PROJEKT

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

V11 – Biznis architektúra

KPB4 – Architektúra riešenia

typ – dokumentácia

mesiac odovzdania – M16

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1 MANAŽÉRSKE ZHRNUTIE

Zainteresované strany

- Manažment (strategické rozhodovanie, SLA)
- SOC tím (operátori, analytici)
- IT oddelenie zákazníka
- Auditor
- Zákazníci (tenanti)
- Regulačné orgány

1.1 Zámer riešenia

Zámerom projektu je vyvinúť technologicky moderné, otvorené a škálovateľné riešenie, ktoré bude schopné podporiť organizácie v efektívnom zvládaní kybernetických hrozieb v súlade s legislatívnymi požiadavkami, ako sú smernice NIS2 a národné zákony o kybernetickej bezpečnosti. Projekt reaguje na potreby najmä malých a stredných organizácií, ktoré často nedisponujú dostatočnými odbornými kapacitami ani rozpočtom na vybudovanie vlastného bezpečnostného centra. Navrhované riešenie tak prinesie cenovo dostupnú a kvalitnú alternatívu, ktorá prispeje k zvýšeniu úrovne kybernetickej bezpečnosti na národnej aj európskej úrovni. Zároveň podporí vzdelávanie odborníkov v tejto oblasti, prehĺbi spoluprácu medzi akademickou sférou a praxou a vytvorí priestor na ďalší výskum a inovácie v oblasti kybernetickej bezpečnosti.

1.2 Ciele riešenia

Hlavným cieľom navrhovaného riešenia je vybudovanie otvoreného, multitenantného a flexibilného SOC riešenia poskytovaného ako cloudová služba, ktorá dokáže reagovať na rastúce nároky na kybernetickú bezpečnosť a zároveň bude cenovo dostupná aj pre organizácie s obmedzenými kapacitami. Tento cieľ bude naplnený prostredníctvom integrácie automatizačných mechanizmov, technológií virtualizácie a pokročilých algoritmov strojového učenia na báze hlbokých neurónových sietí, ktoré umožnia detegovať a predikovať anomálne správanie v systémoch v reálnom čase.

Špecifické ciele zahŕňajú návrh technologického riešenia SOC na úrovni TRL 3, návrh inteligentného monitorovacieho systému vrátane parametrov pre sledovanie a reakciu na incidenty, návrh architektúry elastickej služby INNOSOC s proaktívnym prístupom k ochrane informačných aktív, vývoj vhodných algoritmov strojového učenia a vytvorenie online platformy pre zdieľanie výsledkov projektu a podporu otvorenej vedy.

1.3 KPI riešenia

Pre hodnotenie úspešnosti navrhovaného riešenia budú stanovené kľúčové ukazovatele výkonnosti (KPI).

Medzi kľúčové ukazovatele výkonnosti (KPI) patria:

- MTTR (Mean Time To Recovery) – priemerný čas obnovenia služby
- HA (High Availability) – dostupnosť systému aj pri výpadkoch častí infraštruktúry
- presnosť detekcie anomálií
- rýchlosť reakcie na incident
- počet detekovaných bezpečnostných incidentov

- počet používateľov platformy pre zdieľanie výsledkov
- náklady na prevádzku
- čas implementácie riešenia

1.4 Rozsah riešenia

Riešenie pokrýva návrh a vývoj architektúry multitenantného SOC, ktorý bude fungovať ako služba dostupná prostredníctvom cloudovej infraštruktúry. Zahŕňa návrh virtualizovanej platformy s vysokou mierou automatizácie, ktorá umožní efektívnu správu, monitorovanie a škálovanie podľa potreby. V rámci riešenia bude vybudovaný inteligentný systém pre monitoring infraštruktúry a služieb, ktorý bude schopný rýchlej detekcie a reakcie na incidenty. Projekt sa zameria na integráciu otvorených technológií vrátane open source komponentov, aby bola zabezpečená transparentnosť, udržateľnosť a flexibilita riešenia. Súčasťou riešenia bude aj návrh algoritmov strojového učenia pre detekciu a predikciu bezpečnostných a operačných anomálií, vrátane mechanizmov validácie ich účinnosti. Riešenie sa zároveň rozšíri o platformu na zdieľanie výsledkov a poznatkov v súlade s princípmi otvorenej vedy, čím podporí praktické vzdelávanie a ďalší výskum v oblasti kybernetickej bezpečnosti.

1.5 Stručný popis navrhovaného riešenia

Navrhované riešenie v rámci projektu INNOSOC sa sústreďuje na vybudovanie multitenantného operačného centra kybernetickej bezpečnosti (SOC), ktoré bude poskytované ako otvorená a flexibilná cloudová služba. Riešenie bude využívať virtualizáciu a kontajnerové technológie na zabezpečenie škálovateľnosti a vysokej dostupnosti. Integráciou prvkov automatizácie a pokročilých metód strojového učenia, najmä hlbokých neurónových sietí (DNN), sa zvýši schopnosť systému efektívne detegovať a predikovať anomálie v reálnom čase. Služba bude navrhnutá tak, aby bola dostupná aj pre menšie a stredné organizácie, ktoré často nemajú dostatočné rozpočtové alebo personálne kapacity na budovanie vlastných SOC riešení. Významným aspektom návrhu je orientácia na otvorené technológie, ktoré umožnia budúce rozširovanie a prispôsobovanie platformy podľa aktuálnych potrieb trhu aj legislatívy.

2 ANALÝZA POŽIADAVIEK

2.1 Postup analýzy požiadaviek

Analýza požiadaviek v projekte INNOSOC bude prebiehať systematicky a v súlade s princípmi metodík PRINCE2 a TOGAF, ktoré partneri projektu bežne využívajú na riadenie podobných inovatívnych iniciatív. Tento proces bude realizovaný v niekoľkých fázach s cieľom identifikovať, špecifikovať, validovať a dokumentovať všetky funkčné a nefunkčné požiadavky na navrhované multitenantné SOC riešenie poskytované formou cloudovej služby.

Prvým krokom bude zber požiadaviek prostredníctvom workshopov, individuálnych rozhovorov a dotazníkov so zainteresovanými stranami projektu, vrátane technických expertov, manažmentu, ako aj budúcich používateľov riešenia. V tejto fáze sa budú zisťovať očakávania, potreby a problémy, ktoré riešenie musí adresovať, pričom dôraz sa bude klásť na špecifiká vyplývajúce z legislatívy NIS2 a zákona o kybernetickej bezpečnosti.

Následne budú požiadavky systematicky analyzované a klasifikované podľa priorít, dopadu na projekt a technickej realizovateľnosti. Bude sa rozlišovať medzi požiadavkami na funkcionalitu samotnej SOC platformy (napr. detekcia anomálií, reporting, automatizovaná

reakcia) a nefunkčnými požiadavkami (napr. dostupnosť, výkon, bezpečnosť, škálovateľnosť). Pre účely modelovania a ďalšej validácie budú požiadavky vizualizované pomocou UML a Archimate diagramov, aby sa overilo ich správne pochopenie a súlad s architektonickým návrhom riešenia.

Validácia požiadaviek bude zabezpečená prostredníctvom kontrolných stretnutí, priebežných revízií a spätných väzieb od používateľov aj odborníkov v oblasti kybernetickej bezpečnosti. Takýto iteratívny prístup umožní včas odhaliť prípadné nedostatky alebo konflikty v požiadavkách, ktoré by mohli ohroziť kvalitu výsledného riešenia.

Výsledky analýzy požiadaviek budú priebežne zaznamenávané v centralizovanom systéme riadenia požiadaviek a budú tvoriť súčasť oficiálnej projektovej dokumentácie. Tento postup zabezpečí transparentnosť celého procesu, vysledovateľnosť zmien a zároveň poskytne základ pre overovanie kvality počas vývoja, testovania a implementácie riešenia.

2.2 Motivačná architektúra

**Obsahová náplň tejto podkapitoly bude doplnená neskôr, nakoľko je výstup V11 stále v rozpracovanej verzii.*

2.3 Katalóg požiadaviek a jeho mapovanie na návrh ich riešenia

**Obsahová náplň tejto podkapitoly bude doplnená neskôr, nakoľko je výstup V11 stále v rozpracovanej verzii.*

2.4 Legislatíva, smernice a metodické materiály zohľadnené v riešení

**Obsahová náplň tejto podkapitoly bude doplnená neskôr, nakoľko je výstup V11 stále v rozpracovanej verzii.*

2.5 Akceptačné kritéria

**Obsahová náplň tejto podkapitoly bude doplnená neskôr, nakoľko je výstup V11 stále v rozpracovanej verzii.*

3 BIZNIS ARCHITEKTÚRA RIEŠENIA

Business capibilities:

- Monitoring a analýza bezpečnostných dát
- Incident detection a response (vrátane automatizácie reakcií)
- Správa logov a ich korelácia
- Reporting a vizualizácia stavu bezpečnosti
- Integrácia s EDR/XDR, CTI a ďalšími nástrojmi
- Správa incidentov a ticketing
- Správa assetov a zraniteľností
- Knowledge base pre SOC tímy
- Podpora strojového učenia pre detekciu anomálií

Prepojenia na IT systémy (Application Landscape):

Integrácia s:

- SIEM
- SOAR
- EDR/XDR
- CTI
- Vulnerability scanner
- Ticketing system
- Asset management

Komunikačné rozhrania štandardne cez REST API alebo iné štandardné protokoly. Deployment prostredníctvom Kubernetes s podporou kontajnerizácie.

3.1 Existujúca a cieľová biznis architektúra

**Obsahová náplň tejto podkapitoly bude doplnená neskôr, nakoľko je výstup V11 stále v rozpracovanej verzii.*

3.2 Procesy podporované navrhovaným riešením

Kľúčové procesy podporené riešením (z dokumentov):

- Zber, filtrovanie a normalizácia logov
- Korelácia bezpečnostných udalostí
- Detekcia hrozieb a ich prioritizácia
- Automatizovaná reakcia na incidenty (SOAR playbooky)
- Správa a archivácia incidentov
- Reporting a SLA monitoring
- Pravidelný audit a kontrola konfigurácií
- Integrácia s inými bezpečnostnými systémami

3.3 Vytvorenie informačnej architektúry a mapovanie používateľskej cesty

**Obsahová náplň tejto podkapitoly bude doplnená neskôr, nakoľko je výstup V11 stále v rozpracovanej verzii.*

3.4 Prípad použitia (use case model)

3.4.1 Používateľské roly – aktéri

Táto kapitola popisuje roly – aktérov, ktorí vystupujú v systéme:

- Prevádzkovateľ platformy
- Správca infraštruktúry
- Incident handler
- DevSecOps
- Poskytovateľ služby
- Data Scientist
- ML špecialista
- ML inžinier
- Architekt
- Vedúci tímu SOC
- Prevádzkovateľ
- Prevádzkový tím
- Vedúci SOC
- SOC operátor
- SLA operátor
- SOC analytik
- Forenzný analytik
- Koncový používateľ
- Správca systému
- Operátor
- Analytik
- Auditor

3.4.2 Používateľské príbehy a Prípady použitia

Táto kapitola popisuje používateľské príbehy ako jednotlivé funkčné moduly majú pomôcť zainteresovanej strane napĺňať jej kompetencie a prípady použitia akým spôsobom.

3.4.2.1 User stories a use cases pre SIEM

Ako zákazník chcem, aby platforma monitorovala a analyzovala moje bezpečnostné dáta v reálnom čase, aby som mal istotu, že budem upozornený na potenciálne útoky alebo incidenty bez zbytočných prieťahov.

Ako bezpečnostný analytik chcem, aby SIEM automaticky koreloval udalosti z rôznych zdrojov, aby som mohol efektívne odhaliť komplexné útoky a ich súvislosti.

Ako manažér bezpečnosti chcem mať k dispozícii pravidelné reporty a prehľadné dashboardy, aby som vedel preukázať dodržiavanie SLA a stav bezpečnosti pred vedením spoločnosti.

Ako systémový integrátor chcem, aby sa SIEM dokázal integrovať s inými bezpečnostnými nástrojmi cez štandardné API,aby som zabezpečil funkčnú spoluprácu s EDR, SOAR a inými systémami.

Ako bezpečnostný architekt chcem, aby SIEM šifroval všetky prenášané a uložené údaje, aby bola zaistená dôvernosť a integrita bezpečnostných dát.

Ako DevOps inžinier chcem, aby SIEM bolo možné prevádzkovať v Kubernetes prostredí s multitenantným prístupom,aby bola platforma flexibilná a škálovateľná pre viacero zákazníkov naraz.

UC 1.1 – Zber bezpečnostných údajov

Primárny aktér: Systémový integrátor

Cieľ: Zo zbieraných logov získať kompletné bezpečnostné údaje z rôznych typov zariadení (servery, sieťové prvky, cloud, kontajnery).

Hlavný scenár:

1. Integrátor nakonfiguruje zdroj logov v SIEM systéme
2. SIEM prijíma dáta v rôznych formátoch
3. Dáta sú uložené a pripravené na ďalšie spracovanie

UC 1.2 – Detekcia hrozieb v reálnom čase

Primárny aktér: Bezpečnostný analytik
Cieľ: Zachytiť bezpečnostné incidenty s minimálnym oneskorením
Hlavný scenár:

1. SIEM monitoruje prichádzajúce udalosti
2. Vyhodnocuje ich cez detekčné algoritmy
3. Generuje okamžité upozornenia
4. Upozornenie je zaslané analytikovi

UC 1.3 – Korelácia udalostí

Primárny aktér: Bezpečnostný analytik
Cieľ: Detegovať vzory útokov kombinovaním udalostí z rôznych zdrojov
Hlavný scenár:

1. Analytik definuje korelačné pravidlá
2. SIEM aplikuje pravidlá v reálnom čase
3. V prípade zhody SIEM vygeneruje alert
4. Alert sa zobrazuje na dashboarde

UC 1.4 – Dashboardy a vizualizácia

Primárny aktér: Bezpečnostný analytik, manažér bezpečnosti, auditor
Cieľ: Zobraziť kľúčové metriky a stavy v prehľadnej forme
Hlavný scenár:

1. Používateľ sa prihlási do SIEM rozhrania
2. Vyberie požadované zobrazenie dashboardu
3. Zobrazia sa grafy, tabuľky a prehľady
4. Používateľ môže filtrovať a exportovať dáta

UC 1.5 – Reporting

Primárny aktér: Manažér bezpečnosti, auditor
Cieľ: Získať pravidelné alebo ad-hoc reporty
Hlavný scenár:

1. Manažér nastaví plánovaný report
2. SIEM generuje report v požadovanom formáte
3. Report je doručený e-mailom alebo dostupný na export
4. Auditor si ho overí a archivuje

UC 1.6 – Integrácia systémov

Primárny aktér: Systémový integrátor
Cieľ: Prepojiť SIEM s inými bezpečnostnými systémami
Hlavný scenár:

1. Integrátor nakonfiguruje API konektory
2. SIEM naviaže komunikáciu s externými nástrojmi (napr. SOAR)
3. Otestuje prenos dát
4. Integrácia je pripravená na ostrú prevádzku

UC 1.7 – Zabezpečenie údajov

Primárny aktér: Bezpečnostný architekt
Cieľ: Zaistiť ochranu údajov počas prenosu aj ukladania
Hlavný scenár:

1. Architekt nastaví šifrovanie TLS pre prenos
2. Uložené dáta sú šifrované na diskoch
3. Prístup je riadený cez RBAC
4. Kontroly auditov potvrdia bezpečné nastavenia

UC 1.8 – Škálovateľnosť a rozšíriteľnosť

Primárny aktér: Architekt riešenia, DevOps inžinier
Cieľ: Umožniť rast výkonu a funkcionality bez prerušenia
Hlavný scenár:

1. DevOps nasadí SIEM v Kubernetes
2. Otestuje rozšírenie počtu workerov
3. Overí, že dáta sú spracovávané bez straty
4. Architekt preverí multitenantné oddelenie

UC 1.9 – Rozšírenia (pluginy, pravidlá)

Primárny aktér: Vývojár, DevOps
Cieľ: Dopĺňať SIEM o nové funkcionality
Hlavný scenár:

1. Vývojár pripraví nový plugin
2. Nasadí ho bez potreby vypnutia jadra
3. Testuje jeho funkciu na testovacích logoch
4. Plugin je zaradený do produkcie

3.4.2.2 User stories a use cases pre Spracovanie logov

Ako zákazník chcem, aby všetky moje logy boli zhromaždené a spracované jednotne, aby som mal prehľad o bezpečnostných udalostiach a ich histórii.

Ako bezpečnostný analytik chcem, aby sa logy automaticky normalizovali a filtrovali podľa definovaných pravidiel, aby som vedel rýchlo vyhľadávať a analyzovať bezpečnostné incidenty.

Ako systémový integrátor chcem, aby bolo možné napojiť rôzne logovacie systémy a zdroje, aby som zabezpečil kompletný zber údajov zo všetkých relevantných zariadení a aplikácií.

Ako administrátor chcem, aby logy boli archivované a šifrované, aby bola zabezpečená ich dlhodobá ochrana a auditovateľnosť.

Ako DevOps inžinier chcem, aby bolo možné spracovanie logov horizontálne škálovať, aby systém zvládol rast objemu dát bez výpadkov.

UC 2.1 – Zber logov

Primárny aktér: Systémový integrátor
Cieľ: Zabezpečiť príjem logov z rôznych typov zariadení a systémov
Hlavný scenár:

1. Integrátor definuje zoznam zdrojov logov
2. Nastaví parametre zberu (napr. protokol, port, formát)
3. Systém prijíma a ukladá logy
4. Oznámi úspešné pripojenie zdrojov

UC 2.2 – Normalizácia a filtrovanie

Primárny aktér: Bezpečnostný analytik
Cieľ: Pretransformovať logy do jednotného formátu a odfiltrovať irelevantné záznamy
Hlavný scenár:

1. Analytik nastaví normalizačné pravidlá
2. Systém aplikuje konverzie na prichádzajúce logy
3. Filtrovanie odstráni nepotrebné údaje
4. Výsledné normalizované logy sú pripravené na koreláciu

UC 2.3 – Vyhľadávanie v logoch

Primárny aktér: Bezpečnostný analytik
Cieľ: Rýchlo a efektívne vyhľadávať bezpečnostné udalosti v zozbieraných logoch
Hlavný scenár:

1. Analytik zadá dotaz (napr. kľúčové slovo, časový interval)
2. Systém vyhľadá v indexoch logov
3. Zobrazí výsledky vrátane možnosti filtrovania a fulltextu
4. Analytik vyhodnotí výsledky a môže exportovať nálezy

UC 2.4 – Vizualizácia logov

Primárny aktér: Analytik, administrátor
Cieľ: Prehľadne zobraziť logy v nástrojoch typu Kibana alebo Grafana
Hlavný scenár:

1. Analytik vyberie vizualizačný nástroj
2. Systém poskytne normalizované logy v kompatibilnom formáte
3. Dáta sa vizualizujú v dashboardoch (grafy, tabuľky)
4. Používateľ si môže vizualizácie uložiť

UC 2.5 – Podpora viacerých modulov pre zber

Primárny aktér: Systémový integrátor
Cieľ: Umožniť použitie nástrojov ako Fluent Bit, Fluentd, Logstash, OpenTelemetry či Graylog
Hlavný scenár:

1. Integrátor rozhodne o nástroji pre zber
2. Nastaví príslušné konektory
3. Systém začne spracovávať logy cez vybraný modul
4. Overí funkčnosť integrácie

UC 2.6 – Archivácia logov

Primárny aktér: Administrátor, audítor
Cieľ: Uchovávať logy dlhodobo a bezpečne
Hlavný scenár:

1. Administrátor nastaví politiku archivácie
2. Logy sa komprimujú a šifrujú
3. Ukladajú sa do dlhodobého úložiska
4. Audítor overí prístup a integritu archivovaných dát

UC 2.7 – Vyhľadávanie a filtrovanie (rozšírené)

Primárny aktér: Bezpečnostný analytik
Cieľ: Použiť pokročilé dotazy vrátane regulárnych výrazov
Hlavný scenár:

1. Analytik nastaví komplexný vyhľadávací filter
2. Systém spracuje dotaz na štruktúrované aj nestruktúrované dáta
3. Výsledky sú zoradené a agregované
4. Používateľ môže výsledky exportovať

UC 2.8 – Prepojenie so SIEM

Primárny aktér: Systémový integrátor
Cieľ: Automaticky posielať spracované logy do SIEM systému
Hlavný scenár:

1. Integrátor nastaví cieľový SIEM endpoint
2. Systém odosiela logy cez zabezpečený kanál
3. Overí doručenie a integritu dát
4. Logy sú okamžite pripravené na koreláciu v SIEM

UC 2.9 – Kontajnerizácia a nasadenie

Primárny aktér: DevOps, administrátor infraštruktúry
Cieľ: Prevádzkovať spracovanie logov v kontajneroch
Hlavný scenár:

1. DevOps pripraví Docker image pre spracovanie logov
2. Nasadí systém do Kubernetes prostredia
3. Otestuje škálovanie a redundanciu
4. Administrátor kontroluje prevádzku a monitoring

3.4.2.3 User stories a use cases pre SOAR

Ako zákazník chcem, aby bezpečnostné incidenty boli riešené čo najrýchlejšie a konzistentne, aby som minimalizoval dopady na moju organizáciu.

Ako bezpečnostný analytik chcem automatizovať opakujúce sa reakcie na incidenty, aby som sa mohol sústrediť na komplexnejšie analýzy.

Ako incident handlerchcem mať k dispozícii pripravené playbooky na riešenie incidentov, aby som nemusel manuálne koordinovať každú akciu.

Ako systémový integrátor chcem, aby sa SOAR dokázal prepojiť s ostatnými bezpečnostnými nástrojmi, aby reakcie boli koordinované naprieč celým ekosystémom.

Ako auditor chcem mať možnosť sledovať a auditovať všetky automatizované reakcie, aby som dokázal preveriť postupy riešenia incidentov.

UC 3.1 – Automatizácia reakcií na incidenty

Primárny aktér: Bezpečnostný analytik
Cieľ: Automaticky vykonať reakcie na incidenty na základe vopred definovaných pravidiel
Hlavný scenár:

1. Analytik nastaví playbook pre reakciu
2. SOAR monitoruje incidenty zo SIEM alebo EDR
3. Pri zhode spustí preddefinované kroky (napr. izolácia, blokovanie IP)
4. Loguje vykonané akcie

UC 3.2 – Kategorizácia incidentov

Primárny aktér: Bezpečnostný analytik, incident handler
Cieľ: Priradiť incidenty podľa typu a závažnosti
Hlavný scenár:

1. SOAR prijme incident z iného systému
2. Vyhodnotí jeho parametre (napr. zdroj, typ hrozby, dopad)
3. Priradí prioritu a kategóriu
4. Posunie incident na riešenie príslušnému pracovníkovi

UC 3.3 – Orchestrácia medzi nástrojmi

Primárny aktér: Systémový integrátor
Cieľ: Koordinovať akcie naprieč rôznymi bezpečnostnými nástrojmi
Hlavný scenár:

1. Integrátor nastaví integračné rozhrania (napr. API pre SIEM, CTI, EDR)
2. SOAR spustí koordinované reakcie vo viacerých systémoch
3. Vyhodnotí výsledky reakcií
4. Zaznamená auditnú stopu

UC 3.4 – Tvorba a úprava playbookov

Primárny aktér: Bezpečnostný analytik, DevSecOps
Cieľ: Jednoducho definovať reakčné scenáre bez nutnosti programovania
Hlavný scenár:

1. Analytik otvorí editor playbookov
2. Definuje kroky reakcie pomocou drag-and-drop alebo skriptovania
3. Otestuje ich v simulovanom prostredí
4. Publikuje playbook do produkcie

UC 3.5 – Evidencia a audit reakcií

Primárny aktér: Auditor, manažér bezpečnosti
Cieľ: Uchovávať kompletný záznam o vykonaných akciách
Hlavný scenár:

1. SOAR zaznamenáva každý krok reakcie
2. Ukladá metaúdaje (čas, používateľ, výsledok)
3. Auditor si prehliada históriu
4. Exportuje report pre legislatívne účely

UC 3.6 – Flexibilita reakčných scenárov

Primárny aktér: Bezpečnostný analytik
Cieľ: Jednoducho prispôsobiť reakcie meniacim sa podmienkam
Hlavný scenár:

1. Analytik vyhodnotí nový typ incidentu
2. Upravením playbooku doplní nové kroky
3. Overí testovacie scenáre
4. Nová verzia je okamžite dostupná

UC 3.7 – Integrácia s ekosystémom

Primárny aktér: Systémový integrátor
Cieľ: Napojiť SOAR na ostatné systémy (napr. ticketing, CMDB, SIEM)
Hlavný scenár:

1. Definovanie API pre pripojenie
2. Overenie funkčnosti integrácie
3. Synchronizácia údajov medzi systémami
4. Automatizované spúšťanie reakcií na základe dát z iných systémov

UC 3.8 – Reverzná reakcia

Primárny aktér: Systémový architekt, analytik
Cieľ: V prípade zlyhania obnoviť pôvodný stav
Hlavný scenár:

1. Automatizovaná reakcia zlyhá
2. SOAR vyvolá rollback proces
3. Vráti konfigurácie alebo systém do predchádzajúceho stavu
4. Ohlási analytikovi výsledok

UC 3.9 – Bezpečné spúšťanie aplikácií

Primárny aktér: Správca systému, bezpečnostný architekt
Cieľ: Zabezpečiť, že automatizované reakcie sú vykonávané oprávnene
Hlavný scenár:

1. Správca nastaví prístupové práva na playbooky
2. Každá akcia prejde kontrolou oprávnení
3. SOAR overí identity používateľov
4. Vykoná iba povolené reakcie

3.4.2.4 User stories a use cases pre Detekciu pomocou ML (strojového učenia)

Ako zákazník chcem, aby systém vedel identifikovať aj nové a neznáme typy útokov, aby som bol lepšie chránený pred modernými hrozbami.

Ako bezpečnostný analytik chcem využívať modely strojového učenia na podporu detekcie anomálií, aby som zvýšil presnosť a znížil počet falošných poplachov.

Ako Data Scientist chcem mať možnosť trénovať a testovať modely ML na aktuálnych dátach, aby som zabezpečil, že modely budú relevantné a aktuálne.

Ako bezpečnostný architekt chcem, aby modely boli transparentné a vysvetliteľné, aby som dokázal obhájiť ich rozhodnutia pred auditom alebo manažmentom.

Ako DevOps inžinier chcem, aby ML komponenty boli škálovateľné, aby zvládali veľké množstvo dát a prípadné navyšovanie objemu logov.

UC 4.1 – Detekcia anomálií

Primárny aktér: Bezpečnostný analytik, Data Scientist
Cieľ: Zachytiť anomálie v sieťovej prevádzke, logoch a správaní používateľov
Hlavný scenár:

1. Analytik definuje parametre sledovania
2. ML model monitoruje dáta v reálnom čase
3. Identifikuje odchýlky od bežného správania
4. Generuje upozornenie na podozrivú aktivitu

UC 4.2 – Predikcia incidentov

Primárny aktér: Bezpečnostný analytik, manažér bezpečnosti
Cieľ: Odhadovať pravdepodobnosť budúcich incidentov na základe historických dát
Hlavný scenár:

1. Systém analyzuje historické logy a incidenty
2. ML model vyhodnotí pravdepodobnosť incidentov
3. Vytvorí prediktívne výstupy (napr. incident score)
4. Manažér ich použije pri plánovaní kapacít alebo prevencie

UC 4.3 – Aktualizácia ML modelov

Primárny aktér: Bezpečnostný analytik, manažér bezpečnosti
Cieľ: Odhadovať pravdepodobnosť budúcich incidentov na základe historických dát
Hlavný scenár:

1. Systém analyzuje historické logy a incidenty
2. ML model vyhodnotí pravdepodobnosť incidentov
3. Vytvorí prediktívne výstupy (napr. incident score)
4. Manažér ich použije pri plánovaní kapacít alebo prevencie

UC 4.4 – Podpora viacerých ML knižníc

Primárny aktér: Vývojár ML riešení
Cieľ: Integrovať rôzne algoritmy a knižnice (napr. TensorFlow, PyTorch)
Hlavný scenár:

1. Vývojár vyberie vhodnú knižnicu
2. Implementuje požadovaný algoritmus
3. Otestuje jeho funkciu v rámci platformy
4. Uloží konfiguráciu na opakované použitie

UC 4.5 – Hodnotenie modelov

Primárny aktér: Data Scientist, bezpečnostný architekt
Cieľ: Overiť kvalitu a spoľahlivosť detekcie
Hlavný scenár:

1. Data Scientist spustí hodnotenie modelu
2. Vyhodnotí presnosť, mieru falošne pozitívnych/negatívnych výsledkov
3. Pripraví report pre architekta
4. Architekt schváli alebo navrhne úpravy

UC 4.6 – Vysvetliteľnosť modelov

Primárny aktér: Bezpečnostný analytik, manažér
Cieľ: Porozumieť, prečo ML model vyhodnotil konkrétnu udalosť ako hrozbu
Hlavný scenár:

1. Analytik otvorí detail výstupu modelu
2. Systém zobrazí vysvetlenie (napr. LIME, SHAP)
3. Analytik overí správnosť rozhodnutia
4. Dokumentuje výsledok pre audit

UC 4.7 – Pipeline pre trénovanie

Primárny aktér: ML inžinier, Data Scientist
Cieľ: Bezpečne a efektívne pripravovať trénovacie dáta
Hlavný scenár:

1. ML inžinier nastaví zber dát do pipeline
2. Overí kvalitu a konzistenciu dát
3. Spustí tréning modelu
4. Zaznamená proces a výsledky

UC 4.8 – Integrácia ML výstupov so SIEM/SOAR

Primárny aktér: Systémový integrátor
Cieľ: Posunúť výsledky ML modelov do ďalších bezpečnostných nástrojov
Hlavný scenár:

1. Integrátor nastaví konektor medzi ML modulom a SIEM/SOAR
2. Overí prenos výsledkov
3. SIEM/SOAR použije ML výstupy na koreláciu alebo spustenie reakcie
4. Testuje celú workflow v reálnom prostredí

UC 4.9 – Škálovateľnosť ML infraštruktúry

Primárny aktér: DevOps, ML inžinier
Cieľ: Zabezpečiť výkon aj pri veľkom objeme dát
Hlavný scenár:

1. DevOps pripraví cloud alebo Kubernetes infraštruktúru
2. Otestuje horizontálne škálovanie
3. Monitoruje výkonnostné metriky
4. Optimalizuje náklady na prevádzku

3.4.2.5 User stories a use cases pre Vizualizácia dát

Ako zákazník chcem mať prehľadné a interaktívne dashboardy s kľúčovými údajmi, aby som vedel rýchlo vyhodnotiť bezpečnostnú situáciu v mojej organizácii.

Ako bezpečnostný analytik chcem vizualizovať výsledky detekcie a korelácie incidentov, aby som lepšie pochopil vzťahy medzi jednotlivými udalosťami.

Ako manažér bezpečnosti chcem vidieť SLA reporty a výkonnostné metriky v prehľadnej forme, aby som ich vedel prezentovať vedeniu alebo audítorom.

Ako systémový integrátor chcem, aby sa vizualizácia dala integrovať so SIEM a ďalšími systémami, aby som nemusel manuálne prenášať dáta.

Ako administrátor chcem, aby prístup do vizualizačného rozhrania bol cez jednotné prihlásenie (SSO), aby sa dodržali bezpečnostné politiky organizácie.

UC 5.1 – Tvorba interaktívnych dashboardov

Primárny aktér: Bezpečnostný analytik, manažér bezpečnosti
Cieľ: Zobraziť stav bezpečnostného prostredia v reálnom čase
Hlavný scenár:

1. Analytik otvorí vizualizačný modul
2. Vyberie požadované metriky (napr. počty incidentov, detekované hrozby)
3. Systém zobrazí interaktívne grafy a tabuľky
4. Dashboard je uložený a dostupný na ďalšie použitie

UC 5.2 – Používanie šablón pre vizualizácie

Primárny aktér: Analytik
Cieľ: Využiť preddefinované šablóny na rýchle nasadenie vizualizácií
Hlavný scenár:

1. Analytik si vyberie šablónu (napr. SLA, NIS2 monitoring)
2. Pripojí vhodné dátové zdroje
3. Systém automaticky vygeneruje grafy a reporty
4. Analytik môže prispôsobiť farby, filtre a usporiadanie

UC 5.3 – Integrácia so SIEM

Primárny aktér: Systémový integrátor
Cieľ: Získať vizualizácie priamo z dát SIEM systému
Hlavný scenár:

1. Integrátor nastaví pripojenie na SIEM backend
2. Dáta sa prenášajú v reálnom čase
3. Vizualizačný nástroj ich interpretuje do grafov a tabuliek
4. Výsledky sú dostupné na monitorovanie a reporting

UC 5.4 – Jednotné prihlásenie (SSO)

Primárny aktér: Administrátor
Cieľ: Umožniť bezpečný prístup do vizualizačného rozhrania
Hlavný scenár:

1. Administrátor nastaví SSO (napr. SAML, LDAP, OAuth2)
2. Používateľ sa autentifikuje jedným prihlasovaním
3. Systém overí jeho rolu a práva
4. Zobrazí personalizované dashboardy

UC 5.5 – Korelácia vizualizácií

Primárny aktér: Bezpečnostný analytik
Cieľ: Zobraziť súvislosti medzi udalosťami v prehľadnej forme
Hlavný scenár:

1. Analytik zvolí korelačné pravidlá (napr. časová os, sieťové väzby)
2. Vizualizačný nástroj načíta príslušné dáta
3. Grafické prvky znázornia vzťahy
4. Analytik vyhodnotí zobrazené závislosti

UC 5.6 – Dynamická aktualizácia dát

Primárny aktér: Operátor, analytik
Cieľ: Zobrazovať vždy aktuálne údaje
Hlavný scenár:

1. Systém monitoruje prichádzajúce nové dáta
2. Dashboardy sa aktualizujú v reálnom čase
3. Používateľ nemusí manuálne obnovovať stránku
4. Vizualizácia odráža aktuálny stav

UC 5.7 – Zálohovanie konfigurácií dashboardov

Primárny aktér: Administrátor systému
Cieľ: Uložiť a obnoviť nastavenia vizualizácií
Hlavný scenár:

1. Administrátor exportuje konfiguráciu dashboardu
2. Uloží ju do úložiska (napr. git, cloud)
3. V prípade potreby importuje zálohu späť
4. Dashboard sa obnoví vrátane nastavení a filtrov

UC 5.8 – Viac jazyčné rozhranie

Primárny aktér: Koncový používateľ
Cieľ: Pracovať s dashboardmi vo vlastnom jazyku
Hlavný scenár:

1. Používateľ nastaví preferovaný jazyk
2. GUI sa prispôsobí vybranému jazyku
3. Preklady sú dostupné v celom rozhraní
4. Používateľ pokračuje vo vizualizácii v zvolenom jazyku

UC 5.9 – Prepojenie s externými dátovými zdrojmi

Primárny aktér: Systémový integrátor
Cieľ: Dopĺňať vizualizácie o údaje z iných systémov (napr. CTI, EDR)
Hlavný scenár:

1. Integrátor nastaví konektory na externé zdroje
2. Overí správnosť a integritu dát
3. Vizualizačný modul načíta obohatené údaje
4. Používateľ ich môže zahrnúť do reportov

3.4.2.6 User stories a use cases pre Alterovanie

Ako zákazník chcem byť okamžite informovaný o bezpečnostných incidentoch, aby som mohol čo najskôr reagovať a minimalizoval dopady na prevádzku.

Ako bezpečnostný analytik chcem, aby systém automaticky generoval upozornenia na základe definovaných pravidiel, aby som nemusel manuálne sledovať všetky zdroje.

Ako manažér bezpečnosti chcem, aby alerty podporovali eskaláciu podľa priorít, aby žiadny kritický incident neostal bez povšimnutia.

Ako administrátor chcem mať možnosť prispôsobiť spôsob doručovania alertov, aby vyhovoval technickým a organizačným potrebám našej spoločnosti.

Ako auditor chcem, aby všetky alerty boli archivované a auditovateľné, aby som vedel spätne overiť, ako sa riešili incidenty.

UC 6.1 – Generovanie notifikácií

Primárny aktér: Bezpečnostný analytik
Cieľ: Automaticky upozorniť na bezpečnostné udalosti
Hlavný scenár:

1. Analytik nastaví pravidlá pre generovanie alertov
2. Systém monitoruje udalosti v reálnom čase
3. Pri splnení podmienok vytvorí notifikáciu
4. Upozornenie je doručené cez definovaný kanál

UC 6.2 – Definovanie pravidiel pre alerty

Primárny aktér: Analytik, administrátor
Cieľ: Určiť podmienky, pri ktorých sa majú generovať upozornenia
Hlavný scenár:

1. Používateľ otvorí konfiguráciu alertov
2. Zadá podmienky (napr. typ incidentu, závažnosť, zdroj)
3. Uloží pravidlá
4. Systém ich začne aplikovať na prichádzajúce dáta

UC 6.3 – Viackanálové doručovanie notifikácií

Primárny aktér: Administrátor, manažér
Cieľ: Posielať upozornenia rôznymi spôsobmi
Hlavný scenár:

1. Administrátor nakonfiguruje doručovacie kanály (e-mail, SMS, chat, webhook)
2. Priradí ich ku konkrétnym typom alertov
3. Systém doručuje upozornenia podľa priority a typu
4. Overí úspešné doručenie

UC 6.4. – Automatické vyplnovanie obsahu alertu

Primárny aktér: Bezpečnostný analytik
Cieľ: Uľahčiť čitateľnosť alertu generovaním názvu a popisu
Hlavný scenár:

1. Systém analyzuje incident
2. Vytvorí názov a popis na základe obsahu (napr. zdroj, cieľ, typ útoku)
3. Pripojí tieto údaje do notifikácie
4. Odošle ich adresátovi

UC 6.5 – Eskalačné pravidlá

Primárny aktér: Manažér bezpečnosti, SLA operátor
Cieľ: Zaistiť reakciu na alerty v prípade nečinnosti
Hlavný scenár:

1. Manažér nastaví eskalačné pravidlá (napr. čas, úroveň priorít)
2. Ak analytik nereaguje, alert sa automaticky eskaluje
3. Systém oznámi eskaláciu ďalšiemu pracovníkovi
4. Zaznamená tento proces do logu

UC 6.6 – Okamžité doručovanie v reálnom čase

Primárny aktér: SOC operátor
Cieľ: Minimalizovať oneskorenie pri doručovaní kritických upozornení
Hlavný scenár:

1. Systém vyhodnotí incident ako kritický
2. Odosiela alert okamžite
3. Overí úspešné prijatie
4. SOC operátor reaguje podľa playbooku

UC 6.7 – Archivácia a audit alertov

Primárny aktér: Auditor, manažér SOC
Cieľ: Uložiť všetky upozornenia na neskoršie preverenie
Hlavný scenár:

1. Systém zaznamenáva všetky vygenerované alerty
2. Ukladá ich do archívu
3. Auditor môže vyhľadávať a filtrovať historické dáta
4. Exportuje report pre kontrolu

UC 6.8 – Podmienené generovanie alertov

Primárny aktér: Analytik
Cieľ: Podporiť komplexné „ak-tak“ logické pravidlá
Hlavný scenár:

1. Analytik nastaví viacpodmienkové pravidlá (napr. kombinácia viacerých zdrojov a typov incidentov)
2. Systém tieto pravidlá aplikuje
3. Alert sa vygeneruje len pri splnení všetkých podmienok
4. Zobrazí sa v dashboarde

UC 6.9 – Prepojenie s reakčnými systémami

Primárny aktér: Systémový integrátor
Cieľ: Automaticky preposielať alerty do SOAR alebo ticketingu
Hlavný scenár:

1. Integrátor nakonfiguruje konektory
2. Alerty sa pri generovaní okamžite odosielajú do SOAR alebo ticketingu
3. Spustia ďalšie playbooky alebo vytvoria tiket
4. Overí sa úspešné priradenie

3.4.2.7 User stories a use cases pre EDR/XDR (Endpoint Detection and Response/ Extended Detection and Response)

Ako zákazníkchcem, aby boli moje koncové zariadenia neustále monitorované a chránené, aby sa znížilo riziko kompromitácie a škôd.

Ako bezpečnostný analytikchcem mať možnosť sledovať podozrivú aktivitu na endpointoch v reálnom čase, aby som vedel rýchlo reagovať a riešiť incidenty.

Ako SOC operátor chcem automaticky izolovať podozrivé zariadenia, aby sa zabránilo šíreniu útoku do celej siete.

Ako administrátor systému chcem, aby riešenie podporovalo rôzne prostredia (cloud, on-premise, kontajnery), aby bolo flexibilné a prispôsobené infraštruktúre mojej organizácie.

Ako audítor chcem, aby boli všetky akcie EDR/XDR auditované, aby bolo možné spätne skontrolovať postup riešenia incidentov.

UC 7.1 – Monitorovanie aktivít na koncových zariadeniach

Primárny aktér: Bezpečnostný analytik
Cieľ: Získať informácie o aktivitách na PC, serveroch a kontajneroch
Hlavný scenár:

1. Systém nepretržite zbiera dáta z endpointov
2. Analytik sleduje podozrivé procesy, siete a súbory
3. Pri odhalení anomálie dostane notifikáciu
4. V prípade potreby spustí reakciu

UC 7.2 – Detekcia hrozieb na endpointoch

Primárny aktér: SOC analytik, forenzný analytik
Cieľ: Automaticky rozpoznať známe aj neznáme hrozby
Hlavný scenár:

1. Systém vyhodnocuje správanie procesov a sieťových spojení
2. Porovnáva so signatúrami aj ML modelmi
3. Identifikuje podozrivú aktivitu
4. Generuje upozornenie alebo spustí reakciu

UC 7.3. – Reakcia na incident na endpointoch

Primárny aktér: Bezpečnostný analytik
Cieľ: Rýchlo obmedziť dopad incidentu
Hlavný scenár:

1. Analytik alebo automatika spustí reakciu
2. Systém izoluje koncové zariadenie od siete
3. Ukončí podozrivé procesy alebo odstráni súbory
4. Potvrdí úspešné vyriešenie incidentu

UC 7.4. – Zber auditných údajov

Primárny aktér: Administrátor systému, analytik
Cieľ: Uchovať kompletnú históriu aktivít a udalostí
Hlavný scenár:

1. Systém priebežne zaznamenáva auditné logy
2. Ukladá ich do zabezpečeného úložiska
3. Umožňuje filtrovanie a vyhľadávanie
4. Audítor môže spätne kontrolovať udalosti

UC 7.5. – Dashboard pre správu EDR/XDR

Primárny aktér: SOC operátor, manažér bezpečnosti
Cieľ: Vizualizovať stav zariadení a incidentov
Hlavný scenár:

1. Operátor otvorí EDR/XDR dashboard
2. Sleduje stav zariadení, detekované incidenty a intervencie
3. Filtrovaním získava detailnejšie pohľady
4. Používa prehľady na riadenie bezpečnosti

UC 7.6 – Preposielanie incidentov do SOC

Primárny aktér: Systémový integrátor
Cieľ: Integrovať výstupy EDR/XDR do centrálneho SOC
Hlavný scenár:

1. Integrátor nakonfiguruje rozhranie s SIEM alebo SOAR
2. Incidenty sa automaticky posielajú do SOC
3. SOC ich spracováva a vyhodnocuje v širšom kontexte
4. Potvrdí integráciu a konzistenciu dát

UC 7.7 – Flexibilné zberové režimy

Primárny aktér: Administrátor, integrátor
Cieľ: Podporiť agentové aj bezagentové režimy
Hlavný scenár:

1. Administrátor rozhodne, kde je vhodný agent
2. Nastaví bezagentové snímanie v kontajneroch alebo cloude
3. Overí funkčnosť zberu dát
4. Kombinuje oba prístupy podľa prostredia

UC 7.8 – Automatická reakcia

Primárny aktér: Operátor, analytik
Cieľ: Minimalizovať čas reakcie na incident
Hlavný scenár:

1. Systém vyhodnotí závažný incident
2. Spustí vopred definovanú reakciu bez zásahu človeka
3. Izoluje zariadenie alebo zablokuje proces
4. Zapíše udalosť do logu a informuje analytika

UC 7.9 – Export pre ďalšie systémy

Primárny aktér: ML analytik, integrátor
Cieľ: Odoslať dáta do SIEM, ML alebo iných nástrojov
Hlavný scenár:

1. Integrátor definuje cieľový systém
2. Nastaví formát exportu (JSON, CSV, API)
3. Dáta sa prenášajú pravidelne alebo on-demand
4. Overí integritu prenesených údajov

3.4.2.8 User stories a use cases pre CTI (Cyber Threat Intelligence)

Ako zákazník chcem, aby moja organizácia využívala overené hrozbové spravodajstvo, aby sme boli pripravení na aktuálne aj budúce kybernetické útoky.

Ako bezpečnostný analytik chcem mať prístup k databázam indikátorov kompromitácie (IoC), TTP a reputačných zoznamov, aby som vedel efektívne detegovať a vyhodnocovať hrozby.

Ako SOC operátor chcem, aby sa CTI integrovalo do SIEM/SOAR automaticky, aby som mohol incidenty priamo obohacovať o spravodajské dáta.

Ako manažér bezpečnosti chcem reporty o aktuálnych trendoch hrozieb a kampaniach, aby som dokázal pripraviť organizáciu na relevantné riziká.

Ako systémový integrátor chcem, aby bolo možné CTI jednoducho prepojiť cez API s inými systémami, aby boli hrozbové dáta aktuálne a dostupné v celom ekosystéme.

UC 8.1 – Obohatenie incidentov o hrozbové dáta

Primárny aktér: Bezpečnostný analytik
Cieľ: Získať kontext k incidentom a lepšie určiť prioritu
Hlavný scenár:

1. Analytik prijme incident zo SIEM
2. CTI poskytne informácie o reputácii IP/domén
3. Analytik vyhodnotí riziko a rozhodne o reakcii
4. Incident sa spracuje s bohatším kontextom

UC 8.2 – Získavanie indikátorov kompromitácie (IoC)

Primárny aktér: SOC analytik
Cieľ: Použiť IoC pre detekciu a prevenciu
Hlavný scenár:

1. Systém importuje IoC zo CTI feedov
2. Integruje ich do SIEM pravidiel
3. Deteguje výskyty IoC v prichádzajúcich logoch
4. Generuje alerty pri zhode

UC 8.3 – Reporting trendov a hrozieb

Primárny aktér: Manažér bezpečnosti
Cieľ: Získať prehľad o aktuálnych kampaniach a taktikách útočníkov
Hlavný scenár:

1. CTI modul generuje pravidelný report
2. Obsahuje informácie o TTP (Tactics, Techniques, Procedures)
3. Manažér analyzuje trendy
4. Prijíma opatrenia na zvýšenie odolnosti

UC 8.4 – Integrácia CTI do SIEM/SOAR

Primárny aktér: Systémový integrátor
Cieľ: Automaticky obohatiť incidenty a playbooky
Hlavný scenár:

1. Integrátor nakonfiguruje CTI API konektor
2. Údaje sa synchronizujú do SIEM/SOAR
3. Playbooky využívajú CTI informácie pri reakcii
4. Overí sa konzistencia a aktuálnosť dát

UC 8.5 – Správa reputačných databáz

Primárny aktér: Analytik
Cieľ: Udržiavať kvalitné a aktuálne reputačné zoznamy
Hlavný scenár:

1. Analytik spravuje whitelist/blacklist položky
2. Aktualizuje zoznamy podľa CTI feedov
3. Distribuuje zmeny do bezpečnostných systémov
4. Monitoruje ich efektivitu

UC 8.6 – Obohatenie ML modelov o CTI dáta

Primárny aktér: Data Scientist, bezpečnostný analytik
Cieľ: Zlepšiť presnosť detekcie v ML
Hlavný scenár:

1. ML inžinier integruje CTI feedy do tréningových dát
2. Model sa prispôsobí aktuálnym hrozbám
3. Vyhodnotí sa presnosť a false positives
4. Nový model sa nasadí do produkcie

UC 8.7 – Vyhľadávanie v repozitári CTI

Primárny aktér: SOC analytik
Cieľ: Manuálne overiť podozrivé artefakty
Hlavný scenár:

1. Analytik zadá IP, doménu alebo hash
2. CTI modul vyhľadá informácie v repozitári
3. Zobrazí výsledky (napr. históriu, reputáciu, typ hrozby)
4. Analytik rozhodne o ďalšom kroku

UC 8.8 – Automatizované aktualizácie CTI feedov

Primárny aktér: Administrátor
Cieľ: Zabezpečiť, aby hrozbové dáta boli vždy aktuálne
Hlavný scenár:

1. Administrátor nastaví plán sťahovania feedov
2. Systém automaticky aktualizuje IoC, TTP, reputácie
3. Kontroluje integritu a úplnosť dát
4. Loguje priebeh aktualizácií

UC 8.9 – Zabezpečenie CTI dát

Primárny aktér: Bezpečnostný architekt
Cieľ: Ochrana citlivých hrozbových dát pred únikom
Hlavný scenár:

1. Architekt definuje prístupové práva k CTI dátam
2. Implementuje šifrovanie prenosu aj úložiska
3. Priebežne audituje prístupové logy
4. Reviduje oprávnenia podľa potreby

3.4.2.9 User stories a use cases pre Tiketovací systém

Ako zákazník chcem mať prehľad o stave riešenia svojich bezpečnostných incidentov prostredníctvom tiketov, aby som vedel, kedy a ako boli riešené.

Ako SOC operátor chcem jednoducho vytvárať a aktualizovať tikety pre incidenty, aby som zefektívnil komunikáciu a evidenciu ich spracovania.

Ako manažér bezpečnosti chcem sledovať SLA a eskalácie priamo v tiketovacom systéme, aby som garantoval rýchlu reakciu podľa dohodnutých pravidiel.

Ako audítor chcem mať k dispozícii kompletnú históriu tiketov a ich zmien, aby som vedel preukázať, ako sa incidenty riešili.

Ako integrátor chcem, aby tiketovací systém spolupracoval s ostatnými modulmi (SOAR, SIEM), aby sa tikety vytvárali a aktualizovali automaticky.

UC 9.1 – Vytvorenie tiketu

Primárny aktér: SOC operátor
Cieľ: Zaevidovať nový incident alebo požiadavku
Hlavný scenár:

1. Operátor otvorí formulár na vytvorenie tiketu
2. Vyplní potrebné polia (typ incidentu, priorita, popis)
3. Tiket sa uloží do databázy
4. Pridelí sa zodpovednej osobe

UC 9.2 – Aktualizácia tiketu

Primárny aktér: SOC operátor, analytik
Cieľ: Priebežne dokumentovať stav riešenia incidentu
Hlavný scenár:

1. Operátor otvorí existujúci tiket
2. Doplní nové informácie (napr. priebeh riešenia, priložené dôkazy)
3. Uloží zmeny
4. Systém zaznamená históriu úprav

UC 9.3 – Uzavretie tiketu

Primárny aktér: SOC operátor
Cieľ: Formálne ukončiť riešenie incidentu
Hlavný scenár:

1. Operátor overí, že incident bol vyriešený
2. Zaznamená ukončujúcu správu
3. Tiket sa označí ako uzavretý
4. Archívne sa uchová pre audit

UC 9.4 – Eskalácia tiketu

Primárny aktér: SOC operátor
Cieľ: Formálne ukončiť riešenie incidentu
Hlavný scenár:

1. Operátor overí, že incident bol vyriešený
2. Zaznamená ukončujúcu správu
3. Tiket sa označí ako uzavretý
4. Archívne sa uchová pre audit

UC 9.5 – Prepojenie do SIEM/SOAR

Primárny aktér: Systémový integrátor
Cieľ: Automatizovať vznik a aktualizáciu tiketov
Hlavný scenár:

1. Integrátor nastaví API konektory
2. SIEM alebo SOAR automaticky vytvoria tiket pri incidente
3. Priebežné aktualizácie sa synchronizujú
4. Overí sa konzistencia dát

UC 9.6 – SLA monitoring

Primárny aktér: Manažér bezpečnosti
Cieľ: Sledovať plnenie dohodnutých reakčných časov
Hlavný scenár:

1. Manažér nastaví SLA parametre
2. Systém sleduje časy riešenia jednotlivých tiketov
3. Pri prekročení času upozorní manažéra
4. Exportuje SLA report pre zákazníka

UC 9.7 – Reporting a štatistiky

Primárny aktér: Manažér, auditor
Cieľ: Získať prehľad o výkonnosti riešenia incidentov
Hlavný scenár:

1. Manažér otvorí reporting modul
2. Vyberie rozsah dátumov a filtre (napr. typ incidentu)
3. Systém zobrazí grafy, tabuľky, trendy
4. Reporty je možné exportovať

UC 9.8 – Prístupové práva k tiketom

Primárny aktér: Administrátor
Cieľ: Nastaviť oprávnenia pre rôzne úlohy a role
Hlavný scenár:

1. Administrátor definuje role (napr. operátor, manažér, auditor)
2. Priradí im prístupové práva na čítanie a úpravy
3. Systém kontroluje prístupy pri každej operácii
4. Loguje pokusy o neoprávnený prístup

UC 9.9 – Viackanálové notifikácie ku stavu tiketu

Primárny aktér: Koncový používateľ, zákazník
Cieľ: Byť informovaný o zmene stavu tiketu
Hlavný scenár:

1. Systém zaregistruje aktualizáciu tiketu
2. Odošle oznámenie cez preferovaný kanál (e-mail, SMS, aplikácia)
3. Zákazník dostane správu o zmene
4. Potvrdí prijatie notifikácie

3.4.2.10 User stories a use cases pre Správa rolí a práv

Ako zákazník chcem, aby prístupy do platformy boli prísne riadené podľa rolí, aby sa minimalizovalo riziko zneužitia účtov.

Ako administrátor chcem nastavovať rôzne úrovne oprávnení pre jednotlivých používateľov a skupiny, aby mali prístup len k funkciám, ktoré potrebujú.

Ako manažér bezpečnosti chcem sledovať a auditovať prístupové práva, aby som mal istotu, že sú v súlade s internými a legislatívnymi požiadavkami.

Ako audítor chcem mať k dispozícii prehľad o histórii zmien rolí a práv, aby som vedel overiť, kto a kedy upravoval prístupové oprávnenia.

Ako DevOps inžinier chcem, aby správa rolí bola integrovaná s jednotným prihlasovaním (SSO), aby sa zjednodušilo nasadenie a údržba.

UC 10.1 – Definovanie rolí

Primárny aktér: Administrátor
Cieľ: Vytvárať a spravovať role podľa potrieb organizácie
Hlavný scenár:

1. Administrátor otvorí modul správy rolí
2. Definuje novú rolu (napr. SOC operátor, analytik, manažér)
3. Určí, aké funkcie a dáta môže daná rola využívať
4. Uloží konfiguráciu

UC 10.2 – Priraďovanie práv používateľom

Primárny aktér: Administrátor
Cieľ: Priradiť používateľovi vhodné oprávnenia
Hlavný scenár:

1. Administrátor vyhľadá používateľa
2. Pridelí mu jednu alebo viac rolí
3. Uloží zmeny
4. Používateľ má odteraz prístup iba k povoleným funkciám

UC 10.3 – Audit prístupových práv

Primárny aktér: Auditor, manažér bezpečnosti
Cieľ: Skontrolovať, kto má prístup k čomu
Hlavný scenár:

1. Auditor otvorí zoznam prístupových práv
2. Overí priradené role jednotlivým používateľom
3. Skontroluje históriu zmien
4. Exportuje auditnú správu

UC 10.4 – Integrácia s jednotným prihlásením SSO

Primárny aktér: DevOps inžinier, administrátor
Cieľ: Zabezpečiť centralizovanú správu identít
Hlavný scenár:

1. Administrátor nastaví prepojenie s identity providerom
2. Overí funkčnosť synchronizácie používateľov a rolí
3. Testuje prihlásenie cez SSO
4. Uloží konfiguráciu

UC 10.5 – Revokácia práv

Primárny aktér: Administrátor
Cieľ: Okamžite zrušiť prístup v prípade potreby
Hlavný scenár:

1. Administrátor identifikuje používateľa
2. Odoberie mu rolu alebo deaktivuje účet
3. Systém aplikuje zmenu okamžite
4. Zaznamená sa do auditného logu

UC 10.6 – Delegovanie správy rolí

Primárny aktér: Manažér bezpečnosti
Cieľ: Umožniť spravovať prístupové práva aj ďalším zodpovedným osobám
Hlavný scenár:

1. Manažér vyberie používateľa, ktorý bude spravovať roly
2. Udelí mu špeciálnu rolu „správca rolí“
3. Používateľ dostane prístup do administrácie rolí
4. Manažér monitoruje jeho činnosť

UC 10.7 – Automatická synchronizácia rolí

Primárny aktér: DevOps inžinier
Cieľ: Udržať konzistentné oprávnenia medzi systémami
Hlavný scenár:

1. DevOps nastaví synchronizáciu s HR databázou alebo IAM
2. Systém pravidelne importuje priradené role
3. Aktualizuje ich podľa zmien v HR systéme
4. Loguje každú aktualizáciu

UC 10.8 – Reporting zmien práv

Primárny aktér: Audítor, manažér
Cieľ: Preukázať históriu správy oprávnení
Hlavný scenár:

1. Audítor otvorí report zmien práv
2. Filtrovaním zistí, kto a kedy upravoval roly
3. Porovná zmeny s internými politikami
4. Exportuje report pre kontrolu

UC 10.9 – Nastavenie viacúrovňových práv

Primárny aktér: Administrátor
Cieľ: Definovať jemnejšiu granularitu oprávnení
Hlavný scenár:

1. Administrátor vytvorí hierarchiu rolí (napr. admin, power-user, read-only)
2. Priradí úrovne oprávnení k funkciám
3. Otestuje prístup s jednotlivými rolami
4. Aktivuje nastavenia v produkcii