínált egyedi igényekre szabott legmagasabb szintű védelem
- **Egy modern EDR/XDR végpontvédelmi megoldás által biztosított hozzáadott érték**
 - Device Control – végponti eszközök tiltása, kivétel lehet a titkosított USB pendrive
 - Risk Analysis – Folyamatos kockázati szint értékelése a különböző források által biztosított adatok alapján (OS konfiguráció, felhasználói viselkedés, hálózati forgalom, fenyegetettség mértéke, ismert sérülékenységek alapján)
 - Vulnerability & Patch management – Javítások, foltozások folyamatos és automatizált telepítése (OS & 3rd party) az ismert sérülékenységekre való figyelmeztetés mellett (CVE score)
 - Disk Encryption (Bitlocker) – Laptop merevlemezek titkosítása
 - Application Control – Nem kívánatos alkalmazások használatának tiltása
 - Incident Visibility & Forensics – Szervezet szintű támadási vektor megjelenítése, és a bizonyítékok „nyomozati anyagként” való előkészítése



Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

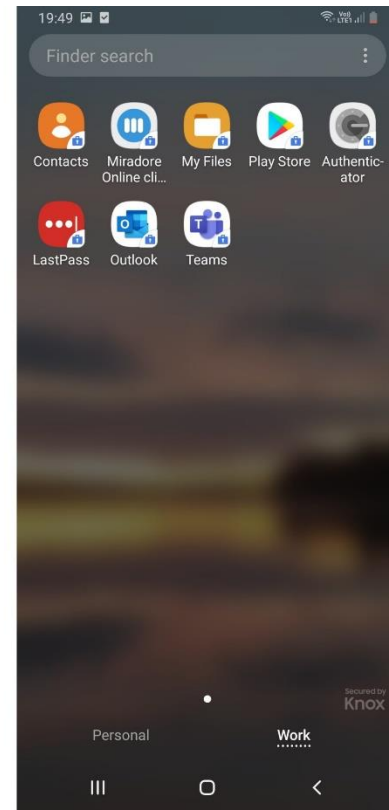
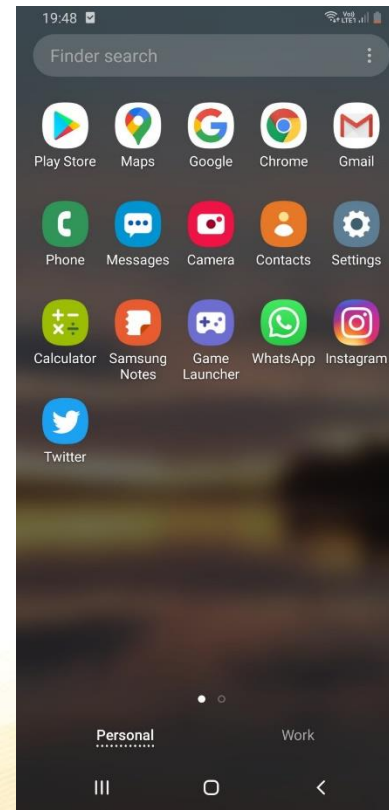


Mobil eszközök védelme

A telefon is számítógép, védeni kell főleg ha vállalati applikációk is elérhetők rajta (levelezés, intranet)



- **Mobile Threat Defense (MTD)**
Mobil eszközre optimalizált végpontvédelem (Wifi, malware, phishing, sérülékenységek jelzése, frissítések telepítése – OS is)
- **Mobile Device Management (MDM, EMM, UEM)**
Mobil eszközök távfelügyeletére szolgál, amivel az eszközök biztonsági beállításai kikényszeríthetők, az eszközök felderíthetők és távolról törölhetők (wipe), alkalmazások telepíthetők, illetve a vállalati applikációk személyes- és munka profilok használatával elkülöníthetők (Android Enterprise)

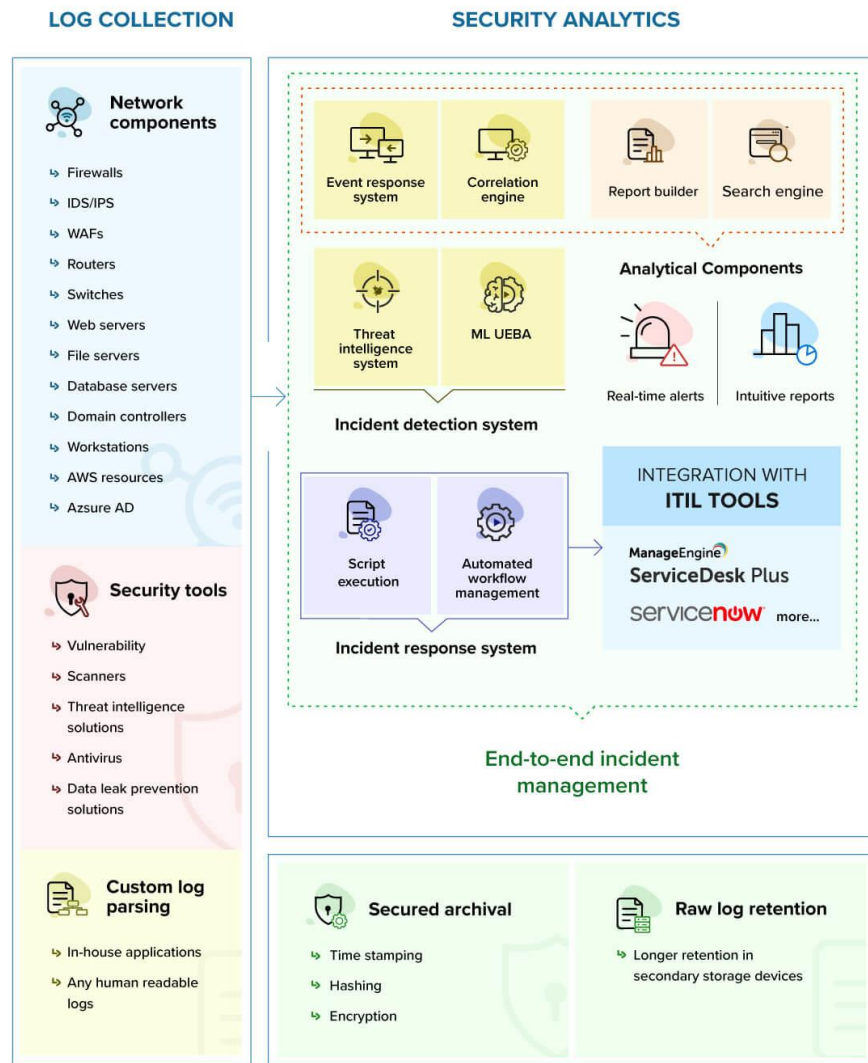


Naplózás, loggyűjtés, SIEM rendszer

- A biztonsági eseményeket gyűjteni kell, ráadásul meg is kell határozni a típusait és forrásait, ügyelve a beérkező információk szűrésére, különben nagy lesz a zaj.
- Forrás kell legyen az EIR. maga, illetve a kiszolgáló infrastruktúra, valamint egyéb alkalmazott biztonsági megoldások
 - Microsoft SQL szerver, MySQL szerver
 - Szerverek -> Windows Event Logs
 - Hálózati eszközök (Switch, Firewall)
 - Biztonsági termékek (WAF, XDR, MTD)
- Hosszabb ideig történő megőrzés biztosítása
- Security Incident&Event Management (SIEM)
 - Korrelációs képesség, anomália érzékelés
 - Automatizált munkafolyamatok
 - Incidens generálás és követés, a nyomozati információk összeállításával



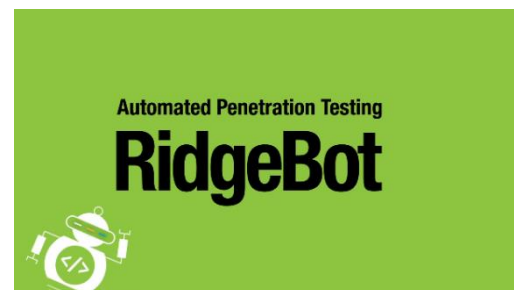
SZEPHŐ



Sérülékenység vizsgálat

NIS2 követelmény az időszakos sérülékenységvizsgálatok elvégzése, mely terület eléggé szerteágazó, különféle módszertanokat követve „önálló szakma” a szakmán belül.

- A behatolás vizsgálat lehet élőerős vagy automatizált forgatókönyv alapú, módszertan alapján Blackbox vagy What/If – Greybox, lépései pedig az alábbiak:
 - Scanning – Feltérképezés
 - Enumeration – Számbavétel
 - Sniffing Credentials – Hitelesítő adatok megszerzése
 - Password cracking – Jelszó feltörés
 - Relay – Lehallgatás
 - Remote Code Execution (RCE) and Defense Evasion - Távoli kódvégrehajtás (RCE) és védelem megkerülése
 - Data Gathering – Adatgyűjtés
 - Lateral movement - hálózati szegmensek átjárhatóság tesztelése
 - Privilege escalation – Emelt szintű hozzáférés megszerzése
 - Data Exfiltration and C&C – Adat kinyerés és parancs eltérítés
 - „Impact” – Hatáskeltés
- Webalkalmazások vizsgálata külön módszertan alapján (OWASP Top 10)
- Léteznek licenszelhető sérülékenységvizsgálati szkennerek alkalmazások is, amikkel tömeges vizsgálatokat lehet elvégezni (Tenable Nessus, Rapid7), emellett automatizált forgatókönyv alapú Machine Learning támogatott behatolás vizsgáló platformok is (Ridgebot, Pentera)



Multifaktoros azonosítás (MFA)

NIS2 követelmény az MFA teljeskörű bevezetése az EIR.-ek védelmében, és nem csak a privilegizált felhasználók számára!



- VPN alapú távoli munkavégzés esetén
- Kívülről elérhető webes felületek esetén (pl.: Outlook Web Access - OWA)
- RDP és SSH alapú rendszergazdai hozzáférések esetén (RADIUS integráció)
- Minden alkalmazás esetén ami támogatja az MFA használatát!
- Mi legyen a „legacy” alkalmazásokkal, a vastag kliens-ként telepített programokkal amik egyáltalán nem készültek fel az MFA használatára?
 - Amennyiben Active Directory címtár alapú az adott EIR.-ben a felhasználó azonosítás, úgy LDAP proxy használható ami beépíti a 2. faktoros azonosítást az LDAP lekérdezés folyamatába
 - A Windows tartományi bejelentkezés folyamatába is beépíthető a 2. faktor ...
- Az MFA azonosításhoz felhasználható Token lehet:
 - mobil alkalmazás (Google/Microsoft authenticator, adott gyártó saját alkalmazása)
 - Hardver token (Yubikey, Token2, Thales)



GreenRocket
Security



Ipari rendszerek kiberbiztonsága

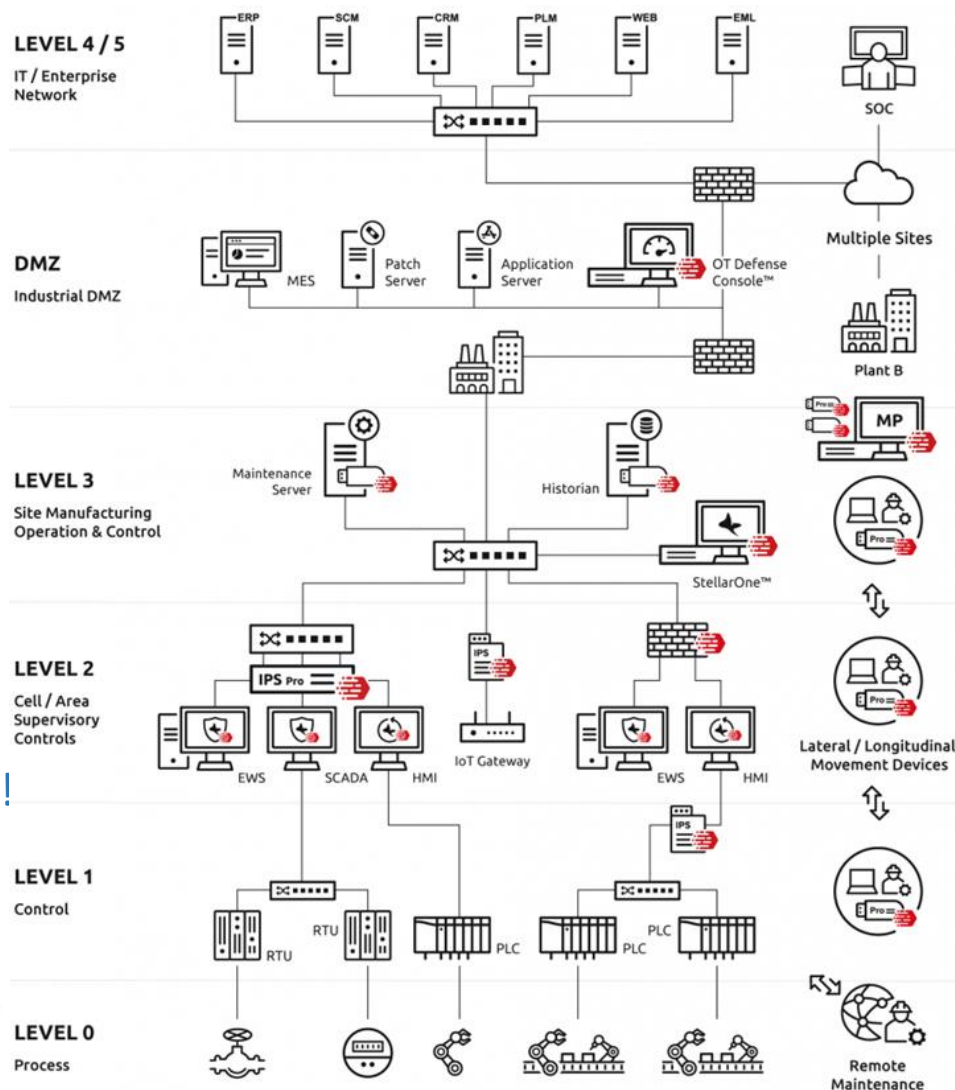
- Information Technology (IT) <-> Operation Technology (OT)
- Teljesen eltérő szemléletmód, 20-30 éves lemaradásban van az OT
- Össze kell hangolni a zéró IT. biztonsággal tervezett ipari protollokat az IT. környezetek megjelenése miatti biztonsági elvárásokkal
- Érintettek a PLC-k, HMI-k, IPC-k, egyéb ipari eszközök (switch, konverter), **TELEKONT Daisy 402/520**, SCADA rendszerek

Védelmi intézkedések:

- OT leltár összeállítása (lássuk)
- Firmware és OS verziók alapján az ismert sérülékenységek meghatározása (tudjuk)
- Firmware frissítések elvégzése (tegyünk)
- IT/OT hálózati határok szegmentálása (korlátozott átjárhatóság)
- **Ipari tűzfalak illetve Behatolásjelző eszközök (IPS/IDS) alkalmazása, szükség esetén Airgap!**
- Elavult operációs rendszerek védelme, virtuális patcheléssel, Learning&Protect



SZÉPHŐ



ITIL folyamatok bevezetése

Az ITIL (Information Technology Infrastructure Library) az informatikai szolgáltatásmenedzsment jól bevált gyakorlatainak gyűjteménye, egy keretrendszer az informatikai folyamatok életciklusának követésére, melynek támogatására dobozos szoftver megoldások állnak rendelkezésre.



- **Eszköz leltár - Asset Management**
 - A hálózatban fellelhető eszközök automatikusan leltárba kerülnek a hardver jellemzőikkel, a telepített szoftverekkel. A nyilvántartás egyedi mezőkkel bővíthető, akár külsős rendszerekből is importálhatók adatok, pl.: vállalatirányítási rendszer leltár és beszerzési modul
- **Szolgáltatásmenedzsment – Service Management (Help-desk)**
 - Incidensek, hibák és szolgáltatás kérések rögzíthetők, a megoldás folyamata zárt rendszerben követhető, jól dokumentálható. SLA szintek határozhatók meg, eskalációs- és jóváhagyási folyamatok indíthatók, nagyfokú automatizáció mellett.
- **Változásmenedzsment – Change Management**
 - A változások jól dokumentált, folyamat vezérelt eljárásként valósulhatnak meg a legjobb gyakorlatok alapján. (igény->tervezés->döntés->megvalósítás->felhasználói teszt->végleges kiadás->véleményezés)
- **Szoftver kiadások, Megoldás gyűjtemény, Konfigurációk kezelése, ...**



Mire figyeljünk oda a már jól bevált üzemeltetési gyakorlatunkon felül?



SZEPHŐ

- Legyen biztonságos, automatizált, könnyen felügyelhető mentési rendszerünk
- A mentéseket ellenőrizzük vissza, tároljuk eltérő helyen
- Legyen elkülönített tartalék üzemeltetési környezetünk vészhelyzetre, ahová rendszeresen (napi szinten) replikálunk a mentésből
- Rendelkeznünk kell berendezett tartalék munkavégzési hellyel is (bútorzat, számítógép, internet – legalább az ügyfélszolgálat és a műszaki szolgálat számára)
- Minden esetben válasszuk szét az adminisztrációs/rendszergazdai magas hozzáférési jogosultsággal rendelkező fiókokat a normál munkavégzéshez használt fiókoktól
- Alkalmazzunk jelszó széfet, a jelszavakat rendszeresen cseréljük, használjunk erős/komplex jelszavakat
- A rendszergazdai munkameneteket auditáljuk - „Mit csinál a rendszergazda?”
- Minden esetben nevesített felhasználókat hozunk létre, a közös használatú hozzáférések nem megengedettek! (admin, diszpécser, ügyfélszolgálat, üzemvitel, gépészek)



Devolutions
Workspace

Mire figyeljünk oda a már jól bevált üzemeltetési gyakorlatunkon felül?



SZÉPHŐ

- Frissítsünk rendszeresen!
 - Operációs rendszereket (Android is), és alkalmazásokat egyaránt
 - Firmwareket is, pl.: Szerverek, SAN/NAS adattárolók, BIOS-ok, IP kamera, IP telefon, egyéb IoT eszközök, nyomtatók, UPS, stb...
- Ne használjunk End of Support, End of Life eszközöket amihez már nem biztosított gyártói támogatás, de legfőképp a biztonsági frissítések már nem elérhetők!
- Windows 10 -> Windows 11 átállás jövő év végéig!
 - Hardver cserével járhat (Min. 8. generációs processzor szükséges, TPM chip megléte)
- Ne engedélyezzünk dokumentálatlan adatkapcsolatokat
 - Szoftver interfészek, VPN távoli elérés (karbantartó cégek), ad-hoc (Teamviewer)
- Rendszeresen ismétlődő biztonságtudatossági oktatásokat kell szervezni, mert hiába van jól felépített védelem, a rendszer leggyengébb láncszeme mindig az ember marad ...

Köszönöm a figyelmet!



Workshop témák:

Mik a NIS2 felkészülés legnagyobb kihívásai

Milyen segítségre lenne szükségem a sikeres felkészülés érdekében

Szakmai eszmecsere, tudás megosztás

Kérdések & Válaszok