V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

Funded by the European Union NextGenerationEU | RECOVERY AND RESILIENCE | GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC | UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics | BRAIN:IT

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Supported log formats (syslog, JSON, CSV, CEF, LEEF...)	The ability of the SIEM to receive and process logs in various standardized formats.	1 = Supports only basic formats (e.g. syslog and JSON); 5 = Supports a wide range of standards including CEF, LEEF, CSV, syslog, JSON, etc.
2	Real-time vs. batch processing	The ability to process logs in real time (streaming) or only in batches.	1 = Batch processing only (e.g. every X hours); 5 = Genuinely real time (latency of seconds or a streaming engine).
3	Event correlation (predefined and custom rules)	The ability to link related events using correlation rules.	1 = Only basic correlation rules with no possibility of modification; 5 = Custom correlation rules + an advanced engine for creating custom correlations.
4	Machine Learning/Behavioural analysis	The ability of the SIEM system to detect anomalies using machine learning.	1 = No ML/behavioural functionality; 5 = Advanced ML models for anomaly detection with self-learning and adaptability.
5	Threat Intelligence (CTI) integration	Integration with threat sources (IOC, TTP), automatic data enrichment.	1 = No or only very limited CTI support; 5 = Integration of multiple CTI sources (MISP, OTX, VirusTotal, Abuse.ch...) and automatic enrichment of their data.
6	Anomaly detection	Detection of non-standard behaviour or deviations from expected behaviour.	1 = Signature-based or manual detection only; 5 = Automatic behavioural detection based on a baseline and adaptive models.
7	Custom alerting rules and thresholds	The ability to define custom rules and conditions for generating alerts.	1 = Only fixed notifications with no possibility of modification; 5 = The ability to define complex conditions, thresholds, filters, logic and alert schemes.
8	Automated responses (e.g. IP blocking, SOAR integration)	The ability to trigger a response (blocking, isolation, notification) automatically.	1 = No automated response whatsoever; 5 = Support for actions such as blocking, isolation and quarantine via integrations with SOAR, EDR, SIEM.
9	Data normalization and enrichment	Transformation of various logs into a unified format and their enrichment (e.g. WHOIS, GEOIP).	1 = No standardization or enrichment. 5 = Automatic mapping of data into a normalized format + enrichment from multiple sources (e.g. CTI, asset DB).
10	Full-text and fast search	The ability to search logs using operators, tags and filters.	1 = Only basic filtering or no search; 5 = Advanced full-text search with operators, filters and fast response.
11	Dashboards (including interactive ones) and their categorization	Data visualization using charts, filters and widgets.	1 = None or only static outputs; 5 = Dynamic, interactive dashboards with support for custom layouts, filters and drill-down.
12	Support for MITRE ATT&CK mapping	The ability to map detections to tactics and techniques according to MITRE ATT&CK.	1 = No support or manual correlation; 5 = Automatic mapping of detections to ATT&CK techniques with visualization and export capability.
13	Retention (flexible, by log type)	The ability to set log retention policies by source and importance.	1 = Fixed retention with no configuration options; 5 = The ability to set different retention policies by log type, source or content.
14	Encryption (both in transit and at rest)	Protection of logs against unauthorized access during transmission and storage.	1 = Logs are not encrypted, not even in transit; 5 = Complete encryption both in transit (TLS, HTTPS) and at rest (AES, GPG, disk-level).
15	System health monitoring (healthcheck)	Monitoring of system performance, availability and functionality.	1 = No monitoring tools or manual only; 5 = Integrated notifications, metrics and alerts in the event of problems (e.g. CPU, disk, memory, processing latency)

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5, where 1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
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 Inteligence (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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

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

V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

Funded by the European Union NextGenerationEU | RECOVERY AND RESILIENCE | GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC | UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics | BRAIN:IT

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Receiving alerts and data from various security systems	The ability to receive alerts and data from various security sources (SIEM, EDR, CTI...).	1 = Support for only some sources or manual import; 5 = Automatic receipt of alerts from various systems including SIEM, EDR, CTI, etc.
2	Data normalization and parsing	Transformation of input data into a standardized format for further processing.	1 = No parsing or simple mapping; 5 = Advanced normalization mechanisms, parsing of various formats.
3	Incident categorization and prioritization	The ability to sort incidents by severity, type, category and importance.	1 = Fixed categories, with no possibility of modification; 5 = Custom categories, priorities, the ability to set scoring and automatic sorting.
4	Ability to create incident tickets both manually and automatically	Support for both manual and automatic creation of incident tickets from input data.	1 = Manual ticket creation only; 5 = Both automatic and manual creation with integration with ticketing systems.
5	Predefined playbooks	Availability of basic response scenarios and automations prepared in advance in the tool.	1 = No pre-prepared playbooks; 5 = A rich library of pre-prepared playbooks for various scenarios.
6	Ability to create custom playbooks without the need for programming	The ability to create and manage playbooks using a visual interface without the need for coding.	1 = Requires manual scripting; 5 = Fully visual low-code/no-code environment.
7	Workflow engine with branching, conditions and loops	The ability to define complex logic in playbooks using decision points.	1 = Sequential actions only, without logic; 5 = Advanced workflow engine with support for IF, LOOP, CASE and other elements.
8	Automated responses: IP blocking, host isolation, escalation	The ability to automatically perform responses such as blocking, isolation or notification.	1 = None or notifications only; 5 = Fully automated responses including interaction with firewall, EDR, SOAR.
9	Orchestration between systems: SIEM, CTI, ticketing, communication tools, firewall, EDR	Interconnection and data exchange with other systems within the incident response process.	1 = Limited or no integration; 5 = Strong orchestration across many types of systems with bidirectional communication.
10	API-first approach (REST, Webhooks)	Accessibility of the tool's functions via an API and support for webhooks for notifications and interactions.	1 = Missing or limited API; 5 = Fully covered API-first approach and webhooks for responses.
11	Support for plug-ins and connectors	The ability to extend the tool's functionality through modules or connectors.	1 = No extensibility; 5 = Support for dozens of plug-ins or the creation of custom ones.
12	Dashboards for incident status and statistics	Clear display of the system status and ongoing incidents.	1 = None or static listings; 5 = Interactive, customizable dashboards with filters and drill-down capabilities.
13	RBAC and audit trail	Role-based access control and logging of changes in the system.	1 = No RBAC or audit trail; 5 = Detailed RBAC policies and recording of all actions.
14	Playbook debugging & testing	The ability to test and debug playbooks before their production deployment.	1 = No support for testing; 5 = A separate test environment, debugging tools and input simulation.
15	SOAR-SIEM synchronization of incident status	Linking of incident status between the SIEM and SOAR for up-to-date visibility.	1 = Manual or no synchronization; 5 = Automated bidirectional synchronization of incident statuses.

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5, where 1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
1	Prijímanie upozornení a dát z rôznych bezpečnostných systémov	0,08
2	Normalizácia a parsovanie dát	0,07
3	Kategorizácia a priorizácia 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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

		Kritériá pre SOAR nástroj														
		Prijímanie upozornení a dát z rôznych bezpečnostných systémov	Normalizácia a parsovanie dát	Kategorizácia a priorizácia incidentov	Možnosť manuálneho aj automatického vytvárania incident ticketov	Preddefinované playbooky	Možnosť tvorby vlastných playbookov bez potreby programovania	Workflow engine s vetvením, podmienkami a slučkami	Automatizované reakcie: blok IP, izolácia hostu, eskalácia	Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR	API-first prístup (REST, Webhooky)	Podpora pre plug-iny a konektory	Dashboardy pre stav a štatistiky incidentov	RBAC a audit trail	Playbook debugging & testing	SOAR-SIEM synchronizácia stavu incidentov	**resulting total for the given solution**
	weights	0,08	0,07	0,07	0,07	0,05	0,08	0,07	0,08	0,08	0,07	0,05	0,06	0,06	0,05	0,06	
available solutions	Shuffle	0,4	0,28	0,28	0,28	0,2	0,4	0,35	0,4	0,4	0,35	0,25	0,24	0,24	0,25	0,24	4,56
	TheHive+ Cortex	0,4	0,28	0,35	0,35	0,15	0,24	0,21	0,32	0,32	0,28	0,15	0,3	0,3	0,15	0,3	4,1
	StackStorm	0,32	0,35	0,28	0,28	0,25	0,24	0,35	0,32	0,4	0,35	0,25	0,18	0,24	0,2	0,24	4,25
	Fasten Health Tracecat	0,24	0,21	0,21	0,21	0,15	0,16	0,21	0,24	0,24	0,28	0,15	0,18	0,18	0,1	0,12	2,86
	FIR (Fast Incident Response)	0,24	0,21	0,28	0,28	0,1	0,16	0,14	0,24	0,24	0,21	0,15	0,18	0,24	0,1	0,18	2,95

V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

Funded by the European Union NextGenerationEU | RECOVERY AND RESILIENCE | GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC | UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics | BRAIN:IT

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Deployment options: on-prem, cloud, hybrid	The ability to deploy the solution in various	1 – Only one environment supported, without flexibility; 5 – Full
2	Support for various OSs (Windows, Linux, macOS)	Support for installing and running the agent on various operating systems.	1 – Support for only one OS; 5 – Native support for Windows, Linux and macOS.
3	Collection of audit data using agents	Collection of audit records on user activities, processes and the system via the agent.	1 – No collection of audit data; 5 – Comprehensive audit trail collection via the agent.
4	File Integrity Monitoring (FIM)	Real-time detection of file changes for the purposes of forensic analysis and integrity.	1 – FIM is completely missing; 5 – Advanced FIM with notifications and rules.
5	Collection of system metrics, processes and behaviour	Monitoring of system behaviour and metrics such as CPU, memory, services and processes.	1 – No metrics, or behaviour is not monitored; 5 – A wide range of system data is covered.
6	Collection of information on vulnerabilities and configurations	Obtaining information on vulnerabilities from configuration data and comparison with CVE databases.	1 – Not available; 5 – Automated collection and mapping against CVE/CPE.
7	Log analysis and correlation with threats	Log analysis with the aim of detecting correlated events and potential threats.	1 – Analysis missing or minimal correlation; 5 – Fully correlated log analysis.
8	Malware and intrusion detection	Identification of malicious software and security breach incidents.	1 – Does not detect malware; 5 – Multi-layer real-time detection.
9	Heuristic and behavioural analysis	Basing detection on behaviour and heuristics rather than on signatures alone.	1 – No heuristics; 5 – Effective behavioural detection of new threats.
10	Support for ML/AI algorithms for threat detection	Use of artificial intelligence algorithms for the detection of anomalies and threats.	1 – ML/AI is not used; 5 – Makes full use of models for anomaly detection.
11	Mapping to the MITRE ATT&CK framework	Classification of detected activities and techniques within the MITRE ATT&CK framework for the purposes of TTP analyses.	1 – No link to ATT&CK; 5 – Automatic classification according to MITRE ATT&CK.
12	Automatic responses (e.g. device isolation, file quarantine)	Automatic response to incidents, such as endpoint isolation or file quarantine.	1 – Response possible only manually; 5 – Fully automatic responses and measures.
13	Low system load of the agent	The agent has a low impact on system performance, which allows deployment on a large scale.	1 – The agent places a significant load on the system; 5 – Minimal impact on performance.
14	Simple central management of agents	A central console for the management, configuration and supervision of all agents.	1 – Manual configuration of each agent; 5 – Fully centralized and scalable.
15	Regular updates of signatures and modules	Regular updates of threat databases, signatures and detection rules.	1 – Manual updates without support; 5 – Regular and automatic updates.

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5, where 1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

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

V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

Funded by the European Union NextGenerationEU | RECOVERY AND RESILIENCE | GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC | UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics | BRAIN:IT

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Free version, open-source solution with the possibility of extension	Availability of basic functionality without a licence and the possibility of extension.	1 = Commercial version only; 5 = Fully open-source with the possibility of extension and customization.
2	Estimated scanning capacity (for example, min. 100 IP/24h)	The ability of the tool to scan large networks efficiently.	1 = Under 50 IPs per day; 5 = 1000+ IPs per day without restrictions.
3	Vulnerability test updates – community and enterprise feed	Frequency and scope of updates of detection patterns.	1 = No/very infrequent updates; 5 = Daily updated community and enterprise feed.
4	Support for CPE, CVE identifiers	The ability to identify vulnerabilities by standardized identifiers.	1 = No CPE/CVE support; 5 = Full support with linkage to databases such as NVD.
5	Acceptable web interface for managing scans and results	Usability of the GUI for managing scans and results.	1 = Non-intuitive CLI interface; 5 = Modern, responsive, clear GUI.
6	No need for agents (agentless)	The ability to perform scans without the need to install an agent on devices.	1 = Agent required for each host; 5 = Full support for agentless mode.
7	Support for scheduling tasks and alerts (optional)	The ability to automate recurring tasks and the generation of alerts.	1 = No scheduling functionality; 5 = Cron-like scheduling + e-mail/REST alerts.
8	Remediation tickets – integration or export	The ability to export findings to a ticketing system or to CSV, JSON, PDF.	1 = No export support; 5 = Direct integration with remediation systems (e.g. Jira, RT).
9	Configurable report formats (e.g. CSV, XML, PDF)	Flexibility of outputs for further processing.	1 = Text or HTML output only; 5 = Support for multiple structured formats.
10	Deployment options: on-premise, cloud/SaaS, VM, Docker	Flexibility of installation in various environments.	1 = Physical servers only; 5 = All variants including containerization and SaaS.
11	Scanning architecture (monolithic or master/sensor)	Scalability and adaptability of scan distribution.	1 = Monolithic solution with no possibility of splitting; 5 = Master/agent architecture with scan distribution.
12	Integrations with tools such as PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	The ability to connect to other security and IT systems.	1 = No support for integrations; 5 = Broad support including plugins and REST API.
13	Support for CVSS 4.0	Support for the latest version of the CVSS scoring system.	1 = No CVSS support; 5 = CVSS 4.0 support with an explanation of impact and risk.
14	Support for EPSS – vulnerability exploitation prediction	Use of vulnerability exploitation probability models.	1 = No EPSS support; 5 = Dynamic score using EPSS.
15	Compliance policies for standards (e.g. GDPR, ISO, CIS, BSI...)	The ability to assess vulnerabilities in relation to standards.	1 = No mapping functionality; 5 = Predefined compliance templates for ISO, GDPR, etc.

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5, where 1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

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

V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

Funded by the European Union NextGenerationEU | RECOVERY AND RESILIENCE | GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC | UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics | BRAIN:IT

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Support for strategic CTI (reports, impact analyses, attack trends)	Acquisition and analysis of information on long-term trends, attack impacts and strategic recommendations.	1 = No support for strategic outputs; 5 = Fully supported strategic reports, trend visualizations and impact analyses.
2	Support for operational CTI (TTPs, group profiling)	The ability to map techniques, tactics and procedures (TTPs) and to identify attacker groups and their behaviour.	1 = No support for operational CTI; 5 = Complete profiling of APT groups, TTPs with ATT&CK integration.
3	Support for tactical CTI (IOCs, IPs, hashes, URLs, domains)	Working with indicators of compromise (IOCs), including their recording, processing and distribution.	1 = Manual entry of IOCs only; 5 = Automated import/export, IOC management, time validity.
4	Automated collection from open-source, community and internal sources	Automatic downloading of data from various sources (e.g. GitHub, feeds, MISP, API systems).	1 = Manual data collection only; 5 = Automated downloading of multiple feeds with scheduling capability.
5	Support for Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	Ready-made connectors or integrations for well-known CTI sources.	1 = No support for these sources; 5 = Fully integrated with regular data updates.
6	Integration with 3rd party services such as VirusTotal, Shodan, DomainTools, URLScan.io	The ability to enrich IOCs and other artefacts using external services.	1 = No integration support; 5 = Direct API connectors with the ability to enrich observables.
7	Ability to normalize CTI data into a unified format	Consolidation of data from various formats into a structured unified output.	1 = Unstructured, heterogeneous data; 5 = Normalization into STIX/JSON or an internal format.
8	Possibility of manual CTI analysis	Interface and tools for security analysts for manual examination of data.	1 = No analytical functionality; 5 = Detailed GUI, interactive elements, timeline, pairing of IOCs and TTPs.
9	Semi-automated or fully automated processing and unification of data	Workflow capability for data processing without the need for manual intervention.	1 = Manual processing only; 5 = Automatic aggregation, filtering, deduplication.
10	Deduplication of threats and information	Removal of redundant IOCs and indicators.	1 = High redundancy without filters; 5 = Advanced deduplication logic by source, time and type.
11	Integration with SIEM and firewall for use in automated detections	Forwarding of IOCs and data directly to detection systems (SIEM, IDS, firewall).	1 = No integration; 5 = Full compatibility via STIX, API or push mechanisms.
12	Mapping to MITRE ATT&CK for TTP analysis and team collaboration	Linking incidents, IOCs and TTPs with the ATT&CK framework.	1 = No mapping; 5 = Visually clear mapping with links and comments.
13	Support for formats such as STIX/TAXII	Use of standardized formats for the exchange of CTI data.	1 = Internal or unstructured output only; 5 = Native STIX creation and TAXII client/server support.
14	Support for the largest number of authoritative CTI sources	An extensive selection of community, public and paid sources.	1 = Support for max. 1–2 sources; 5 = >10 sources + the possibility of adding custom ones.
15	Reduced need for manual analysis – saving analysts' time	Automation and prioritization of threats so that analysts deal only with the relevant ones.	1 = High degree of manual work; 5 = Automation, IOC scoring, relevance tagging and suppression.

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5, where 1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

		Criteria for the CTI tool															
		Podpora strategického CTI (správy, analýzy dopadu, trendy útokov)	Podpora operatívneho CTI (TTP, profilovanie skupín)	Podpora taktického CTI (IOC, IP, hash, URL, domény)	Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	Integrácia s 3rd party službami ako VirusTotal, Shodan, DomainTools, URLScan.io	Schopnosť normalizovať CTI dáta na jednotný formát	Možnosť manuálnej analýzy CTI	Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	Deduplikácia hrozieb a informácií	Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu	Podpora formátov ako STIX/TAXII	Podpora najväčšieho počtu autoritatívnych CTI zdrojov	Zníženie potreby manuálnej analýzy – šetrenie času analytikov	**resulting total for the given solution**
	weights	0,07	0,07	0,09	0,08	0,07	0,06	0,07	0,06	0,08	0,06	0,07	0,06	0,05	0,06	0,05	
evaluate solutions	Modul Threat intel (ELK)	0,21	0,21	0,36	0,24	0,21	0,18	0,21	0,12	0,24	0,18	0,28	0,18	0,15	0,18	0,15	3,1
	MISP	0,14	0,14	0,45	0,32	0,35	0,18	0,28	0,3	0,24	0,24	0,21	0,12	0,25	0,24	0,15	3,61
	OpenCTI	0,35	0,35	0,45	0,4	0,35	0,3	0,35	0,3	0,4	0,3	0,35	0,3	0,25	0,3	0,25	5
	InteliMQ	0,07	0,14	0,36	0,4	0,35	0,24	0,35	0,12	0,4	0,24	0,28	0,12	0,25	0,24	0,2	3,76
	YETI	0,21	0,28	0,36	0,32	0,28	0,18	0,28	0,24	0,24	0,24	0,21	0,24	0,2	0,18	0,15	3,61
	Vulmatch	0,14	0,21	0,45	0,32	0,21	0,12	0,28	0,18	0,32	0,24	0,21	0,12	0,15	0,18	0,2	3,33

V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

Funded by the European Union NextGenerationEU | RECOVERY AND RESILIENCE | GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC | UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics | BRAIN:IT

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Creation, editing and deletion of asset records	The ability of the system to record, modify and delete information about individual assets.	1 = Basic recording only, without modifications; 5 = Full CRUD functionality with change control and audit trail.
2	Differentiation of assets by type – hardware, software, virtual, cloud	The ability to differentiate asset types for better organization and management.	1 = Basic asset types only; 5 = Extended classification including cloud, container and virtual assets.
3	Ability to assign tags, categories, owners and status (e.g. active, under maintenance, decommissioned)	Adding metadata for efficient sorting and management of assets.	1 = Fixed categories *only*; 5 = User-definable tags, status and ownership.
4	Recording of the security status of each asset (e.g. OS versions, last update)	Storing information on vulnerabilities, patch level and system updates.	1 = No security attributes; 5 = Automated recording of security status.
5	Mapping of assets to locations, VLANs, IP ranges, racks	The ability to map the physical and logical location of assets in the network.	1 = Location name only; 5 = Support for comprehensive mapping of IPs, racks, VLANs, zones.
6	Relationships between assets (e.g. server – service – application)	The ability to visualize and manage interconnections between infrastructure components.	1 = No relationships; 5 = Detailed dependency mapping with graphical representation.
7	Integration with monitoring, SIEM, ticketing system, EDR, vulnerability scanner, incident recording	The ability to connect to other SOC tools for automation and data sharing.	1 = No integration; 5 = Multi-level bidirectional integration with relevant systems.
8	Filtering, full-text search and export capabilities	Efficient work with data – searching by various parameters and exporting data.	1 = Basic search only; 5 = Advanced full-text search + exports (CSV, JSON).
9	API support (REST, GraphQL) for asset management and integration	The ability to manage and update asset data using an API.	1 = No API; 5 = Documented REST/GraphQL API for all functions.
10	Ability to create custom fields, attributes, plugins (e.g. NetBox/Django)	User flexibility to adapt the system to their own needs.	1 = Fixed structure; 5 = Fully customizable with support for plugins or scripting.
11	Automated discovery of assets in the network (e.g. SNMP, nmap, APIs of other systems)	Automated collection and updating of asset data from the network and other systems.	1 = Manual data collection; 5 = Automated discovery with scheduling and API inputs.
12	Web interface with editing capabilities and clear management	User-friendly GUI for asset management.	1 = Non-intuitive or CLI only; 5 = Responsive and user-friendly interface.
13	Recording of changes to assets (who changed what and when)	Auditability of all changes for forensic and operational transparency.	1 = No logging of changes; 5 = Detailed audit trail with timestamp and user.
14	Ability to track the asset life cycle (deployment – decommissioning)	Management of the individual phases of an asset's lifetime – from commissioning to decommissioning.	1 = No life cycle; 5 = Comprehensive tracking with notifications and statuses.
15	Notifications of status changes, expirations, service intervals	Automatic notifications upon a change of status or when service intervention is needed.	1 = No notifications; 5 = Configurable notifications based on conditions or a calendar.

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5, where 1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

		Kritériá pre nástroj na Asset management														
		Vytvorenie, editácia a mazanie záznamov o aktívach	Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové	Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené)	Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia)	Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	Väzby medzi aktívami (napr. server – služba – aplikácia)	Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov	Možnosť filtrovania, fulltextového vyhľadávania a exportu	Podpora API (REST, GraphQL) na správu aktív a integráciu	Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django)	Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov)	Webové rozhranie s možnosťou úprav a prehľadnou správou	Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil)	Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie)	Upozornenia na zmenu stavu, expirácie, servisné intervaly	**resulting total for the given solution**
	weights	0,1	0,08	0,07	0,07	0,06	0,06	0,09	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,05	
evaluate solutions	LibreNMS	0,3	0,24	0,21	0,21	0,3	0,12	0,36	0,18	0,24	0,18	0,3	0,24	0,18	0,12	0,15	3,33
	pi.Alert	0,3	0,16	0,14	0,14	0,12	0,06	0,18	0,18	0,18	0,12	0,24	0,18	0,12	0,12	0,1	2,34
	NetBox	0,5	0,4	0,35	0,28	0,3	0,3	0,45	0,3	0,3	0,3	0,18	0,3	0,24	0,18	0,2	4,58
	Ralph	0,5	0,32	0,28	0,35	0,18	0,18	0,36	0,24	0,24	0,24	0,18	0,24	0,24	0,24	0,15	3,94
	GLPI	0,5	0,32	0,35	0,28	0,18	0,24	0,45	0,3	0,24	0,3	0,18	0,24	0,3	0,3	0,25	4,43

V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

Funded by the European Union NextGenerationEU | RECOVERY AND RESILIENCE | GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC | UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics | BRAIN:IT

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Creation and editing of records (tickets)	Basic functionality of a ticketing system – creating, editing and deleting tickets.	1 = Manual creation of records only, without further options; 5 = Advanced options including templates, imports and multi-step inputs.
2	Ability to change ticket statuses (e.g. New, In progress, Closed, Postponed)	The ability to switch between various ticket statuses during its life cycle.	1 = Fixed statuses only, with no possibility of modification; 5 = The ability to add custom statuses and define a workflow.
3	Assignment to a specific handler (L1 analyst, L2/L3 escalation)	Assignment of tickets to specific handlers, including escalation by level.	1 = Manual assignment only; 5 = Automated assignment based on rules or rotation.
4	E-mail notifications of status changes, comments, deadlines	Automatic e-mail notifications of status changes, comments, deadlines.	1 = No e-mail support; 5 = Full notification with the ability to modify templates, changes and interval.
5	Adding attachments (logs, evidence, screenshots, tool outputs)	The ability to add attachments such as logs, screenshots and other evidence.	1 = Text fields only; 5 = Support for various attachment formats, drag&drop, size checking.
6	Ability to record times (creation, update, escalation, closure)	Tracking and recording of time data for the entire ticket life cycle.	1 = No time recording; 5 = Precise logging of all time data and export.
7	Setting incident priority and severity	Setting the priority and severity level of a ticket for better planning.	1 = Text notes only; 5 = Definable priority levels, automatic rules.
8	Ability to create templates for recurring incident types	Creation of templates for the quick entry of frequently recurring incidents.	1 = No templates; 5 = The ability to define custom ticket types linked to rules.
9	Ability to add tags for quick search and filtering	Use of tags to facilitate searching and categorization.	1 = No tags; 5 = Multi-level tags, colour coding, filters.
10	Integration with SIEM, SOAR, CTI, incident recording tools, reporting and asset management tools	Integration with other security tools for automation and workflow.	1 = No integration; 5 = Advanced REST integrations, webhooks, ticket linked to events.
11	REST API and Webhook support	Support for REST API and Webhook interfaces for communication with other systems.	1 = Read-only API; 5 = Full CRUD API, webhooks, authentication.
12	Export to PDF, CSV, JSON formats for documentation and reporting	The ability to export tickets for archiving or reporting purposes.	1 = Simple CSV export only; 5 = Regular export, various formats, scheduling.
13	Modern, responsive web interface	Modern and responsive design for convenient use.	1 = Basic UI only; 5 = Responsive, customizable interface with UX optimization.
14	Recording of all changes, accesses and comments in a ticket	Recording of all actions, changes and comments in a ticket.	1 = No logging of changes; 5 = Complete audit trail recording the time, person and action.
15	Possibility of retrospective review and forensic analysis	The ability to retrospectively analyse the course and history of incidents.	1 = No incident history; 5 = Clear history with filtering, export and visualization capabilities.

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5, where
1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

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

V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

Funded by the European Union NextGenerationEU | RECOVERY AND RESILIENCE | GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC | UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics | BRAIN:IT

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Creation and management of cases with tasks and details	The ability to create incidents as cases with tasks, a description and attributes.	1 = Simple record only; 5 = Complex cases with tasks, attributes, links.
2	Adding and tracking observables (IPs, domains, URLs, hash values)	The ability to track IOCs as part of a case.	1 = No support for IOCs; 5 = Full IOC management including status, history and links.
3	Linking of cases based on common indicators	Automatic or manual identification of related incidents.	1 = No support for linking; 5 = Automatic correlation based on IOCs, time, attack types.
4	Categorization of incidents using tags	The ability to categorize incidents using labels/tags.	1 = No tagging; 5 = Advanced tagging with support for filters and statistics.
5	Automated enrichment of incident information from internal and CTI sources	Integration for the enrichment of IOCs and metadata from CTI or other systems.	1 = Manual addition of data; 5 = Automatic enrichment via API/CTI.
6	Ability to modify the system configuration, manage metrics, create case templates and set rules for sharing tasks and observables between organizations	The ability to customize the platform according to the needs of the organization.	1 = No possibility of modification; 5 = High degree of configurability, UI for templates and workflow.
7	Support for multiple user roles – at least analyst and administrator	RBAC support for various roles.	1 = A single role; 5 = Multiple roles with the ability to assign permissions.
8	Ability to create multiple organizations, sharing rules between them	The ability to operate the system for multiple entities simultaneously.	1 = A single organization without isolation; 5 = Multi-tenant environment with sharing control.
9	Connection to SIEM, SOAR, ticketing and reporting systems and other systems via API or plugins	The possibility of bidirectional data exchange.	1 = No integrations; 5 = API + connectors for multiple systems.
10	Export of incidents to CSV, PDF formats, via REST API	Data export for documentation or reporting.	1 = No export; 5 = Support for multiple formats and via API.
11	Logging of analysts' activities during incident handling (audit trail)	Recording of activities for forensic analysis.	1 = No logging; 5 = Detailed logging of every step and user.
12	Simple management of configurations and updates	The ability to manage the platform without the need to modify the code.	1 = Requires manual intervention; 5 = GUI/web interface for management.
13	Ability to add custom fields or case types according to the needs of the organization	The ability to extend the incident schema.	1 = Fixed structures; 5 = Customizable fields and types.
14	Ensuring traceability and retrospective analysis of incidents	Makes it possible to obtain the complete timeline of an incident.	1 = No reconstruction; 5 = Complete audit trail, timeline, links.
15	Sharing of cases between teams and external partners according to permissions	Support for controlled sharing of cases.	1 = No sharing capability; 5 = Detailed access control at case or item level.

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5,
where 1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

		Kritériá pre nástroj pre Evidenciu a správu incidentov															
		Tvorba a správa prípadov (cases) s úlohami a detailmi	Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	Prepojenie medzi prípadmi na základe spoločných indikátorov	Kategorizácia incidentov pomocou tagov	Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	Podpora viacerých používateľských rolí – minimálne analytik a administrátor	Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi	Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy	Export incidentov do formátov CSV, PDF, cez REST API	Logovanie činností analytikov počas riešenia incidentu (audit trail)	Jednoduchá správa konfigurácií a aktualizácií	Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie	Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov	Zdieľanie prípadov medzi tímami a externými partnermi podľa práv	**resulting total for the given solution**
	weights	0,08	0,07	0,07	0,06	0,08	0,07	0,06	0,06	0,08	0,06	0,06	0,05	0,06	0,07	0,07	
available solutions	TheHive	0,4	0,35	0,35	0,3	0,4	0,35	0,3	0,24	0,4	0,3	0,3	0,2	0,3	0,35	0,35	4,89
	RTIR	0,32	0,21	0,14	0,18	0,24	0,21	0,24	0,12	0,24	0,24	0,18	0,15	0,18	0,28	0,21	3,14
																	0
																	0
																	0

V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

Funded by the European Union NextGenerationEU | RECOVERY AND RESILIENCE | GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC | UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics | BRAIN:IT

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Creation of a basic overview of the security and incident status	The ability to create summaries of the security status, incidents and system activity.	1 = Basic summary only, without details; 5 = Comprehensive overview including trends, metrics and statistics.
2	Ability to download a report or send it automatically (e-mail, webhook)	Manual export of reports or their scheduled automatic distribution.	1 = Manual download only; 5 = Automatic distribution via e-mail, webhook or other channels.
3	Ability to select report content – time period, incident types	The ability to filter report content by time, type or source data.	1 = Fixed, non-definable content; 5 = Fully customizable selection of data and filters.
4	Scheduling of regular (e.g. daily, weekly) reports	The ability to set up report generation based on a schedule.	1 = No scheduling; 5 = Advanced scheduling including multiple frequencies and templates.
5	Ability to generate one-off ad hoc reports	Creation of reports outside the regular schedule as needed.	1 = Scheduled or fixed reports only; 5 = Immediate ad hoc generation with parameter selection.
6	Customization of the visual appearance of the report (logo, colours, header)	The ability to adjust the appearance of the report according to the corporate identity.	1 = No customization; 5 = Fully configurable visual elements (colours, logos, header).
7	Support for export to PDF, CSV, JSON	The ability to export reports to various common formats.	1 = Only one format (e.g. PDF); 5 = Support for multiple export formats including structured ones.
8	Integration with tools such as SIEM, Ticketing, Incident recording, Asset management, CTI, ...	The ability to collect data from other systems and create linked reports.	1 = No integration; 5 = Native support for multiple types of integrations.
9	Ability to integrate charts, tables, statistics, heatmaps	Visualization of data directly in reports in various forms.	1 = Text output only; 5 = Interactive and rich visualizations (charts, maps, metrics).
10	Support for various sources: databases, logs, API outputs	The ability to aggregate data from multiple technical and analytical sources.	1 = Fixed data source only; 5 = Dynamic support for multiple types of sources and connectors.
11	Web/GUI interface for creating and managing reports	User-friendly interface for designing, editing and managing reports.	1 = No interface or CLI only; 5 = Modern, responsive and intuitive GUI with template support.
12	Ability to archive generated reports	The ability to retain reports for retrospective analysis and audit.	1 = Reports are not stored; 5 = Archiving with support for versioning and search.
13	Ability to restrict access to reports by role (RBAC)	Access to reports controlled by roles and permissions.	1 = No access control; 5 = Detailed RBAC with the ability to configure it at report level.
14	Encrypted transmission of reports during automatic distribution	Secure transmission of sensitive data via encrypted channels.	1 = Unencrypted sending; 5 = Encryption of all distributions (e.g. TLS, SFTP).

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5, where
1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

		Kritériá pre Reporting nástroj													resulting total for the given solution
		Vytvorenie základného prehľadu stavu bezpečnosti a incidentov	Možnosť stiahnuť report alebo automaticky odoslať (e-mail, webhook)	Možnosť výberu obsahu reportu – časové obdobie, typy incidentov	Plánovanie pravidelných (napr. denných, týždenných) reportov	Možnosť generovania jednorazových ad-hoc reportov	Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie)	Podpora exportu do PDF, CSV, JSON	Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI, ...	Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy	Podpora rôznych zdrojov: databázy, logy, API výstupy	Webové/GUI rozhranie pre tvorbu a správu reportov	Možnosť archivácie vygenerovaných reportov	Možnosť obmedziť prístup k reportom podľa rolí (RBAC)	Šifrované prenosy reportov pri automatickej distribúcii	
	weights	0,1	0,07	0,07	0,07	0,07	0,05	0,08	0,1	0,07	0,06	0,07	0,06	0,06	0,07	
available solutions	Kibana (ELK)	0,5	0,28	0,28	0,28	0,28	0,15	0,32	0,5	0,35	0,24	0,28	0,18	0,24	0,28	4,16
	Grafana	0,3	0,35	0,28	0,35	0,28	0,25	0,4	0,3	0,35	0,24	0,35	0,18	0,24	0,28	4,15
																0
																0
																0

V5 list of defined criteria
KPB2 – Design of the SOCaaS service; type – list; delivery month – M5

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

List of defined criteria

	criterion name	brief description	explanation of point assignment
1	Creation, editing and versioning of records (guides, playbooks, FAQ)	The ability to create, edit and track versions of documents with a change history.	1 = Manual editing only, without change history; 5 = Full-fledged version control with an overview of changes and the ability to restore an older version.
2	Support for structured documents – categories, sections, tags	Organization of KB documents according to structured rules (categories, tags, sections).	1 = No or minimal organization; 5 = Support for multiple levels of structuring and a tag hierarchy.
3	Full-text search with support for filters and tags	Searching the KB with the ability to filter by tags, categories and content.	1 = Basic search by title; 5 = Advanced search with filtering by content, tags and parameters.
4	Linking KB records to specific incidents or attack types	The ability to link knowledge articles to specific attack types and incidents in other tools.	1 = No linking capability; 5 = Dynamic linking of the KB with incidents, IOCs and CTI platforms.
5	Ability to insert images, logs, links and attachments	The ability to enrich documents with multimedia or data content.	1 = Plain text only; 5 = Support for images, logs, files and links in various formats.
6	RBAC support – different access levels for reading, editing, approval	Access control based on user roles.	1 = No support for permissions; 5 = Detailed RBAC for reading, approval and editing with audit trail.
7	Ability to integrate with ticketing, incident management, SIEM	Linking the KB with other systems for more effective use of the content.	1 = No integration; 5 = REST API and direct integration with multiple tools.
8	Export of documents to PDF, HTML or Markdown format	The ability to export documents for offline use or publishing.	1 = No export; 5 = Export to various formats including templating and styles.
9	Simple and intuitive interface for editing and publishing records	User-friendly GUI for knowledge management.	1 = Complicated or technically oriented interface; 5 = Modern WYSIWYG with simple publishing.
10	Preservation of change history with the ability to restore an older version	Tracking and archiving of changes for each document.	1 = No ability to track changes; 5 = Complete version control with records and rollback.
11	Records of who edited a document and when	Audit trail of document changes with information on authors and time.	1 = No activity records; 5 = Detailed activity history for each document.
12	Ability to create approval workflows for new KB articles	Approval processes for the publication of new articles.	1 = Manual approval without rules; 5 = Fully automated workflow with multi-level approval.

Points:
the point assignment logic for all criteria must be set up so that points can be assigned from 1 to 5, where
1 = the lowest level of fulfilment of the criterion and 5 = full fulfilment of the criterion.

Assignment of weights to individual criteria

	criterion name	weight assigned to the criterion
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
	sum of weights:	**1**

Assignment of points to individual criteria

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

Recalculation taking into account the weights of individual criteria

		Criteria for the tool												
		Vytváranie, editácia a verzovanie záznamov (návody, playbooky, FAQ)	Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky (tags)	Fulltextové vyhľadávanie s podporou filtrov a tagov	Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	Možnosť vkladať obrázky, logy, odkazy a prílohy	Podpora RBAC – rôzne úrovne prístupu pre čítanie, editáciu, schvaľovanie	Možnosť integrácie s ticketingom, incident managementom, SIEM	Export dokumentov do PDF, HTML alebo Markdown formátu	Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	Zachovanie histórie zmien s možnosťou obnovy staršej verzie	Záznamy o tom, kto a kedy upravoval dokument	Možnosť tvorby schvaľovacích workflow pre nové KB články	**resulting total for the given solution**
	weights	0,1	0,08	0,08	0,07	0,08	0,08	0,09	0,07	0,08	0,08	0,09	0,1	
available solution	TheHive	0,4	0,24	0,32	0,35	0,32	0,32	0,45	0,21	0,32	0,32	0,36	0,3	3,91
	BookStack	0,5	0,4	0,32	0,21	0,4	0,4	0,27	0,35	0,4	0,4	0,45	0,4	4,5
	Wiki.js	0,5	0,4	0,4	0,21	0,4	0,4	0,27	0,35	0,4	0,4	0,45	0,5	4,68
														0
														0