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

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

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

A NAPI MŰKÖDÉS STABILIZÁLÁSA

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

2024

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.

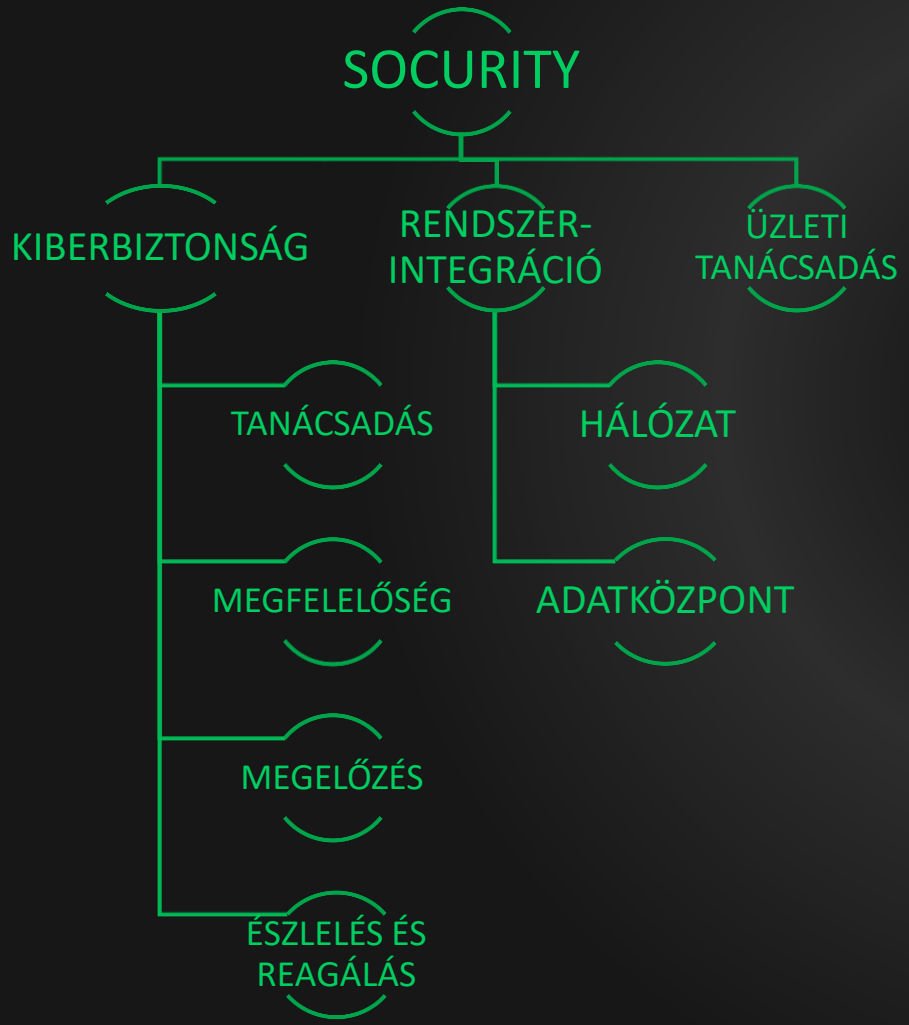
2025

A SOC SZOLGÁLTATÁSAIN KÖVETKEZŐ MÉRFÖLDKÖVE

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

2026

FEDEZZE FEL SZOLGÁLTATÁSAINKAT!



A SOCURITY-nél a digitális korszak üzleti biztonságának élvonalában állunk. Három specializált üzletágunkon keresztül nyújtunk testre szabott megoldásokat:

- Kiberbiztonság
- Rendszerintegráció
- Üzleti tanácsadás

Nem pusztán szolgáltatóként működünk: ügyfeleink hosszú távú partnerei vagyunk a sikerben. A kiválóság, az innováció és a legmagasabb szakmai sztenderdek iránti elkötelezettségünkkel készen állunk arra, hogy vállalkozását a következő szintre emeljük.

KIBERBIZTONSÁGI DIVÍZIÓ

MEGTEREMTJÜK VÁLLALKOZÁSA BIZTONSÁGÁT A FOLYAMATOSAN VÁLTOZÓ KIBERFENYEGETETTSÉG ELLENÉRE

A folyamatos digitális transzformáció korában a kibertámadásokkal szembeni védelem nem lehet alku tárgya. Kiberbiztonsági üzletágunk tapasztalt tanácsadókból és szakértőkből áll, akik mélyen értik a modern vállalatokat érintő összetett kihívásokat.

Átfogó szolgáltatási portfóliónk magában foglalja a stratégiai iránymutatást, a biztonsági architektúra tervezését, a megelőzési megoldásokat, a detektálási és reagálási mechanizmusokat, a megfelelőségi támogatást, valamint a magas szintű szakértői tanácsadást.

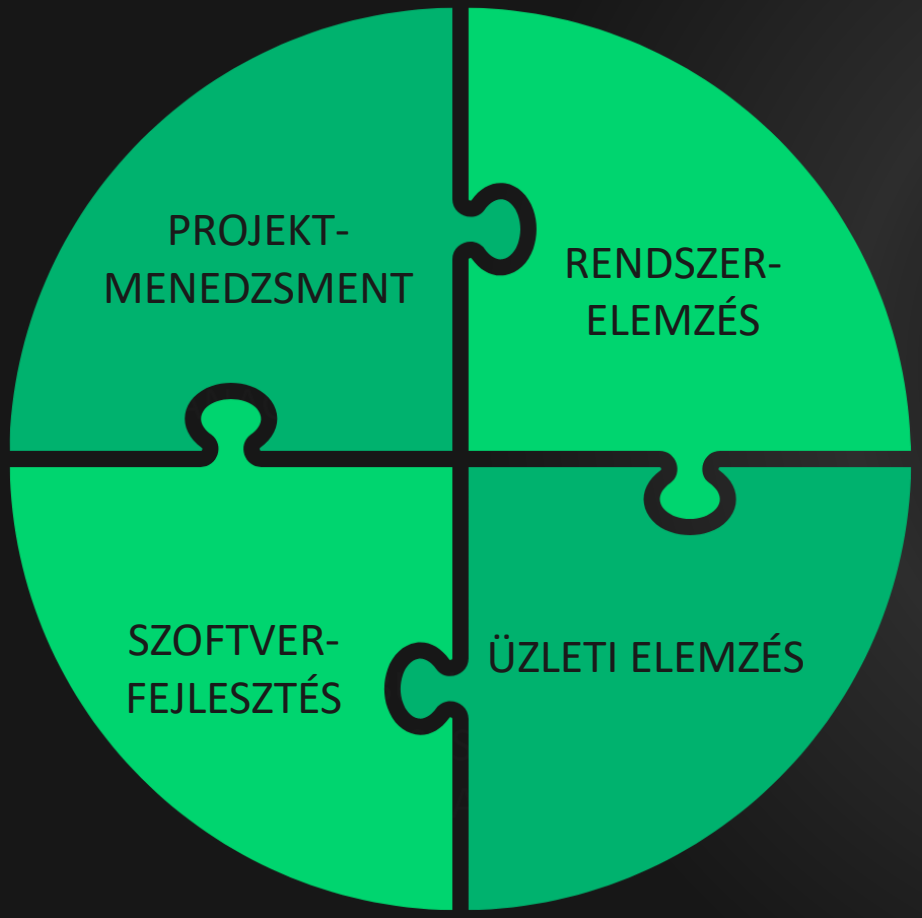
A proaktív védelem iránti elkötelezettségünkkel lehetővé tesszük ügyfeleink számára, hogy magabiztosan navigáljanak az egyre gyorsan változó fenyegetési környezetben.

RENDSZERINTEGRÁCIÓS DIVÍZIÓ

Rendszerintegrációs üzletágunk zöldmezős projektek tervezésére, szállítására, bevezetésére és üzemeltetésére specializálódott, beleértve az on-premise, felhőalapú és hibrid hálózatokat, valamint adatközponti környezeteket.

Emellett kiemelkedő tapasztalattal rendelkezünk barnamezős projektekben is: meglévő rendszerek átfogó felülvizsgálatát végezzük el, frissítéseket hajtunk végre, menedzseljük az eszközbeszerzést és az implementációt, valamint folyamatos üzemeltetési támogatást biztosítunk. A tervezési folyamatunk alapelve a „security by design”, amely garantálja, hogy a biztonság minden projektfázisban központi szerepet kapjon.

ÜZLETI TANÁCSADÁS DIVÍZIÓ



A modern üzleti környezet összetettségében való eligazodáshoz nem csupán stratégiai szemléletre, hanem a megfelelő időben elérhető, releváns szakértelemre is szükség van. Üzleti tanácsadási üzletágunk túlmutat a hagyományos tanácsadási modelleken, és bevezeti az **„Experts-as-a-Service”** szemléletet.

Legyen szó projektmenedzsmentről, üzleti elemzésről, rendszeranalízisről vagy magas szintű szakértői támogatásról, csapatunk zökkenőmentesen illeszkedik ügyfeleink működésébe, és igény szerint biztosít hozzáférést tapasztalt szakemberekből álló erőforrás állományhoz. Ez az innovatív megközelítés biztosítja, hogy ügyfeleink rugalmasak, gyorsan reagálók és felkészültek maradjanak a dinamikusan változó üzleti környezet kihívásaira.

Ügyfeleinket támogatjuk szoftverfejlesztési, automatizációs és egyedi AI-megoldásokkal is; a stabil és hatékony működés érdekében nagy teljesítményű, AI-ready infrastruktúrát tervezünk és szállítunk.

SZOFTVERFEJLESZTÉS

AUTOMATION. INTELLIGENCE. CUSTOM BUSINESS SOFTWARE.

Automatizált tűzfal- és konfigurációs intelligencia: **SyncShield Engine**

Milyen feladatot lát el?

- A **SyncShield Engine** egy újgenerációs automatizációs platform, amely folyamatosan monitorozza, elemzi és szinkronizálja **a tűzfalszabályokat, hálózati objektumokat, szolgáltatásokat és VIP konfigurációkat** gyártófüggetlen környezetekben.
- A manuális karbantartás kiváltásával teljes életciklus-menedzsmentet biztosít: a változások észlelésétől és validálásától az engedélyezésen át egészen a végrehajtásig.

SyncShield Engine by Socurity

FŐ KÉPESSÉGEK

- **Valós idejű változásészlelés:** Folyamatosan figyeli a szabályokat, objektumokat és konfigurációkat, és azonnal azonosít minden módosítást.
- **Automatizált elemzés és egyeztetés:** Összehasonlítja az aktuális és a korábbi állapotokat, kiemeli az eltéréseket, és frissíti az SQL-alapú konfigurációs adattárat.
- **Jira-integráció:** Automatikusan részletes change ticketeket hoz létre, biztosítva a teljes nyomon követhetőséget és az auditkész működést.
- **Kétirányú szinkronizáció:** Összhangban tartja a tűzfalszabályokat és a Jira Insight CMDB elemeket, garantálva a konzisztenciát.
- **Átfogó objektumintelligencia:** Pontosan kezeli a címobjektumokat, csoportokat, szolgáltatásokat, szolgáltatáscsoportokat, hozzáférési listákat és VIP objektumokat.
- **Export, riportálás és audit:** Strukturált naplókat, jelentéseket és exportokat készít mérnöki, SOC-, megfelelőségi és ügyfélkommunikációs célokra.

Automatizált tűzfal- és konfigurációs intelligencia: **SyncShield Engine**

Üzleti értékteremtés

- **Jelentős működési hatékonyság:** Automatizálja a konfigurációs eltérések kezelését, csökkenti az emberi hibák kockázatát, és jelentősen lerövidíti a mérnöki ráfordítást.
- **Erősebb biztonsági szint:** A folyamatos monitorozás és validáció révén lehetővé teszi az incidensek proaktív megelőzését.
- **Megfelelőségre felkészített működés:** Biztosítja minden tűzfalváltozás teljes körű dokumentálását, nyomon követhetőségét és auditálhatóságát.
- **Skálázható és gyártófüggetlen:** Jira- és egyéb IT/SecOps platformokkal való integrációra tervezve, vállalati méretű környezetek támogatásával.

SZAKÉRTŐI SZOLGÁLTATÁSAINK

SCALABLE. AFFORDABLE. PREDICTABLE.

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

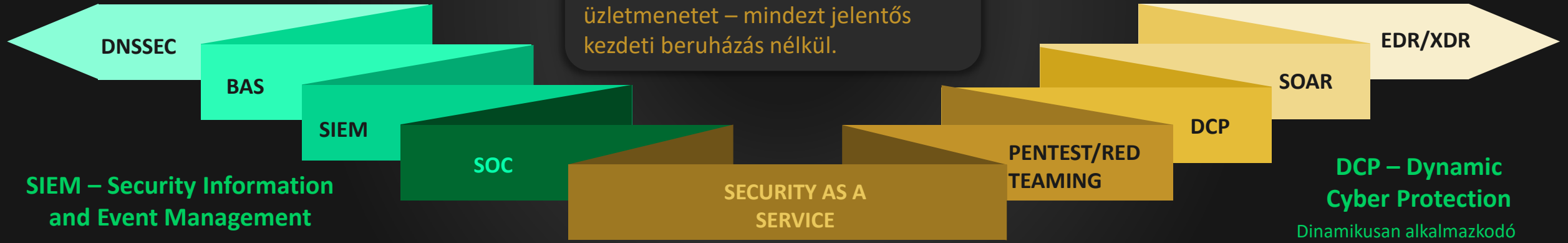
Automatizált technológia, amely kibertámadásokat szimulál a környezet ellen. Biztosítja, hogy a meglévő biztonsági kontrollok valós körülmények között is hatékonyan működnek.

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.

MESTERSÉGES INTELLIGENCIA

AUTOMATION. INTELLIGENCE. CUSTOM BUSINESS SOFTWARES.

MESTERSÉGES INTELLIGENCIA– MEGOLDÁSAINK

AI infrastruktúra és célzottan tervezett hardver

- **Nagy teljesítményű, AI-optimalizált adatközponti infrastruktúrákat** tervezünk és szállítunk, amelyek alkalmasak tanítási (training), következtetési (inference) és nagyléptékű analitikai terhelések kiszolgálására.
- Hardvermegoldásaink **GPU-gyorsított rendszerekre** épülnek a maximális áteresztőképesség és hatékonyság elérése érdekében.
- Teljes körű integrációs szolgáltatásaink biztosítják, hogy a számítási kapacitás, a tárolás, a hálózat és az MLOps **folyamatok egységes, biztonságos és magas rendelkezésre állású AI platformként** működjenek együtt.

Egyedi, vállalati AI megoldások

- Az IBM watsonX portfóliójára építve **teljes mértékben testreszabott AI- és gépi tanulási megoldásokat** tervezünk és valósítunk meg, amelyek konkrét üzleti kihívásokat kezelnek – nem általános modelleket, hanem az Ön folyamataihoz, adataihoz és céljaihoz igazított rendszereket.
- Platformjaink lehetővé teszik az **AI-alapú folyamatautomatizálást, a valós idejű döntéstámogatást, az intelligens munkafolyamatokat,** valamint a meglévő vállalati rendszerekbe történő zökkenőmentes integrációt.
- Csapatunk a teljes életciklust lefedi: **adatfelmérés, adattisztítás, anonimizálás, feature engineering, model- és MLOps működtetés**, valamint folyamatos optimalizálás a hosszú távú pontosság és üzleti érték biztosítása érdekében.

TANÚSÍTVÁNYAINK

PROVEN AUTHENTICITY.

TANÚSÍTVÁNYAINK

Biztonsági tanúsítványaink

- Létesítménybiztonsági minősítés
- Nemzetbiztonsági átvilágítás (személyes minősítés a tulajdonosunk részére)

Minőségbiztosítási tanúsítványaink

- ISO/IEC 27001:2022

- EcoVadis Silver Badge, (90% for Ethics)

- CyberVadis Platinum Badge, (986/1000)

Gyártói tanúsítványaink

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

ÜGYFÉLPROJEKTJEINK, REFERENCIÁK

Stratégiai ügyfeleink

MÁV

2021

SIEM megoldások

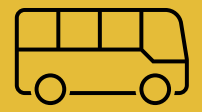
IBM Qradar licenszek
IBM Qradar megújítás

Energiaipari vállalat

2021-től – jelenleg is

SOC feladatok

Biztonsági fókuszú rendszerintegrációs, bevezetési és tanácsadási feladatok ellátása egy nemzetközi energetikai vállalat Security Operations Center (SOC) szervezetének részeként.



Logisztika& Személyszállítás

Stratégiai partnerség

Stratégiai biztonsági szolgáltató

Egy nemzetközi logisztikai és szállítmányozási vállalatnál: hálózati és hálózatbiztonsági szállító
Legutóbbi eredmény: 92%-os megfelelés a NIS2 auditértékelésen

Pénzügy és biztosító

Stratégiai partnerség

Stratégiai biztonsági szolgáltató

Egy nemzetközi biztosítótársaságnál:

- hálózati és hálózatbiztonsági szállító
- DLP projekt sikeres lezárása

Folyamatban: átfogó adatközponti projekt + AI transzformáció

KÖZBESZERZÉS

Társaságunk szerződött szállítóként vesz részt

- a HNET keretmegállapodásban (aktív és passzív hálózati infrastruktúra), valamint
- az ITBT keretmegállapodásban (IT-biztonsági termékek és szolgáltatások),

amelyeket a DKÜ (Digitális Kormányzati Ügynökség) által lebonyolított, nyílt és központosított közbeszerzési eljárások keretében ítéltek oda.
E keretmegállapodások lehetővé teszik, hogy ügyfeleink számára jogszabályi megfelelés mellett, előre meghatározott szerződéses feltételek szerint biztosítsunk nagy volumenű, kritikus hálózati és kiberbiztonsági megoldásokat a közszférában.
Részvételünk garanciát jelent arra, hogy megfelelünk a magas szintű műszaki, pénzügyi és szabályozási követelményeknek, amelyek elengedhetetlenek a kiemelten bizalmi, államigazgatási környezetben történő működéshez.

DKÜ
Digitális Kormányzati Ügynökség Zrt.

A HNET és az ITBT együttműködése révén ügyfeleink számára stabil, hosszú távon fenntartható szolgáltatási jelenlétet biztosítunk a közszférában, miközben megerősítjük szerepünket a nemzeti digitális és kiberbiztonsági infrastruktúra megbízható szakmai partnerként történő fejlesztésében.

LEGFŐBB GYÁRTÓINK

AI

watsonx

Network, Infrastructure and Security Solutions

cisco, DELL, JUNIPER NETWORKS, FORESCOUT, FORTINET, paloalto NETWORKS, ARISTA, RUCKUS COMMSCOPE, veeam, CHECK POINT

SIEM

splunk> a CISCO company, IBM QRadar

Identity and Access Management

DUO, cisco, BeyondTrust, CYBERARK

Endpoint Security

CROWDSTRIKE, ivanti, jamf, SentinelOne

User and Data Security

Forcepoint, THALES, proofpoint

Cloud Security

PRISMA BY PALO ALTO NETWORKS, IBM, zscaler

Vulnerability Management

Qualys, tenable, PICUS

Threat Intelligence

QUOINTELLIGENCE

Application Security

invicti, Acunetix by Invicti, radware, BLACKDUCK, imperva

PARTNEREINK ÉS SZAKTERÜLETEINK

Hálózatbiztonság

- Palo Alto
- Fortinet
- Check Point
- Forcepoint
- Forescout

Endpoint Detection and Response (EDR)

- CrowdStrike Falcon
- SentinelOne

Adatvédelem és mentési megoldások

- Veeam
- Thales
- Rubrik

Digitális kockázatok elleni védelem

- PhishLabs
- SOCradar

Alkalmazásbiztonság

- Radware
- Acunetix
- Blackduck

Jelszó management

- Bitwarden
- Keeper
- 1Password

Végpont-biztonság

- CrowdStrikeFalcon
- Ivanti
- SentinelOne
- Trend Micro ApexOne
- Trend Micro ScanMail Suite for Microsoft Exchange
- Trend Micro PortalProtectSuite for Microsoft SharePoint

Fenyegetettségvizsgálat és -elemzés

- DarkEcho Intelligence
- Quointelligence
- Intel471
- SOCradar
- Hunter.io
- flare.io
- hudsonrock
- intelx.io
- Joe Sandbox
- Anyrun
- Shodan
- PhishLabs
- DomainTools
- Maltego

Sandbox and Advanced Threat Protection

- FortiSandbox
- CheckPoint SandBlast
- Trend Micro Deep Discovery Analyzer
- AC-HunterNetwork ThreatDetection

Biztonságtudatosság fejlesztése

- Proofpoint Security Awareness Training (PSAT)
- Hoxhunt

Hálózat és Infrastruktúra

- Arista
- Cisco
- IBM
- Meraki
- CambiumNetworks
- Juniper
- Ruckus
- Dell
- Vertiv
- Infoblox

Sérülékenység Management

- Qualys
- Tenable
- Picus

Felhőbiztonság

- Zscaler
- Cloudflare
- IBM Cloud
- Prisma (Palo Alto Networks)
- Datadog (cloudSIEM)
- Panther (cloudSIEM)

Privilegizált hozzáférés-kezelés

- CyberArk
- BeyondTrust

További megoldásaink

- Microsoft: átfogó IT és kiberbiztonsági megoldás
- Nozomi: OT és IoT biztonság.
- Galleon Systems: NTP servers and network clocks.
- VirusTotal: Online malware elemzés
- Netcraft: Internet security services

Köszönöm a figyelmet!

Lépjen velünk kapcsolatba:

sales@socurity.hu
+36 70 375 2623