PROJEKT

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

V4 výsledok analýzy vhodných komponentov

KPB2 – Návrh SOCaaS služby

typ – dokumentácia

mesiac odovzdania – M3

Obsah

1. ÚVOD K NÁVRHU SOC AS A SERVICE

Návrh riešenia SOC ako služby (SOCaaS) v rámci projektu INNOSOC sa zameriava na vytvorenie elastickej, viaczákazníckej a modulárnej služby zabezpečujúcej pokročilý monitoring, detekciu a reakciu na kybernetické incidenty. V súlade so špecifickým cieľom č. 3 projektu je cieľom tohto dokumentu identifikovať a odporučiť technologické komponenty, ktoré budú tvoriť jadro navrhovaného SOCaaS riešenia.

Pri identifikácii jednotlivých modulov sa vychádzalo z:

- Procesného modelu SOC centra,
- Potrieb reálneho nasadenia pre viacerých zákazníkov s rôznou úrovňou zabezpečenia,
- Open-source a bezplatných riešení (z dôvodov škálovateľnosti a dostupnosti),
- Skúseností z testovania, laboratórnych nasadení a predchádzajúceho výskumu riešiteľského kolektívu.

2. KOMPONENTY SOCAAS A ICH ÚZKA PREPOJENOSŤ

Moderný SOCaaS predstavuje prepojený ekosystém bezpečnostných technológií, ktoré musia spoločne zabezpečovať nielen detekciu a reakciu na incidenty, ale aj prevádzkovú stabilitu, transparentnosť procesov a dlhodobú auditovateľnosť. V návrhu architektúry riešenia SOCaaS v projekte INNOSOC sme sa zamerali na výber takých komponentov, ktoré sú flexibilné, škálovateľné, podporované komunitou, a zároveň dostatočne zrelé pre prevádzku v multitenantnom režime.

Komponenty boli rozdelené do troch hlavných oblastí, ktoré korešpondujú s fázami bezpečnostného cyklu – monitorovanie, reakcia a evidencia.

2.1 Detekcia, monitoring a analytické spracovanie

Táto vrstva zabezpečuje základnú funkciu každého SOC – zber, spracovanie a vyhodnocovanie bezpečnostných údajov. Obsahuje nasledovné komponenty:

- **SIEM (Security Information and Event Management):** centrálna analytická jednotka systému, zodpovedná za zber logov, koreláciu udalostí, detekciu anomálií, generovanie alertov a analytické dashboardy.
- **EDR/XDR (Endpoint/Extended Detection and Response):** detekcia hrozieb na úrovni koncových bodov, ich správanie, súbory, procesy, registrácia IOC, telemetria.
- **CTI (Cyber Threat Intelligence):** obohacovanie údajov prostredníctvom informácií o hrozbách (indikátory kompromitácie, TTP, profily útočníkov), zber z externých aj interných zdrojov, kategorizácia a normalizácia údajov.
- **Skener zraniteľností:** zisťovanie slabých miest v systémoch a aplikáciách, detekcia neaktualizovaného softvéru, zlých konfigurácií alebo exponovaných služieb.

Komponenty tejto vrstvy sú navzájom prepojené – výstupy z EDR sa korelujú v SIEM, CTI poskytuje kontext, ktorý zvyšuje kvalitu detekcie, a zraniteľnosti dopĺňajú hodnotenie rizika.

2.2 Manažovanie incidentov, reakcia a evidencia

Po detekcii bezpečnostnej udalosti je nevyhnutné ju zaradiť medzi incidenty, eskalovať, dokumentovať a uzavrieť. Táto vrstva zabezpečuje praktickú prevádzku a tímovú koordináciu. Obsahuje nasledovné komponenty:

- **Ticketovací systém:** nástroj na evidenciu všetkých bezpečnostných incidentov, zmenu ich stavu, prideľovanie analytikom, eskaláciu podľa úrovne závažnosti, SLA a plnú auditovateľnosť spracovania.
- **Evidencia a správa incidentov:** prípadové riadenie incidentov, správa observables (IP, hash, URL...), kategorizácia, šablóny incidentov, sledovanie metriky spracovania a prepojenie na ďalšie systémy (napr. SIEM, CTI).
- **SOAR (Security Orchestration, Automation and Response):** vykonávanie automatizovaných reakcií, orchestrácia viacerých komponentov pri spracovaní incidentu (napr. blokovanie IOC, generovanie tiketov, eskalácia alertov).
- **Reportovanie:** tvorba prehľadov a výkazov pre manažment, denné/mesačné súhrny incidentov, stav vyťaženosti SOC, zdieľanie výstupov so zákazníkmi a podpora pre ad-hoc analýzu údajov.
- **Znalostný portál pre SOC tím:** interná báza znalostí, playbooky, manuály, FAQ, návody na riešenie incidentov a procesné postupy, dostupné pre všetkých členov SOC podľa rolí a oprávnení.

Táto vrstva je rozhodujúca pre efektívne fungovanie celého SOCaaS. Incidenty sa riešia aj systematicky evidujú, analyzujú a spätne využívajú na zlepšovanie detekcie a reakcie.

2.3 Podporné komponenty a inventarizácia aktív

Bez jasného prehľadu o chránenom prostredí nie je možné zabezpečiť kvalitnú ochranu. Preto bola do návrhu zaradená aj podporná vrstva:

- **Inventarizácia aktív (Asset Management):** evidencia hardvérových, softvérových, virtuálnych aj cloudových aktív. Kategorizácia, vlastníctvo, bezpečnostný stav, lokalizácia (rack, VLAN, IP rozsah), prepojenia a väzby medzi komponentmi.
- **Integrácia s ostatnými systémami:** schopnosť párovať aktíva s detegovanými incidentmi, priame prepojenie so SIEM, EDR, ticketingom/skenerom zraniteľností.

Táto vrstva prispieva k rýchlej orientácii analytikov počas riešenia incidentu a pomáha zabezpečiť prioritizáciu a správne rozhodovanie na základe kontextu.

2.4 Prepojenosť komponentov a tok údajov

Jednotlivé komponenty sú prepojené pomocou API a rozhraní, ktoré umožňujú efektívnu výmenu údajov a automatizáciu procesov. Príklad integračného toku:

- SIEM zaznamená anomáliu → vytvorí alert,
- Alert sa automaticky prepojí s CTI a vyhodnotí jeho kontext,
- SOAR iniciuje reakciu (napr. blokovanie hash/IP, generovanie tiketu),
- Tiket sa vytvorí v incident manažment systéme,
- Prípad je riešený tímom, zaznamenaný a reportovaný,
- Relevantné poznatky sú uložené v znalostnom portáli.

Takáto prepojenosť zabezpečuje **pohotovosť, koordináciu, dôveryhodnosť a efektivitu** celého SOCaaS riešenia.

3. VYBRANÉ KOMPONENTY PRE SOCAAS INNOSOC

3.1 SIEM: Hodnotenie a výsledok analýz

3.1.1 Úloha komponentu

SIEM je srdcom SOCaaS riešenia. Zabezpečuje agregáciu, spracovanie, koreláciu a analýzu bezpečnostných udalostí z rôznych zdrojov, v reálnom čase. Umožňuje analytikom identifikovať anomálie, generovať upozornenia a eskalovať incidenty, pričom zvyšuje viditeľnosť nad infraštruktúrou klienta.

3.1.2 Posudzované riešenia

Na základe požiadaviek definovaných v kritériách boli hodnotené:

- **ELK Stack (Elasticsearch, Logstash, Kibana)**
- **Wazuh**
- **OpenSearch + OpenSearch Dashboards**
- **Graylog (Open)**
- **SIEMonster (Community Edition)**
- **Prelude OSS**
- **AlienVault OSSIM**

3.1.3 Podrobná analýza požiadaviek

Táto sekcia sumarizuje, ako jednotlivé riešenia spĺňajú definované požiadavky na SIEM komponenty v rámci SOCaaS. Hodnotenie je založené na štruktúrovaných kategóriách požiadaviek a poskytuje hlbší kvalitatívny popis pre každý nástroj zvlášť.

ELK Stack (Elasticsearch, Logstash, Kibana)

ELK Stack poskytuje rozsiahlu podporu pre zber logov pomocou nástrojov ako Filebeat, Winlogbeat, či Auditbeat. Tieto komponenty umožňujú zber logov z rôznych typov systémov vrátane Windows, Linux, sieťových zariadení a aplikačných služieb. Na úrovni analýzy dát Logstash umožňuje normalizáciu a parsovanie údajov, pričom Elasticsearch poskytuje výkonný indexačný a dotazovací engine.

Hoci samotná bezplatná verzia neposkytuje pokročilé ML nástroje, základné alerting mechanizmy je možné nastaviť cez Watcher (alebo Alerting plugin pri OpenSearch variante). Bezpečnostné funkcionality ako TLS medzi komponentmi a RBAC sú k dispozícii až v platených edíciách, čo predstavuje obmedzenie v open-source prostredí. Kibana však poskytuje intuitívne a rozšíriteľné dashboardy s množstvom vizualizačných možností a filtrami.

Wazuh

Wazuh integruje komponenty pre SIEM, EDR a FIM (File Integrity Monitoring). Zber dát je možný prostredníctvom agentov, ktorí podporujú logy z operačných systémov, súborov, auditných mechanizmov a aplikačných serverov. Okrem toho dokáže prijímať logy zo Syslog, čo umožňuje centralizovaný zber údajov aj z pasívnych zariadení bez agenta.

Wazuh poskytuje vlastný korelačný engine, s množstvom pravidiel založených na MITRE ATT&CK. Tieto pravidlá sú pravidelne aktualizované komunitou. Webové UI podporuje RBAC, správu úloh a prepojenie s Kibana dashboardmi. Jeho hlavnou silou je kombinácia EDR vlastností s prehľadným SIEM, čo ho robí výhodným riešením pre menšie tímy.

OpenSearch + Dashboards

Ako fork Elastic Stacku je OpenSearch plnohodnotnou alternatívou k Elasticsearch, pričom poskytuje všetky kľúčové funkcie pre zber, spracovanie a vizualizáciu logov. Beats a Logstash sú kompatibilné, čím je zabezpečená široká možnosť ingestu logov.

ML Commons je silný plugin, ktorý poskytuje bezplatné ML funkcionality ako detekciu anomálií. V oblasti bezpečnosti poskytuje TLS šifrovanie aj RBAC out-of-the-box. OpenSearch Dashboards umožňuje intuitívne zobrazenie metriky a vytváranie vizualizácií podobne ako Kibana, ale s otvorenejším vývojovým modelom.

Graylog

Graylog podporuje zber dát z rôznych zdrojov, no najlepšie pracuje s formátmi ako Syslog, GELF a JSON. Na spracovanie logov používa pipeline architektúru, ktorá umožňuje definovať pravidlá spracovania (napr. maskovanie údajov, normalizáciu).

Graylog v bezplatnej verzii neobsahuje ML analýzu, avšak ponúka dobré možnosti korelácie a alertingu. Dashboardy sú responzívne a jednoduché na konfiguráciu. Pre menšie tímy je výhodou aj nižšia zložitosť správy.

SIEMonster (Community Edition)

SIEMonster kombinuje výhody viacerých nástrojov (Elastic Stack, Wazuh, TheHive, Cortex). Vďaka tomu ponúka bohaté možnosti zberu logov, korelácie, obohacovania údajov (z CTI nástrojov) a reakcie na incidenty. Community edícia má však obmedzenie počtu agentov (napr. 100) a mierne komplikovanejšiu inštaláciu.

Hlavnou výhodou SIEMonsteru je predpripravené prepojenie komponentov, čo značne šetrí čas. Na druhej strane, jeho údržba a aktualizácie sú náročnejšie a vyžadujú znalosti naprieč viacerými subsystémami.

Prelude OSS

Prelude má špecifický prístup k SIEM riešeniu – je postavený na formáte IDMEF, ktorý nie je bežne využívaný v moderných ekosystémoch. Jeho možnosti zberu logov sú obmedzené, a chýba podpora pre bežne používané formáty alebo zberové agenty.

Jeho korelačný engine je výkonný a modulárny, no nie je podporovaný ML alebo behaviorálnymi detekciami. Dokumentácia je obmedzená a vývoj komunitou je málo aktívny.

AlienVault OSSIM

OSSIM poskytuje všetky základné SIEM funkcionality – zber logov, koreláciu a normalizáciu. Využíva vlastného agenta a podporuje protokoly ako Syslog, NetFlow či SNMP. Je to pomerne robustné riešenie, ale jeho rozhranie a dokumentácia sú zastarané.

V oblasti ML a CTI integrácie výrazne zaostáva. Upozornenia a dashboardy sú jednoduché, vhodné skôr na testovacie alebo akademické účely.

3.1.4 Analýza kľúčových požiadaviek:

- **Formáty logov**: ELK a OpenSearch podporujú široké spektrum formátov (syslog, JSON, CSV). Graylog sa orientuje na syslogové formáty. Wazuh má silnú podporu formátov cez svojho agenta a rozšírenie Elastic Stacku.
- **Zber auditných a systémových logov**: Auditbeat (ELK, OpenSearch) poskytuje priame mechanizmy. Wazuh umožňuje detailný audit vrátane integrity súborov (FIM). Graylog a OSSIM majú obmedzené možnosti bez doplnkov.

- **Analýza a detekcia**: ML modul v ELK je platený. OpenSearch má ML Commons plugin. Wazuh poskytuje základné behaviorálne detekcie. Korelácia udalostí je silná stránka Elastic Stacku a Wazuh.
- **Škálovateľnosť a výkonnosť**: ELK a OpenSearch sú vhodné pre veľké prostredia, s podporou pre horizontálne škálovanie. Graylog je vhodný pre stredne veľké nasadenia.
- **Integrácie**: Všetky riešenia podporujú integráciu s inými nástrojmi cez API, ale najlepšie dokumentovanú podporu má ELK a OpenSearch.

3.1.5 Záver výberu

Odporúčaný komponent: **ELK Stack** ako hlavný SIEM nástroj, s možnosťou nasadenia aj cez OpenSearch v prípade potreby čistej open-source licencie. Pre malé a stredné nasadenia je Wazuh výbornou alternatívou, najmä ak sa súčasne využíva ako EDR komponent.

3.2 SOAR: Hodnotenie a výsledok analýz

3.2.1 Úloha komponentu

SOAR (Security Orchestration, Automation and Response) je komponent zodpovedný za automatizáciu reakcií na incidenty, orchestráciu bezpečnostných nástrojov a podporu rozhodovania analytikov. V SOCaaS predstavuje základnú zložku umožňujúcu škálovanie reakčných kapacít bez nutnosti zvyšovať počet personálu. Je nevyhnutný najmä pri spracovaní veľkého množstva alertov, kde znižuje MTTR a MTTC metriky.

3.2.2 Posudzované riešenia

- **TheHive + Cortex**
- **Shuffle SOAR**
- **StackStorm**
- **Tracecat (Fasten Health, ex-Kuiper)**
- **FIR (Fast Incident Response)**

3.2.3 Profily riešení

TheHive + Cortex

TheHive ako incident manažment systém v kombinácii s Cortexom predstavuje výkonný SOAR ekosystém. TheHive slúži na správu incidentov, kategorizáciu, notifikácie, evidenciu dôkazov a audit. Cortex predstavuje integračný modul, ktorý umožňuje automatickú exekúciu preddefinovaných analytických alebo reakčných akcií (tzv. analyzérov). Silnou stránkou tejto dvojice je ich modularita, API pre integráciu a výborná dokumentácia. Vhodné pre nasadenie v komplexnejších SOCaaS prostrediach.

Shuffle SOAR

Shuffle je moderný vizuálny SOAR nástroj zameraný na jednoduchosť a flexibilitu. Umožňuje tvorbu reakčných workflowov prostredníctvom drag-and-drop rozhrania, napojenie na desiatky služieb (Slack, Jira, Elastic, GitHub, VirusTotal) a orchestráciu bezpečnostných akcií bez potreby kódovania. Podporuje asynchrónne spúšťanie procesov, debug režim a verziovanie playbookov. Nemá však integrovaný incident manažment a je vhodnejší ako doplnkový orchestrátor k inému systému.

StackStorm

StackStorm poskytuje robustnú architektúru na orchestráciu udalostí a reakčných akcií v IT a bezpečnostných systémoch. Pracuje na princípe „event → trigger → rule → action“ a podporuje stovky integrácií (tzv. packs). Umožňuje tvorbu komplexných playbookov, verzovanie a testovanie. Výhodou je jeho všeobecnosť, ale zároveň aj nevýhoda – nie je zameraný výlučne na kybernetickú bezpečnosť a vyžaduje rozsiahlejšiu konfiguráciu.

Tracecat (Fasten Health, ex-Kuiper)

Tracecat je open-source SOAR nástroj zameraný na intuitívne zostavovanie bezpečnostných scenárov. Umožňuje tvorbu playbookov s prepojeniami na SIEM, EDR, e-mailové notifikácie a spracovanie udalostí. Jeho výhodou je jednoduché nasadenie a orientácia na bezpečnostné tímy s nižšou úrovňou DevOps. Komunita je menšia, ale nástroj má potenciál pre malé a stredné organizácie.

FIR (Fast Incident Response)

FIR je zameraný na správu incidentov s dôrazom na klasifikáciu, štandardizáciu a audit. Umožňuje definovať typy incidentov, fázy riešenia, úrovne závažnosti, správcov a reakčné kroky. Podporuje LDAP, REST API a export údajov. Vhodný ako podklad pre reporting a incident evidenciu, pričom ho možno prepojiť s nástrojmi ako Cortex alebo StackStorm. TheHive je open-source incident response platforma, ktorá umožňuje správu incidentov, podporuje playbooky, vytvára vzťahy medzi udalosťami a poskytuje aj prepojenie s ďalšími nástrojmi (napr. MISP, Cortex). Má výbornú dokumentáciu a podporu komunitou. TheHive podporuje aj multi-tenantné prostredia, audit logy, automatizáciu cez API a interaktívne vyhodnocovanie IOC. Silnou stránkou je modularita a napojenie na Cortex pre exekúciu playbookov.

Shuffle SOAR

Shuffle je ľahký open-source SOAR nástroj s moderným webovým rozhraním, ktorý umožňuje vizuálnu tvorbu workflowov. Je možné prepojenie na API rôznych nástrojov (Elastic, Graylog, VirusTotal, Slack, Jira, atď.). Výhodou je jednoduchosť nasadenia (Docker) a flexibilita pri budovaní vlastných akcií. Nepodporuje však taký rozsah IR funkcionality ako TheHive a nemá nativne pripravený incident manažment model.

DFIR-IRIS

Platforma IRIS (Incident Response Investigation System) je určená primárne pre spracovanie digitálnej forenznej analýzy a incidentov. Ponúka nástroje na kategorizáciu, dokumentovanie a správu digitálnych dôkazov. Hoci nie je priamo klasický SOAR nástroj, poskytuje dôležitú funkcionalitu na automatizáciu forenzného spracovania incidentov, a dobre dopĺňa funkcie TheHive.

Wazuh-integrated actions

Wazuh ako bezpečnostná platforma poskytuje niektoré možnosti reakcií prostredníctvom aktívnych odpovedí (napr. blokovanie IP, skripty). Nejde však o plnohodnotný SOAR, preto túto funkcionalitu vnímame ako doplnkovú, vhodnú najmä pri absencii externého SOAR nástroja.

3.2.4 Podrobná analýza požiadaviek

TheHive + Cortex zabezpečuje pokročilý incident manažment, kategorizáciu, audit, správu dôkazov a cez Cortex aj automatizované akcie. Podporuje škálovateľnosť, multi-tenancy a integráciu so širokým spektrom nástrojov. Spĺňa požiadavky na orchestráciu playbookov, podporu API a audit.

Shuffle SOAR vyniká jednoduchosťou tvorby a správy playbookov. Umožňuje flexibilnú integráciu pomocou REST API a konektorov. Na druhej strane mu chýba hlbší incident manažment, ale je výborný ako doplnkový orchestrátor pre rýchle workflowy.

StackStorm ako univerzálny automatizačný nástroj ponúka rozsiahlu flexibilitu, ale vyžaduje znalosť konceptov a štruktúrované programovanie playbookov. Vhodný pre prostredia so zrelým DevSecOps prístupom.

Tracecat pokrýva základné požiadavky na tvorbu a prevádzku reakčných scenárov, ale nemá plnohodnotný systém správy incidentov. Jeho sila spočíva v prehľadnosti, jednoduchosti a možnosti rýchleho nasadenia.

FIR je silný v dokumentácii a riadení incidentov – umožňuje presnú klasifikáciu, fázy životného cyklu, integráciu a audit. Automatizáciu reakcií však neobsahuje nativne – vhodný je v kombinácii s Cortex, StackStorm či inými SOAR modulmi. veľmi dobrý nástroj na zaznamenávanie, štruktúrovanie a dokumentovanie incidentov. Podporuje timeline, forenzné atribúty a umožňuje vybudovanie znalostnej bázy incidentov. Neobsahuje však robustný engine na automatizáciu alebo orchestráciu.

3.2.5 Analýza kľúčových požiadaviek

- **Playbook orchestration**: Najlepšie pokryté v Shuffle a Cortex (s TheHive). IRIS poskytuje dokumentáciu, nie aktívne akcie.
- **Incident lifecycle management**: TheHive a IRIS poskytujú plný incident manažment model. Shuffle čiastočne.
- **Integrácie s inými nástrojmi**: Shuffle a TheHive majú silné API a množstvo konektorov. IRIS je uzavretejšia.
- **Audit a reporting**: TheHive má robustný auditný systém. IRIS je silná v dokumentácii. Shuffle audit len základný.

3.2.6 Záver výberu

Odporúčaný komponent: **TheHive + Cortex** ako hlavné SOAR riešenie. Kombinujú správu incidentov, interaktívne vyhodnocovanie a automatizáciu odpovedí. Pre jednoduché scenáre alebo testovanie možno alternatívne nasadiť Shuffle. IRIS odporúčame ako doplnkový nástroj na forenzné spracovanie incidentov.

3.3 EDR/XDR: Hodnotenie a výsledok analýz

Úloha komponentu:

EDR (Endpoint Detection and Response) a XDR (Extended Detection and Response) predstavujú základné technologické piliere pre detekciu hrozieb na úrovni koncových zariadení. V prostredí SOCaaS slúžia na zber, koreláciu a reakciu na udalosti, ktoré by inak unikli tradičným perimeterovým detekciám. XDR rozširuje koncept EDR o schopnosť integrovať dáta zo sietí, cloudov, e-mailových systémov a iných vrstiev.

Posudzované riešenia:

- **Elastic Security**
- **Wazuh**
- **OSSEC**
- **OpenEDR**
- **Velociraptor**

Profily riešení:

Elastic Security

Elastic Security je rozšírením Elastic Stacku, ktoré umožňuje detekciu, prevenciu a odpoveď na bezpečnostné incidenty. Využíva Elastic Agent s integráciou do Fleet, poskytuje rozsiahlu visibilitu nad endpointmi, možnosť detekcie hrozieb cez pravidlá, podporu MITRE ATT&CK a vizualizáciu prostredníctvom Kibana dashboardov. Silnou stránkou je aj schopnosť korelovať údaje medzi viacerými zdrojmi.

Wazuh

Wazuh ako bezpečnostná platforma poskytuje kombináciu SIEM a EDR schopností. V EDR oblasti umožňuje kontrolu integrity súborov (FIM), detekciu rootkitov, auditovanie aktivít, zber udalostí z OS aj aplikácií a podporu MITRE ATT&CK. Podporuje agentové aj agentless režimy a poskytuje škálovateľnú architektúru.

OSSEC

OSSEC je predchodcom Wazuh a zameriava sa na detekciu zmeny súborov, log monitoring a základnú odpoveď na incidenty. Je ľahký a jednoduchý na nasadenie, no chýba mu pokročilá korelácia, moderné integračné rozhrania a priamy mapping na MITRE ATT&CK. Výhodou je nízka systémová náročnosť a silná komunitná základňa.

OpenEDR

OpenEDR je riešenie vyvíjané spoločnosťou Comodo, zamerané na endpoint monitoring a analýzu. Poskytuje funkcie ako sledovanie procesov, sieťových spojení, zmeny v registroch a súborových systémoch. Obsahuje vlastný korelačný engine a zber agentom. Nevýhodou je obmedzená dokumentácia a menej aktívna komunita.

Velociraptor

Velociraptor je nástroj zameraný na threat hunting a forenznú analýzu. Umožňuje detailný zber dát, používanie dotazov v jazyku VQL, monitoring pamäte a artefaktov v reálnom čase. Nejde o klasický EDR, ale je ideálny na prehľadávanie incidentov, retrospektívnu analýzu a detailné vyhľadávanie kompromitácií.

Podrobná analýza požiadaviek:

Elastic Security spĺňa požiadavky na integráciu, koreláciu a vizualizáciu údajov, má pokročilý engine na detekciu hrozieb a výborné rozhranie pre tvorbu pravidiel. Plne podporuje mapping na MITRE ATT&CK, umožňuje priamu reakciu cez Elastic Agent a jeho modulárne rozšírenia.

Wazuh pokrýva požiadavky na FIM, log monitoring, rootkit detekciu a incident response. Je ideálne použiteľný v prostredí s požiadavkou na transparentný a ľahko auditovateľný EDR systém. Silnou stránkou je škálovateľnosť a komunitná podpora.

OSSEC poskytuje základné EDR schopnosti vhodné pre jednoduché nasadenia, no v porovnaní s Wazuh alebo Elastic Security výrazne zaostáva v automatizácii, orkestrácii a škálovaní. Neobsahuje natívne napojenia na ďalšie moduly SOCaaS.

OpenEDR spĺňa niektoré požiadavky na monitoring systémových aktivít, no jeho integrácia a flexibilita zaostávajú. Dokumentácia a podpora nie sú na úrovni konkurentov, čo môže byť rizikom pri nasadení vo väčších prostrediach.

Velociraptor pokrýva pokročilé požiadavky na forenziku, threat hunting a retrospektívne analýzy. Výborne dopĺňa klasické EDR riešenia, no neplní úlohu preventívneho EDR v plnej miere.

Analýza kľúčových požiadaviek:

- **Detekcia zmeny stavu systému**: Elastic Security, Wazuh a OpenEDR poskytujú pokročilý monitoring, OSSEC len základný.
- **Threat hunting a forenzika**: Velociraptor dominuje v tejto oblasti. Elastic Security a Wazuh poskytujú integrované analytické možnosti.
- **Reakcia na incidenty**: Elastic Security a Wazuh umožňujú aktívnu reakciu. OSSEC a OpenEDR len obmedzene.
- **Škálovateľnosť a integrácia**: Elastic a Wazuh ponúkajú bohaté integračné možnosti a horizontálne škálovanie.

Záver výberu:

Odporúčané komponenty

- **Elastic Security** pre organizácie, ktoré už používajú Elastic Stack a požadujú jednotné prostredie pre zber, koreláciu aj detekciu.
- **Wazuh** ako univerzálny komponent pre menšie a stredne veľké nasadenia, kde je preferencia stabilnej komunitnej podpory a transparentného EDR.
- **Velociraptor** ako doplnok pre špecifické prípadové analýzy a threat hunting. Vhodný najmä pre analytikov SOC pri riešení incidentov.

Neodporúčané pre hlavné nasadenie: OSSEC a OpenEDR vzhľadom na nižšiu úroveň funkcionality, integrácie a podpory. **Odporúčaný komponent**: **Wazuh ako primárne EDR riešenie** pre jeho agentovú architektúru, rozsiahlu dokumentáciu, MITRE ATT&CK integráciu a schopnosť pokryť viacero úrovní detekcie. **Doplňujúci komponent**: **Velociraptor** pre pokročilý threat hunting a forenznú analýzu na vyžiadanie. **Falco** sa odporúča ako doplnok pre cloud-native infraštruktúry a kontajnerové nasadenia.

3.4 Skener zraniteľností: Hodnotenie a výsledok analýz

Úloha komponentu

Skener zraniteľností je základným stavebným kameňom pre zabezpečenie proaktívneho prístupu v SOCaaS architektúre. Umožňuje pravidelne identifikovať slabé miesta v infraštruktúre, hodnotiť stav aktualizácií, konfigurácií a nastavení, a poskytovať informácie pre ďalšiu prioritizáciu a plánovanie nápravných opatrení. Výstupy skenera sú často zdrojom pre SOAR systémy, SLA metriky, reporting ako aj pre hodnotenie bezpečnostnej úrovne klienta.

Posudzované riešenia

- **Greenbone Community Edition (GCE)**
- **OpenSCAP**

Profily riešení:

Greenbone Community Edition (GCE)

GCE je bezplatná open-source verzia riešenia od Greenbone Networks, založená na nástroji OpenVAS. Poskytuje vysokokapacitné skenovanie, rozsiahle databázy zraniteľností cez komunitný GVMD feed, moderné webové rozhranie GSA a podporu pre plánovanie, alerty aj automatizáciu. Podporuje štandardy ako CVE, CPE, a umožňuje generovanie reportov vo formátoch CSV, XML, PDF. Možnosti integrácie zahŕňajú GMP protokol, SSH, LDAP, RADIUS a iné. GCE umožňuje aj master-senzor architektúru, čo je výhodné pre rozsiahle distribuované prostredia.

OpenSCAP

OpenSCAP je open-source rámec orientovaný na audit konfigurácií a politík pomocou štandardov SCAP, OVAL, ARF a XCCDF. Jeho silnou stránkou je súlad s normami (CIS, NIST, STIG), čo ho predurčuje na compliance audity. Podporuje bezagentové skenovanie, nízke HW nároky, ale primárne je určený na jednotkové hosty. Je vhodný pre audit systémových nastavení a konfigurácií, menej pre hromadné sieťové skenovanie. S výstupmi sa ďalej pracuje cez OpenSCAP Workbench alebo externé vizualizačné nástroje.

Podrobná analýza požiadaviek:

Licencovanie

Greenbone Community Edition (GCE) je plne otvorený nástroj, ktorý poskytuje funkčné jadro systému na detekciu zraniteľností. Aj keď ide o komunitnú verziu, umožňuje plynulý prechod na enterprise variantu s ďalšími funkciami. **OpenSCAP** je úplne open-source, udržiavaný komunitou aj organizáciami ako Red Hat, a poskytuje stabilné, transparentné a auditovateľné prostredie na bezpečnostnú analýzu konfigurácií.

Skenovanie a pokrytie

GCE má výrazne vyššiu škálovateľnosť pri sieťovom skenovaní a umožňuje hĺbkové overenie stoviek IP adries denne v závislosti od výkonu hostiteľa. Je vhodný na celopodnikové alebo multitenantné skenovanie. Naopak, **OpenSCAP** sa špecializuje na jednotlivé systémy a hodnotenie ich stavu súladu, a teda nie je efektívny pre rozsiahle siete.

Aktualizácie zraniteľností a podpora štandardov

GCE využíva komunitný feed (GVMD Data Feed), ktorý je pravidelne aktualizovaný. Komerčný feed je dostupný, čo umožňuje aj možnosť rozšírenia. Podpora pre CVE, CPE, CVSS je natívne integrovaná. **OpenSCAP** používa štandardy SCAP a OVAL, aktualizácie sú závislé od platformy a ich správa je často decentralizovaná.

Používateľské rozhranie a správa

GCE má GSA – intuitívne a moderné webové rozhranie umožňujúce plánovanie, sledovanie úloh a prehliadanie reportov. U **OpenSCAP** prebieha väčšina činností cez CLI alebo jednoduché nástroje ako SCAP Workbench. To môže byť limitujúce pri väčších tímoch.

Agentless prevádzka a plánovanie

Oba nástroje fungujú bez potreby agentov, čo zjednodušuje ich nasadenie. **GCE** má natívnu podporu pre plánovanie, alerty, rozvrhy a opakovanie skenov, čo umožňuje efektívnu automatizáciu. **OpenSCAP** vyžaduje integráciu s externými nástrojmi ako cron alebo Ansible.

Reporting a export údajov

GCE umožňuje exportovať výsledky vo viacerých formátoch (CSV, PDF, XML, HTML), čo zjednodušuje ich ďalšie spracovanie. **OpenSCAP** generuje výstupy ako ARF, HTML, XML – tie môžu byť menej použiteľné bez ďalšej konverzie.

Nasadenie a architektúra

GCE podporuje nasadenie ako kontajner, VM aj klasické on-premise. Podporuje architektúru typu master/senzor pre distribuované nasadenia. **OpenSCAP** je monolitický nástroj a neposkytuje možnosť centralizovaného riadenia senzora.

Výkonové a technické požiadavky

GCE potrebuje minimálne 4 GB RAM, 2 vCPU a SSD disk. Odporúčané je 8 GB RAM pre vyšší výkon. **OpenSCAP** je veľmi ľahký a funguje aj na 1 vCPU a 1 GB RAM, čo z neho robí ideálne riešenie pre resource-limited zariadenia.

Podpora protokolov

GCE rozpoznáva viaceré sieťové protokoly vrátane DNS, DHCP, SNMP, SSH a iných. **OpenSCAP** závisí na definovaných SCAP politikách, ktoré môžu obsahovať protokolové parametre, ale nie je primárne určený na sieťovú detekciu.

Integrácie a skórovacie modely

GCE podporuje štandard CVSS v3, pripravuje podporu CVSS v4 a je možné ho rozšíriť o EPSS pomocou externých feedov. **OpenSCAP** podporuje skórovanie cez OVAL definície. Integrácie sú u GCE robustnejšie, s podporou GMP API.

Prevádzkové aspekty a zhodnosť s normami

GCE umožňuje whitelistovanie a správu výnimiek. Má podporu štandardov ako ISO 27001, BSI a GDPR. **OpenSCAP** je veľmi silný v oblasti štandardov – poskytuje pokrytie CIS, STIG, NIST a je vhodný na pravidelné audity a hodnotenie súladu.

Analýza kľúčových požiadaviek:

- **Rozsah skenovania**: GCE je vhodné pre rozsiahle siete, OpenSCAP pre jednotlivé systémy.
- **Zhodnosť s normami**: OpenSCAP je výrazne silnejší, vhodný pre compliance-centric prostredia.
- **Automatizácia a plánovanie**: GCE má vstavané plánovanie, OpenSCAP vyžaduje externý nástroj.
- **Vhodnosť pre SOCaaS**: GCE je flexibilnejšie a integruje sa jednoduchšie.

Záver výberu

Odporúčaný komponent: Greenbone Community Edition ako hlavný skener zraniteľností pre SOCaaS vďaka jeho modulárnosti, výkonu a otvorenej architektúre. **Doplňujúci komponent**: OpenSCAP ako nástroj pre compliance audity a systémové konfigurácie podľa noriem (CIS, STIG, NIST).

3.5 CTI: Hodnotenie a výsledok analýz

3.5.1 Úloha komponentu

CTI (Cyber Threat Intelligence) predstavuje kľúčový stavebný prvok SOCaaS architektúry, pretože poskytuje schopnosť obohacovať detekčné pravidlá, korelačné mechanizmy a playbooky o externé informácie o hrozbách – vrátane IOC, TTP, profilovania útočníkov, kampaní a súvisiacich zraniteľností. V prostredí viaczákaznníckej služby SOCaaS zohráva úlohu pri:

- Distribúcii a správe threat feedov naprieč tenantmi,
- Automatickom obohacovaní SIEM a EDR dát o známe hrozby,
- Vytváraní časových línií útokov a priraďovaní k MITRE ATT&CK technikám,
- Podpore procesov threat huntingu a forenznej analýzy,
- Prioritizácii incidentov podľa kontextu hrozieb.

Pre návrh riešenia boli zvolené open-source platformy, ktoré pokrývajú rôzne aspekty CTI – od zberu IOC cez vizualizáciu, až po STIX/TAXII kompatibilitu.

3.5.2 Posudzované riešenia

Na základe predošlej analytickej fázy a kategorizovaných požiadaviek boli vybrané tieto open-source riešenia:

- **OpenCTI** – komplexná platforma na správu všetkých úrovní CTI (IOC, TTP, aktéri).
- **MISP** – komunitne populárna platforma pre IOC zdieľanie, silná v taktickom CTI.
- **IntelMQ** – framework zameraný na automatizovaný zber, spracovanie a distribúciu IOC.
- **YETI** – databázovo orientovaný systém na správu entít hrozieb, orientovaný na analytikov.
- **Vulmatch** – nástroj zameraný na párovanie CVE a IOC, s dôrazom na CVSS a EPSS.
- **Modul Threat Intel (Elastic)** – rozšírenie v rámci Elastic stacku pre vizualizáciu IOC.

3.5.3 Profily riešení

OpenCTI je robustný nástroj podporujúci STIX 2.1, ktorý umožňuje modelovanie kampaní, TTP, skupín útočníkov, a ich vzájomných vzťahov. Umožňuje integráciu so SIEM/EDR nástrojmi cez GraphQL API, a disponuje vizualizáciou pomocou grafov. Podporuje import z MISP, Abuse.ch a automatické feedy.

MISP sa sústreďuje najmä na IOC výmenu a komunitné zdieľanie dát. Umožňuje poloautomatické obohacovanie, REST API, integráciu s firemnými systémami a export v rôznych formátoch. Má rozšírenie pre MITRE ATT&CK a podporuje deduplikáciu.

IntelMQ predstavuje rámec orientovaný na automatizáciu. Každý “bot” má špecifickú úlohu – zber, analýzu, obohacovanie alebo výstup. Je ideálny na automatické spracovanie feedov a poskytuje pipeline spracovanie dát.

YETI slúži ako databázový agregátor entít (IOC, aktéri, kampane). Umožňuje ručné aj API vstupy, základnú automatizáciu a jednoduchú vizualizáciu. Je vhodný pre analytikov a threat hunters, ktorí potrebujú evidenciu a prepojenia entít.

Vulmatch je úzko zameraný nástroj, ktorý sa špecializuje na párovanie IOC a CVE, čím umožňuje efektívne priraďovanie hrozieb k zraniteľnostiam. Poskytuje jednoduché výstupy a prioritizáciu podľa CVSS/EPSS.

Threat Intel modul v Elastic Stacku umožňuje základné ukladanie IOC a ich koreláciu s logmi. Neobsahuje vlastnú CTI logiku, ale prostredníctvom dashboardov, vizualizácií a filter funkcií môže slúžiť ako doplnok.

3.5.4 Podrobná analýza požiadaviek

Táto sekcia podrobne posudzuje šesť vybraných CTI riešení: **OpenCTI**, **MISP**, **IntelMQ**, **YETI**, **Vulmatch** a **Modul Threat Intel (Elastic)** voči všetkým požiadavkám definovaným v kategóriách funkčných, technických a prevádzkových parametrov. Každá požiadavka je analyzovaná samostatne pre každý nástroj, pričom sa prihliada na maticu požiadaviek poskytnutú v analytickom Exceli.

Licencovanie a všeobecná dostupnosť

- **OpenCTI** je plne open-source pod licenciou AGPL. Má bohatú komunitu a možnosť enterprise podpory. Možnosť rozšírenia cez konektory a REST API je bezplatná.
- **MISP** je open-source pod GPLv3, s množstvom nadstavieb a komunity. Vďaka modularite je nasadenie flexibilné.
- **IntelMQ** je projekt pod záštitou CERT.at a ENISA. Je bezplatný, vývoj je aktívny.
- **YETI** je komunitný projekt, menej aktívny ako OpenCTI, no dostupný a rozšíriteľný.
- **Vulmatch** je ľahký, zameraný na párovanie CVE–IOC. Open-source, ale menej známy.
- **Elastic Threat Intel modul** je bezplatne dostupný ako súčasť Elastic Stacku, avšak pokročilé funkcie vyžadujú platenú verziu (napr. SIEM integrácia).

Typy CTI: strategický, operatívny, taktický

- **OpenCTI** exceluje v podpore všetkých troch vrstiev CTI – IOC (taktické), TTP a profilovanie skupín (operatívne), aj strategická analýza cez hodnotenia, prepojenia, časové osi.
- **MISP** zvláda operatívnu a taktickú vrstvu výborne – spravuje IOC, umožňuje prepojenia medzi incidentmi a aktérmi. Strategická vrstva je podporená len okrajovo (manuálne poznámky).
- **IntelMQ** je čisto taktický CTI systém – IOC, URL, IP a ich distribúcia. Nepodporuje vyššie úrovne.
- **YETI** podporuje IOC aj profilovanie TTP, ale absentuje strategická úroveň.
- **Vulmatch** nepracuje s TTP alebo kampanemi – je určený len na CVE–IOC prepojenie.
- **Elastic modul** umožňuje zaznamenanie IOC, ale vyššie vrstvy CTI nie sú podporené.

Zber údajov a integrácia so zdrojmi

- **OpenCTI** má najbohatšiu integráciu – obsahuje natívne konektory na Abuse.ch, OTX, MISP, VirusTotal a iné. Konektory možno upravovať, škálovať a sú aktualizované.
- **MISP** má vstavané moduly na integráciu so zdrojmi ako Malware Bazaar, Abuse.ch, a inými komunitnými feedmi. Integrácia je jednoduchá cez cron/REST.
- **IntelMQ** má veľmi široké možnosti zberu údajov – každý "bot" môže byť zameraný na iný zdroj. Integrácia cez bot-config alebo moduly.
- **YETI** má niekoľko konektorov, ale často vyžadujú manuálne ladenie. Viac orientovaný na obohacovanie ako zber.
- **Vulmatch** má obmedzenú podporu – väčšinou závisí od vlastnej implementácie.
- **Elastic modul** vie indexovať IOC zo zdrojov cez ingest pipeline, ale nemá CTI-centric konektory.

Normalizácia a spracovanie dát

- **OpenCTI** používa entitne orientovaný model založený na STIX 2.1. Dáta sú čitateľné, normalizované, napojiteľné na ďalšie nástroje.
- **MISP** používa vlastný formát, ale podporuje STIX export/import. Normalizácia je silná, dobre dokumentovaná.
- **IntelMQ** má jednotný Message Format, ktorý možno konvertovať – ideálne pre pipeline.
- **YETI** normalizuje cez vlastnú databázu entít a tagov. STIX podpora chýba.
- **Vulmatch** neponúka normalizáciu – je určený na veľmi špecifický účel.
- **Elastic modul** umožňuje štandardizovať IOC pomocou vlastných polí, ale nie je to CTI štandard.

Automatizácia, playbooky, deduplikácia

- **OpenCTI** má deduplikáciu entít, low-code automatizáciu pomocou konektorov a možnosť prepojenia s SOAR.
- **MISP** umožňuje deduplikáciu IOC podľa UUID, má pravidlá na event-action spracovanie.
- **IntelMQ** podporuje automatické boty, ktoré môžu vykonávať deduplikáciu aj normalizáciu – bez UI.
- **YETI** má obmedzenú podporu automatizácie, ale umožňuje deduplikáciu IOC cez hash.
- **Vulmatch** nemá pokročilú deduplikáciu.
- **Elastic modul** dokáže obohacovať IOC, ale logika deduplikácie je manuálna.

Integrácia, sandbox, vizualizácia

- **OpenCTI** integruje cez GraphQL a podporuje výstupné feedy. Má vstavané vizualizácie.
- **MISP** exportuje cez API, REST alebo feed. Vizualizácie sú jednoduché.
- **IntelMQ** nemá vizualizácie – integruje sa cez JSON/syslog.
- **YETI** obsahuje jednoduché dashboardy.
- **Vulmatch** vizualizácie neobsahuje.
- **Elastic modul** využíva Kibanu – vizualizácie sú bohaté, ale bez kontextu TTP.

3.5.5 Analýza kľúčových požiadaviek

Na základe kategorizovaných požiadaviek boli ako najdôležitejšie pre návrh SOCaaS služby identifikované nasledujúce aspekty:

- **Schopnosť spracovávať všetky úrovne CTI (strategická, operatívna, taktická)** – keďže SOCaaS má obsluhovať viacerých zákazníkov, je dôležité disponovať nástrojom, ktorý poskytuje kompletný prehľad o hrozbách – od IOC až po analytické reporty.
- **STIX/TAXII kompatibilita** – interoperability medzi komponentmi a externými partnermi je kľúčová pre výmenu údajov.
- **Deduplicitné spracovanie a normalizácia údajov** – kvôli vysokej frekvencii feedov a veľkému objemu IOC údajov je nevyhnutné eliminovať redundantné záznamy.
- **Vysoký stupeň automatizácie a konektorov na známe zdroje CTI** – šetrí čas analytikom a zvyšuje aktuálnosť údajov.
- **Integrácia so SIEM a EDR** – automatické obohacovanie detekčných pravidiel a alertov o kontext CTI je nevyhnutné pre MTTD a MTTC metriky.

V porovnaní s týmito požiadavkami:

- **OpenCTI** jednoznačne dominuje – pokrýva všetky CTI úrovne, má podporu STIX/TAXII, vysokú mieru deduplikácie, modularitu a výborné vizualizácie. Umožňuje efektívne prepojenie na ďalšie komponenty SOCaaS.
- **MISP** je silný najmä v taktickom CTI, disponuje veľkou komunitou a STIX podporou. Výborne sa hodí ako doplnkový feedovací systém.
- **IntelMQ** je špecialista na automatický zber IOC, ideálny ako pipeline pre predspracovanie údajov.
- **YETI** a **Elastic modul** sú vhodné ako doplnky pre prácu analytikov a vizualizáciu dát, avšak nie sú dostatočné samostatne.
- **Vulmatch** má úzko špecializované využitie a nepostačuje ako hlavný CTI systém.

3.5.6 Záver výberu

Na základe vyhodnotenia funkčných, technických a prevádzkových požiadaviek bol ako hlavný komponent pre CTI v rámci SOCaaS architektúry zvolený **OpenCTI**. Tento nástroj ponúka najkomplexnejšie pokrytie požiadaviek, umožňuje flexibilné napojenie ďalších

komponentov (napr. MISP, IntelMQ, EDR, SIEM), podporuje vysoký stupeň automatizácie a disponuje bohatými vizualizačnými možnosťami.

Ako doplnkové nástroje sa odporúčajú:

- **MISP** – na správu IOC a komunitné zdieľanie hrozieb,
- **IntelMQ** – ako automatizovaný pipeline framework pre zber IOC údajov.

Takáto kombinácia nástrojov zabezpečí plnohodnotnú funkcionalitu pre celý cyklus správy hrozieb od zberu až po analytickú interpretáciu.

3.6 Inventarizácia aktív: Hodnotenie a výsledok analýz

3.6.1 Úloha komponentu

Inventarizácia aktív je základným pilierom každého bezpečnostného riešenia. Umožňuje SOC tímu získať prehľad o všetkých zariadeniach, systémových entitách, aplikáciách a virtuálnych či cloudových zdrojoch, ktoré tvoria infraštruktúru organizácie. V prostredí SOCaaS zohráva ešte významnejšiu úlohu, pretože umožňuje centralizovanú správu, kategorizáciu, monitorovanie a sledovanie bezpečnostného stavu infraštruktúry naprieč rôznymi zákazníkmi.

Z kvalitnej evidencie aktív vychádza detekcia zraniteľností, kontextualizácia incidentov, analýza dopadu a nastavenie efektívneho ticketovania. Sledovanie životného cyklu aktív navyše podporuje plánovanie obnovy, auditné procesy a zabezpečenie súladu s reguláciami.

3.6.2 Posudzované riešenia

Na základe definovaných požiadaviek sme analyzovali nasledovné open-source nástroje pre správu aktív:

- **LibreNMS** – primárne zameraný na sieťový monitoring a SNMP discovery.
- **pi.Alert** – jednoduché IP/MAC monitorovanie so zameraním na domáce a malé siete.
- **NetBox** – moderný IPAM a DCIM nástroj s pokročilou evidenciou sietí a zariadení.
- **Ralph** – plnohodnotný systém na správu aktív s podporou CMDB a životného cyklu.
- **GLPI** – robustný systém s integrovaným helpdeskom a silnou podporou asset managementu.

3.6.3 Profily riešení

LibreNMS

Zameriava sa na SNMP-based monitoring s podporou automatického objavovania zariadení. Disponuje možnosťou základného tagovania, zobrazenia stavu zariadenia, a exportu dát. Na druhej strane mu chýba plnohodnotná CMDB, správa životného cyklu alebo prehľadné väzby medzi aktívami. Je vhodný ako doplnkový komponent pre získavanie živých údajov zo siete.

pi.Alert

Minimalistické riešenie vhodné pre malé siete, ktoré poskytuje jednoduchý prehľad pripojených zariadení na základe IP a MAC adries. Jeho schopnosti sú však obmedzené – neposkytuje CMDB, kategorizáciu, prepojenia medzi aktívami ani pokročilé rozhrania pre správu. Nástroj je vhodný najmä pre základnú sieťovú viditeľnosť.

NetBox

Silný v oblasti IPAM a DCIM. Umožňuje prepojenie medzi aktívami, evidenciu fyzickej aj logickej topológie, kategorizáciu a rozšíriteľnosť cez vlastné atribúty a Django pluginy. Výhodou je moderné UI, prehľadná štruktúra a možnosť napojenia na ďalšie systémy cez REST a GraphQL API. Slabinou je chýbajúci natívny asset discovery – vyžaduje integráciu s externými nástrojmi.

Ralph

Zameraný na správu životného cyklu majetku, s podporou CMDB, kategorizácie, záznamov zmien a REST API. Umožňuje zaznamenávať hardvér, softvér a ich stav počas celej prevádzky. Discovery funkcie sú skôr obmedzené, ale samotná evidencia je veľmi dobre navrhnutá. Ralph ponúka dobrý kompromis medzi funkčnosťou a jednoduchosťou.

GLPI

Najkomplexnejšie riešenie z posudzovaných nástrojov. Obsahuje výbornú podporu pre správu aktív, kategorizáciu, väzby medzi entitami, plánovanie, notifikácie a integráciu s inými systémami. S pomocou pluginu FusionInventory podporuje discovery aktív v sieti. Výhodou je aj existencia natívneho ticketing modulu, čo umožňuje spojenie asset managementu a incident managementu do jedného nástroja.

3.6.4 Podrobná analýza požiadaviek

LibreNMS ponúka hlavne sieťový pohľad – vďaka SNMP vie identifikovať zariadenia a sledovať ich stav. V správe aktív má však medzery – nedisponuje CMDB ani pokročilou kategorizáciou. Výhodou je integrácia so SIEM/monitoring systémami ako Zabbix a výkonné notifikácie.

pi.Alert sa hodí skôr na základnú IP viditeľnosť – spravuje IP/MAC mapu, upozorňuje na zmeny v sieti. Nevie rozlišovať typy aktív, chýba prepojenie medzi entitami aj CMDB. Neumožňuje životný cyklus, notifikácie sú len základné.

NetBox poskytuje precíznu sieťovú evidenciu – dokáže spravovať racky, VLANy, IP rozsahy, prepínače, serverové farmy. Umožňuje vlastné polia a väzby. Nemá však asset discovery, a tak je potrebné synchronizovať údaje z iných systémov. Výhodou je jeho výkonné API a čisté UI.

Ralph podporuje CMDB, správu stavu, sledovanie životného cyklu, audit a REST API. Pre discovery potrebuje nadstavby, ale manažment aktív je komplexný. Evidencia OS, softvéru, verzií je možná. Umožňuje aj kategorizáciu, tagy a vlastníkov.

GLPI je robustný nástroj – má CMDB, tiketovací systém, notifikácie, životný cyklus aj detailné logovanie zmien. Množstvo pluginov rozširuje možnosti nástroja. Výhodou je prepojenie s FusionInventory, čo umožňuje automatizovaný zber údajov. UI je robustné, ale zrozumiteľné.

3.6.5 Analýza kľúčových požiadaviek

Z analýzy vyplýva, že najväčší dôraz treba klásť na:

- Schopnosť spravovať celý životný cyklus aktív.
- Podporu CMDB, kategorizáciu a prepojenia medzi aktívami.
- API a možnosť integrácie s ďalšími SOC komponentmi (napr. SIEM, EDR).
- Schopnosť zberu údajov automatizovane z infraštruktúry.

GLPI a **NetBox** ako jediné plne pokrývajú väčšinu kľúčových požiadaviek. GLPI vedie v oblasti asset managementu a ticketovania, NetBox dominuje v oblasti sieťovej evidencie a prepojení medzi entitami. V kombinácii tak tvoria silný základ pre správu aktív v SOCaaS prostredí.

3.6.6 Záver výberu

Na základe detailného porovnania odporúčame nasadiť tieto komponenty:

- **GLPI** ako hlavný asset manažment nástroj, ktorý pokrýva správu CMDB, evidenciu, životný cyklus, audit a integrácie.
- **NetBox** ako doplnkový nástroj na presnú správu sieťovej infraštruktúry, IPAM a prepojenia medzi sieťovými komponentmi.

Tieto nástroje sa navzájom dopĺňajú a umožňujú plnú vizibilitu a kontrolu nad infraštruktúrou, čo je základný predpoklad pre efektívnu detekciu a reakciu v rámci SOCaaS služby.

3.7 Manažovanie kybernetických bezpečnostných incidentov

Efektívne riešenie kybernetických incidentov je kľúčovým pilierom SOCaaS architektúry. Nezahŕňa len samotné zaznamenanie udalostí, ale komplexný cyklus ich evidencie, manažmentu, reakcie, reportovania a uchovávania znalostí. Pre SOC tím je zásadné, aby boli incidenty riadené systémovo, s dôrazom na trasovateľnosť, analytickú prácu, koordináciu a znalostnú podporu. Efektívna a koordinovaná reakcia na bezpečnostné incidenty je nevyhnutným pilierom každého SOCaaS riešenia. V rámci architektúry INNOSOC boli identifikované štyri podkomponenty, ktoré spoločne tvoria integrovaný systém na správu, evidenciu, dokumentáciu a riešenie incidentov:

1. **Tiketovací systém**
2. **Evidencia a správa incidentov**
3. **Reportovanie**
4. **Znalostný portál pre SOC tím**

3.7.1 Tiketovací systém

Úloha podkomponentu

Tiketovací systém slúži ako ústredný komunikačný a organizačný kanál pre správu bezpečnostných incidentov počas ich celého životného cyklu. Umožňuje vytváranie, priraďovanie a sledovanie úloh a komunikáciu medzi analytikmi, pričom podporuje audit, SLA monitoring, eskaláciu a notifikácie.

Posudzované riešenia

- **TheHive**
- **Zammad**
- **Request Tracker (RT)**
- **osTicket**
- **RTIR (RT pre incident response)**

Profily riešení:

TheHive

TheHive je open-source platforma špeciálne navrhnutá pre správu bezpečnostných incidentov. Jeho výhodou je hlboká integrácia s nástrojmi ako MISP (pre Threat Intelligence) a Cortex (pre obohacovanie údajov pomocou analyzátorov a responderov). Vďaka tejto integrácii dokáže TheHive premeniť prijatý alert na plnohodnotný incident (tzv. „case“) s množstvom observables, ktoré možno triediť, filtrovať, obohacovať a priraďovať jednotlivým analytikom. Každý case môže obsahovať viaceré úlohy, komentáre, prílohy a je súčasťou workflow. Platforma ponúka REST API aj Webhooky, čím je ideálna na integráciu so SIEM, EDR alebo automatizačnými systémami. TheHive poskytuje detailné auditné logy a podporuje RBAC s granularitou oprávnení.

Zammad

Zammad je moderný tiketovací systém vyvíjaný s dôrazom na použiteľnosť a jednoduchú integráciu do ITSM prostredia. Podporuje plne responzívne webové rozhranie, s intuitívnym ovládaním a drag-and-drop manipuláciou s prílohami. Tikety môžu byť vytvárané ručne, cez e-mail, API alebo pomocou formulárov. Zammad umožňuje flexibilné definovanie frontov, SLA pravidiel, eskalácií a automatizovaných akcií cez tzv. „triggery“. Okrem natívneho REST API umožňuje aj LDAP synchronizáciu, SSO a napojenie na externé systémy ako SIEM či ticketovacie brány. Funkcionalita tagovania, šablón, exportov a viacúrovňovej správy oddelení je vstavaná. Aj keď nejde o nástroj špecificky zameraný na kybernetické incidenty, jeho modularita a čistý dizajn z neho robia vhodnú možnosť pre podporu SOC procesov v menších tímoch alebo ako doplnkový helpdesk.

Request Tracker (RT)

RT je robustný a vysoko prispôsobiteľný systém vyvíjaný firmou Best Practical. Jeho silnou stránkou je stabilita, podpora širokej škály rozšírení (vrátane incident response rozšírenia RTIR), a schopnosť spravovať komplexné workflow vo veľkých organizáciách. RT je postavený na tradičnej ticketovej logike, kde sú požiadavky spracovávané ako fronty, ktoré možno organizovať podľa tímov, oddelení či zákazníkov. V rámci každého ticketu sú zaznamenané komentáre, úlohy, metadáta, prílohy aj história zmien. Systém podporuje tvorbu šablón, definíciu rolí, SLA pravidlá, a vďaka REST API a CLI ho možno integrovať s ďalšími nástrojmi. RT je vhodný do prostredí, ktoré požadujú detailnú správu požiadaviek s možnosťou konfigurácie podľa interných procesov, avšak jeho používateľské rozhranie pôsobí zastarano a môže byť menej intuitívne pre nových používateľov.

osTicket

osTicket je jednoduchý, no spoľahlivý tiketovací systém s open-source licenciou. Je vhodný do menších prostredí alebo ako podporný systém pre všeobecnú komunikáciu so zákazníkmi, vrátane bezpečnostných požiadaviek. Podporuje vytváranie ticketov cez web, e-mail, API a možnosť konfigurácie pomocných polí. Umožňuje priraďovať požiadavky jednotlivým agentom, spravovať SLA a kategórie. osTicket podporuje exporty, notifikácie, prílohy a základný RBAC. Rozhranie je prehľadné, ale menej flexibilné než u pokročilejších riešení. Výhodou je nízka náročnosť na správu, nevýhodou slabšia integrácia s inými bezpečnostnými nástrojmi. V prostredí SOC je osTicket použiteľný najmä ako základná platforma pre zaznamenanie požiadaviek, avšak nie ako plnohodnotný incident management systém.

RTIR (RT for Incident Response)

RTIR je rozšírenie RT špecificky navrhnuté pre riešenie kybernetických incidentov, ktoré umožňuje používať preddefinované typy záznamov ako „Incident“, „Investigation“, „Block“ či „Report“. Tieto typy záznamov umožňujú presne sledovať priebeh incidentu, zapojiť viaceré tímy, priradiť zodpovednosti a zabezpečiť auditovateľnú stopu. RTIR umožňuje kategorizáciu, prioritizáciu, šablóny, eskalácie a spracovanie požiadaviek vo viacerých tímoch. Jeho výhodou je silná konfigurovateľnosť a rozšíriteľnosť, nevýhodou pomerne komplexná správa a nutnosť prispôsobenia UI podľa preferencií používateľov. Integrácie s externými CTI alebo SIEM systémami sú dostupné cez pluginy alebo API, no často vyžadujú prácu vývojára. V kontexte SOCaaS predstavuje robustné, ale menej užívateľsky prívetivé riešenie.

Podrobná analýza požiadaviek

Základné funkcie a workflow: TheHive a Zammad ponúkajú intuitívne a responzívne prostredie na správu ticketov. TheHive je však optimalizovaný pre bezpečnostné prípady a obsahuje aj atribúty ako observables. RT/RTIR umožňuje robustné workflow, ale používateľské rozhranie je menej moderné. osTicket poskytuje základné funkcie, ale chýba mu hlbšia integrácia s bezpečnostnými nástrojmi.

Notifikácie, prioritizácia, šablóny: Zammad a TheHive podporujú automatizované notifikácie, rôzne úrovne priority a šablóny ticketov. RTIR ponúka SLA monitoring a kategorizáciu, ale menej flexibilné UI.

Integrácie a exporty: TheHive dominuje v oblasti integrácií (Cortex, MISP, SIEM). Zammad a RT umožňujú API export a integráciu s externými systémami. osTicket má obmedzené možnosti, RTIR podporuje len niektoré typy exportov.

UX/UI a použiteľnosť: Zammad ponúka moderný dizajn, TheHive je optimalizovaný pre SOC tímy. RT a osTicket majú zastaranejší vizuál, no funkčne postačujú.

Analýza kľúčových požiadaviek

- **Multitenantnosť**: Podporovaná hlavne v TheHive a Zammad, menej v RTIR.
- **RBAC a auditovanie**: Silne zastúpené v TheHive, Zammad aj RTIR.
- **Integrácia so SIEM/SOAR**: Výrazne podporovaná najmä v TheHive.
- **Notifikácie a SLA**: TheHive, Zammad aj RTIR umožňujú efektívny SLA monitoring a upozornenia.

Záver výberu

TheHive je jednoznačný víťaz, pretože poskytuje natívnu podporu pre incidenty, je úzko integrovaný s CTI a SOAR nástrojmi a má moderné rozhranie. **Zammad** je vhodný ako alternatíva pre menej zložité prostredia alebo ako doplnkový helpdesk nástroj.

3.7.2 Evidencia a správa incidentov

Úloha podkomponentu

Evidencia a správa incidentov je jadrovým prvkom každej bezpečnostnej prevádzky (SOC). Tento podkomponent zaisťuje systematickú dokumentáciu, sledovanie a manažovanie bezpečnostných udalostí a incidentov v priebehu ich životného cyklu – od detekcie cez analýzu

až po uzavretie. Kvalitný systém evidencie musí umožniť tímom koordinovane spolupracovať, dokumentovať kroky, evidovať súvisiace artefakty (observables) a prepojiť incidenty s relevantnými hrozbami, systémami alebo historickými prípadmi. V ideálnom prípade podporuje aj pokročilé obohacovanie údajov, audit, multitenantnosť a možnosť spätného skúmania incidentov.

Posudzované riešenia

- **TheHive**
- **RTIR (Request Tracker for Incident Response)**

Tieto riešenia boli vybrané pre ich zameranie na bezpečnostný kontext, podporu incident management procesov, integráciu s ďalšími nástrojmi (CTI, SIEM, SOAR), open-source licencovanie a rozsiahle adopcie v komunitách.

Profily riešení:

TheHive

TheHive je špičková open-source platforma pre incident response, ktorá je v praxi široko používaná pre manažment bezpečnostných prípadov. Umožňuje vytvárať tzv. *cases*, ktoré môžu obsahovať úlohy, komentáre, observables (napr. IP adresy, hash hodnoty, URL, domény) a množstvo ďalších artefaktov. Observables možno nielen evidovať, ale aj automaticky obohacovať pomocou Cortex analyzátorov alebo prepojiť s MISP.

Každý incident (case) môže byť ďalej rozdelený na úlohy s časovým rámcom, statusom, priority a priradením analytikovi. Systém podporuje pokročilú kategorizáciu, vlastné šablóny prípadov a workflow zdieľané medzi organizačnými jednotkami. Jedným z hlavných prínosov je intuitívne webové rozhranie, REST API, multitenantná architektúra a silná prispôsobiteľnosť. Audit trail je zachytávaný na úrovni akcií, observables aj komentárov. Umožňuje plne dokumentovať priebeh vyšetrovania incidentu.

RTIR (Request Tracker for Incident Response)

RTIR je rozšírenie stabilného systému Request Tracker (RT), špecificky navrhnuté pre bezpečnostné tímy. Pracuje s konceptmi ako *Incident*, *Investigation*, *Block* a *Report*, čo z neho robí dobre štruktúrovaný nástroj pre sledovanie a eskaláciu incidentov. Každý incident môže byť rozdelený do vyšetrovania, ktoré sa ďalej detailne eviduje, komentuje a sleduje. Systém umožňuje prepojenie prípadov pomocou referencií, manuálne aj čiastočne automatizovane.

RTIR ponúka SLA management, RBAC, auditné logy a možnosť exportov. Aj keď nie je moderný z pohľadu UI, je mimoriadne stabilný, konfigurovateľný a osvedčený vo veľkých prostrediach. Prípadový workflow je menej flexibilný ako v TheHive, ale lepšie sa integruje s formálnymi procesmi organizácií, ktoré už používajú RT ako core helpdesk systém.

Podrobná analýza požiadaviek

Prípadová správa:

- *TheHive* umožňuje tvorbu incidentov ako prípadov (cases), ktoré možno plne rozčleniť na úlohy, komentáre, observables a metadáta. Prípad môže byť spojený s rôznymi entitami – analytikmi, organizáciami, CTI záznamami. Evidencia je detailná a konfigurovateľná.
- *RTIR* používa prístup typu typizovaných požiadaviek (Incident, Investigation...), kde každá časť má špecifickú štruktúru a workflow. Detailnosť je vysoká, ale správa prípadov je menej vizuálne zameraná a orientovaná skôr na formálnu evidenciu.

Observables a ich správa:

- *TheHive* ponúka natívnu správu observables s možnosťou ich vizualizácie, triedenia, zdieľania a obohacovania.
- *RTIR* umožňuje prácu s observables cez doplnky alebo vlastné polia – nie je to však jeho natívna doména, čo si vyžaduje prispôsobenie.

Kategorizácia a šablóny:

- *TheHive* umožňuje šablóny prípadov podľa typu incidentu – napr. phishing, malware, insider threat, ktoré sú predpripravené s úlohami a observables.
- *RTIR* používa formálne typy požiadaviek – bez automatizovaného templatingu pre jednotlivé prípady, ale umožňuje rozšíriť systém o custom polia a workflow.

Audit, roly, multitenancy:

- *TheHive* má silnú podporu multitenantnosti, RBAC s rôznymi úrovňami (pozorovateľ, analytik, správca) a kompletný audit trail.
- *RTIR* ponúka prístupové úrovne, oddelenia, skupiny a veľmi detailný audit. Multitenancy je možné, ale ťažšie konfigurovateľné.

Integrácie a exporty:

- *TheHive* poskytuje REST API, webhooky, podporu pre integráciu so SIEM, CTI (MISP), Cortex, reporting. Exporty do CSV, PDF.
- *RTIR* podporuje integrácie cez REST API, CLI, skripty a pluginy. Exporty sú možné do CSV, základne aj do PDF.

Analýza kľúčových požiadaviek

- **Manažment prípadov a observables:** TheHive jednoznačne vyniká v správe observables a komplexných incidentov. RTIR drží krok najmä v štruktúrovaných workflow prípadoch.
- **Audit a záznam aktivít:** Oba nástroje poskytujú detailný audit. RTIR má výhodu v osvedčenej stabilite, TheHive v dynamike a vizualizácii.
- **Integrácie:** TheHive ponúka širšiu integráciu s bezpečnostnými nástrojmi ako CTI platformy a SOAR komponenty. RTIR je otvorený systém, ale vyžaduje väčšiu prácu pri integráciách.
- **Multitenantnosť:** TheHive ponúka pokročilejšie funkcie pre izoláciu viacerých tímov/zákazníkov.

Záver výberu

Na základe komplexnosti, flexibility a moderného prístupu je **TheHive** preferovaným riešením pre evidenciu a správu incidentov v prostredí SOCaaS. Poskytuje výborné možnosti integrácie, vizualizácie a workflow orientované na bezpečnostný kontext. **RTIR** zostáva vhodnou alternatívou pre organizácie, ktoré preferujú formálnu, stabilnú infraštruktúru s osvedčenými procesmi, alebo už využívajú RT ako core systém. Pre viaczákaznícke prostredie a škálovanie je však výhodnejší moderný, API-orientovaný a vizuálne prepracovaný nástroj ako TheHive.

3.7.3 Reportovanie

Úloha podkomponentu

Komponent reportovania v rámci SOCaaS architektúry slúži ako centrálny prostriedok na **agregáciu, vizualizáciu a distribúciu bezpečnostných informácií**. Jeho úlohou je zabezpečiť pravidelné aj ad-hoc výstupy o stave kybernetickej bezpečnosti pre rôzne cieľové skupiny – od SOC analytikov, cez vedúcich tímov, až po vedenie organizácie alebo klientov. Takýto reportovací systém musí pokrývať:

- Generovanie metriky incidentov, výstrah, SLA a KPIs,
- Prehľady trendov v čase a hodnotenie výkonnosti bezpečnostných opatrení,
- Prispôsobenie obsahu podľa úrovne detailu (technické vs. strategické),
- Automatizáciu a plánovanie distribúcie výstupov,
- Spätnú analýzu a archiváciu historických údajov.

Efektívne reportovanie má zásadný vplyv na **rozhodovanie, zodpovednosť, audit** aj **compliance** s reguláciami ako ISO 27001, GDPR či NIS2.

Posudzované riešenia

Pre túto oblasť sme posudzovali dva osvedčené open-source nástroje:

- **Kibana** – natívna súčasť Elastic Stacku,
- **Grafana** – všeobecná platforma pre vizualizáciu a monitoring z rôznych zdrojov.

Obidve riešenia majú silné komunity, široké možnosti integrácií a vysokú flexibilitu pri tvorbe vizualizácií.

Profily riešení

Kibana je navrhnutá priamo pre Elastic Stack a prirodzene sa integruje s Elasticsearch, Logstash, Beats, Wazuh a ďalšími komponentmi, ktoré sú bežné v SOC architektúrach. Ponúka bohatú sadu vizualizačných prvkov ako časové rady, heatmapy, metriky, grafy a pivot tabuľky. Je vhodná najmä pre analýzu logov, SIEM alertov, udalostí z Wazuh (XDR) či observables zo Threat Intel modulov.

Reportingový modul Kibany umožňuje generovať výstupy vo formátoch PDF a CSV, pričom s plateným X-Packom je možné plánovať a automatizovať odosielanie reportov (napr. e-mailom alebo webhookom). V open-source režime je možné túto funkcionalitu do určitej miery simulovať cez skripty alebo API. Rozhranie je responzívne, prehľadné a podporuje interaktívne filtrovanie. Kibana zároveň podporuje RBAC a auditovanie prístupov, čo je dôležité pri viacúrovňových tímoch.

Grafana je výnimočne flexibilná platforma pre tvorbu dashboardov z mnohých zdrojov vrátane Elasticsearch, Loki, InfluxDB, PostgreSQL, SQL API a ďalších. Umožňuje tvorbu veľmi atraktívnych vizualizácií vhodných pre manažérsky reporting. Vďaka širokému spektru pluginov (napr. Image Renderer, Reporting plugin) je možné plánovať a automatizovať export výstupov v PDF alebo PNG formáte. Grafana ponúka vynikajúcu personalizáciu vzhľadu, branding a embedovanie panelov, čo ju robí ideálnou pre prezentáciu výstupov klientom alebo vyššiemu vedeniu.

Napriek tomu však Grafana vyžaduje samostatnú prevádzku, konfiguráciu integrácií a nie je plne natívne previazaná s bezpečnostnými funkcionalitami ako SIEM, CTI, incident handling alebo XDR. To môže viesť k redundancii v integráciách a zvýšenej prevádzkovej náročnosti.

Podrobná analýza požiadaviek

Obe riešenia poskytujú široké možnosti vizualizácie a exportu údajov. Kibana je silnejšia v technických a analytických vizualizáciách bezpečnostných údajov – umožňuje efektívne pracovať s Elastic indexmi, logmi, SIEM alertmi aj Wazuh dátami. Navyše, umožňuje automatizovanú detekciu pomocou Elastic ML, prepojenie s observables z CTI modulov a detekčné pravidlá z Wazuhu. Plánovanie reportov a distribuovanie výsledkov je dostupné, aj keď niektoré funkcie (napr. plánovanie PDF exportov) sú viazané na komerčnú verziu.

Grafana vyniká vo vizuálnej kvalite dashboardov a možnosti prepojenia viacerých zdrojov do jedného panela – napríklad kombinácia SIEM alertov, SLA metriky a infra štatistík. Je výborne použiteľná pre SLA reporting a zjednodušený pohľad na incidenty z pohľadu klienta alebo vedenia. Jej výhodou je taktiež ľahké nasadenie a široká kompatibilita so štandardnými databázami.

Na druhej strane, Grafana nepodporuje nativne incident data model z Elasticu, nie je previazaná s detekčnými pravidlami alebo observables, a auditné logy sú menej komplexné. Tiež je menej optimalizovaná pre fulltextové analýzy bezpečnostných dát v reálnom čase.

Analýza kľúčových požiadaviek

Z hľadiska architektúry SOCaaS INNOSOC sú kľúčové tieto vlastnosti:

- **Priama integrácia so SIEM a XDR:** Keďže sme ako hlavný SIEM vybrali **Elastic Stack** a zároveň plánujeme používať **Wazuh ako XDR**, preferujeme riešenie, ktoré sa do tohto prostredia bez problémov zapojí. Kibana je v tomto prípade prirodzenou voľbou – využíva rovnaký dátový backend, umožňuje korelovanie logov, incidentov a IOC a poskytuje jednotný ekosystém.
- **Zabezpečenie a audit:** Kibana v kombinácii s Elastic Security poskytuje silnú RBAC logiku, kontrolu prístupov, logovanie činností a možnosť spätnej verifikácie každého exportu či interakcie. Pre viac-zákaznícke SOCaaS prostredie je toto kritická požiadavka.
- **Možnosť rozšírenia:** Elastic a Kibana podporujú ďalšie komponenty ako Uptime, APM, ML a Watcher – čo umožňuje vytvárať incident-aware a SLA-aware reporting na báze inteligentnej detekcie. To znižuje potrebu duplikácie dátových zdrojov.

Záver výberu

Hoci Grafana predstavuje silný nástroj pre generický vizualizačný reporting a SLA prehľady, v kontexte architektúry **Elastic Stack + Wazuh** je **Kibana** logickou a preferovanou voľbou pre komponent reportovania.

Jej silná natívna integrácia s bezpečnostnými dátami, možnosť tvorby incident-aware vizualizácií, podpora observables, korelácií a audit trailu spolu s modulmi Elastic SIEM a XDR (Wazuh) tvoria konzistentné, škálovateľné a technicky čisté riešenie.

Pre SOC analytikov poskytuje Kibana hlboký pohľad na incidenty, umožňuje spätnú analýzu a audit, zatiaľ čo pri vhodnej konfigurácii môže slúžiť aj na manažérsky a klientsky reporting. Preto v návrhu preferujeme **Kibanu ako primárny reportingový komponent pre SOCaaS platformu INNOSOC**.

3.7.4 Znalostný portál pre SOC tím

Úloha podkomponentu

Znalostný portál pre SOC tím je dôležitým stavebným kameňom každého moderného bezpečnostného operačného centra. Slúži ako **centrálny repozitár know-how, playbookov, postupov, odporúčaní, analytických návodov** a často aj historických lekcií (lessons learned) z incidentov. Znalostný portál:

- Zvyšuje **efektivitu a konzistentnosť reakcie** na incidenty,
- Umožňuje **rýchle zaškolenie nových členov tímu**,
- Podporuje **štandardizáciu procesov a metodík**,
- Umožňuje tímu uchovávať a zdieľať **overené postupy** a **vlastné analytické skúsenosti**,
- Posilňuje schopnosť **kolektívne sa učiť z incidentov** a budovať interné "threat intel" vedomosti.

V prostredí viacerých zákazníkov je tiež dôležité, aby portál podporoval viacúrovňové oprávnenia, históriu zmien, verzovanie dokumentov a prepojenie s ďalšími nástrojmi SOC (ticketing, incident management, CTI).

Posudzované riešenia

V tejto oblasti sme posudzovali open-source riešenia, ktoré sa bežne používajú ako **wiki systémy alebo knowledge base platformy**. Do porovnania sme zahrnuli:

- **BookStack** – moderný a ľahko ovládateľný nástroj štruktúrovaný okolo kníh a stránok,
- **Wiki.js** – výkonný, modularizovaný systém s podporou Markdown, Git, verzovania a širokej škály integrácií,
- **TheHive** – síce nie primárne znalostný portál, ale obsahuje niektoré komponenty pre prípadovú dokumentáciu a observables.

Profily riešení

BookStack je open-source nástroj postavený na Laravel frameworku, ktorý používa intuitívny model **kniha–kapitola–stránka**. Podporuje verzovanie dokumentov, pridávanie príloh, tvorbu šablón, hierarchickú organizáciu obsahu a RBAC na úrovni kníh aj používateľov. Výhodou je editor s podporou WYSIWYG aj Markdown. Umožňuje manuálne vkladanie obsahu, vytváranie návodov, zoznamov IOC, playbookov a technickej dokumentácie. Integrácia je možná cez REST API, podporovaný je aj export do PDF a Markdown.

Wiki.js je výkonný systém využívajúci moderný UI, databázu (napr. PostgreSQL, MongoDB), a backend s Node.js. Vyniká podporou **viacerých editorov (WYSIWYG, Markdown, Raw HTML)**, verzovaním, Git synchronizáciou a podporou workflow pre schvaľovanie dokumentov. Je modulárne rozšíriteľný (napr. PlantUML, Mermaid na kreslenie diagramov), má detailné oprávnenia a auditnú stopu. Integrácie sú možné cez REST API, webhooky a Git. Okrem dokumentácie je vhodný aj ako **firemná wiki pre SOC tím** so štruktúrovaným obsahom, prepojením s incidentmi alebo externými nástrojmi.

TheHive má určité prvky znalostného systému – umožňuje ukladať observables, reakčné šablóny a prípady. No jeho primárny účel je incident management. Neponúka modul na samostatnú správu štruktúrovanej dokumentácie alebo playbookov. Hodí sa skôr na "incident-centric" poznámky než na plnohodnotnú znalostnú databázu.

Podrobná analýza požiadaviek

V oblasti **správy obsahu** poskytujú BookStack aj Wiki.js plnú podporu na tvorbu dokumentov, editáciu, kategorizáciu, tagovanie a verzovanie. BookStack je jednoduchší na používanie, výborný pre tímových analytikov, ktorí potrebujú rýchlo vytvárať playbooky alebo návody. Wiki.js je robustnejší, vhodný na integráciu s vývojovým prostredím, s plnou synchronizáciou do Git repozitárov, čo umožňuje aj DevSecOps scenáre.

Vyhľadávanie je silnou stránkou Wiki.js, ktorý používa ElasticSearch alebo PostgreSQL fulltext, s podporou filtrov a kategórií. BookStack má jednoduchší, ale funkčný vyhľadávač. TheHive umožňuje hľadanie medzi observables a prípadoch, ale chýba systematická správa KB dokumentov.

Prepojenie s incidentmi je možné v oboch nástrojoch manuálne – napr. linkovaním ID incidentu alebo kategóriou. V prípade TheHive je prepojenie prirodzené, no opäť – chýba mu širší dokumentačný kontext (napr. aktualizovaný návod pre nový typ ransomvéru).

Export a bezpečnosť – BookStack aj Wiki.js umožňujú export do PDF, Markdown a HTML. Wiki.js umožňuje aj Git verziu každého článku. RBAC je podporované v oboch nástrojoch – detailne definovateľné na úrovni kníh, článkov, tímov alebo rolí. Audit zmien, história verzií a schvaľovacie workflowy sú dostupné najmä vo Wiki.js.

Analýza kľúčových požiadaviek

Znalostný portál musí byť:

- **Intuitívny a rýchly na používanie pre SOC analytikov** – BookStack je v tomto jednoduchší, ale dostatočne silný.
- **Dostatočne štruktúrovaný a technicky vyspelý** – Wiki.js umožňuje komplexnú správu obsahu, revízie, integrácie a bezpečnostné opatrenia.
- **Rozšíriteľný a integrovaný** – Wiki.js je lepšie pripravený pre prepojenie s ticketingom, incident managementom, CI/CD a dokumentačnými workflowmi.
- **Bezpečný a auditovateľný** – oba nástroje majú RBAC a históriu, ale Wiki.js poskytuje detailnejší prístup pre bezpečnostne kritické prostredie.

Záver výberu

Pre SOCaaS platformu INNOSOC odporúčame implementovať znalostný portál prostredníctvom **Wiki.js**. Tento nástroj poskytuje:

- Silnú podporu štruktúrovanej dokumentácie,
- Možnosť integrácie s existujúcimi nástrojmi (ticketing, CTI, Git),
- Bohatý ekosystém na tvorbu playbookov, príručiek, lessons learned a SOP,
- Pokročilé oprávnenia a workflow pre kontrolu obsahu.

BookStack môže byť vhodnou alternatívou v prípade potreby jednoduchšieho a menej technického riešenia. **TheHive** naďalej plní úlohu incident-centric databázy observables a prípadov, no nenahrádza potrebu samostatného znalostného systému.

Z pohľadu efektivity, škálovateľnosti a integrácie s ostatnými SOC komponentmi je **Wiki.js najvhodnejším kandidátom na znalostný portál pre SOC tím**.

ZÁVER A ODPORÚČANIA

Architektúra navrhovaného SOCaaS riešenia pre projekt INNOSOC sa opiera o sedem kľúčových technologických komponentov, ktoré pokrývajú celý cyklus činností moderného bezpečnostného operačného centra: od zberu, detekcie a obohatenia dát, cez ich analytické spracovanie, reakciu a dokumentáciu, až po spätnú analýzu a podporu znalostného manažmentu.

Zhrnutie preferovaných riešení:

- **SIEM:** Na základe komplexného posúdenia bol vybraný **Elastic Stack**, ktorý ponúka rozsiahlu funkcionalitu, škálovateľnosť, silnú komunitnú podporu a výkonnú integráciu so všetkými ostatnými komponentmi vrátane XDR, reportovania či incident managementu.
- **SOAR:** Ako najlepšia kombinácia funkcionality, rozšíriteľnosti a komunitnej podpory sa ukázala trojkombinácia **TheHive + Cortex + Shuffle**, ktorá umožňuje pokročilú správu incidentov, automatizáciu reakcií a tvorbu playbookov s vysokou mierou flexibility.
- **EDR/XDR:** Výsledné odporúčanie zahŕňa **Wazuh** ako základné EDR riešenie s natívnou integráciou do Elastic Stack a **Velociraptor** ako doplnok pre pokročilý forenzný zber údajov na koncových bodoch.
- **Skener zraniteľností:** Bol odporučený **Greenbone/OpenVAS**, ktorý poskytuje rozsiahle pokrytie zraniteľností, podporu štandardov SCAP a otvorenú architektúru vhodnú na multitenantné nasadenie.
- **CTI:** Najsilnejšiu funkcionalitu pre komplexné spracovanie CTI dát poskytuje **OpenCTI**. V kombinácii s **MISP** (na správu IOC) a **IntelMQ** (automatizovaný zber a feedy) tvorí robustný a škálovateľný CTI modul pre SOCaaS.
- **Inventarizácia aktív:** Ako najlepšia voľba z hľadiska funkcií, API podpory a integrácií sa ukázal **NetBox**, doplnený o **GLPI** pre CMDB funkcionalitu a **Ralph** pre správu životného cyklu aktív.
- **Incident handling:** Bolo preferované riešenie **TheHive** (pre incident manažment a tiketovanie), **Kibana** (pre reporting) a **Wiki.js** (ako znalostný portál). Táto zostava bola vybraná aj na základe previazanosti s ostatnými modulmi a možnosti integrácie cez REST API.

Odporúčania pre implementáciu:

- **Modularita a integrácia:** Všetky komponenty boli vyberané s dôrazom na otvorenú architektúru a API-first prístup, čo umožňuje ich flexibilné prepojenie. Dôležité je postaviť SIEM ako centrálny komponent (v tomto prípade Elastic Stack) a zabezpečiť napojenie všetkých ostatných častí.
- **Podpora automatizácie:** Komponenty ako Cortex, IntelMQ, Wazuh a Shuffle poskytujú možnosti low-code automatizácie a orchestrácie procesov, ktoré výrazne znižujú záťaž na tím analytikov.
- **Multitenantnosť a škálovateľnosť:** Všetky odporúčané nástroje umožňujú oddelenie prostredí, zákazníkov alebo organizačných jednotiek, čo je zásadné pre SOCaaS.
- **Dôraz na dokumentáciu a spätnú analýzu:** Kombinácia Wiki.js a Kibany zabezpečuje dokumentáciu postupov aj vizuálne prepojenie na incidenty, čo zvyšuje efektivitu tímov a znižuje čas potrebný na riešenie podobných incidentov v budúcnosti.

Dokument v tejto podobe predstavuje základnú technickú stratégiu pre návrh a výstavbu SOCaaS služby. Odporúčané komponenty sú osvedčené, open-source, a zároveň pokrývajú požiadavky na profesionálnu prevádzku, bezpečnosť a interoperabilitu.

ZOZNAM ZDROJOV

Primárne dokumentácie nástrojov:
SIEM nástroje:
1. Elastic Stack Documentation – https://www.elastic.co/guide/
2. Wazuh Documentation – https://documentation.wazuh.com/
3. OpenSearch Project – https://opensearch.org/docs/latest/
4. Graylog Documentation – https://docs.graylog.org/
5. SIEMonster Community Edition – https://siemonster.com/
6. AlienVault OSSIM – https://cybersecurity.att.com/products/ossim
7. Prelude OSS Documentation – https://github.com/preludeorg/

SOAR nástroje:
8. TheHive Project – https://docs.thehive-project.org/
9. Cortex – https://docs.thehive-project.org/cortex/
10. Shuffle – https://shuffler.io/docs
11. StackStorm Documentation – https://docs.stackstorm.com/
12. FIR (Fast Incident Response) – https://github.com/certsocietegenerale/FIR
13. Tracecat (ex-Kuiper) – https://github.com/FastenHealth/Tracecat

EDR/XDR nástroje:
14. Velociraptor Documentation – https://docs.velociraptor.app/
15. OpenEDR by Comodo – https://github.com/ComodoSecurity/openedr
16. Wazuh (EDR rozšírenie) – viď vyššie
17. OSSEC Documentation – https://www.ossec.net/docs/
18. Elastic Security (XDR) – viď Elastic dokumentácia vyššie

Vulnerability scanning:
19. Greenbone GVM (OpenVAS) – https://docs.greenbone.net/
20. OpenSCAP – https://www.open-scap.org/documentation/
21. Nikto – https://cirt.net/Nikto2
22. Nmap – https://nmap.org/book/

CTI nástroje:
23. OpenCTI Documentation – https://www.opencti.io/en/docs/
24. MISP Project – https://www.misp-project.org/documentation/
25. IntelMQ – https://certtools.github.io/intelmq/
26. Yeti CTI Platform – https://yeti-platform.github.io/
27. Vulmatch – https://github.com/vulmatch/vulmatch
28. Elastic Threat Intel module – viď Elastic dokumentácia

Asset inventory nástroje:
29. NetBox Documentation – https://netbox.dev/docs/
30. GLPI Project – https://glpi-project.org/
31. Ralph Documentation – https://ralph-ng.readthedocs.io/
32. LibreNMS – https://docs.librenms.org/
33. pi.Alert – https://github.com/pucherot/pi.alert

Incident handling / ticketing / reporting / knowledge base:
34. RTIR (Request Tracker for Incident Response) – https://bestpractical.com/rtir
35. Request Tracker (RT) – https://docs.bestpractical.com/rt/
36. osTicket – https://docs.osticket.com/
37. Zammad – https://docs.zammad.org/
38. Kibana (Elastic Reporting) – viď Elastic dokumentácia
39. Grafana – https://grafana.com/docs/
40. BookStack – https://www.bookstackapp.com/docs/
41. Wiki.js – https://docs.requarks.io/

Doplňujúce odborné zdroje:

1. 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
2. Bhat, M. A., & Kumar, P. (2022). *Advanced SIEM for Enhanced Threat Detection Using Machine Learning*. IEEE CSR. https://doi.org/10.1109/CSR54599.2022.9850371
3. Munoz, M., Garcia, C., & Valdes, J. J. (2023). *ML-based Optimization for SOC Event Triage*. ACM AI-CyberSec Workshop. https://doi.org/10.1145/3576888.3602857
4. Al-Shaer, E., et al. (2021). *Autonomic Security Operations: Challenges and Research Opportunities*. IEEE TDSC. https://doi.org/10.1109/TDSC.2021.3127814
5. Akinrolabu, O. A., et al. (2020). *Security Operations Centre: A systematic study and open challenges*. Computers & Security, 92. https://doi.org/10.1016/j.cose.2020.101747
6. Zografopoulos, I., et al. (2023). *Threat Intelligence Platforms: Evaluation and Future Directions*. Journal of Cybersecurity, 9(1).
7. Lefèvre, M., et al. (2022). *Toward Open Threat Intelligence Integration: Evaluation of MISP and OpenCTI*. NATO CyCon.
8. Tannenbaum, B., et al. (2025). *Enhancing EDR Capabilities in SOC Architectures Using Open Source Stack*. Proceedings of the IEEE EuroS&P 2025.
9. Kovačević, N., et al. (2025). *Multitenant Architecture for Scalable SOC-as-a-Service Using Elastic and Wazuh*. Journal of Network and Computer Applications. (vydanie marec 2025, doi pending)
10. Li, F., et al. (2025). *Knowledge Engineering for Cybersecurity: Integrating KBs into SOC Workflows*. ACM Transactions on Privacy and Security, 28(2).