Hogyan tegyünk ütőképesebbé egy SOC-ot?

Horváth Gergely Krisztián CISA CISM CDPSE
Quadron Kibervédelmi Zrt.

EIVOK HTE-SOC minikonferencia - 2023.05.25.

Tartalomjegyzék

Quadron Kibervédelmi Zrt.

Kiberbiztonsági tanácsadó, integrátor és adatelemzési szakértő cég, fő területünk a biztonság!

- Magántulajdonban lévő független nemzetközi cég
- Széleskörű együttműködés Európában
- Budapesti központ, leányvállalat Bahreinben
- 2014-ben alapították, a biztonsági piacon szerzett tapasztalat a 90-es évektől

- Senior biztonsági szakértők, elemzők és mérnökök, több mint 25 éves szakmai tapasztalattal
- A csapat és a hálózat:
  - Több, mint 40 biztonsági szakértő a belső csapat
  - 100+ tanácsadó, mérnök, elemző és fejlesztő

- Piaci fókuszunk: Magyarország, Közel-kelet, Európa, USA, Afrika
- Referenciák a pénzügyi kormányzati, telekommunikációs és olajipari szektorokból
- Több mint 100 aktív ügyfél

FILOZÓFIÁNK – Cyber Resilience

Minden vállalatnak képesnek kell lennie megszakítások nélkül végezni az üzleti tevékenységét!

Minden kritikus adatokat kezelő szervezetnek rendelkeznie kell egy jó kiberbiztonsági tervvel!

Fókuszáljon arra, amit a legjobban csinál!

Mi az Ön kiberbiztonsági védelmét a fenyegetésekkel és kockázatokkal összhangban építjük ki, gondoskodva az üzletmenet ellenálló képességéről és folytonosságáról.

Nincs fennakadás!

A BIZTONSÁGBA VALÓ BEFEKTETÉS
Életciklusok

Tervezés

Meghatározzuk szervezete biztonsági stratégiáját, piaci és megvalósíthatósági elemzést, kockázatértékelést, SW/HW és architektúra tervezést végzünk a megfelelőségi követelményei alapján.

Beszerzés

Elkészítjük az igényfelmérést, gyártó és szállítói elemzéseket, támogatjuk az RFI/RFP készítést, a pályázati eljárást és értékeljük az ajánlatokat az Ön nevében.

Támogatás és üzemeltetés

Naprakészen tartjuk kiberbiztonsági védelmét akár 7x24-es üzemeltetéssel és támogatással, penetrációs teszteléssel, sérülékenység vizsgálattal, biztonsági műveleti és incidenskezelési szogláltatásokkal

Implementáció

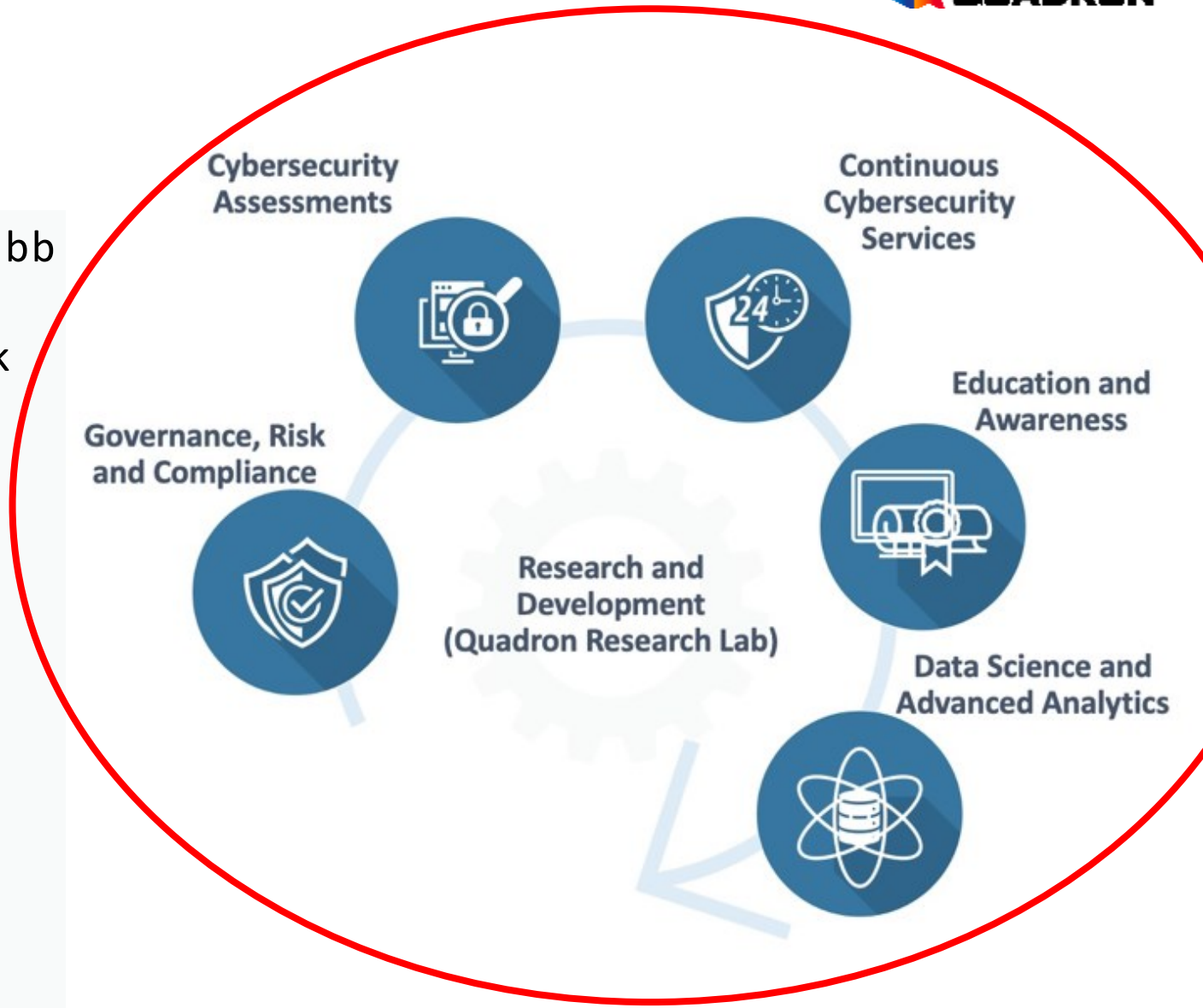
Projekttervezés, rendszertervezés, konfiguráció, optimalizálás és frissítés, HW/SW implementáció és integráció! Az implementációs projektet minőségmenedzsmenttel valósítjuk meg.

ÉRTÉKAJÁNLATUNK
Biztonság. Megerősítve.

A független szakértői tudásunk és a legújabb technológiák és módszerek ötvözésével, a kockázati és kiberbiztonsági szolgáltatások teljes palettáját kínáljuk szervezetére szabottan.

Szolgáltatásaink testreszabott kiberbiztonsági védelmet biztosítanak, összhangban a szervezetét érintő fenyegetésekkel és kockázatokkal.

Biztonság. Megerősítve.



QUADRON SOC
Biztonsági Műveleti Központ

Így dolgozunk:

- 1-3 szintű elemzők, incidenskezelők és multinacionális vállalati háttérrel rendelkező CSIRT-szakértők
- 5/8 – 24/7 működési ablak
- Partnerség a vezető SOC technológiai szállítókkal a SIEM, SOAR és Threat Intelligence területeken
- AI és ML alapú fejlett elemzés olyan vezető szállítókkal, mint a SAS, az Elastic és a Fortinet

SOC szolgáltatási portfóliónk:

- Fejlett biztonsági elemzés
- Naplógyűjtés, incidenskezelés és monitoring
- Események észlelése és reagálása
- Threat Intell and hunting
- Riasztás és jelentés
- SOC értékelés és építés
- Folyamatos penetrációs tesztelés
- Bugbounty
- Személyre szabott szolgáltatások
- B-O-T SOC modell

SOC megerősítése projekt

Felmérés

- Vezetői elvárások
- Architektúra
- Folyamatok
- Képességek

Tervezés

- Komplex fejlesztési terv
- Incidenskezelés
- SOC
- BCMS

Implementáció

- Gyakorlat, Képzés
- Szabályozás
- False pozitív csökkentése
- Kommunikáció

Támogatás

- Folyamatos szakértői keret biztosítása
- Rendszeres gyakorlatok
- Visszamérés

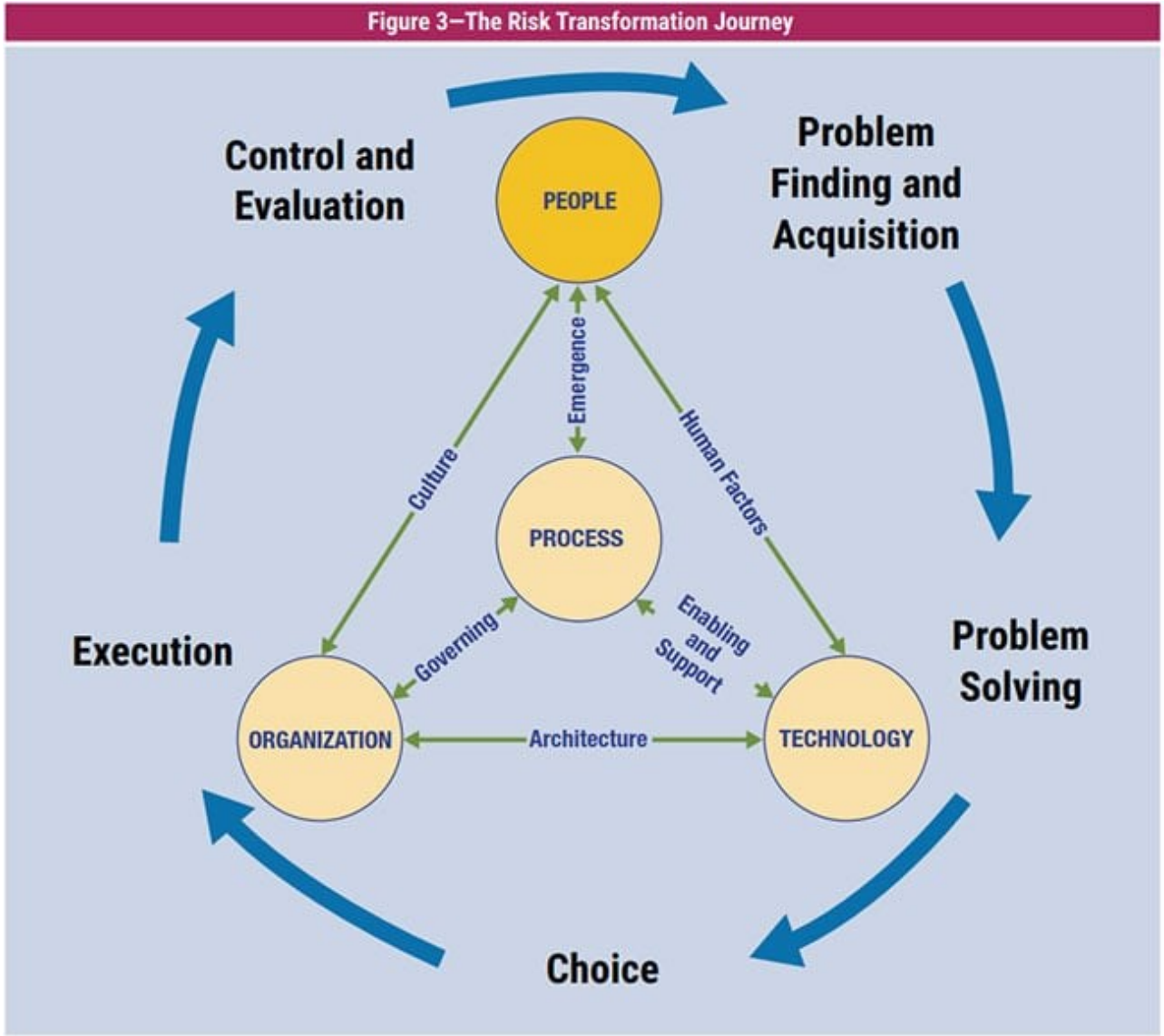
Incidenskezelés holisztikus fejlesztése

Azonosítjuk a **vezetői elvárásokat és külső követelményeket**.

Felmérjük az incidenskezeléshez kapcsolódó **IT infrastruktúrá**t és **SOC eszközök**et.

Felülvizsgáljuk az eljárásrendeket és **folyamatok**at, felmérjük a **szervezet** és a **kollegák képességei**t.

A **komplex incidenskezelés fejlesztési terv**et készítünk és valósítunk meg.



ISACA BMIS alapú holisztikus modell

Hogyan készüljünk fel egy kibertámadásra?

Kontrolláld az adatot
- Adatvagyon leltár
- Védendő adatok
- Adatgazdák és felelősségek

Kontrolláld az infrastruktúrát
- Technológiák
- Architektúra
- Alkalmazások
- Folyamatok

Kontrolláld a felhasználókat
- Azonosítás
- Autentikáció
- Jogosultságok
- Kiemelt és szerviz felhasználó

Kontrolláld az információ áramlást
- Publikus és privát hálózatok
- Távoli elérések
- Publikus és privát felületek

Biztonsági szabályok és kontrollok
- Biztonság menedzsment
- Fejlesztés biztonság
- Hálózat biztonság
- Végpont védelem
- Adatbiztonság

Teszteld az ellenálló képességet
- Sérülékenység vizsgálat
- Forráskód elemzés
- Rendszer hardening
- Jogosultság felülvizsgálat

Kezeld a biztonsági incidenseket
- Incidenskezelési folyamat
- Incidenskezelési technológiák
- Incidenskezelési kompetenciák
- Krízis kezelés
- Forgatókönyvek

Készülj fel a váratlanra
- Elemzések
- Threat hunting
- Gyakorlatok

A megszerzett tapasztalatokkal folyamatosan fejleszd a védelmet!

Ütőképesség növelő lehetséges intézkedések

Szervezési és oktatási intézkedések

- **Irányítási gyakorlatot tartunk** a szervezet vezetői részére kiber incidens esetére
- **Incidenskezelési folyamat és eljárásrend** részletes kidolgozása és oktatása
- **Gyakorlatok**kal csoportos képesség fejlesztést végzünk (incidenskezelés, belső és külső kommunikáció,
- **Egyéni fejlesztési tervet** készítünk, amely kollegának ez szükséges
- **BCMS rendszer**t vezetünk be - Üzleti folyamat leltár és hatáselemzés (BIA), BCM **szabályzat és tervek,**

Technológiai és mérnöki intézkedések

- **False pozitív alertek** számának csökkentése riasztások felülvizsgálatával
- **Chatbot bevezetése** a felhasználókkal való kommunikáció automatizálására
- **MasterCard CyberFront** bevezetése a fenyegetések valós idejű éles környezetben való tesztelésére

Kérdések, elérhetőségeim

Kérem keressen kérdéseivel:

Gergely.horvath@quadron.hu,

vagy

linkedin.com/in/infosecevangelist/