V10 Zoznam funkčných a nefunkčných požiadaviek
KPB4 – Architektúra riešenia; typ – zoznam; mesiac odovzdania – M14

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY
ŽILINSKÁ UNIVERZITA V ŽILINE Fakulta riadenia a informatiky
BRAIN:IT

Úvod

V10 Zoznam funkčných a nefunkčných požiadaviek
KPB4 – Architektúra riešenia; typ – zoznam; mesiac odovzdania – M14

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY | BRAIN:IT

KATALOG_POZIADAVKY

PRÍPRAVNÁ A INICIAČNÁ FÁZA										REALIZAČNÁ FÁZA						
Poradové ID	ID POŽIADAVKY	KATEGÓRIA POŽIADAVKY _funkčná požiadavka _ne-funkčná požiadavka _technická požiadavka	OBLASŤ POŽIADAVKY	NÁZOV POŽIADAVKY	DETAILNÝ POPIS POŽIADAVKY	VLASTNÍK POŽIADAVKY	NÁZOV MODULU (príslušnosť požiadavky k modulu)	ČÍSLO INKREMENTU	POZNÁMKA	Referencia návrhu riešenia z DNR	SPôSOB realizácie	Identifikácia USE CASE	Identifikácia TEST CASE	Použité TESTOVACIE DÁTA	Použité PROSTREDIE	SPôSOB OVERENIA
1	FREQ_001	Funkcna poziadavka	SOCaaS	Proces monitorovania bezpečnostných udalostí	Zabezpečiť proces monitorovania bezpečnostných udalostí – zabezpečuje zber a sledovanie logov, metrických údajov a alertov zo všetkých integrovaných systémov.	UNIZA	SOC všeobecné	Inkrement 1								
2	FREQ_002	Funkcna poziadavka	SOCaaS	Proces detekcie incidentov	Zabezpečiť proces detekcie incidentov – je zodpovedný za identifikáciu anomálií, vzorcov útokov a iných hrozieb prostredníctvom korelačných pravidiel a heuristických mechanizmov.	UNIZA	SOC všeobecné	Inkrement 1								
3	FREQ_003	Funkcna poziadavka	SOCaaS	Proces reakcie na incodenty	Zabezpečiť proces reakcie na incidenty – definuje spôsob, akým tím reaguje na identifikované incidenty. Zahŕňa eskaláciu, priradenie zodpovednosti, vykonanie opatrení, ako aj komunikáciu so zasiahnutými stranami.	UNIZA	SOC všeobecné	Inkrement 1								
4	FREQ_004	Funkcna poziadavka	SOCaaS	Proces správy incidentov	Zabezpečiť proces správy incidentov – zahŕňa evidenciu, klasifikáciu, priraďovanie priorít, dokumentovanie a uzatváranie incidentov.	UNIZA	SOC všeobecné	Inkrement 1								
5	FREQ_005	Funkcna poziadavka	SOCaaS	Proces správy hrozieb	Zabezpečiť proces správy hrozieb (Threat Intelligence) – umožňuje systematickú prácu s informáciami o hrozbách.	UNIZA	SOC všeobecné	Inkrement 1								
6	FREQ_006	Funkcna poziadavka	SOCaaS	Proces reporting a vizualizácia	Zabezpečiť proces reporting a vizualizácia – zabezpečuje pravidelný výstup pre manažment, auditorov a SOC analytikov.	UNIZA	SOC všeobecné	Inkrement 1								
7	FREQ_007	Funkcna poziadavka	SOCaaS	Proces správy poznatkov	Zabezpečiť proces správy poznatkov – zabezpečuje udržiavanie znalostnej bázy playbookov, dokumentácie a odporúčaných reakcií.	UNIZA	SOC všeobecné	Inkrement 1								
8	NREQ_001	No-Funkcna poziadavka	SOCaaS	Základné organizačné roly	V kontexte návrhu SOCaaS pre projekt INKOSOC boli definované základné organizačné roly, ktoré má systém byť schopný zabezpečiť a spravovať: -**"Level 1 (L1) analytik"**: Prvá línia obrany, ktorá monitoruje výstrahy, vykonáva počiatočnú validáciu incidentov a zabezpečuje ich dokumentovanie. Typicky pracuje so SIEM dashboardmi, ticketingovým systémom a databázou znalostí. -**"Level 2 (L2) analytik"**: Skúsenejší analytik, ktorý preberá eskalované prípady od L1. Vykonáva hlbšiu analýzu, využíva korelačné pravidlá, threat intelligence a spolupracuje na tvorbe reakčných opatrení. Často využíva rozhrania SOAR nástrojov a forenzné nástroje. -**"Level 3 (L3) špecialista / inžinier"**: Odborník na zložité incidenty, pokročilý threat hunting, tvorbu detekčných pravidiel a konfiguráciu nástrojov ako SIEM či EDR. Zapája sa aj do architektúry a automatizácie reakcií. -**"Vedúci SOC (SOC manager)"**: Zodpovedá za prevádzku a kapacity SOC tímu, SLA, spoluprácu so zákazníkmi, reporting a kontrolu výkonnosti. Koordinuje ľudské aj technologické zdroje, vrátane plánovania zmien, monitorovania kvality reakcií a rozvoja tímu. -**"Incident handler / incident response lead"**: Rola zodpovedná za koordináciu reakcie na incident – plánovanie úloh, zber dôkazov, komunikáciu so zainteresovanými stranami a tvorbu záverečných reportov. -**"Threat Intelligence analytik"**: Zodpovedá za prácu s hrozbami z CTI zdrojov, tvorbu profilov útočníkov, obohacovanie incidentov o IOC a TTP, sledovanie trendov a zdieľanie výstrah. -**"Správca systémov a architektúry SOC"**: Technická rola zodpovedná za nasadenie, správu a aktualizáciu všetkých komponentov SOCaaS architektúry vrátane ELK Stacku, SOAR, asset managementu a iných nástrojov. Tieto roly nie sú pridané – môžu sa líšiť v závislosti od veľkosti SOC tímu,	BRAINIT	SOC všeobecné	Inkrement 1							
9	FREQ_008	Funkcna poziadavka	SOCaaS	Centralizácia logov	Riešenie musí zabezpečiť zber a centralizáciu logov zo systémov, sietí, koncových bodov a aplikácií.	UNIZA	SOC všeobecné	Inkrement 1								
10	FREQ_009	Funkcna poziadavka	SOCaaS	Normalizácia a obohacovanie údajov	Riešenie musí zabezpečiť normalizáciu a obohacovanie údajov.	UNIZA	SOC všeobecné	Inkrement 1								
11	FREQ_010	Funkcna poziadavka	SOCaaS	Ukladanie a indexovanie údajov	Riešenie musí zabezpečiť ukladanie, indexovanie a uchovávanie údajov.	UNIZA	SOC všeobecné	Inkrement 1								
12	FREQ_011	Funkcna poziadavka	SOCaaS	Tvorba korelačných pravidiel	Riešenie musí zabezpečiť tvorbu korelačných pravidiel a alertov	UNIZA	SOC všeobecné	Inkrement 1								
13	FREQ_012	Funkcna poziadavka	SOCaaS	Vizualizácia výstupov	Riešenie musí zabezpečiť vizualizáciu výstupov	UNIZA	SOC všeobecné	Inkrement 1								
14	FREQ_013	Funkcna poziadavka	SOCaaS	Integrácia s ďalšími nástrojmi	Riešenie musí zabezpečiť integráciu s ďalšími nástrojmi	UNIZA	SOC všeobecné	Inkrement 1								
15	FREQ_014	Funkcna poziadavka	SOCaaS	SOAR	Riešenie musí zabezpečiť SOAR a bude slúžiť na automatizáciu reakčných scenárov, spracovanie alertov do prípadov a ich analýzu.	BRAINIT	SOC všeobecné	Inkrement 1								
16	FREQ_015	Funkcna poziadavka	SOCaaS	Ticketovací systém a incident manažment	Riešenie musí zabezpečiť ticketovací a incident manažment systém poskytne workflow pre riešenie incidentov, eskaláciu, audit a sledovanie riešenia.	UNIZA	SOC všeobecné	Inkrement 1								
17	FREQ_016	Funkcna poziadavka	SOCaaS	Znalostný portál	Riešenie musí zabezpečiť znalostný portál, ktorý bude podporovať reaktívne procesy zdieľaním playbookov, interných politík a návodov.	UNIZA	SOC všeobecné	Inkrement 1								
18	FREQ_017	Funkcna poziadavka	SOCaaS	Inventarizácia a správa aktív	Riešenie musí zabezpečiť inventarizáciu a správu aktív. Správa IT aktív je kľúčová pre mapovanie dopadov hrozieb.	UNIZA	SOC všeobecné	Inkrement 1								
19	FREQ_018	Funkcna poziadavka	SOCaaS	Threat Intelligence	Riešenie musí zabezpečiť Threat Intelligence. Procesy CTI (Cyber Threat Intelligence) umožňujú obohacovanie incidentov o známe hrozby, TTPs a IOCs	UNIZA	SOC všeobecné	Inkrement 1								
20	FREQ_019	Funkcna poziadavka	SOCaaS	Správa zraniteľností	Riešenie musí zabezpečiť správu zraniteľností.	UNIZA	SOC všeobecné	Inkrement 1								
21	FREQ_020	Funkcna poziadavka	SOCaaS	Reporting a spätná analýza	Riešenie musí zabezpečiť reporting a spätnú analýzu.	UNIZA	SOC všeobecné	Inkrement 1								
22	FREQ_021	Funkcna poziadavka	SOCaaS	Onboarding nového zákaznika	Riešenie musí zabezpečiť onboarding nového zákazníka, kde prebieha integrácia jeho infraštruktúry do multitenantného prostredia SOCaaS. To zahŕňa: •nastavenie logovacieho agenta •konfiguráciu korelačných pravidiel •vytvorenie separovaných dashboardov •nastavenie incident managementu pre zákazníka	BRAINIT	SOC všeobecné	Inkrement 1								
23	FREQ_022	Funkcna poziadavka	SOCaaS	Detekcia a eskalácia incidentu	Riešenie musí zabezpečiť detekciu a eskaláciu incidentu. V prostredí musia byť nakonfigurované pravidlá na detekciu anomálií a známych hrozieb. Po detekcii: •sa generuje alert •alert sa automaticky transformuje na incident •Zammad zabezpečuje ticket pre L1 tím a podporu eskalácie, •tím vyhodnotí observables a využije obohatenie	BRAINIT	SOC všeobecné	Inkrement 1								
24	FREQ_023	Funkcna poziadavka	SOCaaS	Správa zraniteľností a inventarizácia	Riešenie musí zabezpečiť správu zraniteľností a inventarizáciu. Pravidelné skeny majú byť prepojené s CMDB. •Assety sú aktualizované na základe detekcie •incidenty viazané na zraniteľnosti sú prepájané do manažment systému	BRAINIT	SOC všeobecné	Inkrement 1								
25	FREQ_024	Funkcna poziadavka	SOCaaS	Proaktívne vyhľadávanie hrozieb	Riešenie musí zabezpečiť proaktívne vyhľadávanie hrozieb (Threat Hunting). Používajú sa pokročilé dotazy, často doplnené o: •CTI dáta •manuálnu analýzu v prípade podozrivých entít •výsledky sú dokumentované ako playbooky	BRAINIT	SOC všeobecné	Inkrement 1								
26	FREQ_025	Funkcna poziadavka	SOCaaS	Tvorba reportov a dashboardov	Riešenie musí zabezpečiť tvorbu reportov a dashboardov. Pre manažment a zákazníkov budú pravidelne generované: •prehľady incidentov •vizualizácie z metrík a ticketingu •exporty pre audit a SLA reporting	BRAINIT	SOC všeobecné	Inkrement 1								
27	FREQ_026	Funkcna poziadavka	SOCaaS	Tvorba znalostnej bázy	Riešenie musí zabezpečiť tvorbu znalostnej bázy. Každý incident alebo nový typ hrozby sa bude dokumentovať formou: •incident summary + lessons learned •zápis v znalostnom portáli •kategorizácia podľa MITRE ATT&CK a dátumov	BRAINIT	SOC všeobecné	Inkrement 1								
28	FREQ_027	Funkcna poziadavka	SOCaaS	Údržba a aktualizácia systému	Riešenie musí zabezpečiť údržbu a aktualizáciu systému. Prevádzkový tím musí mať stanovené: •pravidlá pre aktualizácie komponentov •testovacie prostredie na overenie zmien •centralizovaný monitoring funkčnosti všetkých modulov	BRAINIT	SOC všeobecné	Inkrement 1								

29	FREQ_028	Funkcna poziadavka	SOCaaS	Spracovanie dátových tokov	Riešenie musí zabezpečiť spracovanie dátových tokov. Hlavné úlohy spracovania dátových tokov sú: •Príjem logov a udalostí z viacerých heterogénnych zdrojov •Validácia, normalizácia a obohatenie dát •Priradenie časových pečiatok, identifikátorov a kategórií udalostí •Presmerovanie dát do vhodných indexov pre efektívnu analýzu •Odfiltrovanie redundatných alebo irelevantných údajov •Implementácia pipeline pravidiel a spracovateľských modulov	BRAINIT	SOC všeobecné	Inkrement 1	
30	FREQ_029	Funkcna poziadavka	SOCaaS	Korelačné pravidlá a detekcia hrozieb	Riešenie musí zabezpečiť korelačné pravidlá a detekcia hrozieb. •Alerty na základné IOC – porovnanie s databázou známych indikátorov (IP, URL, hash). •Anomálne správanie používateľov – napr. viacnásobné neúspešné prihlásenie v krátkom čase, login z nového geografického regiónu. •Neštandardné sieťové komunikácie – napr. DNS dotazy na dynamicky generované domény (DGA), odchýlky v čase a objeme dát. •Aktivity s administratívnymi právami – napr. pridanie používateľa do skupiny „Administrators", zmeny ACL, spustenie netsh, powershell. •Reťazenie udalostí – korelácia medzi viacerými logmi v čase: napr. login → súborový prenos → spustenie škodlivého procesu. Tieto pravidlá budú spravované, kde možno: •sledovať detekčné alerty, •nastavovať prahové hodnoty (thresholds), •konfigurovať výnimky a ignorované hodnoty (exceptions), •exportovať a importovať pravidlá ako JSON objekty.	UNIZA	SOC všeobecné	Inkrement 1	
31	FREQ_030	Funkcna poziadavka	SOCaaS	Integrácia s ostatnými komponentmi	Riešenie musí zabezpečiť integráciu s ostatnými komponentmi. Prepojenie so zdrojmi dát Integrácia s nástrojmi incident managementu a SOAR Znalostná databáza a playbooky	UNIZA	SOC všeobecné	Inkrement 1	
32	FREQ_031	Funkcna poziadavka	SOCaaS	Návrh dashboardov	Riešenie musí zabezpečiť návrh dashboardov. Pre uľahčenie prehľadnosti budú dashboardy v rámci SOCaaS rozdelené podľa funkčných vrstiev nasledovne: 1.Globálne prehľady (SOC Overview) Určené pre manažment a SLA reporting – zahŕňajú denné/mesačné štatistiky incidentov, typy hrozieb, top 10 IP adries, krajiny pôvodu útokov, čas vyriešenia ticketov. 2.Alert monitoring dashboardy Zamerané na operatívny monitoring – zobrazujú nové alerty, rozdelenie podľa severity (Critical, High, Medium), časové trendy, a korelácie medzi viacerými zdrojmi. 3.Tematické dashboardy Pokrývajú špecifické oblasti: •EDR aktivity: zaznamenané súbory, procesy, pokusy o exekúciu škodlivého kódu. •Zraniteľnosti a skeny: výsledky z Greenbone alebo OpenSCAP. •Firewall a sieťové logy: prístupy, porty, odhalené scanningové aktivity. 4.Detailné analytické dashboardy – Slúžia pre L2 analytikov a threat hunting. Obsahujú heatmapy, časové rezy, distribúcie podľa hodín, krajín, ASN, výskyt IOC a podobne. 5.Ad-hoc a incident-specific dashboardy – Vznikajú počas vyšetrovania konkrétneho prípadu, kde si analytik zostaví vlastnú vizualizáciu na základe dát z Elasticsearch.	UNIZA	SOC všeobecné	Inkrement 1	
33	FREQ_032	Funkcna poziadavka	SOCaaS	Štruktúra dashboardov	Riešenie musí zabezpečiť štruktúru dashboardov ako sú dashboardy zostavené z jednotlivých panelov, ktoré môžu obsahovať grafy, tabuľky, heatmapy, distribučné histogramy, metriky alebo mapy. Každý dashboard v rámci SOCaaS je navrhnutý ako kompozícia týchto vizualizácií zameraná na konkrétny aspekt monitorovania alebo analýzy. Prehľad systémovej bezpečnosti Korelačné a incidentové dashboardy Vizualizácia sieťovej prevádzky a prístupov Monitorovanie autentifikácií a správania používateľov Integrovaný prehľad pre SOC analytika	UNIZA	SOC všeobecné	Inkrement 1	
34	FREQ_033	Funkcna poziadavka	SOCaaS	Reporting	Riešenie musí zabezpečiť reporting. Reporting v SOCaaS bude plniť niekoľko základných cieľov: •Prevádzkový prehľad – zobrazenie stavu systémov, počtu incidentov, aktivity agentov. •Bezpečnostný reporting – výstupy o detekovaných hrozbách, typoch útokov, trendoch. •Compliance reporting – reporty podľa regulátorných požiadaviek (napr. GDPR, NIS2). •Manažérsky reporting – agregované štatistiky a ukazovatele pre vedenie organizácie. •Zákaznícky reporting – individuálne prehľady pre jednotlivých klientov multitenantného SOCaaS.	UNIZA	SOC všeobecné	Inkrement 1	
35	FREQ_034	Funkcna poziadavka	SOCaaS	Manuálny export reportov	Riešenie musí zabezpečiť manuálny export reportov. Reporty bude možné exportovať ako: •PDF dokument – generovaný snapshot aktuálneho dashboardu. •PNG obraz – statické obrázky jednotlivých vizualizácií. •CSV súbory – surové dáta z tabuliek a dátových polí. •JSON – pre automatizovanú analýzu a ďalšie spracovanie.	UNIZA	SOC všeobecné	Inkrement 1	
36	FREQ_035	Funkcna poziadavka	SOCaaS	Automatizovaný export reportov	Riešenie musí zabezpečiť automatizovaný export reportov. Reporty bude možné exportovať automatizovane: •Periodické reporty – denne, týždenne alebo mesačne generované a distribuované výstupy. •Distribúcia cez e-mail alebo webhook – reporty môžu byť automaticky odoslané na určené adresy alebo endpointy. •Podpora pre templaty a vlastné filtre – možnosť nastaviť podmienky, výbery časových období a formáty podľa potrieb.	UNIZA	SOC všeobecné	Inkrement 1	
37	FREQ_036	Funkcna poziadavka		Customizácia výstupov reportov	Riešenie musí zabezpečiť customizácia výstupov reportov. Bude obsahovať: •Možnosť výberu metrík, polí, časových rozsahov •Personalizácia dizajnu – logá, záhlavie, farebná schéma •Zaradenie vysvetliviek, poznámok a kontextuálneho komentára	UNIZA	SOC všeobecné	Inkrement 1	
38	FREQ_037	Funkcna poziadavka	Virtualizacia, kontajnerizacia, cloud	Podpora IaaS funkcionality	Riešenie vyžaduje plnú funkcionalitu IaaS – správu virtuálnych strojov (VM), diskov, sietí, obrazov, snapshotov a samostatných zdrojov. Platforma musí podporovať vyhľadávanie a správu rôznych typov inštancií, umožniť priradenie zdrojov podľa potreby tenantov a zároveň ponúknuť robustné API rozhranie pre programovateľný prístup. Schopnosť poskytovať kompletnú IaaS funkcionalitu je kľúčová pre zabezpečenie pružného a spoľahlivého prevádzkovania SOC ako služby.	UNIZA	Infraštruktúra	Inkrement 1	
39	NREQ_002	Ne-Funkcna poziadavka	Virtualizacia, kontajnerizacia, cloud	Modularita a architektúra	Modularita architektúry zásadne ovplyvňuje rozšíriteľnosť a škálovateľnosť riešenia. Platforma, ktorá je rozdelená do samostatných komponentov (napr. Nova – compute, Neutron – networking, Cinder – block storage), umožňuje nezávislé nasadzovanie, ladenie a výmenu modulov podľa potrieb. Taktiež je výhodné, ak platforma podporuje modernú architektúru mikroslužieb, pluginy, kontajnerizáciu a orchestračné vrstvy. Vyššia modularita zároveň znižuje riziko výpadku celého systému pri poruche jednej služby.	BRAINIT	Infraštruktúra	Inkrement 1	
40	FREQ_038	Funkcna poziadavka	Virtualizacia, kontajnerizacia, cloud	Podpora orchestrácie a automatizácie	Riešenie má podporovať nástroje ako Heat (OpenStack orchestration), Terraform (infrastucture as code), Ansible (automatizácia) alebo Kubernetes Operator pre efektívnu správu a nasadzovanie komplexných infraštruktúrnych scénarov. Táto schopnosť umožní rýchle škálovanie služieb, automatizované rozbaľovanie prostredí, opakovateľné testovanie aj zotavenie pri výpadkoch. V prostredí SOC, kde sa často menia požiadavky a topológia siete, je orchestrácia nevyhnutná pre zabezpečenie flexibility, udržateľnosti a prevádzkovej efektivity.	UNIZA	Infraštruktúra	Inkrement 1	
41	TREQ_001	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Výkonnosť a škálovateľnosť	Riešenie dokáže efektívne využívať zdroje, je potrebné vedieť limity z hľadiska počtu VM, kontajnerov či tenantov, a aké mechanizmy automatického škálovania podporuje. Dôležitá je aj latencia a celkový výkon pri spracovaní údajov, najmä v reálnom čase pre účely monitoringu bezpečnostných udalostí. Riešenie musí byť schopné rásť s počtom VM, tenantov a služieb. Potreba zabezpečiť horizontálnu a vertikálnu škálovateľnosť. V podmienkach projektu potrebujeme platformu, ktorá dokáže rásť spolu s počtom klientov SOC služby a objemom spracovávaných dát.	BRAINIT	Infraštruktúra	Inkrement 1	
42	TREQ_002	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Spoľahlivosť a stabilita	Riešenie musí byť stabilné v produkčnej prevádzke a obsahovať mechanizmy pre vysoko dostupné nasadenie. Možnosť nasadiť komponenty redundantne (HA – High Availability). V prostredí bezpečnostného centra je dôležité minimalizovať prestoje a zaistiť nepretržitú dostupnosť služby. Pri hodnotení cloudových služieb sa odporúča dôkladne preskúmať minulú výkonnosť, spokojnosť zákazníkov a zvládanie neplánovaných výpadkov. Rovnako potrovnávame SLA (Service Level Agreement) ak sú k dispozícii – hoci v prípade open-source platformy ide skôr o interné garancie, dostupnosť podpory atď.	UNIZA	Infraštruktúra	Inkrement 1	

43	TREQ_003	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Súlad so štandardmi a interoperabilita	Riešenie musí podporovať otvorené štandardy a bežné technológie, čo podmieňuje jej interoperabilitu s inými systémami. Riešenie by malo byť kompatibilné s populárnymi hypervízormi, sieťovými protokolmi, úložiskovými technológiami a rozhraniami pre správu (napr. OpenStack API je de facto štandard pre open-source cloudy). Široká podpora štandardov zároveň uľahčuje integráciu a minimalizuje riziko proprietárnych obmedzení. V prípade využitia Open Source, je potrebné aby platforma vychádzala z osvedčených open-source projektov podporovaných veľkou komunitou. V našom riešení interoperabilita umožní v budúcnosti prepojenie viacerých cloudových prostredí a integráciu ďalších komponentov.	UNIZA	Infraštruktúra	Inkrement 1	
44	NREQ_003	Ne-Funkcna poziadavka	Prevádzka	Náročnosť nasadenia a správy	Je požadované jednoduché nasadenie riešenia, inicializáciu platformy a jej následnú správu s potrebnou znalostnou. Napríklad niektoré open-source platformy sú vysoko konfigurovateľné, ale môžu byť komplexné na nasadenie, čo si vyžaduje skúsený tím alebo využitie automatizačných nástrojov (napr. Ansible skripty a pod.).	UNIZA	Infraštruktúra	Inkrement 1	
45	NREQ_004	Ne-Funkcna poziadavka	Prevádzka	Podpora, dostupnosť dokumentácie a komunita	Riešenie musí byť schopné bežať 24/7 a mať dané SLA parametre. Pri open-source riešeniach je dôležitá veľkosť a aktivita komunity – počet prispievateľov, frekvencia vydávania nových verzií a správ chýb, dostupnosť dokumentácie a znalostnej bázy. Silná komunita a podpora od veľkých IT firiem sú zárukou dlhodobej udržateľnosti projektu.	UNIZA	Infraštruktúra	Inkrement 1	
46	NREQ_005	Ne-Funkcna poziadavka	Bezpečnosť	Autentifikácia a riadenie prístupov	Platforma musí obsahovať zabudované bezpečnostné prvky potrebné na ochranu infraštruktúry a dát v prostredí SOC. Sem patrí napríklad podpora pre viacúrovňovú autentifikáciu a autorizáciu užívateľov, možnosť šifrovania dát (v úložiskách, prenosoch), logovanie a auditovanie udalostí či automatizované bezpečnostné politiky.	UNIZA	Infraštruktúra	Inkrement 1	
47	NREQ_006	Ne-Funkcna poziadavka	Bezpečnosť	Izolácia tenantov a ochrana dát	Riešenie musí zaručiť striktnú izoláciu medzi jednotlivými zákazníkmi (tenantmi) – ich virtuálne stroje, úložiská a siete musia byť oddelené tak, aby sa zabránilo neoprávnenému prístupu alebo úniku dát medzi tenantmi. Zabezpečiť oddelenie výpočtových zdrojov, sieťovú segmentáciu, mechanizmy kontroly prístupu a podobne. Miera izolácie dát medzi tenantmi je zásadným aspektom multitenantných systémov.	UNIZA	Infraštruktúra	Inkrement 1	
48	NREQ_007	Ne-Funkcna poziadavka	Bezpečnosť	Sieťová/monitorovacia integrácia	Prepojiteľnosť a možnosť integrácie s nástrojmi pre monitoring a bezpečnostné dohľadové systémy – najmä SIEM, IDS/IPS (napr. Suricata, Snort), ako aj metrické/logovacie nástroje ako Ceilometer, Grafana, Prometheus. Zohľadňuje tiež schopnosť platformy exportovať bezpečnostné udalosti, podporu API/webhookov a možnosti integrácie s externými bezpečnostnými prvkami.	UNIZA	Infraštruktúra	Inkrement 1	
49	TREQ_004	Technicka poziadavka	Prevádzka	Dostupnosť	Riešenie musí zabezpečiť vysokú dostupnosť v súlade s požadovanými parametrami na prevádzku KDS: - Prevádzkový čas 24/7, - RTO, RPO a Uptime pre jednotlivé služby: - RTO < 60 min - RPO 24 h - Uptime 99,5%	BRAINIT	Infraštruktúra	Inkrement 1	
50	TREQ_005	Technicka poziadavka	Prevádzka	Škálovanie	Riešenie musí umožniť modulárnosť riešenia s možnosťou vertikálneho a horizontálneho škálovania samostatných blokov podľa požiadaviek implementovaného riešenia.	BRAINIT	Infraštruktúra	Inkrement 1	
51	TREQ_006	Technicka poziadavka	Prevádzka	Virtualizácia	Riešenie musí byť prevádzkovateľné vo virtualizovanom prostredí	BRAINIT	Infraštruktúra	Inkrement 1	
52	TREQ_007	Technicka poziadavka	Prevádzka	Kontajnerizácia	Riešenie musí v prípade potreby vedieť využívať kontajnerizáciu	BRAINIT	Infraštruktúra	Inkrement 1	
53	TREQ_008	Technicka poziadavka	Prevádzka	Orchestrácia	Riešenie musí v prípade potreby vedieť využívať orchestračné nástroje	BRAINIT	Infraštruktúra	Inkrement 1	
54	TREQ_009	Technicka poziadavka	Bezpečnosť	Bezpečnostné logy	Riešenie musí zabezpečiť zaznamenávanie bezpečnostných logov v zmysle ZoITVS č. 95/2019 Z.z., vyhlášky č. 179/2020 Z. z. príloha č. 2 odsek "K. Zaznamenávanie udalostí a monitorovanie", Kategória II, bod e), a ZoKB č. 69/2018 Z. z. a jeho vykonávacej vyhlášky 362/2018 vznp paragraf 15.	BRAINIT	Infraštruktúra	Inkrement 1	
55	NREQ_008	Ne-Funkcna poziadavka	Bezpečnosť	Bezpečnostné testovanie	Pred spustením do produkčnej prevádzky musí byť vykonané bezpečnostné a penetračné testovanie v zmysle vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 o riadení projektov.	BRAINIT	SOC všeobecné	Inkrement 1	
56	NREQ_009	Ne-Funkcna poziadavka	Legislatíva	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679	Riešenie musí byť v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (GDPR) a v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.	BRAINIT	SOC všeobecné	Inkrement 1	
57	NREQ_010	Ne-Funkcna poziadavka	Legislatíva	Zákon č. 69/2018	Riešenie musí byť v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.	BRAINIT	SOC všeobecné	Inkrement 1	
58	FREQ_039	Funkcna poziadavka	SOCaaS	Podporované formáty logov	Schopnosť SIEM prijímať a spracovávať logy v rôznych štandardizovaných formátoch. Podporované formáty logov (syslog, JSON, CSV, CEF, LEEF...)	UNIZA	SIEM	Inkrement 1	
59	FREQ_040	Funkcna poziadavka	SOCaaS	Reálny čas vs. dávkové spracovanie	Schopnosť spracovávať logy v reálnom čase (streaming) alebo len v dávkach. Reálny čas vs. dávkové spracovanie	UNIZA	SIEM	Inkrement 1	
60	FREQ_041	Funkcna poziadavka	SOCaaS	Korelácia udalostí	Možnosť prepájať súvisiace udalosti pomocou korelačných pravidiel. Korelácia udalostí (preddefinované a vlastné pravidlá)	UNIZA	SIEM	Inkrement 1	
61	FREQ_042	Funkcna poziadavka	SOCaaS	Machine Learning/Behaviorálna analýza	Schopnosť SIEM systému detegovať anomálie pomocou strojového učenia. Machine Learning/Behaviorálna analýza	UNIZA	SIEM	Inkrement 1	
62	FREQ_043	Funkcna poziadavka	SOCaaS	Threat Intelligence (CTI) integrácia	Integrácia so zdrojmi hrozieb (IOC, TTP), automatické obohacovanie údajov. Threat Intelligence (CTI) integrácia	UNIZA	SIEM	Inkrement 1	
63	FREQ_044	Funkcna poziadavka	SOCaaS	Detekcia anomálií	Detekcia neštandardného správania alebo odchýlok od očakávaného správania. Detekcia anomálií	UNIZA	SIEM	Inkrement 1	
64	FREQ_045	Funkcna poziadavka	SOCaaS	Vlastné alertovacie pravidlá a prahy	Schopnosť definovať vlastné pravidlá a podmienky pre generovanie alertov. Vlastné alertovacie pravidlá a prahy	UNIZA	SIEM	Inkrement 1	
65	FREQ_046	Funkcna poziadavka	SOCaaS	Automatizované reakcie	Možnosť spustiť reakciu (blokovanie, izolácia, notifikácia) automaticky. Automatizované reakcie (napr. blokovanie IP, integrácia SOAR)	UNIZA	SIEM	Inkrement 1	
66	FREQ_047	Funkcna poziadavka	SOCaaS	Normalizácia a obohacovanie dát	Transformácia rôznych logov do jednotného formátu a ich rozšírenie (napr. WHOIS, GEOIP). Normalizácia a obohacovanie dát	UNIZA	SIEM	Inkrement 1	
67	FREQ_048	Funkcna poziadavka	SOCaaS	Fulltextové a rýchle vyhľadávanie	Schopnosť vyhľadávať v logoch cez operátory, tagy, filtre. Fulltextové a rýchle vyhľadávanie	UNIZA	SIEM	Inkrement 1	
68	FREQ_049	Funkcna poziadavka	SOCaaS	Dashboardy a ich kategorizácia	Vizualizácia údajov pomocou grafov, filtrov a widgetov. Dashboardy (vrátane interaktívnych) a ich kategorizácia	UNIZA	SIEM	Inkrement 1	
69	FREQ_050	Funkcna poziadavka	SOCaaS	Podpora pre MITRE ATT&CK mapovanie	Schopnosť mapovať detekcie na taktiky a techniky podľa MITRE ATT&CK. Podpora pre MITRE ATT&CK mapovanie	UNIZA	SIEM	Inkrement 1	
70	FREQ_051	Funkcna poziadavka	SOCaaS	Retencia	Schopnosť nastaviť retenčné politiky logov podľa zdroja a dôležitosti. Retencia (flexibilná, podľa typu logu)	UNIZA	SIEM	Inkrement 1	
71	FREQ_052	Funkcna poziadavka	SOCaaS	Šifrovanie	Ochrana logov pred neoprávneným prístupom pri prenose a ukladaní. Šifrovanie (pri prenose aj uložení)	UNIZA	SIEM	Inkrement 1	
72	FREQ_053	Funkcna poziadavka	SOCaaS	Monitoring stavu systému	Sledovanie výkonu, dostupnosti a funkčnosti systému. Monitoring stavu systému (healthcheck)	UNIZA	SIEM	Inkrement 1	
73	FREQ_054	Funkcna poziadavka	SOCaaS	Prijímanie upozornení a dát z rôznych bezpečnostných systémov	Schopnosť prijímať alerty a dáta z rôznych bezpečnostných zdrojov (SIEM, EDR, CTI...). Prijímanie upozornení a dát z rôznych bezpečnostných systémov	BRAINIT	SOAR	Inkrement 1	
74	FREQ_055	Funkcna poziadavka	SOCaaS	Normalizácia a parsovanie dát	Transformácia vstupných dát do štandardizovaného formátu pre ďalšie spracovanie. Normalizácia a parsovanie dát	BRAINIT	SOAR	Inkrement 1	
75	FREQ_056	Funkcna poziadavka	SOCaaS	Kategorizácia a prioritizácia incidentov	Možnosť triediť incidenty podľa závažnosti, typu, kategórie a dôležitosti. Kategorizácia a prioritizácia incidentov	BRAINIT	SOAR	Inkrement 1	
76	FREQ_057	Funkcna poziadavka	SOCaaS	Možnosť manuálneho aj automatického vytvárania incident ticketov	Podpora ručného aj automatického vytvárania incident ticketov zo vstupných údajov. Možnosť manuálneho aj automatického vytvárania incident ticketov	BRAINIT	SOAR	Inkrement 1	
77	FREQ_058	Funkcna poziadavka	SOCaaS	Preddefinované playbooky	Dostupnosť základných reakčných scenárov a automatizácií vopred pripravených v nástroji. Preddefinované playbooky	BRAINIT	SOAR	Inkrement 1	
78	FREQ_059	Funkcna poziadavka	SOCaaS	Možnosť tvorby vlastných playbookov bez potreby programovania	Schopnosť tvoriť a spravovať playbooky pomocou vizuálneho rozhrania bez nutnosti kódovania. Možnosť tvorby vlastných playbookov bez potreby programovania	BRAINIT	SOAR	Inkrement 1	
79	FREQ_060	Funkcna poziadavka	SOCaaS	Workflow engine s vetvením, podmienkami a slučkami	Možnosť definovať komplexné logiky v playbookoch pomocou rozhodovacích bodov. Workflow engine s vetvením, podmienkami a slučkami	BRAINIT	SOAR	Inkrement 1	
80	FREQ_061	Funkcna poziadavka	SOCaaS	Automatizované reakcie: blok IP, izolácia hostu, eskalácia	Schopnosť automaticky vykonať reakcie ako blokovanie, izolácia či upozornenie. Automatizované reakcie: blok IP, izolácia hostu, eskalácia	BRAINIT	SOAR	Inkrement 1	
81	FREQ_062	Funkcna poziadavka	SOCaaS	Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR	Prepojenie a výmena dát s inými systémami v rámci incident response procesu. Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR	BRAINIT	SOAR	Inkrement 1	
82	FREQ_063	Funkcna poziadavka	SOCaaS	API-first prístup	Prístupnosť funkcií nástroja cez API a podpora webhookov na notifikácie a interakcie. API-first prístup (REST, Webhooky)	BRAINIT	SOAR	Inkrement 1	
83	FREQ_064	Funkcna poziadavka	SOCaaS	Podpora pre plug-iny a konektory	Schopnosť rozšírenia funkcionality nástroja cez moduly alebo konektory. Podpora pre plug-iny a konektory	BRAINIT	SOAR	Inkrement 1	
84	FREQ_065	Funkcna poziadavka	SOCaaS	Dashboardy pre stav a štatistiky incidentov	Prehľadné zobrazenie stavu systému a prebiehajúcich incidentov. Dashboardy pre stav a štatistiky incidentov	BRAINIT	SOAR	Inkrement 1	
85	FREQ_066	Funkcna poziadavka	SOCaaS	RBAC a audit trail	Riadenie prístupov na základe rolí a logovanie zmien v systéme. RBAC a audit trail	BRAINIT	SOAR	Inkrement 1	
86	FREQ_067	Funkcna poziadavka	SOCaaS	Playbook debugging & testing	Možnosť testovať a ladiť playbooky pred ich ostrým nasadením. Playbook debugging & testing	BRAINIT	SOAR	Inkrement 1	

87	FREQ_068	Funkcna poziadavka	SOCaaS	SOAR-SIEM synchronizácia stavu incidentov	Prepojenie stavu incidentov medzi SIEM a SOAR pre aktuálnu viditeľnosť. SOAR-SIEM synchronizácia stavu incidentov	BRAINIT	SOAR	Inkrement 1	
88	FREQ_069	Funkcna poziadavka	SOCaaS	Možnosti nasadenia: on-prem, cloud, hybrid	Možnosť nasadenia riešenia v rôznych prostrediach vrátane lokálneho, cloudového alebo hybridného modelu. Možnosti nasadenia: on-prem, cloud, hybrid	BRAINIT	EDR	Inkrement 1	
89	FREQ_070	Funkcna poziadavka	SOCaaS	Podpora pre rôzne OS	Podpora pre inštaláciu a beh agenta na rôznych operačných systémoch. Podpora pre rôzne OS (Windows, Linux, macOS)	BRAINIT	EDR	Inkrement 1	
90	FREQ_071	Funkcna poziadavka	SOCaaS	Zber auditovacích dát pomocou agentov	Zber auditovacích záznamov o aktivitách používateľov, procesoch a systéme cez agenta. Zber auditovacích dát pomocou agentov	BRAINIT	EDR	Inkrement 1	
91	FREQ_072	Funkcna poziadavka	SOCaaS	File Integrity Monitoring	Detekcia zmeny súborov v reálnom čase pre účely forenznej analýzy a integrity. File Integrity Monitoring (FIM)	BRAINIT	EDR	Inkrement 1	
92	FREQ_073	Funkcna poziadavka	SOCaaS	Zber systémových metrík, procesov a správania	Monitorovanie systémového správania a metrík ako CPU, pamäť, služby a procesy. Zber systémových metrík, procesov a správania	BRAINIT	EDR	Inkrement 1	
93	FREQ_074	Funkcna poziadavka	SOCaaS	Zber informácií o zraniteľnostiach a konfiguráciách	Získavanie informácií o zraniteľnostiach z konfiguračných údajov a porovnanie s databázami CVE. Zber informácií o zraniteľnostiach a konfiguráciách	BRAINIT	EDR	Inkrement 1	
94	FREQ_075	Funkcna poziadavka	SOCaaS	Analýza logov a korelácia s hrozbami	Analýza logov s cieľom detekcie korelovaných udalostí a potenciálnych hrozieb. Analýza logov a korelácia s hrozbami	BRAINIT	EDR	Inkrement 1	
95	FREQ_076	Funkcna poziadavka	SOCaaS	Detekcia malvéru a narušení	Identifikácia škodlivého softvéru a incidentov narušenia bezpečnosti. Detekcia malvéru a narušení	BRAINIT	EDR	Inkrement 1	
96	FREQ_077	Funkcna poziadavka	SOCaaS	Heuristická a behaviorálna analýza	Založenie detekcie na správaní a heuristike namiesto len signatúr. Heuristická a behaviorálna analýza	BRAINIT	EDR	Inkrement 1	
97	FREQ_078	Funkcna poziadavka	SOCaaS	Podpora ML/AI algoritmov na detekciu hrozieb	Využitie algoritmov umelej inteligencie na detekciu anomálií a hrozieb. Podpora ML/AI algoritmov na detekciu hrozieb	BRAINIT	EDR	Inkrement 1	
98	FREQ_079	Funkcna poziadavka	SOCaaS	Mapovanie na MITRE ATT&CK framework	Zaradenie detegovaných aktivít a techník do rámca MITRE ATT&CK pre účely TTP analýz. Mapovanie na MITRE ATT&CK framework	BRAINIT	EDR	Inkrement 1	
99	FREQ_080	Funkcna poziadavka	SOCaaS	Automatické reakcie	Automatická reakcia na incidenty, ako je izolácia koncového bodu alebo karanténa súborov. Automatické reakcie (napr. izolácia zariadenia, karanténa súboru)	BRAINIT	EDR	Inkrement 1	
100	FREQ_081	Funkcna poziadavka	SOCaaS	Nízka systémová záťaž agenta	Agent má nízky vplyv na výkon systému, čo umožňuje nasadenie vo veľkej škále. Nízka systémová záťaž agenta	BRAINIT	EDR	Inkrement 1	
101	FREQ_082	Funkcna poziadavka	SOCaaS	Jednoduché centrálne riadenie agentov	Centrálna konzola na správu, konfiguráciu a dohľad nad všetkými agentmi. Jednoduché centrálne riadenie agentov	BRAINIT	EDR	Inkrement 1	
102	FREQ_083	Funkcna poziadavka	SOCaaS	Pravidelné aktualizácie signatúr a modulov	Pravidelné aktualizácie databáz hrozieb, signatúr a detekčných pravidiel. Pravidelné aktualizácie signatúr a modulov	BRAINIT	EDR	Inkrement 1	
103	FREQ_084	Funkcna poziadavka	SOCaaS	Bezplatná verzia, open-source riešenie s možnosťou rozšírenia	Dostupnosť základnej funkcionality bez licencie a možnosť rozšírenia. Bezplatná verzia, open-source riešenie s možnosťou rozšírenia	BRAINIT	Skener zraniteľností	Inkrement 1	
104	FREQ_085	Funkcna poziadavka	SOCaaS	Odhadovaná kapacita skenovania	Schopnosť nástroja efektívne skenovať veľké siete. Odhadovaná kapacita skenovania (napríklad min. 100 IP/24h)	BRAINIT	Skener zraniteľností	Inkrement 1	
105	FREQ_086	Funkcna poziadavka	SOCaaS	Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed	Frekvencia a rozsah aktualizácií detekčných vzorov. Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed	BRAINIT	Skener zraniteľností	Inkrement 1	
106	FREQ_087	Funkcna poziadavka	SOCaaS	Podpora CPE, CVE identifikátorov	Možnosť identifikácie zraniteľností podľa štandardizovaných identifikátorov. Podpora CPE, CVE identifikátorov	BRAINIT	Skener zraniteľností	Inkrement 1	
107	FREQ_088	Funkcna poziadavka	SOCaaS	Prijateľné webové rozhranie na správu skenovania a výsledkov	Použiteľnosť GUI pre správu skenov a výsledkov. Prijateľné webové rozhranie na správu skenovania a výsledkov	BRAINIT	Skener zraniteľností	Inkrement 1	
108	FREQ_089	Funkcna poziadavka	SOCaaS	Bez potreby agentov	Možnosť realizovať skeny bez nutnosti inštalovať agenta na zariadenia. Bez potreby agentov (agentless)	BRAINIT	Skener zraniteľností	Inkrement 1	
109	FREQ_090	Funkcna poziadavka	SOCaaS	Podpora plánovania úloh a alertov	Možnosť automatizovať opakované úlohy a generovanie upozornení. Podpora plánovania úloh a alertov (volitelné)	BRAINIT	Skener zraniteľností	Inkrement 1	
110	FREQ_091	Funkcna poziadavka	SOCaaS	Tikety na nápravu – integrácia alebo export	Možnosť exportovať nálezy do ticketovacieho systému alebo CSV, JSON, PDF. Tikety na nápravu – integrácia alebo export	BRAINIT	Skener zraniteľností	Inkrement 1	
111	FREQ_092	Funkcna poziadavka	SOCaaS	Konfigurovateľné formáty reportov	Flexibilita výstupov pre ďalšie spracovanie. Konfigurovateľné formáty reportov (napr. CSV, XML, PDF)	BRAINIT	Skener zraniteľností	Inkrement 1	
112	FREQ_093	Funkcna poziadavka	SOCaaS	Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker	Flexibilita inštalácie do rôznych prostredí. Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker	BRAINIT	Skener zraniteľností	Inkrement 1	
113	FREQ_094	Funkcna poziadavka	SOCaaS	Architektúra skenovania	Škálovateľnosť a prispôsobenie distribúcie skenov. Architektúra skenovania (monolitická alebo master/senzor)	BRAINIT	Skener zraniteľností	Inkrement 1	
114	FREQ_095	Funkcna poziadavka	SOCaaS	Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	Možnosť prepojenia s ďalšími bezpečnostnými a IT systémami. Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	BRAINIT	Skener zraniteľností	Inkrement 1	
115	FREQ_096	Funkcna poziadavka	SOCaaS	Podpora pre CVSS 4.0	Podpora najnovšej verzie skórovacieho systému CVSS. Podpora pre CVSS 4.0	BRAINIT	Skener zraniteľností	Inkrement 1	
116	FREQ_097	Funkcna poziadavka	SOCaaS	Podpora pre EPSS – predikcia zneužitia zraniteľností	Využitie modelov pravdepodobnosti zneužitia zraniteľností. Podpora pre EPSS – predikcia zneužitia zraniteľností	BRAINIT	Skener zraniteľností	Inkrement 1	
117	FREQ_098	Funkcna poziadavka	SOCaaS	Politiky súladu s normami	Možnosť hodnotiť zraniteľnosti vo vzťahu k štandardom. Politiky súladu s normami (napr. GDPR, ISO, CIS, BSI...)	BRAINIT	Skener zraniteľností	Inkrement 1	
118	FREQ_099	Funkcna poziadavka	SOCaaS	Podpora strategického CTI	Získavanie a analýza informácií o dlhodobých trendoch, dopadoch útokov a strategických odporúčaniach. Podpora strategického CTI (správy, analýzy dopadu, trendy útokov)	UNIZA	CTI	Inkrement 1	
119	FREQ_100	Funkcna poziadavka	SOCaaS	Podpora operatívneho CTI	Schopnosť mapovať techniky, taktiky a procedúry (TTP), identifikovať útočnícke skupiny a ich správanie. Podpora operatívneho CTI (TTP, profilovanie skupín)	UNIZA	CTI	Inkrement 1	
120	FREQ_101	Funkcna poziadavka	SOCaaS	Podpora taktického CTI	Práca s indikátormi kompromitácie (IOC) a ich evidencia, spracovanie, distribúcia. Podpora taktického CTI (IOC, IP, hash, URL, domény)	UNIZA	CTI	Inkrement 1	
121	FREQ_102	Funkcna poziadavka	SOCaaS	Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	Automatické sťahovanie dát z rôznych zdrojov (napr. GitHub, feeds, MISP, API systémy). Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	UNIZA	CTI	Inkrement 1	
122	FREQ_103	Funkcna poziadavka	SOCaaS	Podpora Abuse.ch, Malware Bazaar, MISP, AlienVault OTX, Anomali Limo	Pripravené konektory alebo integrácie pre známe CTI zdroje. Podpora Abuse.ch, Malware Bazaar, MISP, AlienVault OTX, Anomali Limo	UNIZA	CTI	Inkrement 1	
123	FREQ_104	Funkcna poziadavka	SOCaaS	Integrácia s 3rd party službami	Schopnosť obohacovať IOC a ďalšie artefakty pomocou externých služieb. Integrácia s 3rd party službami ako VirusTotal, Shodan, DomainTools, URLScan.io	UNIZA	CTI	Inkrement 1	
124	FREQ_105	Funkcna poziadavka	SOCaaS	Schopnosť normalizovať CTI dáta na jednotný formát	Konsolidácia dát z rôznych formátov do štruktúrovaného jednotného výstupu. Schopnosť normalizovať CTI dáta na jednotný formát	UNIZA	CTI	Inkrement 1	
125	FREQ_106	Funkcna poziadavka	SOCaaS	Možnosť manuálnej analýzy CTI	Rozhranie a nástroje pre bezpečnostných analytikov na ručné skúmanie dát. Možnosť manuálnej analýzy CTI	UNIZA	CTI	Inkrement 1	
126	FREQ_107	Funkcna poziadavka	SOCaaS	Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	Možnosť workflow pre spracovanie dát bez potreby manuálnych zásahov. Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	UNIZA	CTI	Inkrement 1	
127	FREQ_108	Funkcna poziadavka	SOCaaS	Deduplikácia hrozieb a informácií	Odstraňovanie redundantných IOC a indikátorov. Deduplikácia hrozieb a informácií	UNIZA	CTI	Inkrement 1	
128	FREQ_109	Funkcna poziadavka	SOCaaS	Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	Preposielanie IOC a dát priamo do detekčných systémov (SIEM, IDS, firewall). Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	UNIZA	CTI	Inkrement 1	
129	FREQ_110	Funkcna poziadavka	SOCaaS	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	UNIZA	CTI	Inkrement 1	
130	FREQ_111	Funkcna poziadavka	SOCaaS	Podpora formátov ako STIX/TAXII	Použitie štandardizovaných formátov pre výmenu CTI dát. Podpora formátov ako STIX/TAXII	UNIZA	CTI	Inkrement 1	
131	FREQ_112	Funkcna poziadavka	SOCaaS	Podpora najväčšieho počtu autoritatívnych CTI zdrojov	Rozsiahly výber komunitných, verejných a platených zdrojov. Podpora najväčšieho počtu autoritatívnych CTI zdrojov	UNIZA	CTI	Inkrement 1	
132	FREQ_113	Funkcna poziadavka	SOCaaS	Zníženie potreby manuálnej analýzy	Zautomatizovanie a prioritizácia hrozieb tak, aby sa analytici venovali len relevantným. Zníženie potreby manuálnej analýzy – šetrenie času analytikov	UNIZA	CTI	Inkrement 1	
133	FREQ_114	Funkcna poziadavka	SOCaaS	Vytvorenie, editácia a mazanie záznamov o aktívach	Schopnosť systému evidovať, upravovať a mazať informácie o jednotlivých aktívach. Vytvorenie, editácia a mazanie záznamov o aktívach	UNIZA	Asset management	Inkrement 1	
134	FREQ_115	Funkcna poziadavka	SOCaaS	Rozlíšenie aktív podľa typu	Možnosť rozlíšovať typy aktív pre lepšiu organizáciu a správu. Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové	UNIZA	Asset management	Inkrement 1	
135	FREQ_116	Funkcna poziadavka	SOCaaS	Možnosť priradenia tagov, kategórií, vlastníkov a stavu	Pridávanie metadát pre efektívne triedenie a správu aktív. Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené)	UNIZA	Asset management	Inkrement 1	
136	FREQ_117	Funkcna poziadavka	SOCaaS	Evidencia bezpečnostného stavu každého aktíva	Ukladanie informácií o zraniteľnostiach, patch úrovni a aktualizáciách systému. Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia)	UNIZA	Asset management	Inkrement 1	
137	FREQ_118	Funkcna poziadavka	SOCaaS	Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	Schopnosť mapovať fyzické a logické umiestnenie aktív v sieti. Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	UNIZA	Asset management	Inkrement 1	
138	FREQ_119	Funkcna poziadavka	SOCaaS	Väzby medzi aktívami	Možnosť vizualizovať a spravovať prepojenia medzi komponentmi infraštruktúry. Väzby medzi aktívami (napr. server – služba – aplikácia)	UNIZA	Asset management	Inkrement 1	
139	FREQ_120	Funkcna poziadavka	SOCaaS	Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov	Možnosť prepojenia s ďalšími nástrojmi SOC pre automatizáciu a zdieľanie údajov. Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov	UNIZA	Asset management	Inkrement 1	
140	FREQ_121	Funkcna poziadavka	SOCaaS	Možnosť filtrovania, fulltextového vyhľadávania a exportu	Efektívna práca s údajmi – vyhľadávanie podľa rôznych parametrov a exportovanie údajov. Možnosť filtrovania, fulltextového vyhľadávania a exportu	UNIZA	Asset management	Inkrement 1	
141	FREQ_122	Funkcna poziadavka	SOCaaS	Podpora API na správu aktív a integráciu	Možnosť spravovať a aktualizovať údaje o aktívach pomocou API. Podpora API (REST, GraphQL) na správu aktív a integráciu	UNIZA	Asset management	Inkrement 1	
142	FREQ_123	Funkcna poziadavka	SOCaaS	Možnosť tvorby vlastných polí, atribútov, pluginov	Užívateľská flexibilita pre prispôsobenie systému vlastným potrebám. Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django)	UNIZA	Asset management	Inkrement 1	
143	FREQ_124	Funkcna poziadavka	SOCaaS	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)	UNIZA	Asset management	Inkrement 1	
144	FREQ_125	Funkcna poziadavka	SOCaaS	Webové rozhranie s možnosťou úprav a prehľadnou správou	Používateľsky prívetivé GUI pre správu assetov. Webové rozhranie s možnosťou úprav a prehľadnou správou	UNIZA	Asset management	Inkrement 1	

145	FREQ_126	Funkcna poziadavka	SOCaaS	Zaznamenávanie zmien na aktívach	Auditovateľnosť všetkých zmien pre forenznú a prevádzkovú transparentnosť. Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil)	UNIZA	Asset management	Inkrement 1	
146	FREQ_127	Funkcna poziadavka	SOCaaS	Možnosť sledovať životný cyklus assetov	Správa jednotlivých fáz životnosti aktíva – od zaradenia po vyradenie. Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie)	UNIZA	Asset management	Inkrement 1	
147	FREQ_128	Funkcna poziadavka	SOCaaS	Upozornenia na zmenu stavu, expirácie, servisné intervaly	Automatické notifikácie pri zmene stavu alebo potrebe servisného zásahu. Upozornenia na zmenu stavu, expirácie, servisné intervaly	UNIZA	Asset management	Inkrement 1	
148	FREQ_129	Funkcna poziadavka	SOCaaS	Vytvorenie a editácia záznamov	Základná funkcionalita ticketovacieho systému – vytváranie, editovanie a mazanie ticketov. Vytvorenie a editácia záznamov (ticketov)	BRAINIT	Ticketing	Inkrement 1	
149	FREQ_130	Funkcna poziadavka	SOCaaS	Možnosť meniť stavy ticketu	Schopnosť prepínať medzi rôznymi stavmi ticketu počas jeho životného cyklu. Možnosť meniť stavy ticketu (napr. Nový, V riešení, Uzavretý, Odložený)	BRAINIT	Ticketing	Inkrement 1	
150	FREQ_131	Funkcna poziadavka	SOCaaS	Priradenie na konkrétneho riešiteľa	Priradenie ticketov na konkrétnych riešiteľov vrátane eskalácie podľa úrovne. Priradenie na konkrétneho riešiteľa (L1 analytik, eskalácia L2/L3)	BRAINIT	Ticketing	Inkrement 1	
151	FREQ_132	Funkcna poziadavka	SOCaaS	Emailové notifikácie o zmenách stavu, komentároch, deadline	Automatické emailové notifikácie o zmene stavu, komentároch, deadline. Emailové notifikácie o zmenách stavu, komentároch, deadline	BRAINIT	Ticketing	Inkrement 1	
152	FREQ_133	Funkcna poziadavka	SOCaaS	Pridávanie príloh	Možnosť pridávať prílohy ako logy, snímky obrazovky a iné dôkazy. Pridávanie príloh (logy, dôkazy, screenshoty, výpisy z nástrojov)	BRAINIT	Ticketing	Inkrement 1	
153	FREQ_134	Funkcna poziadavka	SOCaaS	Možnosť evidovať časy	Sledovanie a evidencia časových údajov pre celý životný cyklus ticketu. Možnosť evidovať časy (vytvorenie, aktualizácia, eskalácia, uzavretie)	BRAINIT	Ticketing	Inkrement 1	
154	FREQ_135	Funkcna poziadavka	SOCaaS	Nastavenie priority a závažnosti incidentu	Nastavenie úrovne priority a závažnosti ticketu pre lepšie plánovanie. Nastavenie priority a závažnosti incidentu	BRAINIT	Ticketing	Inkrement 1	
155	FREQ_136	Funkcna poziadavka	SOCaaS	Možnosť vytvárať šablóny pre opakujúce sa typy incidentov	Tvorba šablón pre rýchle zadávanie často sa opakujúcich incidentov. Možnosť vytvárať šablóny pre opakujúce sa typy incidentov	BRAINIT	Ticketing	Inkrement 1	
156	FREQ_137	Funkcna poziadavka	SOCaaS	Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie	Použitie tagov na uľahčenie vyhľadávania a kategorizácie. Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie	BRAINIT	Ticketing	Inkrement 1	
157	FREQ_138	Funkcna poziadavka	SOCaaS	Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi	Integrácia s inými bezpečnostnými nástrojmi na automatizáciu a workflow. Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi	BRAINIT	Ticketing	Inkrement 1	
158	FREQ_139	Funkcna poziadavka	SOCaaS	Podpora REST API a Webhookov	Podpora pre rozhrania REST API a Webhooky na komunikáciu s inými systémami. Podpora REST API a Webhookov	BRAINIT	Ticketing	Inkrement 1	
159	FREQ_140	Funkcna poziadavka	SOCaaS	Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	Možnosť exportovať tickety pre účely archivácie alebo reportingu. Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	BRAINIT	Ticketing	Inkrement 1	
160	FREQ_141	Funkcna poziadavka	SOCaaS	Modemé, responzívne webové rozhranie	Moderný a responzívny dizajn pre pohodlné používanie. Moderné, responzívne webové rozhranie	BRAINIT	Ticketing	Inkrement 1	
161	FREQ_142	Funkcna poziadavka	SOCaaS	Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete	Zaznamenávanie všetkých akcií, zmien a komentárov v tickete. Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete	BRAINIT	Ticketing	Inkrement 1	
162	FREQ_143	Funkcna poziadavka	SOCaaS	Možnosť spätného prehľadu a forenznej analýzy	Schopnosť spätne analyzovať priebeh a históriu incidentov. Možnosť spätného prehľadu a forenznej analýzy	BRAINIT	Ticketing	Inkrement 1	
163	FREQ_144	Funkcna poziadavka	SOCaaS	Tvorba a správa prípadov - cases s úlohami a detailmi	Možnosť vytvárať incidenty ako prípady s úlohami, popisom a atribútmi. Tvorba a správa prípadov (cases) s úlohami a detailmi	UNIZA	Evidencia a správa incid	Inkrement 1	
164	FREQ_145	Funkcna poziadavka	SOCaaS	Pridávanie a sledovanie observables	Možnosť sledovať IOC ako súčasť prípadu. Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	UNIZA	Evidencia a správa incid	Inkrement 1	
165	FREQ_146	Funkcna poziadavka	SOCaaS	Prepojenie medzi prípadmi na základe spoločných indikátorov	Automatická alebo manuálna identifikácia súvisiacich incidentov. Prepojenie medzi prípadmi na základe spoločných indikátorov	UNIZA	Evidencia a správa incid	Inkrement 1	
166	FREQ_147	Funkcna poziadavka	SOCaaS	Kategorizácia incidentov pomocou tagov	Možnosť kategorizovať incidenty pomocou štítkov/tagov. Kategorizácia incidentov pomocou tagov	UNIZA	Evidencia a správa incid	Inkrement 1	
167	FREQ_148	Funkcna poziadavka	SOCaaS	Automatizované obohacovanie informácie o incidente z internych a CTI zdrojov	Integrácia na obohatenie IOC a metadát z CTI alebo iných systémov. Automatizované obohacovanie informácie o incidente z internych a CTI zdrojov	UNIZA	Evidencia a správa incid	Inkrement 1	
168	FREQ_149	Funkcna poziadavka	SOCaaS	Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	Možnosť prispôsobiť platformu podľa potrieb organizácie. Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	UNIZA	Evidencia a správa incid	Inkrement 1	
169	FREQ_150	Funkcna poziadavka	SOCaaS	Podpora viacerých používateľských rolí	Podpora RBAC pre rôzne roly. Podpora viacerých používateľských rolí – minimálne analytik a administrátor	UNIZA	Evidencia a správa incid	Inkrement 1	
170	FREQ_151	Funkcna poziadavka	SOCaaS	Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi	Schopnosť prevádzkovať systém pre viac entít súčasne. Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi	UNIZA	Evidencia a správa incid	Inkrement 1	
171	FREQ_152	Funkcna poziadavka	SOCaaS	Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy	Možnosť obojsmernej výmeny dát. Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy	UNIZA	Evidencia a správa incid	Inkrement 1	
172	FREQ_153	Funkcna poziadavka	SOCaaS	Export incidentov do formátov CSV, PDF, cez REST API	Export dát pre dokumentáciu alebo reportovanie. Export incidentov do formátov CSV, PDF, cez REST API	UNIZA	Evidencia a správa incid	Inkrement 1	
173	FREQ_154	Funkcna poziadavka	SOCaaS	Logovanie činností analytikov počas riešenia incidentu (audit trail)	Evidencia činností pre forenznú analýzu. Logovanie činností analytikov počas riešenia incidentu (audit trail)	UNIZA	Evidencia a správa incid	Inkrement 1	
174	FREQ_155	Funkcna poziadavka	SOCaaS	Jednoduchá správa konfigurácií a aktualizácií	Schopnosť spravovať platformu bez potreby zásahu do kódu. Jednoduchá správa konfigurácií a aktualizácií	UNIZA	Evidencia a správa incid	Inkrement 1	
175	FREQ_156	Funkcna poziadavka	SOCaaS	Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie	Možnosť rozšíriť schému incidentu. Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie	UNIZA	Evidencia a správa incid	Inkrement 1	
176	FREQ_157	Funkcna poziadavka	SOCaaS	Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov	Umožňuje získať úplný časový priebeh incidentu. Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov	UNIZA	Evidencia a správa incid	Inkrement 1	
177	FREQ_158	Funkcna poziadavka	SOCaaS	Zdieľanie prípadov medzi tímami a externými partnermi podľa práv	Podpora riadeného zdieľania prípadov. Zdieľanie prípadov medzi tímami a externými partnermi podľa práv	UNIZA	Evidencia a správa incid	Inkrement 1	
178	FREQ_159	Funkcna poziadavka	SOCaaS	Vytvorenie základného prehľadu stavu bezpečnosti a incidentov	Možnosť vytvárať zhrnutia stavu bezpečnosti, incidentov a aktivity systému. Vytvorenie základného prehľadu stavu bezpečnosti a incidentov	UNIZA	Reporting	Inkrement 1	
179	FREQ_160	Funkcna poziadavka	SOCaaS	Možnosť stiahnuť report alebo automaticky odoslať	Exportovanie reportov manuálne alebo ich plánovaná automatická distribúcia. Možnosť stiahnuť report alebo automaticky odoslať (e-mail, webhook)	UNIZA	Reporting	Inkrement 1	
180	FREQ_161	Funkcna poziadavka	SOCaaS	Možnosť výberu obsahu reportu – časové obdobie, typy incidentov	Možnosť filtrovať obsah reportu podľa času, typu alebo zdrojových údajov. Možnosť výberu obsahu reportu – časové obdobie, typy incidentov	UNIZA	Reporting	Inkrement 1	
181	FREQ_162	Funkcna poziadavka	SOCaaS	Plánovanie pravidelných reportov	Možnosť nastaviť generovanie reportov na základe harmonogramu. Plánovanie pravidelných (napr. denných, týždenných) reportov	UNIZA	Reporting	Inkrement 1	
182	FREQ_163	Funkcna poziadavka	SOCaaS	Možnosť generovania jednorazových ad-hoc reportov	Tvorba reportov mimo pravidelného harmonogramu podľa potreby. Možnosť generovania jednorazových ad-hoc reportov	UNIZA	Reporting	Inkrement 1	
183	FREQ_164	Funkcna poziadavka	SOCaaS	Prispôsobenie vizuálnej podoby reportu	Možnosť upraviť vzhľad reportu podľa firemnej identity. Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie)	UNIZA	Reporting	Inkrement 1	
184	FREQ_165	Funkcna poziadavka	SOCaaS	Podpora exportu do PDF, CSV, JSON	Možnosť exportovať reporty do rôznych bežných formátov. Podpora exportu do PDF, CSV, JSON	UNIZA	Reporting	Inkrement 1	
185	FREQ_166	Funkcna poziadavka	SOCaaS	Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI	Možnosť zbierať údaje z iných systémov a vytvárať prepojené reporty. Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI, ...	UNIZA	Reporting	Inkrement 1	
186	FREQ_167	Funkcna poziadavka	SOCaaS	Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy	Vizualizácia dát priamo v reportoch rôznymi formami. Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy	UNIZA	Reporting	Inkrement 1	
187	FREQ_168	Funkcna poziadavka	SOCaaS	Podpora rôznych zdrojov: databázy, logy, API výstupy	Schopnosť agregovať dáta z viacerých technických a analytických zdrojov. Podpora rôznych zdrojov: databázy, logy, API výstupy	UNIZA	Reporting	Inkrement 1	
188	FREQ_169	Funkcna poziadavka	SOCaaS	Webové/GUI rozhranie pre tvorbu a správu reportov	Používateľsky privetivé rozhranie pre návrh, úpravu a správu reportov. Webové/GUI rozhranie pre tvorbu a správu reportov	UNIZA	Reporting	Inkrement 1	
189	FREQ_170	Funkcna poziadavka	SOCaaS	Možnosť archivácie vygenerovaných reportov	Možnosť uchovávať reporty pre spätnú analýzu a audit. Možnosť archivácie vygenerovaných reportov	UNIZA	Reporting	Inkrement 1	
190	FREQ_171	Funkcna poziadavka	SOCaaS	Možnosť obmedziť prístup k reportom podľa rolí - RBAC	Prístup k reportom riadený rolami a oprávneniami. Možnosť obmedziť prístup k reportom podľa rolí (RBAC)	UNIZA	Reporting	Inkrement 1	
191	FREQ_172	Funkcna poziadavka	SOCaaS	Šifrované prenosy reportov pri automatickej distribúcii	Bezpečný prenos citlivých dát cez šifrované kanály. Šifrované prenosy reportov pri automatickej distribúcii	UNIZA	Reporting	Inkrement 1	
192	FREQ_173	Funkcna poziadavka	SOCaaS	Vytváranie, editácia a verzovanie záznamov	Možnosť vytvárať, upravovať a sledovať verzie dokumentov s históriou zmien. Vytváranie, editácia a verzovanie záznamov (návody, playbooky, FAQ)	UNIZA	SOC knowledge portal	Inkrement 1	
193	FREQ_174	Funkcna poziadavka	SOCaaS	Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky	Organizácia KB dokumentov podľa štruktúrovaných pravidiel (kategórie, tagy, sekcie). Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky (tags)	UNIZA	SOC knowledge portal	Inkrement 1	
194	FREQ_175	Funkcna poziadavka	SOCaaS	Fulltextové vyhľadávanie s podporou filtrov a tagov	Vyhľadávanie v KB s možnosťou filtrovania podľa tagov, kategórií a obsahu. Fulltextové vyhľadávanie s podporou filtrov a tagov	UNIZA	SOC knowledge portal	Inkrement 1	
195	FREQ_176	Funkcna poziadavka	SOCaaS	Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	Možnosť prepojenia znalostných článkov s konkrétnymi typmi útokov a incidentmi v iných nástrojoch. Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	UNIZA	SOC knowledge portal	Inkrement 1	
196	FREQ_177	Funkcna poziadavka	SOCaaS	Možnosť vkladať obrázky, logy, odkazy a prílohy	Schopnosť obohatiť dokumenty o multimediálny alebo dátový obsah. Možnosť vkladať obrázky, logy, odkazy a prílohy	UNIZA	SOC knowledge portal	Inkrement 1	
197	FREQ_178	Funkcna poziadavka	SOCaaS	Podpora RBAC	Riadenie prístupu podľa používateľských rolí. Podpora RBAC – rôzne úrovne prístupu pre čítanie, editáciu, schvaľovanie	UNIZA	SOC knowledge portal	Inkrement 1	
198	FREQ_179	Funkcna poziadavka	SOCaaS	Možnosť integrácie s ticketingom, incident managementom, SIEM	Prepojenie KB s inými systémami pre efektívnejšie používanie obsahu. Možnosť integrácie s ticketingom, incident managementom, SIEM	UNIZA	SOC knowledge portal	Inkrement 1	
199	FREQ_180	Funkcna poziadavka	SOCaaS	Export dokumentov do PDF, HTML alebo Markdown formátu	Možnosť exportu dokumentov na offline použitie alebo publikovanie. Export dokumentov do PDF, HTML alebo Markdown formátu	UNIZA	SOC knowledge portal	Inkrement 1	
200	FREQ_181	Funkcna poziadavka	SOCaaS	Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	Používateľsky privetivé GUI pre správu znalostí. Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	UNIZA	SOC knowledge portal	Inkrement 1	
201	FREQ_182	Funkcna poziadavka	SOCaaS	Zachovanie histórie zmien s možnosťou obnovy staršej verzie	Sledovanie a archivácia zmien pre každý dokument. Zachovanie histórie zmien s možnosťou obnovy staršej verzie	UNIZA	SOC knowledge portal	Inkrement 1	
202	FREQ_183	Funkcna poziadavka	SOCaaS	Záznamy o tom, kto a kedy upravoval dokument	Audit trail zmien dokumentov s informáciou o autoroch a čase. Záznamy o tom, kto a kedy upravoval dokument	UNIZA	SOC knowledge portal	Inkrement 1	
203	FREQ_184	Funkcna poziadavka	SOCaaS	Možnosť tvorby schvaľovacích workflow pre nové KB články	Procesy schvaľovania pre publikáciu nových článkov. Možnosť tvorby schvaľovacích workflow pre nové KB články	UNIZA	SOC knowledge portal	Inkrement 1	

204	FREQ_185	Funkcna poziadavka	SOCaaS	Presnosť detekcie anomálií	Riešenie musí zabezpečiť vyhodnotenie presnosti detekcie anomálií (Precision, Recall, F1). Ako presne algoritmus deteguje anomálie bez ohľadu na triedu. Vyhodnotenie celkovej presnosti pomocou metrík ako Precision, Recall, F1-score alebo AUC-ROC.	UNIZA	AI/ML	Inkrement 1	
205	FREQ_186	Funkcna poziadavka	SOCaaS	Miera falošných poplachov	Riešenie musí zabezpečiť vyhodnotenie miery falošných poplachov (False Positives/Negatives). Ako často algoritmus generuje falošné pozitíva/negatívaZníženie miery falošných poplachov je kľúčové pre použiteľnosť v SOC. Ideálne modely majú veľmi nízky počet FP/FN.	UNIZA	AI/ML	Inkrement 1	
206	FREQ_187	Funkcna poziadavka	SOCaaS	Podpora učenia bez labelov	Riešenie musí zabezpečiť podporu učenia bez labelov (unsupervised). Schopnosť učiť sa zo vstupných dát bez potreby anotácií. Nie všetky modely vyžadujú označené dáta. Unsupervised modely sú výhodné najmä pri veľkých množstvách nelabelovaných údajov.	UNIZA	AI/ML	Inkrement 1	
207	FREQ_188	Funkcna poziadavka	SOCaaS	Výpočtová náročnosť AI/ML	Riešenie musí byť škálovateľné pre výpočtovú náročnosť (CPU/GPU, pamäť). Zdroje požadované na trénovanie a inferenciu modelu. Rôzna záťaž na výpočtové zdroje vrátane náročnosti na GPU, RAM a trvanie trénovania.	UNIZA	AI/ML	Inkrement 1	
208	FREQ_189	Funkcna poziadavka	SOCaaS	Rýchlosť inferencie	Riešenie musí zabezpečiť vyhodnotenie rýchlosti inferencie (čas detekcie). Rýchlosť odozvy pri detekcii. Ako rýchlo dokáže model poskytnúť výsledok na nové dáta. Kritické pre nasadenie v reálnom čase.	UNIZA	AI/ML	Inkrement 1	
209	FREQ_190	Funkcna poziadavka	SOCaaS	Robustnosť voči zmene distribúcie dát	Riešenie musí zabezpečiť robustnosť voči zmene distribúcie dát (drift, noise). Odolnosť voči šumu, zmenám v dátach alebo útokomModel musí byť odolný voči neočakávaným zmenám, fluktuáciám alebo noise, inak prestane fungovať správne.	UNIZA	AI/ML	Inkrement 1	
210	FREQ_191	Funkcna poziadavka	SOCaaS	Schopnosť práce s časovo-sekvenčnými dátami	Riešenie musí byť schopné práce s časovo-sekvenčnými dátami. Vhodnosť pre dáta s časovým vývojom (napr. logy, sieťová prevádzka). Schopnosť zachytiť dočasné vzory a anomálie v časových radoch. Výhodou sú architektúry ako LSTM, Transformer.	UNIZA	AI/ML	Inkrement 1	
211	FREQ_192	Funkcna poziadavka	SOCaaS	Flexibilita vstupných údajov	Riešenie musí byť schopné zabezpečiť flexibilitu vstupných údajov (logy, metriky, tokové dáta). Koľko typov dát model zvládne bez potreby úpravy architektúry. Model musí vedieť pracovať so štruktúrovanými i neštruktúrovanými vstupmi – logy, metriky, sieťové toky.	UNIZA	AI/ML	Inkrement 1	
212	FREQ_193	Funkcna poziadavka	SOCaaS	Adaptívne/online učenia	Riešenie musí mať možnosť adaptívneho/online učenia. Podpora aktualizácie modelu počas prevádzky bez retrénovaniaSchopnosť aktualizovať model bez nutnosti úplného retrénovania, napr. pomocou online learningu.	UNIZA	AI/ML	Inkrement 1	
213	FREQ_194	Funkcna poziadavka	SOCaaS	Vysvetliteľnosti modelu	Riešenie musí mať vysvetliteľný model (interpretability). Možnosť vysvetliť výstup detekcie analytikovi. Možnosť poskytnúť analytikovi zrozumiteľné vysvetlenie, prečo bola anomália detegovaná.	UNIZA	AI/ML	Inkrement 1	
214	TREQ_010	Technicka poziadavka	SOCaaS	Podpora mikroslužieb	Architektúra musí byť založená na samostatne nasaditeľných službách (microservices), z ktorých každá má vlastné API. Každá služba musí byť nezávisle verzovateľná a škálovateľná.	UNIZA	SOC všeobecné	Inkrement 1	
215	TREQ_011	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	CI/CD a orchestrácia	Zavedenie pipeline pre build-test-deploy cyklus. Podpora GitOps, CI, automatizovaný lint, scan, testy, rollout.	UNIZA	SOC všeobecné	Inkrement 1	
216	TREQ_012	Technicka poziadavka	SOCaaS	Kompatibilita s OSS	Všetky súčasti systému musia byť postavené na open-source technológiách. Licencie musia umožňovať úpravy a ďalšie šírenie.	UNIZA	SOC všeobecné	Inkrement 1	
217	TREQ_013	Technicka poziadavka	SOCaaS	Formáty dát	Systém musí spracovávať JSON, YAML, STIX/TAXII (CTI), Syslog, NetFlow/IPFIX. Musí byť zabezpečená normalizácia logov.	UNIZA	SOC všeobecné	Inkrement 1	
218	TREQ_014	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Prístupová architektúra	Prístup do systému má byť riadený napr. cez NGINX Ingress alebo HAProxy. Pre interný prístup má byť použitý VPN server (napr. WireGuard/OpenVPN). Podporovaná TLS 1.3, forward secrecy.	UNIZA	SOC všeobecné	Inkrement 1	
219	TREQ_015	Technicka poziadavka	Bezpečnosť	Bezpečné API	Každé API rozhranie musí podporovať HTTPS (TLS 1.3), autorizáciu cez OAuth2/JWT. API musí byť chránené pred DoS cez rate limiting, throttling a auditovanie prístupov.	UNIZA	SOC všeobecné	Inkrement 1	
220	TREQ_016	Technicka poziadavka	Bezpečnosť	Auditovateľnosť	Každá zmena konfigurácie, interakcia s API, akcia používateľa a incident musí byť logovaná do centralizovaného auditného úložiska.	UNIZA	SOC všeobecné	Inkrement 1	
221	TREQ_017	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Modulárne riešenie	Riešenie musí umožniť dynamické pridávanie plug-inov bez reštartu jadra. Pluginy musia byť izolované (napr. sidecar kontajnery alebo sandboxy).	UNIZA	SOC všeobecné	Inkrement 1	
222	TREQ_018	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Multitenantný deployment	Každý tenant musí mať oddelené namespace, databázu, dashboardy a logy. Musí byť možné nakonfigurovať SLA politiky na úrovni tenanta.	UNIZA	Infraštruktúra	Inkrement 1	
223	TREQ_019	Technicka poziadavka	Bezpečnosť	TLS/SSL šifrovanie	Všetky komunikácie medzi komponentmi (interne aj externe) musia byť šifrované pomocou TLS 1.3. Podpora HSTS, forward secrecy a možnosť vzájomnej autentifikácie cez client certifikáty.	UNIZA	Infraštruktúra	Inkrement 1	
224	TREQ_020	Technicka poziadavka	Bezpečnosť	Riadenie prístupu (RBAC/ABAC)	Riešenie musí podporovať riadenie prístupu na základe rolí (RBAC) a voliteľne na základe atribútov (ABAC). Autentifikácia môže prebiehať cez SSO/OAuth2/SAML.	UNIZA	Infraštruktúra	Inkrement 1	
225	TREQ_021	Technicka poziadavka	Bezpečnosť	Bezpečná správa tajného úložiska	Heslá, API kľúče, certifikáty a tokeny musia byť uložené v tajnom úložisku	BRAINIT	Infraštruktúra	Inkrement 1	
226	TREQ_022	Technicka poziadavka	Bezpečnosť	Bezpečné logovanie a detekcia anomálií	Riešenie musí vytvárať bezpečnostné logy, ktoré umožňujú detekciu podozrivého správania (napr. brute force, neobvyklé API prístupy). Požaduje sa integrácia s SIEM.	BRAINIT	Infraštruktúra	Inkrement 1	
227	TREQ_023	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Ukladanie logov a dát	Logy z endpointov, sietí, bezpečnostných systémov a komponentov musia byť udržiavané podľa politiky retenčného obdobia (napr. 12 mesiacov). Dátové úložisko musí podporovať replikáciu a snapshoty.	BRAINIT	Infraštruktúra	Inkrement 1	
228	TREQ_024	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Zálohovanie konfigurácií a dashboardov	Riešenie musí zabezpečiť automatické denné zálohovanie konfigurácií, pluginov, playbookov a dashboardov.	BRAINIT	Infraštruktúra	Inkrement 1	
229	TREQ_025	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Archivácia a dlhodobé uchovanie	Riešenie musí podporovať automatické presúvanie dát do archívu podľa pravidiel (napr. kompresia, šifrovanie, presun po 90 dňoch).	BRAINIT	Infraštruktúra	Inkrement 1	
230	TREQ_026	Technicka poziadavka	Virtualizacia, kontajnerizacia, cloud	Výkon spracovania dát	Riešenie musí spracovať minimálne 10 000 logov za sekundu v reálnom čase s oneskorením < 5 sekúnd.	BRAINIT	Infraštruktúra	Inkrement 1	

V10 Zoznam funkčných a nefunkčných požiadaviek
KPB4 – Architektúra riešenia; typ – zoznam; mesiac odovzdania – M14

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY | ŽILINSKÁ UNIVERZITA V ŽILINE Fakulta riadenia a informatiky | BRAIN:IT

Moduly a inkrementy

#	Moduly	Inkrement
MOD_01	Infraštruktúra	Inkrement 1
MOD_02	SIEM	Inkrement 1
MOD_03	SOAR	Inkrement 1
MOD_04	EDR	Inkrement 1
MOD_05	Skener zraniteľností	Inkrement 1
MOD_06	CTI	Inkrement 1
MOD_07	Asset management	Inkrement 1
MOD_08	Ticketing	Inkrement 1
MOD_09	Evidencia a správa incidentov	Inkrement 1
MOD_10	Reporting	Inkrement 1
MOD_11	SOC knowledge portal	Inkrement 1
MOD_12	SOC všeobecné	Inkrement 1
MOD_13	AI/ML	Inkrement 1
MOD_14		
MOD_15		

Inkrement
Inkrement 1