PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

V10 – Zoznam funkčných a nefunkčných požiadaviek

KPB4 – Architektúra riešenia

typ – zoznam

mesiac odovzdania – M14

Obsah

1. História DOKUMENTU 8
2. ÚČEL DOKUMENTU, SKRATKY, KONVENCIE A DEFINÍCIE 8
2.1. Použité skratky a pojmy 8
2.2. Konvencie pre typy požiadaviek 9
2.3. Vysvetlenie stĺpcov v katalógu požiadaviek 9
2.3.1. Prípravná a iniciačná fáza 9
2.3.2. Realizačná fáza 10
2.3.3. Metodika 10
3. Katalóg požiadaviek 11
3.1. Funkčné požiadavky 11
3.1.1. FREQ_001 Proces monitorovania bezpečnostných udalostí 11
3.1.2. FREQ_002 Proces detekcie incidentov 11
3.1.3. FREQ_003 Proces reakcie na incodenty 11
3.1.4. FREQ_004 Proces správy incidentov 11
3.1.5. FREQ_005 Proces správy hrozieb 11
3.1.6. FREQ_006 Proces reporting a vizualizácia 11
3.1.7. FREQ_007 Proces správy poznatkov 11
3.1.8. FREQ_008 Centralizácia logov 12
3.1.9. FREQ_009 Normalizácia a obohacovanie údajov 12
3.1.10. FREQ_010 Ukladanie a indexovanie údajov 12
3.1.11. FREQ_011 Tvorba korelačných pravidiel 12
3.1.12. FREQ_012 Vizualizácia výstupov 12
3.1.13. FREQ_013 Integrácia s ďalšími nástrojmi 12
3.1.14. FREQ_014 SOAR 12
3.1.15. FREQ_015 Ticketovací systém a incident manažment 12
3.1.16. FREQ_016 Znalostný portál 12
3.1.17. FREQ_017 Inventarizácia a správa aktív 12
3.1.18. FREQ_018 Threat Intelligence 12
3.1.19. FREQ_019 Správa zraniteľností 12
3.1.20. FREQ_020 Reporting a spätná analýza 12
3.1.21. FREQ_021 Onboarding nového zákazníka 12
3.1.22. FREQ_022 Detekcia a eskalácia incidentu 13
3.1.23. FREQ_023 Správa zraniteľností a inventarizácia 13
3.1.24. FREQ_024 Proaktívne vyhľadávanie hrozieb 13
3.1.25. FREQ_025 Tvorba reportov a dashboardov 13
3.1.26. FREQ_026 Tvorba znalostnej bázy 13
3.1.27. FREQ_027 Údržba a aktualizácia systému 13
3.1.28. FREQ_028 Spracovanie dátových tokov 14
3.1.29. FREQ_029 Korelačné pravidlá a detekcia hrozieb 14
3.1.30. FREQ_030 Integrácia s ostatnými komponentmi 14
3.1.31. FREQ_031 Návrh dashboardov 14
3.1.32. FREQ_032 Štruktúra dashboardov 15
3.1.33. FREQ_033 Reporting 15
3.1.34. FREQ_034 Manuálny export reportov 15
3.1.35. FREQ_035 Automatizovaný export reportov 15
3.1.36. FREQ_036 Customizácia výstupov reportov 15
3.1.37. FREQ_037 Podpora IaaS funkcionality 16
3.1.38. FREQ_038 Podpora orchestrácie a automatizácie 16

3.1.39. FREQ_039 Podporované formáty logov 16
3.1.40. FREQ_040 Reálny čas vs. dávkové spracovanie 16
3.1.41. FREQ_041 Korelácia udalostí 16
3.1.42. FREQ_042 Machine Learning/Behaviorálna analýza 16
3.1.43. FREQ_043 Threat Intelligence (CTI) integrácia 16
3.1.44. FREQ_044 Detekcia anomálií 16
3.1.45. FREQ_045 Vlastné alertovacie pravidlá a prahy 16
3.1.46. FREQ_046 Automatizované reakcie 16
3.1.47. FREQ_047 Normalizácia a obohacovanie dát 17
3.1.48. FREQ_048 Fulltextové a rýchle vyhľadávanie 17
3.1.49. FREQ_049 Dashboardy a ich kategorizácia 17
3.1.50. FREQ_050 Podpora pre MITRE ATT&CK mapovanie 17
3.1.51. FREQ_051 Retencia 17
3.1.52. FREQ_052 Šifrovanie 17
3.1.53. FREQ_053 Monitoring stavu systému 17
3.1.54. FREQ_054 Prijímanie upozornení a dát z rôznych bezpečnostných systémov 17
3.1.55. FREQ_055 Normalizácia a parsovanie dát 17
3.1.56. FREQ_056 Kategorizácia a prioritizácia incidentov 17
3.1.57. FREQ_057 Možnosť manuálneho aj automatického vytvárania incident ticketov 17
3.1.58. FREQ_058 Preddefinované playbooky 17
3.1.59. FREQ_059 Možnosť tvorby vlastných playbookov bez potreby programovania 18
3.1.60. FREQ_060 Workflow engine s vetvením, podmienkami a slučkami 18
3.1.61. FREQ_061 Automatizované reakcie: blok IP, izolácia hostu, eskalácia 18
3.1.62. FREQ_062 Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR 18
3.1.63. FREQ_063 API-first prístup 18
3.1.64. FREQ_064 Podpora pre plug-iny a konektory 18
3.1.65. FREQ_065 Dashboardy pre stav a štatistiky incidentov 18
3.1.66. FREQ_066 RBAC a audit trail 18
3.1.67. FREQ_067 Playbook debugging & testing 18
3.1.68. FREQ_068 SOAR-SIEM synchronizácia stavu incidentov 18
3.1.69. FREQ_069 Možnosti nasadenia: on-prem, cloud, hybrid 18
3.1.70. FREQ_070 Podpora pre rôzne OS 18
3.1.71. FREQ_071 Zber auditovacích dát pomocou agentov 19
3.1.72. FREQ_072 File Integrity Monitoring 19
3.1.73. FREQ_073 Zber systémových metrík, procesov a správania 19
3.1.74. FREQ_074 Zber informácií o zraniteľnostiach a konfiguráciách 19
3.1.75. FREQ_075 Analýza logov a korelácia s hrozbami 19
3.1.76. FREQ_076 Detekcia malvéru a narušení 19
3.1.77. FREQ_077 Heuristická a behaviorálna analýza 19
3.1.78. FREQ_078 Podpora ML/AI algoritmov na detekciu hrozieb 19
3.1.79. FREQ_079 Mapovanie na MITRE ATT&CK framework 19
3.1.80. FREQ_080 Automatické reakcie 19
3.1.81. FREQ_081 Nízka systémová záťaž agenta 19
3.1.82. FREQ_082 Jednoduché centrálne riadenie agentov 19
3.1.83. FREQ_083 Pravidelné aktualizácie signatúr a modulov 20

3.1.84. FREQ_084 Bezplatná verzia, open-source riešenie s možnosťou rozšírenia 20
3.1.85. FREQ_085 Odhadovaná kapacita skenovania 20
3.1.86. FREQ_086 Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed 20
3.1.87. FREQ_087 Podpora CPE, CVE identifikátorov 20
3.1.88. FREQ_088 Prijateľné webové rozhranie na správu skenovania a výsledkov 20
3.1.89. FREQ_089 Bez potreby agentov 20
3.1.90. FREQ_090 Podpora plánovania úloh a alertov 20
3.1.91. FREQ_091 Tikety na nápravu – integrácia alebo export 20
3.1.92. FREQ_092 Konfigurovateľné formáty reportov 20
3.1.93. FREQ_093 Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker 20
3.1.94. FREQ_094 Architektúra skenovania 21
3.1.95. FREQ_095 Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice 21
3.1.96. FREQ_096 Podpora pre CVSS 4.0 21
3.1.97. FREQ_097 Podpora pre EPSS – predikcia zneužitia zraniteľností 21
3.1.98. FREQ_098 Politiky súladu s normami 21
3.1.99. FREQ_099 Podpora strategického CTI 21
3.1.100. FREQ_100 Podpora operatívneho CTI 21
3.1.101. FREQ_101 Podpora taktického CTI 21
3.1.102. FREQ_102 Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov 21
3.1.103. FREQ_103 Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo 21
3.1.104. FREQ_104 Integrácia s 3rd party službami 21
3.1.105. FREQ_105 Schopnosť normalizovať CTI dáta na jednotný formát 22
3.1.106. FREQ_106 Možnosť manuálnej analýzy CTI 22
3.1.107. FREQ_107 Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov 22
3.1.108. FREQ_108 Deduplikácia hrozieb a informácií 22
3.1.109. FREQ_109 Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách 22
3.1.110. FREQ_110 Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu 22
3.1.111. FREQ_111 Podpora formátov ako STIX/TAXII 22
3.1.112. FREQ_112 Podpora najväčšieho počtu autoritatívnych CTI zdrojov 22
3.1.113. FREQ_113 Zníženie potreby manuálnej analýzy 22
3.1.114. FREQ_114 Vytvorenie, editácia a mazanie záznamov o aktívach 22
3.1.115. FREQ_115 Rozlíšenie aktív podľa typu 22
3.1.116. FREQ_116 Možnosť priradenia tagov, kategórií, vlastníkov a stavu 22
3.1.117. FREQ_117 Evidencia bezpečnostného stavu každého aktíva 23
3.1.118. FREQ_118 Mapovanie aktív na lokality, VLANy, IP rozsahy, racky 23
3.1.119. FREQ_119 Väzby medzi aktívami 23
3.1.120. FREQ_120 Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov 23
3.1.121. FREQ_121 Možnosť filtrovania, fulltextového vyhľadávania a exportu 23
3.1.122. FREQ_122 Podpora API na správu aktív a integráciu 23

3.1.123. FREQ_123 Možnosť tvorby vlastných polí, atribútov, pluginov 23
3.1.124. FREQ_124 Automatizovaný discovery assetov v sieti 23
3.1.125. FREQ_125 Webové rozhranie s možnosťou úprav a prehľadnou správou 23
3.1.126. FREQ_126 Zaznamenávanie zmien na aktívach 23
3.1.127. FREQ_127 Možnosť sledovať životný cyklus assetov 23
3.1.128. FREQ_128 Upozornenia na zmenu stavu, expirácie, servisné intervaly 24
3.1.129. FREQ_129 Vytvorenie a editácia záznamov 24
3.1.130. FREQ_130 Možnosť meniť stavy ticketu 24
3.1.131. FREQ_131 Priradenie na konkrétneho riešiteľa 24
3.1.132. FREQ_132 Emailové notifikácie o zmenách stavu, komentároch, deadline 24
3.1.133. FREQ_133 Pridávanie príloh 24
3.1.134. FREQ_134 Možnosť evidovať časy 24
3.1.135. FREQ_135 Nastavenie priority a závažnosti incidentu 24
3.1.136. FREQ_136 Možnosť vytvárať šablóny pre opakujúce sa typy incidentov 24
3.1.137. FREQ_137 Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie 24
3.1.138. FREQ_138 Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi 24
3.1.139. FREQ_139 Podpora REST API a Webhookov 25
3.1.140. FREQ_140 Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting 25
3.1.141. FREQ_141 Moderné, responzívne webové rozhranie 25
3.1.142. FREQ_142 Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete 25
3.1.143. FREQ_143 Možnosť spätného prehľadu a forenznej analýzy 25
3.1.144. FREQ_144 Tvorba a správa prípadov - cases s úlohami a detailmi 25
3.1.145. FREQ_145 Pridávanie a sledovanie observables 25
3.1.146. FREQ_146 Prepojenie medzi prípadmi na základe spoločných indikátorov 25
3.1.147. FREQ_147 Kategorizácia incidentov pomocou tagov 25
3.1.148. FREQ_148 Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov 25
3.1.149. FREQ_149 Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami 26
3.1.150. FREQ_150 Podpora viacerých používateľských rolí 26
3.1.151. FREQ_151 Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi 26
3.1.152. FREQ_152 Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy 26
3.1.153. FREQ_153 Export incidentov do formátov CSV, PDF, cez REST API 26
3.1.154. FREQ_154 Logovanie činností analytikov počas riešenia incidentu (audit trail) 26
3.1.155. FREQ_155 Jednoduchá správa konfigurácií a aktualizácií 26
3.1.156. FREQ_156 Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie 26

3.1.157. FREQ_157 Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov 26
3.1.158. FREQ_158 Zdieľanie prípadov medzi tímami a externými partnermi podľa práv 26
3.1.159. FREQ_159 Vytvorenie základného prehľadu stavu bezpečnosti a incidentov 27
3.1.160. FREQ_160 Možnosť stiahnuť report alebo automaticky odoslať 27
3.1.161. FREQ_161 Možnosť výberu obsahu reportu – časové obdobie, typy incidentov 27
3.1.162. FREQ_162 Plánovanie pravidelných reportov 27
3.1.163. FREQ_163 Možnosť generovania jednorazových ad-hoc reportov 27
3.1.164. FREQ_164 Prispôsobenie vizuálnej podoby reportu 27
3.1.165. FREQ_165 Podpora exportu do PDF, CSV, JSON 27
3.1.166. FREQ_166 Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI 27
3.1.167. FREQ_167 Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy 27
3.1.168. FREQ_168 Podpora rôznych zdrojov: databázy, logy, API výstupy 27
3.1.169. FREQ_169 Webové/GUI rozhranie pre tvorbu a správu reportov 27
3.1.170. FREQ_170 Možnosť archivácie vygenerovaných reportov 28
3.1.171. FREQ_171 Možnosť obmedziť prístup k reportom podľa rolí - RBAC 28
3.1.172. FREQ_172 Šifrované prenosy reportov pri automatickej distribúcii 28
3.1.173. FREQ_173 Vytváranie, editácia a verzovanie záznamov 28
3.1.174. FREQ_174 Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky 28
3.1.175. FREQ_175 Fulltextové vyhľadávanie s podporou filtrov a tagov 28
3.1.176. FREQ_176 Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov 28
3.1.177. FREQ_177 Možnosť vkladať obrázky, logy, odkazy a prílohy 28
3.1.178. FREQ_178 Podpora RBAC 28
3.1.179. FREQ_179 Možnosť integrácie s ticketingom, incident managementom, SIEM 28
3.1.180. FREQ_180 Export dokumentov do PDF, HTML alebo Markdown formátu 28
3.1.181. FREQ_181 Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov 29
3.1.182. FREQ_182 Zachovanie histórie zmien s možnosťou obnovy staršej verzie 29
3.1.183. FREQ_183 Záznamy o tom, kto a kedy upravoval dokument 29
3.1.184. FREQ_184 Možnosť tvorby schvaľovacích workflow pre nové KB články 29
3.1.185. FREQ_185 Presnosť detekcie anomálií 29
3.1.186. FREQ_186 Miera falošných poplachov 29
3.1.187. FREQ_187 Podpora učenia bez labelov 29
3.1.188. FREQ_188 Výpočtová náročnosť AI/ML 29
3.1.189. FREQ_189 Rýchlosť inferencie 29
3.1.190. FREQ_190 Robustnosť voči zmene distribúcie dát 29
3.1.191. FREQ_191 Schopnosť práce s časovo-sekvenčnými dátami 30
3.1.192. FREQ_192 Flexibilita vstupných údajov 30
3.1.193. FREQ_193 Adaptívne/online učenia 30
3.1.194. FREQ_194 Vysvetliteľnosti modelu 30

3.2. Ne-funkčné požiadavky 30
3.2.1. NREQ_001 Základné organizačné roly 30
3.2.2. NREQ_002 Modularita a architektúra 31
3.2.3. NREQ_003 Náročnosť nasadenia a správy 31
3.2.4. NREQ_004 Podpora, dostupnosť dokumentácie a komunita 31
3.2.5. NREQ_005 Autentifikácia a riadenie prístupov 31
3.2.6. NREQ_006 Izolácia tenantov a ochrana dát 31
3.2.7. NREQ_007 Sieťová/monitorovacia integrácia 31
3.2.8. NREQ_008 Bezpečnostné testovanie 32
3.2.9. NREQ_009 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 32
3.2.10. NREQ_010 Zákon č. 69/2018 32
3.3. Technické požiadavky 32
3.3.1. TREQ_001 Výkonnosť a škálovateľnosť 32
3.3.2. TREQ_002 Spoľahlivosť a stabilita 32
3.3.3. TREQ_003 Súlad so štandardmi a interoperabilita 32
3.3.4. TREQ_004 Dostupnosť 33
3.3.5. TREQ_005 Škálovanie 33
3.3.6. TREQ_006 Virtualizácia 33
3.3.7. TREQ_007 Kontajnerizácia 33
3.3.8. TREQ_008 Orchestrácia 33
3.3.9. TREQ_009 Bezpečnostné logy 33
3.3.10. TREQ_010 Podpora mikroslužieb 33
3.3.11. TREQ_011 CI/CD a orchestrácia 33
3.3.12. TREQ_012 Kompatibilita s OSS 33
3.3.13. TREQ_013 Formáty dát 33
3.3.14. TREQ_014 Prístupová architektúra 33
3.3.15. TREQ_015 Bezpečné API 34
3.3.16. TREQ_016 Auditovateľnosť 34
3.3.17. TREQ_017 Modulárne riešenie 34
3.3.18. TREQ_018 Multitenantný deployment 34
3.3.19. TREQ_019 TLS/SSL šifrovanie 34
3.3.20. TREQ_020 Riadenie prístupu (RBAC/ABAC) 34
3.3.21. TREQ_021 Bezpečná správa tajného úložiska 34
3.3.22. TREQ_022 Bezpečné logovanie a detekcia anomálií 34
3.3.23. TREQ_023 Ukladanie logov a dát 34
3.3.24. TREQ_024 Zálohovanie konfigurácií a dashboardov 34
3.3.25. TREQ_025 Archivácia a dlhodobé uchovanie 34
3.3.26. TREQ_026 Výkon spracovania dát 34
Kľúčové zdroje pre katalóg požiadaviek 35
Zoznam zdrojov 35

1. HISTÓRIA DOKUMENTU

Verzia	Dátum	Zmeny	Subjekt
0.1	20.05.2024	Pracovný návrh	BRAINIT
0.9	14.06.2024	Prvá verzia na kontrolu	BRAINIT
1.0	22.06.2024	Finálna verzia na odovzdanie	BRAINIT

2. ÚČEL DOKUMENTU, SKRATKY, KONVENCIE A DEFINÍCIE

Dokument Katalóg požiadaviek obsahuje všeobecný zoznam a prehľad Funkčných, Ne-funkčných a Technických požiadaviek v zmysle nižšie uvedenej konvencie.

2.1. Použité skratky a pojmy

Tabuľka 1 Zoznam skratiek a pojmov, Vlastné spracovanie: (2025)

SKRATKA/POJEM	POPIS
IS	Informačný systém
EÚ	Európska únia
HW	Hardware
SW	Software
NAC	Network Access Control
NDR	Network detection and response
PAM	Privileged Access Management
SIEM	Security Information and Event Management
ZoKB	Zákon o kybernetickej bezpečnosti
NKIVS	Národná koncepcia informatizácie verejnej správy
OOÚ	Ochrana osobných údajov
OVM	Orgán verejnej moci
PaaS	Platform as a service
PILOT	PILOT – Prevádzka riešenia na vybraných aktéroch na produkčnom prostredí.
PoC	PoC – Implementovaný prototyp riešenia
PR	Projektové riadenie
SDL	Security development lifecycle
SLA	Service level agreement
SOAR	Security orchestration, automation and response

2.2. Konvencie pre typy požiadaviek

Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek, sú rozdelené na funkčné (funkcionálne), ne-funkčné (kvalitatívne, legislatívne a pod.) a technické (technologický charakter). Podskupiny v hlavných kategóriách je možné rozšíriť podľa potrieb projektu, napríklad:

Funkcionálne (používateľské) požiadavky majú konvenciu:

FREQxxx

F – Užívateľská požiadavka

R – Označenie požiadavky

xxx – Číslo požiadavky

Nefunkčné (kvalitatívne, legislatívne – Non Functional Requirements – NFR) **požiadavky** majú nasledovnú konvenciu:

NREQxxx

N – Nefukčná požiadavka

R – Označenie požiadavky

xxx – Číslo požiadavky

Technické (technologocký charakter) požiadavky majú nasledovnú konvenciu:

TREQxxx

T – Technologická požiadavka

R – Označenie požiadavky

xxx – Číslo požiadavky

2.3. Vysvetlenie stĺpcov v katalógu požiadaviek

2.3.1. Prípravná a iniciačná fáza

- **PORADOVÉ ID** – Poradové číslo požiadavky
- **ID POŽIADAVKY** – Katalógové číslo požiadavky v zmysle konvencie značenia s rozlíšením kategórie
- **KATEGÓRIA POŽIADAVKY** – Kategória požiadavky v zmysle konvencie rozdelenia na Funkčné, Ne-funkčné a Technické požiadavky
- **OBLASŤ POŽIADAVKY** – Predstavuje príslušnosť k určitej oblasti ako sú napríklad vývoj, služba, prevádzka a iné
- **NÁZOV POŽIADAVKY** – Predstavuje krátky názov požiadavky
- **DETAILNÝ POPIS POŽIADAVKY** – Predstavuje detailnejší popis požiadavky z ktorého je možné identifikovať cieľ požiadavky
- **VLASTNÍK POŽIADAVKY** – Predstavuje vlastníka procesov, biznis vlastníka alebo garanta požiadavky

- **NÁZOV MODULU** – Predstavuje príslušnosť požiadavky k danému modulu
- **ČÍSLO INKREMENTU** – Predstavuje inkrement pre prípad rozdelenia riešenia na viaceré na seba nadväzujúce projektové celky
- **POZNÁMKA** – Poznámka pre prípad potreby zachytiť informáciu, ktorá nezapadá do preddefinovaných stĺpcov a je podstatná na uchovanie

2.3.2. Realizačná fáza

V rámci katalógu požiadaviek boli dopredu definované stĺpce pre potreby pokračovania v prípadnej budúcej realizačnej fáze projektu:

- **Referencia návrhu riešenia z DNR** – Odkaz na kapitolu alebo diagram kde sa daná požiadavka naplní / realizuje
- **Spôsob realizácie** – Krátky a výstižný spôsob realizácie
- **Identifikácia USE CASE** – Referencia na konkrétny Use Case v rámci ktorého je naplnená požiadavka
- **Identifikácia TEST CASE** – Referencia na konkrétny Test Case v rámci ktorého je možný test naplneného Use Case
- **Použité TESTOVACIE DÁTA** – Referencia na použité test dáta
- **Použité PROSTREDIE** – Referencia na použité prostredie pri testovaní
- **SPÔSOB OVERENIA** – Krátky a výstižný spôsob overenia funkčnosti

2.3.3. Metodika

Analýza požiadaviek v projekte INNOSOC bude prebiehať systematicky a v súlade s princípmi metodík PRINCE2, ITTIL a TOGAF, ktoré partneri projektu bežne využívajú na riadenie podobných inovatívnych riešení. Tento proces bude realizovaný v niekoľkých fázach s cieľom identifikovať, špecifikovať, validovať a dokumentovať všetky funkčné a nefunkčné požiadavky na navrhované multitenantné SOC riešenie poskytované formou cloudovej služby.

Prvým krokom bude zber požiadaviek prostredníctvom workshopov, individuálnych rozhovorov a dotazníkov so zainteresovanými stranami projektu, vrátane technických expertov, manažmentu, ako aj budúcich používateľov riešenia. V tejto fáze sa budú zisťovať očakávania, potreby a problémy, ktoré riešenie musí adresovať, pričom dôraz sa bude klásť na špecifiká vyplývajúce z legislatívy NIS2 a zákona o kybernetickej bezpečnosti.

Následne budú požiadavky systematicky analyzované a klasifikované podľa priorít, dopadu na projekt a technickej realizovateľnosti. Bude sa rozlišovať medzi požiadavkami na funkcionalitu (Funkčné požiadavky) samotnej SOC platformy (napr. detekcia anomálií, reporting, automatizovaná reakcia) a ne-funkčnými a technickými požiadavkami (napr. dostupnosť, výkon, bezpečnosť, škálovateľnosť). Pre účely modelovania a ďalšej validácie budú v ďalších fázach projektu požiadavky vizualizované pomocou UML a Archimate diagramov, aby sa overilo ich správne pochopenie a súlad s architektonickým návrhom riešenia.

Validácia požiadaviek bude zabezpečená prostredníctvom kontrolných stretnutí, priebežných revízií a spätných väzieb od používateľov aj odborníkov v oblasti kybernetickej bezpečnosti. Takýto iteratívny prístup umožní včas odhaliť prípadné nedostatky alebo konflikty v požiadavkách, ktoré by mohli ohroziť kvalitu výsledného riešenia.

Výsledky analýzy požiadaviek budú priebežne zaznamenávané v centralizovanom systéme riadenia požiadaviek a budú tvoriť súčasť oficiálnej projektovej dokumentácie. Tento postup zabezpečí transparentnosť celého procesu, vysledovateľnosť zmien a zároveň poskytne základ pre overovanie kvality počas vývoja, testovania a implementácie riešenia.

Tento dokument ako aj Katalóg požiadaviek je stále živým dokumentom a to nie len do ukončenia Detailného Návrhu Riešenia. Bude podliehať neustálej validácií.

3. KATALÓG POŽIADAVIEK

Podrobný prehľad Funkčných, Ne-funkčných a Technických požiadaviek je v rámci prílohy „V10-B - Zoznam funkčných a nefunkčných požiadaviek.xlsx“.

3.1. Funkčné požiadavky

3.1.1. FREQ_001 Proces monitorovania bezpečnostných udalostí

Zabezpečiť proces monitorovania bezpečnostných udalostí – zabezpečuje zber a sledovanie logov, metrických údajov a alertov zo všetkých integrovaných systémov.

3.1.2. FREQ_002 Proces detekcie incidentov

Zabezpečiť proces detekcie incidentov – je zodpovedný za identifikáciu anomálií, vzorcov útokov a iných hrozieb prostredníctvom korelačných pravidiel a heuristických mechanizmov.

3.1.3. FREQ_003 Proces reakcie na incodenty

Zabezpečiť proces reakcie na incidenty – definuje spôsob, akým tím reaguje na identifikované incidenty. Zahŕňa eskaláciu, priradenie zodpovednosti, vykonanie opatrení, ako aj komunikáciu so zasiahnutými stranami.

3.1.4. FREQ_004 Proces správy incidentov

Zabezpečiť proces správy incidentov – zahŕňa evidenciu, klasifikáciu, priraďovanie priorít, dokumentovanie a uzatváranie incidentov.

3.1.5. FREQ_005 Proces správy hrozieb

Zabezpečiť proces správy hrozieb (Threat Intelligence) – umožňuje systematickú prácu s informáciami o hrozbách.

3.1.6. FREQ_006 Proces reporting a vizualizácia

Zabezpečiť proces reporting a vizualizácia – zabezpečuje pravidelný výstup pre manažment, audítorov a SOC analytikov.

3.1.7. FREQ_007 Proces správy poznatkov

Zabezpečiť proces správy poznatkov – zabezpečuje udržiavanie znalostnej bázy playbookov, dokumentácie a odporúčaných reakcií.

3.1.8. FREQ_008 Centralizácia logov

Riešenie musí zabezpečiť zber a centralizáciu logov zo systémov, sietí, koncových bodov a aplikácií.

3.1.9. FREQ_009 Normalizácia a obohacovanie údajov

Riešenie musí zabezpečiť normalizáciu a obohacovanie údajov.

3.1.10. FREQ_010 Ukladanie a indexovanie údajov

Riešenie musí zabezpečiť ukladanie, indexovanie a uchovávanie údajov.

3.1.11. FREQ_011 Tvorba korelačných pravidiel

Riešenie musí zabezpečiť tvorbu korelačných pravidiel a alertov.

3.1.12. FREQ_012 Vizualizácia výstupov

Riešenie musí zabezpečiť vizualizáciu výstupov.

3.1.13. FREQ_013 Integrácia s ďalšími nástrojmi

Riešenie musí zabezpečiť integráciu s ďalšími nástrojmi.

3.1.14. FREQ_014 SOAR

Riešenie musí zabezpečiť SOAR a bude slúžiť na automatizáciu reakčných scenárov, spracovanie alertov do prípadov a ich analýzu.

3.1.15. FREQ_015 Ticketovací systém a incident manažment

Riešenie musí zabezpečiť ticketovací a incident manažment systém poskytne workflow pre riešenie incidentov, eskaláciu, audit a sledovanie riešenia.

3.1.16. FREQ_016 Znalostný portál

Riešenie musí zabezpečiť znalostný portál, ktoré bude podporovať reakčné procesy zdieľaním playbookov, interných politík a návodov.

3.1.17. FREQ_017 Inventarizácia a správa aktív

Riešenie musí zabezpečiť inventarizáciu a správu aktív. Správa IT aktív je kľúčová pre mapovanie dopadov hrozieb.

3.1.18. FREQ_018 Threat Intelligence

Riešenie musí zabezpečiť Threat Intelligence. Procesy CTI (Cyber Threat Intelligence) umožňujú obohacovanie incidentov o známe hrozby, TTPs a IOCs.

3.1.19. FREQ_019 Správa zraniteľností

Riešenie musí zabezpečiť správu zraniteľností.

3.1.20. FREQ_020 Reporting a spätná analýza

Riešenie musí zabezpečiť reporting a spätnú analýzu.

3.1.21. FREQ_021 Onboarding nového zákazníka

Riešenie musí zabezpečiť onboarding nového zákazníka, kde prebieha integrácia jeho infraštruktúry do multitenantného prostredia SOCaaS. To zahŕňa:

- nastavenie logovacieho agenta
- konfiguráciu korelačných pravidiel
- vytvorenie separovaných dashboardov
- nastavenie incident managementu pre zákazníka

3.1.22. FREQ_022 Detekcia a eskalácia incidentu

Riešenie musí zabezpečiť detekciu a eskalácia incidentu. V prostredí musia byť nakonfigurované pravidlá na detekciu anomálií a známych hrozieb. Po detekcii:

- sa generuje alert
- alert sa automaticky transformuje na incident
- Zammad zabezpečuje ticket pre L1 tím a podporu eskalácie,
- tím vyhodnotí observables a využije obohatenie

3.1.23. FREQ_023 Správa zraniteľností a inventarizácia

Riešenie musí zabezpečiť správu zraniteľností a inventarizáciu. Pravidelné skeny majú byť prepojené s CMDB:

- Assety sú aktualizované na základe detekcie
- incidenty viazané na zraniteľnosti sú prepájané do manažment systému

3.1.24. FREQ_024 Proaktívne vyhľadávanie hrozieb

Riešenie musí zabezpečiť proaktívne vyhľadávanie hrozieb (Threat Hunting). Použíjú sa pokročilé dotazy, často doplnené o:

- CTI dáta
- manuálnu analýzu v prípade podozrivých entít
- výsledky sú dokumentované ako playbooky

3.1.25. FREQ_025 Tvorba reportov a dashboardov

Riešenie musí zabezpečiť tvorbu reportov a dashboardov. Pre manažment a zákazníkov budú pravidelne generované:

- prehľady incidentov
- vizualizácie z metrík a ticketingu
- exporty pre audit a SLA reporting

3.1.26. FREQ_026 Tvorba znalostnej bázy

Riešenie musí zabezpečiť tvorbu znalostnej bázy. Každý incident alebo nový typ hrozby sa bude dokumentovať formou:

- incident summary + lessons learned
- zápis v znalostnom portáli
- kategorizácia podľa MITRE ATT&CK a dátumov

3.1.27. FREQ_027 Údržba a aktualizácia systému

Riešenie musí zabezpečiť údržbu a aktualizáciu systému. Prevádzkový tím musí mať stanovené:

- pravidlá pre aktualizácie komponentov
- prostredie na overenie zmien
- centralizovaný monitoring funkčnosti všetkých modulov

3.1.28. FREQ_028 Spracovanie dátových tokov

Riešenie musí zabezpečiť spracovanie dátových tokov. Hlavné úlohy spracovania dátových tokov sú:

- Príjem logov a udalostí z viacerých heterogénnych zdrojov
- Validácia, normalizácia a obohatenie dát
- Priradenie časových pečiatok, identifikátorov a kategórií udalostí
- Presmerovanie dát do vhodných indexov pre efektívnu analýzu
- Odfiltrovanie redundatných alebo irelevantných údajov
- Implementácia pipeline pravidiel a spracovateľských modulov

3.1.29. FREQ_029 Korelačné pravidlá a detekcia hrozieb

Riešenie musí zabezpečiť korelačné pravidlá a detekcia hrozieb:

- Alerty na základné IOC – porovnanie s databázou známych indikátorov (IP, URL,hash).
- Anomálne správanie používateľov – napr. viacnásobné neúspešné prihlásenie v krátkom čase, login z nového geografického regiónu.
- Neštandardné sieťové komunikácie – napr. DNS dotazy na dynamicky generované domény (DGA), odchýlky v čase a objeme dát.
- Aktivity s administratívnymi právami – napr. pridanie používateľa do skupiny „Administrators“, zmeny ACL, spustenie netsh, powershell.
- Reťazenie udalostí – korelácia medzi viacerými logmi v čase: napr. login → súborový prenos → spustenie škodlivého procesu. Tieto pravidlá budú spravované, kde možno:
  - sledovať detekčné alerty,
  - nastavovať prahové hodnoty (thresholds),
  - konfigurovať výnimky a ignorované hodnoty (exceptions),
  - exportovať a importovať pravidlá ako JSON objekty.

3.1.30. FREQ_030 Integrácia s ostatnými komponentmi

Riešenie musí zabezpečiť integráciu s ostatnými komponentmi:

- Prepojenie so zdrojmi dát
- Integrácia s nástrojmi incident managementu a SOAR
- Znalostná databáza a playbooky

3.1.31. FREQ_031 Návrh dashboardov

Riešenie musí zabezpečiť návrh dashboardov. Pre udržanie prehľadnosti budú dashboardy v rámci SOCaaS rozdelené podľa funkčných vrstiev nasledovne:

- 1.Globálne prehľady (SOC Overview) Určené pre manažment a SLA reporting – zahŕňajú denné/měsíčné štatistiky incidentov, typy hrozieb, top 10 IP adries, krajiny pôvodu útokov, čas vyriešenia ticketov.
- 2.Alert monitoring dashboardy Zamerané na operatívny monitoring – zobrazujú nové alerty, rozdelenie podľa severity (Critical, High, Medium), časové trendy, a korelácie medzi viacerými zdrojmi.
- 3.Tematické dashboardy Pokrývajú špecifické oblasti:
  - EDR aktivity: zaznamenané súbory, procesy, pokusy o exekúciu škodlivého kódu.
  - Zraniteľnosti a skeny: výsledky z Greenbone alebo OpenSCAP.
  - Firewall a sieťové logy: prístupy, porty, odhalené scanningové aktivity.

- 4.Detailné analytické dashboardy – Slúžia pre L2 analytikov a threat hunting. Obsahujú heatmapy, časové rezy, distribúcie podľa hodín, krajín, ASN, výskyt IOC a podobne.
- 5.Ad-hoc a incident-specific dashboardy – Vznikajú počas vyšetrovania konkrétneho prípadu, kde si analytik zostaví vlastnú vizualizáciu na základe dát z Elasticsearch.

3.1.32. FREQ_032 Štruktúra dashboardov

Riešenie musí zabezpečiť štruktúru dashboardov ako sú dashboardy zostavené z jednotlivých panelov, ktoré môžu obsahovať grafy, tabuľky, heatmapy, distribučné histogramy, metriky alebo mapy. Každý dashboard v rámci SOCaaS je navrhnutý ako kompozícia týchto vizualizácií zameraná na konkrétny aspekt monitorovania alebo analýzy.

- Prehľad systémovej bezpečnosti
- Korelačné a incidentové dashboardy
- Vizualizácia sieťovej prevádzky a prístupov
- Monitorovanie autentifikácií a správania používateľov
- Integrovaný prehľad pre SOC analytika

3.1.33. FREQ_033 Reporting

Riešenie musí zabezpečiť reporting. Reporting v SOCaaS bude plniť niekoľko základných cieľov:

- Prevádzkový prehľad – zobrazenie stavu systémov, počtu incidentov, aktivity agentov.
- Bezpečnostný reporting – výstupy o detekovaných hrozbách, typoch útokov, trendoch.
- Compliance reporting – reporty podľa regulatórnych požiadaviek (napr. GDPR, NIS2).
- Manažérsky reporting – agregované štatistiky a ukazovatele pre vedenie organizácie.
- Zákaznícky reporting – individuálne prehľady pre jednotlivých klientov multitenantného SOCaaS.

3.1.34. FREQ_034 Manuálny export reportov

Riešenie musí zabezpečiť manuálny export reportov. Reporty bude možné exportovať ako:

- PDF dokument – generovaný snapshot aktuálneho dashboardu.
- PNG obraz – statické obrázky jednotlivých vizualizácií.
- CSV súbory – surové dáta z tabuliek a dátových polí.
- JSON – pre automatizovanú analýzu a ďalšie spracovanie.

3.1.35. FREQ_035 Automatizovaný export reportov

Riešenie musí zabezpečiť automatizovaný export reportov. Reporty bude možné exportovať automatizovane:

- Periodické reporty – denne, týždenne alebo mesačne generované a distribuované výstupy.
- Distribúcia cez e-mail alebo webhook – reporty môžu byť automaticky odoslané na určené adresy alebo endpointy.
- Podpora pre templaty a vlastné filtre – možnosť nastaviť podmienky, výbery časových období a formáty podľa potrieb.

3.1.36. FREQ_036 Customizácia výstupov reportov

Riešenie musí zabezpečiť customizácia výstupov reportov. Bude obsahovať:

- Možnosť výberu metrík, polí, časových rozsahov

- Personalizácia dizajnu – logá, záhlavie, farebná schéma
- Zaradenie vysvetliviek, poznámok a kontextuálneho komentára

3.1.37. FREQ_037 Podpora IaaS funkcionality

Riešenie vyžaduje plnú funkcionalitu IaaS – správu virtuálnych strojov (VM), diskov, sietí, obrazov, snapshotov a samostatných zdrojov. Platforma musí podporovať vytváranie a správu rôznych typov inštancií, umožniť priradenie zdrojov podľa potreby tenantov a zároveň ponúknuť robustné API rozhranie pre programovateľný prístup. Schopnosť poskytovať kompletnú IaaS funkcionalitu je kľúčová pre zabezpečenie pružného a spoľahlivého prevádzkovania SOC ako služby.

3.1.38. FREQ_038 Podpora orchestrácie a automatizácie

Riešenie má podporovať nástroje ako Heat (OpenStack orchestration), Terraform (infrastructure as code), Ansible (automatizácia) alebo Kubernetes Operator pre efektívnu správu a nasadzovanie komplexných infraštruktúrnych scénarov. Táto schopnosť umožní rýchle škálovanie služieb, automatizované rozbaľovanie prostredí, opakovateľné testovanie aj zotavenie pri výpadkoch. V prostredí SOC, kde sa často menia požiadavky a topológia siete, je orchestrácia nevyhnutná pre zabezpečenie flexibility, udržateľnosti a prevádzkovej efektivity.

3.1.39. FREQ_039 Podporované formáty logov

Schopnosť SIEM prijímať a spracovávať logy v rôznych štandardizovaných formátoch. Podporované formáty logov (syslog, JSON, CSV, CEF, LEEF...).

3.1.40. FREQ_040 Reálny čas vs. dávkové spracovanie

Schopnosť spracovávať logy v reálnom čase (streaming) alebo len v dávkach. Reálny čas vs. dávkové spracovanie.

3.1.41. FREQ_041 Korelácia udalostí

Možnosť prepájať súvisiace udalosti pomocou korelačných pravidiel. Korelácia udalostí (preddefinované a vlastné pravidlá).

3.1.42. FREQ_042 Machine Learning/Behaviorálna analýza

Schopnosť SIEM systému detegovať anomálie pomocou strojového učenia. Machine Learning/Behaviorálna analýza.

3.1.43. FREQ_043 Threat Intelligence (CTI) integrácia

Integrácia so zdrojmi hrozieb (IOC, TTP), automatické obohacovanie údajov. Threat Intelligence (CTI) integrácia.

3.1.44. FREQ_044 Detekcia anomálií

Detekcia neštandardného správania alebo odchýlok od očakávaného správania. Detekcia anomálií.

3.1.45. FREQ_045 Vlastné alertovacie pravidlá a prahy

Schopnosť definovať vlastné pravidlá a podmienky pre generovanie alertov. Vlastné alertovacie pravidlá a prahy.

3.1.46. FREQ_046 Automatizované reakcie

Možnosť spustiť reakciu (blokovanie, izolácia, notifikácia) automaticky. Automatizované reakcie (napr. blokovanie IP, integrácia SOAR).

3.1.47. FREQ_047 Normalizácia a obohacovanie dát

Transformácia rôznych logov do jednotného formátu a ich rozšírenie (napr. WHOIS, GEOIP). Normalizácia a obohacovanie dát.

3.1.48. FREQ_048 Fulltextové a rýchle vyhľadávanie

Schopnosť vyhľadávať v logoch cez operátory, tagy, filtre. Fulltextové a rýchle vyhľadávanie.

3.1.49. FREQ_049 Dashboardy a ich kategorizácia

Vizualizácia údajov pomocou grafov, filtrov a widgetov. Dashboardy (vrátane interaktívnych) a ich kategorizácia.

3.1.50. FREQ_050 Podpora pre MITRE ATT&CK mapovanie

Schopnosť mapovať detekcie na taktiky a techniky podľa MITRE ATT&CK. Podpora pre MITRE ATT&CK mapovanie.

3.1.51. FREQ_051 Retencia

Schopnosť nastaviť retenčné politiky logov podľa zdroja a dôležitosti. Retencia (flexibilná, podľa typu logu).

3.1.52. FREQ_052 Šifrovanie

Ochrana logov pred neoprávneným prístupom pri prenose a ukladaní. Šifrovanie (pri prenose aj uložení).

3.1.53. FREQ_053 Monitoring stavu systému

Sledovanie výkonu, dostupnosti a funkčnosti systému. Monitoring stavu systému (healthcheck).

3.1.54. FREQ_054 Prijímanie upozornení a dát z rôznych bezpečnostných systémov

Schopnosť prijímať alerty a dáta z rôznych bezpečnostných zdrojov (SIEM, EDR, CTI...). Prijímanie upozornení a dát z rôznych bezpečnostných systémov.

3.1.55. FREQ_055 Normalizácia a parsovanie dát

Transformácia vstupných dát do štandardizovaného formátu pre ďalšie spracovanie. Normalizácia a parsovanie dát.

3.1.56. FREQ_056 Kategorizácia a prioritizácia incidentov

Možnosť triediť incidenty podľa závažnosti, typu, kategórie a dôležitosti. Kategorizácia a prioritizácia incidentov.

3.1.57. FREQ_057 Možnosť manuálneho aj automatického vytvárania incident ticketov

Podpora ručného aj automatického vytvárania incident ticketov zo vstupných údajov. Možnosť manuálneho aj automatického vytvárania incident ticketov.

3.1.58. FREQ_058 Preddefinované playbooky

Dostupnosť základných reakčných scenárov a automatizácií vopred pripravených v nástroji. Preddefinované playbooky.

3.1.59. FREQ_059 Možnosť tvorby vlastných playbookov bez potreby programovania

Schopnosť tvoriť a spravovať playbooky pomocou vizuálneho rozhrania bez nutnosti kódovania. Možnosť tvorby vlastných playbookov bez potreby programovania.

3.1.60. FREQ_060 Workflow engine s vetvením, podmienkami a slučkami

Možnosť definovať komplexné logiky v playbookoch pomocou rozhodovacích bodov. Workflow engine s vetvením, podmienkami a slučkami.

3.1.61. FREQ_061 Automatizované reakcie: blok IP, izolácia hostu, eskalácia

Schopnosť automaticky vykonať reakcie ako blokovanie, izolácia či upozornenie. Automatizované reakcie: blok IP, izolácia hostu, eskalácia.

3.1.62. FREQ_062 Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR

Prepojenie a výmena dát s inými systémami v rámci incident response procesu. Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR.

3.1.63. FREQ_063 API-first prístup

Prístupnosť funkcií nástroja cez API a podpora webhookov na notifikácie a interakcie. API-first prístup (REST, Webhooky).

3.1.64. FREQ_064 Podpora pre plug-iny a konektory

Schopnosť rozšírenia funkcionality nástroja cez moduly alebo konektory. Podpora pre plug-iny a konektory.

3.1.65. FREQ_065 Dashboardy pre stav a štatistiky incidentov

Prehľadné zobrazenie stavu systému a prebiehajúcich incidentov. Dashboardy pre stav a štatistiky incidentov.

3.1.66. FREQ_066 RBAC a audit trail

Riadenie prístupov na základe rolí a logovanie zmien v systéme. RBAC a audit trail.

3.1.67. FREQ_067 Playbook debugging & testing

Možnosť testovať a ladiť playbooky pred ich ostrým nasadením. Playbook debugging & testing.

3.1.68. FREQ_068 SOAR-SIEM synchronizácia stavu incidentov

Prepojenie stavu incidentov medzi SIEM a SOAR pre aktuálnu viditeľnosť. SOAR-SIEM synchronizácia stavu incidentov.

3.1.69. FREQ_069 Možnosti nasadenia: on-prem, cloud, hybrid

Možnosť nasadenia riešenia v rôznych prostrediach vrátane lokálneho, cloudového alebo hybridného modelu. Možnosti nasadenia: on-prem, cloud, hybrid.

3.1.70. FREQ_070 Podpora pre rôzne OS

Podpora pre inštaláciu a beh agenta na rôznych operačných systémoch. Podpora pre rôzne OS (Windows, Linux, macOS).

3.1.71. FREQ_071 Zber auditovacích dát pomocou agentov

Zber auditovacích záznamov o aktivitách používateľov, procesoch a systéme cez agenta. Zber auditovacích dát pomocou agentov.

3.1.72. FREQ_072 File Integrity Monitoring

Detekcia zmeny súborov v reálnom čase pre účely forenznej analýzy a integrity. File Integrity Monitoring (FIM).

3.1.73. FREQ_073 Zber systémových metrík, procesov a správania

Monitorovanie systémového správania a metrík ako CPU, pamäť, služby a procesy. Zber systémových metrík, procesov a správania.

3.1.74. FREQ_074 Zber informácií o zraniteľnostiach a konfiguráciách

Získavanie informácií o zraniteľnostiach z konfiguračných údajov a porovnanie s databázami CVE. Zber informácií o zraniteľnostiach a konfiguráciách.

3.1.75. FREQ_075 Analýza logov a korelácia s hrozbami

Analýza logov s cieľom detekcie korelovaných udalostí a potenciálnych hrozieb. Analýza logov a korelácia s hrozbami.

3.1.76. FREQ_076 Detekcia malvéru a narušení

Identifikácia škodlivého softvéru a incidentov narušenia bezpečnosti. Detekcia malvéru a narušení.

3.1.77. FREQ_077 Heuristická a behaviorálna analýza

Založenie detekcie na správaní a heuristike namiesto len signatúr. Heuristická a behaviorálna analýza.

3.1.78. FREQ_078 Podpora ML/AI algoritmov na detekciu hrozieb

Využitie algoritmov umelej inteligencie na detekciu anomálií a hrozieb. Podpora ML/AI algoritmov na detekciu hrozieb.

3.1.79. FREQ_079 Mapovanie na MITRE ATT&CK framework

Zaradenie detegovaných aktivít a techník do rámca MITRE ATT&CK pre účely TTP analýz. Mapovanie na MITRE ATT&CK framework.

3.1.80. FREQ_080 Automatické reakcie

Automatická reakcia na incidenty, ako je izolácia koncového bodu alebo karanténa súborov. Automatické reakcie (napr. izolácia zariadenia, karanténa súboru).

3.1.81. FREQ_081 Nízka systémová záťaž agenta

Agent má nízky vplyv na výkon systému, čo umožňuje nasadenie vo veľkej škále. Nízka systémová záťaž agenta.

3.1.82. FREQ_082 Jednoduché centrálne riadenie agentov

Centrálna konzola na správu, konfiguráciu a dohľad nad všetkými agentmi. Jednoduché centrálne riadenie agentov.

3.1.83. FREQ_083 Pravidelné aktualizácie signatúr a modulov

Pravidelné aktualizácie databáz hrozieb, signatúr a detekčných pravidiel. Pravidelné aktualizácie signatúr a modulov.

3.1.84. FREQ_084 Bezplatná verzia, open-source riešenie s možnosťou rozšírenia

Dostupnosť základnej funkcionality bez licencie a možnosť rozšírenia. Bezplatná verzia, open-source riešenie s možnosťou rozšírenia.

3.1.85. FREQ_085 Odhadovaná kapacita skenovania

Schopnosť nástroja efektívne skenovať veľké siete. Odhadovaná kapacita skenovania (napríklad min. 100 IP/24h).

3.1.86. FREQ_086 Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed

Frekvencia a rozsah aktualizácií detekčných vzorov. Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed.

3.1.87. FREQ_087 Podpora CPE, CVE identifikátorov

Možnosť identifikácie zraniteľností podľa štandardizovaných identifikátorov. Podpora CPE, CVE identifikátorov.

3.1.88. FREQ_088 Prijateľné webové rozhranie na správu skenovania a výsledkov

Použiteľnosť GUI pre správu skenov a výsledkov. Prijateľné webové rozhranie na správu skenovania a výsledkov.

3.1.89. FREQ_089 Bez potreby agentov

Možnosť realizovať skeny bez nutnosti inštalovať agenta na zariadenia. Bez potreby agentov (agentless).

3.1.90. FREQ_090 Podpora plánovania úloh a alertov

Možnosť automatizovať opakované úlohy a generovanie upozornení. Podpora plánovania úloh a alertov (voliteľné).

3.1.91. FREQ_091 Tikety na nápravu – integrácia alebo export

Možnosť exportovať nálezy do ticketovacieho systému alebo CSV, JSON, PDF. Tikety na nápravu – integrácia alebo export.

3.1.92. FREQ_092 Konfigurovateľné formáty reportov

Flexibilita výstupov pre ďalšie spracovanie. Konfigurovateľné formáty reportov (napr. CSV, XML, PDF).

3.1.93. FREQ_093 Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker

Flexibilita inštalácie do rôznych prostredí. Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker.

3.1.94. FREQ_094 Architektúra skenovania

Škálovateľnosť a prispôsobenie distribúcie skenov. Architektúra skenovania (monolitická alebo master/senzor).

3.1.95. FREQ_095 Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice

Možnosť prepojenia s ďalšími bezpečnostnými a IT systémami. Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice.

3.1.96. FREQ_096 Podpora pre CVSS 4.0

Podpora najnovšej verzie skórovacieho systému CVSS. Podpora pre CVSS 4.0.

3.1.97. FREQ_097 Podpora pre EPSS – predikcia zneužitia zraniteľností

Využitie modelov pravdepodobnosti zneužitia zraniteľnosti. Podpora pre EPSS – predikcia zneužitia zraniteľností.

3.1.98. FREQ_098 Politiky súladu s normami

Možnosť hodnotiť zraniteľnosti vo vzťahu k štandardom. Politiky súladu s normami (napr. GDPR, ISO, CIS, BSI...).

3.1.99. FREQ_099 Podpora strategického CTI

Získavanie a analýza informácií o dlhodobých trendoch, dopadoch útokov a strategických odporúčaniach. Podpora strategického CTI (správy, analýzy dopadu, trendy útokov).

3.1.100. FREQ_100 Podpora operatívneho CTI

Schopnosť mapovať techniky, taktiky a procedúry (TTP), identifikovať útočnícke skupiny a ich správanie. Podpora operatívneho CTI (TTP, profilovanie skupín).

3.1.101. FREQ_101 Podpora taktického CTI

Práca s indikátormi kompromitácie (IOC) a ich evidencia, spracovanie, distribúcia. Podpora taktického CTI (IOC, IP, hash, URL, domény).

3.1.102. FREQ_102 Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov

Automatické sťahovanie dát z rôznych zdrojov (napr. GitHub, feeds, MISP, API systémy). Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov.

3.1.103. FREQ_103 Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo

Pripravené konektory alebo integrácie pre známe CTI zdroje. Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo.

3.1.104. FREQ_104 Integrácia s 3rd party službami

Schopnosť obohacovať IOC a ďalšie artefakty pomocou externých služieb. Integrácia s 3rd party službami ako VirusTotal, Shodan, DomainTools, URLScan.io.

3.1.105. FREQ_105 Schopnosť normalizovať CTI dáta na jednotný formát

Konsolidácia dát z rôznych formátov do štruktúrovaného jednotného výstupu. Schopnosť normalizovať CTI dáta na jednotný formát.

3.1.106. FREQ_106 Možnosť manuálnej analýzy CTI

Rozhranie a nástroje pre bezpečnostných analytikov na ručné skúmanie dát. Možnosť manuálnej analýzy CTI.

3.1.107. FREQ_107 Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov

Možnosť workflow pre spracovanie dát bez potreby manuálnych zásahov. Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov.

3.1.108. FREQ_108 Deduplikácia hrozieb a informácií

Odstraňovanie redundantných IOC a indikátorov. Deduplikácia hrozieb a informácií.

3.1.109. FREQ_109 Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách

Preposielanie IOC a dát priamo do detekčných systémov (SIEM, IDS, firewall). Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách.

3.1.110. FREQ_110 Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu

Spájanie incidentov, IOC a TTP s ATT&CK frameworkom. Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu.

3.1.111. FREQ_111 Podpora formátov ako STIX/TAXII

Použitie štandardizovaných formátov pre výmenu CTI dát. Podpora formátov ako STIX/TAXII.

3.1.112. FREQ_112 Podpora najväčšieho počtu autoritatívnych CTI zdrojov

Rozsiahly výber komunitných, verejných a platených zdrojov. Podpora najväčšieho počtu autoritatívnych CTI zdrojov.

3.1.113. FREQ_113 Zníženie potreby manuálnej analýzy

Zautomatizovanie a prioritizácia hrozieb tak, aby sa analytici venovali len relevantným. Zníženie potreby manuálnej analýzy – šetrenie času analytikov.

3.1.114. FREQ_114 Vytvorenie, editácia a mazanie záznamov o aktívach

Schopnosť systému evidovať, upravovať a mazať informácie o jednotlivých aktívach. Vytvorenie, editácia a mazanie záznamov o aktívach.

3.1.115. FREQ_115 Rozlíšenie aktív podľa typu

Možnosť rozlišovať typy aktív pre lepšiu organizáciu a správu. Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové.

3.1.116. FREQ_116 Možnosť priradenia tagov, kategórií, vlastníkov a stavu

Pridávanie metadát pre efektívne triedenie a správu aktív. Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené).

3.1.117. FREQ_117 Evidencia bezpečnostného stavu každého aktíva

Ukladanie informácií o zraniteľnostiach, patch úrovni a aktualizáciách systému. Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia).

3.1.118. FREQ_118 Mapovanie aktív na lokality, VLANy, IP rozsahy, racky

Schopnosť mapovať fyzické a logické umiestnenie aktív v sieti. Mapovanie aktív na lokality, VLANy, IP rozsahy, racky.

3.1.119. FREQ_119 Väzby medzi aktívami

Možnosť vizualizovať a spravovať prepojenia medzi komponentmi infraštruktúry. Väzby medzi aktívami (napr. server – služba – aplikácia).

3.1.120. FREQ_120 Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov

Možnosť prepojenia s ďalšími nástrojmi SOC pre automatizáciu a zdieľanie údajov. Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov.

3.1.121. FREQ_121 Možnosť filtrovania, fulltextového vyhľadávania a exportu

Efektívna práca s údajmi – vyhľadávanie podľa rôznych parametrov a exportovanie údajov. Možnosť filtrovania, fulltextového vyhľadávania a exportu.

3.1.122. FREQ_122 Podpora API na správu aktív a integráciu

Možnosť spravovať a aktualizovať údaje o aktívach pomocou API. Podpora API (REST, GraphQL) na správu aktív a integráciu.

3.1.123. FREQ_123 Možnosť tvorby vlastných polí, atribútov, pluginov

Užívateľská flexibilita pre prispôsobenie systému vlastným potrebám. Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django).

3.1.124. FREQ_124 Automatizovaný discovery assetov v sieti

Automatizovaný zber a aktualizácia údajov o aktívach zo siete a iných systémov. Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov).

3.1.125. FREQ_125 Webové rozhranie s možnosťou úprav a prehľadnou správou

Používateľsky prívetivé GUI pre správu assetov. Webové rozhranie s možnosťou úprav a prehľadnou správou.

3.1.126. FREQ_126 Zaznamenávanie zmien na aktívach

Auditovateľnosť všetkých zmien pre forenznú a prevádzkovú transparentnosť. Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil).

3.1.127. FREQ_127 Možnosť sledovať životný cyklus assetov

Správa jednotlivých fáz životnosti aktíva – od zaradenia po vyradenie. Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie).

3.1.128. FREQ_128 Upozornenia na zmenu stavu, expirácie, servisné intervaly

Automatické notifikácie pri zmene stavu alebo potrebe servisného zásahu. Upozornenia na zmenu stavu, expirácie, servisné intervaly.

3.1.129. FREQ_129 Vytvorenie a editácia záznamov

Základná funkcionalita ticketovacieho systému – vytváranie, editovanie a mazanie ticketov. Vytvorenie a editácia záznamov (ticketov).

3.1.130. FREQ_130 Možnosť meniť stavy ticketu

Schopnosť prepínať medzi rôznymi stavmi ticketu počas jeho životného cyklu. Možnosť meniť stavy ticketu (napr. Nový, V riešení, Uzavretý, Odložený).

3.1.131. FREQ_131 Priradenie na konkrétneho riešiteľa

Priradenie ticketov na konkrétnych riešiteľov vrátane eskalácie podľa úrovne. Priradenie na konkrétneho riešiteľa (L1 analytik, eskalácia L2/L3).

3.1.132. FREQ_132 Emailové notifikácie o zmenách stavu, komentároch, deadline

Automatické emailové notifikácie o zmene stavu, komentároch, deadline. Emailové notifikácie o zmenách stavu, komentároch, deadline.

3.1.133. FREQ_133 Pridávanie príloh

Možnosť pridávať prílohy ako logy, snímky obrazovky a iné dôkazy. Pridávanie príloh (logy, dôkazy, screenshoty, výpisy z nástrojov).

3.1.134. FREQ_134 Možnosť evidovať časy

Sledovanie a evidencia časových údajov pre celý životný cyklus ticketu. Možnosť evidovať časy (vytvorenie, aktualizácia, eskalácia, uzavretie).

3.1.135. FREQ_135 Nastavenie priority a závažnosti incidentu

Nastavenie úrovne priority a závažnosti ticketu pre lepšie plánovanie. Nastavenie priority a závažnosti incidentu.

3.1.136. FREQ_136 Možnosť vytvárať šablóny pre opakujúce sa typy incidentov

Tvorba šablón pre rýchle zadávanie často sa opakujúcich incidentov. Možnosť vytvárať šablóny pre opakujúce sa typy incidentov.

3.1.137. FREQ_137 Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie

Použitie tagov na uľahčenie vyhľadávania a kategorizácie. Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie.

3.1.138. FREQ_138 Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi

Integrácia s inými bezpečnostnými nástrojmi na automatizáciu a workflow. Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi.

3.1.139. FREQ_139 Podpora REST API a Webhookov

Podpora pre rozhrania REST API a Webhooky na komunikáciu s inými systémami. Podpora REST API a Webhookov.

3.1.140. FREQ_140 Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting

Možnosť exportovať tickety pre účely archivácie alebo reportingu. Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting.

3.1.141. FREQ_141 Moderné, responzívne webové rozhranie

Moderný a responzívny dizajn pre pohodlné používanie. Moderné, responzívne webové rozhranie.

3.1.142. FREQ_142 Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete

Zaznamenávanie všetkých akcií, zmien a komentárov v tickete. Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete.

3.1.143. FREQ_143 Možnosť spätného prehľadu a forenznej analýzy

Schopnosť spätne analyzovať priebeh a históriu incidentov. Možnosť spätného prehľadu a forenznej analýzy.

3.1.144. FREQ_144 Tvorba a správa prípadov - cases s úlohami a detailmi

Možnosť vytvárať incidenty ako prípady s úlohami, popisom a atribútmi. Tvorba a správa prípadov (cases) s úlohami a detailmi.

3.1.145. FREQ_145 Pridávanie a sledovanie observables

Možnosť sledovať IOC ako súčasť prípadu. Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)

3.1.146. FREQ_146 Prepojenie medzi prípadmi na základe spoločných indikátorov

Automatická alebo manuálna identifikácia súvisiacich incidentov. Prepojenie medzi prípadmi na základe spoločných indikátorov.

3.1.147. FREQ_147 Kategorizácia incidentov pomocou tagov

Možnosť kategorizovať incidenty pomocou štítkov/tagov. Kategorizácia incidentov pomocou tagov.

3.1.148. FREQ_148 Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov

Integrácia na obohatenie IOC a metadát z CTI alebo iných systémov. Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov.

3.1.149. FREQ_149 Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami

Možnosť prispôsobiť platformu podľa potrieb organizácie. Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami.

3.1.150. FREQ_150 Podpora viacerých používateľských rolí

Podpora RBAC pre rôzne roly. Podpora viacerých používateľských rolí – minimálne analytik a administrátor.

3.1.151. FREQ_151 Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi

Schopnosť prevádzkovať systém pre viac entít súčasne. Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi.

3.1.152. FREQ_152 Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy

Možnosť obojsmernej výmeny dát. Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy.

3.1.153. FREQ_153 Export incidentov do formátov CSV, PDF, cez REST API

Export dát pre dokumentáciu alebo reportovanie. Export incidentov do formátov CSV, PDF, cez REST API.

3.1.154. FREQ_154 Logovanie činností analytikov počas riešenia incidentu (audit trail)

Evidencia činností pre forenznú analýzu. Logovanie činností analytikov počas riešenia incidentu (audit trail).

3.1.155. FREQ_155 Jednoduchá správa konfigurácií a aktualizácií

Schopnosť spravovať platformu bez potreby zásahu do kódu. Jednoduchá správa konfigurácií a aktualizácií.

3.1.156. FREQ_156 Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie

Možnosť rozšíriť schému incidentu. Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie.

3.1.157. FREQ_157 Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov

Umožňuje získať úplný časový priebeh incidentu. Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov.

3.1.158. FREQ_158 Zdieľanie prípadov medzi tímami a externými partnermi podľa práv

Podpora riadeného zdieľania prípadov. Zdieľanie prípadov medzi tímami a externými partnermi podľa práv.

3.1.159. FREQ_159 Vytvorenie základného prehľadu stavu bezpečnosti a incidentov

Možnosť vytvárať zhrnutia stavu bezpečnosti, incidentov a aktivity systému. Vytvorenie základného prehľadu stavu bezpečnosti a incidentov.

3.1.160. FREQ_160 Možnosť stiahnuť report alebo automaticky odoslať

Exportovanie reportov manuálne alebo ich plánovaná automatická distribúcia. Možnosť stiahnuť report alebo automaticky odoslať (e-mail, webhook).

3.1.161. FREQ_161 Možnosť výberu obsahu reportu – časové obdobie, typy incidentov

Možnosť filtrovať obsah reportu podľa času, typu alebo zdrojových údajov. Možnosť výberu obsahu reportu – časové obdobie, typy incidentov.

3.1.162. FREQ_162 Plánovanie pravidelných reportov

Možnosť nastaviť generovanie reportov na základe harmonogramu. Plánovanie pravidelných (napr. denných, týždenných) reportov.

3.1.163. FREQ_163 Možnosť generovania jednorazových ad-hoc reportov

Tvorba reportov mimo pravidelného harmonogramu podľa potreby. Možnosť generovania jednorazových ad-hoc reportov.

3.1.164. FREQ_164 Prispôsobenie vizuálnej podoby reportu

Možnosť upraviť vzhľad reportu podľa firemnej identity. Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie).

3.1.165. FREQ_165 Podpora exportu do PDF, CSV, JSON

Možnosť exportovať reporty do rôznych bežných formátov. Podpora exportu do PDF, CSV, JSON.

3.1.166. FREQ_166 Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI

Možnosť zbierať údaje z iných systémov a vytvárať prepojené reporty. Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI a pod.

3.1.167. FREQ_167 Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy

Vizualizácia dát priamo v reportoch rôznymi formami. Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy.

3.1.168. FREQ_168 Podpora rôznych zdrojov: databázy, logy, API výstupy

Schopnosť agregovať dáta z viacerých technických a analytických zdrojov. Podpora rôznych zdrojov: databázy, logy, API výstupy.

3.1.169. FREQ_169 Webové/GUI rozhranie pre tvorbu a správu reportov

Používateľsky prívetivé rozhranie pre návrh, úpravu a správu reportov. Webové/GUI rozhranie pre tvorbu a správu reportov.

3.1.170. FREQ_170 Možnosť archivácie vygenerovaných reportov

Možnosť uchovávať reporty pre spätnú analýzu a audit. Možnosť archivácie vygenerovaných reportov.

3.1.171. FREQ_171 Možnosť obmedziť prístup k reportom podľa rolí – RBAC

Prístup k reportom riadený rolami a oprávneniami. Možnosť obmedziť prístup k reportom podľa rolí (RBAC).

3.1.172. FREQ_172 Šifrované prenosy reportov pri automatickej distribúcii

Bezpečný prenos citlivých dát cez šifrované kanály. Šifrované prenosy reportov pri automatickej distribúcii.

3.1.173. FREQ_173 Vytváranie, editácia a verzovanie záznamov

Možnosť vytvárať, upravovať a sledovať verzie dokumentov s históriou zmien. Vytváranie, editácia a verzovanie záznamov (návody, playbooky, FAQ).

3.1.174. FREQ_174 Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky

Organizácia KB dokumentov podľa štruktúrovaných pravidiel (kategórie, tagy, sekcie). Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky (tags).

3.1.175. FREQ_175 Fulltextové vyhľadávanie s podporou filtrov a tagov

Vyhľadávanie v KB s možnosťou filtrovania podľa tagov, kategórií a obsahu. Fulltextové vyhľadávanie s podporou filtrov a tagov.

3.1.176. FREQ_176 Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov

Možnosť prepojenia znalostných článkov s konkrétnymi typmi útokov a incidentmi v iných nástrojoch. Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov..

3.1.177. FREQ_177 Možnosť vkladať obrázky, logy, odkazy a prílohy

Schopnosť obohatiť dokumenty o multimediálny alebo dátový obsah. Možnosť vkladať obrázky, logy, odkazy a prílohy.

3.1.178. FREQ_178 Podpora RBAC

Riadenie prístupu podľa používateľských rolí. Podpora RBAC – rôzne úrovne prístupu pre čítanie, editáciu, schvaľovanie.

3.1.179. FREQ_179 Možnosť integrácie s ticketingom, incident managementom, SIEM

Prepojenie KB s inými systémami pre efektívnejšie používanie obsahu. Možnosť integrácie s ticketingom, incident managementom, SIEM.

3.1.180. FREQ_180 Export dokumentov do PDF, HTML alebo Markdown formátu

Možnosť exportu dokumentov na offline použitie alebo publikovanie. Export dokumentov do PDF, HTML alebo Markdown formátu.

3.1.181. FREQ_181 Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov

Používateľsky prívetivé GUI pre správu znalostí. Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov.

3.1.182. FREQ_182 Zachovanie histórie zmien s možnosťou obnovy staršej verzie

Sledovanie a archivácia zmien pre každý dokument. Zachovanie histórie zmien s možnosťou obnovy staršej verzie..

3.1.183. FREQ_183 Záznamy o tom, kto a kedy upravoval dokument

Audit trail zmien dokumentov s informáciou o autoroch a čase. Záznamy o tom, kto a kedy upravoval dokument.

3.1.184. FREQ_184 Možnosť tvorby schvaľovacích workflow pre nové KB články

Procesy schvaľovania pre publikáciu nových článkov. Možnosť tvorby schvaľovacích workflow pre nové KB články.

3.1.185. FREQ_185 Presnosť detekcie anomálií

Riešenie musí zabezpečiť vyhodnotenie presnosti detekcie anomálií (Precision, Recall, F1). Ako presne algoritmus deteguje anomálie bez ohľadu na triedu. Vyhodnotenie celkovej presnosti pomocou metrík ako Precision, Recall, F1-score alebo AUC-ROC.

3.1.186. FREQ_186 Miera falošných poplachov

Riešenie musí zabezpečiť vyhodnotenie miery falošných poplachov (False Positives/Negatives). Ako často algoritmus generuje falošné pozitíva/negatívaZníženie miery falošných poplachov je kľúčové pre použiteľnosť v SOC. Ideálne modely majú veľmi nízky počet FP/FN.

3.1.187. FREQ_187 Podpora učenia bez labelov

Riešenie musí zabezpečiť podporu učenia bez labelov (unsupervised). Schopnosť učiť sa zo vstupných dát bez potreby anotácií. Nie všetky modely vyžadujú označené dáta. Unsupervised modely sú výhodné najmä pri veľkých množstvách nelabelovaných údajov.

3.1.188. FREQ_188 Výpočtová náročnosť AI/ML

Riešenie musí byť škálovateľné pre výpočtová náročnosť (CPU/GPU, pamäť). Zdroje požadované na trénovanie a inferenciu modelu. Rôzna záťaž na výpočtové zdroje vrátane náročnosti na GPU, RAM a trvanie trénovania.

3.1.189. FREQ_189 Rýchlosť inferencie

Riešenie musí zabezpečiť vyhodnotenie rýchlosti inferencie (čas detekcie). Rýchlosť odozvy pri detekcii. Ako rýchlo dokáže model poskytnúť výsledok na nové dáta. Kritické pre nasadenie v reálnom čase.

3.1.190. FREQ_190 Robustnosť voči zmene distribúcie dát

Riešenie musí zabezpečiť robustnosť voči zmene distribúcie dát (drift, noise). Odolnosť voči šumu, zmenám v dátach alebo útokomModel musí byť odolný voči neočakávaným zmenám, fluktuáciám alebo noise, inak prestane fungovať správne.

3.1.191. FREQ_191 Schopnosť práce s časovo-sekvenčnými dátami

Riešenie musí byť schopné práce s časovo-sekvenčnými dátami. Vhodnosť pre dáta s časovým vývojom (napr. logy, sieťová prevádzka). Schopnosť zachytiť dočasné vzory a anomálie v časových radoch. Výhodou sú architektúry ako LSTM, Transformer.

3.1.192. FREQ_192 Flexibilita vstupných údajov

Riešenie musí byť schopné zabezpečiť flexibilitu vstupných údajov (logy, metriky, tokové dáta). Koľko typov dát model zvládne bez potreby úpravy architektúry. Model musí vedieť pracovať so štruktúrovanými i neštruktúrovanými vstupmi – logy, metriky, sieťové toky.

3.1.193. FREQ_193 Adaptívne/online učenia

Riešenie musí mať možnosť adaptívneho/online učenia. Podpora aktualizácie modelu počas prevádzky bez retrénovaniaSchopnosť aktualizovať model bez nutnosti úplného retrénovania, napr. pomocou online learningu.

3.1.194. FREQ_194 Vysvetliteľnosti modelu

Riešenie musí mať vysvetliteľný model (interpretability). Možnosť vysvetliť výstup detekcie analytikovi. Možnosť poskytnúť analytikovi zrozumiteľné vysvetlenie, prečo bola anomália detegovaná.

3.2. Ne-funkčné požiadavky

3.2.1. NREQ_001 Základné organizačné roly

V kontexte návrhu SOCaaS pre projekt INNOSOC boli definované základné organizačné roly, ktoré má systém byť schopný zabezpečiť a spravovať:

- **Level 1 (L1) analytik:** Prvá línia obrany, ktorá monitoruje výstrahy, vykonáva počiatočnú validáciu incidentov a zabezpečuje ich dokumentovanie. Typicky pracuje so SIEM dashboardmi, ticketingovým systémom a databázou znalostí.
- **Level 2 (L2) analytik:** Skúsenejší analytik, ktorý preberá eskalované prípady od L1. Vykonáva hlbšiu analýzu, využíva korelačné pravidlá, threat intelligence a spolupracuje na tvorbe reakčných opatrení. Často využíva rozhrania SOAR nástrojov a forenzné nástroje.
- **Level 3 (L3) špecialista/inžinier:** Odborník na zložité incidenty, pokročilý threat hunting, tvorbu detekčných pravidiel a konfiguráciu nástrojov ako SIEM či EDR. Zapája sa aj do architektúry a automatizácie reakcií.
- **Vedúci SOC (SOC manager):** Zodpovedá za prevádzku a kapacity SOC tímu, SLA, spoluprácu so zákazníkmi, reporting a kontrolu výkonnosti. Koordinuje ľudské aj technologické zdroje, vrátane plánovania zmien, monitorovania kvality reakcií a rozvoja tímu.
- **Incident handler/incident response lead:** Rola zodpovedná za koordináciu reakcie na incident – plánovanie úloh, zber dôkazov, komunikáciu so zainteresovanými stranami a tvorbu záverečných reportov.
- **Threat Intelligence analytik:** Zodpovedá za prácu s hrozbami z CTI zdrojov, tvorbu profilov útočníkov, obohacovanie incidentov o IOC a TTP, sledovanie trendov a zdieľanie výstrah.

- **Správca systémov a architektúry SOC:** Technická rola zodpovedná za nasadenie, správu a aktualizáciu všetkých komponentov SOCaaS architektúry vrátane ELK Stacku, SOAR, asset managementu a iných nástrojov.

Tieto roly nie sú rigidné – môžu sa líšiť v závislosti od veľkosti SOC tímu, štruktúry zákazníkov a SLA. V prostredí multitenantnej SOCaaS architektúry je kľúčová aj schopnosť priraďovať analytikov jednotlivým zákazníkom, prípadne ich delegovať na rôzne typy úloh podľa priority a kapacity.

3.2.2. NREQ_002 Modularita a architektúra

Modularita architektúry zásadne ovplyvňuje rozšíriteľnosť a škálovateľnosť riešenia. Platforma, ktorá je rozdelená do samostatných komponentov (napr. Nova – compute, Neutron – networking, Cinder – block storage), umožňuje nezávislé nasadzovanie, ladenie a výmenu modulov podľa potrieb. Taktiež je výhodné, ak platforma podporuje modernú architektúru mikroslužieb, pluginy, kontajnerizáciu a orchestračné vrstvy. Vyššia modularita zároveň znižuje riziko výpadku celého systému pri poruche jednej služby.

3.2.3. NREQ_003 Náročnosť nasadenia a správy

Je požadované jednoduché nasadenie riešenia, inicializáciu platformy a jej následnú správu s potrebnou znalostnoťou. Napríklad niektoré open-source platformy sú vysoko konfigurovateľné, ale môžu byť komplexné na nasadenie, čo si vyžaduje skúsený tím alebo využitie automatizačných nástrojov (napr. Ansible skripty a pod.).

3.2.4. NREQ_004 Podpora, dostupnosť dokumentácie a komunita

Riešenie musí byť schopné bežať 24/7 a mať dané SLA parametre. Pri open-source riešeniach je dôležitá veľkosť a aktivita komunity – počet prispievateľov, frekvencia vydávania nových verzií a opráv chýb, dostupnosť dokumentácie a znalostnej bázy. Silná komunita a podpora od veľkých IT firiem sú zárukou dlhodobej udržateľnosti projektu.

3.2.5. NREQ_005 Autentifikácia a riadenie prístupov

Platforma musí obsahovať zabudované bezpečnostné prvky potrebné na ochranu infraštruktúry a dát v prostredí SOC. Sem patrí napríklad podpora pre viacúrovňovú autentifikáciu a autorizáciu užívateľov, možnosť šifrovania dát (v úložiskách, prenosoch), logovanie a auditovanie udalostí či automatizované bezpečnostné politiky.

3.2.6. NREQ_006 Izolácia tenantov a ochrana dát

Riešenie musí zaručiť striktnú izoláciu medzi jednotlivými zákazníkmi (tenantmi) – ich virtuálne stroje, úložiská a siete musia byť oddelené tak, aby sa zabránilo neoprávnenému prístupu alebo úniku dát medzi tenantmi. Zabezpečiť oddelenie výpočtových zdrojov, sieťovú segmentáciu, mechanizmy kontroly prístupu a podobne. Miera izolácie dát medzi tenantmi je zásadným aspektom multitenantných systémov.

3.2.7. NREQ_007 Sieťová/monitorovacia integrácia

Prepojiteľnosť a možnosť integrácie s nástrojmi pre monitoring a bezpečnostné dohľadové systémy – najmä SIEM, IDS/IPS (napr. Suricata, Snort), ako aj metrické/logovacie nástroje ako Ceilometer, Grafana, Prometheus. Zohľadňuje tiež schopnosť platformy exportovať bezpečnostné udalosti, podporu API/webhookov a možnosti integrácie s externými bezpečnostnými prvkami.

3.2.8. NREQ_008 Bezpečnostné testovanie

Pred spustením do produkčnej prevádzky musí byť vykonané bezpečnostné a penetračné testovanie v zmysle vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 o riadení projektov.

3.2.9. NREQ_009 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679

Riešenie musí byť v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (GDPR) a v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

3.2.10. NREQ_010 Zákon č. 69/2018

Riešenie musí byť v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

3.3. Technické požiadavky

3.3.1. TREQ_001 Výkonnosť a škálovateľnosť

Riešenie dokáže efektívne využívať zdroje, je potrebné vedieť limity z hľadiska počtu VM, kontajnerov či tenantov, a aké mechanizmy automatického škálovania podporuje. Dôležitá je aj latencia a celkový výkon pri spracovaní údajov, najmä v reálnom čase pre účely monitoringu bezpečnostných udalostí. Riešenie musí byť schopné rásť s počtom VM, tenantov a služieb. Potreba zabezpečiť horizontálnu a vertikálnu škálovateľnosť. V podmienkach projektu potrebujeme platformu, ktorá dokáže rásť spolu s počtom klientov SOC služby a objemom spracovávaných dát.

3.3.2. TREQ_002 Spoľahlivosť a stabilita

Riešenie musí byť stabilné v produkčnej prevádzke a obsahovať mechanizmy pre vysoko dostupné nasadenie. Možnosť nasadiť komponenty redundantne (HA – High Availability). V prostredí bezpečnostného centra je dôležité minimalizovať prestoje a zaistiť nepretržitú dostupnosť služby. Pri hodnotení cloudových služieb sa odporúča dôkladne preskúmať minulú výkonnosť, spokojnosť zákazníkov a zvládanie neplánovaných výpadkov. Rovnako porovnávame SLA (Service Level Agreement) ak sú k dispozícii – hoci v prípade open-source platformy ide skôr o interné garancie, dostupnosť podpory atď.

3.3.3. TREQ_003 Súlad so štandardmi a interoperabilita

Riešenie musí podporovať otvorené štandardy a bežné technológie, čo podmieňuje jej interoperabilitu s inými systémami. Riešenie by malo byť kompatibilné s populárnymi hypervízormi, sieťovými protokolmi, úložiskovými technológiami a rozhraniami pre správu (napr. OpenStack API je de facto štandard pre open-source cloudy). Široká podpora štandardov zároveň uľahčuje integráciu a minimalizuje riziko proprietárnych obmedzení. V prípade využitia Open Source, je potrebné aby platforma vychádzala z osvedčených open-source projektov podporovaných veľkou komunitou. V našom riešení interoperabilita umožní v budúcnosti prepojenie viacerých cloudových prostredí a integráciu ďalších komponentov.

3.3.4. TREQ_004 Dostupnosť

Riešenie musí zabezpečiť vysokú dostupnosť v súlade s požadovanými parametrami na prevádzku KDS:

- Prevádzkový čas 24/7,
- RTO, RPO a Uptime pre jednotlivé služby:
- RTO < 60 min
- RPO 24 h
- Uptime 99,5%

3.3.5. TREQ_005 Škálovanie

Riešenie musí umožniť modulárnosť riešenia s možnosťou vertikálneho a horizontálneho škálovania samostatných blokov podľa požiadaviek implementovaného riešenia.

3.3.6. TREQ_006 Virtualizácia

Riešenie musí byť prevádzkovateľné vo virtualizovanom prostredí.

3.3.7. TREQ_007 Kontajnerizácia

Riešenie musí v prípade potreby vedieť využívať kontajnerizáciu.

3.3.8. TREQ_008 Orchestrácia

Riešenie musí v prípade potreby vedieť viužívať orchestračné nástroje.

3.3.9. TREQ_009 Bezpečnostné logy

Riešenie musí zabezpečiť zaznamenávanie bezpečnostných logov v zmysle ZoITVS č. 95/2019 Z.z., vyhlášky č. 179/2020 Z. z. príloha č. 2 odsek "K. Zaznamenávanie udalostí a monitorovanie", Kategória II, bod e), a ZoKB č. 69/2018 Z. z. a jeho vykonávacej vyhlášky 362/2018 vznp paragraf 15.

3.3.10. TREQ_010 Podpora mikroslužieb

Architektúra musí byť založená na samostatne nasaditeľných službách (microservices), z ktorých každá má vlastné API. Každá služba musí byť nezávisle verziovateľná a škálovateľná.

3.3.11. TREQ_011 CI/CD a orchestrácia

Zavedenie pipeline pre build-test-deploy cyklus. Podpora GitOps, CI, automatizovaný lint, scan, testy, rollout.

3.3.12. TREQ_012 Kompatibilita s OSS

Všetky súčasti systému musia byť postavené na open-source technológiách. Licencie musia umožňovať úpravy a ďalšie šírenie.

3.3.13. TREQ_013 Formáty dát

Systém musí spracovávať JSON, YAML, STIX/TAXII (CTI), Syslog, NetFlow/IPFIX. Musí byť zabezpečená normalizácia logov.

3.3.14. TREQ_014 Prístupová architektúra

Prístup do systému má byť riadený napr. cez NGINX Ingress alebo HAProxy. Pre interný prístup má byť použitý VPN server (napr. WireGuard/OpenVPN). Podporovaná TLS

1.3, forward secrecy.

3.3.15. TREQ_015 Bezpečné API

Každé API rozhranie musí podporovať HTTPS (TLS 1.3), autorizáciu cez OAuth2/JWT. API musí byť chránené pred DoS cez rate limiting, throttling a auditovanie prístupov.

3.3.16. TREQ_016 Auditovateľnosť

Každá zmena konfigurácie, interakcia s API, akcia používateľa a incident musí byť logovaná do centralizovaného auditného úložiska.

3.3.17. TREQ_017 Modulárne riešenie

Riešenie musí umožniť dynamické pridávanie plug-inov bez reštartu jadra. Pluginy musia byť izolované (napr. sidecar kontajnery alebo sandboxy).

3.3.18. TREQ_018 Multitenantný deployment

Každý tenant musí mať oddelené namespace, databázu, dashboardy a logy. Musí byť možné nakonfigurovať SLA politiky na úrovni tenanta.

3.3.19. TREQ_019 TLS/SSL šifrovanie

Všetky komunikácie medzi komponentmi (interne aj externe) musia byť šifrované pomocou TLS 1.3. Podpora HSTS, forward secrecy a možnosť vzájomnej autentifikácie cez client certifikáty.

3.3.20. TREQ_020 Riadenie prístupu (RBAC/ABAC)

Riešenie musí podporovať riadenie prístupu na základe rolí (RBAC) a voliteľne na základe atribútov (ABAC). Autentifikácia môže prebiehať cez SSO/OAuth2/SAML.

3.3.21. TREQ_021 Bezpečná správa tajného úložiska

Heslá, API kľúče, certifikáty a tokeny musia byť uložené v tajnom úložisku.

3.3.22. TREQ_022 Bezpečné logovanie a detekcia anomálií

Riešenie musí vytvárať bezpečnostné logy, ktoré umožňujú detekciu podozrivého správania (napr. brute force, neobvyklé API prístupy). Požaduje sa integrácia s SIEM.

3.3.23. TREQ_023 Ukladanie logov a dát

Logy z endpointov, sietí, bezpečnostných systémov a komponentov musia byť udržiavané podľa politiky retenčného obdobia (napr. 12 mesiacov). Dátové úložisko musí podporovať replikáciu a snapshoty.

3.3.24. TREQ_024 Zálohovanie konfigurácií a dashboardov

Riešenie musí zabezpečiť automatické denné zálohovanie konfigurácií, pluginov, playbookov a dashboardov.

3.3.25. TREQ_025 Archivácia a dlhodobé uchovanie

Riešenie musí podporovať automatické presúvanie dát do archívu podľa pravidiel (napr. kompresia, šifrovanie, presun po 90 dňoch).

3.3.26. TREQ_026 Výkon spracovania dát

Riešenie musí spracovať minimálne 10 000 logov za sekundu v reálnom čase s oneskorením < 5 sekúnd.

KĽÚČOVÉ ZDROJE PRE KATALÓG POŽIADAVIEK

Ako hlavný zdroj pre zber a definíciu požiadaviek slúžia výstupy V1 až V9 v rámci ktorých sú uvedené všetky kľúčové informácie.

ZOZNAM ZDROJOV

[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].