PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

podklad pre V4

Koncept SOC v širšom pohľade, terminológia a poskytovatelia

Previazané s pracovným balíkom KPB2 – Návrh SOCaaS služby

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1. KONCEPT SOC

Kybernetická bezpečnosť je v dnešnej digitálnej dobe neodmysliteľnou súčasťou našich životov a podnikových operácií. S rastúcim počtom kybernetických hrozieb a zraniteľností sa stáva nevyhnutným vybudovať efektívne operačné centrum kybernetickej bezpečnosti (SOC), ktoré bude schopné chrániť organizácie pred týmito hrozbami. S nástupom cloudových technológií v oblasti IT infraštruktúry a služieb nám cloudové riešenia poskytujú efektívny a flexibilný rámec pre prevádzku SOC.

1.1. Legislatívne východiská

Základným krokom pre budovanie SOC v Slovenskej republike je znalosť legislatívnych požiadaviek v oblasti kybernetickej bezpečnosti. Z tohto dôvodu je potrebné do tejto časti zhrnúť, aké legislatívne rámce musia byť dodržiavané, a aký vplyv bude mať nová smernica o kybernetickej bezpečnosti NIS2 na poskytovanie SOC služieb.

V rámci projektu boli študované vybrané národné, nadnárodné a európske plány a normy týkajúce sa kybernetickej bezpečnosti. Všetky informácie uvedené v tomto odseku sú čerpané zo smernice NIS2.

Dňa 14. decembra 2022 bola Európskym parlamentom predstavená nová smernica NIS2, ktorá sa zaoberá opatreniami na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Európskej únii (EÚ). Smernica NIS2 predstavuje rozšírenie predchádzajúcej smernice NIS1. V článku 6, v ktorom sú v smernici definované pojmy, je pre tento projekt významný najmä pojem „poskytovateľ riadených bezpečnostných služieb“. Týmto pojmom je označený taký poskytovateľ riadených služieb, ktorého činnosť spočíva vo vykonávaní alebo poskytovaní pomoci pri aktivitách súvisiacich s riadením kybernetických rizík.

Rovnako ako v prípade smernice NIS1, aj smernicou NIS2 sú stanovené opatrenia zamerané na dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v rámci celej EÚ, a to s cieľom zabezpečiť lepšie fungovanie vnútorného trhu. Za týmto účelom sú v smernici definované povinnosti, na základe ktorých sú členské štáty zaviazané doplniť národné stratégie kybernetickej bezpečnosti implementované do národnej legislatívy podľa predchádzajúcej smernice NIS1.

Zo smernice boli vybrané časti týkajúce sa SOCaaS a ďalších poskytovateľov bezpečnostných alebo riadených služieb, ktorými sme sa riadili počas práce na tomto projekte.

1.2. Základná terminológia

Bezpečnostné operačné centrum (SOC) je definované ako interný alebo externý tím odborníkov v oblasti kybernetickej bezpečnosti, prostredníctvom ktorého je zabezpečovaný nepretržitý monitoring celej IT infraštruktúry organizácie. Tento monitoring je vykonávaný s cieľom identifikovať udalosti týkajúce sa kybernetickej bezpečnosti v reálnom čase a zabezpečiť ich čo najrýchlejšie a najefektívnejšie riešenie.

V rámci činnosti SOC sú vyberané, prevádzkované a udržiavané technológie kybernetickej bezpečnosti, ktoré organizácia využíva. Zároveň sú priebežne analyzované údaje o hrozbách s cieľom identifikovať možnosti zlepšenia celkovej úrovne zabezpečenia organizácie.

Za hlavnú výhodu prevádzky SOC centra alebo využívania služieb SOC poskytovaných tretími stranami je považované zjednotenie a koordinácia bezpečnostných nástrojov, postupov a reakcií organizácie na bezpečnostné incidenty. Týmto prístupom je dosahované zlepšenie preventívnych opatrení a bezpečnostných politík, ako aj rýchlejšia, účinnejšia a nákladovo efektívnejšia reakcia na vzniknuté bezpečnostné hrozby. Prevádzka SOC taktiež prispieva k zvýšeniu dôvery zákazníkov a k zjednodušeniu a posilneniu súladu organizácie s priemyselnými, národnými a globálnymi predpismi v oblasti ochrany osobných údajov.

1.2.1. Príprava, plánovanie a prevencia

Inventarizácia aktív

V rámci činností SOC centra musí byť vedený prehľad všetkých aktív, ktoré je potrebné chrániť – a to bez ohľadu na to, či sa nachádzajú v dátovom centre alebo mimo neho (napr. aplikácie, databázy, servery, cloudové služby, koncové zariadenia a pod.). Zároveň musia byť evidované aj všetky nástroje, ktoré sú na ochranu týchto aktív využívané (napr. firewally, antivírusové, anti-malvérové, anti-ransomvérové riešenia, monitorovací softvér a i.). V mnohých prípadoch sú na zisťovanie aktív využívané špecializované softvérové riešenia.

Plánovanie reakcie na incidenty

Za vypracovanie plánu reakcie organizácie na kybernetické incidenty nesie zodpovednosť SOC centrum. V uvedenom pláne musia byť definované konkrétne činnosti, úlohy a zodpovednosti zainteresovaných subjektov, ako aj metriky, prostredníctvom ktorých bude hodnotená úspešnosť realizovanej reakcie na incident.

Rutinná údržba a príprava

Za účelom maximalizácie účinnosti bezpečnostných nástrojov a opatrení je v SOC centre pravidelne vykonávaná preventívna údržba. Tá zahŕňa aplikáciu softvérových záplat a aktualizácií, ako aj priebežnú úpravu firewallov, whitelistov, blacklistov, bezpečnostných politík a postupov monitorovania, klasifikácie a riešenia bezpečnostných incidentov. V rámci týchto činností sú taktiež vytvárané záložné kópie systémov alebo sú poskytované podklady pre návrh a implementáciu zásad a postupov zálohovania, ktoré zabezpečujú kontinuitu činnosti v prípade kybernetického incidentu, vrátane ransomvérového útoku alebo úniku dát.

Pravidelné testovanie

V SOC centre sú pravidelne vykonávané hodnotenia zraniteľnosti. Tieto hodnotenia slúžia na identifikáciu slabých miest v jednotlivých aktívach a vyhodnotenie ich odolnosti voči možným

kybernetickým hrozbám, vrátane odhadov finančných a reputačných strát. Súčasťou týchto aktivít sú aj penetračné testy, ktorými sú simulované reálne útoky na systémy organizácie. Výsledky týchto testov sú následne využívané na úpravu alebo zefektívnenie aplikácií, bezpečnostných politík, osvedčených postupov a plánov reakcie na incidenty.

Udržiavanie aktuálnosti

V SOC centre je zabezpečené neustále sledovanie najnovších trendov v oblasti bezpečnostných technológií a riešení, ako aj získavanie aktuálnych informácií o kybernetických hrozbách. Tieto informácie sú čerpané z rôznych zdrojov – vrátane sociálnych médií, odborných bezpečnostných portálov, komunitných fór a prostredí ako darkweb – a využívané pri rozhodovaní a aktualizácii bezpečnostných opatrení.

1.2.2. Monitorovanie, detekcia a reakcia

Monitorovanie, detekcia a reakcia

V SOC centre je zabezpečovaný nepretržitý dohľad nad celou rozšírenou IT infraštruktúrou – aplikáciami, servermi, systémovým softvérom, výpočtovými zariadeniami, cloudovými pracovnými zaťaženiami a sieťovou infraštruktúrou – 24 hodín denne, 7 dní v týždni a 365 dní v roku. Monitorovanie je zamerané na odhalenie známok známych zneužití a akýchkoľvek podozrivých aktivít.

Na tento účel sú využívané technológie SIEM (Security Information and Event Management) a SOAR (Security Orchestration, Automation and Response).

Využívanie SIEM

Systémy SIEM sú v SOC centrách nasadzované preto, aby bolo možné analyzovať údaje generované firewallmi, sieťovými zariadeniami, systémami na detekciu prienikov a inými zariadeniami. Tieto systémy zabezpečujú zhromažďovanie, filtrovanie, detekciu, klasifikáciu a vyšetrovanie hrozieb. Súčasne môžu byť využívané na implementáciu preventívnych opatrení a predikciu budúcich hrozieb.

Moderné SIEM riešenia sú vybavené umelou inteligenciou, vďaka ktorej môžu byť procesy automatizované a zefektívnené. Učením sa z údajov sa tieto systémy priebežne zlepšujú v identifikácii podozrivých aktivít.

Prepojenie SIEM a SOAR

Systémy SIEM sú často integrované s platformami SOAR, pretože ich schopnosti sa vzájomne dopĺňajú. Vo veľkých SOC centrách sú tieto technológie používané súbežne za účelom optimalizácie prevádzky.

SOAR platformy agregujú, korelujú a analyzujú upozornenia podobne ako SIEM, pričom navyše zabezpečujú integráciu spravodajských informácií o hrozbách a umožňujú automatizáciu procesov vyšetrovania a reakcie na incidenty. Tieto činnosti sa realizujú na základe vopred definovaných postupových manuálov (tzv. playbooks).

Funkcie SOAR systémov

Pomocou SOAR technológií sú zabezpečované tieto činnosti:

- **Zhromažďovanie výstražných údajov** zo všetkých komponentov systému.
- **Vyšetrovanie incidentov**, ich hodnotenie a forenzná analýza.
- **Automatizácia reakčných postupov** podľa preddefinovaných scenárov, čím je zabezpečená rýchla a konzistentná reakcia.
- **Automatická implementácia opatrení** v reakcii na detegované hrozby, pričom tieto opatrenia môžu byť spúšťané automaticky alebo manuálne pracovníkom SOC centra.

Manuálna reakcia bezpečnostného tímu

V prípade, že je incident pracovníkmi SOC centra vyhodnotený ako reálny, je naň reagované s cieľom minimalizovať škody. Medzi bežne vykonávané opatrenia patrí:

- Vyšetrovanie príčin incidentu a identifikácia technických alebo procesných nedostatkov (napr. slabé heslá, neefektívne politiky).
- Vypnutie alebo izolovanie kompromitovaných koncových bodov.
- Presmerovanie alebo blokovanie sieťovej prevádzky z napadnutých segmentov.
- Pozastavenie činnosti aplikácií alebo procesov podozrivých z kompromitácie.
- Odstránenie škodlivých alebo infikovaných súborov.
- Spustenie antivírusových alebo antimalvérových nástrojov.

Nástroje na monitorovanie, forenznú analýzu a reakciu na incidenty

Na účely monitorovania, zberu a analýzy sieťovej prevádzky sú v praxi využívané rôzne nástroje:

- **Sigma –** Je využívaný ako formát pre zdieľanie detekčných pravidiel škodlivého správania v rámci bezpečnostných tímov. Je vytvorený ako open-source štandard, ktorý umožňuje použitie rovnakých detekčných pravidiel naprieč rôznymi SIEM platformami (napr. Splunk, Azure Sentinel), logovacími systémami (Graylog) a databázami (MySQL).
- **YARA –** predstavuje framework založený na pravidlách, určený na identifikáciu a klasifikáciu vzoriek škodlivého softvéru. Pomocou textových aj binárnych vzorov sú vytvárané popisy malvérových rodín a iných digitálnych artefaktov vrátane hexadecimálnych reťazcov.
- **Velociraptor –** Open-source platforma vyvinutá špecialistami DFIR (Digital Forensics and Incident Response) na účely monitorovania koncových bodov, vyhľadávania digitálnych dôkazov a reakcie na incidenty. Velociraptor je využívaný na:
  - Rekonštrukciu aktivít útočníkov.
  - Vyhľadávanie dôkazov o pokročilých hrozbách.
  - Detekciu malvéru a neštandardných sieťových aktivít.
  - Monitorovanie podozrivej činnosti používateľov (napr. kopírovanie na USB).
  - Zisťovanie únikov citlivých údajov mimo organizácie.
  - Dlhodobý zber dát pre účely vyhľadávania hrozieb a retrospektívnych analýz.
- **QRadar –** je komplexný nástroj spoločnosti IBM, ktorý prepája SIEM, SOAR, EDR/XDR/MDR riešenia a poskytuje centralizované používateľské rozhranie. Využíva umelú

inteligenciu na zefektívnenie analýzy incidentov, čím prispieva k lepšej efektivite analytikov SOC centra.

– **Wazuh –** je open-source riešenie na sledovanie bezpečnosti a detekciu hrozieb. Prostredníctvom agentov je zabezpečovaný zber údajov z rôznych zdrojov (napr. logy, udalosti), ktoré sú následne analyzované centrálnym manažérom. Wazuh poskytuje rozšírené možnosti detekcie, generovania výstrah a reakcie na incidenty, čím podporuje kybernetickú bezpečnosť organizácie.

1.2.3. Obnova, zdokonaľovanie a dodržiavanie predpisov

Obnova a náprava

Po zvládnutí incidentu je hrozba odstránená pracovníkmi SOC centra a následne sú vykonané kroky na obnovenie postihnutých prostriedkov do pôvodného stavu pred incidentom. Medzi tieto kroky patrí napríklad vymazanie, obnovenie a opätovné pripojenie diskov, zariadení koncových používateľov a iných koncových bodov, obnova sieťovej prevádzky a reštart aplikácií a procesov. V prípadoch ako je únik údajov alebo ransomvérový útok môže byť obnova zabezpečená aj prepnutím na záložné systémy a zmenou hesiel či autentifikačných údajov.

Následná analýza a zdokonalenie

S cieľom zabrániť opakovaniu incidentu sú všetky nové informácie získané počas jeho riešenia využívané na zlepšenie identifikovaných zraniteľností, aktualizáciu procesov a politík, výber vhodnejších nástrojov kybernetickej bezpečnosti alebo úpravu plánu reakcie na incident. Na strategickej úrovni sa tím SOC centra môže usilovať o identifikáciu trendov alebo nových smerov vývoja kybernetických hrozieb, ktoré by mohli v budúcnosti ovplyvniť bezpečnostný profil organizácie.

Riadenie dodržiavania predpisov

Zaistenie súladu s legislatívnymi a regulačnými požiadavkami patrí medzi základné úlohy SOC centra. Je zabezpečované, aby všetky aplikácie, systémy, bezpečnostné nástroje a procesy spĺňali požiadavky vyplývajúce z platných predpisov o ochrane údajov, ako sú napríklad GDPR, PSD2 a ďalšie regulácie platné v krajine, kde je SOC centrum prevádzkované.

Na území Slovenskej republiky je zabezpečované dodržiavanie požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Osobitne sú dodržiavané §18 (Identifikačné kritériá prevádzkovanej služby) a §19 (Povinnosti prevádzkovateľa základnej služby).

Po kybernetickom incidente je zabezpečené, aby boli všetky dotknuté subjekty – používatelia, regulačné orgány, orgány činné v trestnom konaní a ďalšie zainteresované strany – informované v súlade s príslušnými ustanoveniami, napr. §24 zákona č. 69/2018 Z. z. Zároveň sú uchovávané všetky relevantné údaje o incidente na účely forenzného dokazovania a auditu.

Požiadavky podľa NIST – Príručka na riešenie incidentov

Národným inštitútom pre štandardy a technológie Spojených štátov amerických (NIST) bola vydaná publikácia „NIST Special Publication 800-61 Rev. 2“, známa aj ako „Computer Security Incident Handling Guide“. Táto príručka poskytuje podrobné odporúčania a metodiky pre organizácie v oblasti riadenia kybernetických incidentov.

V dokumente sú definované štandardné postupy pre:

- identifikáciu a klasifikáciu incidentov,
- ich hlásenie, analýzu a riešenie,
- zabezpečenie záznamov a forenznej dokumentácie.

Súčasťou príručky sú aj odporúčania pre vytváranie a implementáciu plánov reakcie na incidenty (Incident Response Plans), ktoré pomáhajú organizáciám rýchlo reagovať na hrozby a zmierňovať ich dopady na infraštruktúru, prevádzku a reputáciu.

1.3. Požiadavky a komponenty SOC centra

Typy modelov SOC centra

Okrem štandardného SOC centra existujú aj iné typy centier a služieb, prostredníctvom ktorých je zabezpečovaná ochrana sietí a digitálnej infraštruktúry organizácií. Tieto centrá môžu mať spoločné alebo prekrývajúce sa vlastnosti a funkcie, pričom nie je striktne definované, aký rozsah musí každé centrum spĺňať. V praxi je rozsah pôsobnosti každého modelu SOC centra prispôsobovaný konkrétnym potrebám organizácie.

1.3.1. Základné typy modelov:

Interné SOC centrum (Internal SOC) – Je zriaďované samotným podnikom. Zamestnanci sú zamestnávaní priamo organizáciou a tvoria interný tím kybernetickej bezpečnosti. SOC je vlastnené a prevádzkované podnikom.

Externé SOC centrum (External SOC, SOCaaS) – Je poskytované externým dodávateľom ako služba. Prevádzka je realizovaná napríklad formou Managed Security Services (MSS). Môže byť implementované ako cloudové riešenie.

Globálne alebo riadiace SOC centrum (Global / Command SOC) – Plní úlohu centrálnej autority, ktorá koordinuje činnosť viacerých menších SOC centier v rámci organizácie alebo regiónu.

Spolu riadené SOC centrum (Co-Managed SOC) – Prevádzka je realizovaná v spolupráci interného IT tímu organizácie a externého dodávateľa SOC služieb. Zodpovednosti a činnosti sú rozdelené medzi obe strany.

MSSP – Poskytovateľ riadených bezpečnostných služieb – Ide o poskytovateľa služieb s mnohými spoločnými črtami so SOC centrami. Detailnejšia špecifikácia je uvedená v časti 4.3.1.

MDR – Riadená detekcia a odpoveď (Managed Detection and Response) – Zameriava sa na

detekciu a aktívnu reakciu na hrozby. Incidenty sú analyzované, falošné poplachy sú odstraňované a skutočné hrozby riešené v mene klienta.

1.3.2. Personálne úrovne v SOC centre

V SOC centre sa pracovné úlohy prideľujú podľa úrovní SOC analytikov. Úrovne sa určujú podľa odborných znalostí a zodpovedností, ktoré sa pre jednotlivé úrovne vyžadujú. V SOC centre sú zvyčajne štyri úrovne:

Úroveň 1 – Analytik výstrah (alertov)

- monitoruje prichádzajúce výstrahy.
- ak zistí že výstraha je pravdivá:
  - spraví základné opatrenia na zmiernenie dopadov danej hrozby.
  - alebo ak je to potrebné, predá riešenie hrozby pracovníkovi úrovne 2.
- ak zistí že incident je nepravdivý:
  - aktualizuje systém pre detekciu incidentov, ktorý danú výstrahu vygeneroval.
  - ak incident nedokáže vyriešiť predá hrozbu pracovníkovi úrovne 2.

Úroveň 2 – Riešiteľ incidentov (Incident Responder)

- skúma incidenty do hĺbky.
- navrhne, ako by sa mal problém riešiť,
- odporučí nápravu (akciu),

Úroveň 3 – Hľadač hrozieb (Threat hunter)

- je to expert v oblasti sietí, koncových zariadení, hrozieb, informácií o hrozbách a reverzného inžinierstva malvéru.
- sleduje procesy malvéru s cieľom určiť jeho vplyv, a ako ho možno odstrániť (vrátane preventívnych opatrení).
- je hlboko zapojený do hľadania potenciálnych hrozieb a implementácie nástrojov na detekciu hrozieb.
- proaktívne hľadá kybernetické hrozby, ktoré sú prítomné v sieti, ale ešte neboli detegované.

SOC manažér (SOC Manager)

- spravuje všetky zdroje v SOC centre.
- slúži ako bod kontaktu pre organizácie, zákazníkov.
- implementujte štandardizované prevádzkové postupy (Standard Operating Procedures, SOPs) pre proces riešenia incidentov, ktoré usmerňujú analytikov prostredníctvom postupov triedenia a reakcie.

Bezpečnostné tímy v kybernetickej bezpečnosti

V rámci rozdelenia úloh a simulácií sa využívajú farebne označené tímy:

- **Červený tím (Red Team)** – Simuluje útočníka. Identifikujú sa slabiny v ochrane.
- **Modrý tím (Blue Team)** – Reaguje na incidenty a zabezpečuje obranné mechanizmy.

- **Fialový tím (Purple Team)** – Integruje činnosti červeného a modrého tímu. Zameriava sa na spoluprácu.
- **Žltý tím (Yellow Team)** – Tvorí ho bezpečnostní architekti a vývojári bezpečnostných systémov.
- **Zelený tím (Green Team)** – Podľa výstupov modrého tímu vylepšuje kód vytvorený žltým tímom.
- **Oranžový tím (Orange Team)** - Využíva poznatky z červenej tímovej analýzy na zvyšovanie povedomia vývojárov.

Činnosť týchto tímov, predovšetkým červeného a modrého, je využívaná v SOC centre na odhaľovanie a odstránenie zraniteľností.

1.3.3. Metriky výkonnosti v SOC centre

Na hodnotenie efektivity prevádzky SOC centra sú využívané rôzne KPI – Key Performance Indicators. Bežne sú sledované nasledovné metriky:

- **Čas zdržania (Dwell Time) –** Doba, počas ktorej mal aktér hrozby prístup do siete pred jeho detekciou a zneškodnením.
- **Priemerný čas detekcie (MTTD – Mean Time to Detect) –** Čas potrebný na identifikáciu reálneho incidentu.
- **Stredný čas na reakciu (MTTR – Mean Time to Respond) –** Čas potrebný na zastavenie a odstránenie incidentu.
- **Priemerný čas na obmedzenie (MTTC – Mean Time to Contain) –** Čas potrebný na lokalizáciu incidentu pred šírením škôd.
- **Čas na kontrolu (Time to Control)** – Doba potrebná na zastavenie šírenia škodlivého softvéru v sieti.

1.4. Výhody a nevýhody SOC

Existuje množstvo dôvodov, pre ktoré by malo byť implementované bezpečnostné operačné centrum (SOC), a to buď formou interného, alebo externého riešenia. Kybernetická bezpečnosť je oblasť, ktorou sa musia zaoberať všetky moderné podniky, pretože s rastom organizácie rastie aj pravdepodobnosť, že sa stane terčom kybernetického útoku.

V tejto časti sú zhrnuté hlavné výhody a nevýhody nasadenia SOC centra. Informácie boli spracované na základe zdrojov .

1.4.1. Výhody SOC centra

Nepretržité monitorovanie

Vďaka nepretržitému monitorovaniu a analýze aktivít naprieč celou sieťovou infraštruktúrou je možné včas identifikovať kybernetické bezpečnostné incidenty a okamžite na ne reagovať. Táto vlastnosť je považovaná za jednu z najzásadnejších, keďže čas je rozhodujúcim faktorom pri efektívnej reakcii na bezpečnostný incident.

Rýchla reakcia na incidenty

V prípade výskytu incidentu je zabezpečená rýchla reakcia analytikov SOC centra. Po prijatí výstrahy je incident preskúmaný, hrozba obmedzená a dôsledky incidentu minimalizované. Týmto spôsobom sa skracuje čas nefunkčnosti systémov a služieb.

Proaktívna detekcia hrozieb

Sledovaním sieťovej aktivity a systémových protokolov sú vyhľadávané anomálie a potenciálne hrozby ešte pred ich vypuknutím. Na základe týchto zistení sú prijímané preventívne opatrenia, ktorými sa predchádza incidentom a škodám.

Integrácia informácií o hrozbách

Analytikom SOC centra je umožnený prístup k aktuálnym informáciám o vznikajúcich typoch útokov a technikách, ktoré sú útočníkmi používané. Vďaka týmto informáciám môže byť zabezpečený náskok pred potenciálnymi hrozbami.

Centralizovaná správa bezpečnosti

SOC centrum funguje ako hlavný uzol pre riadenie bezpečnostnej politiky organizácie. Je poskytovaný centralizovaný prehľad o úrovni bezpečnosti, zjednodušené riadenie bezpečnostných opatrení, presadzovanie interných politík a dodržiavanie regulačných požiadaviek.

Zároveň je umožnené:

- efektívne reagovanie na incidenty v reálnom čase,
- konsolidácia bezpečnostných údajov z rôznych zdrojov,
- koordinácia medzi analytikmi, IT administrátormi a zodpovednými pracovníkmi.

Prispôsobené bezpečnostné riešenia

Riešenia poskytované SOC centrom sú prispôsobované konkrétnym potrebám organizácie. Výber nástrojov, procesov a technológií je realizovaný v súlade s bezpečnostnými výzvami a strategickými cieľmi podniku.

Personalizované SOC centrum umožňuje:

- zosúladenie bezpečnosti s obchodnými cieľmi,
- zabezpečenie súladu s legislatívou a štandardmi,
- ochranu citlivých údajov a predchádzanie neoprávneným prístupom.

Nákladová efektívnosť

Aj keď zriadenie SOC centra predstavuje počiatočnú investíciu, dlhodobé výhody, ako je zníženie výskytu incidentov a ich dopadu, môžu výrazne prevýšiť náklady. Prevenciou incidentov je možné predísť finančným stratám a poškodeniu reputácie.

1.4.2. Nevýhody SOC centra

Veľký objem dát

S narastajúcim počtom výstrah je vyžadované nasadenie pokročilých analytických systémov a kvalifikovaných pracovníkov na ich správne vyhodnotenie a triedenie. Pri vysokej záťaži hrozí riziko nesprávnej klasifikácie alebo prehliadnutia závažných incidentov. Zvýrazňuje sa tým potreba automatizácie a dostatočne veľkého tímu expertov.

Nákladovosť

Budovanie a udržiavanie SOC centra si vyžaduje značné finančné a časové prostriedky. Vzhľadom na dynamický vývoj hrozieb je potrebné zabezpečiť:

- pravidelné aktualizácie systémov,
- kontinuálne vzdelávanie personálu,
- odborné kapacity v oblasti hĺbkovej bezpečnostnej analýzy.

Z týchto dôvodov mnohé organizácie preferujú outsourcing SOC funkcií prostredníctvom služieb typu SOCaaS.

Nedostatok personálnych kapacít

Kybernetická bezpečnosť je odbor náročný na expertízu. Nájdenie a udržanie kvalifikovaných pracovníkov predstavuje významnú výzvu, predovšetkým pri interných riešeniach. Mnohí odborníci preferujú zamestnanie u poskytovateľov SOC služieb, kde je zvyčajne zabezpečené odborné zázemie, výmena poznatkov a atraktívnejšie profesijné prostredie.

2. SOC VS. SOCAAS

Hlavný rozdiel medzi interným SOC centrom a SOCaaS (Security Operations Center as a Service) spočíva v ich správe a vlastníctve.

Interné SOC centrum je zriaďované, vlastnené a prevádzkované samotnou organizáciou, ktorej je určené. V rámci podniku sú zamestnávaní odborníci na kybernetickú bezpečnosť, ktorí zabezpečujú činnosť centra.

Naopak, SOCaaS, teda externé SOC centrum poskytované ako služba, je zabezpečované externým dodávateľom, ktorý poskytuje buď celé SOC centrum alebo len jeho komponenty ako službu. V tejto časti boli informácie čerpané zo zdrojov.

2.1. Funkcionality a charakteristiky SOCaaS

SOCaaS predstavuje cloudový model kybernetickej bezpečnosti poskytovaný formou predplatného. Je navrhnutý ako služba riadenej detekcie hrozieb a reakcie na ne, pričom sú pokryté funkcie a kapacity typické pre plnohodnotné SOC centrum. Tento model slúži na zaplnenie medzier v existujúcich bezpečnostných tímoch organizácií.

Podobne ako interné centrá, aj SOCaaS zabezpečuje:

- nepretržité monitorovanie,
- detekciu hrozieb,
- prevenciu a analýzu útočného priestoru,
- monitorovanie siete, koncových zariadení, databáz a cloudovej infraštruktúry,
- využívanie SIEM systémov, firewallov a threat intelligence nástrojov.

2.2. Rozdiely medzi SOCaaS a Co-Managed SOC

Spolu-riadené SOC centrum (Co-managed SOC)

V modeli spolu-riadeného SOC centra je organizácii poskytovaný bezpečnostný personál od externého dodávateľa (vrátane analytikov 1.–3. úrovne a SOC manažéra), ktorí spolupracujú s interným IT tímom zákazníka. Zariadenia a infraštruktúra pre monitorovanie siete sú vo vlastníctve zákazníka; dodávateľ zabezpečuje len expertízu.

Činnosti v tomto modeli zvyčajne zahŕňajú:

- monitorovanie a detekciu hrozieb,
- vyšetrovanie incidentov,
- prípadne aj dodržiavanie predpisov a návrh nápravných opatrení.

Poskytovanie kompletného riešenia incidentu však nie je garantované – závisí od konkrétneho poskytovateľa služby.

Výhody Co-managed SOC:

- Úspora nákladov – organizácia nemusí zamestnávať vlastný bezpečnostný tím.

Nevýhody Co-managed SOC:

- Zložitosť integrácie – spolupráca dvoch tímov (interného a externého) si vyžaduje vysokú mieru koordinácie.

– Závislosť od dodávateľa – v prípade jeho zlyhania môže dôjsť k narušeniu kybernetickej bezpečnosti.

Tento model je vhodný najmä pre malé a stredné podniky, ktoré nemajú dostatok interných zdrojov na vybudovanie plnohodnotného bezpečnostného tímu.

SOCaaS – Plne outsourcovaný model

SOCaaS je model, v ktorom je bezpečnostné operačné centrum prevádzkované v cloude a poskytované ako služba. Služba je zvyčajne poskytovaná formou predplatného, bez potreby budovania internej infraštruktúry alebo zamestnávania špecialistov.

Služba SOCaaS zahŕňa:

– vzdialené monitorovanie a reakciu na incidenty,
– zabezpečenie odborných znalostí bez potreby ich interného držania,
– úsporu nákladov prostredníctvom škálovateľného modelu.

Funkcionality SOCaaS:

Zabezpečený je technologický balík, ktorý zahŕňa nástroje a procesy v SOC centra, rovnako ako je poskytnutý tím odborníkov (analytici a manažéri).

Implementované sú:

– monitorovacie a výstražné mechanizmy,
– eskalačné matice,
– automatizácia reakcie a analytiky,
– vzdialený dohľad nad bezpečnostnými operáciami.

Po zaškolení a integrácii systémov je zabezpečený nepretržitý dohľad a komunikácia s organizáciou zákazníka. Organizácia má možnosť:

– monitorovať svoju infraštruktúru,
– vykonávať bezpečnostné testy,
– získavať odporúčania na zlepšenie bezpečnostnej úrovne.

Rozsah služby SOCaaS

Nie je stanovené, aké funkcie musí SOCaaS bezpodmienečne obsahovať – preto sa ponuka líši podľa poskytovateľa. Niektorí dodávatelia poskytujú len pasívne monitorovanie a reporting, pričom nápravu incidentov prenechávajú na zákazníka.

Zodpovednosť za bezpečnosť nie je výlučne na strane poskytovateľa služby. Organizácia musí dodržiavať interné bezpečnostné politiky a opatrenia vytvorené v spolupráci s analytikmi SOC centra, a to v súlade s legislatívnymi rámcami.

2.2.1. Výhody služby SOCaaS

Služba SOCaaS (Security Operations Center as a Service) poskytuje výhody porovnateľné s tými, ktoré boli uvedené pri internom SOC centre, a zároveň rieši viaceré nevýhody, ktoré boli identifikované pri implementácii interného SOC. V tejto časti sú prezentované výhody, ktoré sú pre SOCaaS jedinečné.

Nákladová efektívnosť

Služba SOCaaS je poskytovaná formou predplatného. Organizáciám tak odpadá potreba investovať do infraštruktúry, licencií a náboru interných zamestnancov. Týmto spôsobom sú minimalizované počiatočné kapitálové výdavky a optimalizované prevádzkové náklady.

Prístup k odborníkom

Vzhľadom na globálny nedostatok kvalifikovaných špecialistov v oblasti kybernetickej bezpečnosti, je pre mnohé organizácie problematické vytvoriť interný tím analytikov. Využitím služby SOCaaS je zabezpečený prístup k expertom bez potreby ich vlastného zamestnávania.

Automatizované bezpečnostné procesy

Vysoká miera automatizácie a integrácia umelej inteligencie umožňuje efektívne triedenie a vyhodnocovanie výstrah. Opakujúce sa úlohy sú spracovávané automaticky, čím sa zvyšuje efektivita reakcie na incidenty a umožňuje sa zameranie analytikov na kritické úlohy.

2.2.2. Nevýhody služby SOCaaS

Aj napriek početným výhodám predstavuje využitie externých SOC služieb určité výzvy, ktoré sa pri internom SOC vyskytovať nemusia.

Prispôsobenie sa novému procesu

Implementácia služby SOCaaS vyžaduje preorganizovanie interných procesov a akceptáciu nových bezpečnostných protokolov. Zložitosť môže vzniknúť pri zisťovaní kompatibility technologického balíka poskytovateľa so špecifikami IT prostredia organizácie. Je potrebné, aby si zamestnanci osvojili nové politiky a aby analytici poskytovateľa porozumeli infraštruktúre klienta. Zavedenie služby vyžaduje plánované nábehové obdobie.

Regulačné požiadavky

Nie všetci poskytovatelia SOCaaS pokrývajú povinnosti súvisiace s dodržiavaním legislatívy, ako napríklad GDPR, HIPAA, ISO 27001, alebo slovenský zákon č. 69/2018 Z. z.. Overenie súladu je potrebné zabezpečiť individuálne.

Zdieľanie informácií

Aby mohla byť služba vykonávaná efektívne, musí byť poskytovateľovi umožnený prístup k internej infraštruktúre a citlivým údajom. S tým je spojené riziko zneužitia alebo úniku informácií, pretože pracovníci poskytovateľa môžu sledovať aktivitu zamestnancov a mať prístup k dôverným informáciám.

2.2.3. Rozdiely medzi SOCaaS, MSSP a MDR

MSSP – Managed Security Service Provider

MSSP je externý poskytovateľ bezpečnostných služieb, ktorého úlohou je doplniť alebo nahradiť interný bezpečnostný tím organizácie. Okrem monitorovania a správy bezpečnostných zariadení je MSSP zameraný aj na návrh a implementáciu bezpečnostných politík.

Hoci sú technológie a služby podobné ako pri SOC, rozdiel spočíva v nižšej miere analýzy incidentov. MSSP plní skôr úlohu strategického partnera pre návrh bezpečnostného rámca, pričom incidenty sú riešené v menšej hĺbke než v SOC.

MDR – Managed Detection and Response

MDR predstavuje službu špecializovanú na detekciu a reakciu. V porovnaní s MSSP sa sústredí na aktívne odhaľovanie a riešenie incidentov v mene organizácie.

MDR spája technológie a analytikov a využíva vysokú mieru automatizácie. Zameriava sa na komplexné incidenty, pričom konfigurácia siete a bežná správa ostáva zodpovednosťou organizácie.

Nevýhodou MDR je, že pokrýva len oblasť detekcie a reakcie – ostatné oblasti kybernetickej bezpečnosti si vyžadujú vlastný tím.

Charakteristika	MSSP	MDR	SOCaaS
Primárne zameranie	Prevencia, monitoring, návrh politík	Detekcia, reakcia, analýza incidentov	Komplexná ochrana a reakcia na incidenty
Úroveň služieb	Monitoring a konfigurácia	Pokročilá reakcia a forenzná analýza	Všetky fázy – od detekcie po obnovu
Ľudské zdroje	Externí analytici	Externí analytici so špecializáciou	Externý tím pre monitoring a podporu
Technologická náročnosť	Nízka až stredná	Stredná až vysoká	Vysoká – automatizácia, AI, cloud platformy
Potreba interného tímu	Voliteľná (možné úplne nahradiť)	Vyžaduje doplnkový tím	Potrebný základný IT tím

Pre koho je SOCaaS vhodná

Služba SOCaaS je vhodná najmä pre malé a stredné podniky s obmedzenými zdrojmi. Investície do kybernetickej bezpečnosti bývajú pre tieto podniky náročné, pričom SOCaaS ponúka dostupnú možnosť profesionálnej ochrany bez nutnosti budovať vlastný tím a infraštruktúru.

2.2.4. Poskytovatelia SOCaaS na Slovensku a vo svete

Svetoví poskytovatelia SOCaaS

- **Arctic Wolf Networks** – Poskytuje SOCaaS aj MSP služby, riešenia pre kybernetické poistenie a doplnkové služby SOC.
- **Rapid7** – Zameriava sa na MDR, penetračné testy, školenia v oblasti správy zraniteľností, detekcie a automatizácie.
- **Alert Logic** – Poskytuje SOCaaS, MSP služby a bezplatné aj platené školenia.

Ďalšími významnými poskytovateľmi sú **Secureworks, Qualysec, Trustwave a Blackpoint Cyber.**

Slovenskí poskytovatelia SOCaaS

- **ESET** – Ponúka služby MDR a súvisiace bezpečnostné služby pre firemný sektor.
- **Slovak Telekom –** Ponúka dve úrovne služby: SOCaaS Light (notifikácia incidentov) a SOCaaS Plus (okamžitá reakcia).
- **Soitron –** Prevádzkuje Soitron Security Sensor, poskytuje SOC služby, analytiku, poradenstvo a podcast Lokál hosť.
- **Aliter Technologies –** Poskytuje SOCaaS, bližšie informácie dostupné na vyžiadanie.
- **Binary Confidence –** Ponúka 24/7 monitorovanie a riešenie incidentov.
- **TÜV SÜD Slovakia –** Zameraný na sektory kritickej infraštruktúry podľa zákona 69/2018 Z. z., ponúka tri varianty služby: BASIC, STANDARD, PREMIUM.

ZOZNAM ZDROJOV

[1] EUR-Lex, “CELEX_32022L2555_SK_TXT”, Accessed: Oct. 21, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32022L2555&qid=1697886701099
[2] Národný bezpečnostný úrad, “Strategia_kybernetickej_bezpecnosti_2021”, Accessed: Apr. 27, 2024. [Online]. Available: https://www.nbu.gov.sk/612-sk/narodna-strategia-a-akcny-plan-kybernetickej-bezpecnosti/
[3] IBM, “What is Security Operations Center (SOC)? | IBM.” Accessed: Nov. 26, 2023. [Online]. Available: https://www.ibm.com/topics/security-operations-center
[4] Cisco, “Cisco Certified CyberOps Associate - Cisco.” Accessed: Dec. 03, 2023. [Online]. Available: https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/cyberops-associate.html
[5] Clearnetwork, “What is a Managed SOC? Benefits and Variants -.” Accessed: Apr. 25, 2024. [Online]. Available: https://www.clearnetwork.com/what-is-managed-soc-benefits-and-variants/
[6] IBM, “What is Security Operations Center (SOC)? | IBM.” Accessed: Feb. 21, 2024. [Online]. Available: https://www.ibm.com/topics/security-operations-center
[7] GitHub, “GitHub - SigmaHQ/sigma: Main Sigma Rule Repository.” Accessed: Feb. 21, 2024. [Online]. Available: https://github.com/SigmaHQ/sigma?tab=readme-ov-file#readme
[8] Picus Security, “What Is a YARA Rule?” Accessed: Feb. 21, 2024. [Online]. Available: https://www.picussecurity.com/resource/glossary/what-is-a-yara-rule
[9] Rapid7, “Velociraptor Overview :: Velociraptor - Digging deeper!” Accessed: Feb. 21, 2024. [Online]. Available: https://docs.velociraptor.app/docs/overview/
[10] Wazuh, “Wazuh - Open Source XDR. Open Source SIEM.” Accessed: Apr. 12, 2024. [Online]. Available: https://wazuh.com/
[11] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide,” Aug. 2012, doi: 10.6028/NIST.SP.800-61R2.
[12] The National Institute of Standards and Technology (NIST), “SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC.” Accessed: Apr. 24, 2024. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/61/r2/final
[13] Cisco, “Course: 2023_CyberOps.” Accessed: Feb. 21, 2024. [Online]. Available: https://lms.netacad.com/course/view.php?id=2141844
[14] Coursera, “Red Team vs. Blue Team in Cybersecurity | Coursera.” Accessed: Mar. 10, 2024. [Online]. Available: https://www.coursera.org/articles/red-team-vs-blue-team
[15] Tata Communications, “MSSP vs SOC: Unraveling Key Differences for Enterprises.” Accessed: Mar. 08, 2024. [Online]. Available: https://www.tatacommunications.com/knowledge-base/mssp-vs-soc/