PROJEKT

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

V6 popis dashbordov, monitorovacieho a reportovacieho systému

KPB2 – Návrh SOCaaS služby

typ – dokumentácia

mesiac odovzdania – M7

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

OBSAH

1. ÚVOD

Tento dokument predstavuje výstup V6 projektu INNOSOC, ktorého cieľom je detailne popísať návrh architektúry služby SOCaaS (Security Operations Center as a Service), špecifikáciu hlavných rolí a procesov v SOC centre, ako aj návrh a ukážky monitorovacieho a reportingového systému vybudovaného nad open-source platformou ELK (Elasticsearch, Logstash, Kibana). Zvolená architektúra a komponenty vychádzajú z analýzy potrieb viaczákazníckeho, modulárneho a škálovateľného SOC, testovania jednotlivých open-source riešení a skúseností riešiteľského kolektívu.

Výstup reflektuje praktické potreby prevádzky SOC centra v hybridnom a distribuovanom prostredí, zohľadňuje požiadavky na automatizáciu, integráciu, bezpečnosť a reporting, a stavia na odporúčaných komponentoch identifikovaných v predchádzajúcich výstupoch projektu.

2. ARCHITEKTÚRA SYSTÉMU SOCAAS INNOSOC

Architektúra navrhovaného SOCaaS riešenia pozostáva z viacerých modulárnych komponentov, ktoré spolu tvoria súdržný a škálovateľný ekosystém. Architektúra bola navrhnutá s cieľom podporiť bezpečnostný monitoring, detekciu, reakciu, správu incidentov, ako aj tvorbu prehľadov a znalostných databáz.

Základné architektonické oblasti možno rozdeliť nasledovne:

a) Komponenty spracovania a detekcie

- SIEM (Security Information and Event Management): centrálne miesto pre zber a analýzu logov.
- EDR/XDR (Endpoint/Extended Detection and Response): detekcia hrozieb na koncových bodoch.
- CTI (Cyber Threat Intelligence): externé údaje o hrozbách a ich integrácia do procesov.
- Skener zraniteľností: automatizované zisťovanie slabých miest v infraštruktúre.

b) Komponenty reakcie a manažmentu incidentov

- SOAR (Security Orchestration, Automation and Response): koordinácia a automatizácia reakcií.
- Tiketovací systém: evidencia a správa požiadaviek a incidentov.
- Správa incidentov: prípadové riadenie bezpečnostných udalostí.
- Reporting: prehľad výstupov z detekcie, reakcie a stavu bezpečnosti.
- Znalostný portál: dokumentácia a zdieľanie vedomostí medzi členmi tímu.

c) Podporné komponenty a integrácie

- Asset management: evidencia aktív a ich väzieb.
- Integrácia s externými API, sandboxami, databázami IOC/CTI a notifikačnými kanálmi.
- Riadenie prístupov a audit: logovanie činností a zabezpečenie prevádzky.

3. ROLY A PROCESY V SOC CENTRE

3.1. Organizačné roly v SOC

Efektívne fungovanie bezpečnostného operačného centra (SOC) je podmienené jasne definovanými rolami jednotlivých členov tímu, ktorí spolupracujú na detekcii, analýze, eskalácii a mitigácii kybernetických hrozieb. V kontexte návrhu SOCaaS pre projekt INNOSOC boli definované základné organizačné roly nasledovne:

- **Level 1 (L1) analytik**: Prvá línia obrany, ktorá monitoruje výstrahy, vykonáva počiatočnú validáciu incidentov a zabezpečuje ich dokumentovanie. Typicky pracuje so SIEM dashboardmi, ticketingovým systémom a databázou znalostí.
- **Level 2 (L2) analytik**: Skúsenejší analytik, ktorý preberá eskalované prípady od L1. Vykonáva hlbšiu analýzu, využíva korelačné pravidlá, threat intelligence a spolupracuje na tvorbe reakčných opatrení. Často využíva rozhrania SOAR nástrojov a forenzné nástroje.
- **Level 3 (L3) špecialista/inžinier**: Odborník na zložité incidenty, pokročilý threat hunting, tvorbu detekčných pravidiel a konfiguráciu nástrojov ako SIEM či EDR. Zapája sa aj do architektúry a automatizácie reakcií.
- **Vedúci SOC (SOC manager)**: Zodpovedá za prevádzku a kapacity SOC tímu, SLA, spoluprácu so zákazníkmi, reporting a kontrolu výkonnosti. Koordinuje ľudské aj technologické zdroje, vrátane plánovania zmien, monitorovania kvality reakcií a rozvoja tímu.
- **Incident handler/incident response lead**: Rola zodpovedná za koordináciu reakcie na incident – plánovanie úloh, zber dôkazov, komunikáciu so zainteresovanými stranami a tvorbu záverečných reportov.
- **Threat Intelligence analytik**: Zodpovedá za prácu s hrozbami z CTI zdrojov, tvorbu profilov útočníkov, obohacovanie incidentov o IOC a TTP, sledovanie trendov a zdieľanie výstrah.
- **Správca systémov a architektúry SOC**: Technická rola zodpovedná za nasadenie, správu a aktualizáciu všetkých komponentov SOCaaS architektúry vrátane ELK Stacku, SOAR, asset managementu a iných nástrojov.

Tieto roly nie sú rigidné – môžu sa líšiť v závislosti od veľkosti SOC tímu, štruktúry zákazníkov a SLA. V prostredí multitenantnej SOCaaS architektúry je kľúčová aj schopnosť priraďovať analytikov jednotlivým zákazníkom, prípadne ich delegovať na rôzne typy úloh podľa priority a kapacity.

3.2. Procesy v SOC

Bezpečnostné operačné centrum (SOC) funguje ako centrálna jednotka pre riadenie bezpečnosti IT prostredia organizácie. Jeho činnosť je postavená na definovaných procesoch, ktoré zabezpečujú efektívne monitorovanie, detekciu, analýzu a reakciu na kybernetické hrozby. Tieto procesy musia byť presne definované, dobre zdokumentované a pravidelne vyhodnocované, aby zaručili konzistentnú a koordinovanú prevádzku SOC.

V rámci projektu SOCaaS INNOSOC boli definované nasledovné kľúčové procesy, ktoré predstavujú operatívny rámec fungovania SOC centra:

- Proces monitorovania bezpečnostných udalostí – zabezpečuje zber a sledovanie logov, metrických údajov a alertov zo všetkých integrovaných systémov. V našom prípade sa opiera najmä o komponent ELK (Elasticsearch, Logstash, Kibana).

- Proces detekcie incidentov – je zodpovedný za identifikáciu anomálií, vzorcov útokov a iných hrozieb prostredníctvom korelačných pravidiel a heuristických mechanizmov.
- Proces reakcie na incidenty – definuje spôsob, akým tím reaguje na identifikované incidenty. Zahŕňa eskaláciu, priradenie zodpovednosti, vykonanie opatrení, ako aj komunikáciu so zasiahnutými stranami. Je implementovaný v súčinnosti s komponentmi SOAR a Ticketing.
- Proces správy incidentov – zahŕňa evidenciu, klasifikáciu, priraďovanie priorít, dokumentovanie a uzatváranie incidentov. V projekte sa opiera o nástroje ako TheHive, RTIR alebo Zammad.
- Proces správy hrozieb (Threat Intelligence) – umožňuje systematickú prácu s informáciami o hrozbách. Využívajú sa CTI nástroje ako OpenCTI, MISP či IntelMQ, ktoré poskytujú externé aj interné zdroje informácií.
- Proces reporting a vizualizácia – zabezpečuje pravidelný výstup pre manažment, audítorov a SOC analytikov. Vychádza z komponentov Kibana a Grafana a nadväzuje na monitorovací systém ELK.
- Proces správy poznatkov – zabezpečuje udržiavanie znalostnej bázy playbookov, dokumentácie a odporúčaných reakcií. Opiera sa o nástroje ako Wiki.js a BookStack.

Každý z týchto procesov bol v rámci projektu INNOSOC definovaný s ohľadom na štandardy ako NIST 800-61, ISO/IEC 27035 a odporúčania z aktuálnych rámcov MITRE ATT&CK, čo umožňuje vysokú interoperabilitu so štátnymi, komerčnými aj akademickými SOC iniciatívami.

Procesy v SOC centre predstavujú základný pilier jeho efektívneho fungovania. Každý komponent navrhnutý v architektúre SOCaaS INNOSOC je spojený s konkrétnymi procesmi, ktoré zabezpečujú ucelené zvládanie kybernetických hrozieb v celom ich životnom cykle – od detekcie, cez reakciu až po vyhodnotenie a zlepšenie bezpečnostných politík.

3.2.1. Detekcia a monitorovanie (SIEM – ELK Stack)

Procesy detekcie sú realizované prostredníctvom platformy ELK Stack (Elasticsearch, Logstash, Kibana), ktorá tvorí základ monitorovacieho systému. Zahrňujú:

- Zber a centralizáciu logov zo systémov, sietí, koncových bodov a aplikácií.
- Normalizáciu a obohacovanie údajov pomocou Logstash a Beats.
- Ukladanie, indexovanie a uchovávanie údajov v Elasticsearch.
- Tvorbu korelačných pravidiel a alertov.
- Vizualizáciu výstupov v Kibane.
- Integráciu s ďalšími nástrojmi ako Wazuh (EDR), CTI systémy, incident manažment.

Tieto procesy tvoria základ pre identifikáciu incidentov v reálnom čase a umožňujú rýchlu reakciu.

3.2.2. Reakcia na incidenty (SOAR, Incident handling)

Reakčné procesy sú realizované prostredníctvom:

- **SOAR nástroja TheHive + Cortex**: slúži na automatizáciu reakčných scenárov, spracovanie alertov do prípadov a ich analýzu.
- **Ticketovací a incident manažment systém (TheHive, RTIR)**: poskytuje workflow pre riešenie incidentov, eskaláciu, audit a sledovanie riešenia.

- **Znalostný portál (Wiki.js, BookStack)**: podporuje reakčné procesy zdieľaním playbookov, interných politík a návodov.

Tieto nástroje podporujú tím analytikov pri efektívnom riešení incidentov, evidencii observables, dokumentovaní reakcií a spätnej analýze.

3.2.3. Inventarizácia a správa aktív

Správa IT aktív je kľúčová pre mapovanie dopadov hrozieb. Využívame kombináciu:

- **NetBox**, **GLPI**, **Ralph**: na udržiavanie CMDB databázy, prepojenie aktív na lokality, služby, vlastníkov a SLA.

Tieto nástroje zabezpečujú podporu procesov asset discovery, životného cyklu aktív, integráciu so SIEM a incident manažmentom.

3.2.4. Threat Intelligence (CTI)

Procesy CTI (Cyber Threat Intelligence) umožňujú obohacovanie incidentov o známe hrozby, TTPs a IOCs:

- Využívame nástroje ako **OpenCTI**, **MISP**, **IntelMQ** na zber, klasifikáciu a distribúciu threat intel údajov.

Tieto procesy poskytujú analytikom aktuálne informácie o hrozbách a podporujú proaktívny threat hunting.

3.2.5. Správa zraniteľností

Zraniteľnosti identifikované v prostredí sú spracované cez:

- **Greenbone Community Edition (GVM)** ako nástroj pre aktívne skenovanie.

Výsledky sú prepájané s aktívami a posielané do SIEM/incident systému pre ďalšie spracovanie.

3.2.6. Reporting a spätná analýza

- Využitie **Kibana** pre tvorbu pravidelných reportov, ad-hoc prehľadov a auditných výstupov.

Exporty a plánovanie reportingov pokrývajú potreby interného hodnotenia SOC a komunikácie so zákazníkmi.

3.2.7. Súhrn

Procesný model SOCaaS INNOSOC reflektuje osvedčené praktiky, pričom kladie dôraz na:

- Automatizáciu a orchestráciu.
- Prepojenosť nástrojov.
- Transparentnosť riešenia incidentov.
- Dokumentáciu a vedomostnú bázu.
- Efektívnu detekciu, vyhodnotenie a reakciu.

Prepojenie vyššie uvedených procesov zabezpečuje robustné a škálovateľné prostredie pre kybernetickú bezpečnosť viacerých zákazníkov.

3.3. Prevádzkové scenáre a praktické nasadenie

Prevádzkové scenáre popisujú praktické aspekty každodenného fungovania SOCaaS, pričom sa opierajú o predpokladané reálne situácie, s ktorými sa môže tím SOC stretnúť. Ich účelom je zabezpečiť prevádzkyschopnosť služby, efektívnu spoluprácu tímov a optimalizovanú reakciu na hrozby.

1. Onboarding nového zákazníka

Pri onboardingu nového zákazníka prebieha integrácia jeho infraštruktúry do multitenantného prostredia SOCaaS. To zahŕňa:

- nastavenie logovacieho agenta (napr. Filebeat, Winlogbeat),
- konfiguráciu korelačných pravidiel v ELK podľa typov zariadení,
- vytvorenie separovaných dashboardov v Kibane,
- nastavenie incident managementu pre zákazníka v TheHive a Zammad.

2. Detekcia a eskalácia incidentu

V prostredí ELK sú nakonfigurované pravidlá na detekciu anomálií a známych hrozieb. Po detekcii:

- sa generuje alert (napr. cez Wazuh alebo ElastAlert),
- alert sa automaticky transformuje na incident v TheHive,
- Zammad zabezpečuje ticket pre L1 tím a podporu eskalácie,
- tím vyhodnotí observables a využije obohatenie cez OpenCTI alebo MISP.

3. Správa zraniteľností a inventarizácia

Pravidelné skeny prostredníctvom Greenbone (OpenVAS) sú prepojené s CMDB v NetBox alebo Ralph.

- Assety sú aktualizované na základe detekcie z LibreNMS a pi.Alert,
- incidenty viazané na zraniteľnosti sú prepájané do manažment systému (napr. TheHive).

4. Proaktívne vyhľadávanie hrozieb (Threat Hunting)

Používajú sa pokročilé dotazy v Kibane (KQL, Lucene), často doplnené o:

- CTI dáta z OpenCTI alebo YETI,
- manuálnu analýzu v prípade podozrivých entít,
- výsledky sú dokumentované ako playbooky v BookStack alebo Wiki.js.

5. Tvorba reportov a dashboardov

Pre manažment a zákazníkov sú pravidelne generované:

- prehľady incidentov v Kibane (Elastic Reports),
- vizualizácie z metrík a ticketingu (prepojenie s Grafanou),
- exporty pre audit a SLA reporting.

6. Tvorba znalostnej bázy

Každý incident alebo nový typ hrozby sa dokumentuje formou:

- incident summary + lessons learned (TheHive),
- zápis v znalostnom portáli (Wiki.js alebo BookStack),
- kategorizácia podľa MITRE ATT&CK a dátumov.

7. Údržba a aktualizácia systému

Prevádzkový tím má stanovené:

- pravidlá pre aktualizácie komponentov (Wazuh, ELK, TheHive),
- testovacie prostredie na overenie zmien,
- centralizovaný monitoring funkčnosti všetkých modulov.

Tieto scenáre zabezpečujú praktickú prevádzku SOCaaS ako služby, pričom každý z komponentov zohráva jasne definovanú úlohu v architektúre. Dokumentácia incidentov a výsledkov analýz zároveň prispieva k neustálemu zlepšovaniu detekcie a reakcie.

4. MONITOROVACÍ A ANALYTICKÝ SYSTÉM (SIEM – ELK STACK)

4.1. Architektúra a komponenty ELK

Architektúra systému ELK (Elasticsearch, Logstash, Kibana) predstavuje jadro monitorovacieho a analytického systému navrhnutého v rámci SOCaaS INNOSOC. Tento systém zabezpečuje centralizovaný zber, spracovanie, analýzu a vizualizáciu bezpečnostných udalostí v reálnom čase.

Komponenty systému ELK:

- **Elasticsearch** – distribuovaný vyhľadávací a analytický engine, ktorý uchováva a indexuje všetky prijaté logy a dáta. Umožňuje rýchle a komplexné dotazy nad uloženými údajmi a je navrhnutý pre horizontálnu škálovateľnosť.
- **Logstash** – zodpovedá za ingestiu dát, ich parsovanie a normalizáciu. Podporuje široké spektrum vstupov (napr. syslog, beats, REST API), množstvo filter pluginov (grok, mutate, geoip) a výstup do Elasticsearch.
- **Kibana** – vizualizačný nástroj, ktorý poskytuje intuitívne rozhranie pre tvorbu dashboardov, prehliadanie logov a výstupy korelačných pravidiel. Slúži ako hlavné rozhranie pre analytikov a operátorov SOC.
- **Beats** – ľahké agenty (napr. Filebeat, Metricbeat), ktoré sa inštalujú na koncové body a odosielajú logy a metriky do Logstash alebo Elasticsearch.
- **Fleet & Elastic Agent** – centrálne riadený systém pre správu agentov, ktorý umožňuje jednoducho nasadzovať a konfigurovať Elastic Agent na koncových zariadeniach. Elastic Agent poskytuje jednotný spôsob zberu dát, EDR schopnosti a integrácie so SIEM modulmi.

Pre SOCaaS nasadenie bol ELK systém navrhnutý ako multitenantné, škálovateľné riešenie, ktoré môže obsluhovať viacero zákazníkov s oddelenými dátovými tokmi, dashboardmi a analytikou. Elasticsearch umožňuje použitie tzv. index patterns alebo namespaces pre oddelenie tenantov, pričom Kibana zabezpečuje prístup na základe RBAC (Role-Based Access Control).

Dôležitou vlastnosťou architektúry je vysoká dostupnosť – jednotlivé komponenty (Elasticsearch nody, Logstash pipeline, Kibana inštancie) sú nasadzované v redundantnom režime a monitorované cez systém Watcher a Alerting mechanizmy.

Okrem základných komponentov sa využívajú aj doplnkové moduly ako Elastic Security (bývalý SIEM modul), ktorý poskytuje pokročilé možnosti správy detekcií, pravidiel a detekčných alertov s podporou MITRE ATT&CK frameworku.

4.2. Spracovanie dátových tokov

V rámci architektúry ELK Stack v prostredí SOCaaS systému zohráva spracovanie dátových tokov kľúčovú úlohu pri konsolidácii a štandardizácii údajov pochádzajúcich z rôznych zdrojov. Tieto toky môžu zahŕňať logy z koncových zariadení, sieťových prvkov, bezpečnostných nástrojov (napr. EDR, CTI, SOAR), ako aj metadáta z cloudových alebo hybridných prostredí.

Hlavné úlohy spracovania dátových tokov v ELK Stack sú:

- Príjem logov a udalostí z viacerých heterogénnych zdrojov
- Validácia, normalizácia a obohatenie dát
- Priradenie časových pečiatok, identifikátorov a kategórií udalostí
- Presmerovanie dát do vhodných indexov pre efektívnu analýzu
- Odfiltrovanie redundatných alebo irelevantných údajov
- Implementácia pipeline pravidiel a spracovateľských modulov (Logstash, Ingest pipelines v Elasticsearch)

V prostredí INNOSOC sú na spracovanie dát využívané nasledovné komponenty:

- Filebeat: ľahký agent nasadený na koncových zariadeniach, ktorý zberá a forwarduje logy.
- Logstash: centrálna jednotka pre spracovanie dát, umožňuje pokročilú transformáciu údajov.
- Elasticsearch Ingest pipelines: ľahšie pravidlá spracovania integrované priamo v databázovom jadre.
- Wazuh Manager: v prípade XDR spracúva bezpečnostné udalosti (alerts) a zabezpečuje ich štruktúrovanie.
- Integrácie s MISP a TheHive: poskytujú CTI obohatenie o observables, kontextové dáta a hodnotenie reputácie.

Zabezpečenie integrity a dostupnosti dát je dosiahnuté pomocou TLS šifrovania medzi komponentmi a centrálnej správy konfigurácie pipeline modulov. V prostredí viaczákaznícke SOCaaS riešenia sa dáta rozdeľujú na základe namespace (index prefixy) alebo cez logické oddelenie pomocou tagovania pri ingest procese.

4.3. Korelačné pravidlá a detekcia hrozieb

Efektívna detekcia hrozieb v rámci bezpečnostného monitoringu SOCaaS INNOSOC je postavená na využití korelačných pravidiel a analytických techník, ktoré umožňujú odhaliť anomálie, indikátory kompromitácie (IOC) a iné správanie, ktoré poukazuje na potenciálne bezpečnostné incidenty. Vzhľadom na použitie platformy ELK Stack je táto detekcia realizovaná prostredníctvom viacerých vrstiev logickej analýzy a pravidiel, ktoré sa aplikujú na prijaté a spracované logy.

Typy detekčných techník

Detekcia hrozieb je v prostredí INNOSOC založená na kombinácii nasledovných prístupov:

- **Statická detekcia pomocou signatúr** – využíva presne definované patterny (napr. hash hodnoty, domény, názvy procesov), ktoré sú porovnávané s CTI údajmi získanými z MISP alebo OpenCTI. Tieto signatúry sa automaticky načítavajú do Elastic Security prostredníctvom integrácií.
- **Korelačné pravidlá (rule-based detection)** – definované prostredníctvom KQL (Kibana Query Language), Lucene alebo pomocou Elastic Detection Rules. Umožňujú kombinovať viacero podmienok (napr. kombinácia IP adresy, časového okna a typu akcie) do komplexných detekčných scenárov.

- **Anomálna detekcia** – založená na Machine Learning moduloch dostupných v platených verziách Elastic Stack, ktoré analyzujú odchýlky od bežného správania (napr. počet prihlasovaní mimo pracovného času, neštandardný objem prenosov). V open-source prostredí sú tieto prístupy do istej miery simulované cez metriky a threshold alerty.
- **Behaviorálna detekcia a MITRE ATT&CK mapping** – pravidlá sú vytvárané na základe TTPs známych z databázy MITRE ATT&CK, čo umožňuje systematickú detekciu podľa fáz útočného životného cyklu. Napríklad pravidlo sledujúce „Persistence via Scheduled Task“ kontroluje, či bol vytvorený nový schtasks.exe s neznámym parametrom.

Implementácia detekčných pravidiel

V prostredí INNOSOC sú korelačné pravidlá navrhované podľa viacerých scenárov:

- **Alerty na základné IOC** – porovnanie s databázou známych indikátorov (IP, URL, hash).
- **Anomálne správanie používateľov** – napr. viacnásobné neúspešné prihlásenie v krátkom čase, login z nového geografického regiónu.
- **Neštandardné sieťové komunikácie** – napr. DNS dotazy na dynamicky generované domény (DGA), odchýlky v čase a objeme dát.
- **Aktivity s administratívnymi právami** – napr. pridanie používateľa do skupiny „Administrators“, zmeny ACL, spustenie netsh, powershell.
- **Reťazenie udalostí** – korelácia medzi viacerými logmi v čase: napr. login → súborový prenos → spustenie škodlivého procesu.

Tieto pravidlá sú spravované cez modul **Elastic Security Detection Engine**, kde možno:

- sledovať detekčné alerty,
- nastavovať prahové hodnoty (thresholds),
- konfigurovať výnimky a ignorované hodnoty (exceptions),
- exportovať a importovať pravidlá ako JSON objekty.

Automatizácia detekcie a reakcie

Detekčné pravidlá sú napojené na systém reakcie prostredníctvom:

- **Elastic Actions & Connectors** – automatické odosielanie alertov do SOAR nástrojov (TheHive), emailových notifikácií alebo webhookov.
- **Integrácia s Wazuh** – umožňuje generovať alerty na strane koncových zariadení a prenášať ich do Elastic prostredia, kde sú ďalej spracované a vizualizované.
- **Integrácia s Cortex analyzátormi** – umožňuje spúšťať automatické enrichment úlohy pre observables.

Príklady z praxe (z laboratórneho prostredia INNOSOC)

Počas testovania boli vytvorené desiatky detekčných pravidiel, napríklad:

- Pravidlo identifikujúce pokus o laterálne šírenie cez PsExec na viaceré zariadenia v krátkom čase.
- Korelácia medzi DNS dotazmi na podozrivé TLD (napr. .xyz, .top) a následné pripojenie na ne overené IP adresy.
- Vytvorenie „honeypot“ dashboardu s alertmi na neautorizované prístupy na špeciálne pripravené služby.

Výzvy a odporúčania

- Korelačné pravidlá musia byť pravidelne aktualizované podľa aktuálnych trendov hrozieb.
- V prostredí multitenantného SIEM je potrebné zabezpečiť oddelenie pravidiel podľa zákazníkov, čo si vyžaduje prácu s tags, namespaces a samostatnými pipelines.
- Prevádzka detekčných pravidiel s vysokou presnosťou je závislá od kvality vstupných dát a správneho normalizačného procesu (Logstash, Beats).

4.4. Integrácia s ostatnými komponentmi

Efektívne fungovanie SOCaaS riešenia závisí od schopnosti jednotlivých komponentov navzájom spolupracovať. SIEM systém ako centrálne analytické jadro (v našom prípade ELK stack) musí byť prepojený s ostatnými nástrojmi na zber dát, incident management, threat intelligence aj reporting, aby sa vytvoril jednotný ekosystém pre detekciu a reakciu na hrozby.

Prepojenie so zdrojmi dát

SIEM získava dáta z rôznych komponentov infraštruktúry prostredníctvom agentov a integrácií, ktoré zabezpečujú jednotné formátovanie a transport údajov. V našej architektúre sa používajú najmä:

- **Wazuh** ako XDR agent zabezpečuje zber logov z koncových staníc, serverov a zariadení, a tieto dáta odosiela do Logstasha.
- **Logstash a Beats** ako transportná vrstva vykonávajú predspracovanie a normalizáciu údajov pred ich uložením do Elasticsearch.
- **Asset Management systém (napr. NetBox alebo Ralph)** poskytuje kontextové informácie o infraštruktúre a identifikovaných zariadeniach. Tieto údaje môžu byť integrované cez API alebo synchronizované v rámci enrichingu alertov.
- **Vulnerability Scanner (napr. Greenbone)** zdieľa výsledky skenov a identifikované zraniteľnosti, ktoré sa importujú ako záznamy do SIEM a slúžia na tvorbu korelačných pravidiel.
- **CTI platformy (napr. MISP, OpenCTI)** poskytujú externé IOCs a TTPs, ktoré sa používajú v korelačných pravidlách a enrichmente alertov.

Integrácia s nástrojmi incident managementu a SOAR

Zistené alerty z Elasticsearch sa spravidla automaticky alebo poloautomaticky transformujú na incidenty prostredníctvom integrácie so systémami typu:

- **TheHive** – ako hlavný incident manažment systém prijíma alerty cez webhooky alebo prostredníctvom konektorov (napr. ElastAlert → TheHive Connector). Prípad obsahuje observables (napr. IP, domény, hashe) a umožňuje ich manuálne aj automatické obohacovanie.
- **Cortex** – slúži ako SOAR komponenta pre automatizáciu reakcií. Po príchode incidentu do TheHive je možné automaticky spustiť akcie ako WHOIS dotaz, VirusTotal scan alebo izoláciu zariadenia.
- **Zammad alebo RTIR** – ak je potrebná pokročilejšia ticketová evidencia, alerty môžu byť konvertované aj do ticketov v týchto systémoch, pričom sa zachová väzba na analytické dáta z Kibany.
- **Spolupráca s reportingom a dashboardmi**
- **Kibana** poskytuje rozhranie pre sledovanie alertov, analýzu udalostí, tvorbu dashboardov a reporting. Užívatelia si môžu interaktívne filtrovať údaje podľa rôznych kritérií (čas, typ incidentu, zdroj, IP adresa).
- Pre reporting slúžia plánované exporty (PDF/CSV) a dashboard snapshoty, ktoré môžu byť preposielané e-mailom alebo zverejňované na interných portáloch.
- Výsledky z incident manažmentu a enrichment z CTI sú často vizualizované práve cez Kibanu – napr. ako časové osi incidentov, mapa geografického pôvodu IP, alebo top hrozby za posledný mesiac.

Znalostná databáza a playbooky

- Vzniknuté incidenty, alerty a ich riešenia sú dokumentované a archivované v **knowledge portáli** (napr. BookStack, Wiki.js), čím sa zabezpečuje spätná dohľadateľnosť a tvorba tzv. SOC playbookov.
- Prepojenie medzi SIEM alertom → incident manažment → znalostná databáza vytvára konzistentný tok informácií, čím sa skracuje čas reakcie a znižuje zaťaženie analytikov.

5. TVORBA DASHBOARDOV V KIBANE

5.1. Princípy návrhu dashboardov

Dashboardy predstavujú kľúčový nástroj pre rýchlu orientáciu analytikov v dátach o bezpečnostnej situácii. V prostredí SOCaaS plnia úlohu vizuálnej vrstvy nad SIEM systémom, ktorá umožňuje sledovanie trendov, alertov, aktivity útočníkov a výkonu bezpečnostných komponentov v reálnom čase. V našom návrhu sú dashboardy realizované v prostredí **Kibana**, ktoré je natívnou súčasťou ELK Stacku.

Ciele a filozofia návrhu

Pri návrhu dashboardov v rámci SOCaaS sme vychádzali z nasledujúcich zásad:

- **Zrozumiteľnosť a účelovosť** – každý dashboard je navrhnutý pre konkrétny účel (napr. monitoring alertov, prehľad zraniteľností, detekcia anomálií) a prispôsobený cieľovej roli (L1 analytik, SOC manažér, auditor).
- **Minimalizmus a prehľadnosť** – zobrazujeme len relevantné metriky a indikátory, pričom sa vyhýbame vizuálnemu preťaženiu. Každý panel má presne definovanú funkciu.
- **Interaktivita a drill-down** – umožňujeme klikateľné prechody medzi agregovaným prehľadom a detailnými udalosťami. Užívatelia môžu filtrovať podľa času, zdroja, IP adresy alebo typu incidentu.
- **Real-time aktualizácia** – dashboardy zobrazujú aktuálne dáta s možnosťou živého obnovovania (napr. každých 15 sekúnd), čo je dôležité pri aktívnych incidentoch.
- **Unifikácia dát z viacerých zdrojov** – cez Beats a Logstash získavame údaje z rôznych komponentov (EDR, sieťové zariadenia, systémy pre správu aktív) a zobrazujeme ich v jednotnej vizualizačnej vrstve.
- **Možnosť exportu a zdieľania** – dashboardy sú navrhnuté tak, aby ich bolo možné exportovať do PDF, PNG alebo zdieľať ako prepojenie, prípadne ich vložiť do reportovacích šablón.

Typológia a hierarchia dashboardov

Pre udržanie prehľadnosti boli dashboardy v rámci SOCaaS rozdelené podľa funkčných vrstiev nasledovne:

1. **Globálne prehľady (SOC Overview)** Určené pre manažment a SLA reporting – zahŕňajú denné/měsíčné štatistiky incidentov, typy hrozieb, top 10 IP adries, krajiny pôvodu útokov, čas vyriešenia ticketov.
2. **Alert monitoring dashboardy** Zamerané na operatívny monitoring – zobrazujú nové alerty, rozdelenie podľa severity (Critical, High, Medium), časové trendy, a korelácie medzi viacerými zdrojmi.
3. **Tematické dashboardy** Pokrývajú špecifické oblasti:
   - **EDR aktivity**: zaznamenané súbory, procesy, pokusy o exekúciu škodlivého kódu.
   - **Zraniteľnosti a skeny**: výsledky z Greenbone alebo OpenSCAP.
   - **Firewall a sieťové logy**: prístupy, porty, odhalené scanningové aktivity.

4. **Detailné analytické dashboardy** – Slúžia pre L2 analytikov a threat hunting. Obsahujú heatmapy, časové rezy, distribúcie podľa hodín, krajín, ASN, výskyt IOC a podobne.
5. **Ad-hoc a incident-specific dashboardy** – Vznikajú počas vyšetrovania konkrétneho prípadu, kde si analytik zostaví vlastnú vizualizáciu na základe dát z Elasticsearch.

Šablóny a opakovane použiteľné panely

V rámci vývoja boli vytvorené aj **šablóny panelov** (tzv. reusable components), ktoré umožňujú:

- Opakované použitie bežných vizualizácií (napr. časová os, top zdroje, distribúcia IP).
- Tvorbu dashboardov na základe šablóny pre nový projekt alebo zákazníka.
- Jednotný vizuálny štýl pre celý SOCaaS.

5.2. Štruktúra typických dashboardov

V prostredí Kibana sú dashboardy zostavené z jednotlivých panelov, ktoré môžu obsahovať grafy, tabuľky, heatmapy, distribučné histogramy, metriky alebo mapy. Každý dashboard v rámci SOCaaS je navrhnutý ako kompozícia týchto vizualizácií zameraná na konkrétny aspekt monitorovania alebo analýzy.

Základná štruktúra dashboardov typicky vychádza z nasledovného rozdelenia do sekcií:

- Hlavný panel so súhrnnými metrikami: počet incidentov, stav systému, alerty podľa závažnosti.
- Časové trendy: histogramy zachytávajúce počet incidentov alebo alertov v čase.
- Rozdelenie podľa typu: typy útokov, kategórie hrozieb, detegované IOC (Indicators of Compromise).
- Interaktívne filtre: umožňujú výber podľa IP adresy, rozsahu času, zdrojového systému alebo geolokácie.
- Mapa sveta (ak je aktivované geo-IP): zobrazenie geografického rozloženia útokov.
- Panely s drill-down možnosťou: napr. kliknutie na IP otvorí zoznam udalostí alebo alertov súvisiacich s daným zdrojom.

5.3. Ukážky dashboardov a vizualizácií

Efektívna vizualizácia dát v prostredí SOC je kľúčová pre rýchlu identifikáciu incidentov, detekciu trendov a rozhodovanie analytikov. V rámci riešenia SOCaaS INNOSOC boli navrhnuté a implementované viaceré typy dashboardov, ktoré pokrývajú rôzne aspekty monitorovania a incident manažmentu. Tieto dashboardy boli vyvíjané v nástroji **Kibana**, ktorý tvorí súčasť zvoleného SIEM riešenia na báze **Elastic Stack (ELK)**.

5.3.1. Prehľad systémovej bezpečnosti

Prvotný pohľad na celkový stav bezpečnosti systému poskytuje tzv. overview dashboard, ktorý sumarizuje hlavné metriky:

- Počet prijatých logov v čase (log rate)
- Počet aktívnych alertov (detekcií)
- Stav agentov Wazuh/Elastic Agentov
- Počet detegovaných IOC v čase

5.3.2. Korelačné a incidentové dashboardy

Korelačné pravidlá detegujú hrozby na základe logiky, ktorá prepája udalosti z viacerých zdrojov. Výsledkom sú incidentové alerty, ktoré sa zobrazujú v real-time. Dashboardy zobrazujú:

- Časové rozdelenie detekovaných alertov podľa typu
- Kritickosť a klasifikácia incidentov
- Geolokačné rozloženie IP adries útočníkov
- Trendy najčastejších útokov (napr. brute-force, port scan)

5.3.3. Vizualizácia sieťovej prevádzky a prístupov

Prehľad o činnosti používateľov, koncových bodov a sieťovej aktivity je kľúčový. Príslušné dashboardy zahŕňajú:

- Najčastejšie cieľové porty a zdrojové IP adresy
- Anomálne požiadavky (napr. HTTP/HTTPS, DNS)
- Využitie zdrojov podľa služieb a aplikácií
- Prístupy k chráneným segmentom

5.3.4. Monitorovanie autentifikácií a správania používateľov

Identifikácia podozrivého správania (napr. login z neobvyklého geografického miesta, opakované neúspešné prihlásenia) prebieha cez:

- Failed/success login attempts
- Anomálie vo frekvencii prihlásení
- Využitie kont podľa rolí a systémov
- Detekcia neautorizovaných aktivít

5.3.5. Integrovaný prehľad pre SOC analytika

Finálny typ dashboardu kombinuje metriky z viacerých oblastí do jedného interaktívneho rozhrania pre každodennú prácu analytika:

- Widgety na vyhľadávanie podľa IP/hash/domeny
- Rýchle filtre na čas, kritickosť, typ incidentu
- Agregované sumáre (incidenty za 24h, top útočníci)
- Preklik na detailné logy alebo prípady v ticketing systéme

6. REPORTING A EXPORT DÁT

Efektívny reporting predstavuje jeden z kľúčových aspektov prevádzky bezpečnostného operačného centra (SOC). Umožňuje nielen spätnú analýzu incidentov a trendov, ale aj transparentnú komunikáciu voči zainteresovaným stranám (interný manažment, zákazníci, audit, dohľadové orgány).

V rámci SOCaaS INNOSOC je reporting implementovaný prostredníctvom **Elastic Stack**, predovšetkým pomocou nástroja **Kibana**, ktorý umožňuje tvorbu, správu a distribúciu prehľadov v rôznych formátoch a úrovniach detailu.

6.1. Ciele a typy reportingu

Reporting v SOCaaS plní niekoľko základných cieľov:

- **Prevádzkový prehľad** – zobrazenie stavu systémov, počtu incidentov, aktivity agentov.
- **Bezpečnostný reporting** – výstupy o detekovaných hrozbách, typoch útokov, trendoch.
- **Compliance reporting** – reporty podľa regulatórnych požiadaviek (napr. GDPR, NIS2).
- **Manažérsky reporting** – agregované štatistiky a ukazovatele pre vedenie organizácie.
- **Zákaznícky reporting** – individuálne prehľady pre jednotlivých klientov multitenantného SOCaaS.

6.2. Možnosti reportingu v Kibane

Kibana poskytuje viacero možností pre tvorbu a distribúciu reportov.

6.2.1. Manuálny export reportov

Každý dashboard v Kibane je možné exportovať ako:

- **PDF dokument** – generovaný snapshot aktuálneho dashboardu.
- **PNG obraz** – statické obrázky jednotlivých vizualizácií.
- **CSV súbory** – surové dáta z tabuliek a dátových polí.
- **JSON** – pre automatizovanú analýzu a ďalšie spracovanie.

Tieto možnosti umožňujú flexibilné použitie výstupov pre rôzne účely – od príloh v správach, cez technickú dokumentáciu až po vstup pre ďalšie analytické nástroje.

6.2.2. Automatizovaný reporting

Kibana (v spojení s Elastic X-Pack alebo open-source rozšíreniami) podporuje plánovanie a automatizované zasielanie reportov:

- **Periodické reporty** – denne, týždenne alebo mesačne generované a distribuované výstupy.
- **Distribúcia cez e-mail alebo webhook** – reporty môžu byť automaticky odoslané na určené adresy alebo endpointy.
- **Podpora pre templaty a vlastné filtre** – možnosť nastaviť podmienky, výbery časových období a formáty podľa potrieb.

6.2.3. Customizácia výstupov

- **Možnosť výberu metrík, polí, časových rozsahov**
- **Personalizácia dizajnu – logá, záhlavie, farebná schéma**
- **Zaradenie vysvetliviek, poznámok a kontextuálneho komentára**

Kibana umožňuje každému analytikovi pripraviť si reporting presne na mieru – podľa cieľovej skupiny (SOC operátor, manažér, zákazník) a typu informácií.

6.3. Integrácia reportingového systému

Reporting v rámci SOCaaS nie je izolovaný komponent – je prepojený s ďalšími súčasťami architektúry:

- **SIEM (ELK)** – poskytuje primárne dáta, alerty, korelácie.
- **SOAR a Ticketing** – umožňujú zahrnúť štatistiky o incidentoch, čase riešenia, reakciách.
- **EDR/XDR (Wazuh)** – poskytuje koncové dáta a udalosti zo zariadení.
- **CTI a Threat Feed integrácie** – obohacovanie o externé hrozby.
- **CMDB / Asset Management** – rozšírenie kontextu o súvislosti s konkrétnymi aktívami.

6.4. Výzvy a odporúčania

Pri návrhu a prevádzke reportingu je dôležité:

- Definovať **cieľové skupiny a ich potreby** – technický vs. netechnický reporting.
- Zabezpečiť **automatizáciu a pravidelnosť** – manuálny reporting je neudržateľný.
- Vytvárať **interaktívne dashboardy** ako podklad pre živé prezentácie.
- Zabezpečiť **auditovateľnosť a integritu dát** – dôležité pre súlad s reguláciami.
- Rozlišovať medzi **interným a externým reportingom** – obsah, detailnosť, forma.

7. ZÁVER A ODPORÚČANIA

Návrh bezpečnostného operačného centra ako služby (SOCaaS) v projekte INNOSOC vychádza z dôkladnej analýzy komponentov, procesov a nástrojov, ktoré sú nevyhnutné na efektívnu prevádzku multitenantného bezpečnostného dohľadu. Získané poznatky z laboratórnych overení, testovacích nasadení a syntézy vedeckých poznatkov boli transformované do návrhu komplexného riešenia, ktoré rešpektuje požiadavky na otvorenosť, flexibilitu a modularitu.

7.1. Prínosy navrhnutej architektúry

- **Modularita**: Architektúra umožňuje nezávislé nasadzovanie a výmenu komponentov bez narušenia celkového toku.
- **Open-source technológie**: Výber nástrojov, ako sú ELK, Wazuh, TheHive, MISP, Kibana, Grafana a ďalšie, umožňuje znížiť náklady a zároveň zachovať vysokú mieru konfigurovateľnosti.
- **Integrácia**: Kľúčové komponenty (SIEM, SOAR, CTI, EDR, Asset Management) sú navzájom prepojené prostredníctvom API a integračných mechanizmov, čo umožňuje plynulý tok dát.
- **Adaptabilita pre multitenantné prostredie**: Architektúra je navrhnutá tak, aby podporovala správu viacerých zákazníkov s rôznymi úrovňami služieb.
- **Škálovateľnosť**: Všetky zvolené nástroje umožňujú horizontálne škálovanie, čo podporuje rast a rozširovanie služby bez potreby zásadných architektonických zmien.

7.2. Dôvody výberu ELK Stack ako jadra SIEM

- **Elastic Stack (ELK)** bol vybraný ako jadro SIEM riešenia pre jeho schopnosť spracúvať veľké objemy dát v reálnom čase, rozsiahlu komunitnú podporu, dostupnosť doplnkových nástrojov a výbornú vizualizačnú nadstavbu (Kibana).
- Výhodou ELK je tiež prirodzená integrácia s Wazuh (EDR), TheHive (Incident Management) a CTI nástrojmi (napr. MISP), čo vytvára jednotné dátové prostredie pre analytiku a reakciu.

7.3. Riešenie dashboardov a reportovania

- Nástroj **Kibana** bol použitý nielen na vizualizáciu dát, ale aj na implementáciu základného reportingu a prezentácie incidentov, stavov infraštruktúry, výstrah a metriky výkonu.
- Dashboards boli navrhnuté podľa rolí v SOC: L1 analytik, L2 analytik, vedúci operátor, zákaznícky pohľad, technická podpora.
- Reporting bol implementovaný s možnosťou exportov (PDF, CSV, JSON), ako aj plánovaného automatického zasielania pomocou rozšírení Elastic Stack.

7.4. Výzvy a odporúčania pre ďalší rozvoj

- **Zavedenie CI/CD pre bezpečnostné pravidlá**: Odporúča sa zaviesť proces kontinuálnej integrácie a verifikácie korelačných pravidiel a detekcií.
- **Zvýšiť automatizáciu reakcií (SOAR)**: Prehĺbiť využitie TheHive + Cortex a pripojenie playbookov v StackStorm alebo Shuffle.
- **Zefektívniť správu znalostí**: Plne integrovať Wiki.js alebo Bookstack ako SOC knowledge base, previazaný s incidentmi a prípadmi.
- **Rozšíriť reporting pre manažment a zákazníkov**: Pripraviť preddefinované reporty zamerané na SLA, trvanie reakcií a kategorizáciu incidentov.

ZDROJE

Primárne dokumentácie nástrojov a platforiem

1. Elastic Stack Documentation. Elastic.co. https://www.elastic.co/guide/
2. Wazuh Documentation. Wazuh Inc. https://documentation.wazuh.com/
3. OpenCTI Documentation. https://www.opencti.io/en/docs/
4. MISP Project Documentation. https://www.misp-project.org/documentation/
5. IntelMQ Project. CERT.at. https://github.com/certtools/intelmq
6. TheHive Project Documentation. https://docs.thehive-project.org/
7. Cortex Analyzers. https://github.com/TheHive-Project/Cortex-Analyzers
8. NetBox Documentation. NetBox Labs. https://docs.netbox.dev/
9. LibreNMS Documentation. https://docs.librenms.org/
10. GLPI Documentation. https://glpi-project.org/
11. Greenbone Community Edition (GCE). https://docs.greenbone.net/
12. OpenSCAP Official Site. Red Hat Security. https://www.open-scap.org/
13. BookStack Documentation. https://www.bookstackapp.com/docs/
14. Wiki.js Documentation. https://docs.requarks.io/

Doplňujúce odborné a akademické zdroje

15. Bhat, M. A., & Kumar, P. (2022). *Advanced SIEM for Enhanced Threat Detection Using Machine Learning*. In 2022 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE. https://doi.org/10.1109/CSR54599.2022.9850371
16. Nguyen, K., et al. (2021). *A Review of Security Information and Event Management (SIEM) Systems*. Future Internet, 13(8), 204. https://doi.org/10.3390/fi13080204
17. Munoz, M., Garcia, C., & Valdes, J. J. (2023). *ML-based Optimization for SOC Event Triage*. Proceedings of the 2023 ACM Workshop on AI in Cybersecurity. https://doi.org/10.1145/3576888.3602857
18. Akinrolabu, O. A., et al. (2020). *Security Operations Centre: A systematic study and open challenges*. Computers & Security, Volume 92, 101747. https://doi.org/10.1016/j.cose.2020.101747
19. Al-Shaer, E., et al. (2021). *Autonomic Security Operations: Challenges and Research Opportunities*. In IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2021.3127814
20. Kertesz, A., & Kiss, B. (2025). *Cloud-native Architectures for SOC-as-a-Service Platforms*. Journal of Cloud Computing, 14(2), 117–139.
21. Papadopoulos, K., & Vlachos, I. (2025). *A Federated Model for Sharing Threat Intelligence Across SOCs*. Journal of Cybersecurity and Privacy, 5(1), 54–79.
22. Zhang, Y., et al. (2025). *Visualization and Reporting Techniques in Elastic SIEM Environments*. Proceedings of the 2025 International Conference on Networked Systems. [DOI pending]

PRÍLOHY

Táto kapitola zhromažďuje doplnkové materiály a ilustrácie, ktoré dopĺňajú hlavné časti dokumentu a poskytujú prehľad o praktických aspektoch návrhu, testovania a overovania jednotlivých komponentov systému SOCaaS INNOSOC. Obsahuje vizualizácie, schémy, snímky z dashboardov, ukážky konfigurácií a ďalšie podporné výstupy z laboratórneho nasadenia a výskumnej činnosti riešiteľského tímu projektu INNOSOC.

Tieto prílohy slúžia ako podporná dokumentácia ku všetkým hlavným častiam dokumentu a demonštrujú pripravenosť komponentov na reálne nasadenie v prevádzke multitenantného SOCaaS prostredia v rámci projektu INNOSOC. Zároveň potvrdzujú, že výber technológií a návrh integračnej architektúry boli overené nielen teoreticky, ale aj prakticky počas iteratívneho testovania riešení v kontrolovanom prostredí.

Zoznam:

1. podklad pre V6 v rámci KPB2_Koncept SOC centra.docx
2. podklad pre V6 v rámci KPB2_Dashboardy - vizualizácia dát z nástrojov.docx
3. podklad pre V6 v rámci KPB2_Dashboardy - ukážka tvorby vizualizácií v Kibane.docx
4. podklad pre V6 v rámci KPB2_Dashboardy - analýza bezpečnostných udalostí.docx
5. podklad pre V6 v rámci KPB2_Dashborady - ukážka vizualizácií pre analýzu sieťových tokov.docx