NIS2 irányelvről, annak bevezetéséről és a megfeleléshez szükséges megoldásokról

PRIANTO

Intelligible, secure digital transformation

Leading global software distributor focusing on enterprise IT solutions

CYFIRMA

DECODING THREATS

NIS2

AZ ÚJ BIZTONSÁGI IRÁNYELVRŐL DIÓHÉJBAN

A NIS (Network and Information Systems) EU belső piaci működésének javítása érdekében létrehozott kiberbiztonsági irányelv. A hálózati és információs rendszerek biztonságának magas szintjét biztosítja egységesen, az EU teljes területén.

Az irányelv célja biztosítani a tagállamok számára, hogy nagyobb rugalmassággal reagálhassanak a kiberbiztonsági incidensekre, és magasabb szintű védelemmel láthassák el a kritikus infrastruktúrákat, különös tekintettel az ellátási láncok integritására. Szabályozza az érintett szervezeteknél szükséges kiberbiztonsági intézkedéseket és a jelentéstételi kötelezettségeket.

A szervezetek **minden jelentős eseményt 24 órán belül kötelesek bejelenteni** a biztonsági eseményekre reagáló csoportoknak (CSIRT) vagy a nemzeti hatóságnak.

Egy esemény akkor tekintendő jelentősnek, ha:

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

NIS2

BEVEZETENDŐ KIBERBIZTONSÁGI INTÉZKEDÉSEK

A hatály alá tartozó szervezeteknek további kiberbiztonsági kockázattal arányos biztonsági intézkedéseket kell bevezetniük amely kiterjed:

- **a kockázatelemzési és információbiztonsági szabályzatokra**
- **üzletmenet folytonosságra**
- katasztrófa utáni helyreállításra
- **ellátási láncok biztonságának biztosítására**
- **kiberhigiéniai gyakorlatokra és kiberbiztonsági képzésekre**
- titkosításra, kriptográfiai megoldások használatára vonatkozó szabályzatok és eljárások alkalmazására
- **HR biztonságra**
- hitelesítési megoldásokra
- biztonságos hang-, video- és szöveges kommunikációra
- illetve biztonságos vészhelyzeti kommunikációs rendszerek használatára

CYFIRMA
DECODING THREATS

Egy lépéssel a hackerek előtt

PREDIKTÍV KIBERHÍRSZERZÉSI PLATFORM

Kibertámadás elleni védelem és megelőzés

Ki, Miért, Mit, Hogyan és Mikor támad?

CYFIRMA

DECODING THREATS

PRIANTO

Előadó: Donner Krisztián | Presales Manager | Prianto CEE

Felfedezett sérülékenységek (CVE) az elmúlt években

A KIBER-INTELLIGENCIA ALKALMAZÁSA A BIZTONSÁGI MŰVELETEKBEN

A KÜLÖNBSÉG

REAKTÍV

Információ korábbi támadásokról:

- IoC információ
  - Rosszindulatú IP-cím/ URL/ domain név
  - Malware Hash (MD5/SHA) stb.
- Sebezhetőség kihasználása
- Kibernetikai incidens, malware, adathalászat stb.

Biztonsági beszállítók, speciális szervezetek, mint például az ország CIRT / Internet hírek

PROAKTÍV

Jelenlegi fenyegetések és kockázatok:

- Digitális kockázat
  - Megszemélyesített domain
  - Hamis SNS-fiók
  - Érzékeny információk felfedése
- Támadócsoportok és technikák profilja a korábbi incidensek alapján.
- Korábbi támadásokból származó adatok.

OSINT, fenyegetéselhárítók, professzionális kutatók

PREDIKTÍV

Értesüljön a küszöbön álló kiberfenyegetésekről és támadásokról:

- A konkrét vállalatokat - **az Ön ügyfeleit -** célzó fenyegető szereplők motivációi.
- Azonosítsa a fenyegető szereplők által tervezett kibertámadásokat az ügyfelei ellen.
- Aktív kampányok, a fenyegető szereplők jelenlegi tevékenységei, a jövőre vonatkozó tendenciák, a kapcsolódó támadási módszerek és infrastruktúra (TTP/IoC stb.).
- Az ügyfelek rendszerei, amelyeket a fenyegető szereplők célba vesznek.

CYFIRMA
FENYEGETÉSEK FELDERÍTÉSE ÉS PREDIKTÍV KIBERINTELLIGENCIA

DECYFIR

CYFIRMA
DECODING THREATS

CYFIRMA MEGKÖZELÍTÉS

A PREDIKTÍV INTELLIGENCIA ELŐNYEI

Az ellenség megismerése és a szervezetet/ügyfelet fenyegető veszélyek megértése, átállás az eseményalapuról az intelligenciaalapú biztonsági magatartásra

Ez ellenség megismerése	• A DeCYFIR többrétegű kiberinformációs rendszerének segítségével feltárhatja és elemzheti a fenyegetéseket. • Értse meg a szervezet/ügyfél ellen indítható **kibertámadások KIK, MIÉRT, MIÉRT, MIÉRT, MIKOR, HOGYAN, HOGYAN** jellegét.
Erőforrások rangsorolása és optimalizálása	• Használja ki a meglévő biztonsági ellenőrzéseket, amennyire csak lehetséges, eközben reagáljon a szervezetét/ügyfelét célzó, azonosított hackercsoportok támadásaira. • Segít azonosítani a szervezet/ügyfél kiberbiztonsági rendszerében lévő hiányosságokat.
Vezetői döntéshozatal elősegítése	• Stratégiák és ütemtervek felülvizsgálata az azonosított kiberfenyegetésekre adott válaszlépések javítása érdekében. • Azonosítja és javaslatot tesz a kiberbiztonsági helyzet kezelésének megerősítését célzó területekre.

CYFIRMA
DECODING THREATS

PRIANTO

FENYEGETÉSEK DEKÓDOLÁSA ÁTFOGÓ ISMERETEKKEL

FUNKCIÓK A 360 FOKOS ÁTLÁTHATÓSÁG ELÉRÉSE ÉRDEKÉBEN

KÜLSŐ FENYEGETÉSEK KEZELÉSE
EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM)

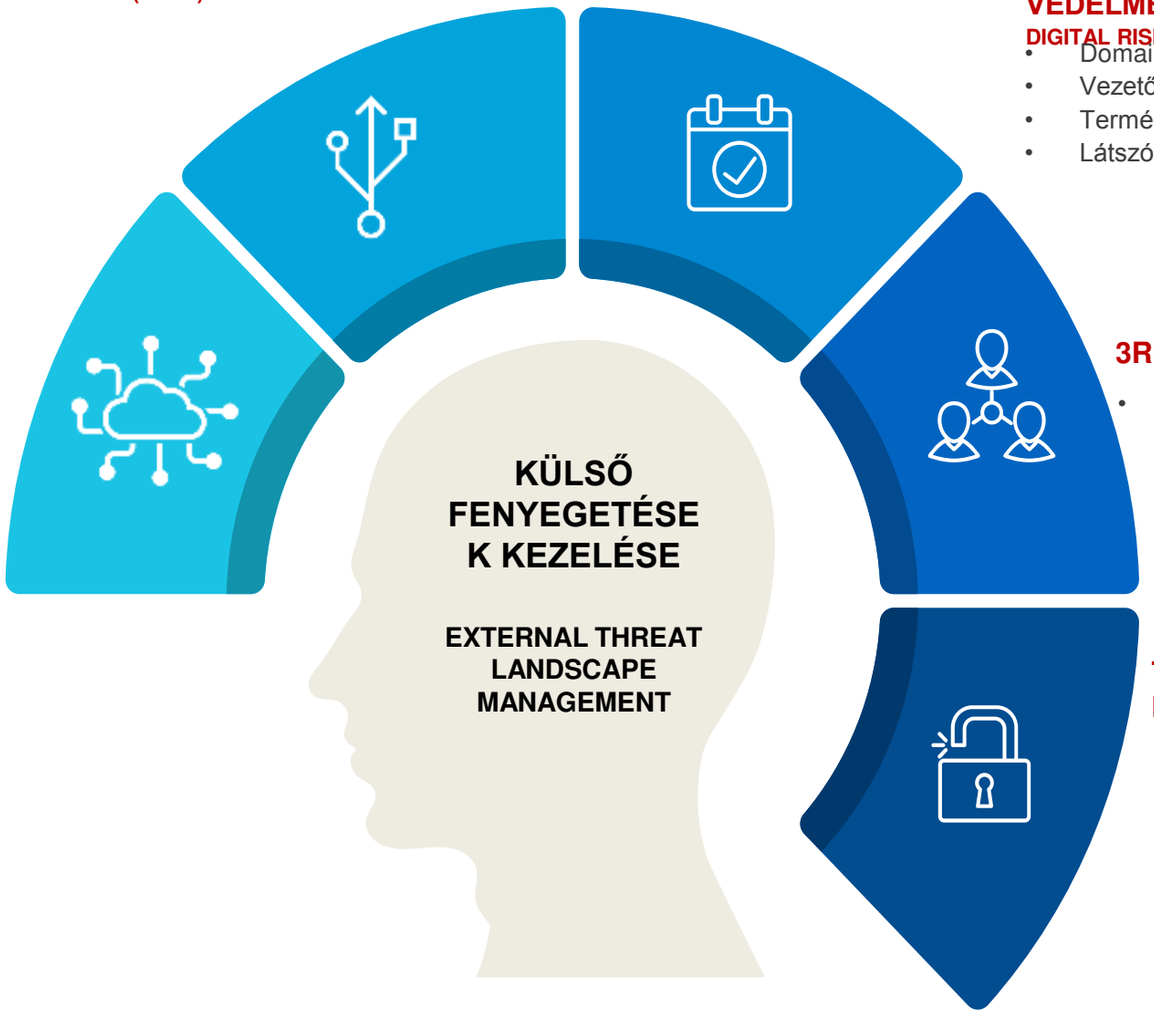
- Hat pillér egyetlen felületen
- Személyre szabott
- Előrejelző
- Kontextualizált

KÜLSŐ TÁMADÁSI FELÜLET KEZELÉSE
EXTERNAL ATTACK SURFACE MANAGEMENT [EASM]

- Domain sebezhetőség
- Tanúsítvány gyengesége
- Konfiguráció a DNS/SMTP/HTTP-ben
- Nyitott portok felderítése
- IP/domain hírnevének ellenőrzése

VALÓS IDEJŰ ADATVÉDELMI INCIDENSEK MEGFIGYELÉSE ÉS FELTÁRÁSA

- E-mail/azonosítók/credential kiszivárgása
- Dark web megfigyelés
- Adathalászat
- Ransomware
- Defacement
- Adatbázis expozíció
- Pénzügyi kiszivárgások/megfigyelés



DIGITÁLIS KOCKÁZATOK FELTÁRÁSA ÉS VÉDELME
DIGITAL RISK DISCOVERY AND PROTECTION [DRDP]

- Domain/IT eszközök megszemélyesítése
- Vezetők/személyek megszemélyesítése
- Termék/megoldás megsértése
- Látszólagos közösségi szolgáltatók

3RD PARTY KOCKÁZATOK FELTÁRÁSA

- A harmadik felek digitális kockázatainak, sebezhetőségeinek és kitettségének, valamint a szervezetre gyakorolt hatásainak nyomon követése.

TÁRSADALMI ÉS NYILVÁNOS KITETTSÉG

- Bizalmas fájl
- Forráskódok
- PII/CII dumpok
- Rosszindulatú mobilalkalmazások

CYFIRMA
DECODING THREATS

A CYFIRMA EGYEDÜLÁLLÓ KÜLSŐ FENYEGETÉSKEZELÉSI MODELLJE

6 FELDERÍTÉSI NÉZET EGYSÉGES PLATFORMON A KIBERFENYEGETÉSEK ÉS -KOCKÁZATOK KEZELÉSE ÉRDEKÉBEN

1

TÁMADÁSI FELÜLET FELTÁRÁSA
ATTACK SURFACE DISCOVERY

Az "ajtók" és "ablakok" azonosítása a szervezetnél

Eredmény: Valós idejű folyamatos felügyelet a kiberbűnözők által hozzáférhető árnyék IT vagy porózus rendszerek azonosítására.

A támadási felület ismerete lehetővé teszi, hogy reális költség-haszon elemzést végezzen az egyes eszközökről, és eldöntse, hogyan csökkentheti a támadási felületet.

2

SEBEZHETŐSÉGI HÍRSZERZÉS
VULNERABILITY INTELLIGENCE

Kulcsok az "ajtókhoz" és "ablakokhoz", amelyek a kiberbűnözők számára elérhetőek

Eredmény: A sebezhetőségeket az eszközökhöz és a kapcsolódó exploitokhoz rendelik hozzá, és kritikusságuk alapján rangsorolják.

Ez lehetővé teszi a vállalkozás számára, hogy optimalizálja az erőforrásokat, és a legfontosabb és legsürgősebb hiányosságokra összpontosítson.

3

MÁRKAVÉDELMI HÍRSZERZÉS
BRAND INTELLIGENCE

Tudja meg, mikor támadják a márkáját

Eredmény: Értse meg, hogy kik, miért és hogyan veszik célba az Ön márkáját, és kapjon teljes képet a márkanév megsértéséről.

Védje meg a márkát, és tartsa meg az ügyfelek hűségét annak biztosításával, hogy azt ne szennyezzék be vállalati kémkedéssel, belső fenyegetésekkel vagy más rosszindulatú rossz szereplőkkel.

4

DIGITÁLIS KOCKÁZATI VÉDELEM
DIGITAL RISK PROTECTION

A digitális profil, az adatszivárgás, a jogsértések és a megszemélyesítések átláthatósága

Eredmény: Feltárja a digitális lábnyomokat, valamint a megszemélyesítés és az adatszivárgás eseteit. Közel valós idejű riasztást kaphat a nyilvánosságra került adatairól.

Ennek ismeretében betömheti a réseket, és elkerülheti a további hírnév- és pénzügyi károkat.

5

HELYZETTUDATOSSÁG
SITUATIONAL AWARENESS

Az újonnan megjelenő fenyegetések, az ellenintézkedések és a potenciális támadási forgatókönyvek megértésével szerezze meg az irányítást a növekvő fenyegetettségi környezet felett.

Eredmény: Gyors áttekintés a kibertámadásokról, incidensekről és jogsértésekről, amelyek az Ön iparágában, az Ön által használt technológiában és az Ön földrajzi területén zajlanak.

Ezek a felfedezések és a következmények fontos üzleti döntésekhez vezethetnek, beleértve a kiberber-beruházásokat is.

6

KIBER-HÍRSZERZÉS
CYBER-INTELLIGENCE

A prediktív, személyre szabott, többrétegű, kontextusba helyezett mesterséges intelligencia elemzi a kibertámadási kampányokat, hogy választ adjon arra, KI, MIÉRT, MI,, MIKOR, HOGYAN készül egy támadásra.

Eredmény: Teljes képet és betekintést kaphat a külső fenyegetésekről.

Tartsa sakkban az ellenséget, kapja meg korán a figyelmeztetést a kibertámadások kivédéséhez, hogy elkerülje az üzletmenetet fenyegető zavarok elkerülése érdekében.

CYFIRMA
DECODING THREATS

CYFIRMA EGYEDI KIBER-HÍRSZERZÉSI MODELL

A CYFIRMA HÍRSZERZÉSI MODELLJE IRÁNYÍTJA A DECYFIR ÉS A DETCT FEJLESZTÉSÉT

TÁMADÁSI FELÜLET FELTÁRÁSA
A szervezetbe vezető "ajtók" és "ablakok" azonosítása

SEBEZHETŐSÉGI HIRSZERZÉS
Kulcsok az "ajtókhoz" és "ablakokhoz", amelyek a kiberbűnözők számára elérhetőek

MÁRKAVÉDELMI HÍRSZERZÉS
Tudja, mikor megtámadják a márkáját

DIGITÁLIS KOCKÁZATVÉDELEM
Digitális profil, az adatszivárgás, a jogsértések és a profil visszaélések felderítése

HELYZET-TUDATOSSÁG
Támadási forgatókönyvek, megjelenő fenyegetések és azok elhárításának megértése révén szerezze meg az irányítást a változó fenyegetettségi környezet felett.

KIBER-HÍRSZERZÉS
A prediktív, személyre szabott, több szintű, kontextusba helyezett intelligencia elemzi a kibertámadási kampányt, hogy megválaszolja, KI, MIÉRT, MIÉRT, MIKOR, HOGYAN.

DETCT BY CYFIRMA

Személyreszabott | Actionable | Széleskörű

Folyamatos és valós idejű megfigyelés

- Ismerje meg támadási felületét
- Közösségi média és webes kitettség
- Személyi adatokkal való visszaélés és jogsértés
- Dark Web Kitettség
- Kitettség Sérülékenységeknek
- Adatszivárgás Monitoring
- Third-Party Risk Monitoring

DECYFIR BY CYFIRMA

Prediktív | Személyreszabott | Hacker nézpont | Többrétegű | Kontextuális

Három hírszerzési réteg

Stratégia
Understand Hackers' and their motivation (Who, Why)

Menedzsment
Understand Hackers' interest and attack readiness (What, When)

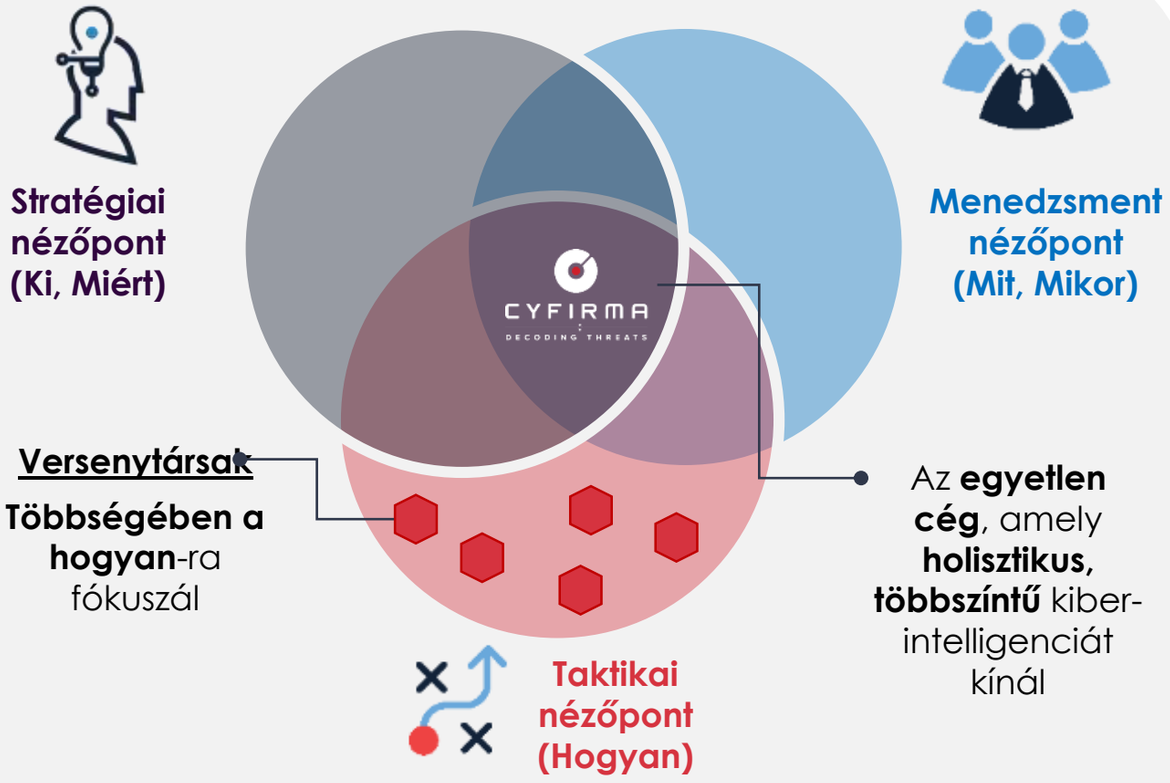
Taktika
Methods, techniques and tools of attack (How)

CYFIRMA
DECODING THREATS

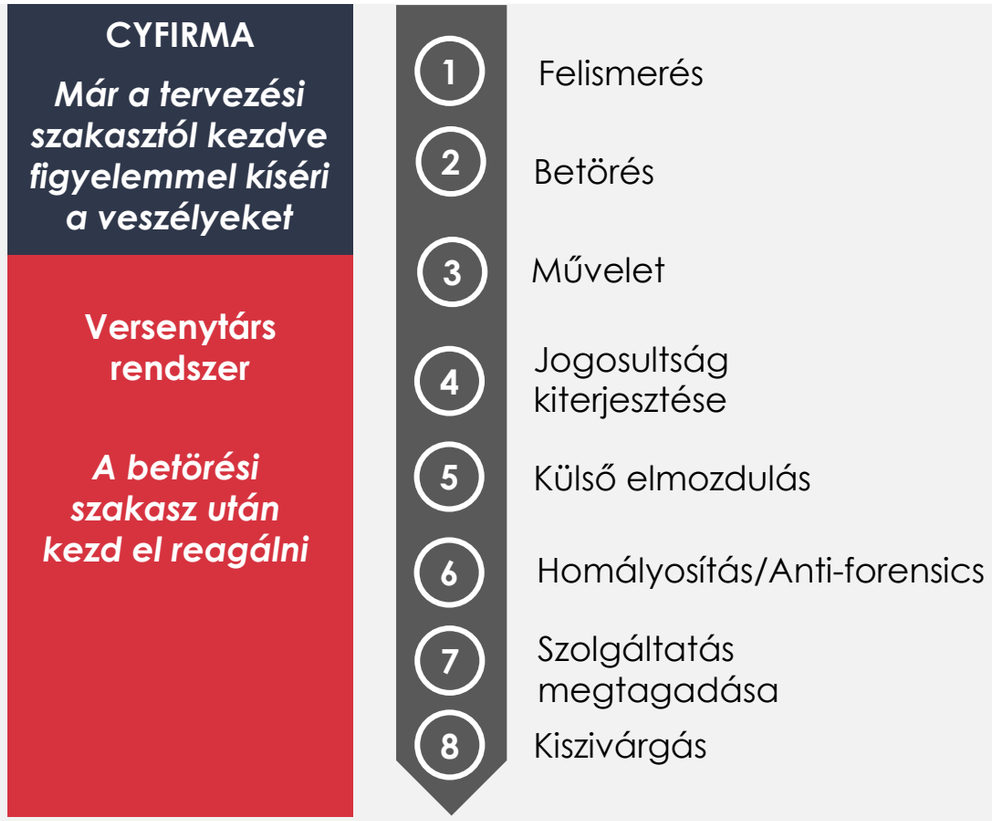
ALTERNATÍV MEGOLDÁSOK

TÖBBSZINTŰ KIBER-INTELLIGENCIA, AMELY MÁR A TERVEZÉSI SZAKASZBAN FELTÁRJA A FENYEGETÉSEKET

POZÍCIONÁLÁS



A CYFIRMA átfogó képet nyújt ügyfeleinek a külső fenyegetésekről



A CYFIRMA már a tervezési szakaszban korai figyelmeztetést ad az ügyfeleknek a támadásokról

DECYFIR ÁTTEKINTÉS

FELTÁRJAI ÉS ELEMZI AZ ÜGYFELET CÉLZÓ FENYEGETÉSEKET A 6 HÍRSZERZÉSI NÉZET ALAPJÁN

Nyilvános/magánadatok automatikus gyűjtése

- Nyilvános információk milliói
- **Hacker gyanús beszélgetések gyűjtése saját fejlesztésűprogrammal**

Surface web (Az Internet)
- **Hírek, blog**
- **SNS**
- **OSINT**

Deep/Dark web

Hacker közösség (zárt)

Elemzés az adatgyűjtés időpontjában

Komplex & saját AI/ML rendszer

Személyre szabott, prediktív, többszintű adatok

A DeCYFIR segítségével a CTI-nek egyedi fenyegetéselhárítási report

DECYFIR BY CYFIRMA

6 hírszerzési nézet EGY platformon belül

- **TÁMADÁSI FELÜLET FELTÁRÁSA**
- **HELYZETFELISMERÉS**
- **SEBEZHETŐSÉGI INFORMÁCIÓK**
- **DIGITÁLIS KOCKÁZATVÉDELEM**
- **MÁRKA INTELLIGENCIA**
- **KIBER-INTELLIGENCIA**

CYFIRMA
DECODING THREATS

DECYFIR – KÜLSŐ FENYEGETÉSEK KEZELÉSE

FELHŐALAPÚ, SAAS, NEM INTRUZÍV PLATFORM

DECYFIR BY CYFIRMA

Külső fenyegetések kezelése

DECYFIR BY CYFIRMA

Prediktív *Személyre szabott* *Hacker nézőpont* *Többszintű* *Akcióképes*

Három szintű intelligencia

Folyamatos és valós idejű adatok

Stratégia

Hackerek és motivációjuk megértése (Ki, Miért)

Menedzsment

A hacker érdeklődésének és támadási készségének megértése (Mit, Mikor)

Taktika

A támadás módszerei, technikái és eszközei (Hogyan)

Ismerje a támadási felületet

Közösségi média és webes jelenlét

Utánzás és jogsértés

Dark Web jelenlét

Sebezhető pontok kitettség

Adatvédelmi incidensek megfigyelése

Harmadik fél kockázatfigyelés

CYFIRMA
DECODING THREATS

ÜGYFÉLRE SZABOTT FENYEGETÉSEK ELŐREJELZÉSE ÉS KIBER-HÍRSZERZÉS

A CYFIRMA ELŐNY

DECYFIR™ TESTRESZABOTT PREDIKTÍV FENYEGETÉS-FELTÁRÁS ÉS HÍRSZERZÉS

1 Prediktív

Előrejelzi a kibertámadásokat azáltal, hogy a kampányok tervezési szakaszában proaktívan azonosítja a fenyegetéseket

2 Kontextuális intelligencia

A kontextuális intelligencia mély elemzést biztosít a hacker, az indíték, a kampány és a módszer közötti pontok összekapcsolásához

3 Kívülről-befelé

Lásd a hackerek lencséjéből. Értsd meg, miért leszel vonzó célpont, és milyen sérülékenységeket lehet kihasználni

4 Személyreszabott

Csökkenti a zajt és személyre szabott intelligenciát biztosít azáltal, hogy csak az ügyfél iparágának, földrajzi elhelyezkedésének és technológiájának megfelelő betekintést biztosít.

5 Többrétegű intelligencia

A többrétegű intelligencia magában foglalja a stratégiai, irányítási és taktikai betekintést

DECYFIR BY CYFIRMA

1. **Korai jelzések** a fenyegetésekről a közelgő támadások jeleinek felismerésével.
2. A **kontextusba helyezett fenyegetés-történet** megválaszolja a ‘KI’, ‘MIT’, ‘MIKOR, ‘MIÉRT’ és ‘HOGYAN’ kérdéseket.
3. Teljes és kontextuális nézet a szervezet külső fenyegetettségéről és kockázati környezetéről a **kívülről befelé / hackerek nézetének biztosításával**, amely részletesen lefedi a fenyegetés szereplőit, motivációit és azokat a kampányokat, amelyek segítségével megtámadhatják a szervezetet.
4. Minőségi és hasznosítható hírszerzés, amely **releváns** és **specifikus** a szervezetre, annak digitális profiljára, IT/OT eszközeire, iparágára, földrajzára és technológiájára.
5. **Többrétegű kiberintelligencia** az üzleti funkciók és tartományok között a biztonsági ellenőrzések hiányosságainak orvoslásához és a robusztus kiberhelyzet kezeléshez.

CYFIRMA DECODING THREATS

A 3 SZINTŰ INTELLIGENCIA – NÉZET

A HÍRSZERZÉSI ELEMZÉSEK INTEGRÁLÁSA A KIBERSTRATÉGIÁBA ÉS A VÉDELMI SZABÁLYOZÁSBA

Hozzontre létre és működtessen egy agilis, proaktív kibervédelmet, többdimenziós kiberfenyegetettségi információkkal.
Alkalmazza a pontos, előrejelző kibernetikai intelligenciát a szervezet döntéshozatalának minden aspektusában.

STRATÉGIAI INTELLIGENCIA

Biztosítja: az agilis, skálázható kiberstratégia és irányítási modellek alapelemeit

Alkalmazási terület: kiberstratégia, irányítás és szabályozás, kockázati nyilvántartás

Érintettek: felső vezetés, Biztonsági Igazgató, CISO

MANAGEMENT INTELLIGENCIA

Fő előnyei: szabályzat/folyamat változtatás a fenyegetők profilja, motivációi és mechanizmusai alapján

Alkalmazási terület: kiber-incidensekre való reagálás, patchek, konfigurációk és frissítések menedzselése

Érintettek: CISO, Biztonsági vezetők and Cybersecurity vezetők

TAKTIKAI INTELLIGENCIA

Alkalmazási terület: biztonsági ellenőrzések, rosszindulatú és kártékony programok aláírásai, adathalász domainek, robothálózatok vezérlő- és irányítóközpontjai, rosszindulatú IPS-ek

Érintettek: operátorok, mint például a CIRT, SOC, NOC és bármely más kapcsolódó csapat.

CYFIRMA
DECODING THREATS

DECYFIR AJÁNLATA

ÁTFOGÓ KÜLSŐ FENYEGETÉS-KEZELÉS

DeCYFIR™ Fenyegetés-felderítés és prediktív kiber-hírszezés - Ügyfélre szabottan

Korai figyelmeztések

Predictive Intelligencia, a kiberfenyegetések és -kockázatok korai észlelése "Outside-In" megközelítéssel

- Az ügyfelet és iparágát fenyegető veszélyek és kockázatok megelőzése
- Az internetes fórumok és az illegális piacok folyamatos figyelemmel kísérése.
- Cselekvésre alkalmas információk és indikátorok jelentése

Out Of Band tanácsadás

CYFIRMA kutatások a legújabb sebezhetőségekről, kibertrendekről, iparág-specifikus betekintésekről stb.

Heti tanácsadás

Az üzleti stratégia támogatása a legújabb külső fenyegetések és kockázatok alapján

A fenyegetettségi tájkép monitorozása

Változások az iparági fenyegetések terén, Fenyegető szereplők a fókuszban, legújabb tevékenységeik, amelyek támadáshoz vezethetnek.

Támadási felület felderítése

Az ügyfél digitális lábnyomának, a változó külső kockázati profilnak, a hackerek által kitett ügyféleszközöknek a nyomon követése és bemutatása.

Hírszerzés és betekintések az adathalászat körül

- A legfrissebb kampányok
- Fenyegető szereplők meghatározása

Proaktív kiberbiztonsági megközelítés

Célja, hogy tanácsadást nyújtson, mielőtt támadás történik

Digitális kockázati profilalkotás

Megszemélyesítés és jogsértés, adatszivárgás és adatszivárgás, sebezhetőségek, Dark Web expozíció stb.

Third-Party kockázatfigyelés

Fedezze fel a 3. fél digitális kockázati profiljait, hogy megértse, hogyan hat ez Önre.

A fenyegető szereplők és kampányok nyomon követése

Elvihető információk az ügyfél digitális kockázatára és profiljára fókuszálva

Célzott taktikai hírszerzés

Fogyasztható és specifikus IOC, kampányokhoz kapcsolódó fenyegetésvadászat, fenyegető szereplő, iparág/technológia/földrajz stb.

Támogatás

Támogatása a DeCYFIR™ QA és az ügyfélcsapat részéről

CYFIRMA
DECODING THREATS

A DECYFIR PLATFORM

DÖNTÉSI ESZKÖZ VEZETŐKNEK, VEZETŐKNEK, ÜZEMELTETŐKNEK

KOCKÁZATALAPÚ NÉZET

STRATÉGIAI

Alkalmazhatóság: Kiber-stratégia, Irányítás és Szabályzatok, Digitális kockázat, Kockázati nyilvántartás

Érintettek: felső vezetés, biztonsági igazgató, CISO

IRÁNYÍTOTT RENDSZERMEGKÖZELÍTÉS

MENEDZSMENT

Alkalmazhatóság: Kiberincidens-válasz, Patch-menedzsment, Konfigurációkezelés, Release- és verzió-kezelés

Érintettek: CISO, biztonsági vezetők és kiberbiztonsági vezetők

MŰKÖDÉSI NÉZET

TAKTIKAI

Alkalmazhatóság: Biztonsági ellenőrzések, rosszindulatú programok aláírásai és mutex, adathalász tartományok, botnet parancs- és vezérlőközpontok, rosszindulatú IPS

Érintettek: Operátorok, mint a CIRT, SOC, NOC és bármely más interfész csapat

CYFIRMA
DECODING THREATS

NIS2

BEVEZETENDŐ KIBERBIZTONSÁGI INTÉZKEDÉSEK

A hatály alá tartozó szervezeteknek további kiberbiztonsági kockázattal arányos biztonsági intézkedéseket kell bevezetniük amely kiterjed:

- a kockázatelemzési és információbiztonsági szabályzatokra
- üzletmenet folytonosságra
- katasztrófa utáni helyreállításra
- ellátási láncok biztonságának biztosítására
- kiberhigiéniai gyakorlatokra és kiberbiztonsági képzésekre
- titkosításra, kriptográfiai megoldások használatára vonatkozó szabályzatok és eljárások alkalmazására
- HR biztonságra
- hitelesítési megoldásokra
- biztonságos hang-, video- és szöveges kommunikációra
- illetve biztonságos vészhelyzeti kommunikációs rendszerek használatára

CYFIRMA ÁTTEKINTÉS
KÜLSŐ FENYEGETÉSEK KEZELÉSÉVEL FOGLALKOZÓ PLATFORM

2017-ben alapította egykori kormányzati hírszerzési vezető és CISO

AI/ML támogatású, felhőalapú SaaS-termékek - DeCYFIR és DeTCT

Több neves díjat nyert, és ezzel globális iparági elismerést szerzett

Meghatározó piaci szereplő Japánban; kiszorította a nagyobb versenytársakat a Fortune 100-as ügyfeleknél

Referencia: Fortune 500 ügyfelek

Digital Hearts, ecbeing, Mitsubishi Corporation, Orchestrating a brighter world NEC, NTT DATA NTT DATA INTELLILINK Corporation, TOSHIBA, TOPPAN, ZUELLIG PHARMA

Megbízható Partnerkapcsolatok

aws partner network | isv accelerate, Digital Hearts, Orchestrating a brighter world NEC, NTT DATA NTT DATA INTELLILINK Corporation, REVEL TECH

Marquee Befektetők Támogatják

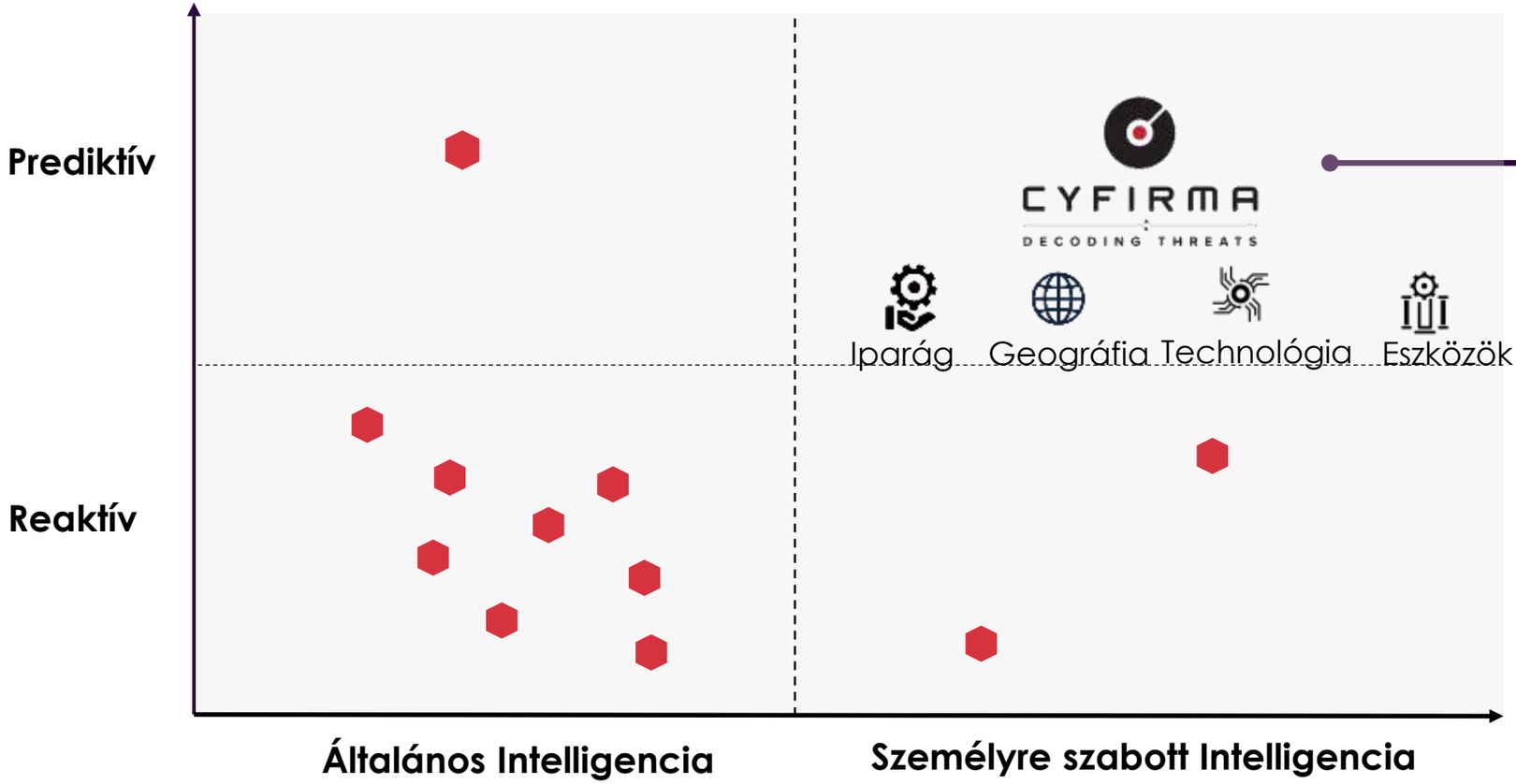
Goldman Sachs, ZODIUS, Z3Partners

5	>100	1.4mn+	145+	25+	~USD 2bn
Régiós jelenlét (Singapore, Japan, India, US, EU)	GB - 8 óránként elemzett adatok	A fenyegetések elemzése és rangsorolása	Előrejelző tanácsadói jelentés	Ügyfelek, akik elkerülték a pénzügyi, hírnévbeli és termelékenységi károkat	Elkerült tárgyi és immateriális veszteségek

CYFIRMA DECODING THREATS

VERSENYKÖRNYEZET

PREDIKTÍV ÉS SZEMÉLYRE SZABOTT KIBERNETIKAI INTELLIGENCIA



FŐ MEGKÜLÖNBÖZTETŐ JEGYEK

Piacvezető és az egyetlen, aki olyan kiberintelligenciát kínál, amely:

- Prediktív
- Személyre szabott - a szervezet eszközei / geográfia / iparág / technológia szerint
- Egyetlen felület – teljes rálátás a fenyegetettségre
- Többszintű – S, M, T
- Kiber-intelligencia kombinálva a támadási felület felderítésével és a digitális kockázatok védelmével
- CISO-k, CRO-k, Security Ops csapatok számára kifejlesztve

Versenytársak

CISO – Chief Information Security Officer

CRO – Chief Risk Officer

DÍJAK ÉS ELISMERÉSEK

A LEGBEFOLYÁSOSABB KIADVÁNYOK ÉS SZERVEZETEK ELISMERÉSE VILÁGSZERTE

Best Practices Award Asia Pacific Cyber Intelligence Technology Innovation Leadership
2020

FROST & SULLIVAN

Recognized as part of Cyber Security TechVision Opportunity Engine
2019

FORRESTER

Now Tech External Threat Intelligence Services
Q4, 2020

Gartner

Recognized in Gartner Tech Radar and Trend Impact Report *2021*
Recognized in Gartner Market Guide for Security Threat Intelligence
2020/2021

IDC

CYFIRMA Recognized for Intelligence-Led Cybersecurity by IDC *2021*

Top 100 Startups
2021

Top 100 Cybersecurity Startups by Cyber Defense Magazine
2020

Global InfoSec Awards by Cyber Defense Magazine
2021

Best Start-up in Asia [CYFIRMA] and Best Cyber Intelligence Solution [DeCYFIR]
2021

iTR

2nd Largest Cyber Intelligence Product Company in Japan
2020

Scale Program
2019 / 2020/ 2021

CYFIRMA
DECODING THREATS

PRIANTO
www.prianto.hu

CYFIRMA

DECODING THREATS

Japan | Singapore | India | USA

KÖSZÖNJÜK

www.cyfirma.com
www.cyfirma.jp

PRIANTO

Prianto Hungary / Prianto GmbH
Róbert Károly Krt. 47/a.
1134 Budapest, Hungary

Tel:+36 1 769 6371
Mob: +36 70 418 7177
Email: contact@prianto.hu
Web: www.prianto.hu

LinkedIn: https://www.linkedin.com/company/prianto-hungary-cee
Facebook: https://www.facebook.com/priantohungary

Sales

- Mario Kosztik (mario.kosztik@prianto.com)
- Mariann Blaskó (mariann.blako@prianto.com)
- Eszter Baté (eszter.bate@prianto.com)

Country Manager

- Olivér Urzica (oliver.urzica@prianto.com)

Marketing

- Anna Birinyi (anna.birinyi@prianto.com)

Presales

- Krisztián Donner (krisztian.donner@prianto.com)