NIS2 – nem csak kötelezettség, hanem **lehetőség** is

PRIANTO

Urzica Olivér – Regionális ügyvezető

2024.03.19, Budapest

PRIANTO

KIBERBIZTONSÁGI kitekintés 2024

A JÖVŐ VÉDELME!

- Kiberbiztonsági tudatosság, belső fenyegetések növekedése
- Ellátási lánc elleni támadások
- Kiemelt fókusz a kritikus infrastruktúrákra
- IT/OT egységes menedzsment
- Nemzetközi állam által támogatott kiberháborúskodás
- SOC-ok (Security Operations Center) előtérben, nagyobb kereslet
- Külső Kiberfenyegetési Intelligencia
- Kiberbiztonság mint szolgáltatás
- Felhőszolgáltatások és MSP-k (kezelt szolgáltatók) elleni támadások
- Data Governance
- Személyazonosság lopás/ megszemélyesítés
- Költséghatékony biztonsági platformok konszolidációja
- Ransomware és phishing támadások
- Kiberbiztonsági szabályozások végrehajtása
- Automatizálásra és láthatóságra való összpontosítás
- AI/ML/UEBA alkalmazása

NIS2 - nem csak jogi kötelezettség, hanem lehetőség is

INNOVÁCIÓ

VERSENYELŐNY

SZOROS KOOPERÁCIÓ

ERŐFORRÁS OPTIMALIZÁLÁS

REZILIENCIA

A NIS2 irányelv és a Kibertan tv. által elvárt védelmi intézkedések

- Rendszer- és információsértetlenség
- Rendszer- és kommunikációvédelem
- Adathordozók védelme
- Konfigurációkezelés
- Karbantartás

- Értékelés, engedélyezés és monitorozás

- Készenléti tervezés
- Fizikai és környezeti védelem

- Rendszer- és szolgáltatásbeszerzés
- Ellátási lánc kockázatkezelése

- Programmenedzsment
- Kockázatelemzés
- Tervezés

- Naplózás és elszámoltathatóság
- Biztonsági események kezelése

- Tudatosság és képzés
- Személyi biztonság

- Identitás és hozzáférés kezelés
- Azonosítás és hitelesítése

Érintett ágazatok

Forrás: sztfh.hu

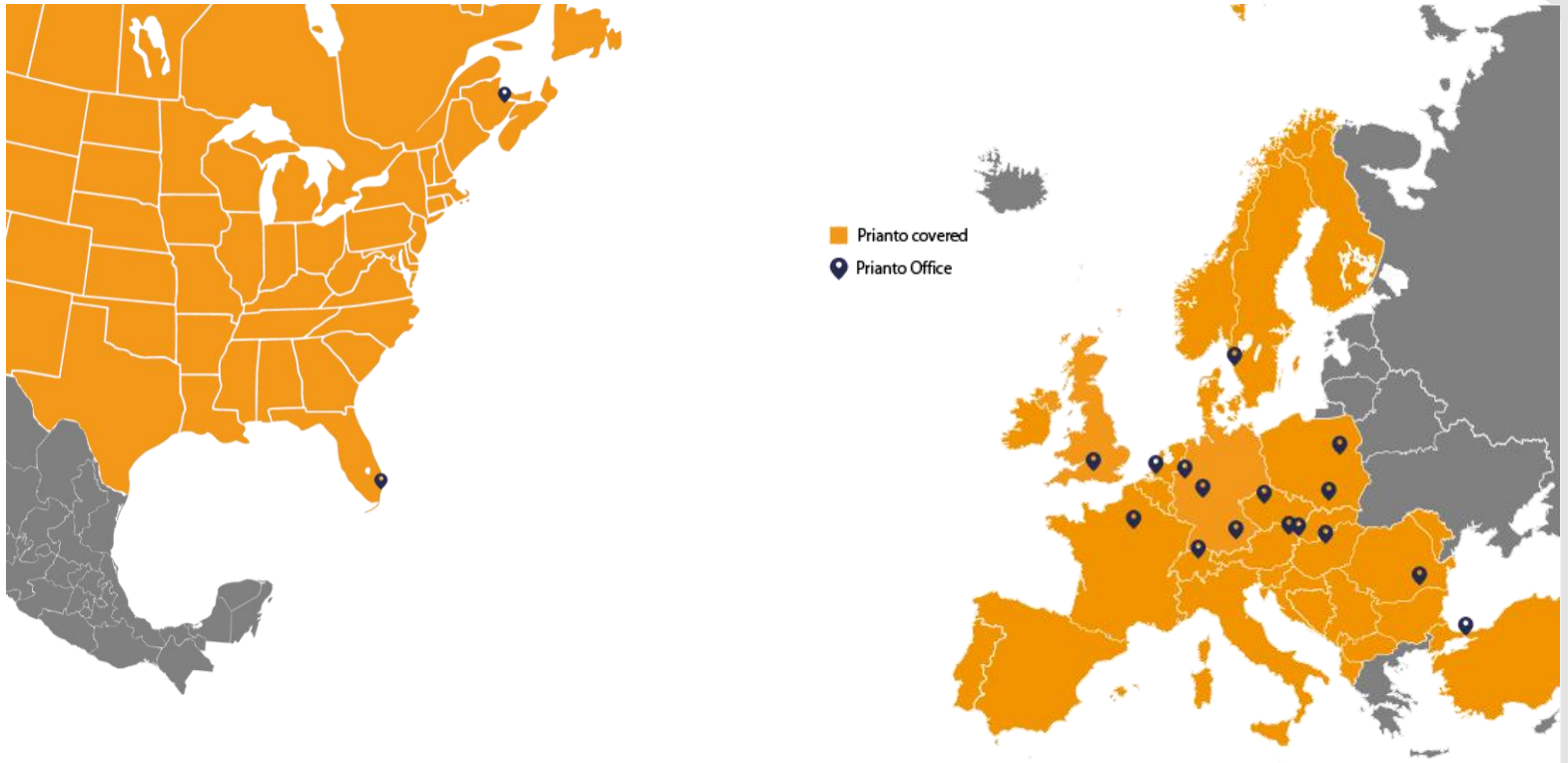
Prianto Csoport

Értéknövelt szoftverdisztribútor
Nagyvállalati IT megoldások és gyártók képviselője

Kiemelt területek:
IT biztonság, virtuálizáció, digitális transzformáció, cloud-SaaS, infrastruktúra kezelés, adatvagyongazdálkodás, MSP

Forgalom 2023: 180M EUR

Alkalmazottak száma: 175



Prianto Csoport:

- 2011 – Prianto UK, Prianto Switzerland
- 2012 – Prianto Austria, Prianto BeNeLux
- 2014 – Prianto Poland
- 2016 – Prianto France
- 2017 – Prianto Czechia, Hungary, Adriatics
- 2019 – Prianto Canada
- 2021 – Prianto USA, Prianto Türkiye
- 2022 – Prianto Romania and Slowakia
- 2023 – Prianto Nordics
- 2023 – Prianto Hungary Kft. megalapítása

PRIANTO

Szolgáltatásaink

Tanácsadás

Szoftver disztribúció

Szoftver-beszerzés

Értékesítés

MSP szolgáltatás

Üzletfejlesztés

Ipar 4.0

Pre-Sales

Műszaki támogatás

Kibervédelem

Implementáció

Marketing támogatás

Kompetencia központ

Digitalizáció

Képzések

Teszt-rendszerek, POC

PRIANTO

PRIANTO mint a NIS2 „**NEURON-HÁLÓZATA**”

Végfelhasználók

MSP/SOC szolgáltatók

IT szállítók

Hatóságok

Szakértők, auditorok

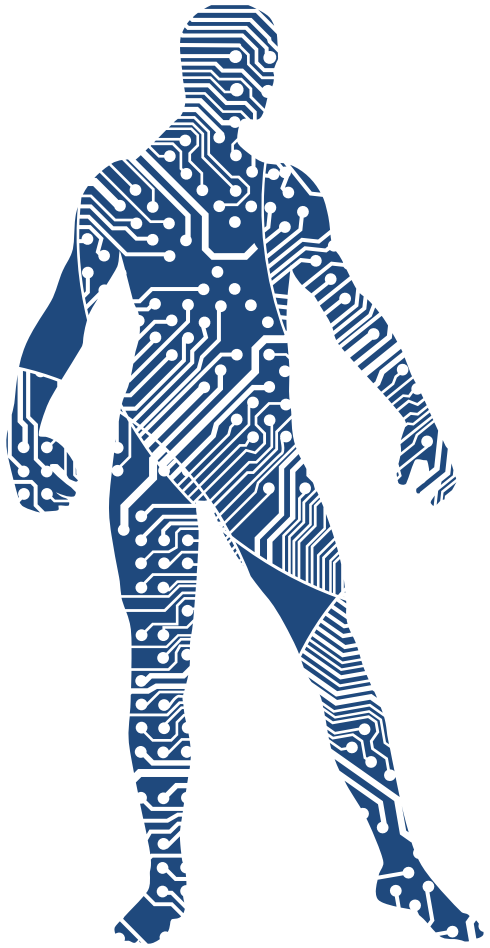
Vendorok

Felmérés → Tanácsadás → Tervezés → Tesztelés → Implementálás → Támogatás

PRIANTO

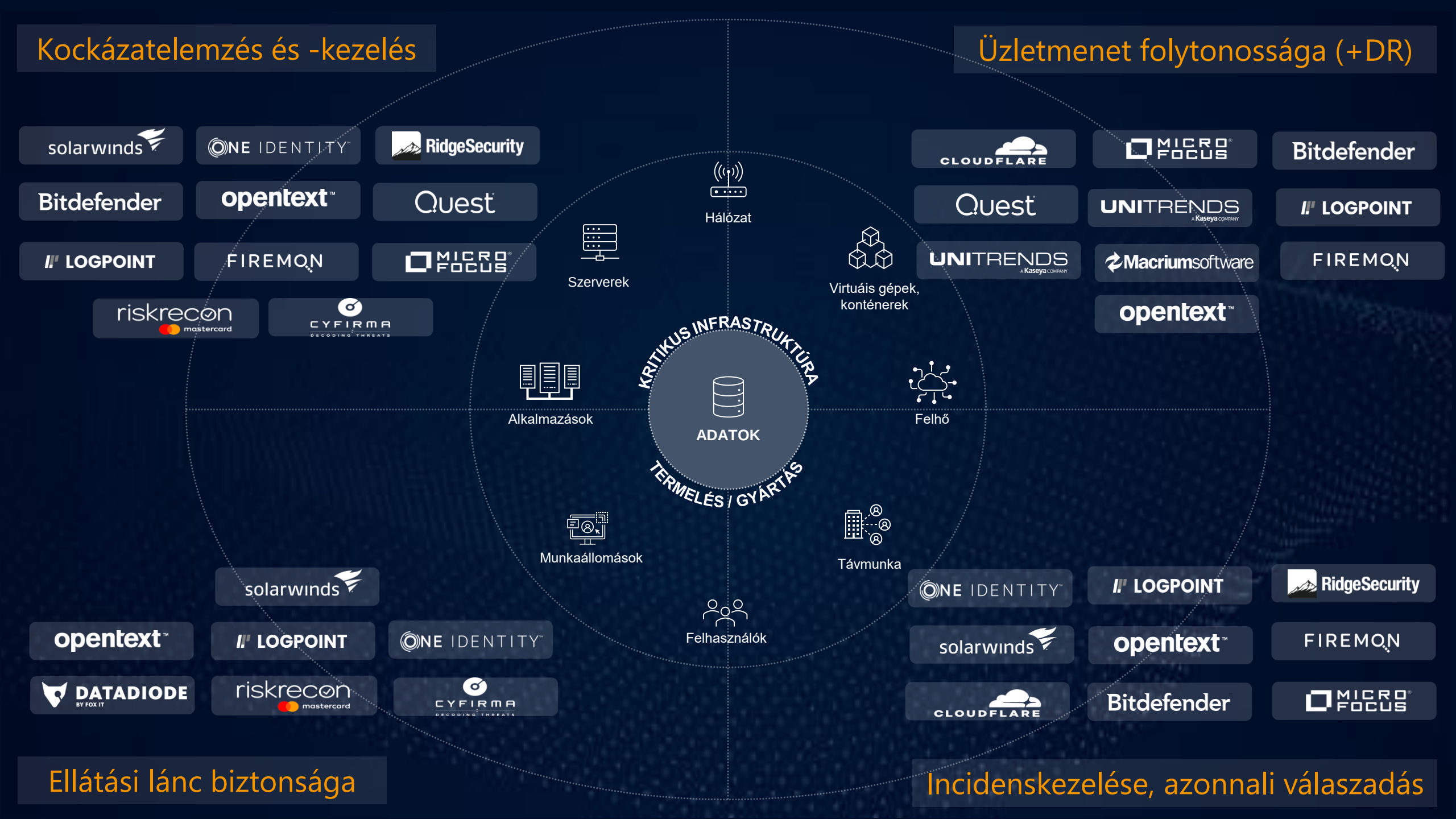
Megoldásaink, amelyek segítenek megfelelni a NIS2/Kibertan.tv.-nek

- Biztonságos hálózati infrastruktúra kialakítása, valós idejű monitorozása és védelem
- SIEM+SOAR+BCS+EDR bevezetése, incidenskezelés
- Sérülékenység-vizsgálat és menedzsment, behatolás tesztelés
- Cyber Threat Intelligence és Threat Hunting megoldások és szolgáltatások



- MSP/SOC megoldások és szolgáltatások
- IT & OT biztonsági és menedzsment megoldások
- Jogosultság, felhasználókezelés és hozzáférés menedzsment megoldások
- Adatmentés, Disaster Recovery és üzletfolytonosságot biztosító megoldások

SZOLGÁLTATÁS & TERMÉK PORTFÓLIÓ


Kockázatelemzés és -kezelés
Üzletmenet folytonossága (+DR)
solarwinds
ONE IDENTITY
RidgeSecurity
Bitdefender
opentext
Quest
LOGPOINT
FIREMON
MICRO FOCUS
riskrecon
mastercard
CYFIRMA
DECODING THREATS
CLOUDFLARE
MICRO FOCUS
Bitdefender
Quest
UNITRENDS
A Kaseya COMPANY
LOGPOINT
UNITRENDS
A Kaseya COMPANY
Macriumsoftware
FIREMON
opentext
Hálózat
Szerverek
Virtuális gépek, konténerek
KRITIKUS INFRASTRUKTÚRA
Alkalmazások
ADATOK
Felhő
TERMELÉS / GYÁRTÁS
Munkaállomások
Távmunka
Felhasználók
solarwinds
opentext
LOGPOINT
ONE IDENTITY
DATADIODE
BY FOX IT
riskrecon
mastercard
CYFIRMA
DECODING THREATS
ONE IDENTITY
LOGPOINT
RidgeSecurity
solarwinds
opentext
FIREMON
CLOUDFLARE
Bitdefender
MICRO FOCUS
Ellátási lánc biztonsága
Incidenskezelése, azonnali válaszadás

Köszönöm a figyelmet!

PRIANTO
Értéknövelt szoftverdisztribútor

Urzica Olivér / CEO
Mob: +36 70 418 7177
Email: oliver.urzica@prianto.com

Kötelezettségek

A rendelkezések kötelező érvényűek a hazai vállalkozások és szervezetek számára. A kötelezettségek közül a legfontosabbakat említjük meg

Incidensbejelentés

A szervezetek minden jelentős eseményt 24 órán belül kötelesek bejelenteni a biztonsági eseményekre reagáló csoportoknak és a felügyeleti hatóságnak.

Jelentős események:

- **súlyos működési zavart okozott vagy képes okozni** a szolgáltatásokban;
- **pénzügyi veszteséget okozott** az érintett szervezetnek;
- **jelentős vagyoni vagy nem vagyoni kárt okozott (képes okozni)** természetes vagy jogi személyek számára.

Kiberbiztonsági intézkedések

A szervezeteknek kiberbiztonsági intézkedéseket kell bevezetniük:

- kockázatelemzési és információbiztonsági szabályzatok,
- üzletmenet folytonossága,
- katasztrófa utáni helyreállítás,
- ellátási láncok biztonsága,
- kiberhigiéniai gyakorlatok és képzések,
- titkosításra vonatkozó szabályzatok és eljárások,
- HR-biztonság,
- hitelesítési megoldások,
- biztonságos hang-, videó- és szöveges kommunikáció,
- vészhelyzeti kommunikációs rendszerek.

A védelmi intézkedéseknek az alábbiakra kell kiterjedniük:

1. információbiztonsági irányítás rendszerére (kockázatmenedzsment keretrendszer)
2. kockázatainak feltárására és kezelésére
3. rendszerenként meghatározandó biztonsági osztálynak megfelelő adminisztratív, logikai és fizikai intézkedések alkalmazására
4. biztonsági események megelőzésére, felismerésére, kezelésére, bejelentésére és hatásainak csökkentésére
5. üzletmenet folytonosság biztosítására
6. rendszerek és az ezek által használt szoftver és hardver termékek beszerzésére, fejlesztésére, és üzemeltetésére
7. alkalmazandó követelmények kiterjesztésére a rendszer létrehozásában, üzemeltetésében, karbantartásában vagy javításában közreműködőkre

Incidensek kezelése, azonnali válaszadás

- **Bitdefender** (Végponti Felderítés és Reagálás - EDR): Az EDR megoldások segíthetnek felderíteni és kivizsgálni a gyanús tevékenységeket az eszközein, lehetővé téve a gyorsabb reagálást a potenciális biztonsági incidensekre.
- **Firemon & Logpoint** (Biztonsági Információ- és Eseménykezelés - SIEM): A SIEM eszközök összegyűjtik a naplókat a különböző biztonsági eszközökről és rendszerekről, központi betekintést nyújtva a biztonsági eseményekbe. Ez segíthet a biztonsági elemzőknek gyorsan azonosítani és rangsorolni az incidenseket.
- **One Identity** (Identitás- és Hozzáférés-menedzsment - IAM): Az erős IAM-gyakorlatok segíthetnek megelőzni a jogosulatlan hozzáférést és korlátozni az esemény által okozott potenciális károkat. A felhasználói hozzáférések és jogosultságok hatékony kezelésével potentially gyorsabban be tudja határolni az eseményt.
- **Solarwinds** (korlátozásokkal): A Solarwinds biztonsági eseménykezelési (SEM) eszközöket kínál, amelyek gyűjthetik és elemezhetik a naplókat a különböző biztonsági eszközökről. Bár nem olyan átfogóak, mint a SIEM megoldások, a SEM még mindig hasznos lehet a biztonsági incidensek azonosításában.

Közvetve Közreműködő Szállítók:

- **Cyfirma & Riskrecon** (Fenyegetésintelligencia): Ezek a platformok betekintést nyújtanak a potenciális fenyegetésekbe és sebezhetőségekbe, lehetővé téve a rendszerek gyenge pontjainak proaktív kezelését és az incidensek megelőzését.
- **Veriato** (Felhasználói Viselkedés Elemzés): A felhasználói tevékenység elemzésével a Veriato segíthet azonosítani a szokatlan viselkedést, amely biztonsági incidensre utalhat.

Kockázatelemzés

- **Bitdefender (Végponti Felderítés és Reagálás - EDR):** Az EDR megoldások, mint a Bitdefender, elemzik a végponti adatokat a potenciális kockázatok, például rosszindulatú programok vagy gyanús tevékenységek azonosítása és értékelése céljából. Ez segít a fenyegetések rangsorolásában az alapján, hogy milyen mértékben befolyásolhatják a rendszereit.
- **Cyfirma & Riskrecon (Fenyegetésintelligencia):** Ezek a platformok fenyegetésintelligencia-adatokat gyűjtenek és elemeznek, betekintést nyújtva a szervezetét érő potenciális fenyegetésekbe és sebezhetőségekbe. Ez a szélesebb körű kockázatelemzés segít megérteni a fenyegetési táj alakulását és rangsorolni a biztonsági erőfeszítéseket.
- **Firemon & Logpoint (Biztonsági Információ- és Eseménykezelés - SIEM):** A SIEM megoldások a különböző biztonsági eszközökről gyűjtik és elemzik a naplókat, lehetővé téve a potenciális kockázatokat jelző trendek és minták azonosítását. Ez segít azonosítani és értékelni az IT infrastruktúrában rejlő biztonsági gyengeségeket.
- **Flexera (IT Eszközmenedzsment - ITAM):** Az ITAM megoldások, mint a Flexera, segíthetnek azonosítani az elavult szoftvereket, a licenc nélküli alkalmazásokat és a nem használt eszközöket. Ezek biztonsági kockázatokat jelenthetnek, az ITAM pedig egy átfogó képet nyújtva az IT eszközparkról segít ezeknek a kockázatoknak a kezelésében.
- **Opentext (Security Content Automation Platform - SCAP):** A SCAP automatizálja a sebezhetőségvizsgálatot és a javítási folyamatokat. A sebezhetőségek proaktív azonosításával és kezelésével jelentősen csökkentheti az általános biztonsági kockázatot.
- **Ridge Security (Sebezhetőség-kezelés):** A Ridge Security eszközöket kínál az IT rendszerek sebezhetőségeinek azonosítására, rangsorolására és javítására. Ez a sebezhetőségkezelés segít a legkritikusabb kockázatokra összpontosítani és javítani az általános biztonsági helyzetet.
- **Riskrecon (Fenyegetésintelligencia):** A Riskrecon a Cyfirmához hasonlóan a fenyegetésintelligenciára összpontosít, betekintést nyújtva a potenciális fenyegetésekbe, és lehetővé teszi a kockázati táj proaktív értékelését.

Ellátási Lánc Biztonsága

- **Flexera** (IT Eszközmenedzsment - ITAM): Megoldásaik segítenek azonosítani és nyomon követni az Ön termékeiben vagy szolgáltatásaiban használt összes szoftverkomponenst. Ez a átfogó betekintés lehetővé teszi a harmadik féltől származó könyvtárakban vagy függőségekben lévő sebezhetőségek pontos beazonosítását az ellátási láncon belül.
- **Cyfirma** & **Riskrecon** (Fenyegetésintelligencia): Ezek a platformok betekintést nyújtanak a beszállítókkal vagy azok szoftverével kapcsolatos potenciális kockázatokba. Az ismert sebezhetőségekről és sérülésekről szóló adatok elemzésével azonosíthatja az ellátási lánc gyenge pontjait.
- **FoxIT Datadiode** (Adatátviteli Biztonság): Az adatdiódák megakadályozzák a rosszindulatú programok vagy a jogosulatlan hozzáférés bejutását a hálózatába fertőzött szoftverfrissítések vagy letöltések révén, ami különösen hasznos a megbízhatatlan beszállítókkal való bánásmódban.
- **One Identity** (Identitás- és Hozzáférés-menedzsment - IAM): Az IAM-megoldások szabályozzák a fejlesztői környezetekhez és a szoftverraktárakhoz való hozzáférést. Ez csökkenti a jogosulatlan módosítások vagy a rosszindulatú kódok beszúrásának kockázatát az ellátási láncon belül.
- **Opentext** (Security Content Automation Platform - SCAP): SCAP-megoldásaik automatizálják a sebezhetőségek vizsgálatát és javítási folyamatait a szoftverkomponensekhez. Ez biztosítja, hogy az ellátási láncban azonosított sebezhetőségeket gyorsan kezeljék.
- **Solarwinds** (korlátozásokkal): A sebezhetőségvizsgáló és naplókezelő eszközök azonosíthatják a saját hálózatában és rendszereiben lévő sebezhetőségeket. Bár nem közvetlenül a beszállítókra összpontosítanak, segíthetnek azonosítani azokat a kihasznált sebezhetőségeket, amelyek az ellátási láncból eredhetnek.

Nem az Ellátási Lánc Biztonságra Összpontosító Szállítók:

- Acunetix, Bitdefender, Cloudflare, Firemon, Logpoint: Ezek a hálózat és alkalmazások biztonságára összpontosítanak, nem magára az ellátási láncra.
- Droplet, Lansweeper, Macrium, Nitro, Sealpath, Smartbear, Stormagic, Teamviewer, Unitrends, Veriato: Ezek a szállítók specifikus feladatokra összpontosítanak, mint a felhőalapú tárhely, az eszközfelfedezés, a mentés és a katasztrófavédelem, a termelékenységi eszközök vagy a felhasználói viselkedéselemzés, és nem relevánsak közvetlenül az ellátási lánc biztonságához.

Üzletmenet Folytonosságának Fenntartása

- **Bitdefender** (Végponti Felderítés és Reagálás - EDR): Az EDR megoldások segíthetnek azonosítani és reagálni a potenciális biztonsági fenyegetésekre, amelyek megzavarhatják a működését.
- **Cloudflare** (DDoS-támadások enyhítése és web alkalmazás tűzfal - WAF): Ezek az eszközök segíthetnek megvédeni a kritikus online szolgáltatásokat a megosztott szolgáltatás-letiltási (DDoS) támadások és a webes alkalmazások sebezhetőségei által okozott kimaradásoktól.
- **Firemon & Logpoint** (Biztonsági Információ- és Eseménykezelés - SIEM): A SIEM megoldások összegyűjtik és elemzik a különböző biztonsági eszközök naplóit, segítve a potenciális incidensek azonosítását, amelyek befolyásolhatják az üzletmenet folytonosságát.
- **Flexera** (IT Eszközmenedzsment - ITAM): Az IT eszközeinek (hardver, szoftver, licencek) átfogó áttekintésével az ITAM segíthet biztosítani, hogy a kritikus rendszerek megfelelően karbantartottak és naprakészek legyenek, csökkentve a kimaradások kockázatát.
- **Macrium & Unitrends** (Biztonsági Mentés és Katasztrófa-helyreállítás): Ezek a megoldások lehetővé teszik az adatok és rendszerek rendszeres biztonsági mentését, lehetővé téve a visszaállítást katasztrófa vagy kimaradás esetén, minimalizálva a leállási időt és az adatvesztést.
- **Opentext** (Security Content Automation Platform - SCAP): A biztonsági hibajavítási folyamatok automatizálása (SCAP megoldások használatával) segíthet biztosítani, hogy rendszerei védettek legyenek az ismert sebezhetőségek ellen, csökkentve a működést megzavaró biztonsági incidensek kockázatát.
- Solarwinds (korlátozásokkal): A Solarwinds különféle IT-menedzsment eszközöket kínál, amelyek közül néhány hasznos lehet az üzletmenet folytonossága szempontjából. Például a hálózati monitorozó eszközök segíthetnek azonosítani a potenciális hálózati problémákat, amelyek megzavarhatják a működést.

Nem Közvetlenül az Üzletmenet Folytonosságához Kapcsolódó Szállítók:

- Acunetix (Webalkalmazás-biztonsági Tesztelés)
- Cyfirma & Riskrecon (Fenyegetésintelligencia)
- Droplet (Felhőalapú Tárhely Platform)
- FoxIT Datadiode (Adatátviteli Biztonság)
- Lansweeper (IT Eszközfelfedezés)
- Nitro (Termékenységi Eszközök)

Védelem katasztrófa ellen, helyreállítás

- **Macrium & Unitrends** (Biztonsági Mentés és Katasztrófa-helyreállítás): Ezek a szállítók alapvető katasztrófavédelmi funkciókat kínálnak. Megoldásaik lehetővé teszik az adatok és rendszerek rendszeres biztonsági mentését, lehetővé téve a visszaállítást katasztrófa vagy kimaradás esetén, minimalizálva a leállási időt és az adatvesztést.
- **Stormagic** (Adattárolás és -kezelés): Bár nem kifejezetten katasztrófavédelmi szoftver, a Stormagic adattárolási megoldásai szerepet játszhatnak. Termékeik segíthetnek biztosítani az adatok elérhetőségét akkor is, ha egy elsődleges tárolórendszer meghibásodik, megkönnyítve az adatok katasztrófa esetén történő visszaállítását.
- **Solarwinds** (korlátozásokkal): A Solarwinds különféle IT-menedzsment eszközöket kínál, amelyek közül néhány hasznos lehet a katasztrófavédelemhez. Például az adattárolási vagy rendszerfelügyeleti termékeikben található mentési és replikációs funkciók segíthetnek az adatmentési folyamatokban.
- **QUEST !!**

Közvetve Közreműködő Szállítók:

- Bitdefender (Végponti Felderítés és Reagálás - EDR): Az EDR megoldások segíthetnek azonosítani és elszigetelni azokat a biztonsági incidenseket, amelyek adatvesztéshez vezethetnek, potentially minimizing the impact of a disaster.
- Firemon & Logpoint (Biztonsági Információ- és Eseménykezelés - SIEM): A SIEM megoldások segíthetnek gyorsabban azonosítani és reagálni a biztonsági incidensekre, ami kritikus fontosságú lehet katasztrófavédelmi forgatókönyv esetén.
- Flexera (IT Eszközmenedzsment - ITAM): Az IT eszközök (hardver, szoftver, licencek) átfogó megértésével az ITAM segíthet biztosítani, hogy a helyreállításhoz szükséges kritikus rendszerek megfelelően dokumentáltak és könnyen elérhetők legyenek.

IT - Biztonsági Ökoszisztéma

Automatizált Etikus Hekkelés, sebezhetőségek felderítése
RidgeSecurity

CYFIRMA DECODING THREATS
Külső fenyegetések felderítése és kezelése

Hibrid infrastruktúra beállításainak elemzése, auditálása, problémák javítása
Runecast

CLOUDFLARE
Zero Trust Network-as-a-Service
DDos védelem, távmunka, …

Tűzfal-házirendek és szabályok központi menedzsmentje
FIREMON

LOGPOINT
Biztonsági események elemzése, automatikus válaszadás

Üzletmenet-kritikus, elavult alkalmazások biztonságos futtatása
Droplet Computing

ONE IDENTITY
Identitások és kiemelt munkamenetek kezelése

Egyirányú adatkapcsolat kiemelten védett hálózatokhoz
DATADIODE BY FOX IT

UNITRENDS
Zsarolóvírus-ellenálló biztonsági mentés

Adatszivárgás elleni védelem és audit
ENDPOINT PROTECTOR | by CoSoSys

(Veriato)
Belső fenyegetések elleni védelem, felhasználó megfigyelés

Kiberbiztonsági tudatosság, belső fenyegetések növekedése

Ellátási lánc elleni támadások

Kiemelt fókusz a kritikus infrastruktúrákra

IT/OT egységes menedzsment

KIBERBIZTONSÁGI

kitekintés 2024

A JÖVŐ VÉDELME!

Nemzetközi állam által támogatott kiberháborúskodás

SOC-ok (Security Operations Center) előtérben, nagyobb kereslet

Külső Kiberfenyegetési Intelligencia

Kiberbiztonság mint szolgáltatás

Felhőszolgáltatások és MSP-k (kezelt szolgáltatók) elleni támadások

Data Governance

Személyazonosság lopás/ megszemélyesítés

Költséghatékony biztonsági platformok konszolidációja

Ransomware és phishing támadások

Kiberbiztonsági szabályozások végrehajtása

Automatizálásra és láthatóságra való összpontosítás

AI/ML/UEBA alkalmazása