V5 zoznam definovaných kritérií

V5_SIEM

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

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

V5_SIEM

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Podporované formáty logov (syslog, JSON, CSV, CEF, LEEF...)	Schopnosť SIEM prijímať a spracovávať logy v rôznych štandardizovaných formátoch.	1 = Podporuje len základné formáty (napr. syslog a JSON); 5 = Podporuje širokú škálu štandardov vrátane CEF, LEEF, CSV, syslog, JSON atď.
2	Reálny čas vs. dávkové spracovanie	Schopnosť spracovávať logy v reálnom čase (streaming) alebo len v dávkach.	1 = Len dávkové spracovanie (napr. každých X hodín); 5 = Skutočne reálny čas (sekundové oneskorenie alebo streaming engine).
3	Korelácia udalostí (preddefinované a vlastné pravidlá)	Možnosť prepájať súvisiace udalosti pomocou korelačných pravidiel.	1 = Iba základné korelačné pravidlá bez možnosti úprav; 5 = Vlastné korelačné pravidlá + pokročilý engine na tvorbu vlastných korelácií.
4	Machine Learning/Behaviorálna analýza	Schopnosť SIEM systému detegovať anomálie pomocou strojového učenia.	1 = Žiadna ML/behaviorálna funkcionalita; 5 = Pokročilé modely ML na detekciu anomálií s vlastným učením a adaptívnosťou.
5	Threat Intelligence (CTI) integrácia	Integrácia so zdrojmi hrozieb (IOC, TTP), automatické obohacovanie údajov.	1 = Žiadna alebo len veľmi obmedzená CTI podpora; 5 = Integrácia viacerých CTI zdrojov (MISP, OTX, VirusTotal, Abuse.ch...) a ich automatické obohacovanie dát.
6	Detekcia anomálií	Detekcia neštandardného správania alebo odchýlok od očakávaného správania.	1 = Len signatúrna alebo manuálna detekcia; 5 = Automatická behaviorálna detekcia založená na baseline a adaptívnych modeloch.
7	Vlastné alertovacie pravidlá a prahy	Schopnosť definovať vlastné pravidlá a podmienky pre generovanie alertov.	1 = Len pevne definované notifikácie bez možnosti úprav; 5 = Možnosť definovať komplexné podmienky, prahy, filtre, logiku a alert schémy.
8	Automatizované reakcie (napr. blokovanie IP, integrácia SOAR)	Možnosť spustiť reakciu (blokovanie, izolácia, notifikácia) automaticky.	1 = Bez akejkoľvek automatizovanej reakcie; 5 = Podpora akcií ako blokovanie, izolácia, karanténa cez integrácie so SOAR, EDR, SIEM.
9	Normalizácia a obohacovanie dát	Transformácia rôznych logov do jednotného formátu a ich rozšírenie (napr. WHOIS, GEOIP).	1 = Neexistuje štandardizácia alebo enrichment. 5 = Automatické mapovanie dát do normalizovaného formátu + obohacovanie z viacerých zdrojov (napr. CTI, asset DB).
10	Fulltextové a rýchle vyhľadávanie	Schopnosť vyhľadávať v logoch cez operátory, tagy, filtre.	1 = Len základné filtrovanie alebo žiadne vyhľadávanie; 5 = Pokročilé fulltextové vyhľadávanie s operátormi, filtrami a rýchlou odozvou.
11	Dashboardy (vrátane interaktívnych) a ich kategorizácia	Vizualizácia údajov pomocou grafov, filtrov a widgetov.	1 = Žiadne alebo len statické výstupy; 5 = Dynamické, interaktívne dashboardy s možnosťou custom layoutov, filtrov a drill-down.
12	Podpora pre MITRE ATT&CK mapovanie	Schopnosť mapovať detekcie na taktiky a techniky podľa MITRE ATT&CK.	1 = Žiadna podpora alebo ručná korelácia; 5 = Automatické mapovanie detekcií na ATT&CK techniky s vizualizáciou a možnosťou exportu.
13	Retencia (flexibilná, podľa typu logu)	Schopnosť nastaviť retenčné politiky logov podľa zdroja a dôležitosti.	1 = Fixná retencia bez možnosti konfigurácie; 5 = Možnosť nastavovať rôzne retenčné politiky podľa typu logu, zdroja alebo obsahu.
14	Šifrovanie (pri prenose aj uložení)	Ochrana logov pred neoprávneným prístupom pri prenose a ukladaní.	1 = Logy nie sú šifrované ani pri prenose; 5 = Kompletné šifrovanie pri prenose (TLS, HTTPS) aj uložení (AES, GPG, disk-level).
15	Monitoring stavu systému (healthcheck)	Sledovanie výkonu, dostupnosti a funkčnosti systému.	1 = Žiadne nástroje na monitorovanie alebo len manuálne; 5 = Integrované notifikácie, metriky a alerty pri problémoch (napr. CPU, disk, pamäť, latencia spracovania)

Body:
logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Podporované formáty logov (syslog, JSON, CSV, CEF, LEEF...)	0,08
2	Reálny čas vs. dávkové spracovanie	0,08
3	Korelácia udalostí (preddefinované a vlastné pravidlá)	0,1
4	Machine Learning/Behaviorálna analýza	0,09
5	Threat Intelligence (CTI) integrácia	0,07
6	Detekcia anomálií	0,08
7	Vlastné alertovacie pravidlá a prahy	0,08
8	Automatizované reakcie (napr. blokovanie IP, integrácia SOAR)	0,07
9	Normalizácia a obohacovanie dát	0,08
10	Fulltextové a rýchle vyhľadávanie	0,06
11	Dashboardy (vrátane interaktívnych) a ich kategorizácia	0,06
12	Podpora pre MITRE ATT&CK mapovanie	0,05
13	Retencia (flexibilná, podľa typu logu)	0,05
14	Šifrovanie (pri prenose aj uložení)	0,03
15	Monitoring stavu systému (healthcheck)	0,02
	súčet váh:	**1**

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia						
		ELK Stack	Wazuh	OpenSearch + Dashboards	Graylog (Open)	SIEMonster (Community)	Prelude OSS	AlienVault OSSIM
Kritériá pre SIEM nástroj	Podporované formáty logov (syslog, JSON, CSV, CEF, LEEF...)	5	4	5	4	4	3	4
	Reálny čas vs. dávkové spracovanie	4	4	4	3	4	3	3
	Korelácia udalostí (preddefinované a vlastné pravidlá)	4	4	3	3	4	3	4
	Machine Learning/Behaviorálna analýza	3	3	2	2	4	2	3
	Threat Intelligence (CTI) integrácia	4	3	3	2	3	2	4
	Detekcia anomálií	4	3	2	3	4	2	4
	Vlastné alertovacie pravidlá a prahy	5	4	4	4	4	3	4
	Automatizované reakcie (napr. blokovanie IP, integrácia SOAR)	3	4	2	2	3	2	4
	Normalizácia a obohacovanie dát	5	4	4	4	3	3	4
	Fulltextové a rýchle vyhľadávanie	5	4	5	4	4	3	4
	Dashboardy (vrátane interaktívnych) a ich kategorizácia	5	4	5	4	3	3	3
	Podpora pre MITRE ATT&CK mapovanie	3	4	2	2	3	2	3
	Retencia (flexibilná, podľa typu logu)	4	3	4	3	4	3	3
	Šifrovanie (pri prenose aj uložení)	4	4	4	4	3	3	4
	Monitoring stavu systému (healthcheck)	3	4	3	4	3	2	3

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia						
		váhy	ELK Stack	Wazuh	OpenSearch + Dashboards	Graylog (Open)	SIEMonster (Community)	Prelude OSS	AlienVault OSSIM
Kritériá pre SIEM nástroj	Podporované formáty logov (syslog, JSON, CSV, CEF, LEEF...)	0,08	0,4	0,32	0,4	0,32	0,32	0,24	0,32
	Reálny čas vs. dávkové spracovanie	0,08	0,32	0,32	0,32	0,24	0,32	0,24	0,24
	Korelácia udalostí (preddefinované a vlastné pravidlá)	0,1	0,4	0,4	0,3	0,3	0,4	0,3	0,4
	Machine Learning/Behaviorálna analýza	0,09	0,27	0,27	0,18	0,18	0,36	0,18	0,27
	Threat Intelligence (CTI) integrácia	0,07	0,28	0,21	0,21	0,14	0,21	0,14	0,28
	Detekcia anomálií	0,08	0,32	0,24	0,16	0,24	0,32	0,16	0,32
	Vlastné alertovacie pravidlá a prahy	0,08	0,4	0,32	0,32	0,32	0,32	0,24	0,32
	Automatizované reakcie (napr. blokovanie IP, integrácia SOAR)	0,07	0,21	0,28	0,14	0,14	0,21	0,14	0,28
	Normalizácia a obohacovanie dát	0,08	0,4	0,32	0,32	0,32	0,24	0,24	0,32
	Fulltextové a rýchle vyhľadávanie	0,06	0,3	0,24	0,3	0,24	0,24	0,18	0,24
	Dashboardy (vrátane interaktívnych) a ich kategorizácia	0,06	0,3	0,24	0,3	0,24	0,18	0,18	0,18
	Podpora pre MITRE ATT&CK mapovanie	0,05	0,15	0,2	0,1	0,1	0,15	0,1	0,15
	Retencia (flexibilná, podľa typu logu)	0,05	0,2	0,15	0,2	0,15	0,2	0,15	0,15
	Šifrovanie (pri prenose aj uložení)	0,03	0,12	0,12	0,12	0,12	0,09	0,09	0,12
	Monitoring stavu systému (healthcheck)	0,02	0,06	0,08	0,06	0,08	0,06	0,04	0,06
výsledný súčet pre dané riešenie			4,13	3,71	3,43	3,13	3,62	2,62	3,65

V5_SOAR

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

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

V5_SOAR

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Prijímanie upozornení a dát z rôznych bezpečnostných systémov	Schopnosť prijímať alerty a dáta z rôznych bezpečnostných zdrojov (SIEM, EDR, CTI…).	1 = Podpora len niektorých zdrojov alebo manuálny import; 5 = Automatické prijímanie alertov z rôznych systémov vrátane SIEM, EDR, CTI, atď.
2	Normalizácia a parsovanie dát	Transformácia vstupných dát do štandardizovaného formátu pre ďalšie spracovanie.	1 = Bez parsovania alebo jednoduché mapovanie; 5 = Pokročilé normalizačné mechanizmy, parsovanie rôznych formátov.
3	Kategorizácia a prioritizácia incidentov	Možnosť triediť incidenty podľa závažnosti, typu, kategórie a dôležitosti.	1 = Fixné kategórie, bez možností úprav; 5 = Vlastné kategórie, priority, možnosť nastavovať scoring a automatické triedenie.
4	Možnosť manuálneho aj automatického vytvárania incident ticketov	Podpora ručného aj automatického vytvárania incident ticketov zo vstupných údajov.	1 = Len ručné vytváranie ticketov; 5 = Automatické aj manuálne vytváranie s integráciou na ticketing systémy.
5	Preddefinované playbooky	Dostupnosť základných reakčných scenárov a automatizácií vopred pripravených v nástroji.	1 = Bez vopred pripravených playbookov; 5 = Bohatá knižnica vopred pripravených playbookov pre rôzne scenáre.
6	Možnosť tvorby vlastných playbookov bez potreby programovania	Schopnosť tvoriť a spravovať playbooky pomocou vizuálneho rozhrania bez nutnosti kódovania.	1 = Vyžaduje manuálne skriptovanie; 5 = Plne vizuálne prostredie typu low-code/no-code.
7	Workflow engine s vetvením, podmienkami a slučkami	Možnosť definovať komplexné logiky v playbookoch pomocou rozhodovacích bodov.	1 = Len sekvenčné akcie bez logiky; 5 = Pokročilý workflow engine s podporou IF, LOOP, CASE a ďalších prvkov.
8	Automatizované reakcie: blok IP, izolácia hostu, eskalácia	Schopnosť automaticky vykonať reakcie ako blokovanie, izolácia či upozornenie.	1 = Žiadne alebo len notifikácie; 5 = Plne automatizované reakcie vrátane interakcie s firewall, EDR, SOAR.
9	Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR	Prepojenie a výmena dát s inými systémami v rámci incident response procesu.	1 = Obmedzená alebo žiadna integrácia; 5 = Silná orchestrácia naprieč mnohými typmi systémov s obojsmernou komunikáciou.
10	API-first prístup (REST, Webhooky)	Prístupnosť funkcií nástroja cez API a podpora webhookov na notifikácie a interakcie.	1 = Chýbajúce alebo obmedzené API; 5 = Plne pokrytý API-first prístup a webhooky pre reakcie.
11	Podpora pre plug-iny a konektory	Schopnosť rozšírenia funkcionality nástroja cez moduly alebo konektory.	1 = Žiadna rozšíriteľnosť; 5 = Podpora pre desiatky plug-inov alebo tvorbu vlastných.
12	Dashboardy pre stav a štatistiky incidentov	Prehľadné zobrazenie stavu systému a prebiehajúcich incidentov.	1 = Žiadne alebo statické výpisy; 5 = Interaktívne, prispôsobiteľné dashboardy s filtrami a drill-down možnosťami.
13	RBAC a audit trail	Riadenie prístupov na základe rolí a logovanie zmien v systéme.	1 = Bez RBAC alebo audit trailu; 5 = Detailné RBAC politiky a zaznamenávanie všetkých akcií.
14	Playbook debugging & testing	Možnosť testovať a ladiť playbooky pred ich ostrým nasadením.	1 = Žiadna podpora pre testovanie; 5 = Samostatné testovacie prostredie, ladiace nástroje a simulácia vstupov.
15	SOAR-SIEM synchronizácia stavu incidentov	Prepojenie stavu incidentov medzi SIEM a SOAR pre aktuálnu viditeľnosť.	1 = Manuálna alebo žiadna synchronizácia; 5 = Automatizovaná obojsmerná synchronizácia stavov incidentov.

Body:
logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Prijímanie upozornení a dát z rôznych bezpečnostných systémov	0,08
2	Normalizácia a parsovanie dát	0,07
3	Kategorizácia a prioritizácia incidentov	0,07
4	Možnosť manuálneho aj automatického vytvárania incident ticketov	0,07
5	Preddefinované playbooky	0,05
6	Možnosť tvorby vlastných playbookov bez potreby programovania	0,08
7	Workflow engine s vetvením, podmienkami a slučkami	0,07
8	Automatizované reakcie: blok IP, izolácia hostu, eskalácia	0,08
9	Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR	0,08
10	API-first prístup (REST, Webhooky)	0,07
11	Podpora pre plug-iny a konektory	0,05
12	Dashboardy pre stav a štatistiky incidentov	0,06
13	RBAC a audit trail	0,06
14	Playbook debugging & testing	0,05
15	SOAR-SIEM synchronizácia stavu incidentov	0,06
	súčet váh:	**1**

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia				
		Shuffle	TheHive+ Cortex	StackStorm	Fasten Health Tracecat	FIR (Fast Incident Response)
Kritériá pre SIEM nástroj	Prijímanie upozornení a dát z rôznych bezpečnostných systémov	5	5	4	3	3
	Normalizácia a parsovanie dát	4	4	5	3	3
	Kategorizácia a prioritizácia incidentov	4	5	4	3	4
	Možnosť manuálneho aj automatického vytvárania incident ticketov	4	5	4	3	4
	Preddefinované playbooky	4	3	5	3	2
	Možnosť tvorby vlastných playbookov bez potreby programovania	5	3	3	2	2
	Workflow engine s vetvením, podmienkami a slučkami	5	3	5	3	2
	Automatizované reakcie: blok IP, izolácia hostu, eskalácia	5	4	4	3	3
	Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR	5	4	5	3	3
	API-first prístup (REST, Webhooky)	5	4	5	4	3
	Podpora pre plug-iny a konektory	5	3	5	3	3
	Dashboardy pre stav a štatistiky incidentov	4	5	3	3	3
	RBAC a audit trail	4	5	4	3	4
	Playbook debugging & testing	5	3	4	2	2
	SOAR-SIEM synchronizácia stavu incidentov	4	5	4	2	3

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia				
		váhy	Shuffle	TheHive+ Cortex	StackStorm	Fasten Health Tracecat	FIR (Fast Incident Response)
Kritériá pre SIEM nástroj	Prijímanie upozornení a dát z rôznych bezpečnostných systémov	0,08	0,4	0,4	0,32	0,24	0,24
	Normalizácia a parsovanie dát	0,07	0,28	0,28	0,35	0,21	0,21
	Kategorizácia a prioritizácia incidentov	0,07	0,28	0,35	0,28	0,21	0,28
	Možnosť manuálneho aj automatického vytvárania incident ticketov	0,07	0,28	0,35	0,28	0,21	0,28
	Preddefinované playbooky	0,05	0,2	0,15	0,25	0,15	0,1
	Možnosť tvorby vlastných playbookov bez potreby programovania	0,08	0,4	0,24	0,24	0,16	0,16
	Workflow engine s vetvením, podmienkami a slučkami	0,07	0,35	0,21	0,35	0,21	0,14
	Automatizované reakcie: blok IP, izolácia hostu, eskalácia	0,08	0,4	0,32	0,32	0,24	0,24
	Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR	0,08	0,4	0,32	0,4	0,24	0,24
	API-first prístup (REST, Webhooky)	0,07	0,35	0,28	0,35	0,28	0,21
	Podpora pre plug-iny a konektory	0,05	0,25	0,15	0,25	0,15	0,15
	Dashboardy pre stav a štatistiky incidentov	0,06	0,24	0,3	0,18	0,18	0,18
	RBAC a audit trail	0,06	0,24	0,3	0,24	0,18	0,24
	Playbook debugging & testing	0,05	0,25	0,15	0,2	0,1	0,1
	SOAR-SIEM synchronizácia stavu incidentov	0,06	0,24	0,3	0,24	0,12	0,18
výsledný súčet pre dané riešenie			4,56	4,1	4,25	2,88	2,95

V5_EDR

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

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

V5_EDR

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Možnosti nasadenia: on-prem, cloud, hybrid	Možnosť nasadenia riešenia v rôznych prostrediach vrátane	1 – Podporované iba jedno prostredie bez flexibility; 5 – Plná podpora všetkých modelov
2	Podpora pre rôzne OS (Windows, Linux, macOS)	Podpora pre inštaláciu a beh agenta na rôznych operačných systémoch.	1 – Podpora iba pre jeden OS; 5 – Nativna podpora pre Windows, Linux aj macOS.
3	Zber auditovacích dát pomocou agentov	Zber auditovacích záznamov o aktivitách používateľov, procesoch a systéme cez agenta.	1 – Žiadny zber auditovacích dát; 5 – Komplexný zber audit trail cez agenta.
4	File Integrity Monitoring (FIM)	Detekcia zmeny súborov v reálnom čase pre účely forenznej analýzy a integrity.	1 – FIM úplne chýba; 5 – Pokročilý FIM s notifikáciami a pravidlami.
5	Zber systémových metrík, procesov a správania	Monitorovanie systémového správania a metrík ako CPU, pamäť, služby a procesy.	1 – Žiadne metriky alebo správanie sa nesleduje; 5 – Pokrytý široký rozsah systémových údajov.
6	Zber informácií o zraniteľnostiach a konfiguráciách	Získavanie informácií o zraniteľnostiach z konfiguračných údajov a porovnanie s databázami CVE.	1 – Nie je k dispozícii; 5 – Automatizovaný zber a mapovanie voči CVE/CPE.
7	Analýza logov a korelácia s hrozbami	Analýza logov s cieľom detekcie korelovaných udalostí a potenciálnych hrozieb.	1 – Chýba analýza alebo minimálna korelácia; 5 – Plne korelovaná analýza logov.
8	Detekcia malvéru a narušení	Identifikácia škodlivého softvéru a incidentov narušenia bezpečnosti.	1 – Nedetekuje malvér; 5 – Viacvrstvová detekcia v reálnom čase.
9	Heuristická a behaviorálna analýza	Založenie detekcie na správaní a heuristike namiesto len signatúr.	1 – Žiadna heuristika; 5 – Efektívna behaviorálna detekcia nových hrozieb.
10	Podpora ML/AI algoritmov na detekciu hrozieb	Využitie algoritmov umelej inteligencie na detekciu anomálií a hrozieb.	1 – ML/AI sa nepoužíva; 5 – Plne využíva modely pre detekciu anomálií.
11	Mapovanie na MITRE ATT&CK framework	Zaradenie detegovaných aktivít a techník do rámca MITRE ATT&CK pre účely TTP analýz.	1 – Bez prepojenia na ATT&CK; 5 – Automatická klasifikácia podľa MITRE ATT&CK.
12	Automatické reakcie (napr. izolácia zariadenia, karanténa súboru)	Automatická reakcia na incidenty, ako je izolácia koncového bodu alebo karanténa súborov.	1 – Reakcia možná len manuálne; 5 – Plne automatické reakcie a opatrenia.
13	Nízka systémová záťaž agenta	Agent má nízky vplyv na výkon systému, čo umožňuje nasadenie vo veľkej škále.	1 – Agent výrazne zaťažuje systém; 5 – Minimálny dopad na výkon.
14	Jednoduché centrálne riadenie agentov	Centrálna konzola na správu, konfiguráciu a dohľad nad všetkými agentmi.	1 – Manuálna konfigurácia každého agenta; 5 – Plne centralizované a škálovateľné.
15	Pravidelné aktualizácie signatúr a modulov	Pravidelné aktualizácie databáz hrozieb, signatúr a detekčných pravidiel.	1 – Manuálne aktualizácie bez podpory; 5 – Pravidelné a automatické aktualizácie.

Body:
logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Možnosti nasadenia: on-prem, cloud, hybrid	0,05
2	Podpora pre rôzne OS (Windows, Linux, macOS)	0,07
3	Zber auditovacích dát pomocou agentov	0,07
4	File Integrity Monitoring (FIM)	0,06
5	Zber systémových metrík, procesov a správania	0,07
6	Zber informácií o zraniteľnostiach a konfiguráciách	0,06
7	Analýza logov a korelácia s hrozbami	0,07
8	Detekcia malvéru a narušení	0,10
9	Heuristická a behaviorálna analýza	0,09
10	Podpora ML/AI algoritmov na detekciu hrozieb	0,06
11	Mapovanie na MITRE ATT&CK framework	0,06
12	Automatické reakcie (napr. izolácia zariadenia, karanténa súboru)	0,08
13	Nízka systémová záťaž agenta	0,06
14	Jednoduché centrálne riadenie agentov	0,07
15	Pravidelné aktualizácie signatúr a modulov	0,07
	súčet váh:	**1**

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia				
		Elastic Security	Wazuh	OSSEC	OpenEDR	Velociraptor
Kritériá pre SIEM nástroj	Možnosti nasadenia: on-prem, cloud, hybrid	5	5	4	4	4
	Podpora pre rôzne OS (Windows, Linux, macOS)	5	5	4	4	4
	Zber auditovacích dát pomocou agentov	4	5	4	4	3
	File Integrity Monitoring (FIM)	4	5	5	4	3
	Zber systémových metrík, procesov a správania	4	4	3	5	3
	Zber informácií o zraniteľnostiach a konfiguráciách	4	4	2	3	2
	Analýza logov a korelácia s hrozbami	5	4	3	4	3
	Detekcia malvéru a narušení	5	4	2	5	3
	Heuristická a behaviorálna analýza	4	3	2	4	3
	Podpora ML/AI algoritmov na detekciu hrozieb	4	3	1	4	2
	Mapovanie na MITRE ATT&CK framework	5	4	2	4	3
	Automatické reakcie (napr. izolácia zariadenia, karanténa súboru)	4	3	2	5	2
	Nízka systémová záťaž agenta	3	4	5	3	5
	Jednoduché centrálne riadenie agentov	4	5	3	4	3
	Pravidelné aktualizácie signatúr a modulov	5	4	2	4	2

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia				
		váhy	Elastic Security	Wazuh	OSSEC	OpenEDR	Velociraptor
Kritériá pre SIEM nástroj	Možnosti nasadenia: on-prem, cloud, hybrid	0,05	0,24	0,24	0,19	0,19	0,19
	Podpora pre rôzne OS (Windows, Linux, macOS)	0,07	0,34	0,34	0,27	0,27	0,27
	Zber auditovacích dát pomocou agentov	0,07	0,27	0,34	0,27	0,27	0,20
	File Integrity Monitoring (FIM)	0,06	0,23	0,29	0,29	0,23	0,17
	Zber systémových metrík, procesov a správania	0,07	0,27	0,27	0,20	0,34	0,20
	Zber informácií o zraniteľnostiach a konfiguráciách	0,06	0,23	0,23	0,12	0,17	0,12
	Analýza logov a korelácia s hrozbami	0,07	0,34	0,27	0,20	0,27	0,20
	Detekcia malvéru a narušení	0,10	0,48	0,38	0,19	0,48	0,29
	Heuristická a behaviorálna analýza	0,09	0,35	0,26	0,17	0,35	0,26
	Podpora ML/AI algoritmov na detekciu hrozieb	0,06	0,23	0,17	0,06	0,23	0,12
	Mapovanie na MITRE ATT&CK framework	0,06	0,29	0,23	0,12	0,23	0,17
	Automatické reakcie (napr. izolácia zariadenia, karanténa súboru)	0,08	0,31	0,23	0,15	0,38	0,15
	Nízka systémová záťaž agenta	0,06	0,17	0,23	0,29	0,17	0,29
	Jednoduché centrálne riadenie agentov	0,07	0,27	0,34	0,20	0,27	0,20
	Pravidelné aktualizácie signatúr a modulov	0,07	0,34	0,27	0,13	0,27	0,13
výsledný súčet pre dané riešenie			4,35	4,09	2,86	4,13	2,97

V5_Skener zraniteľností

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY | Žilinská univerzita v Žiline Fakulta riadenia a informatiky | BRAIN:IT

V5_Skener zraniteľností

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Bezplatná verzia, open-source riešenie s možnosťou rozšírenia	Dostupnosť základnej funkcionality bez licencie a možnosť rozšírenia.	1 = Len komerčná verzia; 5 = Plne open-source s možnosťou rozšírenia a customizácie.
2	Odhadovaná kapacita skenovania (napríklad min. 100 IP/24h)	Schopnosť nástroja efektívne skenovať veľké siete.	1 = Pod 50 IP denne; 5 = 1000+ IP denne bez obmedzení.
3	Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed	Frekvencia a rozsah aktualizácií detekčných vzorov.	1 = Žiadne/veľmi zriedkavé aktualizácie; 5 = Denne aktualizovaný komunitný aj podnikový feed.
4	Podpora CPE, CVE identifikátorov	Možnosť identifikácie zraniteľností podľa štandardizovaných identifikátorov.	1 = Žiadna podpora CPE/CVE; 5 = Úplná podpora s väzbou na databázy ako NVD.
5	Prijateľné webové rozhranie na správu skenovania a výsledkov	Použiteľnosť GUI pre správu skenov a výsledkov.	1 = Neintuitívne CLI rozhranie; 5 = Moderné, responzívne, prehľadné GUI.
6	Bez potreby agentov (agentless)	Možnosť realizovať skeny bez nutnosti inštalovať agenta na zariadenia.	1 = Povinnosť agenta pre každý host; 5 = Plná podpora agentless režimu.
7	Podpora plánovania úloh a alertov (voliteľné)	Možnosť automatizovať opakované úlohy a generovanie upozornení.	1 = Žiadna plánovacia funkcionalita; 5 = Cron-like plánovanie + e-mail/REST alerty.
8	Tikety na nápravu – integrácia alebo export	Možnosť exportovať nálezy do ticketovacieho systému alebo CSV, JSON, PDF.	1 = Žiadna podpora exportu; 5 = Priama integrácia s nápravnými systémami (napr. Jira, RT).
9	Konfigurovateľné formáty reportov (napr. CSV, XML, PDF)	Flexibilita výstupov pre ďalšie spracovanie.	1 = Len textový alebo HTML výstup; 5 = Podpora viacerých štruktúrovaných formátov.
10	Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker	Flexibilita inštalácie do rôznych prostredí.	1 = Len fyzické servery; 5 = Všetky varianty vrátane kontajnerizácie a SaaS.
11	Architektúra skenovania (monolitická alebo master/senzor)	Škálovateľnosť a prispôsobenie distribúcie skenov.	1 = Monolitické riešenie bez možnosti rozdelenia; 5 = Master/agent architektúra s distribúciou skenu.
12	Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	Možnosť prepojenia s ďalšími bezpečnostnými a IT systémami.	1 = Bez podpory integrácií; 5 = Široká podpora vrátane pluginov a REST API.
13	Podpora pre CVSS 4.0	Podpora najnovšej verzie skórovacieho systému CVSS.	1 = Žiadna CVSS podpora; 5 = Podpora CVSS 4.0 s vysvetlením dopadu a rizika.
14	Podpora pre EPSS – predikcia zneužitia zraniteľností	Využitie modelov pravdepodobnosti zneužitia zraniteľnosti.	1 = Žiadna EPSS podpora; 5 = Dynamické skóre s využitím EPSS.
15	Politiky súladu s normami (napr. GDPR, ISO, CIS, BSI...)	Možnosť hodnotiť zraniteľnosti vo vzťahu k štandardom.	1 = Žiadna mapovacia funkcionalita; 5 = Preddefinované compliance šablóny pre ISO, GDPR atď.

Body:

logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Bezplatná verzia, open-source riešenie s možnosťou rozšírenia	0,07
2	Odhadovaná kapacita skenovania (napríklad min. 100 IP/24h)	0,07
3	Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed	0,08
4	Podpora CPE, CVE identifikátorov	0,07
5	Prijateľné webové rozhranie na správu skenovania a výsledkov	0,07
6	Bez potreby agentov (agentless)	0,07
7	Podpora plánovania úloh a alertov (voliteľné)	0,07
8	Tikety na nápravu – integrácia alebo export	0,06
9	Konfigurovateľné formáty reportov (napr. CSV, XML, PDF)	0,06
10	Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker	0,07
11	Architektúra skenovania (monolitická alebo master/senzor)	0,06
12	Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	0,06
13	Podpora pre CVSS 4.0	0,06
14	Podpora pre EPSS – predikcia zneužitia zraniteľností	0,06
15	Politiky súladu s normami (napr. GDPR, ISO, CIS, BSI...)	0,07
	súčet váh:	1

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia	
		Greenbone Community edition	OpenSCAP
Kritériá pre SIEM nástroj	Bezplatná verzia, open-source riešenie s možnosťou rozšírenia	5	5
	Odhadovaná kapacita skenovania (napríklad min. 100 IP/24h)	4	3
	Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed	4	3
	Podpora CPE, CVE identifikátorov	5	4
	Prijateľné webové rozhranie na správu skenovania a výsledkov	4	3
	Bez potreby agentov (agentless)	5	4
	Podpora plánovania úloh a alertov (voliteľné)	4	2
	Tikety na nápravu – integrácia alebo export	3	2
	Konfigurovateľné formáty reportov (napr. CSV, XML, PDF)	5	4
	Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker	5	3
	Architektúra skenovania (monolitická alebo master/senzor)	5	3
	Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	3	2
	Podpora pre CVSS 4.0	4	3
	Podpora pre EPSS – predikcia zneužitia zraniteľností	4	2
	Politiky súladu s normami (napr. GDPR, ISO, CIS, BSI...)	4	5

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia	
		váhy	Greenbone Community edition	OpenSCAP
Kritériá pre SIEM nástroj	Bezplatná verzia, open-source riešenie s možnosťou rozšírenia	0,07	0,35	0,35
	Odhadovaná kapacita skenovania (napríklad min. 100 IP/24h)	0,07	0,28	0,21
	Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed	0,08	0,32	0,24
	Podpora CPE, CVE identifikátorov	0,07	0,35	0,28
	Prijateľné webové rozhranie na správu skenovania a výsledkov	0,07	0,28	0,21
	Bez potreby agentov (agentless)	0,07	0,35	0,28
	Podpora plánovania úloh a alertov (voliteľné)	0,07	0,28	0,14
	Tikety na nápravu – integrácia alebo export	0,06	0,18	0,12
	Konfigurovateľné formáty reportov (napr. CSV, XML, PDF)	0,06	0,30	0,24
	Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker	0,07	0,35	0,21
	Architektúra skenovania (monolitická alebo master/senzor)	0,06	0,30	0,18
	Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	0,06	0,18	0,12
	Podpora pre CVSS 4.0	0,06	0,24	0,18
	Podpora pre EPSS – predikcia zneužitia zraniteľností	0,06	0,24	0,12
	Politiky súladu s normami (napr. GDPR, ISO, CIS, BSI...)	0,07	0,28	0,35
výsledný súčet pre dané riešenie			4,28	3,23

V5_CTI

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

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

V5_CTI

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Podpora strategického CTI (správy, analýzy dopadu, trendy útokov)	Získavanie a analýza informácií o dlhodobých trendoch, dopadoch útokov a strategických odporúčaniach.	1 = Žiadna podpora strategických výstupov; 5 = Plne podporované strategické reporty, vizualizácie trendov a dopadové analýzy.
2	Podpora operatívneho CTI (TTP, profilovanie skupín)	Schopnosť mapovať techniky, taktiky a procedúry (TTP), identifikovať útočnícke skupiny a ich správanie.	1 = Žiadna podpora operatívneho CTI; 5 = Kompletné profilovanie APT skupín, TTP s integráciou ATT&CK.
3	Podpora taktického CTI (IOC, IP, hash, URL, domény)	Práca s indikátormi kompromitácie (IOC) a ich evidencia, spracovanie, distribúcia.	1 = Len manuálne vloženie IOC; 5 = Automatizovaný import/export, IOC management, časová platnosť.
4	Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	Automatické sťahovanie dát z rôznych zdrojov (napr. GitHub, feeds, MISP, API systémy).	1 = Iba manuálny zber dát; 5 = Automatizované sťahovanie viacerých feedov s možnosťou plánovania.
5	Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	Pripravené konektory alebo integrácie pre známe CTI zdroje.	1 = Bez podpory týchto zdrojov; 5 = Plne integrované s pravidelnou aktualizáciou dát.
6	Integrácia s 3rd party službami ako VirusTotal, Shodan, DomainTools, URLScan.io	Schopnosť obohacovať IOC a ďalšie artefakty pomocou externých služieb.	1 = Žiadna podpora integrácie; 5 = Priame API konektory s možnosťou enrichovania observables.
7	Schopnosť normalizovať CTI dáta na jednotný formát	Konsolidácia dát z rôznych formátov do štruktúrovaného jednotného výstupu.	1 = Nestruktúrované, nesúrodé dáta; 5 = Normalizácia do STIX/JSON alebo interného formátu.
8	Možnosť manuálnej analýzy CTI	Rozhranie a nástroje pre bezpečnostných analytikov na ručné skúmanie dát.	1 = Žiadna analytická funkcionalita; 5 = Detailné GUI, interaktívne prvky, časová os, párovanie IOC a TTP.
9	Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	Možnosť workflow pre spracovanie dát bez potreby manuálnych zásahov.	1 = Iba manuálne spracovanie; 5 = Automatické agregovanie, filtrovanie, deduplikácia.
10	Deduplikácia hrozieb a informácií	Odstraňovanie redundantných IOC a indikátorov.	1 = Vysoká redundancia bez filtrov; 5 = Pokročilá logika na deduplikáciu podľa zdroja, času a typu.
11	Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	Preposielanie IOC a dát priamo do detekčných systémov (SIEM, IDS, firewall).	1 = Žiadna integrácia; 5 = Plná kompatibilita cez STIX, API alebo push mechanizmy.
12	Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu	Spájanie incidentov, IOC a TTP s ATT&CK frameworkom.	1 = Žiadne mapovanie; 5 = Vizuálne prehľadné mapovanie s väzbami a komentármi.
13	Podpora formátov ako STIX/TAXII	Použitie štandardizovaných formátov pre výmenu CTI dát.	1 = Len interný alebo nestruktúrovaný výstup; 5 = Nativná STIX tvorba a TAXII client/server podpora.
14	Podpora najväčšieho počtu autoritatívnych CTI zdrojov	Rozsiahly výber komunitných, verejných a platených zdrojov.	1 = Podpora max 1–2 zdrojov; 5 = >10 zdrojov + možnosť pridania vlastných.
15	Zníženie potreby manuálnej analýzy – šetrenie času analytikov	Zautomatizovanie a prioritizácia hrozieb tak, aby sa analytici venovali len relevantným.	1 = Vysoká miera ručnej práce; 5 = Automatizácia, scoring IOC, tagging relevance a suppression.

Body:

logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Podpora strategického CTI (správy, analýzy dopadu, trendy útokov)	0,07
2	Podpora operatívneho CTI (TTP, profilovanie skupín)	0,07
3	Podpora taktického CTI (IOC, IP, hash, URL, domény)	0,09
4	Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	0,08
5	Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	0,07
6	Integrácia s 3rd party službami ako VirusTotal, Shodan, DomainTools, URLScan.io	0,06
7	Schopnosť normalizovať CTI dáta na jednotný formát	0,07
8	Možnosť manuálnej analýzy CTI	0,06
9	Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	0,08
10	Deduplikácia hrozieb a informácií	0,06
11	Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	0,07
12	Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu	0,06
13	Podpora formátov ako STIX/TAXII	0,05
14	Podpora najväčšieho počtu autoritatívnych CTI zdrojov	0,06
15	Zníženie potreby manuálnej analýzy – šetrenie času analytikov	0,05
	súčet váh:	1

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia					
		Modul Threat intel (ELK)	MISP	OpenCTI	IntelMQ	YETI	Vulmatch
Kritériá pre SIEM nástroj	Podpora strategického CTI (správy, analýzy dopadu, trendy útokov)	3	2	5	1	3	2
	Podpora operatívneho CTI (TTP, profilovanie skupín)	3	2	5	2	4	3
	Podpora taktického CTI (IOC, IP, hash, URL, domény)	4	5	5	4	4	5
	Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	3	4	5	5	4	4
	Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	3	5	5	5	4	3
	Integrácia s 3rd party službami ako VirusTotal, Shodan, DomainTools, URLScan.io	3	3	5	4	3	2
	Schopnosť normalizovať CTI dáta na jednotný formát	3	4	5	5	4	4
	Možnosť manuálnej analýzy CTI	2	5	5	2	4	3
	Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	3	3	5	5	3	4
	Deduplikácia hrozieb a informácií	3	4	5	4	4	4
	Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	4	3	5	4	3	3
	Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu	3	2	5	2	4	2
	Podpora formátov ako STIX/TAXII	3	5	5	5	4	3
	Podpora najväčšieho počtu autoritatívnych CTI zdrojov	3	4	5	4	3	3
	Zníženie potreby manuálnej analýzy – šetrenie času analytikov	3	3	5	4	3	4

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia					
		váhy	Modul Threat intel (ELK)	MISP	OpenCTI	IntelMQ	YETI	Vulmatch
Kritériá pre SIEM nástroj	Podpora strategického CTI (správy, analýzy dopadu, trendy útokov)	0,07	0,21	0,14	0,35	0,07	0,21	0,14
	Podpora operatívneho CTI (TTP, profilovanie skupín)	0,07	0,21	0,14	0,35	0,14	0,28	0,21
	Podpora taktického CTI (IOC, IP, hash, URL, domény)	0,09	0,36	0,45	0,45	0,36	0,36	0,45
	Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	0,08	0,24	0,32	0,40	0,40	0,32	0,32
	Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	0,07	0,21	0,35	0,35	0,35	0,28	0,21
	Integrácia s 3rd party službami ako VirusTotal, Shodan, DomainTools, URLScan.io	0,06	0,18	0,18	0,30	0,24	0,18	0,12
	Schopnosť normalizovať CTI dáta na jednotný formát	0,07	0,21	0,28	0,35	0,35	0,28	0,28
	Možnosť manuálnej analýzy CTI	0,06	0,12	0,30	0,30	0,12	0,24	0,18
	Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	0,08	0,24	0,24	0,40	0,40	0,24	0,32
	Deduplikácia hrozieb a informácií	0,06	0,18	0,24	0,30	0,24	0,24	0,24
	Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	0,07	0,28	0,21	0,35	0,28	0,21	0,21
	Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu	0,06	0,18	0,12	0,30	0,12	0,24	0,12
	Podpora formátov ako STIX/TAXII	0,05	0,15	0,25	0,25	0,25	0,20	0,15
	Podpora najväčšieho počtu autoritatívnych CTI zdrojov	0,06	0,18	0,24	0,30	0,24	0,18	0,18
	Zníženie potreby manuálnej analýzy – šetrenie času analytikov	0,05	0,15	0,15	0,25	0,20	0,15	0,20
výsledný súčet pre dané riešenie			3,1	3,61	5	3,76	3,61	3,33

V5_Asset_management

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

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

V5_Asset_management

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Vytvorenie, editácia a mazanie záznamov o aktívach	Schopnosť systému evidovať, upravovať a mazať informácie o jednotlivých aktívach.	1 = Len základná evidencia bez úprav; 5 = Plná CRUD funkcionalita s kontrolou zmien a audit trail.
2	Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové	Možnosť rozlišovať typy aktív pre lepšiu organizáciu a správu.	1 = Len základné typy aktív; 5 = Rozšírené triedenie vrátane cloudových, kontajnerov a virtuálnych
3	Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené)	Pridávanie metadát pre efektívne triedenie a správu aktív.	1 = Len pevne dané kategórie; 5 = Užívateľsky definovateľné tagy, stav a vlastníctvo.
4	Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia)	Ukladanie informácií o zraniteľnostiach, patch úrovni a aktualizáciách systému.	1 = Žiadne bezpečnostné atribúty; 5 = Automatizovaná evidencia bezpečnostného stavu.
5	Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	Schopnosť mapovať fyzické a logické umiestnenie aktív v sieti.	1 = Len názov lokality; 5 = Podpora komplexného mapovania IP, rack, VLAN, zón.
6	Väzby medzi aktívami (napr. server – služba – aplikácia)	Možnosť vizualizovať a spravovať prepojenia medzi komponentmi infraštruktúry.	1 = Bez väzieb; 5 = Detailné mapovanie závislostí s grafickou reprezentáciou.
7	Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov	Možnosť prepojenia s ďalšími nástrojmi SOC pre automatizáciu a zdieľanie údajov.	1 = Žiadna integrácia; 5 = Viacúrovňová bidirekčná integrácia s relevantnými systémami.
8	Možnosť filtrovania, fulltextového vyhľadávania a exportu	Efektívna práca s údajmi – vyhľadávanie podľa rôznych parametrov a exportovanie údajov.	1 = Len základné vyhľadávanie; 5 = Pokročilé fulltextové vyhľadávanie + exporty (CSV, JSON).
9	Podpora API (REST, GraphQL) na správu aktív a integráciu	Možnosť spravovať a aktualizovať údaje o aktívach pomocou API.	1 = Bez API; 5 = Dokumentované REST/GraphQL API pre všetky funkcie.
10	Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django)	Užívateľská flexibilita pre prispôsobenie systému vlastným potrebám.	1 = Pevne definovaná štruktúra; 5 = Plne prispôsobiteľná s podporou pluginov alebo skriptovania.
11	Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov)	Automatizovaný zber a aktualizácia údajov o aktívach zo siete a iných systémov.	1 = Manuálny zber údajov; 5 = Automatizované discovery s plánovaním a API vstupmi.
12	Webové rozhranie s možnosťou úprav a prehľadnou správou	Používateľsky privetivé GUI pre správu assetov.	1 = Neintuitívne alebo len CLI; 5 = Responzívne a používateľsky priateľské rozhranie.
13	Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil)	Auditovateľnosť všetkých zmien pre forenznú a prevádzkovú transparentnosť.	1 = Žiadne logovanie zmien; 5 = Detailný audit trail s časovou pečiatkou a užívateľom.
14	Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie)	Správa jednotlivých fáz životnosti aktíva – od zaradenia po vyradenie.	1 = Bez životného cyklu; 5 = Komplexné sledovanie s upozorneniami a stavmi.
15	Upozornenia na zmenu stavu, expirácie, servisné intervaly	Automatické notifikácie pri zmene stavu alebo potrebe servisného zásahu.	1 = Bez upozornení; 5 = Konfigurovateľné upozornenia podľa podmienok alebo kalendára.

Body:
logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Vytvorenie, editácia a mazanie záznamov o aktívach	0,1
2	Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové	0,08
3	Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené)	0,07
4	Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia)	0,07
5	Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	0,06
6	Väzby medzi aktívami (napr. server – služba – aplikácia)	0,06
7	Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov	0,09
8	Možnosť filtrovania, fulltextového vyhľadávania a exportu	0,06
9	Podpora API (REST, GraphQL) na správu aktív a integráciu	0,06
10	Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django)	0,06
11	Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov)	0,06
12	Webové rozhranie s možnosťou úprav a prehľadnou správou	0,06
13	Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil)	0,06
14	Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie)	0,06
15	Upozornenia na zmenu stavu, expirácie, servisné intervaly	0,05
	súčet váh:	**1**

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia				
		LibreNMS	pi.Alert	NetBox	Ralph	GLPI
Kritériá pre SIEM nástroj	Vytvorenie, editácia a mazanie záznamov o aktívach	3	3	5	5	5
	Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové	3	2	5	4	4
	Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené)	3	2	5	4	5
	Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia)	3	2	4	5	4
	Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	5	2	5	3	3
	Väzby medzi aktívami (napr. server – služba – aplikácia)	2	1	5	3	4
	Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov	4	2	5	4	5
	Možnosť filtrovania, fulltextového vyhľadávania a exportu	3	3	5	4	5
	Podpora API (REST, GraphQL) na správu aktív a integráciu	4	3	5	4	4
	Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django)	3	2	5	4	5
	Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov)	5	4	3	3	3
	Webové rozhranie s možnosťou úprav a prehľadnou správou	4	3	5	4	4
	Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil)	3	2	4	4	5
	Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie)	2	2	3	4	5
	Upozornenia na zmenu stavu, expirácie, servisné intervaly	3	2	4	3	5

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia				
		váhy	LibreNMS	pi.Alert	NetBox	Ralph	GLPI
Kritériá pre SIEM nástroj	Vytvorenie, editácia a mazanie záznamov o aktívach	0,10	0,30	0,30	0,50	0,50	0,50
	Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové	0,08	0,24	0,16	0,40	0,32	0,32
	Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené)	0,07	0,21	0,14	0,35	0,28	0,35
	Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia)	0,07	0,21	0,14	0,28	0,35	0,28
	Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	0,06	0,30	0,12	0,30	0,18	0,18
	Väzby medzi aktívami (napr. server – služba – aplikácia)	0,06	0,12	0,06	0,30	0,18	0,24
	Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov	0,09	0,36	0,18	0,45	0,36	0,45
	Možnosť filtrovania, fulltextového vyhľadávania a exportu	0,06	0,18	0,18	0,30	0,24	0,30
	Podpora API (REST, GraphQL) na správu aktív a integráciu	0,06	0,24	0,18	0,30	0,24	0,24
	Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django)	0,06	0,18	0,12	0,30	0,24	0,30
	Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov)	0,06	0,30	0,24	0,18	0,18	0,18
	Webové rozhranie s možnosťou úprav a prehľadnou správou	0,06	0,24	0,18	0,30	0,24	0,24
	Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil)	0,06	0,18	0,12	0,24	0,24	0,30
	Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie)	0,06	0,12	0,12	0,18	0,24	0,30
	Upozornenia na zmenu stavu, expirácie, servisné intervaly	0,05	0,15	0,10	0,20	0,15	0,25
výsledný súčet pre dané riešenie			3,33	2,34	4,58	3,94	4,43

V5_Ticketing

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

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

V5_Ticketing

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Vytvorenie a editácia záznamov (ticketov)	Základná funkcionalita ticketovacieho systému – vytváranie, editovanie a mazanie ticketov.	1 = Len manuálne vytváranie záznamov bez ďalších možností; 5 = Pokročilé možnosti vrátane šablón, importov a viacstupňových vstupov.
2	Možnosť meniť stavy ticketu (napr. Nový, V riešení, Uzavretý, Odložený)	Schopnosť prepínať medzi rôznymi stavmi ticketu počas jeho životného cyklu.	1 = Iba pevne dané stavy bez možnosti úprav; 5 = Možnosť pridať vlastné stavy, definovať workflow.
3	Priradenie na konkrétneho riešiteľa (L1 analytik, eskalácia L2/L3)	Priradenie ticketov na konkrétnych riešiteľov vrátane eskalácie podľa úrovne.	1 = Iba ručné priradenie; 5 = Automatizované priradenie podľa pravidiel alebo rotácie.
4	Emailové notifikácie o zmenách stavu, komentároch, deadline	Automatické emailové notifikácie o zmene stavu, komentároch, deadline.	1 = Bez podpory emailov; 5 = Plná notifikácia s možnosťou úprav šablón, zmien a intervalu.
5	Pridávanie príloh (logy, dôkazy, screenshoty, výpisy z nástrojov)	Možnosť pridávať prílohy ako logy, snímky obrazovky a iné dôkazy.	1 = Iba textové polia; 5 = Podpora rôznych formátov príloh, drag&drop, kontrola veľkosti.
6	Možnosť evidovať časy (vytvorenie, aktualizácia, eskalácia, uzavretie)	Sledovanie a evidencia časových údajov pre celý životný cyklus ticketu.	1 = Bez časovej evidencie; 5 = Presné logovanie všetkých časových údajov a export.
7	Nastavenie priority a závažnosti incidentu	Nastavenie úrovne priority a závažnosti ticketu pre lepšie plánovanie.	1 = Len textové poznámky; 5 = Definovateľné úrovne priority, automatické pravidlá.
8	Možnosť vytvárať šablóny pre opakujúce sa typy incidentov	Tvorba šablón pre rýchle zadávanie často sa opakujúcich incidentov.	1 = Bez šablón; 5 = Možnosť definovať vlastné typy ticketov s prepojením na pravidlá.
9	Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie	Použitie tagov na uľahčenie vyhľadávania a kategorizácie.	1 = Žiadne značky; 5 = Viacúrovňové značky, farebné rozlíšenie, filtre.
10	Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi	Integrácia s inými bezpečnostnými nástrojmi na automatizáciu a workflow.	1 = Žiadna integrácia; 5 = Pokročilé REST integrácie, webhooky, ticket prepojený s udalosťami.
11	Podpora REST API a Webhookov	Podpora pre rozhrania REST API a Webhooky na komunikáciu s inými systémami.	1 = API len na čítanie; 5 = Full CRUD API, webhooky, autentifikácia.
12	Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	Možnosť exportovať tickety pre účely archivácie alebo reportingu.	1 = Len jednoduchý CSV export; 5 = Pravidelný export, rôzne formáty, plánovanie.
13	Moderné, responzívne webové rozhranie	Moderný a responzívny dizajn pre pohodlné používanie.	1 = Len základné UI; 5 = Responzívne, prispôsobiteľné rozhranie s UX optimalizáciou.
14	Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete	Zaznamenávanie všetkých akcií, zmien a komentárov v tickete.	1 = Bez logovania zmien; 5 = Kompletný audit trail so záznamom času, osoby a akcie.
15	Možnosť spätného prehľadu a forenznej analýzy	Schopnosť spätne analyzovať priebeh a históriu incidentov.	1 = Žiadna história incidentov; 5 = Prehľadná história s možnosťou filtrovania, exportu a vizualizácie.

Body:

logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Vytvorenie a editácia záznamov (ticketov)	0,07
2	Možnosť meniť stavy ticketu (napr. Nový, V riešení, Uzavretý, Odložený)	0,07
3	Priradenie na konkrétneho riešiteľa (L1 analytik, eskalácia L2/L3)	0,07
4	Emailové notifikácie o zmenách stavu, komentároch, deadline	0,07
5	Pridávanie príloh (logy, dôkazy, screenshoty, výpisy z nástrojov)	0,07
6	Možnosť evidovať časy (vytvorenie, aktualizácia, eskalácia, uzavretie)	0,07
7	Nastavenie priority a závažnosti incidentu	0,06
8	Možnosť vytvárať šablóny pre opakujúce sa typy incidentov	0,06
9	Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie	0,06
10	Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi	0,08
11	Podpora REST API a Webhookov	0,07
12	Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	0,06
13	Moderné, responzívne webové rozhranie	0,06
14	Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete	0,07
15	Možnosť spätného prehľadu a forenznej analýzy	0,06
	súčet váh:	**1**

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia			
		TheHive	Zammad	Request Tracker (RT)	osTicket
Kritériá pre SIEM nástroj	Vytvorenie a editácia záznamov (ticketov)	5	5	4	4
	Možnosť meniť stavy ticketu (napr. Nový, V riešení, Uzavretý, Odložený)	5	5	4	4
	Priradenie na konkrétneho riešiteľa (L1 analytik, eskalácia L2/L3)	5	4	4	3
	Emailové notifikácie o zmenách stavu, komentároch, deadline	4	5	4	4
	Pridávanie príloh (logy, dôkazy, screenshoty, výpisy z nástrojov)	5	5	4	4
	Možnosť evidovať časy (vytvorenie, aktualizácia, eskalácia, uzavretie)	5	4	4	3
	Nastavenie priority a závažnosti incidentu	5	5	4	3
	Možnosť vytvárať šablóny pre opakujúce sa typy incidentov	4	5	3	3
	Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie	5	5	3	3
	Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi	5	4	3	2
	Podpora REST API a Webhookov	5	5	4	3
	Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	4	4	4	4
	Moderné, responzívne webové rozhranie	4	5	3	3
	Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete	5	4	4	3
	Možnosť spätného prehľadu a forenznej analýzy	5	4	3	3

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia			
		váhy	TheHive	Zammad	Request Tracker (RT)	osTicket
Kritériá pre SIEM nástroj	Vytvorenie a editácia záznamov (ticketov)	0,07	0,35	0,35	0,28	0,28
	Možnosť meniť stavy ticketu (napr. Nový, V riešení, Uzavretý, Odložený)	0,07	0,35	0,35	0,28	0,28
	Priradenie na konkrétneho riešiteľa (L1 analytik, eskalácia L2/L3)	0,07	0,35	0,28	0,28	0,21
	Emailové notifikácie o zmenách stavu, komentároch, deadline	0,07	0,28	0,35	0,28	0,28
	Pridávanie príloh (logy, dôkazy, screenshoty, výpisy z nástrojov)	0,07	0,35	0,35	0,28	0,28
	Možnosť evidovať časy (vytvorenie, aktualizácia, eskalácia, uzavretie)	0,07	0,35	0,28	0,28	0,21
	Nastavenie priority a závažnosti incidentu	0,06	0,30	0,30	0,24	0,18
	Možnosť vytvárať šablóny pre opakujúce sa typy incidentov	0,06	0,24	0,30	0,18	0,18
	Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie	0,06	0,30	0,30	0,18	0,18
	Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi	0,08	0,40	0,32	0,24	0,16
	Podpora REST API a Webhookov	0,07	0,35	0,35	0,28	0,21
	Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	0,06	0,24	0,24	0,24	0,24
	Moderné, responzívne webové rozhranie	0,06	0,24	0,30	0,18	0,18
	Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete	0,07	0,35	0,28	0,28	0,21
	Možnosť spätného prehľadu a forenznej analýzy	0,06	0,30	0,24	0,18	0,18
výsledný súčet pre dané riešenie			4,75	4,59	3,68	3,26

V5_Evidencia, správa incidentov

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

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

V5_Evidencia, správa incidentov

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Tvorba a správa prípadov (cases) s úlohami a detailmi	Možnosť vytvárať incidenty ako prípady s úlohami, popisom a atribútmi.	1 = Iba jednoduchý záznam; 5 = Komplexné prípady s úlohami, atribútmi, väzbami.
2	Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	Možnosť sledovať IOC ako súčasť prípadu.	1 = Žiadna podpora pre IOC; 5 = Plná správa IOC vrátane stavu, histórie a väzieb.
3	Prepojenie medzi prípadmi na základe spoločných indikátorov	Automatická alebo manuálna identifikácia súvisiacich incidentov.	1 = Žiadna podpora prepájania; 5 = Automatická korelácia na základe IOC, času, typov útokov.
4	Kategorizácia incidentov pomocou tagov	Možnosť kategorizovať incidenty pomocou štítkov/tagov.	1 = Bez tagovania; 5 = Pokročilé tagovanie s podporou filtrov a štatistík.
5	Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	Integrácia na obohatenie IOC a metadát z CTI alebo iných systémov.	1 = Manuálne pridávanie údajov; 5 = Automatické enrichovanie cez API/CTI.
6	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.	1 = Bez možnosti úprav; 5 = Vysoká miera konfigurovateľnosti, UI pre šablóny a workflow.
7	Podpora viacerých používateľských rolí – minimálne analytik a administrátor	Podpora RBAC pre rôzne roly.	1 = Jedna rola; 5 = Viacero rolí s možnosťou priraďovania práv.
8	Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi	Schopnosť prevádzkovať systém pre viac entít súčasne.	1 = Jedna organizácia bez izolácie; 5 = Multitenantné prostredie s kontrolou zdieľania.
9	Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy	Možnosť obojsmernej výmeny dát.	1 = Bez integrácií; 5 = API + konektory pre viac systémov.
10	Export incidentov do formátov CSV, PDF, cez REST API	Export dát pre dokumentáciu alebo reportovanie.	1 = Žiadny export; 5 = Podpora viacerých formátov a cez API.
11	Logovanie činností analytikov počas riešenia incidentu (audit trail)	Evidencia činností pre forenznú analýzu.	1 = Žiadne logovanie; 5 = Detailné logovanie každého kroku a používateľa.
12	Jednoduchá správa konfigurácií a aktualizácií	Schopnosť spravovať platformu bez potreby zásahu do kódu.	1 = Vyžaduje manuálny zásah; 5 = GUI/web rozhranie pre správu.
13	Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie	Možnosť rozšíriť schému incidentu.	1 = Pevne dané štruktúry; 5 = Prispôsobiteľné polia a typy.
14	Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov	Umožňuje získať úplný časový priebeh incidentu.	1 = Žiadna rekonštrukcia; 5 = Kompletný audit trail, časová os, väzby.
15	Zdieľanie prípadov medzi tímami a externými partnermi podľa práv	Podpora riadeného zdieľania prípadov.	1 = Žiadna možnosť zdieľania; 5 = Detailná kontrola prístupu na úrovni prípadu alebo položky.

Body:

logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Tvorba a správa prípadov (cases) s úlohami a detailmi	0,08
2	Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	0,07
3	Prepojenie medzi prípadmi na základe spoločných indikátorov	0,07
4	Kategorizácia incidentov pomocou tagov	0,06
5	Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	0,08
6	Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	0,07
7	Podpora viacerých používateľských rolí – minimálne analytik a administrátor	0,06
8	Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi	0,06
9	Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy	0,08
10	Export incidentov do formátov CSV, PDF, cez REST API	0,06
11	Logovanie činností analytikov počas riešenia incidentu (audit trail)	0,06
12	Jednoduchá správa konfigurácií a aktualizácií	0,05
13	Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie	0,06
14	Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov	0,07
15	Zdieľanie prípadov medzi tímami a externými partnermi podľa práv	0,07
	súčet váh:	**1**

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia	
		TheHive	RTIR
Kritériá pre SIEM nástroj	Tvorba a správa prípadov (cases) s úlohami a detailmi	5	4
	Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	5	3
	Prepojenie medzi prípadmi na základe spoločných indikátorov	5	2
	Kategorizácia incidentov pomocou tagov	5	3
	Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	5	3
	Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	5	3
	Podpora viacerých používateľských rolí – minimálne analytik a administrátor	5	4
	Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi	4	2
	Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy	5	3
	Export incidentov do formátov CSV, PDF, cez REST API	5	4
	Logovanie činností analytikov počas riešenia incidentu (audit trail)	5	3
	Jednoduchá správa konfigurácií a aktualizácií	4	3
	Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie	5	3
	Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov	5	4
	Zdieľanie prípadov medzi tímami a externými partnermi podľa práv	5	3

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia	
		váhy	TheHive	RTIR
Kritériá pre SIEM nástroj	Tvorba a správa prípadov (cases) s úlohami a detailmi	0,08	0,40	0,32
	Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	0,07	0,35	0,21
	Prepojenie medzi prípadmi na základe spoločných indikátorov	0,07	0,35	0,14
	Kategorizácia incidentov pomocou tagov	0,06	0,30	0,18
	Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	0,08	0,40	0,24
	Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	0,07	0,35	0,21
	Podpora viacerých používateľských rolí – minimálne analytik a administrátor	0,06	0,30	0,24
	Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi	0,06	0,24	0,12
	Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy	0,08	0,40	0,24
	Export incidentov do formátov CSV, PDF, cez REST API	0,06	0,30	0,24
	Logovanie činností analytikov počas riešenia incidentu (audit trail)	0,06	0,30	0,18
	Jednoduchá správa konfigurácií a aktualizácií	0,05	0,20	0,15
	Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie	0,06	0,30	0,18
	Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov	0,07	0,35	0,28
	Zdieľanie prípadov medzi tímami a externými partnermi podľa práv	0,07	0,35	0,21
výsledný súčet pre dané riešenie			4,89	3,14

V5_Reporting

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

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

V5_Reporting

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Vytvorenie základného prehľadu stavu bezpečnosti a incidentov	Možnosť vytvárať zhrnutia stavu bezpečnosti, incidentov a aktivity systému.	1 = Len základný súhrn bez podrobností; 5 = Komplexný prehľad vrátane trendov, metrik a štatistík.
2	Možnosť stiahnuť report alebo automaticky odoslať (e-mail, webhook)	Exportovanie reportov manuálne alebo ich plánovaná automatická distribúcia.	1 = Len manuálne stiahnutie; 5 = Automatická distribúcia cez e-mail, webhook alebo iné kanály.
3	Možnosť výberu obsahu reportu – časové obdobie, typy incidentov	Možnosť filtrovať obsah reportu podľa času, typu alebo zdrojových údajov.	1 = Fixný, nedefinovateľný obsah; 5 = Úplne prispôsobiteľný výber údajov a filtrov.
4	Plánovanie pravidelných (napr. denných, týždenných) reportov	Možnosť nastaviť generovanie reportov na základe harmonogramu.	1 = Žiadne plánovanie; 5 = Pokročilé plánovanie vrátane viacerých frekvencií a šablón.
5	Možnosť generovania jednorazových ad-hoc reportov	Tvorba reportov mimo pravidelného harmonogramu podľa potreby.	1 = Len plánované alebo fixné reporty; 5 = Okamžité ad-hoc generovanie s výberom parametrov.
6	Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie)	Možnosť upraviť vzhľad reportu podľa firemnej identity.	1 = Žiadne prispôsobenie; 5 = Plne konfigurovateľné vizuálne prvky (farby, logá, záhlavie).
7	Podpora exportu do PDF, CSV, JSON	Možnosť exportovať reporty do rôznych bežných formátov.	1 = Len jeden formát (napr. PDF); 5 = Podpora viacnásobných exportných formátov vrátane štruktúrovaných.
8	Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI, …	Možnosť zbierať údaje z iných systémov a vytvárať prepojené reporty.	1 = Žiadna integrácia; 5 = Nativná podpora viacerých typov integrácií.
9	Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy	Vizualizácia dát priamo v reportoch rôznymi formami.	1 = Len textový výstup; 5 = Interaktívne a bohaté vizualizácie (grafy, mapy, metriky).
10	Podpora rôznych zdrojov: databázy, logy, API výstupy	Schopnosť agregovať dáta z viacerých technických a analytických zdrojov.	1 = Len fixný dátový zdroj; 5 = Dynamická podpora viacerých typov zdrojov a konektorov.
11	Webové/GUI rozhranie pre tvorbu a správu reportov	Používateľsky prívetivé rozhranie pre návrh, úpravu a správu reportov.	1 = Žiadne rozhranie alebo len CLI; 5 = Moderné, responzívne a intuitívne GUI s podporou šablón.
12	Možnosť archivácie vygenerovaných reportov	Možnosť uchovávať reporty pre spätnú analýzu a audit.	1 = Reporty sa neukladajú; 5 = Archivácia s podporou verzovania a vyhľadávania.
13	Možnosť obmedziť prístup k reportom podľa rolí (RBAC)	Prístup k reportom riadený rolami a oprávneniami.	1 = Žiadna kontrola prístupu; 5 = Detailné RBAC s možnosťou nastavenia na úrovni reportu.
14	Šifrované prenosy reportov pri automatickej distribúcii	Bezpečný prenos citlivých dát cez šifrované kanály.	1 = Nešifrované odosielanie; 5 = Šifrovanie všetkých distribúcií (napr. TLS, SFTP).

Body:
logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Vytvorenie základného prehľadu stavu bezpečnosti a incidentov	0,1
2	Možnosť stiahnuť report alebo automaticky odoslať (e-mail, webhook)	0,07
3	Možnosť výberu obsahu reportu – časové obdobie, typy incidentov	0,07
4	Plánovanie pravidelných (napr. denných, týždenných) reportov	0,07
5	Možnosť generovania jednorazových ad-hoc reportov	0,07
6	Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie)	0,05
7	Podpora exportu do PDF, CSV, JSON	0,08
8	Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI, ...	0,1
9	Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy	0,07
10	Podpora rôznych zdrojov: databázy, logy, API výstupy	0,06
11	Webové/GUI rozhranie pre tvorbu a správu reportov	0,07
12	Možnosť archivácie vygenerovaných reportov	0,06
13	Možnosť obmedziť prístup k reportom podľa rolí (RBAC)	0,06
14	Šifrované prenosy reportov pri automatickej distribúcii	0,07
	súčet váh:	**1**

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia	
		Kibana (ELK)	Grafana
Kritériá pre SIEM nástroj	Vytvorenie základného prehľadu stavu bezpečnosti a incidentov	5	3
	Možnosť stiahnuť report alebo automaticky odoslať (e-mail, webhook)	4	5
	Možnosť výberu obsahu reportu – časové obdobie, typy incidentov	4	4
	Plánovanie pravidelných (napr. denných, týždenných) reportov	4	5
	Možnosť generovania jednorazových ad-hoc reportov	4	4
	Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie)	3	5
	Podpora exportu do PDF, CSV, JSON	4	5
	Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI, ...	5	3
	Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy	5	5
	Podpora rôznych zdrojov: databázy, logy, API výstupy	4	4
	Webové/GUI rozhranie pre tvorbu a správu reportov	4	5
	Možnosť archivácie vygenerovaných reportov	3	3
	Možnosť obmedziť prístup k reportom podľa rolí (RBAC)	4	4
	Šifrované prenosy reportov pri automatickej distribúcii	4	4

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia	
		váhy	Kibana (ELK)	Grafana
Kritériá pre SIEM nástroj	Vytvorenie základného prehľadu stavu bezpečnosti a incidentov	0,1	0,50	0,30
	Možnosť stiahnuť report alebo automaticky odoslať (e-mail, webhook)	0,07	0,28	0,35
	Možnosť výberu obsahu reportu – časové obdobie, typy incidentov	0,07	0,28	0,28
	Plánovanie pravidelných (napr. denných, týždenných) reportov	0,07	0,28	0,35
	Možnosť generovania jednorazových ad-hoc reportov	0,07	0,28	0,28
	Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie)	0,05	0,15	0,25
	Podpora exportu do PDF, CSV, JSON	0,08	0,32	0,40
	Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI, ...	0,10	0,50	0,30
	Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy	0,07	0,35	0,35
	Podpora rôznych zdrojov: databázy, logy, API výstupy	0,06	0,24	0,24
	Webové/GUI rozhranie pre tvorbu a správu reportov	0,07	0,28	0,35
	Možnosť archivácie vygenerovaných reportov	0,06	0,18	0,18
	Možnosť obmedziť prístup k reportom podľa rolí (RBAC)	0,06	0,24	0,24
	Šifrované prenosy reportov pri automatickej distribúcii	0,07	0,28	0,28
výsledný súčet pre dané riešenie			4,16	4,15

V5_SOC knowledge portal

V5 zoznam definovaných kritérií
KPB2 – Návrh SOCaaS služby; typ – zoznam; mesiac odovzdania – M5

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

V5_SOC knowledge portal

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Vytváranie, editácia a verzovanie záznamov (návody, playbooky, FAQ)	Možnosť vytvárať, upravovať a sledovať verzie dokumentov s históriou zmien.	1 = Len manuálna úprava bez histórie zmien; 5 = Plnohodnotná verzovacia kontrola s prehľadom zmien a možnosťou obnovy staršej verzie.
2	Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky (tags)	Organizácia KB dokumentov podľa štruktúrovaných pravidiel (kategórie, tagy, sekcie).	1 = Žiadna alebo minimálna organizácia; 5 = Podpora viacerých úrovní štruktúrovania a hierarchie tagov.
3	Fulltextové vyhľadávanie s podporou filtrov a tagov	Vyhľadávanie v KB s možnosťou filtrovania podľa tagov, kategórií a obsahu.	1 = Základné vyhľadávanie podľa názvu; 5 = Pokročilé vyhľadávanie s filtrom podľa obsahu, tagov a parametrov.
4	Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	Možnosť prepojenia znalostných článkov s konkrétnymi typmi útokov a incidentmi v iných nástrojoch.	1 = Žiadna možnosť prepojenia; 5 = Dynamické prepájanie KB s incidentmi, IOC a CTI platformami.
5	Možnosť vkladať obrázky, logy, odkazy a prílohy	Schopnosť obohatiť dokumenty o multimediálny alebo dátový obsah.	1 = Len čistý text; 5 = Podpora obrázkov, logov, súborov a odkazov v rôznych formátoch.
6	Podpora RBAC – rôzne úrovne prístupu pre čítanie, editáciu, schvaľovanie	Riadenie prístupu podľa používateľských rolí.	1 = Žiadna podpora oprávnení; 5 = Detaily RBAC pre čítanie, schvaľovanie, úpravy s audit trail.
7	Možnosť integrácie s ticketingom, incident managementom, SIEM	Prepojenie KB s inými systémami pre efektívnejšie používanie obsahu.	1 = Bez integrácie; 5 = REST API a priama integrácia s viacerými nástrojmi.
8	Export dokumentov do PDF, HTML alebo Markdown formátu	Možnosť exportu dokumentov na offline použitie alebo publikovanie.	1 = Bez exportu; 5 = Export do rôznych formátov vrátane šablónovania a štýlov.
9	Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	Používateľsky prívetivé GUI pre správu znalostí.	1 = Zložité alebo technicky orientované rozhranie; 5 = Moderné WYSIWYG s jednoduchým publikovaním.
10	Zachovanie histórie zmien s možnosťou obnovy staršej verzie	Sledovanie a archivácia zmien pre každý dokument.	1 = Bez možnosti sledovania zmien; 5 = Kompletný version control so záznamami a rollback.
11	Záznamy o tom, kto a kedy upravoval dokument	Audit trail zmien dokumentov s informáciou o autoroch a čase.	1 = Bez záznamu aktivít; 5 = Detailná história aktivít pre každý dokument.
12	Možnosť tvorby schvaľovacích workflow pre nové KB články	Procesy schvaľovania pre publikáciu nových článkov.	1 = Manuálne schvaľovanie bez pravidiel; 5 = Plne automatizované workflow s viacúrovňovým schvaľovaním.

Body:

logiku priraďovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Vytváranie, editácia a verzovanie záznamov (návody, playbooky, FAQ)	0,1
2	Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky (tags)	0,08
3	Fulltextové vyhľadávanie s podporou filtrov a tagov	0,08
4	Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	0,07
5	Možnosť vkladať obrázky, logy, odkazy a prílohy	0,08
6	Podpora RBAC – rôzne úrovne prístupu pre čítanie, editáciu, schvaľovanie	0,08
7	Možnosť integrácie s ticketingom, incident managementom, SIEM	0,09
8	Export dokumentov do PDF, HTML alebo Markdown formátu	0,07
9	Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	0,08
10	Zachovanie histórie zmien s možnosťou obnovy staršej verzie	0,08
11	Záznamy o tom, kto a kedy upravoval dokument	0,09
12	Možnosť tvorby schvaľovacích workflow pre nové KB články	0,1
	súčet váh:	**1**

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia		
		TheHive	BookStack	Wiki.js
Kritériá pre SIEM nástroj	Vytváranie, editácia a verzovanie záznamov (návody, playbooky, FAQ)	4	5	5
	Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky (tags)	3	5	5
	Fulltextové vyhľadávanie s podporou filtrov a tagov	4	4	5
	Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	5	3	3
	Možnosť vkladať obrázky, logy, odkazy a prílohy	4	5	5
	Podpora RBAC – rôzne úrovne prístupu pre čítanie, editáciu, schvaľovanie	4	5	5
	Možnosť integrácie s ticketingom, incident managementom, SIEM	5	3	3
	Export dokumentov do PDF, HTML alebo Markdown formátu	3	5	5
	Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	4	5	5
	Zachovanie histórie zmien s možnosťou obnovy staršej verzie	4	5	5
	Záznamy o tom, kto a kedy upravoval dokument	4	5	5
	Možnosť tvorby schvaľovacích workflow pre nové KB články	3	4	5

Prepočet so zohľadnením váh jednotlivých kritérií

			dostupné riešenia		
		váhy	TheHive	BookStack	Wiki.js
Kritériá pre SIEM nástroj	Vytváranie, editácia a verzovanie záznamov (návody, playbooky, FAQ)	0,10	0,40	0,50	0,50
	Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky (tags)	0,08	0,24	0,40	0,40
	Fulltextové vyhľadávanie s podporou filtrov a tagov	0,08	0,32	0,32	0,40
	Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	0,07	0,35	0,21	0,21
	Možnosť vkladať obrázky, logy, odkazy a prílohy	0,08	0,32	0,40	0,40
	Podpora RBAC – rôzne úrovne prístupu pre čítanie, editáciu, schvaľovanie	0,08	0,32	0,40	0,40
	Možnosť integrácie s ticketingom, incident managementom, SIEM	0,09	0,45	0,27	0,27
	Export dokumentov do PDF, HTML alebo Markdown formátu	0,07	0,21	0,35	0,35
	Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	0,08	0,32	0,40	0,40
	Zachovanie histórie zmien s možnosťou obnovy staršej verzie	0,08	0,32	0,40	0,40
	Záznamy o tom, kto a kedy upravoval dokument	0,09	0,36	0,45	0,45
	Možnosť tvorby schvaľovacích workflow pre nové KB články	0,10	0,30	0,40	0,50
výsledný súčet pre dané riešenie			3,91	4,50	4,68