SOCURITY

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

SIEM A FRAUD ELLENI KÜZDELEMBEN

IBM QRadar szerepe a modern fraud és kiberfenyegetések felismerésében és kezelésében

Szijjártó Viktor
Cybersecurity engineer
sales@socurity.hu

Pénzintézeti Fraud konferencia, 2026.04.21. , Budapest

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 költséget jelent, 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

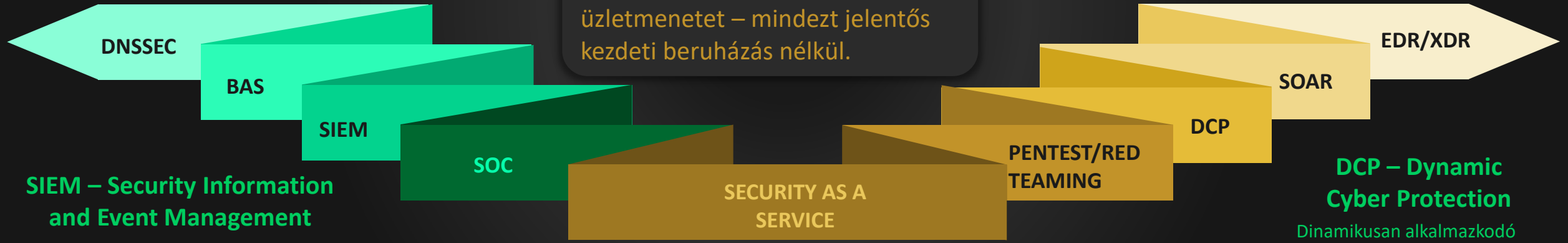
Automatizált technológia, amely kibertámadásokat szimulál a környezet ellen. Biztosítja, hogy a meglévő biztonsági kontrollok valós körülmények között is hatékonyan működnek.

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.

EGY NAP A PÉNZINTÉZET ÉLETÉBŐL – AMIT NEM LÁTUNK

A pénzügyi szektor az egyik legtöbbet támadott iparág – globális adatszivárgások 27%-a

Csak 2025 első felében több mint 2,47 milliárd $ értékű kriptovalutát loptak el kibertámadások és csalások révén, meghaladva a 2024-es teljes éves veszteséget.

Bybit tőzsde 2025 február - 1,45 milliárd $ értékű Ethereum - legnagyobb egyedi kriptovaluta-lopás.

AI Fraud - A pénzügyi szervezetek 45%-a AI által vezérelt kibertámadási kísérletet - banki megszemélyesítésre irányuló deepfake hangalapú csalások.

Az EU pénzügyi szektorában bekövetkezett behatolások közel 60%-a phishing és social engineering

THREAT LANDSCAPE – 2 NAGY CSOPORT:

Belső fenyegetések
(insider threat)

Külső támadások
(APT, ransomware)

THREAT LANDSCAPE

INSIDER THREAT

01

Belsős alkalmazott privilegizált jogosultságokkal

02

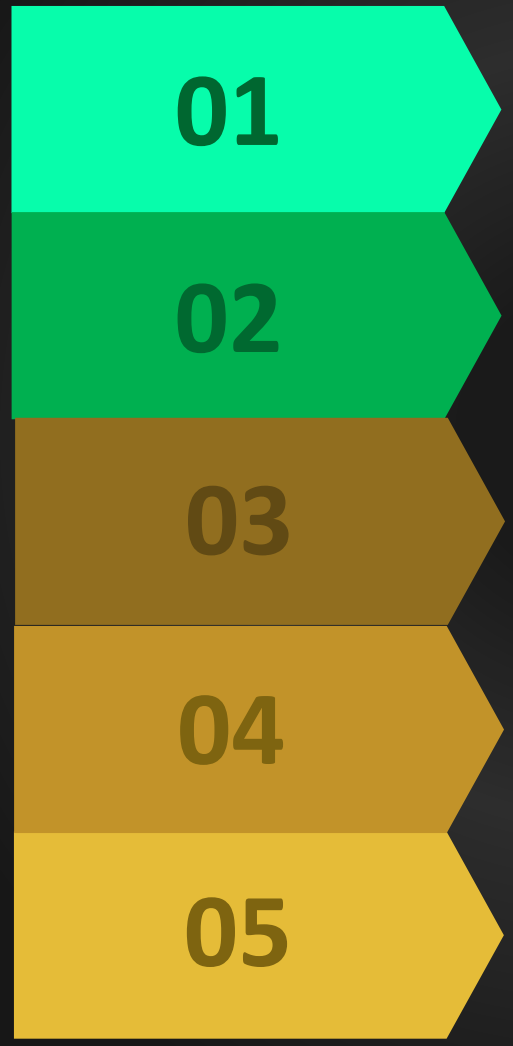
Hozzáfér a szervezet rendszereihez, adataihoz, infrastruktúrájához

03

Szándékos káros célok – adatlopás, szenzitív információkkal való kereskedés

THREAT LANDSCAPE

KÜLSŐ TÁMADÁSOK



APT – Államilag támogatott hackercsoportok

Kémkedés, kritikus infrastruktúra megbénítása, piaci stratégiai előny megszerzése

Ransomware – Zsarolóvírus

Váltságdíj kripto a szenzitív titkosított adatok visszafejtéséért

Ha nem fizetnek -> Adatok kiszivárogtatása

FRAUD TÍPUSOK

Account takeover (ATO)

Felhasználói fiók támadó általi megszemélyesesítése

Business Email Compromise (BEC)

Céges e-mail cím támadó általi megszemélyesítése

Synthetic Identity Fraud (SIF)

Hibrid személyazonosság (valós + kitalált)

Card-not-present Fraud (CNP)

- Visszaélés lopott adatokkal
- Kártyaadatok megszerzése - Phishing, Social Engineering, Darknet (Fullz)
- Tranzakciók fizikai kártya nélkül

A DETEKTÁLÁS PROBLÉMÁJA ÉS KIHÍVÁSAI

Silo struktúra - széttagoltság

- Core banking rendszerek (legacy)
- Modern digitális megoldások (mobilbank)
- Különböző fraud rendszerek

Kihívás:

- Korlátozott logolás
- Nehéz integráció
- Rendszer nem lecserélhető
- Központi vizibilitás hiánya
- Korreláció hiánya

MI AZ IBM QRADAR?

SIEM – Security Information and Event Management

- Logelemző rendszer – SOC központi eleme
- Korrelációs engine

- Valós idejű, usecase és ML alapú detekció
- Log és flow adatok elemzése
- Riasztások kontextus alapján
- On-premise / hybrid / cloud

UEBA

QRadar UEBA (User and Entity Behavior Analytics)

- Baseline viselkedés felépítése Machine Learning segítségével

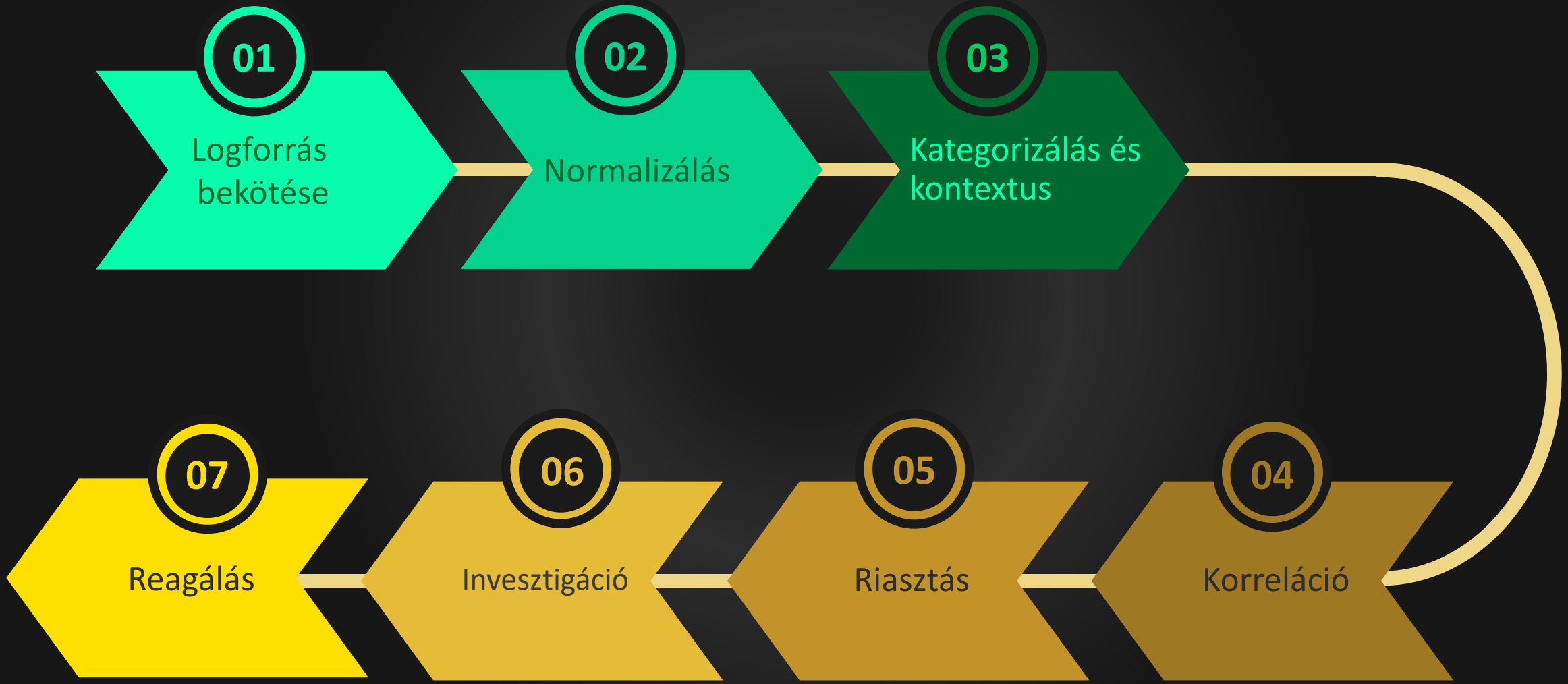
Anomália detektálás:

- Munkaidőn kívüli hozzáférések
- Szokatlan volumenű adatforgalom
- Jogosultság-módosítás

Qradar WatsonX AI Investigation Assistant

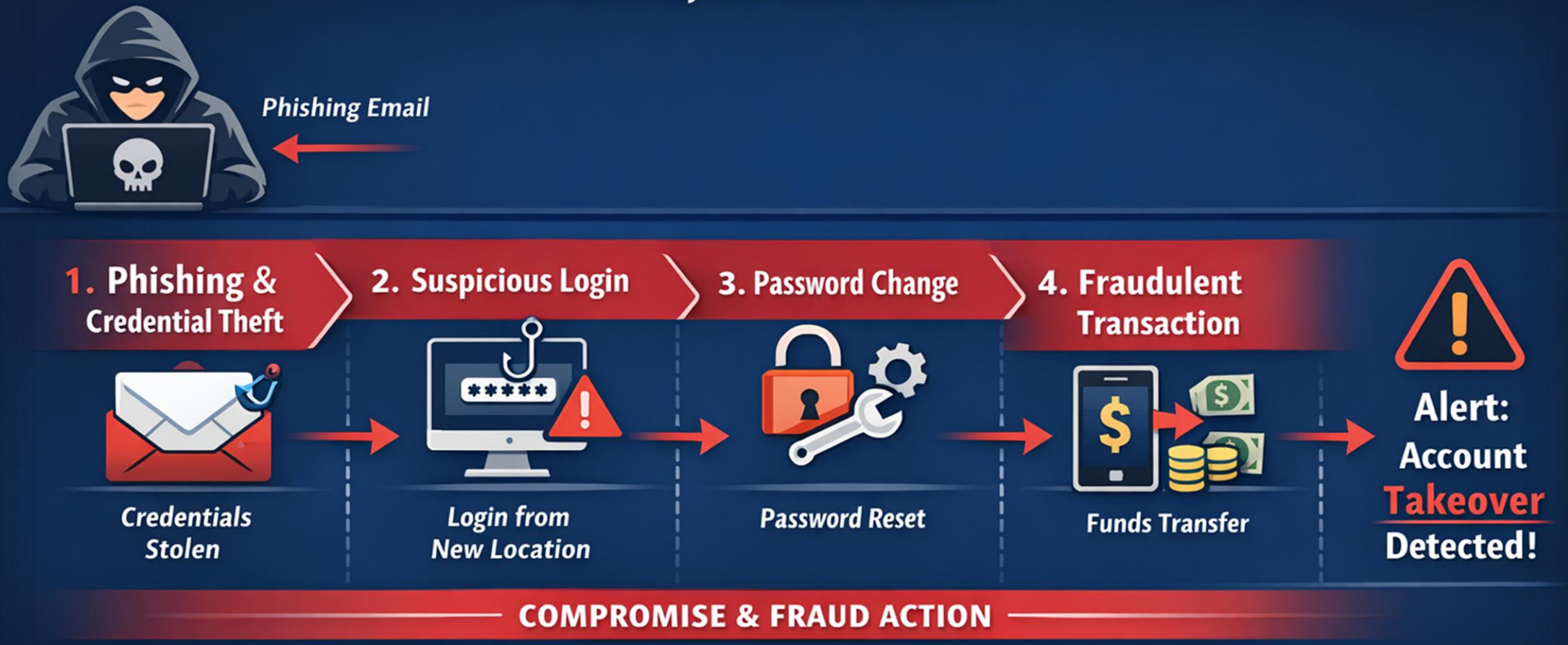
- Qradar AI chat-en lévő kérdések megválaszolása
- Offense-összefoglaló
- Javaslatok response lépésekre
- AQL query

IBM Qradar működése



Use Case 1: Account Takeover Attack

A Fraud & Cyber Attack Scenario



Use Case 2:

Insider Fraud

A Cyber & Fraud Attack Scenario

1 Off-Hours Login

Unusual Activity
Late Night Access

2 Sensitive Data Access

Bulk Download
of Customer Data

3 Suspicious Export

Large Data Transfers
External Uploads

4 Fraud Indicators

Unauthorized Actions
Policy Violations

Alert: Insider Fraud Detected!

Use Case 3:

Credential Stuffing Attack

A Mass Login Attack Using Stolen Credentials

1 Stolen Credentials

Leaked Username & Password Lists

2 Botnet Automation

Bots Attempt Thousands of Logins

3 Mass Login Attempts

Targeting Banking, Web & Cloud Apps

4 Account Takeover

Successful Logins Lead to Fraud & Theft

Alert: Credential Stuffing Detected!

A RENDSZER ÜZLETI ÉRTÉKE

IBM tanulmány alapján:

- SOC hatékonyság növekedése: + **~40%**
- Gyorsabb detekció
- Fraud veszteség csökkentés
- Reputációs kockázat mérséklése
- Compliance támogatás
- Szabályozói bírságok elkerülése

ÖSSZEFOGLALVA

- A fraud és a kibertámadások összefonódnak → Integrált védelemre van szükség
- A QRadar kontextust ad az eseményeknek → gyorsabb, pontosabb detektálás
- A megfelelőség (DORA, PSD2) nem teher, hanem lehetőség az automatizálásra

Köszönöm a figyelmet!

Lépjen velünk kapcsolatba:

sales@socurity.hu
+36 70 375 2623