V10 List of functional and non-functional requirements

PREPARATORY AND INITIATION PHASE									
Sequence ID	REQUIREMENT ID	REQUIREMENT CATEGORY _functional requirement _non-functional requirement technical requirement	REQUIREMENT AREA	REQUIREMENT NAME	DETAILED REQUIREMENT DESCRIPTION	REQUIREMENT OWNER	MODULE NAME (assignment of the requirement to a module)	INCREMENT NUMBER	NOTE
1	FREQ_001	Functional requirement	SOCaaS	Security event monitoring process	Ensure the security event monitoring process – ensures the collection and tracking of logs, metric data and alerts from all integrated systems	UNIZA	SOC general	Inkrement 1	
2	FREQ_002	Functional requirement	SOCaaS	Incident detection process	Ensure the incident detection process – is responsible for identifying anomalies, attack patterns and other threats by means of correlation rules and heuristic mechanisms	UNIZA	SOC general	Inkrement 1	
3	FREQ_003	Functional requirement	SOCaaS	Incident response process	Ensure the incident response process – defines the way in which the team responds to identified incidents. It includes escalation, assignment of responsibility, execution of measures and communication with affected parties	UNIZA	SOC general	Inkrement 1	
4	FREQ_004	Functional requirement	SOCaaS	Incident management process	Ensure the incident management process – includes recording, classifying, prioritizing, documenting and closing incidents	UNIZA	SOC general	Inkrement 1	
5	FREQ_005	Functional requirement	SOCaaS	Threat management process	Ensure the threat management process (Threat Intelligence) – enables systematic work with threat information	UNIZA	SOC general	Inkrement 1	
6	FREQ_006	Functional requirement	SOCaaS	Reporting and visualization process	Ensure the reporting and visualization process – ensures regular output for management, auditors and SOC analysts	UNIZA	SOC general	Inkrement 1	
7	FREQ_007	Functional requirement	SOCaaS	Knowledge management process	Ensure the knowledge management process – ensures the maintenance of a knowledge base of playbooks, documentation and recommended responses	UNIZA	SOC general	Inkrement 1	
8	NREQ_001	Non-functional requirement	SOCaaS	Basic organizational roles	In the context of the SOCaaS design for the INNOSOC project, basic organizational roles have been defined which the system is to be able to support and manage: •**Level 1 (L1) analyst**: The first line of defence, which monitors alerts, performs initial validation of incidents and ensures that they are documented. Typically works with SIEM dashboards, the ticketing system and the knowledge base. •**Level 2 (L2) analyst**: A more experienced analyst who takes over escalated cases from L1. Performs deeper analysis, uses correlation rules and threat intelligence, and collaborates on the development of response measures. Frequently uses the interfaces of SOAR tools and forensic tools. •**Level 3 (L3) specialist / engineer**: An expert in complex incidents, advanced threat hunting, the creation of detection rules and the configuration of tools such as SIEM or EDR. Is also involved in architecture and response automation. •**SOC lead (SOC manager)**: Responsible for the operation and capacity of the SOC team, SLAs, cooperation with customers, reporting and performance control. Coordinates both human and technological resources, including change planning, monitoring the quality of responses and team development. •**Incident handler / incident response lead**: A role responsible for coordinating incident response – task planning, evidence collection, communication with stakeholders and the preparation of final reports. •**Threat Intelligence analyst**: Responsible for working with threats from CTI sources, creating attacker profiles, enriching incidents with IOCs and TTPs, monitoring trends and sharing alerts. •**SOC systems and architecture administrator**: A technical role responsible for the deployment, administration and updating of all components of the SOCaaS architecture, including the ELK Stack, SOAR, asset management and other tools. These roles are not rigid – they may vary depending on the size of the SOC team, the customer structure and SLAs. In a multi-tenant	BRAINIT	SOC general	Inkrement 1	
9	FREQ_008	Functional requirement	SOCaaS	Log centralization	The solution must ensure the collection and centralization of logs from systems, networks, endpoints and applications	UNIZA	SOC general	Inkrement 1	
10	FREQ_009	Functional requirement	SOCaaS	Data normalization and enrichment	The solution must ensure data normalization and enrichment	UNIZA	SOC general	Inkrement 1	
11	FREQ_010	Functional requirement	SOCaaS	Data storage and indexing	The solution must ensure the storage, indexing and retention of data	UNIZA	SOC general	Inkrement 1	
12	FREQ_011	Functional requirement	SOCaaS	Creation of correlation rules	The solution must ensure the creation of correlation rules and alerts	UNIZA	SOC general	Inkrement 1	
13	FREQ_012	Functional requirement	SOCaaS	Visualization of outputs	The solution must ensure the visualization of outputs	UNIZA	SOC general	Inkrement 1	
14	FREQ_013	Functional requirement	SOCaaS	Integration with other tools	The solution must ensure integration with other tools	UNIZA	SOC general	Inkrement 1	
15	FREQ_014	Functional requirement	SOCaaS	SOAR	The solution must ensure SOAR, which will be used to automate response scenarios, process alerts into cases and analyse them	BRAINIT	SOC general	Inkrement 1	
16	FREQ_015	Functional requirement	SOCaaS	Ticketing system and incident management	The solution must ensure a ticketing and incident management system that will provide a workflow for incident handling, escalation, auditing and tracking of resolution	UNIZA	SOC general	Inkrement 1	
17	FREQ_016	Functional requirement	SOCaaS	Knowledge portal	The solution must ensure a knowledge portal that will support response processes by sharing playbooks, internal policies and	UNIZA	SOC general	Inkrement 1	
18	FREQ_017	Functional requirement	SOCaaS	Asset inventory and management	The solution must ensure asset inventory and management. IT asset management is key to mapping the impacts of threats	UNIZA	SOC general	Inkrement 1	
19	FREQ_018	Functional requirement	SOCaaS	Threat Intelligence	The solution must ensure Threat Intelligence. CTI (Cyber Threat Intelligence) processes enable the enrichment of incidents with known threats, TTPs and IOCs	UNIZA	SOC general	Inkrement 1	
20	FREQ_019	Functional requirement	SOCaaS	Vulnerability management	The solution must ensure vulnerability management	UNIZA	SOC general	Inkrement 1	
21	FREQ_020	Functional requirement	SOCaaS	Reporting and retrospective analysis	The solution must ensure reporting and retrospective analysis	UNIZA	SOC general	Inkrement 1	
22	FREQ_021	Functional requirement	SOCaaS	Onboarding of a new customer	The solution must ensure the onboarding of a new customer, during which their infrastructure is integrated into the multi-tenant SOCaaS environment. This includes: •setting up the logging agent •configuration of correlation rules •creation of separate dashboards •setting up incident management for the customer	BRAINIT	SOC general	Inkrement 1	
23	FREQ_022	Functional requirement	SOCaaS	Incident detection and escalation	The solution must ensure incident detection and escalation. Rules for detecting anomalies and known threats must be configured in the environment. After detection: •an alert is generated •the alert is automatically transformed into an incident •Zammad provides a ticket for the L1 team and support for escalation, •the team evaluates the observables and uses enrichment	BRAINIT	SOC general	Inkrement 1	
24	FREQ_023	Functional requirement	SOCaaS	Vulnerability management and inventory	The solution must ensure vulnerability management and inventory. Regular scans are to be linked to the CMDB. •Assets are updated on the basis of detection •incidents tied to vulnerabilities are linked into the management system	BRAINIT	SOC general	Inkrement 1	
25	FREQ_024	Functional requirement	SOCaaS	Proactive threat hunting	The solution must ensure proactive threat hunting (Threat Hunting). Advanced queries will be used, often supplemented with: •CTI data •manual analysis in the case of suspicious entities •results are documented as playbooks	BRAINIT	SOC general	Inkrement 1	
26	FREQ_025	Functional requirement	SOCaaS	Creation of reports and dashboards	The solution must ensure the creation of reports and dashboards. The following will be generated regularly for management and customers: •incident overviews •visualizations from metrics and ticketing •exports for audit and SLA reporting	BRAINIT	SOC general	Inkrement 1	
27	FREQ_026	Functional requirement	SOCaaS	Creation of a knowledge base	The solution must ensure the creation of a knowledge base. Each incident or new type of threat will be documented in the form of: •incident summary + lessons learned •an entry in the knowledge portal •categorization according to MITRE ATT&CK and dates	BRAINIT	SOC general	Inkrement 1	
28	FREQ_027	Functional requirement	SOCaaS	System maintenance and updates	The solution must ensure system maintenance and updates. The operations team must have established: •rules for component updates •a test environment for verifying changes •centralized monitoring of the functionality of all modules	BRAINIT	SOC general	Inkrement 1	
29	FREQ_028	Functional requirement	SOCaaS	Processing of data flows	The solution must ensure data stream processing. The main tasks of data stream processing are: •Receiving logs and events from multiple heterogeneous sources •Validation, normalization and enrichment of data •Assignment of timestamps, identifiers and event categories •Routing of data to appropriate indices for efficient analysis •Filtering out redundant or irrelevant data •Implementation of pipeline rules and processing modules	BRAINIT	SOC general	Inkrement 1	
30	FREQ_029	Functional requirement	SOCaaS	Correlation rules and threat detection	The solution must ensure correlation rules and threat detection. •Alerts on basic IOCs – comparison against a database of known indicators (IP, URL, hash). •Anomalous user behaviour – e.g. multiple failed logins within a short time, login from a new geographical region. •Non-standard network communications – e.g. DNS queries for dynamically generated domains (DGA), deviations in timing and data volume. •Activities with administrative privileges – e.g. adding a user to the "Administrators" group, ACL changes, execution of netsh, powershell. •Event chaining – correlation across multiple logs over time: e.g. login → file transfer → execution of a malicious process. These rules will be managed, where it will be possible to: •track detection alerts, •set threshold values (thresholds), •configure exceptions and ignored values (exceptions), •export and import rules as JSON objects.	UNIZA	SOC general	Inkrement 1	
31	FREQ_030	Functional requirement	SOCaaS	Integration with other components	The solution must ensure integration with other components. Connection to data sources Integration with incident management and SOAR tools Knowledge base and playbooks	UNIZA	SOC general	Inkrement 1	
32	FREQ_031	Functional requirement	SOCaaS	Dashboard design	The solution must ensure dashboard design. To maintain clarity, dashboards within SOCaaS will be divided according to functional layers as follows: 1.Global overviews (SOC Overview) Intended for management and SLA reporting – they include daily/monthly incident statistics, threat types, top 10 IP addresses, countries of origin of attacks, ticket resolution time. 2.Alert monitoring dashboards Focused on operational monitoring – they display new alerts, breakdown by severity (Critical, High, Medium), time trends and correlations across multiple sources. 3.Thematic dashboards They cover specific areas: •EDR activities: recorded files, processes, attempts to execute malicious code. •Vulnerabilities and scans: results from Greenbone or OpenSCAP. •Firewall and network logs: accesses, ports, detected scanning activities. 4.Detailed analytical dashboards – They serve L2 analysts and threat hunting. They contain heatmaps, time slices, distributions by hour, country, ASN, occurrence of IOCs and the like. 5.Ad hoc and incident-specific dashboards – These are created during the investigation of a specific case, where the analyst builds their own visualization based on data from Elasticsearch.	UNIZA	SOC general	Inkrement 1	
33	FREQ_032	Functional requirement	SOCaaS	Dashboard structure	The solution must ensure a dashboard structure whereby dashboards are composed of individual panels that may contain charts, tables, heatmaps, distribution histograms, metrics or maps. Each dashboard within SOCaaS is designed as a composition of these visualizations focused on a specific aspect of monitoring or analysis. System security overview Correlation and incident dashboards Visualization of network traffic and access Monitoring of authentications and user behaviour Integrated overview for the SOC analyst	UNIZA	SOC general	Inkrement 1	
34	FREQ_033	Functional requirement	SOCaaS	Reporting	The solution must ensure reporting. Reporting in SOCaaS will fulfil several basic objectives: •Operational overview – display of the status of systems, the number of incidents, agent activity. •Security reporting – outputs on detected threats, attack types, trends. •Compliance reporting – reports according to regulatory requirements (e.g. GDPR, NIS2). •Management reporting – aggregated statistics and indicators for the organization's leadership. •Customer reporting – individual overviews for the individual clients of the multi-tenant SOCaaS.	UNIZA	SOC general	Inkrement 1	
35	FREQ_034	Functional requirement	SOCaaS	Manual export of reports	The solution must ensure manual export of reports. It will be possible to export reports as: •PDF document – a generated snapshot of the current dashboard. •PNG image – static images of individual visualizations. •CSV files – raw data from tables and data fields. •JSON – for automated analysis and further processing	UNIZA	SOC general	Inkrement 1	
36	FREQ_035	Functional requirement	SOCaaS	Automated export of reports	The solution must ensure automated export of reports. It will be possible to export reports automatically: •Periodic reports – outputs generated and distributed daily, weekly or monthly. •Distribution via e-mail or webhook – reports may be sent automatically to specified addresses or endpoints. •Support for templates and custom filters – the ability to set conditions, time period selections and formats as needed.	UNIZA	SOC general	Inkrement 1	
37	FREQ_036	Functional requirement		Customization of report outputs	The solution must ensure customization of report outputs. It will include: •The ability to select metrics, fields, time ranges •Design personalization – logos, header, colour scheme •Inclusion of explanatory notes, remarks and contextual commentary	UNIZA	SOC general	Inkrement 1	
38	FREQ_037	Functional requirement	Virtualization, containerization, cloud	Support for IaaS functionality	The solution requires full IaaS functionality – management of virtual machines (VMs), disks, networks, images, snapshots and standalone resources. The platform must support the creation and management of various instance types, allow resources to be allocated according to tenants' needs and at the same time offer a robust API for programmatic access. The ability to provide complete IaaS functionality is key to ensuring the flexible and reliable operation of SOC as a service.	UNIZA	Infrastructure	Inkrement 1	
39	NREQ_002	Non-functional requirement	Virtualization, containerization, cloud	Modularity and architecture	The modularity of the architecture fundamentally affects the extensibility and scalability of the solution. A platform that is divided into separate components (e.g. Nova – compute, Neutron – networking, Cinder – block storage) allows modules to be independently deployed, tuned and replaced as needed. It is also advantageous if the platform supports a modern microservices architecture, plugins, containerization and orchestration layers. Greater modularity also reduces the risk of an outage of the entire system in the event of a failure of a single service.	BRAINIT	Infrastructure	Inkrement 1	
40	FREQ_038	Functional requirement	Virtualization, containerization, cloud	Support for orchestration and automation	The solution is to support tools such as Heat (OpenStack orchestration), Terraform (infrastructure as code), Ansible (automation) or Kubernetes Operator for the efficient management and deployment of complex infrastructure scenarios. This capability will enable rapid scaling of services, automated roll-out of environments, repeatable testing and recovery from outages. In a SOC environment, where requirements and network topology change frequently, orchestration is essential for ensuring flexibility, sustainability and operational efficiency.	UNIZA	Infrastructure	Inkrement 1	
41	TREQ_001	Technical requirement	Virtualization, containerization, cloud	Performance and scalability	The solution can use resources efficiently; it is necessary to know the limits in terms of the number of VMs, containers or tenants, and which automatic scaling mechanisms it supports. Latency and overall performance in data processing are also important, especially in real time for the purposes of security event monitoring. The solution must be capable of growing with the number of VMs, tenants and services. There is a need to ensure horizontal and vertical scalability. Under the conditions of the project, we need a platform that can grow together with the number of clients of the SOC service and the volume of data processed.	BRAINIT	Infrastructure	Inkrement 1	
42	TREQ_002	Technical requirement	Virtualization, containerization, cloud	Reliability and stability	The solution must be stable in production operation and include mechanisms for highly available deployment. The possibility of deploying components redundantly (HA – High Availability). In a security centre environment, it is important to minimize downtime and ensure continuous availability of the service. When evaluating cloud services, it is recommended to examine thoroughly past performance, customer satisfaction and the handling of unplanned outages. Likewise, we compare SLAs (Service Level Agreements) where available – although in the case of an open-source platform these are rather internal guarantees, availability of support, etc.	UNIZA	Infrastructure	Inkrement 1	
43	TREQ_003	Technical requirement	Virtualization, containerization, cloud	Compliance with standards and interoperability	The solution must support open standards and common technologies, which is a precondition for its interoperability with other systems. The solution should be compatible with popular hypervisors, network protocols, storage technologies and management interfaces (e.g. the OpenStack API is the de facto standard for open-source clouds). Broad support for standards also facilitates integration and minimizes the risk of proprietary restrictions. If Open Source is used, it is necessary for the platform to be based on proven open-source projects supported by a large community. In our solution, interoperability will enable the future interconnection of multiple cloud environments and the integration of further components.	UNIZA	Infrastructure	Inkrement 1	
44	NREQ_003	Non-functional requirement	Operation	Deployment and administration effort	Simple deployment of the solution, initialization of the platform and its subsequent administration with the necessary know-how are required. For example, some open-source platforms are highly configurable but may be complex to deploy, which requires an experienced team or the use of automation tools (e.g. Ansible scripts, etc.).	UNIZA	Infrastructure	Inkrement 1	
45	NREQ_004	Non-functional requirement	Operation	Support, availability of documentation and community	The solution must be capable of running 24/7 and have defined SLA parameters. For open-source solutions, the size and activity of the community are important – the number of contributors, the frequency of new releases and bug fixes, and the availability of documentation and a knowledge base. A strong community and support from large IT companies are a guarantee of the long-term sustainability of the project.	UNIZA	Infrastructure	Inkrement 1	
46	NREQ_005	Non-functional requirement	Security	Authentication and access control	The platform must include built-in security features necessary to protect infrastructure and data in a SOC environment. These include, for example, support for multi-level authentication and authorization of users, the possibility of data encryption (in storage, in transit), logging and auditing of events, and automated security policies.	UNIZA	Infrastructure	Inkrement 1	
47	NREQ_006	Non-functional requirement	Security	Tenant isolation and data protection	The solution must guarantee strict isolation between individual customers (tenants) – their virtual machines, storage and networks must be separated so as to prevent unauthorized access or data leakage between tenants. Separation of computing resources, network segmentation, access control mechanisms and the like must be ensured. The degree of data isolation between tenants is a fundamental aspect of multi-tenant systems.	UNIZA	Infrastructure	Inkrement 1	
48	NREQ_007	Non-functional requirement	Security	Network/monitoring integration	Connectivity and the possibility of integration with monitoring tools and security surveillance systems – in particular SIEM, IDS/IPS (e.g. Suricata, Snort), as well as metric/logging tools such as Ceilometer, Grafana, Prometheus. It also takes into account the platform's ability to export security events, support for APIs/webhooks and the possibilities of integration with external security elements.	UNIZA	Infrastructure	Inkrement 1	
49	TREQ_004	Technical requirement	Operation	Availability	The solution must ensure high availability in accordance with the required parameters for the operation of KDS: - Operating time 24/7, - RTO, RPO and Uptime for individual services: - RTO < 60 min - RPO 24 h - Uptime 99.5%	BRAINIT	Infrastructure	Inkrement 1	
50	TREQ_005	Technical requirement	Operation	Scaling	The solution must allow modularity of the solution with the possibility of vertical and horizontal scaling of separate blocks according to the requirements of the implemented solution	BRAINIT	Infrastructure	Inkrement 1	
51	TREQ_006	Technical requirement	Operation	Virtualization	The solution must be operable in a virtualized environment	BRAINIT	Infrastructure	Inkrement 1	
52	TREQ_007	Technical requirement	Operation	Containerization	The solution must be able to use containerization where necessary	BRAINIT	Infrastructure	Inkrement 1	
53	TREQ_008	Technical requirement	Operation	Orchestration	The solution must be able to use orchestration tools where necessary	BRAINIT	Infrastructure	Inkrement 1	
54	TREQ_009	Technical requirement	Security	Security logs	The solution must ensure the recording of security logs pursuant to the Act on Information Technologies in Public Administration (ZoITVS) No. 95/2019 Coll., Decree No. 179/2020 Coll., Annex No. 2, paragraph "K. Event logging and monitoring", Category II, point e), and the Cybersecurity Act (ZoKB) No. 69/2018 Coll. and its implementing Decree 362/2018, as amended, Section 15	BRAINIT	Infrastructure	Inkrement 1	
55	NREQ_008	Non-functional requirement	Security	Security testing	Before launch into production operation, security and penetration testing must be carried out pursuant to Decree of the Ministry of Investments, Regional Development and Informatization of the Slovak Republic No. 401/2023 on project management	BRAINIT	SOC general	Inkrement 1	
56	NREQ_009	Non-functional requirement	Legislation	Regulation (EU) 2016/679 of the European Parliament and of the Council	The solution must comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), and with Act No. 18/2018 Coll. on the protection of personal data and on amendments to certain acts, as amended	BRAINIT	SOC general	Inkrement 1	
57	NREQ_010	Non-functional requirement	Legislation	Act No. 69/2018	The solution must comply with Act No. 69/2018 Coll. on cybersecurity and on amendments to certain acts	BRAINIT	SOC general	Inkrement 1	
58	FREQ_039	Functional requirement	SOCaaS	Supported log formats	The ability of the SIEM to receive and process logs in various standardized formats. Supported log formats (syslog, JSON, CSV, CEF, LEEF...)	UNIZA	SIEM	Inkrement 1	
59	FREQ_040	Functional requirement	SOCaaS	Real-time vs. batch processing	The ability to process logs in real time (streaming) or only in batches. Real-time vs. batch processing	UNIZA	SIEM	Inkrement 1	
60	FREQ_041	Functional requirement	SOCaaS	Event correlation	The possibility of linking related events using correlation rules. Event correlation (predefined and custom rules)	UNIZA	SIEM	Inkrement 1	
61	FREQ_042	Functional requirement	SOCaaS	Machine Learning/Behavioural analysis	The ability of the SIEM system to detect anomalies using machine learning. Machine Learning/Behavioural analysis	UNIZA	SIEM	Inkrement 1	
62	FREQ_043	Functional requirement	SOCaaS	Threat Intelligence (CTI) integration	Integration with threat sources (IOC, TTP), automatic data enrichment. Threat Intelligence (CTI) integration	UNIZA	SIEM	Inkrement 1	
63	FREQ_044	Functional requirement	SOCaaS	Anomaly detection	Detection of non-standard behaviour or deviations from expected behaviour. Anomaly detection	UNIZA	SIEM	Inkrement 1	
64	FREQ_045	Functional requirement	SOCaaS	Custom alerting rules and thresholds	The ability to define custom rules and conditions for generating alerts. Custom alerting rules and thresholds	UNIZA	SIEM	Inkrement 1	
65	FREQ_046	Functional requirement	SOCaaS	Automated responses	The possibility of triggering a response (blocking, isolation, notification) automatically. Automated responses (e.g. IP blocking, SOAR integration)	UNIZA	SIEM	Inkrement 1	
66	FREQ_047	Functional requirement	SOCaaS	Data normalization and enrichment	Transformation of various logs into a unified format and their enrichment (e.g. WHOIS, GEOIP). Data normalization and enrichment	UNIZA	SIEM	Inkrement 1	
67	FREQ_048	Functional requirement	SOCaaS	Full-text and fast search	The ability to search logs using operators, tags and filters. Full-text and fast search	UNIZA	SIEM	Inkrement 1	
68	FREQ_049	Functional requirement	SOCaaS	Dashboards and their categorization	Data visualization using charts, filters and widgets. Dashboards (including interactive ones) and their categorization	UNIZA	SIEM	Inkrement 1	
69	FREQ_050	Functional requirement	SOCaaS	Support for MITRE ATT&CK mapping	The ability to map detections to tactics and techniques according to MITRE ATT&CK. Support for MITRE ATT&CK mapping	UNIZA	SIEM	Inkrement 1	
70	FREQ_051	Functional requirement	SOCaaS	Retention	The ability to set log retention policies according to source and importance. Retention (flexible, by log type)	UNIZA	SIEM	Inkrement 1	
71	FREQ_052	Functional requirement	SOCaaS	Encryption	Protection of logs against unauthorized access in transit and at rest. Encryption (both in transit and at rest)	UNIZA	SIEM	Inkrement 1	
72	FREQ_053	Functional requirement	SOCaaS	System health monitoring	Monitoring of system performance, availability and functionality. System health monitoring (healthcheck)	UNIZA	SIEM	Inkrement 1	
73	FREQ_054	Functional requirement	SOCaaS	Receiving alerts and data from various security systems	The ability to receive alerts and data from various security sources (SIEM, EDR, CTI...). Receiving alerts and data from various security systems	BRAINIT	SOAR	Inkrement 1	
74	FREQ_055	Functional requirement	SOCaaS	Data normalization and parsing	Transformation of input data into a standardized format for further processing. Data normalization and parsing	BRAINIT	SOAR	Inkrement 1	
75	FREQ_056	Functional requirement	SOCaaS	Incident categorization and prioritization	The possibility of sorting incidents by severity, type, category and importance. Incident categorization and prioritization	BRAINIT	SOAR	Inkrement 1	
76	FREQ_057	Functional requirement	SOCaaS	Ability to create incident tickets both manually and automatically	Support for both manual and automatic creation of incident tickets from input data. Possibility of both manual and automatic creation of incident tickets	BRAINIT	SOAR	Inkrement 1	
77	FREQ_058	Functional requirement	SOCaaS	Predefined playbooks	Availability of basic response scenarios and automations prepared in advance in the tool. Predefined playbooks	BRAINIT	SOAR	Inkrement 1	
78	FREQ_059	Functional requirement	SOCaaS	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. Possibility of creating custom playbooks without the need for programming	BRAINIT	SOAR	Inkrement 1	
79	FREQ_060	Functional requirement	SOCaaS	Workflow engine with branching, conditions and loops	The possibility of defining complex logic in playbooks using decision points. Workflow engine with branching, conditions and loops	BRAINIT	SOAR	Inkrement 1	
80	FREQ_061	Functional requirement	SOCaaS	Automated responses: IP blocking, host isolation, escalation	The ability to automatically perform responses such as blocking, isolation or notification. Automated responses: IP block, host isolation, escalation	BRAINIT	SOAR	Inkrement 1	
81	FREQ_062	Functional requirement	SOCaaS	Orchestration between systems: SIEM, CTI, ticketing, communication tools, firewall, EDR	Interconnection and data exchange with other systems within the incident response process. Orchestration between systems: SIEM, CTI, ticketing, communication tools, firewall, EDR	BRAINIT	SOAR	Inkrement 1	
82	FREQ_063	Functional requirement	SOCaaS	API-first approach	Accessibility of the tool's functions via API and support for webhooks for notifications and interactions. API-first approach (REST, Webhooks)	BRAINIT	SOAR	Inkrement 1	
83	FREQ_064	Functional requirement	SOCaaS	Support for plug-ins and connectors	The ability to extend the tool's functionality through modules or connectors. Support for plug-ins and connectors	BRAINIT	SOAR	Inkrement 1	
84	FREQ_065	Functional requirement	SOCaaS	Dashboards for incident status and statistics	A clear overview of the system status and ongoing incidents. Dashboards for incident status and statistics	BRAINIT	SOAR	Inkrement 1	
85	FREQ_066	Functional requirement	SOCaaS	RBAC and audit trail	Role-based access control and logging of changes in the system. RBAC and audit trail	BRAINIT	SOAR	Inkrement 1	
86	FREQ_067	Functional requirement	SOCaaS	Playbook debugging & testing	The possibility of testing and debugging playbooks before their live deployment. Playbook debugging & testing	BRAINIT	SOAR	Inkrement 1	
87	FREQ_068	Functional requirement	SOCaaS	SOAR-SIEM synchronization of incident status	Linking of incident status between SIEM and SOAR for up-to-date visibility. SOAR-SIEM incident status synchronization	BRAINIT	SOAR	Inkrement 1	
88	FREQ_069	Functional requirement	SOCaaS	Deployment options: on-prem, cloud, hybrid	The possibility of deploying the solution in various environments, including an on-premises, cloud or hybrid model. Deployment options: on-prem, cloud, hybrid	BRAINIT	EDR	Inkrement 1	
89	FREQ_070	Functional requirement	SOCaaS	Support for various OS	Support for installing and running the agent on various operating systems. Support for various OS (Windows, Linux, macOS)	BRAINIT	EDR	Inkrement 1	
90	FREQ_071	Functional requirement	SOCaaS	Collection of audit data using agents	Collection of audit records on user activities, processes and the system via the agent. Collection of audit data using agents	BRAINIT	EDR	Inkrement 1	
91	FREQ_072	Functional requirement	SOCaaS	File Integrity Monitoring	Real-time detection of file changes for the purposes of forensic analysis and integrity. File Integrity Monitoring (FIM)	BRAINIT	EDR	Inkrement 1	
92	FREQ_073	Functional requirement	SOCaaS	Collection of system metrics, processes and behaviour	Monitoring of system behaviour and metrics such as CPU, memory, services and processes. Collection of system metrics, processes and behaviour	BRAINIT	EDR	Inkrement 1	
93	FREQ_074	Functional requirement	SOCaaS	Collection of information on vulnerabilities and configurations	Obtaining information on vulnerabilities from configuration data and comparison with CVE databases. Collection of information on vulnerabilities and configurations	BRAINIT	EDR	Inkrement 1	
94	FREQ_075	Functional requirement	SOCaaS	Log analysis and correlation with threats	Log analysis with the aim of detecting correlated events and potential threats. Log analysis and correlation with threats	BRAINIT	EDR	Inkrement 1	
95	FREQ_076	Functional requirement	SOCaaS	Malware and intrusion detection	Identification of malicious software and security breach incidents. Malware and intrusion detection	BRAINIT	EDR	Inkrement 1	
96	FREQ_077	Functional requirement	SOCaaS	Heuristic and behavioural analysis	Basing detection on behaviour and heuristics rather than on signatures alone. Heuristic and behavioural analysis	BRAINIT	EDR	Inkrement 1	
97	FREQ_078	Functional requirement	SOCaaS	Support for ML/AI algorithms for threat detection	Use of artificial intelligence algorithms to detect anomalies and threats. Support for ML/AI algorithms for threat detection	BRAINIT	EDR	Inkrement 1	
98	FREQ_079	Functional requirement	SOCaaS	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. Mapping to the MITRE ATT&CK framework	BRAINIT	EDR	Inkrement 1	
99	FREQ_080	Functional requirement	SOCaaS	Automatic responses	Automatic response to incidents, such as endpoint isolation or file quarantine. Automatic responses (e.g. device isolation, file quarantine)	BRAINIT	EDR	Inkrement 1	
100	FREQ_081	Functional requirement	SOCaaS	Low system load of the agent	The agent has a low impact on system performance, which enables deployment at large scale. Low system load of the agent	BRAINIT	EDR	Inkrement 1	
101	FREQ_082	Functional requirement	SOCaaS	Simple central management of agents	A central console for the management, configuration and supervision of all agents. Simple central management of agents	BRAINIT	EDR	Inkrement 1	
102	FREQ_083	Functional requirement	SOCaaS	Regular updates of signatures and modules	Regular updates of threat databases, signatures and detection rules. Regular updates of signatures and modules	BRAINIT	EDR	Inkrement 1	
103	FREQ_084	Functional requirement	SOCaaS	Free version, open-source solution with the possibility of extension	Availability of basic functionality without a licence and the possibility of extension. Free version, open-source solution with the possibility of extension	BRAINIT	Vulnerability scanner	Inkrement 1	
104	FREQ_085	Functional requirement	SOCaaS	Estimated scanning capacity	The ability of the tool to scan large networks efficiently. Estimated scanning capacity (for example, min. 100 IP/24h)	BRAINIT	Vulnerability scanner	Inkrement 1	
105	FREQ_086	Functional requirement	SOCaaS	Vulnerability test updates – community and enterprise feed	Frequency and scope of updates of detection patterns. Vulnerability test updates – community and enterprise feed	BRAINIT	Vulnerability scanner	Inkrement 1	
106	FREQ_087	Functional requirement	SOCaaS	Support for CPE, CVE identifiers	The possibility of identifying vulnerabilities according to standardized identifiers. Support for CPE, CVE identifiers	BRAINIT	Vulnerability scanner	Inkrement 1	
107	FREQ_088	Functional requirement	SOCaaS	Acceptable web interface for managing scans and results	Usability of the GUI for managing scans and results. Acceptable web interface for managing scanning and results	BRAINIT	Vulnerability scanner	Inkrement 1	
108	FREQ_089	Functional requirement	SOCaaS	No need for agents	The possibility of performing scans without the need to install an agent on devices. No need for agents (agentless)	BRAINIT	Vulnerability scanner	Inkrement 1	
109	FREQ_090	Functional requirement	SOCaaS	Support for task and alert scheduling	The possibility of automating repeated tasks and the generation of alerts. Support for task and alert scheduling (optional)	BRAINIT	Vulnerability scanner	Inkrement 1	
110	FREQ_091	Functional requirement	SOCaaS	Remediation tickets – integration or export	The possibility of exporting findings to a ticketing system or to CSV, JSON, PDF. Remediation tickets – integration or export	BRAINIT	Vulnerability scanner	Inkrement 1	
111	FREQ_092	Functional requirement	SOCaaS	Configurable report formats	Flexibility of outputs for further processing. Configurable report formats (e.g. CSV, XML, PDF)	BRAINIT	Vulnerability scanner	Inkrement 1	
112	FREQ_093	Functional requirement	SOCaaS	Deployment options: on-premise, cloud/SaaS, VM, Docker	Flexibility of installation in various environments. Deployment options: on-premise, cloud/SaaS, VM, Docker	BRAINIT	Vulnerability scanner	Inkrement 1	
113	FREQ_094	Functional requirement	SOCaaS	Scanning architecture	Scalability and customization of scan distribution. Scanning architecture (monolithic or master/sensor)	BRAINIT	Vulnerability scanner	Inkrement 1	
114	FREQ_095	Functional requirement	SOCaaS	Integrations with tools such as PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	The possibility of interconnection with other security and IT systems. Integrations with tools such as PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	BRAINIT	Vulnerability scanner	Inkrement 1	
115	FREQ_096	Functional requirement	SOCaaS	Support for CVSS 4.0	Support for the latest version of the CVSS scoring system. Support for CVSS 4.0	BRAINIT	Vulnerability scanner	Inkrement 1	
116	FREQ_097	Functional requirement	SOCaaS	Support for EPSS – vulnerability exploitation prediction	Use of models of the probability of vulnerability exploitation. Support for EPSS – prediction of vulnerability exploitation	BRAINIT	Vulnerability scanner	Inkrement 1	
117	FREQ_098	Functional requirement	SOCaaS	Standards compliance policies	The possibility of assessing vulnerabilities in relation to standards. Standards compliance policies (e.g. GDPR, ISO, CIS, BSI...)	BRAINIT	Vulnerability scanner	Inkrement 1	
118	FREQ_099	Functional requirement	SOCaaS	Support for strategic CTI	Obtaining and analysing information on long-term trends, attack impacts and strategic recommendations. Support for strategic CTI (reports, impact analyses, attack trends)	UNIZA	CTI	Inkrement 1	
119	FREQ_100	Functional requirement	SOCaaS	Support for operational CTI	The ability to map techniques, tactics and procedures (TTP) and to identify attacker groups and their behaviour. Support for operational CTI (TTP, group profiling)	UNIZA	CTI	Inkrement 1	
120	FREQ_101	Functional requirement	SOCaaS	Support for tactical CTI	Working with indicators of compromise (IOC) and their recording, processing and distribution. Support for tactical CTI (IOC, IP, hash, URL, domains)	UNIZA	CTI	Inkrement 1	
121	FREQ_102	Functional requirement	SOCaaS	Automated collection from open-source, community and internal sources	Automatic downloading of data from various sources (e.g. GitHub, feeds, MISP, API systems). Automated collection from open-source, community and internal sources	UNIZA	CTI	Inkrement 1	
122	FREQ_103	Functional requirement	SOCaaS	Support for Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	Ready-made connectors or integrations for well-known CTI sources. Support for Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	UNIZA	CTI	Inkrement 1	
123	FREQ_104	Functional requirement	SOCaaS	Integration with 3rd party services	The ability to enrich IOCs and other artefacts using external services. Integration with 3rd party services such as VirusTotal, Shodan, DomainTools, URLScan.io	UNIZA	CTI	Inkrement 1	
124	FREQ_105	Functional requirement	SOCaaS	Ability to normalize CTI data into a unified format	Consolidation of data from various formats into a structured unified output. The ability to normalize CTI data to a unified format	UNIZA	CTI	Inkrement 1	
125	FREQ_106	Functional requirement	SOCaaS	Possibility of manual CTI analysis	An interface and tools for security analysts to examine data manually. Possibility of manual CTI analysis	UNIZA	CTI	Inkrement 1	
126	FREQ_107	Functional requirement	SOCaaS	Semi-automated or fully automated processing and unification of data	Workflow capability for data processing without the need for manual intervention. Semi-automated or fully automated processing and unification of data	UNIZA	CTI	Inkrement 1	
127	FREQ_108	Functional requirement	SOCaaS	Deduplication of threats and information	Removal of redundant IOCs and indicators. Deduplication of threats and information	UNIZA	CTI	Inkrement 1	
128	FREQ_109	Functional requirement	SOCaaS	Integration with SIEM and firewall for use in automated detections	Forwarding of IOCs and data directly to detection systems (SIEM, IDS, firewall). Integration with SIEM and firewall for use in automated detections	UNIZA	CTI	Inkrement 1	
129	FREQ_110	Functional requirement	SOCaaS	Mapping to MITRE ATT&CK for TTP analysis and team collaboration	Linking incidents, IOCs and TTPs with the ATT&CK framework. Mapping to MITRE ATT&CK for TTP analysis and team collaboration	UNIZA	CTI	Inkrement 1	
130	FREQ_111	Functional requirement	SOCaaS	Support for formats such as STIX/TAXII	Use of standardized formats for the exchange of CTI data. Support for formats such as STIX/TAXII	UNIZA	CTI	Inkrement 1	
131	FREQ_112	Functional requirement	SOCaaS	Support for the largest number of authoritative CTI sources	An extensive selection of community, public and paid sources. Support for the largest number of authoritative CTI sources	UNIZA	CTI	Inkrement 1	
132	FREQ_113	Functional requirement	SOCaaS	Reducing the need for manual analysis	Automation and prioritization of threats so that analysts deal only with the relevant ones. Reducing the need for manual analysis – saving analysts' time	UNIZA	CTI	Inkrement 1	
133	FREQ_114	Functional requirement	SOCaaS	Creation, editing and deletion of asset records	The ability of the system to record, modify and delete information on individual assets. Creation, editing and deletion of asset records	UNIZA	Asset management	Inkrement 1	
134	FREQ_115	Functional requirement	SOCaaS	Distinguishing assets by type	The possibility of distinguishing asset types for better organization and management. Distinguishing assets by type – hardware, software, virtual, cloud	UNIZA	Asset management	Inkrement 1	
135	FREQ_116	Functional requirement	SOCaaS	Possibility of assigning tags, categories, owners and status	Adding metadata for efficient sorting and management of assets. Possibility of assigning tags, categories, owners and status (e.g. active, under maintenance, decommissioned)	UNIZA	Asset management	Inkrement 1	
136	FREQ_117	Functional requirement	SOCaaS	Recording the security status of each asset	Storing information on vulnerabilities, patch level and system updates. Recording the security status of each asset (e.g. OS versions, last update)	UNIZA	Asset management	Inkrement 1	
137	FREQ_118	Functional requirement	SOCaaS	Mapping of assets to locations, VLANs, IP ranges, racks	The ability to map the physical and logical location of assets in the network. Mapping of assets to sites, VLANs, IP ranges, racks	UNIZA	Asset management	Inkrement 1	
138	FREQ_119	Functional requirement	SOCaaS	Relationships between assets	The possibility of visualizing and managing interconnections between infrastructure components. Relationships between assets (e.g. server – service – application)	UNIZA	Asset management	Inkrement 1	
139	FREQ_120	Functional requirement	SOCaaS	Integration with monitoring, SIEM, ticketing system, EDR, vulnerability scanner, incident recording	The possibility of interconnection with other SOC tools for automation and data sharing. Integration with monitoring, SIEM, ticketing system, EDR, vulnerability scanner, incident records	UNIZA	Asset management	Inkrement 1	
140	FREQ_121	Functional requirement	SOCaaS	Filtering, full-text search and export capabilities	Efficient work with data – searching by various parameters and exporting data. Possibility of filtering, full-text search and export	UNIZA	Asset management	Inkrement 1	
141	FREQ_122	Functional requirement	SOCaaS	API support for asset management and integration	The possibility of managing and updating asset data via API. API support (REST, GraphQL) for asset management and integration	UNIZA	Asset management	Inkrement 1	
142	FREQ_123	Functional requirement	SOCaaS	Possibility of creating custom fields, attributes, plugins	User flexibility to customize the system to their own needs. Possibility of creating custom fields, attributes, plugins (e.g. NetBox/Django)	UNIZA	Asset management	Inkrement 1	
143	FREQ_124	Functional requirement	SOCaaS	Automated discovery of assets in the network	Automated collection and updating of asset data from the network and other systems. Automated discovery of assets in the network (e.g. SNMP, nmap, APIs from other systems)	UNIZA	Asset management	Inkrement 1	
144	FREQ_125	Functional requirement	SOCaaS	Web interface with editing capabilities and clear management	User-friendly GUI for asset management. Web interface with editing capability and clear management	UNIZA	Asset management	Inkrement 1	
145	FREQ_126	Functional requirement	SOCaaS	Recording changes to assets	Auditability of all changes for forensic and operational transparency. Recording changes to assets (who changed what and when)	UNIZA	Asset management	Inkrement 1	
146	FREQ_127	Functional requirement	SOCaaS	Possibility of tracking the asset life cycle	Management of the individual phases of an asset's life – from commissioning to decommissioning. Possibility of tracking the asset life cycle (deployment – decommissioning)	UNIZA	Asset management	Inkrement 1	
147	FREQ_128	Functional requirement	SOCaaS	Notifications of status changes, expirations, service intervals	Automatic notifications upon a change of status or the need for service intervention. Alerts on status changes, expirations, service intervals	UNIZA	Asset management	Inkrement 1	
148	FREQ_129	Functional requirement	SOCaaS	Creation and editing of records	Basic functionality of a ticketing system – creating, editing and deleting tickets. Creation and editing of records (tickets)	BRAINIT	Ticketing	Inkrement 1	
149	FREQ_130	Functional requirement	SOCaaS	Possibility of changing ticket statuses	The ability to switch between different ticket statuses during its life cycle. Possibility of changing ticket statuses (e.g. New, In progress, Closed, Postponed)	BRAINIT	Ticketing	Inkrement 1	
150	FREQ_131	Functional requirement	SOCaaS	Assignment to a specific resolver	Assignment of tickets to specific resolvers, including escalation by level. Assignment to a specific resolver (L1 analyst, escalation to L2/L3)	BRAINIT	Ticketing	Inkrement 1	
151	FREQ_132	Functional requirement	SOCaaS	E-mail notifications of status changes, comments, deadlines	Automatic e-mail notifications of status changes, comments, deadlines. E-mail notifications of status changes, comments, deadlines	BRAINIT	Ticketing	Inkrement 1	
152	FREQ_133	Functional requirement	SOCaaS	Adding attachments	The possibility of adding attachments such as logs, screenshots and other evidence. Adding attachments (logs, evidence, screenshots, tool outputs)	BRAINIT	Ticketing	Inkrement 1	
153	FREQ_134	Functional requirement	SOCaaS	Possibility of recording times	Tracking and recording of time data for the entire ticket life cycle. Possibility of recording times (creation, update, escalation, closure)	BRAINIT	Ticketing	Inkrement 1	
154	FREQ_135	Functional requirement	SOCaaS	Setting incident priority and severity	Setting the priority and severity level of a ticket for better planning. Setting the priority and severity of an incident	BRAINIT	Ticketing	Inkrement 1	
155	FREQ_136	Functional requirement	SOCaaS	Ability to create templates for recurring incident types	Creation of templates for quick entry of frequently recurring incidents. Possibility of creating templates for recurring incident types	BRAINIT	Ticketing	Inkrement 1	
156	FREQ_137	Functional requirement	SOCaaS	Ability to add tags for quick search and filtering	Use of tags to facilitate searching and categorization. Possibility of adding tags for quick searching and filtering	BRAINIT	Ticketing	Inkrement 1	
157	FREQ_138	Functional requirement	SOCaaS	Integration with SIEM, SOAR, CTI, incident recording tools, reporting and asset management tools	Integration with other security tools for automation and workflow. Integration with SIEM, SOAR, CTI, incident recording tools, reporting tools and asset management tools	BRAINIT	Ticketing	Inkrement 1	
158	FREQ_139	Functional requirement	SOCaaS	REST API and Webhook support	Support for REST API interfaces and Webhooks for communication with other systems. Support for REST API and Webhooks	BRAINIT	Ticketing	Inkrement 1	
159	FREQ_140	Functional requirement	SOCaaS	Export to PDF, CSV, JSON formats for documentation and reporting	The possibility of exporting tickets for archiving or reporting purposes. Export to PDF, CSV, JSON formats for documentation and reporting	BRAINIT	Ticketing	Inkrement 1	
160	FREQ_141	Functional requirement	SOCaaS	Modern, responsive web interface	Modern and responsive design for convenient use. Modern, responsive web interface	BRAINIT	Ticketing	Inkrement 1	
161	FREQ_142	Functional requirement	SOCaaS	Recording of all changes, accesses and comments in a ticket	Recording of all actions, changes and comments in a ticket. Recording of all changes, accesses and comments in a ticket	BRAINIT	Ticketing	Inkrement 1	
162	FREQ_143	Functional requirement	SOCaaS	Possibility of retrospective review and forensic analysis	The ability to retrospectively analyse the course and history of incidents. Possibility of retrospective review and forensic analysis	BRAINIT	Ticketing	Inkrement 1	
163	FREQ_144	Functional requirement	SOCaaS	Creation and management of cases with tasks and details	The possibility of creating incidents as cases with tasks, a description and attributes. Creation and management of cases with tasks and details	UNIZA	Incident recording and	Inkrement 1	
164	FREQ_145	Functional requirement	SOCaaS	Adding and tracking observables	The ability to track IOCs as part of a case. Adding and tracking observables (IP, domains, URL, hash values)	UNIZA	Incident recording and	Inkrement 1	
165	FREQ_146	Functional requirement	SOCaaS	Linking of cases based on common indicators	Automatic or manual identification of related incidents. Linking between cases based on common indicators	UNIZA	Incident recording and	Inkrement 1	
166	FREQ_147	Functional requirement	SOCaaS	Categorization of incidents using tags	The possibility of categorizing incidents using labels/tags. Categorization of incidents using tags	UNIZA	Incident recording and	Inkrement 1	
167	FREQ_148	Functional requirement	SOCaaS	Automated enrichment of incident information from internal and CTI sources	Integration for enriching IOCs and metadata from CTI or other systems. Automated enrichment of incident information from internal and CTI sources	UNIZA	Incident recording and	Inkrement 1	
168	FREQ_149	Functional requirement	SOCaaS	Ability to modify the system configuration, manage metrics, create case templates and set rules for sharing tasks and observables between organizations	The possibility of customizing the platform according to the organization's needs. The possibility of modifying the system configuration, managing metrics, creating case templates and setting rules for sharing tasks and observables between organizations	UNIZA	Incident recording and	Inkrement 1	
169	FREQ_150	Functional requirement	SOCaaS	Support for multiple user roles	RBAC support for various roles. Support for multiple user roles – at least analyst and administrator	UNIZA	Incident recording and	Inkrement 1	
170	FREQ_151	Functional requirement	SOCaaS	Ability to create multiple organizations, sharing rules between them	The ability to operate the system for multiple entities simultaneously. Possibility of creating multiple organizations and sharing rules between them	UNIZA	Incident recording and	Inkrement 1	
171	FREQ_152	Functional requirement	SOCaaS	Connection to SIEM, SOAR, ticketing and reporting systems and other systems via API or plugins	Possibility of bidirectional data exchange. Connection to SIEM, SOAR, ticketing and reporting systems and other systems via API or plugins	UNIZA	Incident recording and	Inkrement 1	
172	FREQ_153	Functional requirement	SOCaaS	Export of incidents to CSV, PDF formats, via REST API	Data export for documentation or reporting. Export of incidents to CSV, PDF formats, via REST API	UNIZA	Incident recording and	Inkrement 1	
173	FREQ_154	Functional requirement	SOCaaS	Logging of analysts' activities during incident handling (audit trail)	Recording of activities for forensic analysis. Logging of analysts' activities during incident handling (audit trail)	UNIZA	Incident recording and	Inkrement 1	
174	FREQ_155	Functional requirement	SOCaaS	Simple management of configurations and updates	The ability to manage the platform without the need to intervene in the code. Simple management of configurations and updates	UNIZA	Incident recording and	Inkrement 1	
175	FREQ_156	Functional requirement	SOCaaS	Ability to add custom fields or case types according to the needs of the organization	Possibility of extending the incident schema. Possibility of adding custom fields or case types according to the organization's needs	UNIZA	Incident recording and	Inkrement 1	
176	FREQ_157	Functional requirement	SOCaaS	Ensuring traceability and retrospective analysis of incidents	Makes it possible to obtain the complete timeline of an incident. Ensuring retrospective traceability and analysis of incidents	UNIZA	Incident recording and	Inkrement 1	
177	FREQ_158	Functional requirement	SOCaaS	Sharing of cases between teams and external partners according to permissions	Support for controlled sharing of cases. Sharing of cases between teams and external partners according to permissions	UNIZA	Incident recording and	Inkrement 1	
178	FREQ_159	Functional requirement	SOCaaS	Creation of a basic overview of the security and incident status	The possibility of creating summaries of the security status, incidents and system activity. Creation of a basic overview of the security status and incidents	UNIZA	Reporting	Inkrement 1	
179	FREQ_160	Functional requirement	SOCaaS	Possibility of downloading a report or sending it automatically	Exporting reports manually or their scheduled automatic distribution. Possibility of downloading a report or sending it automatically (e-mail, webhook)	UNIZA	Reporting	Inkrement 1	
180	FREQ_161	Functional requirement	SOCaaS	Ability to select report content – time period, incident types	The possibility of filtering report content by time, type or source data. Possibility of selecting report content – time period, incident types	UNIZA	Reporting	Inkrement 1	
181	FREQ_162	Functional requirement	SOCaaS	Scheduling of regular reports	The possibility of setting up report generation based on a schedule. Scheduling of regular (e.g. daily, weekly) reports	UNIZA	Reporting	Inkrement 1	
182	FREQ_163	Functional requirement	SOCaaS	Ability to generate one-off ad hoc reports	Creation of reports outside the regular schedule as needed. Possibility of generating one-off ad-hoc reports	UNIZA	Reporting	Inkrement 1	
183	FREQ_164	Functional requirement	SOCaaS	Customization of the visual appearance of the report	The possibility of adjusting the appearance of the report according to the corporate identity. Customization of the visual appearance of the report (logo, colours, header)	UNIZA	Reporting	Inkrement 1	
184	FREQ_165	Functional requirement	SOCaaS	Support for export to PDF, CSV, JSON	The possibility of exporting reports to various common formats. Support for export to PDF, CSV, JSON	UNIZA	Reporting	Inkrement 1	
185	FREQ_166	Functional requirement	SOCaaS	Integration with tools such as SIEM, Ticketing, Incident records, Asset management, CTI	The possibility of collecting data from other systems and creating linked reports. Integration with tools such as SIEM, Ticketing, Incident records, Asset management, CTI	UNIZA	Reporting	Inkrement 1	
186	FREQ_167	Functional requirement	SOCaaS	Ability to integrate charts, tables, statistics, heatmaps	Visualization of data directly in reports in various forms. Possibility of integrating charts, tables, statistics, heatmaps	UNIZA	Reporting	Inkrement 1	
187	FREQ_168	Functional requirement	SOCaaS	Support for various sources: databases, logs, API outputs	The ability to aggregate data from multiple technical and analytical sources. Support for various sources: databases, logs, API outputs	UNIZA	Reporting	Inkrement 1	
188	FREQ_169	Functional requirement	SOCaaS	Web/GUI interface for creating and managing reports	A user-friendly interface for designing, editing and managing reports. Web/GUI interface for creating and managing reports	UNIZA	Reporting	Inkrement 1	
189	FREQ_170	Functional requirement	SOCaaS	Ability to archive generated reports	The possibility of retaining reports for retrospective analysis and audit. Possibility of archiving generated reports	UNIZA	Reporting	Inkrement 1	
190	FREQ_171	Functional requirement	SOCaaS	Possibility of restricting access to reports by role - RBAC	Access to reports controlled by roles and permissions. Possibility of restricting access to reports by role (RBAC)	UNIZA	Reporting	Inkrement 1	
191	FREQ_172	Functional requirement	SOCaaS	Encrypted transmission of reports during automatic distribution	Secure transfer of sensitive data via encrypted channels. Encrypted transfer of reports during automatic distribution	UNIZA	Reporting	Inkrement 1	
192	FREQ_173	Functional requirement	SOCaaS	Creation, editing and versioning of records	The possibility of creating, editing and tracking versions of documents with a history of changes. Creation, editing and versioning of records (guides, playbooks, FAQ)	UNIZA	SOC knowledge porta	Inkrement 1	
193	FREQ_174	Functional requirement	SOCaaS	Support for structured documents – categories, sections, tags	Organization of KB documents according to structured rules (categories, tags, sections). Support for structured documents – categories, sections, labels (tags)	UNIZA	SOC knowledge porta	Inkrement 1	
194	FREQ_175	Functional requirement	SOCaaS	Full-text search with support for filters and tags	Searching the KB with the possibility of filtering by tags, categories and content. Full-text search with support for filters and tags	UNIZA	SOC knowledge porta	Inkrement 1	
195	FREQ_176	Functional requirement	SOCaaS	Linking KB records to specific incidents or attack types	The possibility of linking knowledge articles with specific attack types and incidents in other tools. Linking KB records with specific incidents or attack types	UNIZA	SOC knowledge porta	Inkrement 1	
196	FREQ_177	Functional requirement	SOCaaS	Ability to insert images, logs, links and attachments	The ability to enrich documents with multimedia or data content. Possibility of inserting images, logs, links and attachments	UNIZA	SOC knowledge porta	Inkrement 1	
197	FREQ_178	Functional requirement	SOCaaS	RBAC support	Access control according to user roles. RBAC support – different access levels for reading, editing, approval	UNIZA	SOC knowledge porta	Inkrement 1	
198	FREQ_179	Functional requirement	SOCaaS	Ability to integrate with ticketing, incident management, SIEM	Linking the KB with other systems for more efficient use of content. Possibility of integration with ticketing, incident management, SIEM	UNIZA	SOC knowledge porta	Inkrement 1	
199	FREQ_180	Functional requirement	SOCaaS	Export of documents to PDF, HTML or Markdown format	The possibility of exporting documents for offline use or publication. Export of documents to PDF, HTML or Markdown format	UNIZA	SOC knowledge porta	Inkrement 1	
200	FREQ_181	Functional requirement	SOCaaS	Simple and intuitive interface for editing and publishing records	User-friendly GUI for knowledge management. Simple and intuitive interface for editing and publishing records	UNIZA	SOC knowledge porta	Inkrement 1	
201	FREQ_182	Functional requirement	SOCaaS	Preservation of change history with the ability to restore an older version	Tracking and archiving of changes for each document. Retention of the change history with the possibility of restoring an older version	UNIZA	SOC knowledge porta	Inkrement 1	
202	FREQ_183	Functional requirement	SOCaaS	Records of who edited a document and when	Audit trail of document changes with information on authors and time. Records of who edited a document and when	UNIZA	SOC knowledge porta	Inkrement 1	
203	FREQ_184	Functional requirement	SOCaaS	Ability to create approval workflows for new KB articles	Approval processes for the publication of new articles. Possibility of creating approval workflows for new KB articles	UNIZA	SOC knowledge porta	Inkrement 1	
204	FREQ_185	Functional requirement	SOCaaS	Anomaly detection accuracy	The solution must ensure evaluation of anomaly detection accuracy (Precision, Recall, F1). How accurately the algorithm detects anomalies regardless of class. Evaluation of overall accuracy using metrics such as Precision, Recall, F1-score or AUC-ROC	UNIZA	AI/ML	Inkrement 1	
205	FREQ_186	Functional requirement	SOCaaS	False alarm rate	The solution must ensure evaluation of the false alarm rate (False Positives/Negatives). How often the algorithm generates false positives/negativesReducing the false alarm rate is key to usability in a SOC. Ideal models have a very low number of FP/FN	UNIZA	AI/ML	Inkrement 1	
206	FREQ_187	Functional requirement	SOCaaS	Support for learning without labels	The solution must ensure support for learning without labels (unsupervised). The ability to learn from input data without the need for annotations. Not all models require labelled data. Unsupervised models are advantageous particularly with large amounts of unlabelled data	UNIZA	AI/ML	Inkrement 1	
207	FREQ_188	Functional requirement	SOCaaS	Computational demands of AI/ML	The solution must be scalable with respect to computational demands (CPU/GPU, memory). Resources required for model training and inference. Varying load on computing resources, including GPU and RAM demands and training duration	UNIZA	AI/ML	Inkrement 1	
208	FREQ_189	Functional requirement	SOCaaS	Inference speed	The solution must ensure evaluation of inference speed (detection time). Response speed in detection. How quickly the model can provide a result on new data. Critical for real-time deployment	UNIZA	AI/ML	Inkrement 1	
209	FREQ_190	Functional requirement	SOCaaS	Robustness to changes in data distribution	The solution must ensure robustness to changes in data distribution (drift, noise). Resilience to noise, changes in data or attacks The model must be resilient to unexpected changes, fluctuations or noise, otherwise it will stop working correctly	UNIZA	AI/ML	Inkrement 1	
210	FREQ_191	Functional requirement	SOCaaS	Ability to work with time-sequential data	The solution must be capable of working with time-sequential data. Suitability for data evolving over time (e.g. logs, network traffic). The ability to capture temporal patterns and anomalies in time series. Architectures such as LSTM and Transformer are an advantage.	UNIZA	AI/ML	Inkrement 1	
211	FREQ_192	Functional requirement	SOCaaS	Flexibility of input data	The solution must be capable of ensuring flexibility of input data (logs, metrics, flow data). How many data types the model can handle without the need to modify the architecture. The model must be able to work with both structured and unstructured inputs – logs, metrics, network flows	UNIZA	AI/ML	Inkrement 1	
212	FREQ_193	Functional requirement	SOCaaS	Adaptive/online learning	The solution must have the capability of adaptive/online learning. Support for updating the model during operation without retrainingThe ability to update the model without the need for complete retraining, e.g. by means of online learning	UNIZA	AI/ML	Inkrement 1	
213	FREQ_194	Functional requirement	SOCaaS	Model explainability	The solution must have an explainable model (interpretability). The ability to explain the detection output to the analyst. The ability to provide the analyst with a comprehensible explanation of why the anomaly was detected	UNIZA	AI/ML	Inkrement 1	
214	TREQ_010	Technical requirement	SOCaaS	Microservices support	The architecture must be based on independently deployable services (microservices), each of which has its own API. Each service must be independently versionable and scalable	UNIZA	SOC general	Inkrement 1	
215	TREQ_011	Technical requirement	Virtualization, containerization, cloud	CI/CD and orchestration	Introduction of a pipeline for the build-test-deploy cycle. Support for GitOps, CI, automated lint, scan, tests, rollout	UNIZA	SOC general	Inkrement 1	
216	TREQ_012	Technical requirement	SOCaaS	OSS compatibility	All components of the system must be built on open-source technologies. Licences must permit modification and further distribution	UNIZA	SOC general	Inkrement 1	
217	TREQ_013	Technical requirement	SOCaaS	Data formats	The system must process JSON, YAML, STIX/TAXII (CTI), Syslog, NetFlow/IPFIX. Log normalization must be ensured	UNIZA	SOC general	Inkrement 1	
218	TREQ_014	Technical requirement	Virtualization, containerization, cloud	Access architecture	Access to the system is to be controlled e.g. via NGINX Ingress or HAProxy. A VPN server (e.g. WireGuard/OpenVPN) is to be used for internal access. TLS 1.3 and forward secrecy supported	UNIZA	SOC general	Inkrement 1	
219	TREQ_015	Technical requirement	Security	Secure API	Every API must support HTTPS (TLS 1.3) and authorization via OAuth2/JWT. The API must be protected against DoS through rate limiting, throttling and access auditing	UNIZA	SOC general	Inkrement 1	
220	TREQ_016	Technical requirement	Security	Auditability	Every configuration change, API interaction, user action and incident must be logged to a centralized audit store	UNIZA	SOC general	Inkrement 1	
221	TREQ_017	Technical requirement	Virtualization, containerization, cloud	Modular solution	The solution must allow plug-ins to be added dynamically without restarting the core. Plugins must be isolated (e.g. sidecar containers or sandboxes)	UNIZA	SOC general	Inkrement 1	
222	TREQ_018	Technical requirement	Virtualization, containerization, cloud	Multi-tenant deployment	Each tenant must have a separate namespace, database, dashboards and logs. It must be possible to configure SLA policies at tenant level	UNIZA	Infrastructure	Inkrement 1	
223	TREQ_019	Technical requirement	Security	TLS/SSL encryption	All communications between components (both internal and external) must be encrypted using TLS 1.3. Support for HSTS, forward secrecy and the possibility of mutual authentication via client certificates	UNIZA	Infrastructure	Inkrement 1	
224	TREQ_020	Technical requirement	Security	Access control (RBAC/ABAC)	The solution must support role-based access control (RBAC) and, optionally, attribute-based access control (ABAC). Authentication may take place via SSO/OAuth2/SAML	UNIZA	Infrastructure	Inkrement 1	
225	TREQ_021	Technical requirement	Security	Secure management of the secret store	Passwords, API keys, certificates and tokens must be stored in a secret store	BRAINIT	Infrastructure	Inkrement 1	
226	TREQ_022	Technical requirement	Security	Secure logging and anomaly detection	The solution must generate security logs that enable the detection of suspicious behaviour (e.g. brute force, unusual API access). Integration with SIEM is required	BRAINIT	Infrastructure	Inkrement 1	
227	TREQ_023	Technical requirement	Virtualization, containerization, cloud	Storage of logs and data	Logs from endpoints, networks, security systems and components must be retained according to the retention period policy (e.g. 12 months). The data storage must support replication and snapshots	BRAINIT	Infrastructure	Inkrement 1	
228	TREQ_024	Technical requirement	Virtualization, containerization, cloud	Backup of configurations and dashboards	The solution must ensure automatic daily backup of configurations, plugins, playbooks and dashboards	BRAINIT	Infrastructure	Inkrement 1	
229	TREQ_025	Technical requirement	Virtualization, containerization, cloud	Archiving and long-term retention	The solution must support the automatic moving of data to the archive according to rules (e.g. compression, encryption, moving after 90 days)	BRAINIT	Infrastructure	Inkrement 1	
230	TREQ_026	Technical requirement	Virtualization, containerization, cloud	Data processing performance	The solution must process at least 10,000 logs per second in real time with a latency of ≤ 5 seconds	BRAINIT	Infrastructure	Inkrement 1	

IMPLEMENTATION PHASE						
Solution design reference from the DNR	IMPLEMENTATION method	USE CASE identification	TEST CASE identification	TEST DATA used	ENVIRONMENT used	VERIFICATION METHOD

V10 List of functional and non-functional requirements

KPB4 – Solution architecture; type – list; month of delivery – M14



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

#	Modules	Increment
MOD_01	Infrastructure	Increment 1
MOD_02	SIEM	Increment 1
MOD_03	SOAR	Increment 1
MOD_04	EDR	Increment 1
MOD_05	Vulnerability scanner	Increment 1
MOD_06	CTI	Increment 1
MOD_07	Asset management	Increment 1
MOD_08	Ticketing	Increment 1
MOD_09	Incident recording and management	Increment 1
MOD_10	Reporting	Increment 1
MOD_11	SOC knowledge portal	Increment 1
MOD_12	SOC general	Increment 1
MOD_13	AI/ML	Increment 1
MOD_14		
MOD_15		

Increment
Increment 1