HADMÉRNÖK

XIII. Évfolyam 2. szám – 2018. június

A SECURITY OPERATIONS CENTER (SOC): A KIBERBIZTONSÁGI CSAPATMUNKA ÉS KIHÍVÁSAI

THE SECURITY OPERATIONS CENTER (SOC): TEAMWORK AND ITS CHALLENGES IN CYBERSECURITY

HÁMORNIK Balázs Péter

(ORCID: 0000-0001-8085-1259)

hamornik@erg.bme.hu

Absztrakt

A kiberbiztonsági munka eddig jellemzően technológiai szempontból került a honvédelem fókuszába, lehetővé téve a megfelelő eszközök beszerzését és üzemeltetését. Azonban az technológiai és az egyéni munka szintjén felül a csapatban végzett kiberbiztonsági munka is figyelmet érdemel. A biztonsági műveleti központok azaz Security Operations Center (SOC) és Computer Emergency Response Team-ek (CERT) a kibervédelem kulcs szervezeti egységei. E részlegekben a megfelelő csapattagok kiválasztása, megtartása, együttműködésük feltételeinek biztosítása és fejlesztése a hatékony biztonsági monitorozás egyik záloga. Tanulmányomban e csapat szintű tényezőket tekintem át.
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *Security Operations Center, kiberbiztonság, csapatmunka, emberi tényezők*

Abstract

Cybersecurity is an emerging field of national security where usually the technical aspects of defence take the first place. The cyber defence is heavily relaying on teamwork where the members of SOC (Security Operations Center) or CERT (Computer Emergency Response Team). To make cybersecurity monitoring and incident response efficient human factors are required to be taken into consideration such as selection and retention of team members, enabling and enhancing their collaboration by tools and skills. In this study, these team level features of setting up and operating a SOC are reviewed.
The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in the Ludovika Research Group.

Keywords: *Security Operations Center, cybersecurity, teamwork, human factors*

A kézirat benyújtásának dátuma (Date of the submission): 2018.01.28.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.02.06.

BEVEZETÉS

A kiberbiztonság napjainkban az egyik elsőszámú nemzetbiztonsági területté válik világszerte. A különböző nemzetek ezzel a kihívással különleges kibervédelmi alakulatok létrehozásával tudják sikerrel felvenni a harcot. Az ilyen csapatok közül az egyik leghatékonyabb a „Computer Emergency Response Team" (CERT – számítógép vészhelyzet kezelő csoport) vagy más néven "Computer Security Incident Response Team" (CSIRT – Számítógép biztonsági incidens kezelő csoport). Egy ilyen csapat képes egy szervezetet vagy hasonló szervezetek csoportját védeni. A siker kulcsa esetükben a kiberbiztonsággal kapcsolatos információ folyamatos gyűjtése és elemzése. Ez a folyamatos felügyelet megvalósítható biztonsági műveleti központ formájában (Security Operations Center – SOC), amely napjaink modern incidenskezelésnek központi eleme [1].
Magyarországon számos CERT vagy CSIRT létezik, amelyek egy része a piaci cégeket védi, és vannak, amelyek törvényi előírás alapján jöttek létre. Ez utóbbiak közé tartozik a CERT-Hungary, amely a teljes magyar kormányzati és önkormányzati incidenskezelésért felelős. Emellett a MILCERT látja el a Magyar Honvédség kiberbiztonsági incidenseinek kezelését. Annak ellenére, hogy e szervezeti egységek között az együttműködés alapvető fontosságú első lépésben a belső működésük, saját csapatuk megszilárdítására kell fókuszáljanak [2]. Sajnos az információbiztonság és kibervédelem legnagyobb problémája a világszintű szakemberhiány. Katonai területen ez akár egyszerűen az állománynak erre a területre való vezénylésével is megoldható lenne, azonban ezek a hagyományos megoldások nem működnek jól napjaink tudásközpontú munkaköreiben, amilyen a kiberbiztonság is. Emiatt is jelentős fontosságú a kiberbiztonság, és ezen belül is a csapatmunka human aspektusának vizsgálata, amelynek eredményei segítségével támogathatók hazánk nemzetbiztonsági törekvései a kibervédelemben.

A kiberbiztonság területén az utóbbi időben a figyelem fókuszába egy specializált műveleti célú szervezeti egység került: a biztonsági műveleti központ vagy ismertebb angol rövidítése szerint a SOC (Security Operations Center). A szervezetek és a szervezeti egységek olyan kihívásokkal nézne szembe napjainkban, mint az általános szaktudás és az emberi erőforrások hiánya a szektorban annak következtében, hogy nagymértékben megnőtt az igény a kiberbiztonsági szakemberekre. Ez nehézséget gördít a SOC-k kialakítása elé. Ennek okán a klasszikus tankönyvi, 3 vonalból álló SOC megvalósítása gyakran nem lehetséges, hanem szolgáltató partnerek bevonásával kell a megoldást megtalálni. Elöljáróban fontos kiemelni, hogy a jó SOC nem csupán egy riasztásfeldolgozó műveletsor, hanem fenyegetettségekkel kapcsolatos hírszerzési (Threat Intelligence, TI) adatok felhasználója és előállítója, amely szoros kapcsolatban dolgozik az incidenskezelést ellátó csapattal (hacsak ez nem a SOC része is egyben), illetve proaktívan keresi a lehetséges fenyegetettségeket (hunting). A SOC nemcsak saját, szervezeten belüli formában valósítható meg, hanem kiszervezetten, szolgáltatók által is. Az ilyen szolgáltatókkal különböző hibrid modellek alakíthatók ki a SOC bizonyos részeinek, funkcióinak házon belül tartására, illetve kiszervezésére. Jellemző az első vonalbeli riasztáskezelés és a TI partnerek általi biztosítása.

Minden SOC számra elsődleges kihívás a rálátás megteremtése és biztosítása a védeni kívánt informatikai rendszerre. Mielőtt bármely szervezet is belevágna egy SOC kialakításába, lényeges, hogy fenntartható költségvetést tervezzen be az üzemeltetése első két-három évére. Ennyi időre mindenképp szükség van a csapat, a folyamatok és a technológia kialakulására, megszilárdulására. Ennél hamarabb elvárni a befektetések megtérülését idejekorán véget vethet az SOC életének.

A BIZTONSÁGI MŰVELETI KÖZPONTOK FOGALMA ÉS MODELLJEI

A biztonsági műveleti központ vagy SOC (Security Operations Center) egy olyan csapatot jelent, amely éjjel-nappali műszakban működik, és amelynek egyaránt feladata a megelőzés, a felderítés és a kiberbiztonsági fenyegetésekre, eseményekre adható válaszok kidolgozása, valamint a szervezet vagy létesítmény biztonsági előírásainak vizsgálata és értékelése [3].

Amellett, hogy egy szervezet a saját maga védelmére létrehoz egy SOC-ot, üzletileg sok esetben előnyösebb, ha más, erre szakosodott szolgáltatóktól veszi igénybe a biztonsági műveleti központok nyújtotta állandó védelmet. Ezt a szolgáltatást „Managed SOC”-nak nevezik, és a szolgáltatást egy „Managed Security Service Provider” (MSSP – menedzselt biztonsági szolgáltató) szervezet nyújtja. A menedzselt szolgáltatás egy megosztott erőforrásokból felépülő szolgáltatás, amely nemcsak egyetlen szervezetre vagy személyre épül. Az SOC ilyenkor földrajzi elhelyezkedésében elkülönül a védelme alá tartozó szervezettől, akár külön kontinensen is lehetnek. Egy MSSP és annak SOC-csapatai egyszerre több szervezetet is kiszolgálnak különböző kibervédelmi szolgáltatásokkal (például a SOC mellett forensics (igazságügyi) vagy malware (rosszindulatú szoftver) analízis).

Egy teljesen működőképes SOC állandó üzemet igényel, legalább 8-10 fővel. Csak a fenntartáshoz két ember szükséges műszakonként, akik párosával, 12 órás váltott műszakokban dolgoznak 3 vagy 4 napot, egyenlő arányú pihenőnapokkal. Ez egy kétfős műszak esetén lehetővé teszi, hogy egy fő monitorozással, míg a másik a kivizsgálásokkal foglalkozzon, valamint jól megoldott a helyettesítés (például egy betegség esetén) is [3]. Azonban ez nem tartalmazza a vezetési, a fluktuációs, a szabadságokkal kapcsolatos problémákat, illetve olyan más speciális funkciókat, mint a rosszindulatú programok visszafejtése, a kriminalisztika és a fenyegetettségek proaktív elemzése (Threat Intelligence, TI, fenyegetettségi információ szolgáltatás) és kezelése, amelyek nem minden SOC központi tevékenységi körébe tartoznak bele.

Alapvetően öt SOC-ot különböztethetünk meg működési modelljük alapján [4]. Ezeket az 1. táblázat foglalja össze.

SOC-modell	Jellemzők	Jellemző alkalmazása
Virtuális SOC	Nincs saját külön létesítménye. Részmunkaidős csapattagok. Reaktív működés: kritikus riasztás, incidens esetén kezd működni. Ez az elsődleges modell, ha teljesen kiszervezik az MSSP-nek a SOC-t.	Kis- és közepes vállalkozások, kisebb nagyvállalatok.
Többfunkciós SOC/NOC	Külön létesítmény és kijelölt csapat, amely nemcsak a biztonságot érintő feladatokat lát el, hanem más kritikus IT-műveleteket is végez egy helyen (hálózat üzemeltetési központ), a nap 24 órájában, ezzel csökkentve a költségeket.	Kis- közepes és alacsony kockázatú nagyvállalatok, ahol a hálózati és biztonsági funkciókat már ugyanezek vagy átfedő személyek és csoportok végzik.
Elosztott vagy társmenedzselt SOC	Saját és félig erre kijelölt csapattagok. Tipikusan heti 5 napban, napi 8 órás üzemelés (8/5). Az MSSP bevonásakor ez társmenedzselt.	Kis- és közepes méretű vállalatok.
Saját SOC	Saját, elkülönült létesítmény. Külön csapat. Teljesen házon belüli működés. 24/7-es működés.	Nagyvállalatok, szolgáltatók, nagy kockázatú szervezetek.
Irányító SOC	Más SOC-k koordinálása. Threat Intelligence szolgáltatás, helyzettudatosság és további szakértelmek nyújtása a SOC-knak. Ritkán vesz részt közvetlenül a napi működésben.	Óriásvállalatok és szolgáltatók; kormányok, hadsereg, hírszerzés.

1. táblázat Az SOC működési modelljei [4]

A MŰKÖDÉSHEZ LÉNYEGES KÉPESSÉGEK, ÉS A SZAKEMBEREK MEGTARTÁSA

A SOC elemzői munkakörnek általában alacsony a munkaerő-megtartó képessége: még azok a szolgáltatók is, amelyek karriert és fejlődési lehetőséget is képesek nyújtani, állandóan küzdenek a SOC-elemzők három-négy évnél hosszabb megtartásával. Ennek okai között

megjelenik a váltott műszakokban végzett és monoton munka. Emellett a terület egy ritka és keresett készségkészletet igényel, és ez azt eredményezi, hogy gyakran az ugródeszka szerepét tölti be a munkavállalók karrierjében, tovább súlyosbítva azt a globális képzett szakemberhiányt, amely az ágazatban tapasztalható.

Egy létszámhiányos vagy tapasztalatlan elemzőkből álló SOC azért fog küzdeni, hogy a funkcióit ellátsa. Így az események észlelése és a fenyegetésekre való reagálás hatásfoka alacsony lesz. Ha a szervezet hosszabb ideig nem rendelkezik kellő személyzettel, ez szintén hozzájárulhat az elemzők lemorzsolódásához, és a meglévő szakemberekre nagyobb munkaterhelés kerül.

Ezek alapján azt lehet megállapítani, hogy a SOC-ban a kezdetektől ki kell alakítani egy stratégiát a munkaerő megtartására, mert a biztonsági ipar ezen a részén hiány alakult ki – és marad fent várhatóan a következő években is – a képzett biztonsági elemzőkben. Ez az SOC tervezése és üzemeltetése során is a humán erőforrással foglalkozó szakemberek bevonását indikálja.

Amennyiben a finanszírozás korlátozottan biztosított, a döntéseinknél fent kell tartani az egyensúlyt az üzleti érdekek és a kritikus belső biztonsági funkciók között. Bizonyos alacsonyabb szintű biztonsági funkciókat, mint az eszközkezelés (device management) végezheti egy MSSP, amely képes tartani a megfelelő szolgáltatási szintet, valamint kedvezőbb áron dolgozik, viszont előnyös, ha az elemzés és az incidenskezelés házon belül marad. Az MSSP-ek szintén képesek támogatást adni a belső SOC-csapatnak a váratlan vagy szokatlan események kezelésében, olyan időszakokban, mint a szabadságolások, a nagy biztonsági incidensek vagy a létesítményekkel kapcsolatos problémák esetén.

Ennek biztosítására a fejlesztés elején érdemes kijelölni jól meghatározott célokat és mutatókat, amik szükségesek ahhoz, hogy a SOC biztonsági céljai érvényesülni tudjanak az üzleti érdekekkel szemben.

A kezdetekkor anyagilag biztosítani kell az első két-három évben az SOC működését, valamint azt, hogy a költségvetés fenntartható legyen a továbbiakban is. Általában ennyi idő alatt a folyamatok és a technológia kezelése beágyazódik a szervezetbe, és a dolgozók megfelelő szintű jártasságot szereznek. Tehát a SOC egy hosszú kifutású fejlesztés, amelyben nem gyors a megtérülés, viszont a technológiai és emberi tényezők kikristályosodásával garantálható a legmagasabb szintű információbiztonság. Emellett fontos kiemelni, hogy a menedzselt szolgáltatásként működő SOC (managed-SOC, MSSP által) nem minden esetben optimális megoldás: javasolt a kritikus biztonsági funkciók házon belül tartása [4].

A biztonsági események és az információ kezelésének kritikus képességei

A biztonsági események sikeres kezeléséhez elsődlegesen naplókezelés (log management) és jelentéskészítés, dokumentálás szükséges, olyanok, amelyek megfelelnek a szektor szabályozásainak. Ahhoz, hogy a SOC a legfontosabb területeken helyt álljon, három helyzetre kell tervezni [4]:

1. A szabályozásoknak való megfelelésre (Compliance).
2. Fenyegetettségmenedzsmentre (Threat Management).
3. Security Information and Event Management (SIEM – Biztonsági információ és eseménykezelő) szoftverre, amelyet megfelelően üzemeltenek és konfigurálnak.

A következő kritikus képességek azonosíthatók az SOC hatékonyságában:

- Valós idejű monitorozás: a támadások lefolyásának nyomon követése és elemzése az összes alkalmazáson és a rendszeren keresztül, valamint a felhasználói tevékenység megfigyelése, nyomon követése és elemzése.
- Threat Intelligence (TI): a fenyegetések proaktív felderítése friss és aktuális adatok, az ismert támadási minták alapján.

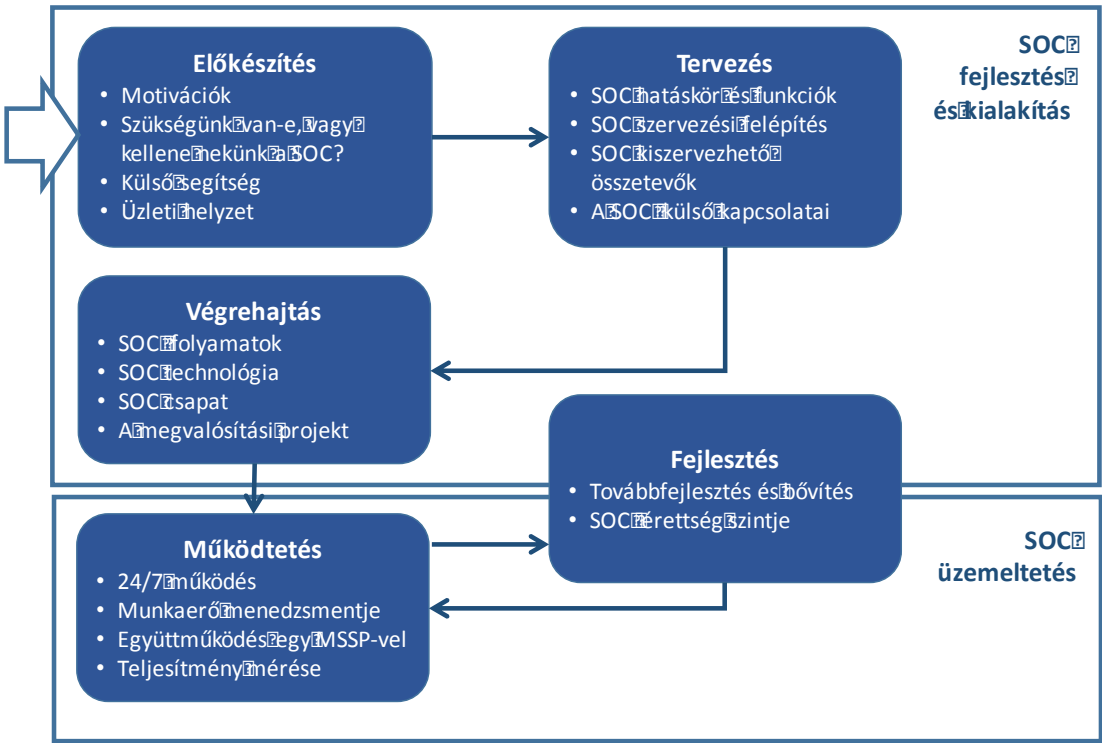
- Viselkedésprofilozás: riasztással minden normális viselkedéstől való eltérés esetén a megfigyelés során.
- Adat- és felhasználói monitorozás: a privilegizált felhasználók tevékenységének és az érzékeny adatokhoz való hozzáférésük folyamatos monitorozása legtöbbször része a szabályozásoknak való megfelelésnek.
- Alkalmazás-felügyelet.
- Elemzés és analitika.
- A naplófájlok kezelése és jelentés (report) készítése.
- Az eszközök és alkalmazások telepítésének, illetve támogatásának egyszerűsítése.

Az SOC-ok középpontjában a fent említett SIEM-szoftverek állnak, amelyek összesítik, összekapcsolják a rendelkezésre álló biztonsági szempontból releváns adatokat, és riasztásokat adnak az események kockázatosnak ítélt mintázatai esetén. Ezekre a központi fontosságú szoftverekre a későbbiekben részletesen kitérek.

A SOC tervezésének, megvalósításának, üzemeltetésének és fejlesztésének kulcskérdései

A legtöbb SOC központi képessége és feladata a biztonsági szempontból releváns események monitorozása. Általánosságban az SOC feladatkörei közé tartozik továbbá a fenyegetettségek és sebezhetőségek kezelése, a biztonsági eszközök kezelése és karbantartása, a kiberbiztonsági incidensek kezelése, a szabályozásoknak való megfelelés biztosítása, a biztonsági tréningek. Az információbiztonsági képzések biztosítása a szervezetben, illetve a szabályozásoknak való megfelelés biztosítása egyre kevésbé része napjainkban egy SOC feladatainak. Ezzel szemben a fenyegetettségek proaktív felderítése (Threat hunting, fenyegetettség vadászat) és a Threat Intelligence lassanként új SOC-funkciókká válnak.

A következőkben az 1. ábra segítségével időrendben tekintem át a SOC-ot érintő legfontosabb kérdéseket, a tervezéstől a létező biztonsági műveleti központ továbbfejlesztéséig [4].



1. ábra Egy SOC fejlesztése, kialakítása és üzemeltetése [4]

Előkészítés

A legjellemzőbb motiváció, ami egy SOC kialakítását indokolja, a kiberbiztonsági műveletek centralizálásának igénye, a szervezet egészére való rálátás javítása, a fenyegetettségek feltárásának javítása. Emellett az egyre növekvő, észlelt vagy valós kockázatok kezelésének igénye, a fenyegetettségeknek való kitettség csökkentése is lényeges motiváló tényező. Mindezek mellett jogszabályok és előírások is meghatározhatják a központosított kibervédelmi monitorozást és műveleteket, amire a SOC nyújtja a legjobb megoldást.

Az előkészítés fontos előfeltétele, hogy a szervezet alapvető IT-üzemeltetési érettséggel rendelkezzen. A monitorozáshoz naplózási folyamatok, a logok megfelelő generálása, kezelése, megtartása szükséges, és az a tudás a hálózati kontextusról, ami ezek értelmezését biztosítja. Emellett lényeges előfeltétel és a tervezés során figyelembe veendő, hogy a monitorozást és a biztonsági események detektálását végző SOC mellett incidenskezelésre, válaszadásra alkalmas csapatnak is kell a szervezet rendelkezésére állnia (bár ez esetenként tervezhető a SOC-on belülre is).

Egy szervezet a SOC megvalósításában és üzemeltetésében is tervezhet külső partnerekkel. E partnerek között lehet olyan, amelyik megépíti a SOC-ot, amelynek kiszervezhető a SOC (MSSP, managed SOC), amelyek megoldható a saját SOC-csapat kiegészítése külső szakemberekkel, állandó jelleggel vagy időszakosan (például súlyos incidensek idejére). Azt azonban figyelembe kell venni, hogy a felelősség nem szervezhető ki. A végső felelősség a biztonságért a szervezeté marad. A legjobb MSSP-partner sem tud incidenst detektálni olyan rendszerben, amire nincs rálátása vagy nincs hozzáférése.

Tervezés

A tervezés első lépése, hogy a fent említett SOC-tevékenységek és -felelősségek közül kiválasztják a megvalósítani kívánt elemeket (belső vagy kiszervezett formában). Az egyik alapvetőbb kérdés, az incidensekre való válaszadás (Incident Response, IR, incidens kezelés) funkciójának SOC-on belül vagy kívül (külön Computer Security Incient Response Team-ben, azaz CSIRT-ben) való megvalósítása szerint a következő előnyök és hátrányok jelenhetnek meg [4].

	Előnyök	Hátrányok
IR a SOC részeként	A felderítés és a reagálás közötti szorosabb integráció. Csökkenti az erőforrás-igényeket, mivel nem szükséges extra menedzsmentréteg. Több lehetőséget kínál a karrierfolyamathoz és a munkahelyi rotációhoz a SOC-on belül.	A feladatokat el kell különíteni, amikor a SOC személyzetével kapcsolatos figyelmeztető jelzések vizsgálata zajlik. Az IR-csapat függetlenségének hiánya a felderítéssel és a kezdeti riasztással kapcsolatos kérdésekre utal, amelyet a SOC kezel. Összetett a kiszervezése, mert az IR egy olyan funkció, amely nem könnyen szervezhető ki. A magasabb IR-munkaterhelés negatívan befolyásolhatja az észlelési tevékenységeket.
IR irányítása egy elkülönített CSIRT-tel	Az IR csapat függetlensége lehetővé teszi a SOC-forrásokkal kapcsolatos események kivizsgálását. Könnyebb kiszervezni a SOC felügyeleti funkciót, mivel az IR-tevékenységeket külön kezelik.	Valószínűleg párhuzamosságokat okoz és kiegészítő erőforrást igényel (legalább vezetési szinten). Csökkenti a karrierfejlődési lehetőséget a SOC-on belül. A kis jelentőségű SOC-szerepek valószínűleg kevésbé vonzóak a tehetségek vonzására.
IR a SOC és a CSIRT között elosztva	Csökkenti a CSIRT erőforrásigényét, amikor teljesen különválasztják a csoportokat (a SOC lehet az IR-csapat technikai része). Javítja a CSIRT-ben bekövetkező események átadását a teljesen különálló csoportokhoz képest.	Nincsenek tisztázva a felelőségek és a szerepek. A függetlenség esetleges hiánya a SOC-forrásokkal kapcsolatos események kivizsgálása során.

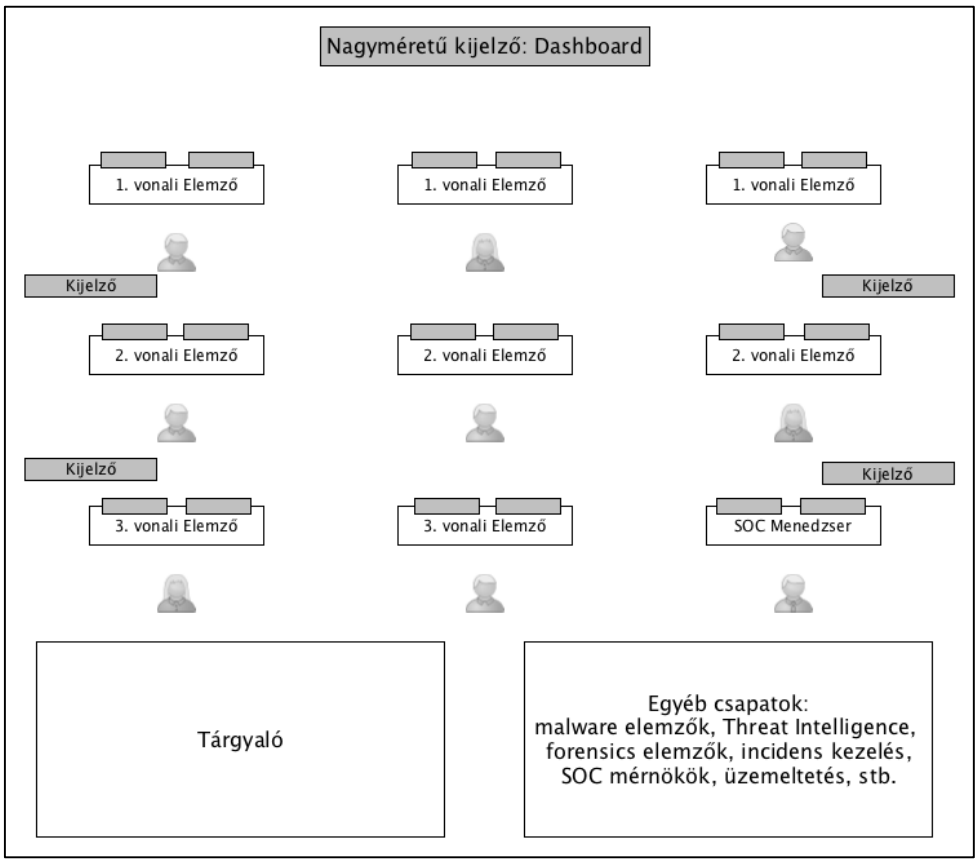
2. táblázat Előnyök és hátrányok az IR külső vagy belső formája esetén [4]

A SOC-ok megvalósításának öt, korábban bemutatott modellje terjedt el (lásd 1. táblázat). Ezek közül a tervezés fázisában szükséges választani.
A külső partnereknek való kiszervezés kérdésben fontos kiemelni, hogy az MSSP-k rendszerint biztonsági monitorozást vagy biztonsági eszközök kezelését ajánlják ügyfeleiknek. Kevéssé jellemző, hogy nem napi üzemeltetési jellegű feladatokat (például biztonsági vezetés, átfogó programok megtervezése) kiszerveznének.

A SOC megvalósítása

Ahogy azt megfogalmaztuk, a SOC fő tevékenysége *a monitorozás és a detektálás*. Napjainkban jellemzően egyre nagyobb hangsúly esik a fenyegetettségek proaktív megismerésére, az ezekkel kapcsolatos hírek, tapasztalatok megosztására, amit Threat Intelligence, TI néven említek. A modern SOC-ok feladatai között így megjelenik a proaktív keresés (vadászat, threat hunting) és a Threat Intelligence is.

A SOC megvalósítása során lényeges az eszköztár megválasztása. Az eszközök három csoportba sorolhatók: rálátást biztosítanak, elemzést tesznek lehetővé és cselekvést, menedzselést szolgálnak. Általánosan számos eszköz integrálható a SOC-ban lévő rendszerekbe, hogy a heterogenitás és a túlzott komplexitás elkerülhető legyen és a folyamatosan figyelmet igénylő felületek száma limitált legyen. Az integrációk legjellemzőbb fókuszpontja a SIEM szokott lenni: ehhez kapcsolódik a legtöbb eszköz és ebben jeleníti meg adatait és riasztásait mintegy összefogó felületként. Ennek okán és amiatt, hogy a csapatmunkában központi helyet foglal el a SIEM (Security Information and Event Management) csak erre térek ki térek részletesebben: a különböző technológiákból és forrásokból származó események és logok konszolidálására és korrelálására, figyelmeztetések generálására vagy a gyanús, illetve privilegizált tevékenységek elemzésére használják. Egyetlen keresőfelületet biztosít a naplófájlokhoz, illetve fel lehet használni vizsgálati és threat hunting tevékenységekre is. A SIEM-et gyakran tekintik az SOC legfontosabb eszközének.



2. ábra A SOC különböző szakemberei, és munkaállomásaik elhelyezkedése egy tipikus a SOC-ban [1]

A SOC nemcsak technológiából, de szakemberek csapatából vagy együttműködő csapataiból is áll, ahogy ez a 2. ábrán is látható.

A legfőbb tevékenységet jelentő monitorozást jellemzően legalább két vonalba (level vagy tier) szervezett elemző (analyst) csapat látja el, egymáshoz eszkalációs sorrendben kapcsolódva:

- Az első vonal (Level/Tier 1): az itt szolgálatban lévő elemzők az első körös riasztásrendezést, áttekintést végzik. Ők az első pont, ahol a SOC belép egy eseménnyel kapcsolatos tevékenységbe. Jellemzően 24/7-es munkarendben dolgoznak, több műszakban váltva egymást.
- A második vonal (Level/Tier 2): itt nagyobb tapasztalatú és képzettebb elemzők dolgoznak, akik az első vonal által hozzájuk továbbított riasztásokat elemzik, és reagálnak azokra. Bizonyos esetekben ezek a szakemberek igény szerint dolgoznak, nem éjjel-nappalos műszakokban.

További fontos szerepek a SOC-csapatban a következők lehetnek: a SOC-csapatot vezető menedzser, a műszakot vezető menedzser, a SOC műszaki és tartalmi feladatait vezető menedzser, TI-elemző, IR-szakértő (amennyiben ez a SOC-on belül van).

A SOC csapattal kapcsolatos, a megvalósítás során leginkább lényeges kérdés a képzett szakemberek hiánya a területen. Tapasztalataink szerint nemcsak a nemzetközi, de a hazai piacon is jellemző az, hogy a SOC-szakemberek karrierútja az első vonalból indul (Level 1 SOC analyst), ahova fiatal pályakezdőket vesznek fel, és őket képzik, ezzel elkerülve a tapasztalt szakemberek költséges alkalmazását. Az ilyen karrierút-tervezés implikálja, hogy a következő vonal és a specifikusabb SOC-pozíciók felé haladni tapasztalattal, idővel, képzéssel lehet (szenioritás jellemzi ezeket a feladatköröket). Ez a megközelítés nem segít abban, hogy az első vonalban dolgozó elemzőket megtartsák, elégedettségük és munkájuk minősége kellő szintű legyen. Viszont a képzésükbe invesztált költségek kárba vesznek, ha ők távoznak a szervezetből. Rájuk nehezedik a legnagyobb stressz is, pontosan az alacsony státuszú pozíció és a 24/7-es munkarend miatt, ami a kiégés és pályaelhagyás okozója lehet. A kockázatot fokozza az, hogy a munkaerőhiány miatt a cégek egymástól agresszívan igyekeznek szakembereket átcsábítani. E probléma kivédését szolgálhatja, ha a különböző SOC-vonalakat és -szerepeket nem szenioritás alapján értelmezzük, hanem a SOC célját szolgáló, azonosan fontos, de más képességeket igénylő területekként. Ezek között a szakemberek megadott rend szerint rotálhatók, ami a klasszikus munkapszichológia egyik alapvető elégedettségjavító módszere. Ezzel az elégedettség és a hatékonyság is növelhető, viszont a stresszes (például első vonalbeli) pozíciókban a kiégés csökkenthető. Az erősen versengő munkaerőpiaci helyzet miatt a szakemberek javadalmazásán és a motiváló karrierúton kockázatos megtakarítani [1].

Egy saját, fizikai SOC-biztonsággal üzemelő szint megvalósítása jellemzően 18-24 hónapot vesz igénybe. Ebben benne van a fizikai hely létrehozása (irodabérlés és annak berendezése a SOC igényei szerint), a szakemberek kiválasztása, felvétele, kiképzése a csapatba, az eszközök beszerzése és telepítése, végül az üzemeltetés folyamatainak kidolgozása és finomhangolása.

A megvalósítás összefoglaló jellegű mérföldkövei a következők [4].

1. Személyzet
    a. Kiválasztás, felvétel vagy cégen belüli munkatársak átvétele.
    b. A szerepek kijelölése.
    c. Képzés és a képességbeli hiányok lefedése.
    d. Megtervezni a külső partnerek szakembereinek esetleges bevonását.
2. Folyamatok
    a. A fő folyamatok definiálása (például riasztásértékelés, -rendezés, eszkalálás stb.).
    b. A meglévő IT-biztonsági folyamatok áttekintése és az SOC-hoz alakítása.

   c. A folyamatok átadása azt azokat végrehajtó elemzőknek.
3. Eszközök
   a. A meglévő eszköztár áttekintése.
   b. A szükséges eszközök beszerzése.
   c. Eszközök telepítése.
   d. A tartalom létrehozása (például SIEM riasztási szabályai, use case-ek).
   e. Integráció.
   f. A folyamatok illesztése a meglévő eszközökhöz.

A SOC üzemeltetése

Az informatikai eszközök üzemeltetése IT-üzemeltetési feladatokat takar, speciális ismeretekkel az információbiztonság területén. Egy olyan kardinális fontosságú folyamatos üzemeltetési feladat van, amelyet ki kell emeljek: ez a SIEM riasztási szabályok frissítése, pontosítása és létrehozása. Tapasztalataink szerint magyar és nemzetközi viszonylatban egyaránt a legnagyobb feladat, ami a SOC dolgozóira nehezedik (inkább második vonaltól vagy mérnöki szinten), az a riasztási szabályok folyamatos frissítése, finomhangolása az aktuális események, észlelt támadási minták vagy TI alapján. A SOC lelkét adó SIEM sosincsen készen, a riasztásokat generáló szabályoknak folyamatosan követnie kell a változó támadási módszereket. Ez a végtelen versenyfutás jelentős üzemeltetési feladat a képzett kibervédelmi szakembereknek, és nagy stresszforrás is. A szabályokra való hagyatkozáson változtathat az a mostanság kibontakozó trend, ami az UEBA-megoldások (User and Enitity Behaviour Analytics, felhasználó és entitás viselkedés elemzés) elterjedésével, gépi tanulással és prediktív adatelemzéssel igyekszik a manuális szabálybeállítást proaktívan automatizálni.

Az emberierőforrás-menedzsment irányból nézve az üzemeltetési kérdések origója az, hogy a SOC egyik alapvető kritériuma a 24/7-es üzemelés, azaz munkanapokon és hétvégén, éjjel és nappal egyaránt el kell látni a kiberbiztonsági feladatokat. Ennek biztosítására elméleti minimumként 6 emberre van szükség. Azonban ez a valóságban jellemzően nem elegendő. Egyfelől jogi korlátozásai vannak (munkajog, illetve előfordul, hogy nem lehet dolgozó egyedül a munkahelyen). Másfelől a szabadságolásokat, a képzéseket és a váratlan távolléteket is figyelembe kell venni. Sőt, a különböző SOC-feladatokat ellátó szakemberekből is elegendőre van szükség, hogy minden pozícióra jusson kellő számú teljes állásos ember. Ha ezeket is figyelembe vesszük, a minimális üzemeltetési létszám 20 körül állapítható meg, de a gyakorlati minimum sem lehet kevesebb, mint 9 fő [3].

Az üzemeltetés kérdéskörének része, hogy a valóságban a különböző SOC-pozíciók nem egyformán vonzóak, nem egyformán áll rendelkezésre szakember ezekbe. A munkaidőn kívüli műszakok (éjjel, hétvégén) jellemzően kevésbé népszerűek, és az ekkor végzett munka magasabb stresszel is jár, ami a kiégés veszélyét fokozza. Problémák forrása lehet, hogy a normál munkaidőn (hivatali időn) kívül dolgozó szakemberek kevésbé felügyelhetők: a nem a munkájukhoz kapcsolódó tevékenységek így gyakoribbak és nehezebben érhetők tetten. Emellett az ő teljesítményértékelésük is problémásabb a rosszabb láthatóság miatt. A normál munkaidőn kívüli műszakozás miatt a dolgozók egy részének a képzések és csapatépítések szervezése is nehezebb, mivel jellemzően a többséget érintő munkaidőn kívülre esnek, amikor ők vannak szolgálatban. Globális cégek esetében kiváló megoldást nyújthat, ha a Föld három különböző pontjára telepítenek SOC-csapatokat, amelyek munkaidőjükkel, némi átfedést is beleértve, lefedik a teljes glóbuszt és az összes időzónát.

Azonban a cégek nagy részének ez a megoldás nem reális, méretük vagy költségvetésük miatt. Számukra a munkaerő-menedzsment különböző megoldásainak alkalmazása nyújthat segítséget. A monitorozás ellátása egy kifejezetten nehéz, kevert helyzetét adja a műszakozásnak és a speciális képességekre való igénynek. Az első vonalban (level 1) kezdő elemzők jellemzően fiatalok és kezdők, akiknek a megtartása válik elsődleges problémává,

mivel a lehető leghamarabb magasabb pozícióba törekednek, és ennek útja az egyes szervezetek között gyorsabb, mint szervezeten belül. Különösen igaz ez a jelenlegi munkaerőhiányos, kompetitív munkaerőpiacon. A SOC-menedzser feladata a kezdő pozíciók felől érkező, előre lépésre való törekvés helyes kezelése (például a munkakörök rotációjával). Emiatt az állandónak tervezett létszám betöltése a megfelelő szakemberekkel folyamatos kiválasztást és felvételt kell eredményezzen. Megoldások lehetnek a következők [1], [3], [4]:

- Minden SOC-elemző számára tegyen a beosztás lehetővé szabad éjszakákat és szabad hétvégéket.
- Minden elemző számára legyen elérhető képzés és fejlődési lehetőség.
- A munkaköri rotáció előbb említett példája széles körben segíti orvosolni a nyomást a tovább lépésre, illetve ezzel jól kombinálja a munkában való képzési lehetőséget is (új munkakörben új képességeket sajátít el).
- Tapasztalt szakemberek is kerüljenek a csapatokba, akik legyenek elérhetőek a kezdő csapattagok számára is.
- A kiválasztás és a munkaerő-felvétel legyen a normál tevékenység része (ehhez lényeges az szakmai kapcsolatrendszer életben tartása).
- Az automatizálás (például gépi tanulás útján) és az eszközök összehangolása segítségével csökkenthetők az unalmas repetitív munkafeladatok, amelyek jelentős stresszforrások.

A SOC fejlesztése és bővítése

A már sikerrel megtervezett, beüzemelt és üzemeltetett SOC sincsen véglegesen készen. Ahogy említettük, a szabályok folyamatos karbantartása mindig jelentős erőfeszítéseket igényel, és figyelmet követel az újabb technológiák alkalmazása is az egyre változó támadási módok ellen és a SOC hatékonyságának fokozására. Barros és Chuvakin elemzése szerint [4] a jelenleg és a közeli jövőben arra lehet számítani, hogy a SOC-kban elterjed a Threat Intelligence (TI), a proaktív hunting szemlélet, többet fognak használni analitikai eszközöket, például UEBA céljára és big data szintű elemzésekre.

A következő fontos fejlődési irány az eltávolodás a kizárólag riasztásokra épülő folyamatokról:

- Számos korábban is tárgyalt, akár tervezési, akár üzemeltetési nehézség oka, hogy az ember számára feldolgozhatatlanul sok riasztás keletkezik a biztonsági rendszerben. A központi dashboardok felületein (automatikusan frissülő áttekintő felületeken) ezért leginkább csak a legmagasabb kockázati értékű elemeket érdemes megjeleníteni, amihez a legvalószínűbben kapcsolódhat biztonsági incidens.
- Az automatizálás és az összehangolást biztosító eszközök szerepe megnövekszik. Azonban az automatizálás semmiképp nem lehet még teljes körű: teljesen automatizált SOC-ra nem lehet még számítani.
- Az álcázásos technikák alkalmazása segíthet megérteni a támadók eszköztárát, taktikáját, a viselkedésüket kontextusba helyezve.
- Lényeges folyamat a Threat Intelligence információ előállításának növekvő elterjedésére. Az ilyen információ legautentikusabb forrásai maguk a fenyegetettségeknek kitett szervezetek lehetnek.
- Majdhogynem szektorfüggetlen trend a fejlett analitikai eszközök egyre nagyobb elterjedése és alkalmazása a kiberbiztonság területén. Ennek leginkább várható alkalmazásai az UEBA-megoldások. Az ilyen eszközök jellemzően (de nem kizárólagosan) összesített SIEM-adatok utólagos elemzését végzik, kiegészítve a felhasználók azonosítását segítő adatokkal és algoritmusokkal. Emellett a prediktív analitikán, gépi tanuláson alapuló módszerek lehetővé teszik a szabályalapú

riasztásokon való túllépést, és inkább illeszkednek a proaktív hunting stílusú tevékenységekhez.
- Végezetül lényeges trend, hogy a SOC-ok értékelésében jelentős szerep jut a gyakorlatoknak. Ezek során külső (vagy belső) támadóként viselkedő szakértőket kérnek fel, hogy próbatámadást végezzenek, és eközben a SOC teljesítményét értékelik.

Végezetül nemcsak a siker tényezőiről, hanem a lehetséges buktatókról és kockázatokról is ejteni kell pár szót. Jellemző buktató lehet limitált személyi, eszközbeli és anyagi források mellett belevágni a SOC kialakításába. Probléma, ha a SOC szervezeti támogatás nélkül valósul meg, valós céllal, de más csapatokhoz való kapcsolódások nélkül. A hatékony működés gátja az is, ha túl sok riasztás önti el a SOC-ot a különböző (nem feltétlenül helyesen) hangolt eszközökből. Nehézséget okozhat, ha az egyedüli fókusz a SIEM-en van, és nincs rálátás más, esetleg fontos eszközökre, adatokra. A SOC hatékonyságának és jó működésének buktatója lehet, ha a csapat egyedül a riasztások feldolgozására fókuszál anélkül, hogy mélyebb elemzést végezne és átfogó mintázatokat azonosítana. Ez összefügg azzal, hogy ha a szervezet nem tanul az egyedi eseményekből és incidensekből, és nem állít elő TI-adatot, akkor az veszélyt jelenthet a sikerére nézve. Alapvetőbb szervezeti buktató, ha a meglévő NOC (Network Operation Center, amely a hálózatüzemeltetést hivatott ellátni) vagy az IT-helpdesk próbál meg SOC szolgáltatásokat nyújtani. És végül jelentős, fennmaradást veszélyeztető buktató lehet az eddigiekben részletesen tárgyalt munkaerő-megtartás hiánya: ha nincs erre a szervezetnek stratégiája, könnyen elveszítheti a képzett szakembereket és az SOC számára nélkülözhetetlen szaktudást is.

A SIEM SZEREPE A SOC-BAN

A biztonsági műveleti központok azaz SOC-ok szíve-lelke technológiai szempontból a SIEM (Security Information and Event Management, Biztonsági információ és eseménykezelő) alkalmazás. Ez gyűjti, aggregálja, korrelálja a szervezetben fellelhető, biztonsági szempontból releváns adatokat. A korreláció során azokat értelmes mintákba rendezi, amelyeket a SOC-t üzemeltető kiberbiztonsági szakemberek szabályok (SIEM-rules) formájában definiálnak a rendelkezésre álló adatokból és a lehetséges támadási mintázatok alapján [3]. A SIEM a szabályok alapján az elvárt mintázat megjelenésekor riasztást küld az elemzők (SOC analysts) számára, akik 24/7es munkarendben felügyelik a SIEM felületeit, dashboardjait. A riasztások kezelése, ennek dokumentált követése lehetővé teszi az incidensmenedzsment folyamat elvégzését a SIEM-en belül. Végül a támadás irányának rendszeren belüli azonosítása után következhet a védekezés, az elhárítás, az esetleges károk javítása (visszaállítás), amelyek már a SIEM-en kívül történnek. Az incidenskezelés lezárultával a legtöbb SIEM lehetőséget ad a jogi célú dokumentálásra, bizonyítékok gyűjtésére, forensics riportok készítésére. A SIEM-technológia alapvető képessége, hogy a széles körű adatgyűjtés különböző forrásaiból és azok elemzéséből képes feltárni, ábrázolni az összefüggéseket. Emellett a megadott szabályok alapján képes a kockázatos eseménymintázatokra riasztásokat adni.

A SIEM-ek összetevői és alapvető képességei összefoglalva a következők:
- *Adataggregálás:* a naplófájlt kezelő rendszer számos adatforrást aggregál, többek között hálózati adatokat, szervereket, adatbázisokat, alkalmazásokat.
- *Korrelálás:* a SIEM közös jellemzőket és kapcsolatokat keres a begyűjtött adatokban ahhoz, hogy értelmes egységekbe rendezze azokat. A korrelálás hoz létre az adatból értelmes információt.
- *Riasztás:* a korrelált események automatikus értékelése alapján riasztásokat küld a beavatkozást igénylő eseményekről. A riasztás kerülhet a SIEM felületére és külső csatornákon keresztül (például e-mail, API) is eljuthat a SOC-elemzőhöz.

- *SIEM dashboardok:* a SIEM összegző felületei, amelyeken az események adatait informatív elrendezésben mutatják be, grafikonok és táblázatok segítségével. Ez lehetővé teszi, hogy esemény- és tevékenység-mintázatokat azonosítson az elemző.
- *Előírásoknak való megfelelés:* a SIEM-ek alkalmasak arra, hogy az adott szektort érintő jogszabályi előírásoknak való megfelelés ellenőrzéséhez szükséges adatokat gyűjtsék és összegezzék jelentések, riportok formájában. Ezek alkalmazhatóak tervezési és ellenőrzési (auditálási) helyzetekben.
- *Adatok megtartása:* hosszú távú adattárolók alkalmazhatók arra, hogy a korreláció segítésére régebbi adatok is elérhetőek legyenek, illetve az iparági előírások is meghatározhatnak adattárolási kötelezettséget. A hosszú távú adattárolás elengedhetetlen a biztonsági incidensek későbbi kivizsgálásakor (forensics), mivel az ritka esetnek számít, hogy egy adatlopást például akkor lepleznek le, amikor az történik. Jellemzően napok, hetek, hónapok után derül fény rá, és zajlik le a nyomozás.
- *Jogi eljárást megalapozó elemzés (forensic analysis):* a SIEM-ek ezen képessége lehetővé teszi, hogy különböző hálózati elemekhez tartozó naplófájlokat keressenek, időszakokra vagy más kritériumokara szűkítve. Ez megkíméli az elemzőt, hogy nagy mennyiségű logot kellejen áttekintenie és fejben aggregálnia.

Naplófájlok (log fájlok)

A SIEM-ek legalapvetőbb adatforrásai a rendszer különböző pontjain gyűjtött naplófájlok, azaz logok. A naplózásban és a naplófájlok beállításaiban az alábbiak az irányadóak [5]: *„A naplóforrásokat úgy kell beállítani, hogy a bejegyzések mindig a megfelelő tartalommal, a megfelelő helyen keletkezzenek és a szükséges ideig legyenek megtartva.* […] *Feltételezve, hogy a logforrás lehetőséget ad a naplózás finomhangolására, a kezdeti beállításokat kellő körültekintéssel kell megtenni. Előfordulhat ugyanis az, hogy egyetlen forrás olyan mennyiségű adatot generál, amit a felállított infrastruktúra nem tud kezelni. Ez adatvesztéshez vezethet, lelassíthatja vagy akár teljesen elérhetetlenné teszi a naplózó szolgáltatást, szélsőséges esetben akár a teljes hálózat átviteli sebességére is hathat. A fenti problémák megelőzése érdekében a naplózást először nem produktív környezetben kell kipróbálni, különösen a leggyakoribb források és a legkritikusabb szolgáltatások esetén. Az egyes gyártók általában tudnak információt adni a naplózással kapcsolatban."* [5]

Ezenfelül Krasznay ugyanitt helyesen rávilágít arra, hogy *„előre meg kell határozni a logrotálás paramétereit is. Ez azt jelenti, hogy a felgyűlt bejegyzéseket csak egy előre meghatározott méretig vagy ideig kell egy naplóállományban gyűjteni, utána ezt archiválni kell. Így garantálható, hogy mindig lesz szabad tárolókapacitás a naplózáshoz."* A megfelelő mennyiségű, részletességű (verbosity) és elérhető, illetve archivált formában rendelkezésre álló log teszi lehetővé a SIEM hatékony üzemeltetését.

A logokkal kapcsolatban a SIEM mint log aggregáló alkalmazás miatt fontos tisztázni, hogy mely alkalmazások az információbiztonság szempontjából milyen naplózást végeznek. Ennek jó szempontjait adja a Common Criteria for Information Technology Evaluation [6] (az információ technológiai értékelés közös szabvány) nevű szabvány, amelyben egy teljes úgynevezett család foglalkozik a naplózással kapcsolatos funkcionális követelményekkel, emellett minden egyes biztonsági funkcióhoz meghatározza a naplózandó eseményeket. A szabvány 6 területre osztja a logokkal kapcsolatos tevékenységeket [5]:

- *Automatikus válaszadás:* milyen események következnek akkor, amikor lehetséges biztonsági szabálysértést észlel a rendszer.
- *Naplóadatok létrehozása:* meghatározza, hogy milyen típusú tevékenységeket kell rögzíteni, milyen minimális információtartalommal, hogy az jól használható legyen.

- *Biztonsági naplóelemzés:* pl. a SIEM alkalmazása naplóadatokon a biztonsági események kiszűrésére (riasztás) és megértésére a hatékony incidenskezelés vagy a forensics eljárás érdekében.
- *Biztonsági naplóadatok áttekintése:* annak meghatározása, hogy milyen módon lehet a jogosult felhasználónak lehetővé tenni a naplóadatok megtekintését. Praktikusan a naplóbejegyzések felhasználói felületére vonatkozó követelmények tartoznak ide.
- *Naplóesemények kiválasztása:* azon lehetőségek felsorolása, amelynek segítségével a logok halmazából egy adott tulajdonsággal rendelkező eseményeket ki lehet választani. Gyakorlatilag a riportkészítés követelménye pl. forensics nyomozáshoz használható logok elérése által.
- *Események tárolása:* a logállományok létrehozásának és tárolásának feltételeivel foglalkozó követelmény, amely pl. a forensics célú, az eseményt időben később követő elemzést lehetővé teszi.

Emberi tényezők a SIEM üzemeltetésében

Azonban a logok és adatok csak a sikeres alkalmazás egyik aspektusai [3]. Az emberi tényező központi fontosságú a SOC-kban, és ez a SIEM-ek használatára is igaz.

A hatékony SIEM és a hatékony SOC másik aspektusa a technikai mellett a humán. Az emberi tényező központi szerepet játszik a hatékony riasztási szabályok (SIEM rules) definiálásában: a szakemberek tudása, tapasztalatai és képességei meghatározzák, milyen komplexitású események mintázatait, milyen gyorsan és milyen heterogén adatokra alapozva képesek szabályokba önteni, ezzel riasztani az ilyen támadások esetén, lehetővé téve a hatékony védekezést. Szintén az emberi tényezőn múlik, hogy a SIEM dashboardjait, ahol sok más információ mellett a riasztások is megjelennek, milyen képességű, éberségű, motivációjú elemző szakemberek figyelik. A jó SIEM-elemző képzése és megtartása a szervezetben a SOC-kat érintő munkaerőhiány egyik fő oka, amelytől a későbbiekben sem várható, hogy enyhül [3], [4]. Szintén az emberi tényezőn múlik, hogy a SIEM-et használó, a dashboardjait felügyelő elemző miképp tud hatékonyan együttműködni, csapatban dolgozni más szakemberekkel: malware elemzőkkel, forensics elemzőkkel, szerveradminisztrátorokkal a műszakban vagy a műszakok között, illetve kliensekkel MSSP esetén [1]. A technológia önmagában azonban nem elegendő. A szakképzett munkaerő, a fejlett technológia és a fenyegetettségekről, a hálózat elemeiről, a használóról szóló kontextuális információ együtt teszi lehetővé a hatékony védelmet. A külső és belső kontextus, a helyzetről szóló, a helyzettudatosságot lehetővé tevő információ lehetővé teszi, hogy a SIEM akár célozott, fejlett támadásokat is detektáljon. Ebben fontos kiemelni, hogy a technológia, az eszközkészlet, az információ a szakemberek csapatával együttesen alkot ütőképes SOC-t, amelyet az ergonómia fogalmaival élve jól működő szociotechnikai rendszernek tekinthetünk [1], [7].

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A SOC-k egy változó információbiztonsági környezetben kell helytálljanak, a folytonosan megújuló technológiákat integrálva eszköztárukba. Mindezt azért, hogy gyors és hatékony formában tudjanak védekezni az egyre gyakoribb és kifinomultabb támadásokkal szemben. Különösen nagy hangsúlyt fektettünk – a technológián és a folyamatokon kívül – a csapatot alkotó szakemberekre, mivel a jelenlegi kiberbiztonsági munkaerőpiacon jelentős verseny zajlik értük. Az emberi tényező így kitüntetett fontosságúnak tekinthető. Az hogy a sikeres teljesítmény csapatmunka kérdése a SOC-ban rávilágít az együttműködés képességének vizsgálatára, fejlesztésére a kiberbiztonságban dolgozó szakemberek esetében. Emellett a

csapatmunkát lehetővé tevő technológiai eszközök, azok megléte, használhatósága is olyan vizsgálandó terület, amely segíthet a közeljövőben átfogóbb képet adni a SOC-okban végzett kiberbiztonsági munka sikerének tényezőiről.

A fent áttekintett komplex feladatok és kihívások rendszeréből látható, hogy a kiberbiztonsági munka frontvonalában a SOC áll a technológia és humán tényezők szempontjából egyaránt. Ennek okán a kritikus fontosságú üzleti vagy állami, illetve katonai informatikai rendszerek védelmére biztonsági üzemeltetési központokba szükséges invesztálni. Azonban ahogy az elemzések és a Magyarországon megfigyelhető tendencia a saját SOC-ok kialakítása az állami és katonai területen, illetve nagyobb vállaltoknál és a lokális vagy globális biztonsági szolgáltatás nyújtása MSSP-ként is. Ez azt is jelenti, hogy komplexitás minden szintje megjelenik hazánkban. A szervezetek vagy állami szervek méretével vagy kritikus jellegével ezen összetettség növekszik vagy elvárt lenne a növekedése. A komplexitás pedig nem csak a SOC technológiai komplexitását, vele az eszközök számát és költségeit növeli, hanem a személyi állományra is nagyobb kihívást ró. A 24/7-es monitorozás önmagában a műszakozás terhét teszi a dolgozókra, akiket az így érő stressz hajlamosabbá tehet a lemorzsolódóra. Természetesen a komplexitás az egyre összetetted és költségesebb, de hatékonyságot ígérő kiberbiztonsági szoftvereket igényel, úgy mint a SIEM alapfeltételként, ezen felül kiegészülve TI és UEBA megoldásokkal. Cikkemmel ezeket a komplex kihívásokat és az ezekre adott elfogadottnak tartott válaszokat mutattam be annak érdekében, hogy a hazai kiberbiztonsági területen lehetőség legyen SOC-ok kialakításának támogatásra különös tekintettel az emberi tényezőkre mindebben.

FELHASZNÁLT IRODALOM

[1] HÁMORNIK, B.P.; KRASZNAY, CS.: *A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers* In: NICHOLSON, D.; CHAM, E. (Eds): Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, Springer International Publishing, 2017. pp. 224–236.

[2] KASSAI, K.: *A 2013. Évi l. Törvény végrehajtása érdekében a magyar honvédségnél szükséges elektronikus információvédelmi szakfeladatok*; Hadmérnök, VIII. 4. (2013) 191–200. o.

[3] MUNIZ, J.; MCINTYRE, G.; ALFARDAN, N.: *Security Operations Center: Building, Operating, and Maintaining your SOC*; Cisco Press, 2015.

[4] BARROS, A.; CHUVAKIN, A.: *How to Plan, Design, Operate and Evolve a SOC*; https://blogs.gartner.com/anton-chuvakin/2016/10/25/our-how-to-plan-design-operate-and-evolve-a-soc-papper-is-published/ (letöltve: 2016.10.25)

[5] KRASZNAY, CS.: *Naplózás e-kormányzati rendszerekben*; 2010. http://krasznay.hu/presentation/nws2010_krasznay.pdf (letöltve: 2017.09.02)

[6] *Common Criteria for Information Technology Security Evaluation 2009*. https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3%20-%20marked%20changes.pdf (letöltve: 2017.10.25)

[7] GOODALL, J.R.; LUTTERS, W.G.; KOMLODI, A.: *I Know My Network: Collaboration and Expertise in Intrusion Detection*. Proceedings of ACM Conference On Computer Supported Cooperative Work. 2004. pp. 342–345.