PROJECT

Multi-tenant cybersecurity operations centre designed
as an open cloud service with machine learning elements

V10 – List of functional and non-functional requirements

KPB4 – Solution architecture

type – list

submission month – M14

Funded by the European Union
NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

1. DOCUMENT history 8
2. PURPOSE OF THE DOCUMENT, ABBREVIATIONS, CONVENTIONS AND DEFINITIONS 8
2.1. Abbreviations and terms used 8
2.2. Conventions for requirement types 9
2.3. Explanation of the columns in the requirements catalogue 9
2.3.1. Preparatory and initiation phase 9
2.3.2. Implementation phase 10
2.3.3. Methodology 10
3. Requirements catalogue 11
3.1. Functional requirements 11
3.1.1. FREQ_001 Security event monitoring process 11
3.1.2. FREQ_002 Incident detection process 11
3.1.3. FREQ_003 Incident response process 11
3.1.4. FREQ_004 Incident management process 11
3.1.5. FREQ_005 Threat management process 11
3.1.6. FREQ_006 Reporting and visualization process 11
3.1.7. FREQ_007 Knowledge management process 11
3.1.8. FREQ_008 Log centralization 12
3.1.9. FREQ_009 Data normalization and enrichment 12
3.1.10. FREQ_010 Data storage and indexing 12
3.1.11. FREQ_011 Creation of correlation rules 12
3.1.12. FREQ_012 Visualization of outputs 12
3.1.13. FREQ_013 Integration with other tools 12
3.1.14. FREQ_014 SOAR 12
3.1.15. FREQ_015 Ticketing system and incident management 12
3.1.16. FREQ_016 Knowledge portal 12
3.1.17. FREQ_017 Asset inventory and management 12
3.1.18. FREQ_018 Threat Intelligence 12
3.1.19. FREQ_019 Vulnerability management 12
3.1.20. FREQ_020 Reporting and retrospective analysis 12
3.1.21. FREQ_021 Onboarding of a new customer 12
3.1.22. FREQ_022 Incident detection and escalation 13
3.1.23. FREQ_023 Vulnerability management and inventory 13
3.1.24. FREQ_024 Proactive threat hunting 13
3.1.25. FREQ_025 Creation of reports and dashboards 13
3.1.26. FREQ_026 Building a knowledge base 13
3.1.27. FREQ_027 System maintenance and updating 13
3.1.28. FREQ_028 Data flow processing 14
3.1.29. FREQ_029 Correlation rules and threat detection 14
3.1.30. FREQ_030 Integration with other components 14
3.1.31. FREQ_031 Dashboard design 14
3.1.32. FREQ_032 Dashboard structure 15
3.1.33. FREQ_033 Reporting 15
3.1.34. FREQ_034 Manual export of reports 15
3.1.35. FREQ_035 Automated export of reports 15
3.1.36. FREQ_036 Customization of report outputs 16
3.1.37. FREQ_037 Support for IaaS functionality 16

3.1.38. FREQ_038 Support for orchestration and automation 16
3.1.39. FREQ_039 Supported log formats 16
3.1.40. FREQ_040 Real-time vs. batch processing 16
3.1.41. FREQ_041 Event correlation 16
3.1.42. FREQ_042 Machine Learning/Behavioural analysis 16
3.1.43. FREQ_043 Threat Intelligence (CTI) integration 16
3.1.44. FREQ_044 Anomaly detection 17
3.1.45. FREQ_045 Custom alerting rules and thresholds 17
3.1.46. FREQ_046 Automated responses 17
3.1.47. FREQ_047 Data normalization and enrichment 17
3.1.48. FREQ_048 Full-text and fast search 17
3.1.49. FREQ_049 Dashboards and their categorization 17
3.1.50. FREQ_050 Support for MITRE ATT&CK mapping 17
3.1.51. FREQ_051 Retention 17
3.1.52. FREQ_052 Encryption 17
3.1.53. FREQ_053 System status monitoring 17
3.1.54. FREQ_054 Receiving alerts and data from various security systems 17
3.1.55. FREQ_055 Data normalization and parsing 17
3.1.56. FREQ_056 Incident categorization and prioritization 18
3.1.57. FREQ_057 Possibility of both manual and automatic creation of incident tickets 18
3.1.58. FREQ_058 Predefined playbooks 18
3.1.59. FREQ_059 Possibility of creating custom playbooks without the need for programming 18
3.1.60. FREQ_060 Workflow engine with branching, conditions and loops 18
3.1.61. FREQ_061 Automated responses: IP blocking, host isolation, escalation 18
3.1.62. FREQ_062 Orchestration across systems: SIEM, CTI, ticketing, communication tools, firewall, EDR 18
3.1.63. FREQ_063 API-first approach 18
3.1.64. FREQ_064 Support for plug-ins and connectors 18
3.1.65. FREQ_065 Dashboards for incident status and statistics 18
3.1.66. FREQ_066 RBAC and audit trail 18
3.1.67. FREQ_067 Playbook debugging & testing 19
3.1.68. FREQ_068 SOAR-SIEM synchronization of incident status 19
3.1.69. FREQ_069 Deployment options: on-prem, cloud, hybrid 19
3.1.70. FREQ_070 Support for various OSs 19
3.1.71. FREQ_071 Collection of audit data using agents 19
3.1.72. FREQ_072 File Integrity Monitoring 19
3.1.73. FREQ_073 Collection of system metrics, processes and behaviour 19
3.1.74. FREQ_074 Collection of information on vulnerabilities and configurations 19
3.1.75. FREQ_075 Log analysis and correlation with threats 19
3.1.76. FREQ_076 Malware and intrusion detection 19
3.1.77. FREQ_077 Heuristic and behavioural analysis 19
3.1.78. FREQ_078 Support for ML/AI algorithms for threat detection 19
3.1.79. FREQ_079 Mapping to the MITRE ATT&CK framework 20
3.1.80. FREQ_080 Automatic responses 20
3.1.81. FREQ_081 Low system load of the agent 20

3.1.82. FREQ_082 Simple central management of agents 20
3.1.83. FREQ_083 Regular updates of signatures and modules 20
3.1.84. FREQ_084 Free version, open-source solution with the possibility of extension 20
3.1.85. FREQ_085 Estimated scanning capacity 20
3.1.86. FREQ_086 Updates of vulnerability tests – community and enterprise feed 20
3.1.87. FREQ_087 Support for CPE and CVE identifiers 20
3.1.88. FREQ_088 Acceptable web interface for managing scans and results 20
3.1.89. FREQ_089 No need for agents 20
3.1.90. FREQ_090 Support for scheduling tasks and alerts 20
3.1.91. FREQ_091 Remediation tickets – integration or export 21
3.1.92. FREQ_092 Configurable report formats 21
3.1.93. FREQ_093 Deployment options: on-premise, cloud/SaaS, VM, Docker 21
3.1.94. FREQ_094 Scanning architecture 21
3.1.95. FREQ_095 Integrations with tools such as PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice 21
3.1.96. FREQ_096 Support for CVSS 4.0 21
3.1.97. FREQ_097 Support for EPSS – prediction of vulnerability exploitation 21
3.1.98. FREQ_098 Standards compliance policies 21
3.1.99. FREQ_099 Support for strategic CTI 21
3.1.100. FREQ_100 Support for operational CTI 21
3.1.101. FREQ_101 Support for tactical CTI 21
3.1.102. FREQ_102 Automated collection from open-source, community and internal sources 21
3.1.103. FREQ_103 Support for Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo 22
3.1.104. FREQ_104 Integration with 3rd party services 22
3.1.105. FREQ_105 Ability to normalize CTI data to a uniform format 22
3.1.106. FREQ_106 Possibility of manual CTI analysis 22
3.1.107. FREQ_107 Semi-automated or fully automated processing and unification of data 22
3.1.108. FREQ_108 Deduplication of threats and information 22
3.1.109. FREQ_109 Integration with SIEM and firewall for use in automated detections 22
3.1.110. FREQ_110 Mapping to MITRE ATT&CK for TTP analysis and team collaboration 22
3.1.111. FREQ_111 Support for formats such as STIX/TAXII 22
3.1.112. FREQ_112 Support for the largest number of authoritative CTI sources 22
3.1.113. FREQ_113 Reducing the need for manual analysis 22
3.1.114. FREQ_114 Creating, editing and deleting asset records 23
3.1.115. FREQ_115 Distinguishing assets by type 23
3.1.116. FREQ_116 Possibility of assigning tags, categories, owners and status 23
3.1.117. FREQ_117 Recording the security status of each asset 23
3.1.118. FREQ_118 Mapping assets to locations, VLANs, IP ranges, racks 23
3.1.119. FREQ_119 Relationships between assets 23

3.1.120. FREQ_120 Integration with monitoring, SIEM, ticketing system, EDR, vulnerability scanner, incident records 23
3.1.121. FREQ_121 Possibility of filtering, full-text search and export 23
3.1.122. FREQ_122 API support for asset management and integration 23
3.1.123. FREQ_123 Possibility of creating custom fields, attributes, plugins 23
3.1.124. FREQ_124 Automated discovery of assets in the network 23
3.1.125. FREQ_125 Web interface with editing capability and clear management 23
3.1.126. FREQ_126 Recording changes to assets 24
3.1.127. FREQ_127 Possibility of tracking the asset life cycle 24
3.1.128. FREQ_128 Notifications of status changes, expirations, service intervals 24
3.1.129. FREQ_129 Creating and editing records 24
3.1.130. FREQ_130 Possibility of changing ticket statuses 24
3.1.131. FREQ_131 Assignment to a specific resolver 24
3.1.132. FREQ_132 E-mail notifications of status changes, comments, deadlines 24
3.1.133. FREQ_133 Adding attachments 24
3.1.134. FREQ_134 Possibility of recording times 24
3.1.135. FREQ_135 Setting incident priority and severity 24
3.1.136. FREQ_136 Possibility of creating templates for recurring types of incidents 24
3.1.137. FREQ_137 Possibility of adding tags for quick search and filtering 24
3.1.138. FREQ_138 Integration with SIEM, SOAR, CTI, incident recording tools, reporting and asset management tools 25
3.1.139. FREQ_139 Support for REST API and Webhooks 25
3.1.140. FREQ_140 Export to PDF, CSV, JSON formats for documentation and reporting 25
3.1.141. FREQ_141 Modern, responsive web interface 25
3.1.142. FREQ_142 Recording of all changes, accesses and comments in the ticket 25
3.1.143. FREQ_143 Retrospective review and forensic analysis capability 25
3.1.144. FREQ_144 Creation and management of cases with tasks and details 25
3.1.145. FREQ_145 Adding and tracking observables 25
3.1.146. FREQ_146 Linking cases on the basis of shared indicators 25
3.1.147. FREQ_147 Categorization of incidents using tags 25
3.1.148. FREQ_148 Automated enrichment of incident information from internal and CTI sources 25
3.1.149. FREQ_149 Ability to modify the system configuration, manage metrics, create case templates and set rules for sharing tasks and observables between organizations 26
3.1.150. FREQ_150 Support for multiple user roles 26
3.1.151. FREQ_151 Ability to create multiple organizations and sharing rules between them 26
3.1.152. FREQ_152 Connection to SIEM, SOAR, ticketing and reporting systems and other systems via API or plugins 26
3.1.153. FREQ_153 Export of incidents to CSV and PDF formats and via REST API 26
3.1.154. FREQ_154 Logging of analysts' activities during incident handling (audit trail) 26

3.1.155. FREQ_155 Simple management of configurations and updates 26
3.1.156. FREQ_156 Ability to add custom fields or case types according to the organization's needs 26
3.1.157. FREQ_157 Ensuring retrospective traceability and analysis of incidents 26
3.1.158. FREQ_158 Sharing of cases between teams and external partners according to permissions 26
3.1.159. FREQ_159 Creation of a basic overview of the security status and incidents 27
3.1.160. FREQ_160 Ability to download a report or send it automatically 27
3.1.161. FREQ_161 Ability to select report content – time period, incident types 27
3.1.162. FREQ_162 Scheduling of regular reports 27
3.1.163. FREQ_163 Ability to generate one-off ad hoc reports 27
3.1.164. FREQ_164 Customization of the visual appearance of reports 27
3.1.165. FREQ_165 Support for export to PDF, CSV, JSON 27
3.1.166. FREQ_166 Integration with tools such as SIEM, ticketing, incident records, asset management, CTI 27
3.1.167. FREQ_167 Ability to integrate charts, tables, statistics, heatmaps 27
3.1.168. FREQ_168 Support for various sources: databases, logs, API outputs. 27
3.1.169. FREQ_169 Web/GUI interface for creating and managing reports 27
3.1.170. FREQ_170 Ability to archive generated reports 27
3.1.171. FREQ_171 Ability to restrict access to reports by role - RBAC 28
3.1.172. FREQ_172 Encrypted transfer of reports during automatic distribution. 28
3.1.173. FREQ_173 Creation, editing and versioning of entries 28
3.1.174. FREQ_174 Support for structured documents – categories, sections, tags 28
3.1.175. FREQ_175 Full-text search with support for filters and tags 28
3.1.176. FREQ_176 Linking KB entries to specific incidents or attack types 28
3.1.177. FREQ_177 Ability to insert images, logs, links and attachments 28
3.1.178. FREQ_178 RBAC support 28
3.1.179. FREQ_179 Ability to integrate with ticketing, incident management, SIEM 28
3.1.180. FREQ_180 Export of documents to PDF, HTML or Markdown format 28
3.1.181. FREQ_181 Simple and intuitive interface for editing and publishing entries 28
3.1.182. FREQ_182 Retention of change history with the option to restore an earlier version 29
3.1.183. FREQ_183 Records of who edited a document and when 29
3.1.184. FREQ_184 Ability to create approval workflows for new KB articles 29
3.1.185. FREQ_185 Anomaly detection accuracy 29
3.1.186. FREQ_186 False alarm rate 29
3.1.187. FREQ_187 Support for learning without labels 29
3.1.188. FREQ_188 Computational demands of AI/ML 29
3.1.189. FREQ_189 Inference speed 29
3.1.190. FREQ_190 Robustness to changes in data distribution 29
3.1.191. FREQ_191 Ability to work with time-sequence data 29
3.1.192. FREQ_192 Flexibility of input data 30

3.1.193. FREQ_193 Adaptive/online learning 30
3.1.194. FREQ_194 Model explainability 30
3.2. Non-functional requirements 30
3.2.1. NREQ_001 Basic organizational roles 30
3.2.2. NREQ_002 Modularity and architecture 31
3.2.3. NREQ_003 Deployment and administration effort 31
3.2.4. NREQ_004 Support, availability of documentation and community 31
3.2.5. NREQ_005 Authentication and access control 31
3.2.6. NREQ_006 Tenant isolation and data protection 31
3.2.7. NREQ_007 Network/monitoring integration 31
3.2.8. NREQ_008 Security testing 31
3.2.9. NREQ_009 Regulation (EU) 2016/679 of the European Parliament and of the Council 32
3.2.10. NREQ_010 Act No. 69/2018 32
3.3. Technical requirements 32
3.3.1. TREQ_001 Performance and scalability 32
3.3.2. TREQ_002 Reliability and stability 32
3.3.3. TREQ_003 Compliance with standards and interoperability 32
3.3.4. TREQ_004 Availability 32
3.3.5. TREQ_005 Scaling 33
3.3.6. TREQ_006 Virtualization 33
3.3.7. TREQ_007 Containerization 33
3.3.8. TREQ_008 Orchestration 33
3.3.9. TREQ_009 Security logs 33
3.3.10. TREQ_010 Microservices support 33
3.3.11. TREQ_011 CI/CD and orchestration 33
3.3.12. TREQ_012 Compatibility with OSS 33
3.3.13. TREQ_013 Data formats 33
3.3.14. TREQ_014 Access architecture 33
3.3.15. TREQ_015 Secure API 34
3.3.16. TREQ_016 Auditability 34
3.3.17. TREQ_017 Modular solution 34
3.3.18. TREQ_018 Multi-tenant deployment 34
3.3.19. TREQ_019 TLS/SSL encryption 34
3.3.20. TREQ_020 Access control (RBAC/ABAC) 34
3.3.21. TREQ_021 Secure management of the secrets store 34
3.3.22. TREQ_022 Secure logging and anomaly detection 34
3.3.23. TREQ_023 Storage of logs and data 34
3.3.24. TREQ_024 Backup of configurations and dashboards 34
3.3.25. TREQ_025 Archiving and long-term retention 34
3.3.26. TREQ_026 Data processing performance 34
Key sources for the requirements catalogue 35
List of sources 35

1. DOCUMENT HISTORY

Version	Date	Changes	Entity
0.1	20.05.2024	Working draft	BRAINIT
0.9	14.06.2024	First version for review	BRAINIT
1.0	22.06.2024	Final version for submission	BRAINIT

2. PURPOSE OF THE DOCUMENT, ABBREVIATIONS, CONVENTIONS AND DEFINITIONS

The Requirements Catalogue document contains a general list and overview of the Functional, Non-functional and Technical requirements in accordance with the convention set out below.

2.1. Abbreviations and terms used

Table 1 List of abbreviations and terms, Own elaboration: (2025)

ABBREVIATION/TERM	DESCRIPTION
IS	Information system
EU	European Union
HW	Hardware
SW	Software
NAC	Network Access Control
NDR	Network detection and response
PAM	Privileged Access Management
SIEM	Security Information and Event Management
ZoKB	Cybersecurity Act
NKIVS	National Concept of Public Administration Informatization
OOÚ	Personal data protection
OVM	Public authority
PaaS	Platform as a service
PILOT	PILOT – Operation of the solution at selected actors in the production environment.
PoC	PoC – Implemented prototype of the solution
PR	Project management
SDL	Security development lifecycle
SLA	Service level agreement
SOAR	Security orchestration, automation and response

2.2. Conventions for requirement types

The main categories of requirements within the requirements catalogue are divided into functional, non-functional (qualitative, legislative, etc.) and technical (of a technological nature). The subgroups within the main categories may be extended according to the needs of the project, for example:

Functional (user) requirements follow the convention:

FREQxxx

F – User requirement

R – Requirement designation

xxx – Requirement number

Non-functional (qualitative, legislative – Non Functional Requirements – NFR) **requirements** follow the convention below:

NREQxxx

N – Non-functional requirement

R – Requirement designation

xxx – Requirement number

Technical (of a technological nature) requirements follow the convention below:

TREQxxx

T – Technological requirement

R – Requirement designation

xxx – Requirement number

2.3. Explanation of the columns in the requirements catalogue

2.3.1. Preparatory and initiation phase

- **SEQUENCE ID** – Sequence number of the requirement
- **REQUIREMENT ID** – Catalogue number of the requirement in accordance with the labelling convention, distinguishing the category
- **REQUIREMENT CATEGORY** – Category of the requirement in accordance with the convention of division into Functional, Non-functional and Technical requirements
- **REQUIREMENT AREA** – Represents membership of a particular area, such as development, service, operation and others
- **REQUIREMENT NAME** – Represents the short name of the requirement
- **DETAILED REQUIREMENT DESCRIPTION** – Represents a more detailed description of the requirement from which the objective of the requirement can be identified
- **REQUIREMENT OWNER** – Represents the process owner, business owner or guarantor of the requirement

- **MODULE NAME** – Represents the assignment of the requirement to the given module
- **INCREMENT NUMBER** – Represents the increment in case the solution is divided into several consecutive project parts
- **NOTE** – A note for cases where it is necessary to capture information that does not fit into the predefined columns and is essential to retain

2.3.2. Implementation phase

Within the requirements catalogue, columns were defined in advance for the purposes of continuing in a possible future implementation phase of the project:

- **Solution design reference from the DNR** – Reference to the chapter or diagram where the given requirement is fulfilled / implemented
- **Implementation method** – A short and concise method of implementation
- **USE CASE identification** – Reference to the specific Use Case within which the requirement is fulfilled
- **TEST CASE identification** – Reference to the specific Test Case within which the fulfilled Use Case can be tested
- **TEST DATA used** – Reference to the test data used
- **ENVIRONMENT used** – Reference to the environment used during testing
- **VERIFICATION METHOD** – A short and concise method of verifying functionality

2.3.3. Methodology

The analysis of requirements in the INNOSOC project will be carried out systematically and in accordance with the principles of the PRINCE2, ITTIL and TOGAF methodologies, which the project partners commonly use to manage similar innovative solutions. This process will be implemented in several phases with the aim of identifying, specifying, validating and documenting all functional and non-functional requirements for the proposed multi-tenant SOC solution provided as a cloud service.

The first step will be the gathering of requirements through workshops, individual interviews and questionnaires with project stakeholders, including technical experts, management and future users of the solution. In this phase, the expectations, needs and problems that the solution must address will be identified, with emphasis on the specifics arising from the NIS2 legislation and the Cybersecurity Act.

Subsequently, the requirements will be systematically analysed and classified according to priority, impact on the project and technical feasibility. A distinction will be made between requirements for the functionality (Functional requirements) of the SOC platform itself (e.g. anomaly detection, reporting, automated response) and non-functional and technical requirements (e.g. availability, performance, security, scalability). For the purposes of modelling and further validation, the requirements will be visualized in later phases of the project using UML and Archimate diagrams in order to verify that they have been correctly understood and are consistent with the architectural design of the solution.

Validation of the requirements will be ensured through review meetings, ongoing revisions and feedback from both users and cybersecurity experts. Such an iterative approach will make it possible to detect in good time any shortcomings or conflicts in the requirements that could jeopardize the quality of the resulting solution.

The results of the requirements analysis will be recorded on an ongoing basis in a centralized requirements management system and will form part of the official project documentation. This procedure will ensure the transparency of the entire process and the traceability of changes, and at the same time provide a basis for quality verification during the development, testing and implementation of the solution.

This document, as well as the Requirements Catalogue, is a living document, and not only until the completion of the Detailed Design of the Solution. It will be subject to continuous validation.

3. REQUIREMENTS CATALOGUE

A detailed overview of the Functional, Non-functional and Technical requirements is provided in the annex “V10-B - Zoznam funkčných a nefunkčných požiadaviek.xlsx”.

3.1. Functional requirements

3.1.1. FREQ_001 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.

3.1.2. FREQ_002 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.

3.1.3. FREQ_003 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.

3.1.4. FREQ_004 Incident management process

Ensure the incident management process – includes recording, classifying, prioritizing, documenting and closing incidents.

3.1.5. FREQ_005 Threat management process

Ensure the threat management process (Threat Intelligence) – enables systematic work with threat information.

3.1.6. FREQ_006 Reporting and visualization process

Ensure the reporting and visualization process – ensures regular output for management, auditors and SOC analysts.

3.1.7. FREQ_007 Knowledge management process

Ensure the knowledge management process – ensures the maintenance of a knowledge base of playbooks, documentation and recommended responses.

3.1.8. FREQ_008 Log centralization

The solution must ensure the collection and centralization of logs from systems, networks, endpoints and applications.

3.1.9. FREQ_009 Data normalization and enrichment

The solution must ensure data normalization and enrichment.

3.1.10. FREQ_010 Data storage and indexing

The solution must ensure the storage, indexing and retention of data.

3.1.11. FREQ_011 Creation of correlation rules

The solution must ensure the creation of correlation rules and alerts.

3.1.12. FREQ_012 Visualization of outputs

The solution must ensure the visualization of outputs.

3.1.13. FREQ_013 Integration with other tools

The solution must ensure integration with other tools.

3.1.14. FREQ_014 SOAR

The solution must ensure SOAR, which will be used to automate response scenarios, process alerts into cases and analyse them.

3.1.15. FREQ_015 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.

3.1.16. FREQ_016 Knowledge portal

The solution must ensure a knowledge portal that will support response processes by sharing playbooks, internal policies and guides.

3.1.17. FREQ_017 Asset inventory and management

The solution must ensure asset inventory and management. IT asset management is key to mapping the impacts of threats.

3.1.18. FREQ_018 Threat Intelligence

The solution must ensure Threat Intelligence. CTI (Cyber Threat Intelligence) processes enable the enrichment of incidents with known threats, TTPs and IOCs.

3.1.19. FREQ_019 Vulnerability management

The solution must ensure vulnerability management.

3.1.20. FREQ_020 Reporting and retrospective analysis

The solution must ensure reporting and retrospective analysis.

3.1.21. FREQ_021 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

3.1.22. FREQ_022 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 supports escalation,
- the team evaluates the observables and uses enrichment

3.1.23. FREQ_023 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

3.1.24. FREQ_024 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

3.1.25. FREQ_025 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

3.1.26. FREQ_026 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

3.1.27. FREQ_027 System maintenance and updates

The solution must ensure system maintenance and updates. The operations team must have established:

- rules for component updates

- an environment for verifying changes
- centralized monitoring of the functionality of all modules

3.1.28. FREQ_028 Data stream processing

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
- Redirection of data to appropriate indices for efficient analysis
- Filtering out redundant or irrelevant data
- Implementation of pipeline rules and processing modules

3.1.29. FREQ_029 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 possible:
  - track detection alerts,
  - set threshold values (thresholds),
  - configure exceptions and ignored values (exceptions),
  - export and import rules as JSON objects.

3.1.30. FREQ_030 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

3.1.31. FREQ_031 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.

3.1.32. FREQ_032 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

3.1.33. FREQ_033 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.

3.1.34. FREQ_034 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.

3.1.35. FREQ_035 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.

3.1.36. FREQ_036 Customization of report outputs

The solution must ensure customization of report outputs. It will include:

- Option to select metrics, fields and time ranges
- Design personalization – logos, header, colour scheme
- Inclusion of explanatory notes, remarks and contextual commentary

3.1.37. FREQ_037 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.

3.1.38. FREQ_038 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.

3.1.39. FREQ_039 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...).

3.1.40. FREQ_040 Real-time vs. batch processing

The ability to process logs in real time (streaming) or only in batches. Real-time vs. batch processing.

3.1.41. FREQ_041 Event correlation

The ability to link related events by means of correlation rules. Event correlation (predefined and custom rules).

3.1.42. FREQ_042 Machine Learning/Behavioural analysis

The ability of the SIEM system to detect anomalies using machine learning. Machine Learning/Behavioural analysis.

3.1.43. FREQ_043 Threat Intelligence (CTI) integration

Integration with threat sources (IOC, TTP), automatic data enrichment. Threat Intelligence (CTI) integration.

3.1.44. FREQ_044 Anomaly detection

Detection of non-standard behaviour or deviations from expected behaviour. Anomaly detection.

3.1.45. FREQ_045 Custom alerting rules and thresholds

The ability to define custom rules and conditions for generating alerts. Custom alerting rules and thresholds.

3.1.46. FREQ_046 Automated responses

The ability to trigger a response (blocking, isolation, notification) automatically. Automated responses (e.g. IP blocking, SOAR integration).

3.1.47. FREQ_047 Data normalization and enrichment

Transformation of various logs into a uniform format and their enrichment (e.g. WHOIS, GEOIP). Data normalization and enrichment.

3.1.48. FREQ_048 Full-text and fast search

The ability to search logs using operators, tags, filters. Full-text and fast search.

3.1.49. FREQ_049 Dashboards and their categorization

Visualization of data using charts, filters and widgets. Dashboards (including interactive ones) and their categorization.

3.1.50. FREQ_050 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.

3.1.51. FREQ_051 Retention

The ability to set log retention policies according to source and importance. Retention (flexible, by log type).

3.1.52. FREQ_052 Encryption

Protection of logs against unauthorized access in transit and at rest. Encryption (both in transit and at rest).

3.1.53. FREQ_053 System status monitoring

Monitoring of system performance, availability and functionality. System status monitoring (healthcheck).

3.1.54. FREQ_054 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.

3.1.55. FREQ_055 Data normalization and parsing

Transformation of input data into a standardized format for further processing. Data normalization and parsing.

3.1.56. FREQ_056 Categorization and prioritization of incidents

The ability to sort incidents by severity, type, category and importance. Categorization and prioritization of incidents.

3.1.57. FREQ_057 Ability to create incident tickets both manually and automatically

Support for both manual and automatic creation of incident tickets from input data. Ability to create incident tickets both manually and automatically.

3.1.58. FREQ_058 Predefined playbooks

Availability of basic response scenarios and automations prepared in advance in the tool. Predefined playbooks.

3.1.59. FREQ_059 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. Ability to create custom playbooks without the need for programming.

3.1.60. FREQ_060 Workflow engine with branching, conditions and loops

The ability to define complex logic in playbooks using decision points. Workflow engine with branching, conditions and loops.

3.1.61. FREQ_061 Automated responses: IP block, host isolation, escalation

The ability to automatically perform responses such as blocking, isolation or notification. Automated responses: IP block, host isolation, escalation.

3.1.62. FREQ_062 Orchestration between systems: SIEM, CTI, ticketing, communication tools, firewall, EDR

Interconnection and exchange of data with other systems within the incident response process. Orchestration between systems: SIEM, CTI, ticketing, communication tools, firewall, EDR.

3.1.63. FREQ_063 API-first approach

Accessibility of the tool's functions via API and support for webhooks for notifications and interactions. API-first approach (REST, Webhooks).

3.1.64. FREQ_064 Support for plug-ins and connectors

The ability to extend the tool's functionality through modules or connectors. Support for plug-ins and connectors.

3.1.65. FREQ_065 Dashboards for incident status and statistics

Clear display of the system status and ongoing incidents. Dashboards for incident status and statistics.

3.1.66. FREQ_066 RBAC and audit trail

Role-based access control and logging of changes in the system. RBAC and audit trail.

3.1.67. FREQ_067 Playbook debugging & testing

The ability to test and debug playbooks before their live deployment. Playbook debugging & testing.

3.1.68. FREQ_068 SOAR-SIEM synchronization of incident status

Linking of incident status between SIEM and SOAR for up-to-date visibility. SOAR-SIEM synchronization of incident status.

3.1.69. FREQ_069 Deployment options: on-prem, cloud, hybrid

The ability to deploy the solution in various environments, including a local, cloud or hybrid model. Deployment options: on-prem, cloud, hybrid.

3.1.70. FREQ_070 Support for various OSs

Support for installing and running the agent on various operating systems. Support for various OSs (Windows, Linux, macOS).

3.1.71. FREQ_071 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.

3.1.72. FREQ_072 File Integrity Monitoring

Real-time detection of file changes for the purposes of forensic analysis and integrity. File Integrity Monitoring (FIM).

3.1.73. FREQ_073 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.

3.1.74. FREQ_074 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.

3.1.75. FREQ_075 Log analysis and correlation with threats

Analysis of logs with the aim of detecting correlated events and potential threats. Log analysis and correlation with threats.

3.1.76. FREQ_076 Detection of malware and intrusions

Identification of malicious software and security breach incidents. Detection of malware and intrusions.

3.1.77. FREQ_077 Heuristic and behavioural analysis

Basing detection on behaviour and heuristics rather than on signatures alone. Heuristic and behavioural analysis.

3.1.78. FREQ_078 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.

3.1.79. FREQ_079 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.

3.1.80. FREQ_080 Automatic responses

Automatic response to incidents, such as endpoint isolation or file quarantine. Automatic responses (e.g. device isolation, file quarantine).

3.1.81. FREQ_081 Low system load of the agent

The agent has a low impact on system performance, which enables large-scale deployment. Low system load of the agent.

3.1.82. FREQ_082 Simple central management of agents

A central console for the management, configuration and supervision of all agents. Simple central management of agents.

3.1.83. FREQ_083 Regular updates of signatures and modules

Regular updates of threat databases, signatures and detection rules. Regular updates of signatures and modules.

3.1.84. FREQ_084 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.

3.1.85. FREQ_085 Estimated scanning capacity

The ability of the tool to scan large networks efficiently. Estimated scanning capacity (for example min. 100 IP/24h).

3.1.86. FREQ_086 Updates of vulnerability tests – community and enterprise feed

Frequency and scope of updates of detection patterns. Updates of vulnerability tests – community and enterprise feed.

3.1.87. FREQ_087 Support for CPE, CVE identifiers

The ability to identify vulnerabilities according to standardized identifiers. Support for CPE, CVE identifiers.

3.1.88. FREQ_088 Acceptable web interface for managing scanning and results

Usability of the GUI for managing scans and results. Acceptable web interface for managing scanning and results.

3.1.89. FREQ_089 No need for agents

The ability to perform scans without the need to install an agent on devices. No need for agents (agentless).

3.1.90. FREQ_090 Support for scheduling tasks and alerts

The ability to automate recurring tasks and the generation of alerts. Support for scheduling tasks and alerts (optional).

3.1.91. FREQ_091 Remediation tickets – integration or export

The ability to export findings to a ticketing system or to CSV, JSON, PDF. Remediation tickets – integration or export.

3.1.92. FREQ_092 Configurable report formats

Flexibility of outputs for further processing. Configurable report formats (e.g. CSV, XML, PDF).

3.1.93. FREQ_093 Deployment options: on-premise, cloud/SaaS, VM, Docker

Flexibility of installation in various environments. Deployment options: on-premise, cloud/SaaS, VM, Docker.

3.1.94. FREQ_094 Scanning architecture

Scalability and customization of scan distribution. Scanning architecture (monolithic or master/sensor).

3.1.95. FREQ_095 Integrations with tools such as PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice

The ability to connect with other security and IT systems. Integrations with tools such as PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice.

3.1.96. FREQ_096 Support for CVSS 4.0

Support for the latest version of the CVSS scoring system. Support for CVSS 4.0.

3.1.97. FREQ_097 Support for EPSS – prediction of vulnerability exploitation

Use of vulnerability exploitation probability models. Support for EPSS – prediction of vulnerability exploitation.

3.1.98. FREQ_098 Policies for compliance with standards

The ability to assess vulnerabilities in relation to standards. Policies for compliance with standards (e.g. GDPR, ISO, CIS, BSI...).

3.1.99. FREQ_099 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).

3.1.100. FREQ_100 Support for operational CTI

The ability to map techniques, tactics and procedures (TTPs), identify attacker groups and their behaviour. Support for operational CTI (TTP, group profiling).

3.1.101. FREQ_101 Support for tactical CTI

Working with indicators of compromise (IOCs) and their recording, processing and distribution. Support for tactical CTI (IOC, IP, hash, URL, domains).

3.1.102. FREQ_102 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.

3.1.103. FREQ_103 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.

3.1.104. FREQ_104 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.

3.1.105. FREQ_105 Ability to normalize CTI data into a uniform format

Consolidation of data from various formats into a structured uniform output. Ability to normalize CTI data into a uniform format.

3.1.106. FREQ_106 Possibility of manual CTI analysis

An interface and tools for security analysts to examine data manually. Possibility of manual CTI analysis.

3.1.107. FREQ_107 Semi-automated or fully automated processing and unification of data

The possibility of workflows for processing data without the need for manual intervention. Semi-automated or fully automated processing and unification of data.

3.1.108. FREQ_108 Deduplication of threats and information

Removal of redundant IOCs and indicators. Deduplication of threats and information.

3.1.109. FREQ_109 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.

3.1.110. FREQ_110 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.

3.1.111. FREQ_111 Support for formats such as STIX/TAXII

Use of standardized formats for the exchange of CTI data. Support for formats such as STIX/TAXII.

3.1.112. FREQ_112 Support for the largest number of authoritative CTI sources

A broad selection of community, public and paid sources. Support for the largest number of authoritative CTI sources.

3.1.113. FREQ_113 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.

3.1.114. FREQ_114 Creation, editing and deletion of asset records

The ability of the system to record, modify and delete information about individual assets. Creation, editing and deletion of asset records.

3.1.115. FREQ_115 Differentiation of assets by type

The ability to distinguish asset types for better organization and management. Differentiation of assets by type – hardware, software, virtual, cloud.

3.1.116. FREQ_116 Ability to assign tags, categories, owners and status

Adding metadata for efficient sorting and management of assets. Ability to assign tags, categories, owners and status (e.g. active, under maintenance, decommissioned).

3.1.117. FREQ_117 Recording of the security status of each asset

Storing information on vulnerabilities, patch level and system updates. Recording of the security status of each asset (e.g. OS version, last update).

3.1.118. FREQ_118 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 locations, VLANs, IP ranges, racks.

3.1.119. FREQ_119 Relationships between assets

The ability to visualize and manage interconnections between infrastructure components. Relationships between assets (e.g. server – service – application).

3.1.120. FREQ_120 Integration with monitoring, SIEM, ticketing system, EDR, vulnerability scanner, incident records

The ability to connect with other SOC tools for automation and data sharing. Integration with monitoring, SIEM, ticketing system, EDR, vulnerability scanner, incident records.

3.1.121. FREQ_121 Filtering, full-text search and export capability

Efficient work with data – searching by various parameters and exporting data. Filtering, full-text search and export capability.

3.1.122. FREQ_122 API support for asset management and integration

The ability to manage and update asset data via API. API support (REST, GraphQL) for asset management and integration.

3.1.123. FREQ_123 Ability to create custom fields, attributes, plugins

User flexibility to adapt the system to their own needs. Ability to create custom fields, attributes, plugins (e.g. NetBox/Django).

3.1.124. FREQ_124 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, API from other systems).

3.1.125. FREQ_125 Web interface with editing capability and clear management

User-friendly GUI for asset management. Web interface with editing capability and clear management.

3.1.126. FREQ_126 Recording of changes to assets

Auditability of all changes for forensic and operational transparency. Recording of changes to assets (who changed what and when).

3.1.127. FREQ_127 Ability to track the asset life cycle

Management of the individual phases of an asset's life – from commissioning to decommissioning. Ability to track the asset life cycle (deployment – decommissioning).

3.1.128. FREQ_128 Alerts on 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.

3.1.129. FREQ_129 Creation and editing of records

Basic functionality of the ticketing system – creating, editing and deleting tickets. Creation and editing of records (tickets).

3.1.130. FREQ_130 Ability to change ticket statuses

The ability to switch between various ticket statuses during its life cycle. Ability to change ticket statuses (e.g. New, In progress, Closed, Postponed).

3.1.131. FREQ_131 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).

3.1.132. FREQ_132 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.

3.1.133. FREQ_133 Adding attachments

The ability to add attachments such as logs, screenshots and other evidence. Adding attachments (logs, evidence, screenshots, tool outputs).

3.1.134. FREQ_134 Ability to record times

Tracking and recording of time data for the entire life cycle of a ticket. Ability to record times (creation, update, escalation, closure).

3.1.135. FREQ_135 Setting incident priority and severity

Setting the priority and severity level of a ticket for better planning. Setting incident priority and severity.

3.1.136. FREQ_136 Ability to create templates for recurring incident types

Creation of templates for the quick entry of frequently recurring incidents. Ability to create templates for recurring incident types.

3.1.137. FREQ_137 Ability to add tags for quick searching and filtering

Use of tags to facilitate searching and categorization. Ability to add tags for quick searching and filtering.

3.1.138. FREQ_138 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 and asset management tools.

3.1.139. FREQ_139 Support for REST API and Webhooks

Support for REST API and Webhook interfaces for communication with other systems. Support for REST API and Webhooks.

3.1.140. FREQ_140 Export to PDF, CSV, JSON formats for documentation and reporting

The ability to export tickets for archiving or reporting purposes. Export to PDF, CSV, JSON formats for documentation and reporting.

3.1.141. FREQ_141 Modern, responsive web interface

Modern and responsive design for convenient use. Modern, responsive web interface.

3.1.142. FREQ_142 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.

3.1.143. FREQ_143 Retrospective review and forensic analysis capability

The ability to retrospectively analyse the course and history of incidents. Retrospective review and forensic analysis capability.

3.1.144. FREQ_144 Creation and management of cases with tasks and details

The ability to create incidents as cases with tasks, a description and attributes. Creation and management of cases with tasks and details.

3.1.145. FREQ_145 Adding and tracking observables

The ability to track IOCs as part of a case. Adding and tracking observables (IP, domains, URL, hash values)

3.1.146. FREQ_146 Linking cases on the basis of shared indicators

Automatic or manual identification of related incidents. Linking cases on the basis of shared indicators.

3.1.147. FREQ_147 Categorization of incidents using tags

The ability to categorize incidents using labels/tags. Categorization of incidents using tags.

3.1.148. FREQ_148 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.

3.1.149. FREQ_149 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 organization's needs. Ability to modify the system configuration, manage metrics, create case templates and set rules for sharing tasks and observables between organizations.

3.1.150. FREQ_150 Support for multiple user roles

RBAC support for various roles. Support for multiple user roles – at least analyst and administrator.

3.1.151. FREQ_151 Ability to create multiple organizations and sharing rules between them

The ability to operate the system for multiple entities simultaneously. Ability to create multiple organizations and sharing rules between them.

3.1.152. FREQ_152 Connection to SIEM, SOAR, ticketing and reporting systems and other systems via API or plugins

The possibility of bidirectional data exchange. Connection to SIEM, SOAR, ticketing and reporting systems and other systems via API or plugins.

3.1.153. FREQ_153 Export of incidents to CSV and PDF formats and via REST API

Export of data for documentation or reporting. Export of incidents to CSV and PDF formats and via REST API.

3.1.154. FREQ_154 Logging of analysts' activities during incident handling (audit trail)

Recording of activities for forensic analysis. Logging of analysts' activities during incident handling (audit trail).

3.1.155. FREQ_155 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.

3.1.156. FREQ_156 Ability to add custom fields or case types according to the organization's needs

The ability to extend the incident schema. Ability to add custom fields or case types according to the organization's needs.

3.1.157. FREQ_157 Ensuring retrospective traceability and analysis of incidents

Makes it possible to obtain the complete timeline of an incident. Ensuring retrospective traceability and analysis of incidents.

3.1.158. FREQ_158 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.

3.1.159. FREQ_159 Creation of a basic overview of the security status and incidents

The ability to create summaries of the security status, incidents and system activity. Creation of a basic overview of the security status and incidents.

3.1.160. FREQ_160 Ability to download a report or send it automatically

Exporting reports manually or their scheduled automatic distribution. Ability to download a report or send it automatically (e-mail, webhook).

3.1.161. FREQ_161 Ability to select report content – time period, incident types

The ability to filter report content by time, type or source data. Ability to select report content – time period, incident types.

3.1.162. FREQ_162 Scheduling of regular reports

The ability to set up report generation based on a schedule. Scheduling of regular (e.g. daily, weekly) reports.

3.1.163. FREQ_163 Ability to generate one-off ad hoc reports

Creation of reports outside the regular schedule as needed. Ability to generate one-off ad hoc reports.

3.1.164. FREQ_164 Customization of the visual appearance of reports

The ability to adjust the appearance of a report according to the corporate identity. Customization of the visual appearance of reports (logo, colours, header).

3.1.165. FREQ_165 Support for export to PDF, CSV, JSON

The ability to export reports to various common formats. Support for export to PDF, CSV, JSON.

3.1.166. FREQ_166 Integration with tools such as SIEM, ticketing, incident records, asset management, CTI

The ability to collect data from other systems and create linked reports. Integration with tools such as SIEM, ticketing, incident records, asset management, CTI, etc.

3.1.167. FREQ_167 Ability to integrate charts, tables, statistics, heatmaps

Visualization of data directly in reports in various forms. Ability to integrate charts, tables, statistics, heatmaps.

3.1.168. FREQ_168 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.

3.1.169. FREQ_169 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.

3.1.170. FREQ_170 Ability to archive generated reports

The ability to retain reports for retrospective analysis and audit. Ability to archive generated reports.

3.1.171. FREQ_171 Ability to restrict access to reports by role – RBAC

Access to reports controlled by roles and permissions. Ability to restrict access to reports by role (RBAC).

3.1.172. FREQ_172 Encrypted transfer of reports during automatic distribution

Secure transfer of sensitive data via encrypted channels. Encrypted transfer of reports during automatic distribution.

3.1.173. FREQ_173 Creation, editing and versioning of entries

The ability to create, edit and track versions of documents with a change history. Creation, editing and versioning of entries (guides, playbooks, FAQ).

3.1.174. FREQ_174 Support for structured documents – categories, sections, tags

Organization of KB documents according to structured rules (categories, tags, sections). Support for structured documents – categories, sections, tags.

3.1.175. FREQ_175 Full-text search with support for filters and tags

Searching in the KB with the ability to filter by tags, categories and content. Full-text search with support for filters and tags.

3.1.176. FREQ_176 Linking KB entries to specific incidents or attack types

The ability to link knowledge articles to specific attack types and incidents in other tools. Linking KB entries to specific incidents or attack types..

3.1.177. FREQ_177 Ability to insert images, logs, links and attachments

The ability to enrich documents with multimedia or data content. Ability to insert images, logs, links and attachments.

3.1.178. FREQ_178 RBAC support

Access control according to user roles. RBAC support – different levels of access for reading, editing, approval.

3.1.179. FREQ_179 Ability to integrate with ticketing, incident management, SIEM

Linking the KB with other systems for more efficient use of content. Ability to integrate with ticketing, incident management, SIEM.

3.1.180. FREQ_180 Export of documents to PDF, HTML or Markdown format

The ability to export documents for offline use or publication. Export of documents to PDF, HTML or Markdown format.

3.1.181. FREQ_181 Simple and intuitive interface for editing and publishing entries

User-friendly GUI for knowledge management. Simple and intuitive interface for editing and publishing entries.

3.1.182. FREQ_182 Retention of change history with the option to restore an earlier version

Tracking and archiving of changes for each document. Retention of change history with the option to restore an earlier version..

3.1.183. FREQ_183 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.

3.1.184. FREQ_184 Ability to create approval workflows for new KB articles

Approval processes for the publication of new articles. Ability to create approval workflows for new KB articles.

3.1.185. FREQ_185 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.

3.1.186. FREQ_186 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.

3.1.187. FREQ_187 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.

3.1.188. FREQ_188 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.

3.1.189. FREQ_189 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.

3.1.190. FREQ_190 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 attacksThe model must be resilient to unexpected changes, fluctuations or noise, otherwise it will stop working correctly.

3.1.191. FREQ_191 Ability to work with time-sequence data

The solution must be capable of working with time-sequence data. Suitability for data that evolve 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.

3.1.192. FREQ_192 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.

3.1.193. FREQ_193 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.

3.1.194. FREQ_194 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.

3.2. Non-functional requirements

3.2.1. NREQ_001 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 SOCaaS architecture environment, the ability

to assign analysts to individual customers, or to delegate them to various types of tasks according to priority and capacity, is also key.

3.2.2. NREQ_002 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.

3.2.3. NREQ_003 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.).

3.2.4. NREQ_004 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.

3.2.5. NREQ_005 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.

3.2.6. NREQ_006 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.

3.2.7. NREQ_007 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.

3.2.8. NREQ_008 Security testing

Before going into production operation, security and penetration testing must be carried out in accordance with Decree No. 401/2023 of the Ministry of Investments, Regional Development and Informatization of the Slovak Republic on project management.

3.2.9. NREQ_009 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.

3.2.10. NREQ_010 Act No. 69/2018

The solution must comply with Act No. 69/2018 Coll. on cybersecurity and on amendments to certain acts.

3.3. Technical requirements

3.3.1. TREQ_001 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.

3.3.2. TREQ_002 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.

3.3.3. TREQ_003 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.

3.3.4. TREQ_004 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%

3.3.5. TREQ_005 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.

3.3.6. TREQ_006 Virtualization

The solution must be operable in a virtualized environment.

3.3.7. TREQ_007 Containerization

The solution must be able to use containerization where necessary.

3.3.8. TREQ_008 Orchestration

The solution must be able to use orchestration tools where necessary.

3.3.9. TREQ_009 Security logs

The solution must ensure the recording of security logs in accordance with ZoITVS No. 95/2019 Coll., Decree No. 179/2020 Coll., Annex No. 2, section "K. Event logging and monitoring", Category II, point e), and ZoKB No. 69/2018 Coll. and its implementing Decree 362/2018, as amended, Section 15.

3.3.10. TREQ_010 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.

3.3.11. TREQ_011 CI/CD and orchestration

Introduction of a pipeline for the build-test-deploy cycle. Support for GitOps, CI, automated lint, scan, tests, rollout.

3.3.12. TREQ_012 Compatibility with OSS

All components of the system must be built on open-source technologies. Licences must permit modification and further distribution.

3.3.13. TREQ_013 Data formats

The system must process JSON, YAML, STIX/TAXII (CTI), Syslog, NetFlow/IPFIX. Log normalization must be ensured.

3.3.14. TREQ_014 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.

3.3.15. TREQ_015 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.

3.3.16. TREQ_016 Auditability

Every configuration change, API interaction, user action and incident must be logged to a centralized audit store.

3.3.17. TREQ_017 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).

3.3.18. TREQ_018 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.

3.3.19. TREQ_019 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.

3.3.20. TREQ_020 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.

3.3.21. TREQ_021 Secure management of the secrets store

Passwords, API keys, certificates and tokens must be stored in a secrets store.

3.3.22. TREQ_022 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.

3.3.23. TREQ_023 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.

3.3.24. TREQ_024 Backup of configurations and dashboards

The solution must ensure automatic daily backup of configurations, plugins, playbooks and dashboards.

3.3.25. TREQ_025 Archiving and long-term retention

The solution must support the automatic movement of data to an archive according to rules (e.g. compression, encryption, transfer after 90 days).

3.3.26. TREQ_026 Data processing performance

The solution must process at least 10,000 logs per second in real time with a latency of < 5 seconds.

KEY SOURCES FOR THE REQUIREMENTS CATALOGUE

Outputs V1 to V9 serve as the main source for gathering and defining the requirements, as they contain all the key information.

LIST OF SOURCES

[1] AXELOS Limited (2023). PRINCE2® 7 Managing Successful Projects, PeopleCert, p. 342, ISBN: 9789925344604.

[2] AXELOS Limited (2021). ITIL® 4 Foundation official AXELOS guidance manual 2022, PeopleCert, p. 209, ISBN: 9789925600007.

[3] The Open Group (2022). The TOGAF® Standard, 10th Edition - ADM Practitioners' Guide, Van Haren Publishing, p. 160, ISBN: 9789401808712.

[4] Wiegers K., Beatty J. , (2013). Software Requirements (Developer Best Practices) 3rd Edition, Microsoft Press, p. 672, ISBN: 9780735679665.

[5] Bonnema G. M. , Broenink J. F. , Veenvliet K. T. , (2015). Systems Design and Engineering 1st Edition, CRC Press, p. 132, ISBN: 9781498751261.

[6] The Open Group (2022). Life The TOGAF® Standard, 10th Edition, The Open Group. Available online: https://www.opengroup.org/togaf/10thedition

[7] Wiegers K., "Požadavky na software," 2008, https://www.daryzivota.sk/pozadavky-na-software, ISBN: 9788025118771.

[8] "Čo je to funkčná požiadavka? - definícia z technológie - vývoj 2024." [Online]. Available: https://sk.theastrologypage.com/functional-requirement. [Accessed: 12-Apr-2024].

[9] "Typy požiadaviek na výber SaaS - Vitajte v IT profesionáloch." [Online]. Available: https://sk.itpedia.nl/2017/01/04/sisp-2-2-soorten-requirements/. [Accessed: 12-Apr-2024].