Prípady použitia diagramy

UC_00 - Inicializácia a konfigurácia SOCaaS

Obrázok 2 : UC_00 - Inicializácia a konfigurácia SOCaaS

Prípad použitia	UC_00 - Inicializácia a konfigurácia SOCaaS
Cie¾	Use case popisuje prvotnú inicializáciu a nastavenie SOCaaS pre nového zákazníka. Zahŕňa aktiváciu logovacích zdrojov, nastavenie integračných bodov, dashboardov a základných bezpečnostných procesov.

Vstupná podmienka	Zákazník má vytvorený tenant.
Vstupná podmienka	Architekt má konfiguraèné oprávnenia.
Vstupná podmienka	
Výstupná podmienka	SOCaaS je úspešne inicializovaný a pripravený na monitorovanie a detekciu.
Výstupná podmienka	Aktivované sú základné moduly: logovanie, SIEM korelácie, dashboardy, incident management.
Výstupná podmienka	Logy zo všetkých povinných zdrojov obsahujú povinné polia pre detekciu.

Basic Path	Basic Path

Krok	**Aktivita**
1	Architekt spustí proces inicializácie pre nového zákazníka.
2	Systém naèíta profil zákazníka a pripraví konfiguraèné rozhranie.
3	
4	Systém vykoná inicializaèné úkony (registrácia zdrojov, aktivácia agentov, vytváranie dashboardov).
5	Architekt potvrdí konfiguráciu.
6	Systém uloží konfiguráciu a oznámi úspešné dokonèenie.

ALT_00_01 – Neúplný profil zákazníka	Alternate

Krok	**Aktivita**
1	Systém zistí chýbajúce údaje.
2	Upozorní architekta na doplnenie.
3	Proces pokraèuje po doplnení informácií.

ALT_00_02 – Nedostupné logovacie zdroje / infra	Alternate

Krok	**Aktivita**
1	
2	
3	Proces pokraèuje s obmedzenou funkcionalitou.

Prípad použitia	UC_00a - Overenie zákazníckeho profilu
Cie¾	Systém overí, či zákaznícky tenant obsahuje všetky povinné údaje (identifikačné, technické, integračné).

Vstupná podmienka	Tenant existuje v systéme.

Výstupná podmienka	Profil zákazníka je potvrdený ako kompletný.

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevádzkovate¾ platformy spustí overenie profilu.
2	Systém naèíta údaje zákazníka.
3	Systém skontroluje povinné polia.
4	Overenie je úspešné.

ALT_00a_01 – Neúplné údaje	Alternate

Krok	**Aktivita**
1	Systém vyžiada doplnenie chýbajúcich údajov

ALT_00a_02 – Tenantu chýba technická konfigurácia	Alternate

Krok	**Aktivita**
1	Systém zastaví proces a upozorní správcu.

Naviazané funkèné požiadavky	
FREQ_021 - Onboarding nového zákazníka	SOCaaS. To zahàòa: • nastavenie logovacieho agenta • konfiguráciu korelaèných pravidiel • vytvorenie separovaných dashboardov • nastavenie incident managementu pre zákazníka
Prípad použitia	UC_00b – Aktivácia logovacích agentov
Cie¾	Systém aktivuje logovacích agentov zákazníka pre odosielanie logov do SOCaaS.

Vstupná podmienka	Zákaznícke systémy sú dostupné.
Vstupná podmienka	Komunikaèné kanály sú otvorené.
Výstupná podmienka	Logovacie agenty sú aktívne a odosielajú dáta.

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevádzkovate¾ platformy spustí aktiváciu.
2	Systém kontaktuje logovacích agentov.
3	
4	Agenti sú aktivovaní.

ALT_00b_01 – Agent neodpovedá	Alternate

Krok	**Aktivita**
1	Systém oznámi chybu, pokraèuje neskôr.

ALT_00b_02 – Chybné API k¾úèe	Alternate

Krok	**Aktivita**
1	Systém vyžiada opätovné nahratie k¾úèov.

Naviazané funkèné požiadavky	
FREQ_008 - Centralizácia logov	
Prípad použitia	UC_00c – Nastavenie korelácií a dashboardov

Cie¾	Systém vytvorí preddefinované korelačné pravidlá a dashboardy pre monitoring bezpečnostných udalostí.

Vstupná podmienka	SIEM modul je aktívny.
Vstupná podmienka	Logy prichádzajú do systému.
Výstupná podmienka	Korelaèné pravidlá a dashboardy sú nakonfigurované.

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevádzkovate¾ platformy spustí nastavenie.
2	Systém naèíta template korelácií.
3	Systém vytvorí dashboardy pre monitorovanie.
4	Konfigurácia je uložená.

ALT_00c_02 –	Alternate

Krok	**Aktivita**
1	Systém vytvorí len minimálnu verziu. (poslednú spustite¾nú)

ALT_00c_01 – Korelaèné pravidlo je neplatné	Alternate

Krok	**Aktivita**
1	Systém ho preskoèí a nahlási chybu.

Naviazané funkèné požiadavky	
FREQ_001 - Proces monitorovania bezpeènostných udalostí	– zabezpeèuje zber a sledovanie logov, metrických údajov a alertov zo všetkých integrovaných systémov.
FREQ_006 - Proces reporting a vizualizácia	– zabezpeèuje pravidelný výstup pre manažment, audítorov a SOC analytikov.
Prípad použitia	UC_00d – Nastavenie incident managementu
Cie¾	Systém aktivuje workflow pre správu incidentov a priradenia rolí.

Vstupná podmienka	Ticketing alebo SOAR modul je inicializovaný.
Výstupná podmienka	Incident lifecycle (triage → analýza → uzavretie) je pripravený.

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevádzkovate¾ platformy spustí konfiguráciu.
2	Systém naèíta workflow šablóny.
3	Systém vytvorí incidentné kategórie a priority.
4	Priradí roly (Analytik, Operátor, Manažér).

ALT_00d_01 – Neexistujú roly používate¾ov	Alternate

Krok	**Aktivita**
1	Systém zastaví workflow a požiada správcu o pridanie rolí.

ALT_00d_02 – Ticketing modul je nedostupný	Alternate

Krok	**Aktivita**

1	Systém aktivuje len základný SOAR fallback.
Naviazané funkèné požiadavky	
FREQ_004 - Proces správy incidentov	– zahàòa evidenciu, klasifikáciu, priraïovanie priorít, dokumentovanie a uzatváranie incidentov.

Obrázok Diagram Sequence : UC_01 - Monitorovať bezpečnostné udalosti

Prípad použitia	
Cie¾	Use case opisuje nepretržité monitorovanie bezpečnostných udalostí v rámci SOCaaS. Zahŕňa zber udalostí, ich normalizáciu, obohacovanie a prípravu alertov pre následný proces detekcie incidentov.

Vstupná podmienka	Logovacie agenty sú aktívne.
Vstupná podmienka	SIEM modul SOCaaS je funkèný.
Vstupná podmienka	UC_00 (inicializácia) bol úspešne dokonèený.
Výstupná podmienka	Udalosti sú spracované a posunuté do procesu detekcie incidentov.
Výstupná podmienka	Alerty sú zobrazené operátorovi.
Výstupná podmienka	Monitoring beží v reálnom èase.

Basic Path		Basic Path
Krok	**Aktivita**	
1	Operátor sleduje riadiaci dashboard v SOCaaS.	
2	UC_01a: Systém prijíma udalosti z logovacích zdrojov.	
3	UC_01b: Systém normalizuje a obohacuje dáta.	
4	UC_01c: Systém ukladané údaje indexuje pre rýchle vyh¾adávanie.	
5	SOCaaS generuje alerty na základe korelaèných pravidiel.	
6	Operátor vidí výsledné bezpeènostné udalosti.	
7	Use case konèí, monitoring pokraèuje bez obmedzenia. Operátor vyhodnotí alert.	
8	Ak je kritický →	
9	Use Case konèí – monitoring pokraèuje ïalej.	
ALT_01_01 – Nedostupné logy alebo agenti		Exception
Krok	**Aktivita**	
1	SOCaaS nedostáva dáta zo zdroja.	
2	Systém vytvorí „Missing logs“ alert.	
3		
ALT_01_02 –		Exception
Krok	**Aktivita**	
1		
2	Systém zapne ochranné mechanizmy (rate-limiting, buffering).	

3	Operátor je upozornený o riziku straty udalostí.
Naviazané funkèné požiadavky	
FREQ_001 - Proces monitorovania bezpeènostných udalostí	– zabezpeèuje zber a sledovanie logov, metrických údajov a alertov zo všetkých integrovaných systémov.
Prípad použitia	UC_01a - Zber logov
Cie¾	Zabezpečuje technický príjem logovacích dát zo systémov, aplikácií, zariadení a zdrojov do SIEM platformy. Je základom monitorovacieho procesu.

Vstupná podmienka	Komunikaèný kanál medzi systémom a agentom je funkèný.
Vstupná podmienka	Logovací agent je aktívny.
Výstupná podmienka	Logy sú pripravené na ïalší krok – normalizáciu.
Výstupná podmienka	SOCaaS prijal nové logy.
Basic Path	Basic Path

Krok	**Aktivita**
1	Logovací agent odosiela bezpeènostné udalosti.
2	SOCaaS prijme dáta.
3	Overí sa formát a integrita logov.
4	Logy sú odovzdané do procesu normalizácie.

ALT_01a_01 – Logy sa nedoruèujú	Alternate

Krok	**Aktivita**
1	SOCaaS nezaznamená žiadne dáta zo zdroja.
2	Systém vytvorí „Missing logs“ upozornenie.
3	Správca dostane notifikáciu.

ALT_01a_02 – Nevalidný formát logu	Alternate

Krok	**Aktivita**
1	Log má chybný formát alebo chýbajúce polia.
2	SOCaaS ho odmietne a uloží do quarantine bufferu.
3	Notifikácia sa pošle integrátorovi.

Naviazané funkèné požiadavky	
FREQ_008 - Centralizácia logov	
Prípad použitia	UC_01b – Normalizácia a obohacovanie údajov
Cie¾	Use case zabezpečuje normalizáciu logov do jednotného formátu a obohacovanie informáciami z CTI, asset databázy alebo užívateľských údajov.

Vstupná podmienka	Existuje konfigurácia normalizaèných pravidiel.
Vstupná podmienka	UC_01a (zber logov) bol úspešný.
Výstupná podmienka	Log je normalizovaný a obohatený.
Výstupná podmienka	Dáta sú pripravené na uloženie a indexáciu.
Basic Path	Basic Path

Krok	**Aktivita**
1	SOCaaS naèíta prijaté logy.

2	Použije sa normalizaèný profil pod¾a typu zdroja.
3	Obohatenie dát (IP reputácia, hostname, používate¾).
4	Výsledný event je pripravený pre indexáciu.

ALT_01a_01 – Neznámy typ logu	Alternate

Krok	**Aktivita**
1	Systém použije fallback normalizaèný profil.

ALT_01a_02 – Chýba CTI feed	Alternate

Krok	**Aktivita**
1	Systém vykoná normalizáciu bez obohatenia a oznaèí event ako „unenriched“.

Naviazané funkèné požiadavky	
FREQ_009 - Normalizácia a obohacovanie údajov	

Prípad použitia	UC_01c – Indexácia a ukladanie údajov
Cie¾	Use case sa stará o uloženie normalizovaných bezpečnostných udalostí do úložiska a ich indexáciu pre rýchle vyhľadávanie a korelačné mechanizmy.

Vstupná podmienka	Normalizácia dát (UC_01b) je dokonèená.
Vstupná podmienka	Úložisko a cluster sú dostupné.
Výstupná podmienka	Udalosti sú uložené v SIEM databáze.
Výstupná podmienka	Indexy sú pripravené pre query systémy.

Basic Path	Basic Path

Krok	**Aktivita**
1	Systém prevezme normalizované dáta.
2	Zapíše ich do úložiska (DB alebo distrib. index).
3	Vytvorí/aktualizuje indexy.
4	Event je k dispozícii pre korelaèné pravidlá.

ALT_01c_01 – Úložisko nedostupné	Alternate

Krok	**Aktivita**
1	Systém uloží dáta do bufferu a vytvorí alert.

ALT_01c_02 – Vyèerpanie úložného priestoru	Alternate

Krok	**Aktivita**
1	Systém aktivuje cleanup alebo alertuje prevádzku.

Naviazané funkèné požiadavky	
FREQ_010 - Ukladanie a indexovanie údajov	

Obrázok Diagram Sequence : UC_02 - Vizualizovať a reportovať bezpečnostné údaje

Prípad použitia	UC_02 –
Cie¾	Systém umožňuje SOC operátorom a správcovi zobrazovať bezpečnostné udalosti pomocou dashboardov, filtrov, grafov a tabuľkových výstupov. Umožňuje tiež generovanie reportov a export dát pre manažment, audit alebo zákazníkov.

Vstupná podmienka	Dashboardy sú definované v konfigurácii (UC_00c).
Vstupná podmienka	UC_01c – Dáta sú indexované a dostupné pre vizualizáciu.
Vstupná podmienka	UC_01 – Monitorovanie beží a poskytuje dáta.
Výstupná podmienka	Aktivita je zaznamenaná v audit logu.
Výstupná podmienka	Report bol vygenerovaný alebo exportovaný (ak bolo iniciované).
Výstupná podmienka	Používate¾ vidí aktualizované vizualizácie.

Basic Path	Basic Path

Krok	**Aktivita**
1	Aktér otvorí modul „Vizualizácia a reporting“.
2	Systém naèíta dostupné dashboardy a reporty pod¾a role aktéra.
3	Aktér otvorí dashboard → systém zobrazí grafy, metriky, tabu¾ky.
4	
5	
6	Systém zostaví report pod¾a vybraného formátu a šablóny.
7	

ALT_02_01 – Nedostupné dáta	Alternate

Krok	**Aktivita**
1	Dashboard vráti prázdny dataset.
2	Systém zobrazí varovanie.
3	

ALT_02_02 – Chybné oprávnenia	Alternate

Krok	**Aktivita**
1	Aktér (napr. Prevádzkovate¾) otvorí dashboard mimo jeho tenantu.
2	Systém zobrazí chybu „Nedostatoèné oprávnenia“.

ALT_02_03 – Generovanie reportu zlyhalo	Alternate

Krok	**Aktivita**
1	Zobrazí chybové hlásenie.
2	Uloží chybu do audit logu.
3	Aktér (napr. Prevádzkovate¾) otvorí dashboard mimo jeho tenantu.

Naviazané funkèné požiadavky	
FREQ_006 - Proces reporting a vizualizácia	– zabezpeèuje pravidelný výstup pre manažment, audítorov a SOC analytikov.

Prípad použitia	UC_02a –
Cie¾	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.

Vstupná podmienka	Systém je inicializovaný a nakonfigurovaný (UC_00).
Vstupná podmienka	Všetky zdroje logov sú aktívne a dáta sú prijímané (UC_01).
Vstupná podmienka	Používate¾ je autentifikovaný a má rolu umožòujúcu zobrazenie dashboardov.
Výstupná podmienka	Dashboard bol zobrazený s aktuálnymi dátami.
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	Aktér otvorí modul Dashboardov.
2	Systém naèíta dostupné dashboardy pod¾a roly.
3	Aktér vyberie dashboard na zobrazenie.
4	Systém naèíta a zrenderuje vizualizácie (grafy, heatmapy, tabu¾ky).
5	Systém aktualizuje vizualizácie v reálnom èase alebo v definovaných intervaloch.

ALT_02a_02 – Používate¾ nemá oprávnenie na konkrétny dashboard	Alternate

Krok	**Aktivita**
1	Systém skryje dashboard alebo zobrazí „Access Denied“.
2	

ALT_02a_01 – Nenaèítajú sa dáta	Alternate

Krok	**Aktivita**
1	
2	Namiesto grafov zobrazí správu: „Dáta nie sú dostupné.“
3	

Naviazané funkèné požiadavky	
FREQ_012 - Vizualizácia výstupov	
FREQ_032 - Štruktúra dashboardov	abu¾ky, heatmapy, distribuèné histogramy, metriky alebo mapy. Každý dashboard v rámci SOCaaS je navrhnutý ako kompozícia týchto vizualizácií zameraná na konkrétny aspekt monitorovania alebo analýzy. Preh¾ad systémovej bezpeènosti Korelaèné a incidentové dashboardy Monitorovanie autentifikácií a správania používate¾ov Integrovaný preh¾ad pre SOC analytika

FREQ_031 - Návrh dashboardov	rstiev nasledovne: 1. Globálne preh¾ady (SOC Overview) Urèené pre manažment a SLA reporting – zahàòajú denné/mìsíèné štatistiky incidentov, typy hrozieb, top 10 IP adries, krajiny pôvodu útokov, èas vyriešenia ticketov. 2. Alert monitoring dashboardy Zamerané na operatívny monitoring – zobrazujú nové alerty, rozdelenie pod¾a severity (Critical, High, Medium), èasové trendy, a korelácie medzi viacerými zdrojmi. 3. Tematické dashboardy Pokrývajú špecifické oblasti: • EDR aktivity: zaznamenané súbory, procesy, pokusy o exekúciu škodlivého kódu. • Zranite¾nosti a skeny: výsledky z Greenbone alebo OpenSCAP. • 4. Detailné analytické dashboardy – Slúžia pre L2 analytikov a threat hunting. Obsahujú heatmapy, èasové rezy, distribúcie pod¾a hodín, krajín, ASN, výskyt IOC a podobne. 5. Ad-hoc a incident-specific dashboardy – Vznikajú poèas vyšetrovania konkrétneho prípadu, kde si analytik zostaví vlastnú vizualizáciu na základe dát z Elasticsearch.
Prípad použitia	UC_02b –
Cie¾	Používateľ vytvorí jednorazový report alebo uloží reportovaciu šablónu založenú na dátach z dashboardov alebo udalostí.

Vstupná podmienka	Dashboardy sú dostupné a dáta sú indexované (UC_01).
Vstupná podmienka	Používate¾ má oprávnenie „Create Report“.
Výstupná podmienka	Report je uložený v systéme.
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	Aktér otvorí modul Reportov.
2	
3	Vyberie: typ reportu, èasový rozsah, šablónu alebo vlastný dizajn.
4	Systém naèíta potrebné dáta.
5	Používate¾ potvrdí generovanie.
6	Systém vygeneruje report a uloží ho do databázy reportov.

ALT_02b_02 – Nedostupné dáta pre report	Alternate

Krok	**Aktivita**
1	Systém zobrazí hlásenie „Dáta pre vybrané obdobie nie sú dostupné“.
2	Operátor, Prevádkovate¾ alebo Správca zvolí iné obdobie.

ALT_02b_01 – Nevalidný parameter reportu	Alternate

Krok	**Aktivita**
1	Systém zistí chýbajúci parameter (èasové obdobie, zdroj dát...).
2	Zobrazí chybu a vyžiada doplnenie.

Naviazané funkène požiadavky

FREQ_033 - Reporting	• Prevádzkový preh¾ad – zobrazenie stavu systémov, poètu incidentov, aktivity agentov. • Bezpeènostný reporting – výstupy o detekovaných hrozbách, typoch útokov, trendoch. • Compliance reporting – reporty pod¾a regulatórnych požiadaviek (napr. GDPR, NIS2). • Manažérsky reporting – agregované štatistiky a ukazovatele pre vedenie organizácie. • Zákaznícky reporting – individuálne preh¾ady pre jednotlivých klientov multitenantného SOCaaS.
Prípad použitia	UC_02c –
Cie¾	Používateľ exportuje existujúci report do PDF, CSV, JSON alebo PNG a môže ho odoslať emailom alebo webhookom.

Vstupná podmienka	Existuje vygenerovaný report (UC_02b).
Vstupná podmienka	Používate¾ má práva „Export Report“.
Výstupná podmienka	Systém vytvoril súbor vo zvolenom formáte.
Výstupná podmienka	Súbor bol stiahnutý alebo odoslaný na externý endpoint.

Basic Path	Basic Path

Krok	**Aktivita**
1	Používate¾ otvorí detail reportu.
2	
3	Vyberie formát (PDF/CSV/JSON/PNG).
4	Systém vygeneruje export.
5	Súbor sa stiahne alebo odošle pod¾a nastavenia.

ALT_02c_02 – Nedostatoèné oprávnenia	Alternate

Krok	**Aktivita**
1	Systém zobrazí „Access Denied“.
2	

ALT_02c_01 – Export zlyhá (timeout, ve¾ký dataset)	Alternate

Krok	**Aktivita**
1	Systém oznámi chybu exportu.
2	Ponúkne offline export alebo rozdelenie dát.

Naviazané funkèné požiadavky	
FREQ_034 - Manuálny export reportov	• 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 ïalšie spracovanie.
FREQ_165 - Podpora exportu do PDF, CSV, JSON	
	-mail, webhook)

Obrázok Diagram Sequence : UC_03 - Spravovať detekčné a korelačné pravidlá

Prípad použitia	
Cie¾	Tento use case pokrýva aktivity analytikov a správcov pri tvorbe, správe a údržbe detekčných a korelačných pravidiel v prostredí SOCaaS. Tieto pravidlá umožňujú detekciu bezpečnostných hrozieb na základe IOC, behaviorálnych anomálií, reťazenia udalostí alebo prahových hodnôt. Use case sa zameriava výlučne na proces správy pravidiel – ich definovanie, ladenie, klasifikáciu a mapovanie na bezpečnostné rámce (napr. MITRE ATT&CK).

Vstupná podmienka	Aktéri majú prístup do administraèného rozhrania na tvorbu pravidiel.
Vstupná podmienka	Systém podporuje definovanie, správu a verzovanie detekèných pravidiel.
Výstupná podmienka	Nové pravidlo je vytvorené alebo existujúce pravidlo je upravené, deaktivované alebo vymazané.
Výstupná podmienka	Pravidlo je verzované, validované a pripravené na nasadenie do produkèného prostredia.
Výstupná podmienka	Pravidlo je dostupné na vyhodnocovanie bezpeènostných udalostí (UC_04).

Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik alebo správca otvorí rozhranie pre správu detekèných pravidiel.
2	Vytvorí nové pravidlo alebo vyh¾adá existujúce.
3	Definuje podmienky: typ udalosti, IOC/indikátor, frekvencia výskytu, zdrojové/destinované entity,
4	
5	Pravidlo je uložené a verzované.
6	
7	

ALT_03_01 – Pravidlo sa testuje na historických dátach (debugging)	Alternate

Krok	**Aktivita**
1	Analytik použije nástroj na testovanie pravidiel voèi historickým logom.
2	Výsledky sa zobrazia, pravidlo sa následne upraví alebo schváli.

ALT_03_02 – Pravidlo sa vytvorí cez no-code rozhranie	Alternate

Krok	**Aktivita**
1	Analytik použije vizuálne rozhranie (drag & drop) na vytvorenie podmienok bez písania syntaxe.
2	Platforma automaticky vytvorí podkladový kód pravidla.

Naviazané funkèné požiadavky

FREQ_029 - Korelaèné pravidlá a detekcia hrozieb	• Alerty na základné IOC – porovnanie s databázou známych indikátorov (IP, URL, hash). • Anomálne správanie používate¾ov – napr. viacnásobné neúspešné prihlásenie v krátkom èase, login z nového geografického regiónu. •– napr. DNS dotazy na dynamicky generované domény (DGA), odchýlky v èase a objeme dát. • Aktivity s administratívnymi právami – napr. pridanie používate¾a do skupiny „Administrators“, zmeny ACL, spustenie netsh, powershell. •– korelácia medzi viacerými logmi v èase: napr. login ? súborový prenos ? spustenie škodlivého procesu. Tieto pravidlá budú spravované, kde možno: • • • •objekty.
FREQ_045 - Vlastné alertovacie pravidlá a prahy	
FREQ_041 - Korelácia udalostí	
FREQ_050 - Podpora pre MITRE ATT&CK mapovanie	
FREQ_011 - Tvorba korelaèných pravidiel	

UC_04 –

Obrázok Diagram Sequence : UC_04 – Upozorniť a eskalovať bezpečnostný incident

Prípad použitia	UC_04 –
Cie¾	Po tom, ako systém deteguje a založí bezpečnostný incident (UC_01, UC_03), je cieľom UC_04 zabezpečiť, aby sa o ňom včas dozvedol správny človek (1st level), aby incident niekto prevzal a aby sa pri nečinnosti alebo zhoršení závažnosti incident automaticky posunul na vyššiu úroveň

Vstupná podmienka	Existuje incident –
Vstupná podmienka	Sú nastavené notifikaèné a eskalaèné politiky
Vstupná podmienka	Sú známe kontaktné kanály a on-call rozpis
Výstupná podmienka	Relevantný príjemca bol notifikovaný
Výstupná podmienka	Incident má zaznamenanú históriu notifikácií/escalácií
Výstupná podmienka	V prípade neèinnosti prebehla eskalácia pod¾a SLA

Basic Path	Basic Path

Krok	**Aktivita**
1	Vznik alebo zmena incidentu
2	Vyhodnotenie notifikaènej politiky
3	Výber primárnych príjemcov
4	Generovanie notifikaènej správy
5	Odoslanie notifikácie primárnymi kanálmi
6	Èakanie na potvrdenie (acknowledgement)

7	Potvrdenie incidentu Analytikom/Operátorom
8	Zastavenie ïalšej eskalácie
9	Aktualizácia histórie incidentu

ALT_01 – Zlyhanie primárneho notifikaèného kanála	Alternate

Krok	**Aktivita**
1	Odoslanie notifikácie zlyhá (napr. e-mail server nedostupný).
2	Systém automaticky vyskúša alternatívny kanál (napr. SMS, iný mailový gateway, chat).
3	Do histórie incidentu sa zaznamená neúspešný pokus aj následný fallback.
4	Ak všetky kanály zlyhajú, incident dostane príznak „notifikácia neúspešná“ a systém automaticky vytvorí interný ticket pre správcu infraštruktúry.

ALT_02 - Incident nie je v SLA èase potvrdený - eskalácia	Alternate

Krok	**Aktivita**
1	Po uplynutí SLA intervalu nedošlo k potvrdeniu incidentu.
2	Systém automaticky eskaluje incident na vyššiu úroveò (Manažér, Vedúci SOC): zvýšenie priority / závažnosti incidentu, odoslanie eskalaènej notifikácie Manažérovi cez jeho preferované kanály.
3	Do histórie incidentu sa pridá záznam o neprevzatí v SLA a o vykonanej eskalácii.
4	Volite¾ne sa spustí ïalší playbook (napr. èiastoèné automatizované opatrenia, predpripravené akcie).

Naviazané funkèné požiadavky	
	a incident ticketov
FREQ_128 - Upozornenia na zmenu stavu, expirácie, servisné intervaly	Automatické notifikácie pri zmene stavu alebo potrebe servisného zásahu. Upozornenia na zmenu stavu, expirácie, servisné intervaly
FREQ_056 - Kategorizácia a prioritizácia incidentov	
FREQ_015 - Ticketovací systém a incident manažment	ledovanie riešenia.
FREQ_003 - Proces reakcie na incidenty	– definuje spôsob, akým tím reaguje na identifikované incidenty. Zahàòa eskaláciu, priradenie zodpovednosti, vykonanie opatrení, ako aj komunikáciu so zasiahnutými stranami.

UC_05 –

Obrázok Diagram Sequence : UC_05 – Riešiť a uzatvoriť bezpečnostný incident

Prípad použitia	UC_05 –
Cie¾	Po detekcii incidentu a odoslaní upozornení (UC_01, UC_03, UC_04) tento UC pokrýva celý proces riešenia incidentu – od prevzatia, analýzy a realizácie nápravných opatrení až po uzatvorenie incidentu a kompletné zdokumentovanie jeho priebehu (časová os, dôkazy, prepojené prípady). Výsledkom je incident, ktorý má jasného vlastníka, realizované kroky, zaznamenané časy a pripravené podklady pre prípadné „poučenie“

Vstupná podmienka	Incident je založený a notifikovaný
Vstupná podmienka	Incident má priradeného vlastníka / tím
Vstupná podmienka	Dostupné sú relevantné dáta a logy

Výstupná podmienka	Incident má zdokumentovaný priebeh a výsledok
Výstupná podmienka	Bol vykonaný dohodnutý súbor nápravných opatrení
Výstupná podmienka	Incident je uzatvorený alebo preklasifikovaný

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevzatie incidentu Analytikom
2	Zber a doplnenie dôkazov
3	Analýza a identifikácia príèin
4	Návrh nápravných opatrení
5	Realizácia opatrení Správcom
6	Sledovanie èasov a priebehu riešenia
7	Kontrola a schválenie výsledku
8	Uzatvorenie incidentu
9	Príprava podkladov pre pouèenie

ALT_ 01 – Incident je vyhodnotený ako false positive	Alternate

Krok	**Aktivita**
1	Po analýze Analytik zistí, že incident nevznikol (nesprávna korelácia, testovací traffic).
2	Analytik aktualizuje incident na stav „false positive“ a struène zdokumentuje dôvod.
3	Incident je uzatvorený, ale zostáva v histórii vrátane dôkazov –

ALT_02 –	Alternate

Krok	**Aktivita**
1	Správca zistí, že navrhované opatrenie má vysoký dopad na prevádzku (napr. odstavenie kritickej služby).
2	
3	Incident zostáva v stave „otvorený – èaká na plánované opatrenia“ s evidovanými èasmi a rizikom.

Prípad použitia	UC_05a –
Cie¾	Analytik detailne preskúma incident – pozrie si časovú os udalostí, logy, IOC, doplní dôkazy a vytvorí ucelený obraz o príčine a rozsahu incidentu.

Vstupná podmienka	Incident je založený a priradený Analytikovi.
Vstupná podmienka	K incidentu sú dostupné základné logy a udalosti z monitorovacieho systému.
Výstupná podmienka	Incident obsahuje doplnené dôkazy (logy, prílohy, IOC).
Výstupná podmienka	Je popísaná predbežná príèina incidentu a rozsah dopadu.

Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik otvorí detail incidentu.
2	Zobrazí si èasovú os súvisiacich udalostí a logov.
3	Identifikuje podozrivé udalosti a indikátory kompromitácie.
4	Stiahne alebo si vyžiada doplòujúce logy/prílohy a pripojí ich k incidentu.
5	Na základe zhromaždených dát popíše predbežnú príèinu a rozsah incidentu.

6	Aktualizuje prioritu incidentu, ak je to potrebné.

ALT_01 – Nedostupné alebo neúplné logy	Alternate

Krok	**Aktivita**
1	Analytik zistí, že logy sú neúplné alebo chýbajú; v incidente založí úlohu pre Správcu na nápravu (dopnutie logovania, export zo zdrojového systému) a ïalej pracuje s tým, èo má k dispozícii.

ALT_02 – Incident sa ukáže ako false positive	Alternate

Krok	**Aktivita**
1	Analytik po analýze vyhodnotí, že nejde o skutoèný incident; incident oznaèí ako „false positive“, struène zdokumentuje dôvod a UC_05 sa ukonèí.

Naviazané funkèné požiadavky	
FREQ_133 - Pridávanie príloh	ov)
	ia, uzavretie)
Prípad použitia	UC_05b –
Cie¾	Analytik a Správca vytvárajú, priraďujú a sledujú úlohy, ktoré predstavujú konkrétne nápravné alebo preventívne opatrenia súvisiace s incidentom.

Vstupná podmienka	K incidentu existuje základná analýza (UC_05a).
Vstupná podmienka	Je jasné, aké systémy alebo služby incident ovplyvòuje.
Výstupná podmienka	Incident má vytvorený zoznam úloh s priradenými zodpovednými osobami a termínmi.
Výstupná podmienka	Stav jednotlivých úloh odráža reálny priebeh riešenia (plánované, v riešení, hotové).

Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik na základe analýzy navrhne konkrétne nápravné opatrenia.
2	V incidente vytvorí úlohy a priradí ich konkrétnym Správcom alebo tímom.
3	Ku každej úlohe nastaví prioritu a termín.
4	Správcovia priebežne aktualizujú stav úloh pod¾a realizácie opatrení.
5	Systém zaznamenáva èasy vytvorenia, zaèiatku a dokonèenia úloh.
6	Analytik sleduje stav úloh a pod¾a potreby pripomína alebo eskaluje oneskorené úlohy.
7	Po dokonèení k¾úèových úloh aktualizuje Analytik stav incidentu.

ALT_01 – Úloha má vysoký dopad na prevádzku	Alternate

Krok	**Aktivita**
1	zamietne s komentárom.

ALT_02 – Úloha nie je realizovate¾ná v plánovanom termíne	Alternate

Krok	**Aktivita**
1	Správca aktualizuje termín a dôvod v úlohe; Analytik pod¾a potreby upraví prioritu incidentu alebo informuje Manažéra.

Naviazané funkèné požiadavky

FREQ_144 - Tvorba a správa prípadov - cases s úlohami a detailmi	

Prípad použitia	UC_05c –
Cie¾	Po vykonaní nápravných opatrení Analytik (príp. Manažér) rozhodne o finálnom stave incidentu, zdokumentuje záver a prepojí incident s inými súvisiacimi prípadmi.

Vstupná podmienka	K¾úèové úlohy incidentu sú dokonèené alebo je rozhodnuté o akceptovaní zostávajúceho rizika.
Vstupná podmienka	Monitoring neukazuje pretrvávajúce indikátory útoku alebo je ich výskyt vysvetlený.
Výstupná podmienka	
Výstupná podmienka	Incident je prepojený s ïalšími relevantnými incidentmi/prípadmi alebo kampaòami, ak existujú.

Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik skontroluje, že všetky dôležité úlohy sú dokonèené a systémy sú stabilné.
2	Overí v monitoringu, že sa neobjavujú nové súvisiace udalosti.
3	
4	Vyplní závereèné zhrnutie: príèina, dopad, vykonané opatrenia.
5	Nastaví finálny stav incidentu (napr. „uzatvorený“).
6	Pri kritických incidentoch požiada Manažéra o schválenie uzatvorenia.
7	Incident sa presunie do archívu a je pripravený pre proces „lessons learned“.

ALT_01 – Zistené nové súvisiace udalosti pri uzatváraní	Alternate

Krok	**Aktivita**
1	b.

ALT_02 –	Alternate

Krok	**Aktivita**
1	Analytik identifikuje, že incident patrí do väèšej kampane; nastaví ho ako podriadený k nadradenému prípadu a upraví závereèné zhrnutie.

Naviazané funkèné požiadavky	
FREQ_146 - Prepojenie medzi prípadmi na základe spoloèných indikátorov	Automatická alebo manuálna identifikácia súvisiacich incidentov. Prepojenie medzi prípadmi na základe spoloèných indikátorov

UC_06 –

Obrázok Diagram Sequence : UC_06 – Vyhodnotiť incidenty a zlepšiť detekciu aj povedomiel

Prípad použitia	UC_06 –

Cie¾	Po vyriešení a uzatvorení incidentu (UC_05) tento UC zabezpečuje, aby sa z incidentu systém aj ľudia poučili: incident sa zhodnotí (post-incident / post-mortem), zistenia sa premietnu do úprav detekčných pravidiel a ML modelov, pripraví sa alebo aktualizuje školenie / usmernenie pre zamestnancov.

Vstupná podmienka	Incident je uzatvorený
Vstupná podmienka	Sú dostupné údaje o incidente
Vstupná podmienka	Existuje aspoò základný proces „lessons learned“
Výstupná podmienka	Incident má spracovaný záznam „lessons learned“
Výstupná podmienka	Sú navrhnuté alebo vykonané úpravy detekcie/ML
Výstupná podmienka	Je pripravené alebo aktualizované školenie / guidance pre používate¾ov

Basic Path	Basic Path

Krok	**Aktivita**
1	Výber incidentov na vyhodnotenie
2	Príprava podkladov na vyhodnotenie
3	Post-incident meeting / hodnotenie
4	Zápis lessons learned a odporúèaní
5	Návrh úprav detekcie a ML modelov
6	modelu pri anomáliách) a tieto zistenia zahrnie do návrhu úprav.
7	Záznam v znalostnej báze je prelinkovaný s konkrétnym incidentom (resp. typom útoku), aby sa dal pri podobných prípadoch rýchlo
8	Výstupy sú uložené v znalostnom portáli / knowledge base a komunikované relevantným ¾uïom.
9	Schva¾ovanie a plánovanie nasadenia zmien
10	Príprava školenia / awareness materiálov
11	Distribúcia poznatkov
12	Záver UC

ALT_01 – Nedostatok dát na kvalitné vyhodnotenie	Alternate

Krok	**Aktivita**
1	Pri analýze sa ukáže, že nie sú dostupné všetky potrebné logy alebo historické údaje; tím síce spraví základné lessons learned, ale zároveò vytvorí úlohy na zlepšenie logovania a zberu dát do budúcna.

ALT_02 – Návrh úprav detekcie/ML sa zamietne	Alternate

Krok	**Aktivita**
1	Data Scientist alebo Developer pripravia návrh zmien, ale Manažér ich na základe rizík alebo nákladov neschváli; odporúèania sa uložia v knowledge base a zmeny sa prípadne prehodnotia neskôr.

ALT_03 – Identifikovaná potreba cieleneho školenia zamestnancov	Alternate

Krok	**Aktivita**
1	neho školenia, ktoré je priradené vybranej skupine používate¾ov.

Naviazané funkèné požiadavky	
FREQ_016 - Znalostný portál	ov.
FREQ_176 - Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	rétnymi incidentmi alebo typmi útokov
FREQ_007 - Proces správy poznatkov	– zabezpeèuje udržiavanie znalostnej bázy playbookov, dokumentácie a odporúèaných reakcií.
	ie bez oh¾adu na triedu. Vyhodnotenie celkovej presnosti pomocou metrík ako Precision, Recall, F1-score alebo AUC-ROC.
FREQ_026 - Tvorba znalostnej bázy	• incident summary + lessons learned • zápis v znalostnom portáli • kategorizácia pod¾a MITRE ATT&CK a dátumov

UC_07 –

Obrázok Diagram Sequence : UC_07 – Automatizovať reakciu na incident

Prípad použitia	UC_07 –
Cie¾	UC_07 rieši situáciu, keď je incident už detegovaný a v riešení (UC_05), ale namiesto čisto manuálnych krokov sa použijú automatizované alebo poloautomatizované playbooky. Systém na základe typu incidentu a TTP navrhne vhodné playbooky, orchestruje technické zásahy (blokovanie, izolácia, vypnutie účtu, ticketing) a všetko auditne zaznamená.

Vstupná podmienka	Incident je v stave „v riešení“
Vstupná podmienka	Pre daný typ incidentu existujú dostupné playbooky
Vstupná podmienka	Sú funkèné integrácie na cie¾ové systémy
Výstupná podmienka	Vybrané playbooky boli vykonané (auto / semi-auto)
Výstupná podmienka	Všetky automatizované zásahy sú auditne zaznamenané v incidente
Výstupná podmienka	Incident je v stave, ktorý odráža výsledok automatizovanej reakcie

Basic Path	Basic Path

Krok	Aktivita
1	Analytik otvorí incident v stave „v riešení“ a systém mu zobrazí zoznam navrhnutých playbookov pod¾a typu incidentu a použitých techník.
2	Analytik vyberie vhodný playbook a zvolí režim vykonania (napr. simulácia, poloautomatický režim, plne automatický pri nízkom riziku).
3	Systém zobrazí preh¾ad plánovaných krokov playbooku (napr. blok IP, izolácia endpointu, zakázanie úètu, vytvorenie ticketu).
4	Pri poloautomatickom režime systém pred vykonaním každého kroku vyžiada od Analytika potvrdenie alebo preskoèenie kroku.
5	Systém postupne vykonáva schválené kroky cez integrácie na cie¾ové systémy a priebežne zaznamenáva stav (úspech/zlyhanie).
6	Po skonèení playbooku systém zhrnie výsledok: ktoré akcie prebehli úspešne, èo zlyhalo a kde je treba manuálny zásah.
7	
8	Analytik na základe výsledku aktualizuje stav incidentu (napr. containment hotový, èaká sa na monitoring, èaká sa na ïalšie úlohy pod¾a UC_05).
9	Incident pokraèuje ïalej v UC_05 (detailná analýza, doplnenie úloh, uzatvorenie).

ALT_01 – Nenašiel sa vhodný playbook	Alternate

Krok	**Aktivita**
1	_05 a incident oznaèí ako kandidáta na vytvorenie nového playbooku v budúcnosti.

ALT_02 – Kritický krok playbooku zlyhá	Alternate

Krok	**Aktivita**
1	Pri vykonávaní automatizovaného kroku (napr. blokovanie na firewalle) dôjde k chybe; systém krok oznaèí ako neúspešný, zaznamená detail chyby a Analytik sa rozhodne, èi krok zopakuje, nahradí ho iným opatrením alebo priradí manuálnu úlohu Správcovi.

ALT_03 – Playbook sa spustí iba v simulaènom režime	Alternate

Krok	**Aktivita**
1	Na základe politiky Manažéra sú vybrané playbooky povolené len v režime simulácie; Analytik spustí simuláciu, systém zobrazí, aké akcie by boli vykonané a aký by bol dopad, a až následne Analytik rozhodne, ktoré z nich sa vykonajú manuálne alebo formou èiastoènej automatizácie.

Naviazané funkèné požiadavky	
FREQ_038 - Podpora orchestrácie a automatizácie	le škálovanie služieb, automatizované rozba¾ovanie prostredí, opakovate¾né testovanie aj zotavenie pri výpadkoch. V prostredí SOC, kde sa èasto menia požiadavky a topológia siete, je orchestrácia nevyhnutná pre zabezpeèenie flexibility, udržate¾nosti a prevádzkovej efektivity.
FREQ_046 - Automatizované reakcie	SOAR)
FREQ_061 - Automatizované reakcie: blok IP, izolácia hostu, eskalácia	eskalácia
FREQ_058 - Preddefinované playbooky	
FREQ_014 - SOAR	

UC_08 – Proaktívne h¾adanie hrozieb

Obrázok Diagram Sequence : UC_08 – Proaktívne hľadanie hrozieb

Prípad použitia	UC_08 – Proaktívne h¾adanie hrozieb
Cie¾	UC_08 rieši proaktívne hľadanie hrozieb v historických a aktuálnych dátach mimo bežných alertov. Analytik cieľavedome hľadá podozrivé vzory správania (TTP, IOC), ktoré doteraz nevyvolali incident ani upozornenie, ukladá si huntingové scenáre a z nálezov vie priamo zakladať nové incidenty.

Vstupná podmienka	Sú k dispozícii historické a aktuálne logy/telemetria
Vstupná podmienka	Existuje aspoò základná sada huntingových dopytov alebo scenárov
Vstupná podmienka	Analytik má prístup k dashboardom a nástrojom na ad-hoc dotazy
Výstupná podmienka	Prebehol aspoò jeden huntingový beh

Výstupná podmienka	Nálezy sú zdokumentované a prepojené na incidenty alebo knowledge base
Výstupná podmienka	Huntingové scenáre sú uložené pre opakované použitie

Basic Path	Basic Path

Krok	**Aktivita**
1	Výber huntingového cie¾a
2	Otvorenie huntingového pracovného priestoru
3	Tvorba alebo výber dopytu / scenára
4	Spustenie hunting behu nad dátami
5	Analýza nálezov
6	Prevod nálezov na incidenty alebo obohatenie existujúcich incidentov
7	Uloženie huntingového scenára
8	Dokumentácia výsledkov
9	Plánovanie opakovaného huntovania

ALT_01 – Hunting neodhalí niè významné	Alternate

Krok	**Aktivita**
1	Huntingový dopyt nevráti žiadne podozrivé nálezy alebo všetky nálezy sú po kontrole legitímne; Analytik záznam o huntingu uloží

ALT_02 – Hunting odhalí rozsiahlu kampaò	Alternate

Krok	**Aktivita**
1	Hunting identifikuje viaceré súvisiace nálezy, ktoré naznaèujú rozsiahlejší útok; Analytik vytvorí nadradený incident/kampaò, priradí k nemu všetky súvisiace nálezy a incidenty a informuje Manažéra o potrebe zvýšenej pozornosti.

ALT_03 – Dopyt je príliš nároèný alebo pomalý	Alternate

Krok	**Aktivita**
1	Spustený huntingový dopyt prechádza nad ve¾kým objemom dát a systémy ho vyhodnotia ako príliš nároèný; systém upozorní Analytika

Naviazané funkèné požiadavky	
	Efektívna práca s údajmi –
FREQ_078 - Podpora ML/AI algoritmov na detekciu hrozieb	Využitie algoritmov umelej inteligencie na detekciu anomálií a hrozieb. Podpora ML/AI algoritmov na detekciu hrozieb
FREQ_024 - Proaktívne vyh¾adávanie hrozieb	• CTI dáta • manuálnu analýzu v prípade podozrivých entít • výsledky sú dokumentované ako playbooky
FREQ_048 - Fulltextové a rýchle vyh¾adávanie	

UC_09 –

Obrázok Diagram Sequence : UC_09 – Spravovať Threat Intelligence a indikátory kompromitácie

Prípad použitia	UC_09 –
Cie¾	UC_09 rieši správu Threat Intelligence: prijímanie a integráciu CTI feedov, prácu s indikátormi kompromitácie (IOC), ich deduplikáciu a sledovanie v čase. Cieľom je, aby SOC vedel centrálne spravovať hrozby, obohacovať incidenty a logy o TI informácie a mať poriadok v observables.

Vstupná podmienka	Existujú dostupné TI zdroje
Vstupná podmienka	Sú nakonfigurované integrácie na TI zdroje
Vstupná podmienka	Systém má úložisko pre TI a IOC
Výstupná podmienka	TI dáta sú naèítané, normalizované a uložené
Výstupná podmienka	Redundantné alebo konfliktné IOC sú deduplikované alebo zlúèené
Výstupná podmienka	IOC/observables sú prepojené s incidentmi, prípadmi alebo aktívami a majú sledovate¾nú históriu

Basic Path	Basic Path

Krok	**Aktivita**
1	Naèítanie TI z externých zdrojov
2	Normalizácia a uloženie TI
3	Deduplikácia a zlúèenie IOC
4	Správa životného cyklu IOCSpráva životného cyklu IOC
5	Prepojenie IOC na incidenty a prípady
6	Zverejnenie TI pre ostatné èasti systému
7	Monitoring kvality TI

ALT_01 –	Alternate

Krok	**Aktivita**
1	Pri naèítaní TI je zdroj doèasne nedostupný alebo vracia chyby; systém zaznamená incident na integráciu, použije poslednú platnú sadu IOC a upozorní Správcu na problém.

ALT_02 – Konfliktné informácie o tej istej hrozbe	Alternate

Krok	**Aktivita**
1	Viacero TI zdrojov poskytne rozdielne alebo protichodné informácie o rovnakom IOC; systém uchová všetky varianty so zdrojmi, oznaèí IOC ako konfliktné a nechá na Analytikovi, aby vybral dôveryhodnejší zdroj.

ALT_03 – IOC je vyhodnotený ako neaktuálny alebo nespo¾ahlivý	Alternate

Krok	**Aktivita**
1	Analytik zistí, že daný IOC už nie je relevantný alebo bol oznaèený ako omyl; zmení jeho stav na neaktívny, pridá komentár a systém zabezpeèí, aby sa ïalej nepoužíval v nových detekciách.

Naviazané funkèné požiadavky	
FREQ_043 - Threat Intelligence (CTI) integrácia	Integrácia so zdrojmi hrozieb (IOC, TTP), automatické obohacovanie údajov. Threat Intelligence (CTI) integrácia
FREQ_145 - Pridávanie a sledovanie observables	
FREQ_018 - Threat Intelligence	rozby, TTPs a IOCs

FREQ_108 - Deduplikácia hrozieb a informácií	Odstraòovanie redundantných IOC a indikátorov. Deduplikácia hrozieb a informácií
FREQ_101 - Podpora taktického CTI	Práca s indikátormi kompromitácie (IOC) a ich evidencia, spracovanie, distribúcia. Podpora taktického CTI (IOC, IP, hash, URL, domény)

UC_10 –

Obrázok Diagram Sequence : UC_10 – Riadiť súlad, metriky a manažérsky reporting

Prípad použitia	UC_10 –
Cie¾	UC_10 rieši “vrchné poschodie” SOCaaS – aby mal manažment a audítori prehľad: ako sa SOCu darí (KPI, SLA, trend incidentov), či je systém v súlade s normami/predpismi, či sú všetky dôležité veci dohľadateľné spätne cez reporty, logy a audity.

Vstupná podmienka	Systém dlhodobo zbiera dáta o incidentoch, reakciách, playbookoch a TI
Vstupná podmienka	Existujú definované metriky/KPI a SLA
Vstupná podmienka	Je nastavená aspoò základná politika súladu (normy, interné smernice)
Výstupná podmienka	Manažér a Auditor majú k dispozícii preh¾adné metriky a reporty o stave bezpeènosti a SOC služieb
Výstupná podmienka	Identifikované problémy v KPI/SLA alebo súlade sú zaznamenané a majú priradené odporúèania/opatrenia
Výstupná podmienka	Vytvorené reporty sú archivované a doh¾adate¾né pre budúce audity

Basic Path	Basic Path

Krok	**Aktivita**
1	Manažér otvorí manažérsky preh¾ad SOC
2	Výber oblasti záujmu
3	Zobrazenie agregovaných metrík a trendov
4	Identifikácia odchýlok alebo problémov
5	Detailný drill-down
6	Zadanie požiadavky na report / analýzu
7	Zaznamenanie zistení a odporúèaní
8	Prepojenie na opatrenia

ALT_01 – Nedostupné alebo neúplné metriky	Alternate

Krok	**Aktivita**
1	

ALT_02 – Identifikované porušenie SLA alebo normy	Alternate

Krok	**Aktivita**
1	Z metrík a reportov vyplynie, že boli porušené SLA alebo požiadavky normy; Manažér zaregistruje zistenie ako oficiálny nález a spustí interné opatrenia (napr. incident kvality služby, korekèné opatrenia).

Naviazané funkèné požiadavky	
FREQ_098 - Politiky súladu s normami	
FREQ_020 - Reporting a spätná analýza	
FREQ_157 - Zabezpeèenie spätnej doh¾adate¾nosti a analýzy incidentov	

Prípad použitia	UC_10a –
Cie¾	UC_10a rozširuje UC_10 o detailné sledovanie KPI, SLA a celkového stavu bezpečnosti. Manažér, Auditor alebo Prevádzkovateľ si v dashboardoch pozrú trendové grafy, prehľady podľa tímov/zákazníkov a celkový „zdravotný stav“ SOCaaS.

Vstupná podmienka	Z UC_10 – manažérsky preh¾ad je dostupný.
Vstupná podmienka	Sú definované KPI a SLA (napr. MTTR, MTTD, % incidentov v SLA).
Výstupná podmienka	Identifikované odchýlky v KPI/SLA sú zdokumentované.
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	
2	Systém zobrazí dashboard s KPI a SLA (include UC_02a –
3	Manažér filtruje metriky pod¾a obdobia, tímu, typu incidentu alebo zákazníka.
4	Systém zobrazuje trendové grafy, priemery, percentá plnenia SLA a porovnania s cie¾ovými hodnotami.
5	Manažér identifikuje problémy (napr. konkrétny tím má dlhé èasy reakcie) a oznaèí ich na detailnej analýzy alebo nápravné opatrenia.

ALT_10a_01 – KPI alebo SLA nie sú ešte definované	Alternate

Krok	**Aktivita**
1	ené zdroje dát.

Naviazané funkèné požiadavky	
FREQ_073 - Zber systémových metrík, procesov a správania	
FREQ_159 - Vytvorenie základného preh¾adu stavu bezpeènosti a incidentov	ncidentov

Prípad použitia	UC_10b – Tvorba a plánovanie manažérskych a compliance reportov
Cie¾	UC_10b rieši praktickú prácu s reportami pre manažment a audity: tvorbu, konfiguráciu obsahu, plánovanie pravidelných reportov a ich jednorazové generovanie.

Vstupná podmienka	Systém má k dispozícii agregované dáta z ostatných UC (incidenty, TI, playbooky, KPI).
Vstupná podmienka	Užívate¾ má dostatoèné oprávnenia na tvorbu reportov.
Výstupná podmienka	Vznikajú šablóny reportov pre manažment/regulátora.
Výstupná podmienka	Sú nastavené pravidelné aj ad-hoc reporty pod¾a potrieb.

Basic Path	Basic Path

Krok	Aktivita
1	Manažér alebo Auditor otvorí sekciu „Reporty“ v rámci UC_10.
2	Zvolí typ reportu (manažérsky preh¾ad, incident overview, compliance report).
3	– výber metrik, èasového obdobia, filtrov.
4	Používate¾ si zvolí, èi ide o jednorazový report, alebo pravidelný (denný/týždenný/mesaèný).
5	– PDF/CSV/…
6	Vygenerovaný report sa uloží a je dostupný v archíve reportov.

ALT_01 – Nekompletný report z dôvodu chýbajúcich dát	Alternate

Krok	Aktivita
1	

Naviazané funkèné požiadavky	
FREQ_025 - Tvorba reportov a dashboardov	• preh¾ady incidentov • vizualizácie z metrík a ticketingu • exporty pre audit a SLA reporting
FREQ_162 - Plánovanie pravidelných reportov	
– èasové obdobie, typy incidentov	– èasové obdobie, typy incidentov

Prípad použitia	UC_10c –
Cie¾	UC_10c rieši bezpečnostnú a auditnú stránku reportovania: kto čo vidí, kto čo sprístupnil, či sú reporty archivované a či je možné rekonštruovať, kto mal aké údaje k dispozícii.

Vstupná podmienka	V systéme existujú vygenerované reporty (UC_10b).
Vstupná podmienka	Sú definované roly a prístupové politiky (RBAC).
Výstupná podmienka	Prístup k reportom je obmedzený pod¾a rolí a zodpovedností.
Výstupná podmienka	Existuje auditná stopa, kto a kedy s reportami pracoval.
Výstupná podmienka	Dôležité reporty sú archivované pre potreby budúcich auditov.

Basic Path	Basic Path

Krok	Aktivita
1	Manažér alebo Auditor otvorí správu reportov a prístupov.
2	Pre jednotlivé typy reportov nastaví, ktoré roly alebo konkrétni používatelia k nim majú prístup.
3	
4	
5	

ALT_01 – Pokus o prístup k reportu bez oprávnenia	Alternate

Krok	Aktivita
1	

Naviazané funkèné požiadavky	
FREQ_066 - RBAC a audit trail	Riadenie prístupov na základe rolí a logovanie zmien v systéme. RBAC a audit trail

UC_11 –

Obrázok Diagram Sequence : UC_11 – Spravovať aktíva a prostredie zákazníka

Prípad použitia	UC_11 –
Cie¾	Cieľom UC_11 je, aby SOCaaS poznal, čo vlastne chráni – všetky relevantné aktíva zákazníka (servery, aplikácie, siete, cloud služby...) a ich vzťahy. Umožňuje evidovať aktíva, rozlišovať ich typy, mapovať ich na lokality/VLAN/IP a sledovať ich životný cyklus, aby sa incidenty, hrozby a zraniteľnosti dali viazať na konkrétne časti prostredia.

Vstupná podmienka	Zákazník je onboardnutý v systéme (UC_00) a má vytvorený základný profil.
Vstupná podmienka	Systém má k dispozícii modul / sekciu pre evidenciu aktív.
Vstupná podmienka	
Výstupná podmienka	
Výstupná podmienka	
Výstupná podmienka	Zmeny v aktívach (pridanie, úprava, vyradenie) sú evidované a životný cyklus je sledovate¾ný.

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevádzkovate¾ otvorí modul „Aktíva“ pre konkrétneho zákazníka.
2	
3	
4	Správca doplní technické údaje – IP adresy, hostname, prostredie (prod/test/dev).
5	
6	Prevádzkovate¾ nastaví stav aktíva v životnom cykle (napr. „v prevádzke“, „v nasadzovaní“, „vyradené“).
7	Systém uloží záznam o aktíve a sprístupní ho ostatným modulom (incident mgmt, TI, vuln mgmt, reporting).
8	Pri ïalšej zmene (upgrade, migrácia, vyradenie) Správca aktualizuje záznam o aktíve a systém zaznamená zmenu v histórii.

ALT_11_01 – Import aktív z externého CMDB	Alternate

Krok	**Aktivita**
1	Namiesto ruèného vytvárania záznamov Prevádzkovate¾ zvolí import z externého CMDB alebo inventarizaèného nástroja; systém naèíta zoznam aktív, zobrazí náh¾ad a umožní ich hromadné uloženie alebo spárovanie s existujúcimi záznamami.

ALT_11_02 – Detegovaný duplikát aktíva	Alternate

Krok	**Aktivita**
1	Pri ukladaní nového aktíva systém zistí, že už existuje záznam s rovnakými k¾úèovými identifikátormi (napr. IP/hostname); používv

ALT_11_03 – Zmena kritickosti aktíva		Alternate
Krok	**Aktivita**	
1		

Naviazané funkèné požiadavky	
FREQ_017 - Inventarizácia a správa aktív	
FREQ_114 - Vytvorenie, editácia a mazanie záznamov o aktívach	vach
	Správa jednotlivých fáz životnosti aktíva — vyradenie)
FREQ_115 - Rozlíšenie aktív pod¾a typu	– hardvér, softvér, virtuálne, cloudové
FREQ_118 - Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	

UC_12 –

UC_12 pokrýva vulnerability management v SOCaaS:
od prijatia výstupov zo skenerov zraniteľností, cez ich priradenie na konkrétne aktíva (UC_11), prioritizáciu podľa rizika, až po plánovanie a sledovanie nápravných opatrení.
Cieľom je mať ucelený prehľad o tom, kde sme deraví, čo je najdôležitejšie opraviť a v akom čase.

Obrázok Diagram Sequence : UC_12 – Riadiť zraniteľnosti a bezpečnostné nálezy

Prípad použitia	UC_12 –
Cie¾	UC_12 pokrýva vulnerability management v SOCaaS: od prijatia výstupov zo skenerov zraniteľností, cez ich priradenie na konkrétne aktíva (UC_11), prioritizáciu podľa rizika, až po plánovanie a sledovanie nápravných opatrení. Cieľom je mať ucelený prehľad o tom, kde sme deraví, čo je najdôležitejšie opraviť a v akom čase.

Vstupná podmienka	Existujú výsledky skenovania zranite¾ností alebo iné bezpeènostné nálezy
Vstupná podmienka	Aktíva sú zaevidované v systéme
Vstupná podmienka	Je definovaná základná politika priorizácie zranite¾ností
Výstupná podmienka	Zranite¾nosti sú zaevidované a priradené ku konkrétnym aktívam.
Výstupná podmienka	
Výstupná podmienka	Stav riešenia (neopravené / v riešení / opravené / akceptované riziko) je sledovaný a doh¾adate¾ný.

Basic Path		Basic Path
Krok	**Aktivita**	
1	Import alebo zadanie zranite¾ností	
2	Normalizácia a zoskupenie nálezov	
3	Priradenie zranite¾ností na aktíva	
4	Výpoèet a nastavenie priority zranite¾nostíVýpoèet a nastavenie priority zranite¾ností	
5	Vytvorenie remediation plánu	
6	Realizácia nápravných opatrení	
7	Re-scan alebo overenie stavu	

8	Aktualizácia stavu zranite¾ností
9	Reporting a prepojenie s incidentmi

ALT_12_01 –	Alternate

Krok	**Aktivita**
1	žér po diskusii rozhodne, èi sa riziko doèasne akceptuje, alebo sa zavedú kompenzaèné opatrenia (network segmentácia, zvýšený monitoring). Stav zranite¾nosti sa nastaví na „akceptované riziko“ alebo „kompenzované“.

ALT_12_02 – Detegovaný duplicitný alebo obsolete nález	Alternate

Krok	**Aktivita**
1	elevantná; nález sa oznaèí ako duplicitný alebo obsolete, prièom sa uchová referenèný záznam pre audit.

ALT_12_03 –	Alternate

Krok	**Aktivita**
1	

Naviazané funkèné požiadavky	
FREQ_097 - Podpora pre EPSS – predikcia zneužitia zranite¾ností	Využitie modelov pravdepodobnosti zneužitia zranite¾nosti. Podpora pre EPSS – predikcia zneužitia zranite¾ností
FREQ_023 - Správa zranite¾ností a inventarizácia	• Assety sú aktualizované na základe detekcie • incidenty viazané na zranite¾nosti sú prepájané do manažment systému
FREQ_019 - Správa zranite¾ností	
FREQ_074 - Zber informácií o zranite¾nostiach a konfiguráciách	Získavanie informácií o zranite¾nostiach z konfiguraèných údajov a porovnanie s databázami CVE. Zber informácií o zranite¾nostiach a konfiguráciách
FREQ_086 - Aktualizácie testov na zranite¾nosti – komunitný a podnikový feed	Frekvencia a rozsah aktualizácií detekèných vzorov. Aktualizácie testov na zranite¾nosti – komunitný a podnikový feed

UC_13 –

Obrázok Diagram Sequence : UC_13 – Navrhnúť a udržiavať bezpečnostnú architektúru SOCaaS prostredia zákazníka

Prípad použitia	UC_13 –

Cie¾	UC_13 rieši návrh a priebežnú údržbu technickej a bezpečnostnej architektúry pre konkrétneho zákazníka: ako je zákazník napojený na SOCaaS, aké systémy, zóny a logovacie zdroje sa integrujú, akými kanálmi tečú dáta (agent, syslog, API, VPN, peering…), ako sú prepojené SIEM, SOAR, TI, ticketing, EDR, vuln skenery, asset mgmt. Výstupom je schválený a udržiavaný architektonický návrh (topológia, integračné body, dátové toky), a zoznam povinných log zdrojov a typov logov ktorý slúži ako podklad pre onboarding (UC_00), monitoring (UC_01), správu aktív (UC_11), zraniteľností (UC_12) a automatizáciu (UC_07).

Vstupná podmienka	
Vstupná podmienka	Zákazník poskytol potrebný preh¾ad o svojom prostredí (aspoò high-level architektúra, typy systémov, siete).
Vstupná podmienka	
Výstupná podmienka	Existuje zdokumentovaný a schválený architektonický návrh napojenia prostredia zákazníka na SOCaaS (topológia, integraèné body, tok dát).
Výstupná podmienka	Sú definované integraèné kanály (aký systém → akým spôsobom → do ktorého modulu SOCaaS).
Výstupná podmienka	Zmeny v architektúre sú sledovate¾né (verzie, kto schválil, kedy) a použite¾né ako vstup pre onboarding a prevádzku.
Výstupná podmienka	Je definovaný a zdokumentovaný zoznam povinných log zdrojov a typov logov pre onboarding zákazníka do SOCaaS (vrátane minimálne potrebných polí pre detekciu hrozieb).

Basic Path	Basic Path

Krok	**Aktivita**
1	Zber požiadaviek a vstupov
2	Analýza existujúcej architektúry zákazníka
3	Návrh dátových tokov a integraèných patternov vrátane identifikácie povinných log zdrojov a typov logov
4	Návrh integrácií s nástrojmi zákazníka
5	Posúdenie bezpeènostných princípov a rizík
6	Schválenie architektonického návrhu
7	Odoslanie návrhu do realizácie
8	Priebežná údržba architektúry

ALT_13_01 –	Alternate

Krok	**Aktivita**
1	ávrh tak, aby využíval alternatívne integraèné patterny alebo zúžený rozsah monitoringu a zmeny znovu predloží na schválenie.

ALT_13_02 – Zmeny v prostredí zákazníka po nasadení	Alternate

Krok	**Aktivita**
1	Poèase zákazník pridá nové systémy, migruje do cloudu alebo zmení topológiu; Architekt vytvorí revíziu architektonického návrhu, doplní nové integraèné body a Prevádzkovate¾ naplánuje a vykoná potrebné zmeny v konfigurácii SOCaaS.

ALT_13_03 – Návrh neprejde bezpeènostným alebo výkonnostným posúdením	Alternate

Krok	**Aktivita**
1	Pri posúdení návrhu sa zistí, že navrhované riešenie nevyhovuje (príliš ve¾ké latencie, neakceptovate¾né riziká, nedostatoèné škálovanie); návrh sa vráti Architektovi na prepracovanie a až po zapracovaní pripomienok je znovu predložený na schválenie.

Naviazané funkèné požiadavky	
FREQ_030 - Integrácia s ostatnými komponentmi	Prepojenie so zdrojmi dát Integrácia s nástrojmi incident managementu a SOAR Znalostná databáza a playbooky
FREQ_166 - Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI	entov, Asset management, CTI, ...
FREQ_120 - Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zranite¾ností, evidencia incidentov	émom, EDR, skenerom zranite¾ností, evidencia incidentov
FREQ_095 - Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	, Verinice
FREQ_013 - Integrácia s ïalšími nástrojmi	

UC_14 –

Obrázok Diagram Sequence : UC_14 – Pracovať s portálom zákazníka a spolupracovať

Prípad použitia	UC_14 –
Cie¾	UC_14 rieši pohľad zákazníka na SOCaaS – cez webový portál, kde: vidí svoje incidenty, KPI, reporty a aktíva, vie spolupracovať so SOC (komentáre, prílohy, schvaľovanie opatrení), môže si prispôsobiť portál pre viac organizácií/jednotiek. Portál je moderné, responzívne webové rozhranie, multi-tenant, a podporuje aj pokročilejšie nastavenia (šablóny, zdieľanie, integračné hooky v pod-UC).

Vstupná podmienka	Zákazník je onboardnutý (UC_00) a má vytvorenú aspoò jednu organizáciu / tenant.
Vstupná podmienka	Pre používate¾ov sú vytvorené úèty a priradené roly (napr. „Manažér bezpeènosti“).
Vstupná podmienka	Portál je dostupný cez zabezpeèené webové rozhranie (HTTPS, SSO/Federácia ak treba).
Výstupná podmienka	Používate¾ má cez portál preh¾ad o svojich incidentoch, KPI a aktívach.
Výstupná podmienka	
Výstupná podmienka	Portál rešpektuje multi-tenant model – dáta sú oddelené medzi organizáciami a nastavenia sú prispôsobené potrebám konkrétnej organizácie.

Basic Path		Basic Path
Krok	**Aktivita**	

1	Koncový používate¾ sa prihlási do portálu zákazníka (SSO / meno + heslo / MFA pod¾a politiky).
2	Systém zobrazí úvodný preh¾ad – dashboard so stavom incidentov, základnými KPI a upozorneniami
3	
4	
5	
6	
7	
8	Systém všetky interakcie (prístup k incidentom, komentáre, zmeny v nastaveniach) auditne zaznamenáva a zabezpeèuje, aby boli vidite¾né len v rámci danej organizácie.

ALT_14_01 – Používate¾ nemá priradenú žiadnu organizáciu	Alternate

Krok	**Aktivita**
1	Po prihlásení systém zistí, že úèet nie je naviazaný na žiadnu organizáciu; zobrazí informáciu o chýbajúcom priradení a odporuèí

ALT_14_02 – Obmedzené zobrazenie pod¾a roly	Alternate

Krok	**Aktivita**
1	Používate¾ má len rolu s obmedzenými právami (napr. „read-only“); portál skryje niektoré akèné prvky (editácia, schva¾ovanie) a umožní iba prezeranie incidentov a reportov.

Naviazané funkèné požiadavky	
FREQ_141 - Moderné, responzívne webové rozhranie	Moderný a responzívny dizajn pre pohodlné používanie. Moderné, responzívne webové rozhranie
nie úloh a observables medzi organizáciami	

Prípad použitia	UC_14a –
Cie¾	UC_14a rozširuje UC_14 o konkrétnu prácu s incidentmi/ticketmi z pohľadu zákazníka: vidieť zoznam incidentov, otvoriť detail, vytvoriť nový „ticket“ alebo doplniť informácie, meniť stavy (Nový, V riešení, Uzavretý, Odložený), cieľovo smerovať incident na správneho riešiteľa (L1/L2/L3, konkrétny tím).

Vstupná podmienka	Platí precondition z UC_14 – používate¾ je prihlásený a má organizáciu.
Vstupná podmienka	
Výstupná podmienka	Incidenty/tickety sú vytvorené alebo aktualizované pod¾a akcií zákazníka.
Výstupná podmienka	Incident má nastavený aktuálny stav a priradeného riešite¾a.

Basic Path	Basic Path

Krok	**Aktivita**
1	Používate¾ v portáli otvorí sekciu „Incidenty / Tickety“.
2	Systém zobrazí zoznam incidentov s filtrom pod¾a stavu, typu, priority alebo obdobia.
3	Používate¾ vyberie konkrétny incident a otvorí jeho detail.

4	ešení“).
5	
6	Systém zmeny uloží, aktualizuje zobrazenie v portáli a sprístupní ich SOC analytikom.

ALT_14a_01 –	Alternate

Krok	**Aktivita**
1	rí nový záznam a priradí ho do frontu SOC.

ALT_14a_02 – Zmena stavu nie je povolená	Alternate

Krok	**Aktivita**
1	ystém zmenu odmietne a zobrazí informáciu o nedostatoèných právach.

Naviazané funkèné požiadavky	
FREQ_131 - Priradenie na konkrétneho riešite¾a	Priradenie ticketov na konkrétnych riešite¾ov vrátane eskalácie pod¾a úrovne. Priradenie na konkrétneho riešite¾a (L1 analytik, eskalácia L2/ L3)
FREQ_129 - Vytvorenie a editácia záznamov	Základná funkcionalita ticketovacieho systému – vytváranie, editovanie a mazanie ticketov. Vytvorenie a editácia záznamov (ticketov)
	Uzavretý, Odložený)
Prípad použitia	UC_14b –
Cie¾	UC_14b rozširuje UC_14 o kolaboračnú vrstvu pri riešení incidentu: komentáre medzi zákazníkom a SOC, emailové notifikácie o zmenách stavu, komentároch a deadlinoch, auditná stopa všetkých zmien a prístupov v tickete.

Vstupná podmienka	Incident existuje a je dostupný v portáli (UC_14a).
Vstupná podmienka	
Výstupná podmienka	K incidentu sú pridané komentáre a/alebo prípadné zmeny stavu iniciované zákazníkom.
Výstupná podmienka	Všetky zmeny a prístupy sú auditne zaznamenané; príslušné strany dostávajú notifikácie.

Basic Path	Basic Path

Krok	**Aktivita**
1	Používate¾ otvorí detail incidentu v portáli.Používate¾ otvorí detail incidentu v portáli.
2	Systém uloží komentár, zaznamená, kto a kedy ho pridal.
3	Systém uloží komentár, zaznamená, kto a kedy ho pridal.
4	Systém odošle emailové notifikácie relevantným stranám (Analytik, ïalší zástupcovia zákazníka) o novom komentári alebo zmene stavu.
5	Analytik odpovie cez svoj nástroj; odpoveï sa synchronizuje do portálu a zobrazí sa zákazníkovi ako ïalší komentár.
6	

ALT_14b_01 – Notifikácie sú pre konkrétneho používate¾a vypnuté	Alternate

Naviazané funkèné požiadavky

FREQ_142 - Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete	Zaznamenávanie všetkých akcií, zmien a komentárov v tickete. Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete
FREQ_132 - Emailové notifikácie o zmenách stavu, komentároch, deadline	Automatické emailové notifikácie o zmene stavu, komentároch, deadline. Emailové notifikácie o zmenách stavu, komentároch, deadline

Prípad použitia	UC_14c –
Cie¾	UC_14c rozširuje UC_14 o konfiguračnú časť pre zákazníka: nastavenie priorít a závažnosti incidentov z pohľadu zákazníka, nastavenie integračných kanálov (REST API / Webhooky) pre napojenie portálu na interné nástroje zákazníka (ticketing, chat, ITSM).

Vstupná podmienka	
Vstupná podmienka	Pre organizáciu sú definované aspoò základné priority a kategórie incidentov.
Výstupná podmienka	Sú definované preferované priority/závažnosti incidentov pre danú organizáciu.
Výstupná podmienka	Sú nakonfigurované (ak treba) integraèné kanály – napr. Webhooky pre notifikácie do interného ticketingu.

Basic Path	Basic Path

Krok	**Aktivita**
1	Manažér v portáli otvorí sekciu „Nastavenia organizácie“.
2	a).
3	V èasti „Integrácie“ zadá koncové URL pre Webhooky alebo API tokeny pre napojenie na interný ticketovací/ITSM systém.
4	Systém overí základnú konektivitu a uloží nastavenia.
5	Pri ïalších zmenách stavu incidentu alebo pri nových incidentoch systém pod¾a nastavení posiela notifikácie cez REST API / Webhooky do systémov zákazníka.

ALT_14c_01 – Neplatné alebo nedostupné integraèné rozhranie	Alternate

Krok	**Aktivita**
1	Pri uložení nastavení integrácie testovací request zlyhá (timeout, 4xx, 5xx); systém na to upozorní Manažéra a integráciu uloží buï ako neaktívnu, alebo vyžaduje opravu parametrov.

Naviazané funkèné požiadavky	
FREQ_139 - Podpora REST API a Webhookov	Podpora pre rozhrania REST API a Webhooky na komunikáciu s inými systémami. Podpora REST API a Webhookov
FREQ_135 - Nastavenie priority a závažnosti incidentu	Nastavenie úrovne priority a závažnosti ticketu pre lepšie plánovanie. Nastavenie priority a závažnosti incidentu

UC_15 –

Obrázok Diagram Sequence : UC_15 – Spravovať prevádzku SOCaaS platformy

Prípad použitia	UC_15 –

Cie¾	UC_15 rieši technickú prevádzku SOCaaS platformy tak, aby: bola stabilná, výkonná a dostupná, agenty a senzory nezaťažovali zbytočne prostredie zákazníka, sa platforma priebežne aktualizovala (signatúry, moduly), bola pod kontrolou kapacita spracovania/skenovania. Cieľom je, aby SOCaaS bežal spoľahlivo, vedel zvládnuť očakávaný objem dát a neohrozoval výkon systémov zákazníka.

Vstupná podmienka	SOCaaS platforma je nasadená v produkènom prostredí (on-prem/cloud/SaaS).
Vstupná podmienka	Existujú monitorovacie nástroje a mechanizmy na sledovanie stavu platformy a agentov.
Vstupná podmienka	Sú definované základné prevádzkové parametre –
Výstupná podmienka	Stav platformy a nasadených agentov je priebežne monitorovaný a známy Prevádzkovate¾ovi.
Výstupná podmienka	Aktualizácie signatúr a modulov sú vykonávané riadeným spôsobom a bez výrazného výpadku služby.
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	
2	Systém priebežne monitoruje stav nasadených agentov u zákazníkov –
3	Pri náraste poètu zákazníkov alebo objemu dát Prevádzkovate¾ vyhodnotí kapacitu spracovania/ skenovania a porovná ju s oèakávaným rastom.
4	Na základe politiky aktualizácií naplánuje Prevádzkovate¾ pravidelné aktualizácie signatúr a modulov (napr. mimo špièky), aby minimalizoval dopad na výkon.
5	Systém vykoná aktualizácie a overí, èi sú agenty a komponenty po aktualizácii funkèné a reportujú v oèakávanom rozsahu.
6	
7	Všetky prevádzkové zásahy (aktualizácie, zmeny konfigurácie, zásahy do kapacity) sú zaznamenané pre potreby auditu a diagnostiky.

ALT_15_01 –	Alternate

Krok	**Aktivita**
1	guráciu (frekvenciu skenovania, rozsah dát), prípadne navrhne rozšírenie kapacity alebo optimalizáciu nasadenia.

ALT_15_02 – Zlyhanie aktualizácie signatúr alebo modulov	Alternate

Krok	**Aktivita**
1	kovate¾ identifikuje dotknuté systémy, vráti ich na poslednú stabilnú verziu alebo zopakuje aktualizáciu s upravenými parametrami.

Naviazané funkèné požiadavky	
FREQ_085 - Odhadovaná kapacita skenovania	
FREQ_053 - Monitoring stavu systému	Sledovanie výkonu, dostupnosti a funkènosti systému. Monitoring stavu systému (healthcheck)

FREQ_082 - Jednoduché centrálne riadenie agentov	Centrálna konzola na správu, konfiguráciu a doh¾ad nad všetkými agentmi. Jednoduché centrálne riadenie agentov
FREQ_083 - Pravidelné aktualizácie signatúr a modulov	Pravidelné aktualizácie databáz hrozieb, signatúr a detekèných pravidiel. Pravidelné aktualizácie signatúr a modulov

UC_16 –

Obrázok Diagram Sequence : UC_16 – Prispôsobiť reporty, exporty a dokumenty potrebám organizácie

Prípad použitia	UC_16 –
Cie¾	UC_16 rieši konfiguráciu podoby výstupov zo SOCaaS: vzhľad reportov podľa firemnej identity (logo, farby, záhlavie), formáty exportov (CSV, XML, PDF, HTML, Markdown), export incidentov a dokumentov pre ďalšie spracovanie alebo archiváciu. Nadväzuje na UC_10b (ktorý rieši obsah a plánovanie reportov) tým, že umožňuje detailné nastavenie prezentácie a exportu, aby výstupy zapadli do prostredia zákazníka a do jeho nástrojov.

Vstupná podmienka	
Vstupná podmienka	
Vstupná podmienka	SOCaaS platforma podporuje viac formátov exportu a základné šablóny vzh¾adu.
Výstupná podmienka	Sú definované šablóny vzh¾adu reportov pre jednotlivé organizácie (logo, farby, záhlavie).
Výstupná podmienka	Pre konkrétne typy reportov/incitentov sú nastavené preferované exportné formáty.
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	Manažér alebo Auditor otvorí v portáli sekciu „Nastavenie reportov a exportov“.
2	
3	V èasti Vzh¾ad zvolí alebo upraví šablónu:
4	n).
5	
6	Po potvrdení systém uloží šablónu vzh¾adu a preferované exportné formáty pre daný typ reportu/ dokumentu.
7	
8	nizácie.

ALT_16_01 – Požadovaný exportný formát nie je podporovaný	Alternate

Krok	**Aktivita**
1	. CSV namiesto XLSX, PDF namiesto DOCX).

ALT_16_02 – Chyba pri exporte ve¾kého objemu dát	Alternate

Krok	Aktivita
1	Pri exporte reportu s ve¾kým poètom záznamov dôjde k prekroèeniu limitu alebo timeoutu; systém export preruší, informuje používate¾a a ponúkne zúženie rozsahu (kratšie obdobie, filtrované dáta) alebo asynchrónny export.

ALT_16_03 – Zmena firemnej identity	Alternate

Krok	Aktivita
1	Organizácia zmení logo alebo korporátne farby; Manažér otvorí nastavenia vzh¾adu, upraví šablónu (logo, farby) a po uložení budú

Naviazané funkèné požiadavky	
FREQ_153 - Export incidentov do formátov CSV, PDF, cez REST API	Export dát pre dokumentáciu alebo reportovanie. Export incidentov do formátov CSV, PDF, cez REST API
FREQ_164 - Prispôsobenie vizuálnej podoby reportu	
FREQ_180 - Export dokumentov do PDF, HTML alebo Markdown formátu	
FREQ_169 - Webové/GUI rozhranie pre tvorbu a správu reportov	Používate¾sky prívetivé rozhranie pre návrh, úpravu a správu reportov. Webové/GUI rozhranie pre tvorbu a správu reportov
FREQ_092 - Konfigurovate¾né formáty reportov	Flexibilita výstupov pre ïalšie spracovanie. Konfigurovate¾né formáty reportov (napr. CSV, XML, PDF)

UC_17 –

Obrázok Diagram Sequence : UC_17 – Spravovať používateľov a roly v SOCaaS platforme

Prípad použitia	
Cie¾	UC_17 rieši administráciu používateľov a rolí v rámci SOCaaS: vytváranie a úpravu účtov, priraďovanie rolí (SOC, zákazník, auditor…), nastavenie prístupov cez RBAC, prípadné doplnenie vlastných atribútov. Je to systémový/administrátorský UC, ktorý podporuje všetky ostatné UC tým, že určuje, kto čo v platforme môže vidieť a robiť.

Vstupná podmienka	SOCaaS platforma beží a má prístupné administrátorské webové rozhranie.
Vstupná podmienka	Aktuálne prihlásený používate¾ má administrátorské oprávnenia na správu úètov a rolí.
Výstupná podmienka	Vytvorené, upravené alebo deaktivované používate¾ské úèty sú uložené v systéme.
Výstupná podmienka	Používate¾om sú priradené vhodné roly pod¾a RBAC modelu.
Výstupná podmienka	Prípadné vlastné atribúty/metadata sú nastavené a použite¾né v ïalších èastiach systému.

Basic Path	Basic Path

Krok	Aktivita

1	Prevádzkovate¾ sa prihlási do administrátorského webového rozhrania.
2	Otvorí sekciu „Používatelia a roly“.
3	
4	Pri vytváraní úètu zadá základné údaje (meno, kontakty, identifikátor úètu) a vyberie jednu alebo viac používate¾ských rolí (napr. SOC analytik, Manažér, Zákazník, Auditor).
5	
6	Systém uloží zmeny a zobrazí používate¾a v preh¾adnom zozname; rozhranie umožní filtrovanie a vyh¾adávanie pod¾a mena, roly a ïalších atribútov.
7	

ALT_17_01 – Pokus o zmenu, na ktorú používate¾ nemá oprávnenie	Alternate

Krok	**Aktivita**
1	statoèné oprávnenie.

ALT_17_02 – Neplatná kombinácia rolí	Alternate

Krok	**Aktivita**
1	Pri ukladaní úètu systém zistí, že zvolená kombinácia rolí je v rozpore s RBAC politikou (napr. konflikt záujmov); administrátor

Naviazané funkène požiadavky	
	etBox/Django)
FREQ_180 - Export dokumentov do PDF, HTML alebo Markdown formátu	
FREQ_164 - Prispôsobenie vizuálnej podoby reportu	
FREQ_092 - Konfigurovate¾né formáty reportov	Flexibilita výstupov pre ïalšie spracovanie. Konfigurovate¾né formáty reportov (napr. CSV, XML, PDF)
FREQ_178 - Podpora RBAC	Riadenie prístupu pod¾a používate¾ských rolí. Podpora RBAC – rôzne úrovne prístupu pre èítanie, editáciu, schva¾ovanie
FREQ_153 - Export incidentov do formátov CSV, PDF, cez REST API	Export dát pre dokumentáciu alebo reportovanie. Export incidentov do formátov CSV, PDF, cez REST API
FREQ_181 - Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	Používate¾sky prívetivé GUI pre správu znalostí. Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov
FREQ_169 - Webové/GUI rozhranie pre tvorbu a správu reportov	Používate¾sky prívetivé rozhranie pre návrh, úpravu a správu reportov. Webové/GUI rozhranie pre tvorbu a správu reportov
FREQ_150 - Podpora viacerých používate¾ských rolí	Podpora RBAC pre rôzne roly. Podpora viacerých používate¾ských rolí – minimálne analytik a administrátor

UC_18 –

Obrázok Diagram Sequence : UC_18 – Spravovať organizácie, tímy a štruktúru prípadov

Prípad použitia	UC_18 –

Cie¾	UC_18 rieši administráciu organizácií/tenantov a spôsob, akým sa incidenty/prípady v rámci nich štruktúrujú: založenie a úprava organizácií / tímov, nastavenie kategórií, typov a vlastníkov prípadov, definovanie šablón incidentov a spôsobu ich zdieľania medzi tímami a externými partnermi. Stojí na UC_17 (používatelia a roly) a UC_14 (portál zákazníka) a dopĺňa ich o „organizačno-procesnú“ vrstvu.

Vstupná podmienka	Používate¾ je prihlásený a má oprávnenia na správu organizácií/štruktúry prípadov.
Vstupná podmienka	SOCaaS má vytvorených aspoò pár používate¾ov (UC_17) a minimálne jednu organizáciu/ tenant (UC_14).
Výstupná podmienka	Organizácie/ tímy majú nastavenú štruktúru prípadov (typy, kategórie, vlastníci).
Výstupná podmienka	Sú definované šablóny pre opakujúce sa incidenty a spôsob ich zdie¾ania medzi tímami/ partnermi.
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	Manažér alebo Prevádzkovate¾ otvorí v administrácii sekciu „Organizácie a prípady“.
2	Vyberie existujúcu organizáciu (tenant) alebo vytvorí novú a priradí k nej tímy (napr. „SOC L1“, „SOC L2“, „IT zákazníka“).
3	Pre organizáciu nastaví typy prípadov/incidentov (napr. „Phishing“, „Malware“, „Politika“, „Vuln nález“) a základné kategórie.
4	Pre jednotlivé typy incidentov vytvorí šablóny – predvyplnené polia, odporúèané položky, požadované informácie.
5	K typom incidentov a šablónam priradí vlastníkov, tagy a kategórie (napr. „kritické“, „regulaèné“, „interné“), aby bolo možné na
6	
7	Systém uloží štruktúru organizácie, šablóny a pravidlá zdie¾ania; nové incidenty sa vytvárajú pod¾a týchto nastavení.

ALT_18_01 – Vytvorenie vlastného typu prípadu pre konkrétnu organizáciu	Alternate

Krok	**Aktivita**
1	Organizácia má špecifický typ prípadu (napr. „Compliance nález“), ktorý neexistuje v globálnej schéme; Manažér pridá nový typ prípadu len pre túto organizáciu a vytvorí k nemu vlastnú šablónu.

ALT_18_02 – Obmedzenie zdie¾ania prípadov s externým partnerom	Alternate

Krok	**Aktivita**
1	dú a upraví pravidlá zdie¾ania tak, aby tieto prípady boli prístupné len interným tímom.

Naviazané funkèné požiadavky	
FREQ_147 - Kategorizácia incidentov pomocou tagov	
FREQ_158 - Zdie¾anie prípadov medzi tímami a externými partnermi pod¾a práv	Podpora riadeného zdie¾ania prípadov. Zdie¾anie prípadov medzi tímami a externými partnermi pod¾a práv

	e, v údržbe, vyradené)

UC_19 –

Obrázok Diagram Sequence : UC_19 – Riadiť uchovávanie, ochranu a auditovanie dát SOCaaS

Prípad použitia	UC_19 –
Cie¾	UC_19 rieši správu dát v SOCaaS z pohľadu platformy: kde a ako sa logy ukladajú, indexujú a uchovávajú, aké retenčné politiky platia pre jednotlivé zdroje logov, ako sú logy chránené a šifrované, ako sa vedú auditovacie záznamy o aktivitách používateľov a analytikov. Cieľom je, aby SOCaaS spĺňal požiadavky na bezpečné ukladanie a auditovateľnosť dát, a zároveň podporoval forenznú analýzu.

Vstupná podmienka	SOCaaS platforma je v prevádzke (UC_15) a prijíma logy z rôznych zdrojov (UC_01).
Vstupná podmienka	Existuje úložisko logov / dát (SIEM / data lake), ktoré podporuje konfiguráciu retencie a šifrovania.
Vstupná podmienka	Je definovaná aspoò základná politika uchovávania a bezpeènosti logov (napr. pod¾a typu logu alebo regulácie).
Výstupná podmienka	Pre logy/dáta sú nastavené reteènè politiky pod¾a zdroja a dôležitosti.
Výstupná podmienka	Logy sú chránené pri prenose aj uložení (nastavené šifrovanie).
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	Návrh architektúry ukladania a retencie
2	Nastavenie reteènèých politík pod¾a zdroja a dôležitosti
3	Zapnutie a overenie šifrovania logov
4	Konfigurácia zberu auditovacích záznamov
5	Monitorovanie stavu uchovávania a audit trailu
6	Vyhodnocovanie požiadaviek auditorov
7	Úprava politík na základe zistení

ALT_19_01 – Nedostatoèná kapacita pre nastavenú retenciu	Alternate

Krok	**Aktivita**
1	Pri dlhších reteènèých dobách Operátor zistí, že úložisko nemá dostatoènú kapacitu; spoloène s Architektom buï upravia retenciu (napr. rozdielne pod¾a typu logu), alebo navrhnú rozšírenie úložiska.

ALT_19_02 – Požiadavka audítora na dlhšiu retenciu		Alternate
Krok	**Aktivita**	
1	Auditor alebo regulátor požaduje dlhšiu retenciu pre konkrétny typ logov (napr. prihlasovacie logy); Architekt a Operátor upravi	

ALT_19_03 – Incident s kompromitáciou úložiska logov		Alternate
Krok	**Aktivita**	
1	Operátor na základe zistení sprísnia šifrovanie, prístupové práva alebo segmentáciu úložiska.	

Naviazané funkèné požiadavky	
FREQ_039 - Podporované formáty logov	CEF, LEEF...)
FREQ_051 - Retencia	
FREQ_071 - Zber auditovacích dát pomocou agentov	Zber auditovacích záznamov o aktivitách používate¾ov, procesoch a systéme cez agenta. Zber auditovacích dát pomocou agentov
FREQ_052 - Šifrovanie	Ochrana logov pred neoprávneným prístupom pri prenose a ukladaní. Šifrovanie (pri prenose aj uložení)
FREQ_154 - Logovanie èinností analytikov poèas riešenia incidentu (audit trail)	Evidencia èinností pre forenznú analýzu. Logovanie èinností analytikov poèas riešenia incidentu (audit trail)

UC_20 –

Obrázok Diagram Sequence : UC_20 – Spravovať znalostnú bázu a knižnicu playbookov

Prípad použitia	UC_20 –
Cie¾	UC_20 rieši, aby mal SOC centrálne a riadene: znalostnú bázu (KB) – články, návody, lessons learned, postupy, knižnicu playbookov – manuálne aj automatizované reakčné postupy, proces schvaľovania, verzovania a publikovania tohto obsahu.

Vstupná podmienka	Existuje modul pre knowledge base a playbooky dostupný pre Analytika a Manažéra.
Vstupná podmienka	Sú definované roly a práva na tvorbu, úpravu a schva¾ovanie obsahu.
Vstupná podmienka	V systéme už existujú aspoò základné KB èlánky alebo playbooky (napr. inicializaèný set).
Výstupná podmienka	Znalostná báza obsahuje aktuálne, verzované a kategorizované záznamy.
Výstupná podmienka	Knižnica playbookov obsahuje publikované a použite¾né playbooky naviazané na typy incidentov.
Výstupná podmienka	Každý záznam má doh¾adate¾nú históriu a informáciu, kto ho vytvoril a schválil.

Basic Path		Basic Path
Krok	**Aktivita**	
1		

2	Analytik vytvorí nový záznam alebo otvorí existujúci a doplní obsah pod¾a aktuálnych poznatkov z incidentov, TI alebo huntovania.
3	Analytik priradí záznam k typom incidentov, kategóriám a tagom, aby bol jednoducho vyh¾adate¾ný v iných UC.
4	Analytik uloží záznam ako draft a odošle ho na schválenie Manažérovi alebo vlastníkovi oblasti.
5	Manažér skontroluje obsah, porovná zmeny s predchádzajúcou verziou a rozhodne o schválení alebo vrátení na úpravu.
6	Po schválení systém oznaèí novú verziu ako platnú a starú verziu presunie do histórie so záznamom o dátume a autorovi zmeny.
7	Platný záznam je sprístupnený v relevantných èastiach systému (napr. v detaile incidentu, v playbook engine, v portáli zákazníka).
8	Systém zaznamená všetky operácie nad záznamom (vytvorenie, úpravy, schválenie) pre audit a forenznú analýzu.

ALT_20_01 – Záznam je vrátený na dopracovanie	Alternate

Krok	**Aktivita**
1	Manažér neodsúhlasí navrhovaný obsah, pridá komentár s pripomienkami a záznam sa vráti Analytikovi do stavu draft.

ALT_20_02 – Záznam je oznaèený ako zastaraný	Alternate

Krok	**Aktivita**
1	nie, no zostane dostupný v histórii.

Naviazané funkèné požiadavky	
	EM
FREQ_140 - Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	
FREQ_174 - Podpora štruktúrovaných dokumentov – kategórie, sekcie, znaèky	Organizácia KB dokumentov pod¾a štruktúrovaných pravidiel (kategórie, tagy, sekcie). Podpora štruktúrovaných dokumentov – kategórie, sekcie, znaèky (tags)
FREQ_175 - Fulltextové vyh¾adávanie s podporou filtrov a tagov	
FREQ_173 - Vytváranie, editácia a verzovanie záznamov	playbooky, FAQ)
Prípad použitia	UC_20a –
Cie¾	UC_20a detailne rieši životný cyklus KB článkov – vytváranie, úpravy, štruktúru, tagovanie a väzbu na incidenty.

Vstupná podmienka	Platí preconditions z UC_20.
Vstupná podmienka	
Výstupná podmienka	KB obsahuje aktuálne, štruktúrované èlánky s bohatým obsahom, históriou zmien a audit trailom.

Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik otvorí v module „Znalostná báza“ zoznam KB èlánkov.
2	Analytik vytvorí nový KB èlánok alebo otvorí existujúci záznam na úpravu.
3	Analytik upraví obsah èlánku, doplní štruktúru (sekcie, podsekcie), tagy a kategórie.

4	Analytik vloží relevantné prílohy, logy alebo snímky obrazovky, ktoré pomáhajú pri riešení podobných incidentov.
5	Analytik uloží záznam, systém zaznamená autora a èas zmeny a pod¾a potreby ho odošle na schválenie.

ALT_20a_01 - Zlúèenie dvoch príbuzných KB záznamov	Alternate

Krok	**Aktivita**
1	Analytik identifikuje dva ve¾mi podobné èlánky v znalostnej báze, vytvorí jeden konsolidovaný záznam a pôvodné èlánky oznaèí ako archivované s odkazom na nový konsolidovaný èlánok.

ALT_20a_02 - Pokus o úpravu bez dostatoèných oprávnení	Alternate

Krok	**Aktivita**
1	vneniach a ponechá záznam bez zmeny.

Naviazané funkèné požiadavky	
FREQ_183 - Záznamy o tom, kto a kedy upravoval dokument	Audit trail zmien dokumentov s informáciou o autoroch a èase. Záznamy o tom, kto a kedy upravoval dokument

Prípad použitia	UC_20b –
Cie¾	UC_20b rieši návrh, úpravu a údržbu playbookov, ktoré SOC využíva pri automatizovanej alebo poloautomatizovanej reakcii (UC_07).

Vstupná podmienka	V systéme je dostupný workflow/playbook engine.
Vstupná podmienka	
Výstupná podmienka	Playbooky majú definované kroky, vetvenie a integraèné body a sú otestované pred nasadením do produkcie.

Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik alebo Developer otvorí sekciu „Playbooky“ v SOCaaS rozhraní.
2	Používate¾ založí nový playbook alebo otvorí existujúci na úpravu.
3	V grafickom editore definuje jednotlivé kroky playbooku, ich poradie, vetvenie a podmienky vykonania.
4	
5	Používate¾ spustí test playbooku v debug/simulaènom režime a overí, že kroky prebiehajú pod¾a oèakávaní.
6	Po úspešnom teste odošle playbook na schválenie Manažérovi a po schválení je oznaèený ako „produkèný“ pre UC_07.

ALT_20b_01 - Playbook neprejde testom v simulaènom režime	Alternate

Krok	**Aktivita**
1	Po spustení testu playbooku v simulaènom režime systém zistí chybu v niektorom kroku alebo chýbajúce parametre, test skonèí s chybou a playbook zostane v stave draft, kým ho Analytik alebo Developer neupravia.

ALT_20b_02 - Uloženie playbooku s neúplnou konfiguráciou	Alternate

Krok	**Aktivita**

1	m ukladanie odmietne a zvýrazní chýbajúce alebo neplatné nastavenia.

Naviazané funkèné požiadavky	
FREQ_067 - Playbook debugging & testing	
	bez potreby programovania
FREQ_060 - Workflow engine s vetvením, podmienkami a sluèkami	

Prípad použitia	UC_20c –
Cie¾	UC_20c rieši governance vrstvu nad KB a playbookmi – schvaľovanie, verzovanie, audit zmien a workflow schválení.

Vstupná podmienka	Existujú drafty alebo upravené verzie KB èlánkov a playbookov (UC_20a, UC_20b).
Vstupná podmienka	
Výstupná podmienka	Každý záznam má stav (draft, v schva¾ovaní, publikovaný, archivovaný) a sledovanú históriu zmien a autorov.

Basic Path	Basic Path

Krok	**Aktivita**
1	Manažér otvorí zoznam KB èlánkov a playbookov, ktoré èakajú na schválenie.
2	Manažér vyberie konkrétny záznam a zobrazí si aktuálnu verziu spolu s preh¾adom zmien oproti predchádzajúcej verzii.
3	Manažér rozhodne, èi záznam schváli, vráti na dopracovanie alebo oznaèí na archiváciu.
4	Pri schválení systém nastaví novú verziu ako platnú, staršiu verziu presunie do histórie a zaznamená dátum a autora schválenia.
5	Systém pod¾a nastaveného workflow informuje relevantných používate¾ov, že nový èlánok alebo playbook je publikovaný a dostupný na použitie.

ALT_20c_01 - Zistená chyba v obsahu po publikovaní	Alternate

Krok	**Aktivita**
1	Po publikovaní novej verzie KB èlánku alebo playbooku si Analytik všimne faktickú chybu, vytvorí opravnú verziu, odošle ju na zrýchlené schválenie a po schválení sa opravná verzia stane platnou.

ALT_20c_02 - Primárny schva¾ovate¾ nie je dostupný	Alternate

Krok	**Aktivita**
1	Záznam èaká na schválenie, ale primárny Manažér je dlhodobo nedostupný, systém po uplynutí definovaného èasu ponúkne schválenie náhradnému schva¾ovate¾ovi pod¾a nastaveného schva¾ovacieho workflow.

Naviazané funkèné požiadavky	

UC_21 –

Obrázok Diagram Sequence : UC_21 – Spravovať a vyhodnocovať modely strojového učenia pre detekciu incidentov

Prípad použitia	UC_21 –

Cie¾	UC_21 rieši životný cyklus ML modelov, ktoré používame na detekciu incidentov a anomálií v SOCaaS: návrh a trénovanie modelov, meranie kvality (FP/FN, presnosť, rýchlosť), robustnosť voči zmene dát, adaptívne/online učenie pri bežiacom systéme.

Vstupná podmienka	SOCaaS má komponent(y) detekcie postavené na ML (anomálie, klasifikátory, scoring).
Vstupná podmienka	Sú dostupné historické dáta/logy na tréning a testovanie modelov.
Vstupná podmienka	
Výstupná podmienka	
Výstupná podmienka	
Výstupná podmienka	Sú evidované výsledky hodnotenia modelov pre ïalšie rozhodovanie a audit.

Basic Path	Basic Path

Krok	**Aktivita**
1	Data Scientist vyberie dátový set (historické logy, incidenty) ako podklad pre tréning alebo testovanie modelu.
2	Data Scientist natrénuje nový model alebo upraví existujúci model na základe aktuálnych požiadaviek na detekciu.
3	Systém vyhodnotí kvalitu modelu na validaènom sete vrátane metriky falošných poplachov a nezachytených incidentov (FP/FN).
4	
5	– èas potrebný na spracovanie nových udalostí v podmienkach blízkych reálnej prevádzke.
6	a kvalitu detekcie
7	Ak model spåòa požadované metriky, Manažér schváli jeho nasadenie do produkcie, Prevádzkovate¾ zabezpeèí nasadenie modelu v detekènom engine.
8	Po nasadení systém priebežne zbiera spätnú väzbu z reálnej prevádzky (skutoèné FP/FN) a pripravuje podklady pre ïalšie ladnie alebo adaptívne uèenie.

ALT_21_02 – Model je príliš pomalý pre reálny èas	Alternate

Krok	**Aktivita**
1	hitektúru, zjednoduší model alebo navrhne offloading na iné prostredie (napr. dedikovaný GPU server).

ALT_21_03 – Objaví sa výrazný dátový drift po nasadení	Alternate

Krok	**Aktivita**
1	Po èase sa zistí, že nové typy udalostí alebo správania znížili kvalitu detekcie; systém upozorní na drift, Data Scientist pripraví aktualizovaný tréningový set a spustí adaptívne/online uèenie, aby model reflektoval nové dáta.

ALT_21_01 – Model má príliš vysoký poèet falošných poplachov (FP)	Alternate

Krok	**Aktivita**

1	Po vyhodnotení sa ukáže, že model generuje neakceptovate¾ne ve¾a FP; Data Scientist upraví architektúru, hyperparametre alebo prahové hodnoty a proces tréningu a hodnotenia zopakuje, kým sa nedosiahne prijate¾ná úroveò.

Naviazané funkèné požiadavky	
FREQ_193 - Adaptívne/online uèenia	
FREQ_186 - Miera falošných poplachov	t FP/FN.

UC_22 –

Obrázok Diagram Sequence : UC_22 – Spravovať a nasadzovať detekčné balíčky a pravidlá

Prípad použitia	UC_22 –
Cie¾	UC_22 rieši životný cyklus detekčného obsahu (pravidlá, korelačné pravidlá, signatúry, „content packy“) v SOCaaS: návrh a úpravu detekčných pravidiel a balíčkov, testovanie na historických alebo syntetických dátach, riadené nasadenie do produkcie, vrátane možnosti rollbacku, obmedzené nasadenie pre vybraných tenantov/zákazníkov. UC_22 nerieši samotný runtime detekcie (to je v UC_03), ale proces návrhu, testovania a riadeného nasadzovania detekčných pravidiel a balíčkov do enginu.

Vstupná podmienka	Existuje detekèný engine (UC_03), ktorý podporuje konfiguráciu pravidiel/balíèkov.
Vstupná podmienka	Platforma má mechanizmus na testovanie pravidiel (oddelené testovacie prostredie alebo test mód).
Vstupná podmienka	
Výstupná podmienka	Nové alebo upravené detekèné pravidlá sú otestované, schválené a nasadené do produkcie alebo zamietnuté.
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik otvorí modul „Detekèné pravidlá a balíèky“ a zobrazí zoznam existujúcich pravidiel.
2	Analytik vytvorí nové pravidlo alebo upraví existujúce, definuje podmienky, prahové hodnoty a mapovanie na typ incidentu.
3	Analytik uloží zmenu ako návrh (draft) a spustí test pravidla na historických alebo syntetických dátach v testovacom režime.
4	Systém vyhodnotí výsledky testu – poèet zásahov, potenciálne falošné poplachy a dopad na existujúcu detekciu.
5	Analytik na základe výsledkov testov prípadne upraví pravidlo a test zopakuje, kým nedosiahne akceptovate¾né správanie.
6	Analytik odošle pravidlo na schválenie Manažérovi alebo definovanému ownerovi detekèného obsahu.

7	Manažér zhodnotí dopad pravidla (najmä na poèet alertov, typy hrozieb a dotknutých zákazníkov/ tenantov) a rozhodne o schválení alebo vrátení na úpravu.
8	Po schválení Developer / DevSecOps spustí nasadenie pravidla do produkcie, prípadne len pre vybrané tenanty alebo v obmedzenom („canary“) režime.
9	Systém zaznamená všetky zmeny (verziu pravidla, autora, schva¾ovate¾a, èas nasadenia) a monitoruje dopady na alerty a výkon.

ALT_22_01 – Test pravidla odhalí extrémne ve¾a zásahov	Alternate

Krok	**Aktivita**
1	Analytik po kroku 4 zistí, že pravidlo by generovalo neprimerané množstvo alertov; pravidlo upraví (sprísnenie podmienok, doplnenie filtrov) a test zopakuje, kým nedosiahne prijate¾ný poèet zásahov.

ALT_22_02 – Nasadené pravidlo negatívne ovplyvní produkciu	Alternate

Krok	**Aktivita**
1	Po nasadení v kroku 8 systém zistí výrazný nárast poètu alertov, latencie alebo chýb; Prevádzkovate¾ alebo DevSecOps iniciuje návrat k predchádzajúcej verzii pravidiel a nové pravidlo sa oznaèí ako „vyžaduje úpravu/test“.

ALT_22_03 –	Alternate

Krok	**Aktivita**
1	Pri schva¾ovaní v kroku 7 Manažér rozhodne, že pravidlo je relevantné len pre urèitý typ zákazníka (napr. konkrétny sektor alebo tenant); pri nasadzovaní sa zvolí len podmnožina tenantov, na ktorých sa pravidlo aplikuje

Naviazané funkèné požiadavky	
FREQ_042 - Machine Learning/ Behaviorálna analýza	
FREQ_044 - Detekcia anomálií	Detekcia neštandardného správania alebo odchýlok od oèakávaného správania. Detekcia anomálií
FREQ_040 - Reálny èas vs. dávkové spracovanie	
FREQ_022 - Detekcia a eskalácia incidentu	námych hrozieb. Po detekcii: • sa generuje alert • alert sa automaticky transformuje na incident • Zammad zabezpeèuje ticket pre L1 tím a podporu eskalácie, • tím vyhodnotí observables a využije obohatenie
FREQ_075 - Analýza logov a korelácia s hrozbami	Analýza logov s cie¾om detekcie korelovaných udalostí a potenciálnych hrozieb. Analýza logov a korelácia s hrozbami

UC_23 –

Obrázok Diagram Sequence : UC_23 – Spravovať a prevádzkovať skenovanie zraniteľností

Prípad použitia	UC_23 –

Cie¾	UC_23 rieši prevádzku a správu skenovania zraniteľností v rámci SOCaaS: plánovanie a spúšťanie skenov, priradenie skenov na aktíva a siete, technickú architektúru skenovania (master/senzor), integráciu nálezov do ticketov a do procesu správy zraniteľností (UC_12).

Vstupná podmienka	Sú známe aspoò základné aktíva a rozsahy sietí (UC_11) urèené na skenovanie.
Vstupná podmienka	V prostredí je nasadený nástroj na skenovanie zranite¾ností (on-prem, VM alebo SaaS).
Vstupná podmienka	
Výstupná podmienka	Skenovanie zranite¾ností pre vybrané rozsahy prebehlo pod¾a plánu alebo na požiadanie.
Výstupná podmienka	Nálezy sú obohatené o CPE/CVE a CVSS skóre a sú dostupné pre UC_12.
Výstupná podmienka	Relevantné nálezy sú exportované alebo prepojené do ticketov na nápravu.

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevádzkovate¾ alebo Správca otvorí modul „Skenovanie zranite¾ností“ a zobrazí preh¾ad existujúcich skenovacích profilov.
2	Prevádzkovate¾ vyberie rozsahy (IP, siete, skupiny aktív) a zvolí typ skenu (plný, rýchly, autentifikovaný).
3	
4	
5	Po dokonèení skenu systém spracuje výsledky, priradí zranite¾nostiam CPE/CVE identifikátory a vypoèíta CVSS skóre.Po dokonèení skenu systém spracuje výsledky, priradí zranite¾nostiam CPE/ CVE identifikátory a vypoèíta CVSS skóre.
6	iešené.Analytik alebo Správca si zobrazí výsledky skenovania, filtruje nálezy pod¾a závažnosti a rozsahu a oznaèí tie, ktoré maj
7	Systém vytvorí alebo aktualizuje tikety na nápravu v integrovanom ticketovacom systéme alebo exportuje nálezy vo zvolenom formáte pre ïalšie spracovanie.

ALT_23_01 –	Alternate

Krok	**Aktivita**
1	Poèas skenu nie sú niektoré systémy dostupné alebo sú blokované firewallom; systém tieto èasti oznaèí ako „neskenované“, Prevádz

ALT_23_02 –	Alternate

Krok	**Aktivita**
1	

Naviazané funkèné požiadavky	
FREQ_096 - Podpora pre CVSS 4.0	Podpora najnovšej verzie skórovacieho systému CVSS. Podpora pre CVSS 4.0
FREQ_087 - Podpora CPE, CVE identifikátorov	
FREQ_090 - Podpora plánovania úloh a alertov	

FREQ_091 - Tikety na nápravu – integrácia alebo export	– integrácia alebo export
FREQ_094 - Architektúra skenovania	

UC_24 – Orchestrácia integrácií medzi SOCaaS a externými systémami

Obrázok Diagram Sequence : UC_24 – Orchestrácia integrácií medzi SOCaaS a externými systémami

Prípad použitia	UC_24 – Orchestrácia integrácií medzi SOCaaS a externými systémami
Cie¾	UC_24 rieši technickú a procesnú orchestráciu integrácií medzi SOCaaS a ďalšími systémami: SIEM, SOAR, CTI, ticketing, komunikačné nástroje, firewall, EDR, API integrácie, webhooky, plug-iny a konektory, jednotné riadenie dátových tokov a akcií naprieč týmito systémami. Cieľom je, aby incident response, automatizácia (UC_07) a správa incidentov fungovali ako jeden prepojený ekosystém, nie ako izolované nástroje.

Vstupná podmienka	Architektúra integrácií zákazníka a SOCaaS je navrhnutá (UC_13) a existuje aspoò základné napojenie na SIEM/SOAR/ticketing.
Vstupná podmienka	SOCaaS platforma podporuje REST API, webhooky a plug-in/konektorový mechanizmus.
Vstupná podmienka	
Výstupná podmienka	Definované integraèné väzby a flow medzi SOCaaS, SIEM, SOAR, CTI, ticketingom, firewallmi, EDR a ïalšími systémami sú aktívne a monitorované.
Výstupná podmienka	Incidenty a udalosti sú konzistentne synchronizované medzi systémami (stav, ID, odkazy).
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevádzkovate¾ otvorí modul „Integrácie a orchestrácia“ a zobrazí preh¾ad existujúcich integraèných väzieb (SIEM, SOAR, CTI, ticketing, EDR, firewall, komunikaèné nástroje).
2	Developer alebo Prevádzkovate¾ vytvorí novú integraènú väzbu alebo upraví existujúcu, zvolí cie¾ový systém (napr. ticketovací systém, CTI, firewall) a typ integrácie (API, webhook, plug-in).
3	Používate¾ nakonfiguruje autentifikáciu, endpointy, formáty dát a mapovanie polí medzi SOCaaS a cie¾ovým systémom.
4	→ vytvor ticket, zmena stavu incidentu → aktualizuj ticket, IOC z TI → aktualizuj blokovací zoznam vo firewalle).
5	
6	íkov/tenantov.
7	–
8	Systém priebežne loguje úspešné a neúspešné integraèné volania, zobrazuje štatistiky a upozoròuje Prevádzkovate¾a na chyby alebo výpadky integraèných kanálov.

ALT_24_01 – Zlyhanie integraèného volania	Alternate

Krok	**Aktivita**

1	Poèas testu alebo produkèného volania API/webhooku externý systém vráti chybu alebo nie je dostupný; SOCaaS záznam oznaèí ako neúspešný, uloží detail chyby a pod¾a nastavenia buï zopakuje volanie s retry politikou, alebo vytvorí interný incident/prehlásenie pre Prevádzkovate¾a.

ALT_24_02 – Konflikt pri mapovaní dát medzi systémami	Alternate

Krok	**Aktivita**
1	Pri nastavovaní mapovania polí medzi SOCaaS a externým systémom sa zistí, že niektoré povinné polia v cie¾ovom systéme nie je moe ktoré sa integrácia používa.

Naviazané funkèné požiadavky	
FREQ_063 - API-first prístup	
FREQ_138 - Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi	Integrácia s inými bezpeènostnými nástrojmi na automatizáciu a workflow. Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi
FREQ_064 - Podpora pre plug-iny a konektory	
FREQ_152 - Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ïalšie systémy cez API alebo pluginy	
FREQ_062 - Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikaèné nástroje, firewall, EDR	Prepojenie a výmena dát s inými systémami v rámci incident response procesu. Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikaèné nástroje, firewall, EDR

UC_25 –

Obrázok Diagram Sequence : UC_25 – Spravovať threat intelligence (CTI) a IOC lifecycle

Prípad použitia	UC_25 –
Cie¾	UC_25 rieši kompletný lifecycle CTI v SOCaaS: získavanie CTI z rôznych zdrojov (feeds, MISP, open-source, vendor), normalizáciu, obohacovanie a prioritizáciu CTI dát, distribúciu IOC/TTP do detekcie (SIEM, EDR, firewall, SOAR) a do incidentov.

Vstupná podmienka	SOCaaS má modul CTI (alebo je integrovaný s externým CTI nástrojom).
Vstupná podmienka	Sú definované CTI zdroje (komunitné, komerèné, interné) a základná politika, ktoré zdroje sú „trusted“.
Vstupná podmienka	Detekèné systémy (SIEM, EDR, firewall, IDS, SOAR) podporujú príjem IOC/TTP z CTI.
Výstupná podmienka	CTI dáta sú systematicky zbierané, normalizované, obohatené a agregované.
Výstupná podmienka	Hrozby sú prioritizované a z relevantných IOC/TTP sú vytvorené podklady pre detekciu, hunting a incidenty.
Výstupná podmienka	IOC/TTP sú distribuované do detekèných systémov a incident managementu konzistentným spôsobom (s audit trailom).

Basic Path	Basic Path

Krok	**Aktivita**

1	Analytik otvorí modul „Threat Intelligence“ a zobrazí preh¾ad aktívnych CTI zdrojov a posledných aktualizácií.
2	Systém periodicky alebo na požiadanie stiahne nové CTI dáta zo všetkých nakonfigurovaných zdrojov (open-source, komunitné, vendor, interné).Systém periodicky alebo na požiadanie stiahne nové CTI dáta zo všetkých nakonfigurovaných zdrojov (open-source, komunitné, vendor, interné).
3	CTI pipeline dáta normalizuje, obohacuje a agreguje – spája IOC, dopåòa kontext, spája s historickými incidentmi a logmi.
4	tnych zákazníkov).
5	a incidentoch.
6	CTI modul vytvorí pre vybrané IOC/TTP výstupy pre detekciu (napr. block listy, SIEM pravidlá, hunting queries) a pripraví ich na distribúciu do pripojených systémov.
7	Analytik má v incidentoch a hunting nástrojoch k dispozícii obohatené CTI – vidí kampane, TTP, skupiny a súvisiace IOC.
8	Systém priebežne zaznamenáva, ktoré CTI zdroje a IOC/TTP boli použité v reálnych incidentoch a hunting prípadoch a tieto informácie používa na ïalšie dolaïovanie scoringu a relevancie.

ALT_25_01 –	Alternate

Krok	**Aktivita**
1	Po èase sa ukáže, že konkrétny CTI zdroj má nekvalitné alebo duplicitné dáta, prípadne je dlhodobo nedostupný; Manažér alebo CTI špecialista zdroj deaktivuje, prípadne zníži jeho váhu v scoringu.

ALT_25_02 – Prebytok CTI a zahltenie analytikov	Alternate

Krok	**Aktivita**
1	Systém deteguje, že množstvo nových IOC/hrozieb výrazne prevyšuje kapacitu analytikov; CTI špecialista upraví scoring, filtre a prahy tak, aby sa do popredia dostali len najrelevantnejšie hrozby (napr. pod¾a sektora, geolokácie, expozície aktív).

ALT_25_03 – Nesúlad CTI medzi zákazníkmi/tenantmi	Alternate

Krok	**Aktivita**
1	Niektorý IOC je relevantný len pre konkrétneho zákazníka (napr. pod¾a jeho technológií alebo geografie); systém podporuje per-tenant filtráciu CTI, takže IOC/TTP sa distribuujú len tým zákazníkom, ktorých sa týkajú.

Naviazané funkèné požiadavky	
FREQ_112 - Podpora najväèšieho poètu autoritatívnych CTI zdrojov	Rozsiahly výber komunitných, verejných a platených zdrojov. Podpora najväèšieho poètu autoritatívnych CTI zdrojov
FREQ_100 - Podpora operatívneho CTI	(TTP, profilovanie skupín)
FREQ_113 - Zníženie potreby manuálnej analýzy	Zautomatizovanie a prioritizácia hrozieb tak, aby sa analytici venovali len relevantným. Zníženie potreby manuálnej analýzy – šetrenie èasu analytikov
FREQ_168 - Podpora rôznych zdrojov: databázy, logy, API výstupy	
FREQ_099 - Podpora strategického CTI	Získavanie a analýza informácií o dlhodobých trendoch, dopadoch útokov a strategických odporúèaniach. Podpora strategického CTI (správy, analýzy dopadu, trendy útokov)
Prípad použitia	UC_25a –

Cie¾	UC_25a rieši ingest a napojenie CTI zdrojov: definovanie zdrojov (feeds, MISP, API, vendor portály), automatizované sťahovanie, použitie štandardizovaných formátov.

Vstupná podmienka	CTI modul je dostupný v SOCaaS.
Vstupná podmienka	Sú známe CTI zdroje, ku ktorým máme prístup (API k¾úèe, URL, autentifikácia).
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	Developer otvorí sekciu „CTI zdroje“ a zobrazí zoznam existujúcich zdrojov.
2	Developer pridá nový zdroj CTI (feed, MISP, vendor API) a zadá potrebné prístupové údaje.
3	
4	Systém otestuje pripojenie, stiahne vzorku dát a overí formát a konzistenciu.
5	Po úspešnom teste je zdroj oznaèený ako aktívny a zapojený do pravidelného CTI ingestu.

ALT_25a_01 – Chyba pri pripojení k CTI zdroju	Alternate

Krok	**Aktivita**
1	Test v kroku 4 zlyhá (chybný API k¾úè, expired token, nedostupný endpoint); systém zobrazí chybu, deaktivuje zdroj a ponechá ho v stave „vyžaduje opravu konfigurácie“.

ALT_25a_02 – Limit alebo kvóty na CTI zdroji	Alternate

Krok	**Aktivita**
1	SOC analytika

Naviazané funkène požiadavky	
FREQ_103 - Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	Pripravené konektory alebo integrácie pre známe CTI zdroje. Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo
FREQ_102 - Automatizované zhromažïovanie z open-source, komunitných a interných zdrojov	ce, komunitných a interných zdrojov
FREQ_111 - Podpora formátov ako STIX/TAXII	Použitie štandardizovaných formátov pre výmenu CTI dát. Podpora formátov ako STIX/TAXII

Prípad použitia	UC_25b –
Cie¾	UC_25b rieši pipeline spracovania CTI: normalizáciu rôznych formátov na jednotný model, obohacovanie IOC a artefaktov z externých služieb, workflow pre automatické/poloautomatické spracovanie CTI.

Vstupná podmienka	CTI dáta sú stiahnuté zo zdrojov (UC_25a).
Vstupná podmienka	Sú nakonfigurované integraèné služby na obohatenie (VirusTotal, Shodan, …).
Výstupná podmienka	CTI dáta sú v jednotnom formáte, obohatené a preverené, pripravené na scoring a distribúciu.

Basic Path	Basic Path

Krok	**Aktivita**
1	Systém prijme nové CTI dáta zo zdrojov a uloží ich do bufferu na spracovanie.
2	CTI pipeline transformuje rôzne formáty do jednotného štruktúrovaného modelu (IOC, TTP, kampane, meta).
3	Pre každý IOC alebo relevantný artefakt pipeline volite¾ne vykoná obohatenie cez externé služby (VirusTotal, Shodan, DomainTools, …).
4	Workflow engine aplikuje definované kroky spracovania – deduplikáciu, filtrovanie, first-seen/last-seen logiku a technické validácie.
5	Výsledné CTI záznamy sú uložené v jednotnej podobe a oznaèené stavom (nové, spracované, nepotvrdené, vyradené).

ALT_25b_01 – Externé obohatenie je doèasne nedostupné	Alternate

Krok	**Aktivita**
1	Pri kroku 3 niektorá externá služba (napr. VirusTotal) neodpovie vèas; systém oznaèí stav obohatenia ako „pending“ a naplánuje opakovaný pokus neskôr bez blokovania celého pipeline.

ALT_25b_02 – Konflikt pri normalizácii CTI dát	Alternate

Krok	**Aktivita**
1	Rôzne zdroje poskytnú pre rovnaký IOC konfliktné informácie; pipeline oznaèí záznam na manuálnu revíziu CTI špecialistom, ktorý vyberie alebo skombinuje správne hodnoty.

Naviazané funkène požiadavky	
FREQ_107 - Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	zjednocovanie údajov
FREQ_104 - Integrácia s 3rd party službami	omainTools, URLScan.io

Prípad použitia	UC_25c –
Cie¾	UC_25c rieši push CTI do zvyšku ekosystému: preposielanie IOC do SIEM/IDS/EDR/firewallov, využitie CTI v detekcii, playbookoch a incidentoch,

Vstupná podmienka	CTI dáta sú spracované a prioritizované (UC_25, UC_25b).
Vstupná podmienka	Existujú integraène väzby na detekène systémy (UC_24).
Výstupná podmienka	Relevantné IOC/TTP sú nasadené v detekèných systémoch.
Výstupná podmienka	Incidenty a hunting prípady sú obohatené CTI metadátami.

Basic Path	Basic Path

Krok	**Aktivita**
1	CTI modul vyberie IOC/TTP, ktoré sú oznaèené ako „relevantné na distribúciu“ pod¾a scoringu a politiky.
2	
3	Systém vygeneruje výstupné artefakty (block listy, SIEM pravidlá, feedy) a odošle ich cez integraèné kanály (API, plug-in, CTI rozhranie).

4	
5	Pri vzniku incidentu SOCaaS incident automaticky obohatí informáciami z CTI – prepojí IOC, TTP a MITRE ATT&CK techniky.

ALT_25c_01 – Detekèný systém neprijme niektoré IOC	Alternate

Krok	**Aktivita**
1	

ALT_25c_02 – IOC je po èase oznaèený ako false positive alebo nerelevantný	Alternate

Krok	**Aktivita**
1	Na základe spätnej väzby z incidentov sa zistí, že niektoré IOC spôsobujú spam v detekcii; CTI modul tieto IOC stiahne z distribúcie a upraví scoring/politiku, aby sa podobné hrozby v budúcnosti hodnotili inak.

Naviazané funkèné požiadavky	
FREQ_110 - Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu	Spájanie incidentov, IOC a TTP s ATT&CK frameworkom. Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu
FREQ_109 - Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	Preposielanie IOC a dát priamo do detekèných systémov (SIEM, IDS, firewall). Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách
FREQ_148 - Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	Integrácia na obohatenie IOC a metadát z CTI alebo iných systémov. Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov

UC_26 –

Obrázok Diagram Sequence : UC_26 – Konfigurovať plánovanie a export reportov

Prípad použitia	UC_26 –
Cie¾	UC_26 rieši praktickú správu reportov v SOCaaS: nastavenie automatického generovania a distribúcie reportov, customizáciu obsahu a vzhľadu reportov, generovanie jednorazových ad-hoc reportov pre manažérov alebo audit.

Vstupná podmienka	V systéme existuje modul reportovania (UC_10) s definovanými typmi reportov (incidenty, SLA, KPI…).
Vstupná podmienka	Sú nakonfigurované kanály distribúcie (minimálne e-mail, ideálne aj webhook/integraèné endpointy).
Výstupná podmienka	Pre jednotlivé typy reportov sú nastavené harmonogramy generovania, príjemcovia a formáty exportu.
Výstupná podmienka	
Výstupná podmienka	Reporty obsahujú zvolené metriky, grafy a vizualizácie v požadovanom dizajne.

Basic Path	Basic Path

Krok	**Aktivita**

1	Manažér alebo Prevádzkovate¾ otvorí modul „Reporty a export“ a zobrazí dostupné typy reportov.
2	
3	Používate¾ nakonfiguruje harmonogram generovania reportu (denne, týždenne, mesaène) a zoznam príjemcov alebo cie¾ových endpointov.
4	Používate¾ upraví vzh¾ad reportu – logo organizácie, záhlavie, poznámky, prípadne štruktúru sekcií.
5	Používate¾ zvolí formát exportu (PDF, CSV, JSON) a spôsob doruèenia (e-mail, webhook, uloženie do úložiska).
6	Systém v definovaných èasoch automaticky vygeneruje report, doplní vybrané grafy, tabu¾ky a štatistiky a odošle ho na zvolené kanály.
7	

ALT_26_01 – Vytvorenie jednorazového ad-hoc reportu	Alternate

Krok	**Aktivita**
1	Manažér potrebuje mimoriadny report mimo plánovaného cyklu; v module zvolí typ reportu, nastaví filtre a èasové obdobie a spustí jednorazové generovanie, prièom systém vygeneruje report len raz bez zmeny existujúcich harmonogramov.

ALT_26_02 – Neúspešné doruèenie automaticky generovaného reportu	Alternate

Krok	**Aktivita**
1	Pri pravidelnom exporte reportu dôjde k chybe pri odoslaní e-mailu alebo webhooku; systém report uloží, oznaèí distribúciu ako n

Naviazané funkène požiadavky	
FREQ_036 - Customizácia výstupov reportov	• • Personalizácia dizajnu – logá, záhlavie, farebná schéma • Zaradenie vysvetliviek, poznámok a kontextuálneho komentára
FREQ_035 - Automatizovaný export reportov	• Periodické reporty – denne, týždenne alebo mesaène generované a distribuované výstupy. • Distribúcia cez e-mail alebo webhook – • Podpora pre templaty a vlastné filtre –b.
FREQ_140 - Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	

UC_27 –

Obrázok Diagram Sequence : UC_27 – Spravovať bezpečnostný stav a vzťahy aktív

Prípad použitia	UC_27 –

Cie¾	UC_27 rozširuje asset management o „smart CMDB“: eviduje bezpečnostný stav každého aktíva (patch level, zraniteľnosti, posledné zmeny), zobrazuje a spravuje väzby medzi aktívami (server–služba–aplikácia), využíva automatizovaný discovery a API integrácie, vedie audit zmien na aktívach.

Vstupná podmienka	Základný inventár aktív je založený (UC_11) – existujú aspoò k¾úèové servery, siete, aplikácie.
Vstupná podmienka	Sú k dispozícii zdroje dát pre discovery (skeny, CMDB, cloud API…).
Vstupná podmienka	Používatelia majú definované roly pre èítanie/úpravu aktív.
Výstupná podmienka	Pre každé aktívum je evidovaný aktuálny bezpeènostný stav (verzie, patch úroveò, zranite¾nosti).
Výstupná podmienka	Medzi aktívami sú definované väzby (topológia / závislosti).
Výstupná podmienka	Zmeny na aktívach sú auditovate¾né (kto, èo, kedy) a dostupné pre forenznú a prevádzkovú analýzu.

Basic Path	Basic Path

Krok	**Aktivita**
1	Správca alebo Prevádzkovate¾ otvorí modul „Aktíva“ a zobrazí preh¾ad aktív s ich aktuálnym bezpeènostným stavom.
2	nty prostredia.
3	Systém spustí discovery a identifikuje nové alebo zmenené aktíva, prièom ich porovná s existujúcim inventárom.
4	Správca skontroluje novo nájdené alebo zmenené aktíva, priradí ich do správnych kategórií a pod¾a potreby upraví detaily (vlastn
5	Správca alebo Architekt doplní alebo upraví väzby medzi aktívami (napr. server → služba → aplikácia → databáza), aby odrážali skutoèné závislosti.
6	Systém automaticky aktualizuje bezpeènostný stav aktív na základe vstupov zo skenovania, patch managementu alebo iných integraèných zdrojov.
7	históriu.

ALT_27_01 – Konflikt medzi discovery a existujúcim inventárom	Alternate

Krok	**Aktivita**
1	Discovery nájde aktívum, ktoré už v inventári existuje, ale s iným oznaèením alebo parametrami; systém oznaèí konflikt, Správca vyberie, èi záznam zlúèi, prepíše, alebo ponechá ako nové aktívum.

ALT_27_02 – Zlyhanie automatizovaného discovery	Alternate

Krok	**Aktivita**
1	

Naviazané funkèné požiadavky	
FREQ_119 - Väzby medzi aktívami	– služba – aplikácia)
FREQ_124 - Automatizovaný discovery assetov v sieti	Automatizovaný zber a aktualizácia údajov o aktívach zo siete a iných systémov. Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov)
FREQ_117 - Evidencia bezpeènostného stavu každého aktíva	Ukladanie informácií o zranite¾nostiach, patch úrovni a aktualizáciách systému. Evidencia bezpeènostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia)

FREQ_122 - Podpora API na správu aktív a integráciu	
FREQ_126 - Zaznamenávanie zmien na aktívach	l)

UC_28 –

Obrázok Diagram Sequence : UC_28 – Nasadiť a udržiavať SOCaaS v rôznych prostrediach

Prípad použitia	UC_28 –
Cie¾	UC_28 rieši nasadenie a technickú prevádzku SOCaaS platformy v rôznych prostrediach: on-premise u zákazníka, v cloude, hybridne, ako vlastné IaaS prostredie pre SOCaaS, s jasnými pravidlami údržby, aktualizácií a monitoringu, vrátane použitia open-source/bezplatnej edície ako základnej platformy. Je to technicko-prevádzkový UC, ktorý rozširuje prevádzku platformy (napr. UC o prevádzke SOCaaS) o multi-deployment / IaaS pohľad.

Vstupná podmienka	Architektúra SOCaaS riešenia je navrhnutá (topológia, moduly, integraèné body).
Vstupná podmienka	
Vstupná podmienka	Prevádzkovate¾ má definované procesy na monitoring, údržbu a aktualizácie komponentov.
Výstupná podmienka	SOCaaS je nasadený v zvolenom prostredí (on-prem/cloud/hybrid/IaaS) a je monitorovaný.
Výstupná podmienka	Sú nastavené pravidlá údržby, aktualizácií a testovania zmien v samostatnom prostredí.
Výstupná podmienka	

Basic Path		Basic Path
Krok	**Aktivita**	
1	Architekt spolu s Prevádzkovate¾om rozhodne, èi bude SOCaaS nasadený on-premise, v cloude alebo v hybridnom modeli.	
2	Prevádzkovate¾ pripraví cie¾ové prostredie – vytvorí potrebné virtuálne stroje, siete, úložiská a ïalšie zdroje v IaaS.	
3	Prevádzkovate¾ nainštaluje alebo nasadí SOCaaS komponenty v zvolenej forme (napr. VM, Docker kontajnery, cloud/SaaS inštancia).	
4	Prevádzkovate¾ nastaví centralizovaný monitoring funkènosti modulov (zber metrik, health-checks, logovanie stavu).	
5		
6	Prevádzkovate¾ definuje pravidlá údržby a aktualizácií – okná údržby, poradie nasadzovania zmien a postup rollbacku.	
7	ky) na zabezpeèenie výkonu a dostupnosti.	
ALT_28_01 —→ cloud alebo hybrid)		Alternate
Krok	**Aktivita**	

1	Na základe rastu alebo požiadaviek zákazníka sa ukáže, že pôvodné on-prem nasadenie už nevyhovuje; Architekt navrhne prechod na cloud alebo hybridný model, Prevádzkovate¾ pripraví nové prostredie a postupný presun komponentov tak, aby zostala zachovaná dos

ALT_28_02 – Aktualizácia spôsobí problémy v produkènom prostredí	Alternate

Krok	**Aktivita**
1	Po nasadení aktualizácie pod¾a krokov 5–6 sa zistí, že niektorý modul nefunguje správne; Prevádzkovate¾ použije pripravený rollback postup, vráti sa na predošlú verziu a aktualizáciu najprv opraví a otestuje v staging prostredí pred ïalším pokusom.

Naviazané funkène požiadavky	
FREQ_093 - Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker	Flexibilita inštalácie do rôznych prostredí. Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker
FREQ_027 - Údržba a aktualizácia systému	• pravidlá pre aktualizácie komponentov • testovacie prostredie na overenie zmien • centralizovaný monitoring funkènosti všetkých modulov
FREQ_037 - Podpora IaaS funkcionality	Riešenie vyžaduje plnú funkcionalitu IaaS –ho prevádzkovania SOC ako služby.
	nia
FREQ_069 - Možnosti nasadenia: on-prem, cloud, hybrid	prem, cloud, hybrid

UC_29 –

Obrázok Diagram Sequence : UC_29 – Vysvetliť a analyzovať anomálie detegované ML modelmi

Prípad použitia	UC_29 –
Cie¾	UC_29 rieši, aby SOCaaS vedel zrozumiteľne vysvetliť anomálie detegované modelmi strojového učenia: zobraziť kontext dátového toku (logy, metriky, sieťové toky), ukázať časový priebeh signálov, ktoré viedli k anomálii, pracovať s unsupervised modelmi (bez labelov), a dať analytikovi interpretáciu „prečo to model označil“.

Vstupná podmienka	V SOCaaS sú nasadené ML modely na detekciu anomálií (UC_21) a generujú anomálne udalosti/alerty.
Vstupná podmienka	– validované, normalizované, obohatené a ukladané.
Vstupná podmienka	Používate¾ (Analytik, Data Scientist) má prístup k modulu „ML anomálie a vysvetlenia“.
Výstupná podmienka	Pre vybranú anomáliu existuje vysvetlenie detekcie – v èase, nad relevantnými vstupmi a s textovým komentárom.
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**

1	Analytik otvorí modul „ML anomálie“ a vyberie konkrétnu anomáliu alebo incident, ktorý bol detegovaný ML modelom.
2	Systém naèíta z dátového pipeline všetky súvisiace udalosti — ktoré prešli validáciou, normalizáciou, obohatením a boli priradené do správnych indexov a èasových peèiatok.
3	Systém identifikuje, ktorý ML model anomáliu detegoval (supervised/unsupervised) a naèíta jeho výstupy (skóre, prípadne èlenstvo v klustri).
4	– k¾úèové signály, èasové úseky a vlastnosti, ktoré najviac prispeli k rozhodnutiu modelu.
5	Systém zobrazí èasový priebeh vybraných metrík a logových udalostí (time series) s vyznaèením intervalu, v ktorom bola anomália detegovaná.
6	Systém zobrazí rozklad vstupov pod¾a typu (logy, metriky, tokové dáta) a ukáže, ktoré skupiny vstupov najviac ovplyvnili detekciu, vrátane prípadu, keï pochádzajú z rôznych zdrojov.
7	Analytik doplní vlastnú interpretáciu, oznaèí detekciu ako „true positive“, „false positive“ alebo „nejasné“ a uloží spätnú väzb

ALT_29_01 – Nedostatoèné dáta na vysvetlenie anomálie	Alternate

Krok	**Aktivita**
1	Pri pokuse o vysvetlenie systém zistí, že v zvolenom èasovom úseku chýbajú niektoré logy alebo metriky (dáta neboli uložené alebo spracované); systém upozorní analytika na obmedzené vysvetlenie, zobrazí len dostupné dáta a oznaèí vysvetlenie ako „neúplné“.

ALT_29_02 – Analytik pretrénuje dôveru v konkrétny model	Alternate

Krok	**Aktivita**
1	Analytik opakovane oznaèí detegované anomálie z jedného modelu ako „false positive“; systém túto spätnú väzbu agreguje a zobrazí Data Scientistovi odporúèanie pre revíziu modelu (prípadne jeho nahradenie iným typom, vrátane zmeny prahu alebo architektúry).

Naviazané funkèné požiadavky	
FREQ_192 - Flexibilita vstupných údajov	_
FREQ_194 - Vysvetlite¾nosti modelu	tikovi zrozumite¾né vysvetlenie, preèo bola anomália detegovaná.
FREQ_028 - Spracovanie dátových tokov	• Príjem logov a udalostí z viacerých heterogénnych zdrojov • Validácia, normalizácia a obohatenie dát • Priradenie èasových peèiatok, identifikátorov a kategórií udalostí • Presmerovanie dát do vhodných indexov pre efektívnu analýzu • Odfiltrovanie redudantných alebo irelevantných údajov • Implementácia pipeline pravidiel a spracovate¾ských modulov
FREQ_187 - Podpora uèenia bez labelov	všetky modely vyžadujú oznaèené dáta. Unsupervised modely sú výhodné najmä pri ve¾kých množstvách nelabelovaných údajov.

UC_30 –

Obrázok Diagram Sequence : UC_30 – Spravovať endpoint detekciu a reakciu (EDR) v rámci SOCaaS

Prípad použitia	UC_30 –

Cie¾	UC_30 rieši, ako SOCaaS centrálne riadi EDR/XDR vrstvu: prijíma alerty a logy z EDR/antivírus/OS nástrojov, normalizuje a obohacuje ich, zobrazuje stav incidentov na dashboardoch, napája ich na celkový proces detekcie incidentov (UC_03) a reakcie (UC_07).

Vstupná podmienka	Na koncových bodoch zákazníka je nasadený EDR/AV/host-based senzor (alebo integraèný agent).
Vstupná podmienka	SOCaaS má integraèné konektory na zber logov a alertov z EDR a ïalších bezpeènostných nástrojov.
Vstupná podmienka	Sú definované základné korelaèné pravidlá a heuristiky pre detekciu endpointových incidentov.
Výstupná podmienka	Alerty a logy z endpoint nástrojov sú prijaté, normalizované a obohatené a využité v detekcii incidentov.
Výstupná podmienka	Stav endpoint incidentov je preh¾adne zobrazovaný na dashboardoch pre analytikov a manažment.
Výstupná podmienka	Endpoint incidenty sú napojené na automatizované reakcie (UC_07), ak je to povolené politikou.

Basic Path	Basic Path

Krok	**Aktivita**
1	
2	Systém prijíma alerty a dáta z rôznych bezpeènostných nástrojov (EDR, AV, OS logy) a zaraïuje ich do jednotného pipeline spracovania.
3	Pipeline transformuje rôzne logy z endpointov do jednotného formátu, dopåòa WHOIS/GEOIP a ïalší kontext a ukladá ich do vhodných indexov pre koreláciu.
4	Detekèný engine (UC_03) používa normalizované endpoint dáta v korelaèných pravidlách a heuristike na identifikáciu potenciálnych incidentov.
5	Keï vznikne incident s pôvodom na koncovom bode, systém ho zobrazí na dashboardoch spolu s kontextom (host, používate¾, typ hrozby, èasová os).
6	Analytik pracuje s endpoint incidentom priamo v SOCaaS – filtruje, triedi, drill-down do detailu logov a obohatenia, prípadne manuálne eskaluje alebo uzatvára.
7	Ak je pre daný typ incidentu definovaný playbook, SOCaaS vyvolá UC_07 a ponúkne automatizované alebo poloautomatizované reakcie (izolácia, karanténa, blokovanie).

ALT_30_01 – Neúplná alebo chybná integrácia EDR	Alternate

Krok	**Aktivita**
1	EDR nástroj neodosiela všetky oèakávané typy alertov alebo logov; systém upozorní Prevádzkovate¾a, že z daného zdroja prichádzaj

ALT_30_02 – Prebytok endpoint alertov (alert fatigue)	Alternate

Krok	**Aktivita**
1	Po napojení EDR príde extrémne ve¾ké množstvo alertov nízkej závažnosti; Analytik a Prevádzkovate¾ upravia filtre, korelaèné pravidlá a prahy tak, aby sa na dashboardoch zobrazovali len relevantné incidenty a zvyšok zostal ako nízko-prioritné udalosti v pozadí.

Naviazané funkèné požiadavky	
FREQ_054 - Prijímanie upozornení a dát z rôznych bezpeènostných systémov	peènostných systémov

FREQ_049 - Dashboardy a ich kategorizácia	Vizualizácia údajov pomocou grafov, filtrov a widgetov. Dashboardy (vrátane interaktívnych) a ich kategorizácia
FREQ_047 - Normalizácia a obohacovanie dát	Transformácia rôznych logov do jednotného formátu a ich rozšírenie (napr. WHOIS, GEOIP). Normalizácia a obohacovanie dát
FREQ_065 - Dashboardy pre stav a štatistiky incidentov	Preh¾adné zobrazenie stavu systému a prebiehajúcich incidentov. Dashboardy pre stav a štatistiky incidentov
FREQ_002 - Proces detekcie incidentov	– je zodpovedný za identifikáciu anomálií, vzorcov útokov a iných hrozieb prostredníctvom korelaèných pravidiel a heuristických mechanizmov.

Prípad použitia	UC_30a –
Cie¾	UC_30a rieši nasadenie a životný cyklus EDR agenta / senzora: inštaláciu na rôzne OS, aktualizácie a konfiguráciu, prípadne využitie agentless režimu tam, kde agent nie je možný

Vstupná podmienka	Je vybraný EDR/endpoint nástroj, ktorý bude použitý v SOCaaS.
Vstupná podmienka	Sú k dispozícii zoznamy koncových bodov a ich OS.
Výstupná podmienka	EDR agent je nasadený alebo nakonfigurovaný (aj v agentless režime) na relevantných koncových bodoch.
Výstupná podmienka	Konfigurácie a aktualizácie agentov sa spravujú centrálne bez zásahov do kódu.

Basic Path	Basic Path

Krok	**Aktivita**
1	
2	Prevádzkovate¾ pripraví inštalaèné balíèky alebo politiky pre nasadenie EDR agenta na podporované OS.
3	Správca nasadí agenta (alebo nakonfiguruje agentless pripojenie) na vybrané koncové body pod¾a politiky zákazníka.
4	Prevádzkovate¾ centrálne nastaví konfiguráciu agentov –
5	ení.

	Alternate

Krok	**Aktivita**
1	ess režim (napr. zber logov cez syslog, WMI, API) a oznaèí tieto zariadenia v systéme ako „agentless“.

Naviazané funkèné požiadavky

FREQ_070 - Podpora pre rôzne OS	Podpora pre inštaláciu a beh agenta na rôznych operaèných systémoch. Podpora pre rôzne OS (Windows, Linux, macOS)
FREQ_155 - Jednoduchá správa konfigurácií a aktualizácií	
FREQ_089 - Bez potreby agentov	

Prípad použitia	UC_30b –
Cie¾	UC_30b rieši samotnú detekciu malvéru, narušení a podozrivého správania na endpointoch: FIM (File Integrity Monitoring), detekciu malvéru, heuristickú/behaviorálnu analýzu.

Vstupná podmienka	Na koncových bodoch beží EDR/agent (UC_30a).
Vstupná podmienka	
Výstupná podmienka	Podozrivé správanie (malvér, narušenia, FIM udalosti) je detegované a mapované na incidenty v SOCaaS.

Basic Path	Basic Path

Krok	**Aktivita**
1	EDR agent monitoruje zmeny súborov, procesov a systémových volaní na koncovom bode.
2	
3	EDR engine analyzuje správanie procesov a pamäte, aby identifikoval znaky malvéru alebo narušenia bezpeènosti.
4	Heuristické a behaviorálne pravidlá (prípadne modely) vyhodnotia kombináciu udalostí a urèia, èi ide o podozrivú aktivitu.
5	Pri prekroèení prahov alebo zodpovedajúcom vzore EDR vytvorí alert, ktorý je následne spracovaný v UC_30/UC_03 ako incident alebo kandidát na incident.

ALT_30b_01 - Podozrivé správanie bez jednoznaèného verdiktu	Alternate

Krok	**Aktivita**
1	Heuristika vyhodnotí aktivitu ako podozrivú, ale nie dostatoène silnú na automatickú klasifikáciu; EDR odošle „low confidence“ a

Naviazané funkèné požiadavky	
FREQ_076 - Detekcia malvéru a narušení	Identifikácia škodlivého softvéru a incidentov narušenia bezpeènosti. Detekcia malvéru a narušení
FREQ_077 - Heuristická a behaviorálna analýza	Založenie detekcie na správaní a heuristike namiesto len signatúr. Heuristická a behaviorálna analýza
FREQ_072 - File Integrity Monitoring	Detekcia zmeny súborov v reálnom èase pre úèely forenznej analýzy a integrity. File Integrity Monitoring (FIM)

Prípad použitia	UC_30c –
Cie¾	UC_30c rieši automatizované/poloautomatizované reakcie na endpoint incidenty a ich mapovanie na MITRE ATT&CK: izolácia zariadenia, karanténa súboru, blokovanie procesov, prepojenie so SOAR playbookmi, bezpečný prenos forenzných dát a reportov.

Vstupná podmienka	Pre endpoint typy incidentov sú definované playbooky reakcie (UC_07).
Vstupná podmienka	EDR nástroj podporuje automatické akcie na koncových bodoch (izolácia, karanténa, blokovanie).
Vstupná podmienka	SOCaaS má mapovanie aktivít na MITRE ATT&CK.
Výstupná podmienka	Endpoint incidenty sú mapované na ATT&CK TTP a použité v reportoch a CTI.
Výstupná podmienka	Automatizované reakcie sú vykonané bezpeène a auditovate¾ne, vrátane bezpeèného prenosu reportov a forenzných dát.

Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik alebo systém identifikuje endpoint incident, pri ktorom je vhodná automatizovaná reakcia (napr. malvér na koncovej stanici).
2	SOCaaS priradí incidentu relevantné MITRE ATT&CK techniky a zobrazuje ich v detaile incidentu.

3	Analytik spustí playbook alebo systém automaticky vyhodnotí podmienky a vykoná akciu (izolácia zariadenia, karanténa súboru, zablokovanie procesu).
4	
5	Systém vygeneruje súhrnný report o priebehu incidentu a vykonaných reakciách a bezpeène ho odošle cez šifrovaný kanál (napr. manažérovi alebo zákazníkovi).

ALT_30c_01 - Automatizovaná reakcia je zablokovaná politikou	Alternate

Krok	**Aktivita**
1	Manažér nastavil politiku, že na kritických serveroch nie je dovolená plne automatická izolácia; pri takom incidente SOCaaS ponúkne len „poloautomatickú“ akciu vyžadujúcu explicitné potvrdenie analytikom.

Naviazané funkène požiadavky	
FREQ_172 - Šifrované prenosy reportov pri automatickej distribúcii	Bezpeèný prenos citlivých dát cez šifrované kanály. Šifrované prenosy reportov pri automatickej distribúcii
FREQ_079 - Mapovanie na MITRE ATT&CK framework	Zaradenie detegovaných aktivít a techník do rámca MITRE ATT&CK pre úèely TTP analýz. Mapovanie na MITRE ATT&CK framework
FREQ_080 - Automatické reakcie	Automatická reakcia na incidenty, ako je izolácia koncového bodu alebo karanténa súborov. Automatické reakcie (napr. izolácia zariadenia, karanténa súboru)

UC_31 –

Obrázok Diagram Sequence : UC_31 – Poskytovať pracovný priestor pre manuálnu analýzu hrozieb (CTI workspace)

Prípad použitia	UC_31 –
Cie¾	UC_31 rieši, aby SOCaaS poskytoval dedikovaný pracovný priestor pre manuálnu analýzu hrozieb (CTI): analytik si vie otvoriť konkrétnu hrozbu, IOC alebo kampaň, vidí znormalizované dáta z viacerých CTI zdrojov, má nástroje na ručné skúmanie, filtrovanie a doplĺňanie komentárov.

Vstupná podmienka	CTI pipeline je funkèná (UC_25) – CTI dáta sú stiahnuté a technicky spracované.
Vstupná podmienka	
Výstupná podmienka	Pre vybrané hrozby / IOC existujú ruène doplnené analýzy a komentáre od analytika.
Výstupná podmienka	

Basic Path	Basic Path

Krok	**Aktivita**
1	
2	Systém naèíta z CTI úložísk všetky dostupné informácie o danej hrozbe – IOC, popisy, zdrojové feedy – a zobrazí ich v jednotnom, normalizovanom formáte.
3	Analytik použije dostupné nástroje (filtrovanie, pivotovanie na IOC, prepojenie na incidenty a logy) na ruèné preskúmanie dát a kontextu hrozby.
4	Analytik doplní vlastné komentáre, hodnotenie relevancie, odporúèania a prípadne oznaèí hrozbu pre konkrétnych zákazníkov/segmenty.
5	portoch.

ALT_31_01 – CTI dáta pre hrozbu sú neúplné alebo nekonzistentné	Alternate

Krok	**Aktivita**
1	Analytik v kroku 2 zistí, že informácie o hrozbe z rôznych zdrojov si odporujú alebo sú neúplné; oznaèí záznam ako „vyžaduje doplnenie“, doplní manuálne poznámky a CTI špecialista neskôr upraví zdroje alebo scoring.

ALT_31_02 – Analytik otvorí CTI workspace priamo z incidentu	Alternate

Krok	**Aktivita**
1	Pri vyšetrovaní incidentu v UC_06 klikne na prepojenú hrozbu/IOC; systém otvorí CTI workspace už predfiltrovaný na relevantné IO

Naviazané funkène požiadavky	
FREQ_005 - Proces správy hrozieb	– umožòuje systematickú prácu s informáciami o hrozbách.
FREQ_055 - Normalizácia a parsovanie dát	Transformácia vstupných dát do štandardizovaného formátu pre ïalšie spracovanie. Normalizácia a parsovanie dát

UC_32 –

Obrázok 34 : UC_32 – Monitorovať skenovanie zraniteľností a synchronizovať stav súvisiacich incidentov

Prípad použitia	UC_32 –
Cie¾	UC_32 rieši operatívny pohľad na skenovanie zraniteľností a súvisiace incidenty: poskytuje webové rozhranie na správu skenov a výsledkov (nad funkciami z UC_23), zobrazuje, ktoré nálezy boli už prekonvertované na incidenty, a zabezpečuje synchronizáciu stavu incidentov medzi SIEM a SOAR, aby mali analytici všade konzistentný stav.

Vstupná podmienka	Skenovanie zranite¾ností je technicky nastavené a beží pod¾a UC_23.
Vstupná podmienka	Existuje integraèné napojenie medzi SIEM a SOAR (pod¾a UC_24).
Vstupná podmienka	
Výstupná podmienka	Používatelia majú k dispozícii preh¾adné webové rozhranie, cez ktoré vidia skeny, ich stav a výsledky.
Výstupná podmienka	Nálezy zo skenovania, ktoré sú spracované ako incidenty, majú synchronizovaný stav medzi SIEM a SOAR (napr. „open / in progress / resolved“).

Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik alebo Správca otvorí modul „Skenovanie a incidenty“ vo webovom rozhraní SOCaaS a vidí preh¾ad spustených a plánovaných skenov.
2	Používate¾ si vyberie konkrétny sken a zobrazí detail – rozsah, èas spustenia, stav, poèet nájdených zranite¾ností a základné štatistiky.
3	V tom istom rozhraní si používate¾ zobrazí zoznam nálezov skenovania, prièom každý nález je prepojený na svoj aktuálny stav (nový, v riešení, uzatvorený) a informáciu, èi k nemu už existuje incident v SIEM/SOAR.

4	Systém zobrazuje, pre ktoré nálezy bol vytvorený incident v SOAR a automaticky overuje, aký stav má tento incident v SIEM (napr. „open“, „assigned“, „resolved“).
5	Pri zmene stavu incidentu v SOAR (napr. po vykonaní playbooku) modul UC_32 cez integraènú vrstvu aktualizuje stav incidentu aj v SIEM, aby mali analytici a manažment všade konzistentnú informáciu.
6	

ALT_32_01 – Incident v SOAR existuje, ale SIEM stav nepozná	Alternate

Krok	**Aktivita**
1	Pri kroku 4 systém zistí, že v SOAR existuje incident nad konkrétnym nálezom, ale v SIEM sa nenachádza korešpondujúci záznam (napr. integraèná chyba alebo historický incident); systém nález oznaèí ako „nekonzistentný“ a upozorní Prevádzkovate¾a, aby skontroloval integraèné pravidlá alebo manuálne zarovnal incidenty.

ALT_32_02 –	Alternate

Krok	**Aktivita**
1	Pri naèítaní preh¾adu v kroku 1 alebo 2 dôjde k chybe v API (napr. skener nedostupný); UI zobrazí upozornenie, ktoré skeny/výsle

Naviazané funkèné požiadavky	
FREQ_068 - SOAR-SIEM synchronizácia stavu incidentov	
FREQ_088 - Prijate¾né webové rozhranie na správu skenovania a výsledkov	