PROJEKT

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

Previazané s balíkom KPB4 – Architektúra riešenia

Previazané s výstupom
V10 – Zoznam funkčných a nefunkčných požiadaviek
a V11 – Biznis architektúra

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

OBSAH

1 SIEM (CORE SECURITY ENGINE A ÚLOŽISKO LOGOV?) 4
1.1 FUNKČNÉ POŽIADAVKY 4
1.2 NEFUNKČNÉ POŽIADAVKY 7
2 SPRACOVANIE LOGOV 11
2.1 FUNKČNÉ POŽIADAVKY 11
2.2 NEFUNKČNÉ POŽIADAVKY 12
3 SOAR 15
3.1 FUNKČNÉ POŽIADAVKY 15
3.2 NEFUNKČNÉ POŽIADAVKY 17
4 DETEKCIA POMOCOU ML 20
4.1 FUNKČNÉ POŽIADAVKY 20
4.2 NEFUNKČNÉ POŽIADAVKY 21
5 VIZUALIZÁCIA DÁT 24
5.1 FUNKČNÉ POŽIADAVKY 24
5.2 NEFUNKČNÉ POŽIADAVKY 25
6 ALERTOVANIE 28
6.1 FUNKČNÉ POŽIADAVKY 28
6.2 NEFUNKČNÉ POŽIADAVKY 29
7 EDR/XDR 32
7.1 FUNKČNÉ POŽIADAVKY 32
7.2 NEFUNKČNÉ POŽIADAVKY 34
8 CYBER THREAT INTELLIGENCE – CTI 37
8.1 FUNKČNÉ POŽIADAVKY 38
8.2 NEFUNKČNÉ POŽIADAVKY 40
9 ASSET MANAGEMENT 43
9.1 FUNKČNÉ POŽIADAVKY 43
9.2 NEFUNKČNÉ POŽIADAVKY 44
10 SKENER ZRANITEĽNOSTI 47
10.1 FUNKČNÉ POŽIADAVKY 47
10.2 NEFUNKČNÉ POŽIADAVKY 49
11 ZDROJE BEZPEČNOSTNÝCH ÚDAJOV 52
11.1 FUNKČNÉ POŽIADAVKY 52
11.2 NEFUNKČNÉ POŽIADAVKY 53
12 KNOWLEDGE BASE 56

12.1 FUNKČNÉ POŽIADAVKY 56
12.2 NEFUNKČNÉ POŽIADAVKY 57
13 TICKETING 60
13.1 FUNKČNÉ POŽIADAVKY 60
13.2 NEFUNKČNÉ POŽIADAVKY 61
14 EVIDENCIA A SPRÁVA INCIDENTOV 64
14.1 FUNKČNÉ POŽIADAVKY 64
14.2 NEFUNKČNÉ POŽIADAVKY 65
15 REPORTOVANIE 68
15.1 FUNKČNÉ POŽIADAVKY 68
15.2 NEFUNKČNÉ POŽIADAVKY 69
16 ADMINISTRATÍVA SYSTÉMU 71
16.1 FUNKČNÉ POŽIADAVKY 71
16.2 NEFUNKČNÉ POŽIADAVKY 72
17 VOLITEĽNÉ ROZŠÍRENIA 74
17.1 FUNKČNÉ POŽIADAVKY 74
17.2 NEFUNKČNÉ POŽIADAVKY 75
18 TECHNICKÉ POŽIADAVKY – SUMÁRNE 78
18.1 BEZPEČNOSTNÉ TECHNICKÉ POŽIADAVKY 81
18.2 POŽIADAVKY NA ÚLOŽISKO A ZÁLOHOVANIE 82
18.3 VÝKONNOSTNÉ METRIKY A TECHNICKÉ KPI 83

1 SIEM (CORE SECURITY ENGINE A ÚLOŽISKO LOGOV?)

Úloha v SOC (krátky textový opis):

SIEM agreguje a analyzuje bezpečnostné dáta z rôznych zdrojov, ako sú sieťové zariadenia, servery a aplikácie, a poskytuje real-time analýzu bezpečnostných upozornení. Týmto spôsobom umožňuje SOC tímu identifikovať a reagovať na potenciálne bezpečnostné incidenty rýchlo a efektívne. SIEM využíva pravidlá a algoritmy na koreláciu udalostí, čo pomáha pri identifikácii vzorcov a trendov, ktoré by mohli indikovať bezpečnostné hrozby. SOC tím, ktorý pozostáva z bezpečnostných analytikov, inžinierov a manažérov, využíva SIEM na monitorovanie, analýzu a reakciu na bezpečnostné incidenty. SIEM tiež pomáha pri vytváraní reportov o bezpečnostných udalostiach a poskytuje upozornenia, ak analýza odhalí potenciálny bezpečnostný problém. Spoločne SIEM a SOC umožňujú organizáciám proaktívne monitorovať a reagovať na kybernetické hrozby, čím zvyšujú celkovú bezpečnosť a agilitu organizácie.

Východisko zo zámeru projektu INNOSOC:

SIEM predstavuje jeden z hlavných pilierov navrhovanej cloudovej SOCaaS platformy, ktorá má byť škálovateľná, otvorená, automatizovaná a schopná detekcie anomálií s podporou ML.

Typy požiadaviek na systém:

- **Funkčné**
  - Čo má systém robiť – konkrétne správanie a funkcie.
- **Nefunkčné**
  - Ako má systém fungovať – vlastnosti kvality
- **Technické**
  - Technické špecifiká, platformy, technológie, HW/SW požiadavky, API, kompatibilita.

ISO/IEC/IEEE 29148:2018 - Systems and software engineering — Life cycle processes — Requirements engineering - norma pre **inžinierstvo požiadaviek** (requirements engineering) a **procesy životného cyklu systémov a softvéru.**

1.1 FUNKČNÉ POŽIADAVKY

1. Zber logov bezpečnostných údajov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zber bezpečnostných logov zo všetkých typov zdrojov	Zber logov z rôznych IT zdrojov vrátane serverov, sieťových zariadení, endpointov, kontajnerov a cloudových služieb	Vstupné údaje a zdroje	Systémový integrátor

2. Korelácia udalostí			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Korelácia bezpečnostných udalostí	Definovanie a vykonávanie pravidiel na koreláciu udalostí z viacerých zdrojov s cieľom identifikovať vzory útokov a incidentov.	Spracovanie údajov	Bezpečnostný analytik

3. Detekcia hrozieb			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Detekcia hrozieb v reálnom čase	Spracovávať údajov v reálnom čase a generovanie bezpečnostných upozornení s minimálnym oneskorením.	Časové požiadavky	Bezpečnostný analytik

4. Dashboard			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prehľadné vizualizácie a dashboardy	Vizualizovanie zozbieraných a spracovaných dát formou dashboardov, grafov a prehľadov pre operatívne aj manažérske účely.	Používateľské rozhranie	Bezpečnostný analytik, Manažér bezpečnosti, auditor

5. Reporting			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Tvorba a export reportov	Tvorba pravidelných aj ad-hoc reportov o bezpečnostnom stave, výskyte incidentov a plnení SLA.	Výstupné údaje	Manažér bezpečnosti, auditor

6. Integrácia systémov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia so sprievodnými nástrojmi	Zabezpečenie komunikácie s ostatnými bezpečnostnými systémami cez štandardné API a podporovať výmenu dát.	Rozhrania s inými systémami	Systémový integrátor

7. Zabezpečenie údajov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Šifrovanie a bezpečnosť dát	Ochrana všetkých prenášaných a uložených údajov šifrovaním a prístupovým manažmentom (TLS, RBAC).	Bezpečnostné požiadavky	Bezpečnostný architekt

8. Spracovanie údajov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Škálovateľnosť spracovania dát	Spracovanie veľkého množstva dát s možnosťou horizontálneho škálovania.	Výkonnostné požiadavky	Architekt riešenia

9. Rozšírenia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Rozšíriteľnosť systémových modulov	Dopĺňanie vlastných pravidiel, modulov a rozšírení (pluginov) bez zásahu do jadra.	Adaptabilita	Vývojár, DevOps

10. Nasadenie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Multitenantné kontajnerové nasadenie	Oddelenie zákazníkov (tenantov) a možnosť nasadenia v Kubernetes prostredí.	Architektúra systému a deployment	DevOps inžinier

1.2 NEFUNKČNÉ POŽIADAVKY

1. Podpora OSS			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora otvoreného kódu (open source)	SIEM riešenie musí byť otvorené (open-source), aby bolo možné zabezpečiť transparentnosť, flexibilitu a nízke náklady.	Softvérové obmedzenia	systémový architekt, manažér

2. Výkonové nároky			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Výkonové požiadavky na hardvér (HW požiadavky na zdroje)	Zohľadniť spotrebu RAM, CPU, diskového priestoru a prípadne GPU ak sa používa ML.	Výkon	administrátor

3. OS kompatibilita			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Výkonové požiadavky na hardvér (HW požiadavky na zdroje)	Systém by mal fungovať minimálne na Linux serverových distribúciách.	Prispôsobivosť	systémový integrátor

4. Integrácia s nástrojmi			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia s inými nástrojmi (napr. XDR, vizualizačné nástroje)	SIEM musí podporovať štandardné API pre integráciu so SOAR, EDR, vizualizáciou a pod.	Rozhrania	vývojár integrácie, bezpečnostný analytik

5. Škálovanie systému			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Škálovateľnosť a výkonnostná elasticita (Škálovanie výkonu)	Systém musí zvládnuť dynamický nárast objemu logov a počet zdrojov.	Výkon	architekt riešenia

6. Šifrovanie dát			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Šifrovanie dát pri prenose a v úložisku	TLS/SSL pre prenos, šifrovanie logov v úložisku.	Bezpečnostné požiadavky	bezpečnostný architekt

7. Riadenie prístupu			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**

Riadenie prístupu na báze rolí (RBAC)	Možnosť definovania oprávnení na úrovni používateľa/skupiny.	Bezpečnostné požiadavky	administrátor systému

8. Korelácia udalostí			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Analytické schopnosti a korelácia dát (Korelácia dát)	Automatizovaná korelácia logov z viacerých zdrojov na detekciu incidentov.	Funkčné výkonnostné požiadavky (aj analytické)	bezpečnostný analytik

9. Správa dát			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Normalizácia a archivácia dát	Normalizácia vstupných logov, podpora archivácie, kompresie, vyhľadávania.	Požiadavky na údaje	administrátor, audítor

10. Užívateľské rozhranie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Používateľské rozhranie a UX (GUI)	Intuitívne a konfigurovateľné GUI na správu incidentov a sledovanie stavu systému.	Užívateľské požiadavky na údaje	bezpečnostný analytik

11. Aktualizácie a konfigurácia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora aktualizácií a jednoduchá konfigurácia	Možnosť aktualizácie bez výpadku služby a dostupnosť dokumentácie.	Udržateľnosť	administrátor, devops

12. Multitenancia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora multitenancie	Oddelenie údajov viacerých zákazníkov, samostatné politiky a prístupové práva.	Bezpečnostné a prevádzkové požiadavky	poskytovateľ služby, prevádzkovateľ platformy

13. Regulačná zhoda			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Súlad s legislatívou a normami (napr. GDPR, NIS2)	SIEM musí umožňovať naplniť požiadavky ako uchovávanie údajov podľa legislatívy.	Legislatívne požiadavky	audítor, bezpečnostný manažér

14. Nasaditeľnosť v kontajneroch			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Kontajnerizácia a jednoduché nasadenie (napr. Kubernetes)	Riešenie musí podporovať moderné nasadenie (Docker, Helm charts, Kubernetes).	Inštalačné požiadavky	devops, systémový architekt

2 SPRACOVANIE LOGOV

Úloha v SOC (krátky textový opis):

Zber, normalizácia, filtrácia a ukladanie logov z rôznych zdrojov.

2.1 FUNKČNÉ POŽIADAVKY

1. Zber logov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zber logov z rôznych typov zariadení a systémov	Zber logov z rôznych typov zariadení a systémov vrátane serverov, endpointov, sieťových zariadení a aplikácií.	Vstupné údaje a zdroje	Systémový integrátor

2. Filtrovanie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Normalizácia a filtrovanie logo	Normalizáciu vstupných logov do jednotného formátu a ich filtrovanie podľa definovaných pravidiel.	Spracovanie údajov	Bezpečnostný analytik

3. Vyhľadávanie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Vyhľadávanie v zozbieraných logoch	Rýchle a efektívne vyhľadávanie v zozbieraných logoch, vrátane fulltextu a filtrov.	Používateľské rozhranie	Bezpečnostný analytik

4. Vizualizácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Vizualizácia zozbieraných logov	Kompatibilita s vizualizačnými nástrojmi ako Kibana alebo Grafana.	Výstupné údaje	Analytik, administrátor

5. Rozšírenia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora rôznych modulov na zber logov	Podpora nástrojov ako Fluent Bit, Fluentd, Logstash, OpenTelemetry alebo Graylog na zber logov.	Rozhrania s inými systémami	Systémový integrátor

2.2 NEFUNKČNÉ POŽIADAVKY

1. Viaczdrojový zber			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora viacerých typov logov z rôznych zdrojov	Systém musí byť schopný prijímať logy z rôznych typov zariadení, systémov a cloud služieb (napr. syslog, audit, aplikácie).	Rozhrania	systémový integrátor

2. Normalizácia logov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora normalizácie logov	Pre účely korelácie a spracovania musia byť logy normalizované do jednotného formátu.	Požiadavky na údaje	bezpečnostný analytik, administrátor

3. Vyhľadávanie logov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Výkonné vyhľadávanie a filtrovanie záznamov	Systém musí poskytovať fulltextové a štruktúrované vyhľadávanie, napr. pomocou regulárnych výrazov alebo dotazov.	Výkon	bezpečnostný analytik

4. Vizualizačná kompatibilita			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Kompatibilita s vizualizačnými nástrojmi (napr. Kibana, Grafana)	Logy musia byť spracované tak, aby sa dali efektívne zobrazovať vo vizualizačných nástrojoch.	Interoperabilita	analytik, architekt riešenia

5. Škálovanie spracovania			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora horizontálnej škálovateľnosti	Riešenie musí zvládať vysoký objem dát s možnosťou horizontálneho rozšírenia podľa zaťaženia.	Výkon	systémový architekt, devops

6. Prepojenie so SIEM			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora integrácie so SIEM a ďalšími systémami	Spracovanie logov musí byť pripravené na automatizovaný prenos výstupov do nadriadeného SIEM riešenia.	Rozhrania	systémový integrátor

7. Archivácia logov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Efektívne ukladanie a archivácia logov	Systém musí podporovať archiváciu logov so šifrovaním a kompresiou, pričom musí byť schopný dlhodobého uchovávania.	Bezpečnostné požiadavky	administrátor, audítor

8. Kontajnerizovateľnosť			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora kontajnerizácie	Riešenie má byť ľahko nasaditeľné ako Docker kontajner a konfigurovateľné pre rôzne prostredia.	Inštalačné požiadavky	devops, správca infraštruktúry

3 SOAR

Úloha v SOC (krátky textový opis):

Automatizácia bezpečnostných operácií a orchestrácia reakcií na incidenty napr. pomocou playbookov. Pokročilá automatizácia workflow incidentov naprieč rôznymi systémami.

3.1 FUNKČNÉ POŽIADAVKY

1. Automatizácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Automatizácia reakcií na bezpečnostné incidenty	Definovanie a vykonanie automatických reakcií na bezpečnostné incidenty (napr. izolácia zariadenia, notifikácia tímu, blokovanie IP) prostredníctvom vopred pripravených playbookov.	Spracovanie údajov	Bezpečnostný analytik

2. Kategorizácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Kategorizácia a triedenie incidentov	Triedenie incidentov podľa typu, závažnosti, zdroja, a ich automatické priradenie na riešenie podľa nastavených politík.	Spracovanie incidentov	Bezpečnostný analytik, Incident handler

3. Orchestrácia procesov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Orchestrácia procesov medzi nástrojmi	Koordinovanie akcií naprieč rôznymi nástrojmi (napr. SIEM, CTI, EDR), vrátane automatizovaného volania API, skriptovania a prepojenia reakcií v rámci incident managementu.	Rozhrania s inými systémami	Systémový integrátor

4. Playbook			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Tvorba a úprava playbookov	Vytváranie reakčných scenárov (playbookov) pomocou drag-and-drop alebo skriptovacieho rozhrania bez potreby hlbokých programátorských zručností.	Používateľské rozhranie	Bezpečnostný analytik, DevSecOps

5. Evidencia aj 6 rovnaké			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Evidencia a audit vykonaných akcií	Uchovávanie histórie všetkých vykonaných automatizovaných akcií, reakcií a rozhodnutí v rámci riešenia incidentov, a umožniť ich auditovateľnosť.	Bezpečnostné požiadavky	Auditor, Manažér bezpečnosti

~~6. Evidencia~~			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Evidencia a audit vykonaných akcií	Uchovávanie histórie všetkých vykonaných automatizovaných akcií, reakcií a rozhodnutí v rámci riešenia incidentov, a umožniť ich auditovateľnosť.	Bezpečnostné požiadavky	Auditor, Manažér bezpečnosti

3.2 NEFUNKČNÉ POŽIADAVKY

1. Automatizované scenáre			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora workflow a playbookov (automatizované scenáre reakcie)	SOAR systém musí umožniť definovanie a prevádzku automatizovaných reakcií formou grafických alebo skriptovaných „playbookov“.	Výkonnostné požiadavky	bezpečnostný analytik, systémový integrátor

2. Integrácia s ekosystémom			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť prepojenia na ďalšie systémy (SIEM, EDR, ticketing)	Riešenie musí umožniť priamu integráciu na ostatné bezpečnostné komponenty na výmenu údajov a spúšťanie akcií.	Rozhrania	systémový integrátor

3. Konfigurovateľné playbooky			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Flexibilita v konfigurácii scenárov	Užívatelia musia mať možnosť vytvárať a prispôsobovať playbooky bez nutnosti pokročilých programátorských znalostí.	Používateľské požiadavky	bezpečnostný analytik

4. Audit činností			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zaznamenávanie a audit činností systému	Všetky automatizované akcie, rozhodnutia a reakcie musia byť logované a auditovateľné.	Bezpečnostné požiadavky	audítor, manažér bezpečnosti

5. Kategorizácia incidentov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť kategorizácie incidentov a pravidiel ich riešenia	Systém musí podporovať definovanie rôznych typov incidentov a reakčných stratégií na základe ich triedy, závažnosti a dopadu.	výkonnostné požiadavky	bezpečnostný analytik

6. API rozhranie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Rozhranie pre integráciu s API	SOAR musí poskytovať REST API (alebo podobné) pre externé integrácie a prípadnú nadväznosť na ďalšie systémy (TheHive, Cortex, atď.).	Rozhrania	vývojár, integrátor

7. Reverzná reakcia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora rollback mechanizmu pri zlyhaní reakcie	Riešenie musí byť schopné v prípade chyby alebo neúspechu automatizácie vrátiť zmeny do pôvodného stavu alebo vykonať alternatívnu akciu.	Spoľahlivosť	systémový architekt, analytik

8. Bezpečné akcie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Bezpečnosť spúšťaných akcií a ochrana pred zneužitím	Každá automatizovaná akcia musí prebiehať v kontrolovanom režime a byť oprávnená na základe definovaných prístupových práv	Bezpečnostné požiadavky	správca systému, bezpečnostný architekt

4 DETEKCIA POMOCOU ML

Úloha v SOC (krátky textový opis):

Využitie modelov strojového učenia na podporu činnosti SOC centra, napr. detekciu neznámych hrozieb a anomálií.

4.1 FUNKČNÉ POŽIADAVKY

1. Detekcia anomálií			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Detekcia sieťových a operačných anomálií pomocou ML	Detegovanie anomálií v sieťovej prevádzke, logoch, správaní systémov a používateľov pomocou modelov strojového učenia.	Spracovanie údajov	Bezpečnostný analytik, Data Scientist

2. Predikcia incidentov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Predikcia bezpečnostných incidentov na základe historických dát	Predikovanie potenciálnych incidentov a hrozieb na základe analýzy historických údajov z logov a iných zdrojov.	Výstupné údaje	Analytik, Manažér bezpečnosti

3. Aktualizácia ML			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Tréning a aktualizácia ML modelov	Rozhranie a nástroje pre trénovanie, testovanie a ladenie modelov ML vrátane možnosti aktualizovať modely na základe nových dát.	Adaptabilita	Data Scientist, DevOps

4. Knižnice ML			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora rôznych typov modelov a knižníc	Integrácia rôznych typov algoritmov (napr. klasifikácia, detekcia anomálií) a knižníc ako TensorFlow, PyTorch, scikit-learn.	Rozhrania s inými systémami	Vývojár ML riešení

5. Hodnotenie modelov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Vyhodnocovanie výkonnosti ML modelov	Hodnotenie presnosti, falošne pozitívnych a negatívnych výsledkov a iných metrík výkonnosti ML modelov.	Kvalitatívne požiadavky	Data Scientist, bezpečnostný architekt

4.2 NEFUNKČNÉ POŽIADAVKY

1. Presnosť detekcie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Presnosť detekcie anomálií (napr. sieťových, phishing, spam, malware)	Algoritmy musia byť optimalizované pre nízky počet falošne pozitívnych a falošne negatívnych hlásení.	Presnosť výstupu	bezpečnostný analytik, ML špecialista

2. Rýchlosť reakcie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Rýchlosť spracovania dát a reakcie (real-time detekcia)	Výpočtové operácie ML modelov musia byť navrhnuté tak, aby fungovali s nízkou latenciou v reálnom čase.	Výkon	systémový architekt, ML inžinier

3. Viaczdrojové dáta			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora rôznych typov dát (napr. logy, pakety, sieťové toky, auditné dáta)	Systém musí byť schopný prijímať a spracovávať rôzne typy vstupov pre učenie aj detekciu.	Rozhrania	ML vývojár, systémový integrátor

4. Škálovateľnosť výpočtov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Škálovateľnosť výpočtovej infraštruktúry pre trénovanie a inferenciu	Tréning a nasadenie ML modelov musí byť možné horizontálne rozširovať (napr. cez Kubernetes, GPU clustre).	Výkon	ML inžinier, devops

5. Modulárne modely			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora výberu a ladenia algoritmov (modulárnosť riešenia)	Riešenie má umožniť výber rôznych typov modelov a ich konfigurovateľnosť (napr. supervised/unsupervised learning).	Prispôsobiteľnosť	ML špecialista, vývojár

6. Pipeline pre učenie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zber a príprava dát pre trénovanie modelov (data pipeline)	Musí byť podporený bezpečný, škálovateľný a auditovateľný spôsob zberu, čistenia a prípravy trénovacích dát.	Požiadavky na údaje	ML inžinier, bezpečnostný analytik

7. Správa modelov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zabezpečenie správy a uchovávania ML modelov (verzie, audity)	Modely musia byť spravované ako artefakty (verzie, revízie, auditné záznamy).	Udržateľnosť	ML vývojár, architekt

8. Vysvetliteľnosť modelu			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť vysvetlenia výsledku ML modelu (explainability)	Systém má poskytovať vysvetlenie výsledkov modelu (napr. LIME, SHAP), aby analytik vedel pochopiť, prečo model klasifikoval udalosť ako hrozbu.	Použiteľnosť / Auditovateľnosť	bezpečnostný analytik, manažér

9. Integrácia výstupov ML			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia ML výstupov do ostatných komponentov (napr. SIEM, SOAR)	Výsledky detekcie musia byť zdieľateľné so SIEM a SOAR pre ďalšie spracovanie.	Rozhrania	systémový integrátor

5 VIZUALIZÁCIA DÁT

Úloha v SOC (krátky textový opis):

Poskytovanie prehľadných a interaktívnych dashboardov pre vizuálnu analýzu bezpečnostných údajov.

5.1 FUNKČNÉ POŽIADAVKY

1. Dashboard			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Tvorba interaktívnych dashboardov	Vytváranie a spravovanie interaktívnych dashboardov, ktoré zobrazujú stav bezpečnostného prostredia, incidenty, výkonnostné metriky a ďalšie kľúčové ukazovatele.	Používateľské rozhranie	Bezpečnostný analytik, manažér bezpečnosti

2. Šablóna			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora šablón pre rôzne typy vizualizácií	Možnosť tvorby a používania preddefinovaných šablón pre rôzne scenáre (napr. NIS2 monitoring, SLA reporty, anomálie).	Výstupné údaje	Bezpečnostný analytik

3. SIEM integrácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia vizualizačného modulu so SIEM a logovacím systémom	Prepojenie so SIEM/logovacím backendom, pre zobrazenie údajov z rôznych zdrojov v reálnom čase	Rozhrania s inými systémami	Systémový integrátor

4. Prihlásenie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora SSO autentifikácie	Prístup k vizualizačnému rozhraniu prostredníctvom jednotného prihlásenia (SSO) s prístupovými právami viazanými na rolu používateľa.	Bezpečnostné požiadavky	Administrátor, bezpečnostný architekt

5. Korelácie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Korelácia dát vo vizualizáciách	Zobrazovanie výsledkov korelačných pravidiel a prehľadné znázornenie ich vzťahov (napr. časové línie, sieťové väzby).	Vizuálna analytika	Bezpečnostný analytik

5.2 NEFUNKČNÉ POŽIADAVKY

1. Grafické rozhranie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Grafické používateľské rozhranie (GUI)	Riešenie musí mať intuitívne a prehľadné GUI rozhranie, ktoré umožní jednoduchú orientáciu a správu bezpečnostných údajov.	Používateľské požiadavky	bezpečnostný analytik, operátor

2. Konfigurovateľné dashboardy			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť tvorby a úpravy dashboardov	Užívatelia musia mať možnosť vytvárať vlastné vizualizácie, meniť widgety a panely podľa potrieb.	Prispôsobiteľnosť	analytik, vedúci tímu SOC

3. Vizualizačné šablóny			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora šablón a vizualizačných predlôh	Systém má podporovať preddefinované šablóny pre rôzne typy reportov (napr. podľa typu hrozby, assetu, služby).	Efektivita použitia	analytik, manažér

4. Jednotné prihlásenie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
SSO autentifikácia do vizualizačného nástroja	Podpora centralizovanej autentifikácie (napr. SAML, LDAP, OAuth2) pre jednoduchý a bezpečný prístup.	Bezpečnostné požiadavky	správca systému, prevádzkovateľ

5. Korelačné vizualizácie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Korelačné pravidlá a ich vizualizácia	Vizualizačný systém má podporovať zobrazenie výsledkov korelácie udalostí a ich časových alebo kauzálnych väzieb.	Funkčné výkonnostné požiadavky	bezpečnostný analytik

6. Prepojenie dát

Zameranie	Popis	ISO/IEC/IEEE 29148:2018 kategória	Rola
Integrácia na externé dáta a systémy (napr. CTI, SIEM)	Vizualizačné komponenty musia umožniť získavanie a prepájanie údajov z viacerých zdrojov.	Rozhrania	systémový integrátor

7. Dynamická aktualizácia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Reagovanie na zmenu dát v reálnom čase (live refresh)	Zobrazenia sa musia vedieť automaticky aktualizovať pri príchode nových dát bez manuálneho zásahu.	Výkon	operátor, analytik, integrátor

8. Jazyková lokalizácia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora viacjazyčnosti a lokalizácie rozhrania	GUI by malo byť lokalizované, minimálne do slovenského a anglického jazyka.	Použiteľnosť	koncový používateľ

9. Záloha vizualizácií			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zálohovanie konfigurácií dashboardov	Možnosť exportu/nahratia konfigurácie dashboardov pre účely zálohy alebo migrácie.	Udržateľnosť	administrátor systému

6 ALERTOVANIE

Úloha v SOC (krátky textový opis):

Notifikácie v reálnom čase o bezpečnostných incidentoch na základe definovaných pravidiel.

6.1 FUNKČNÉ POŽIADAVKY

1. Automatizácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Generovanie notifikácií o bezpečnostných udalostiach	Automatické generovanie notifikácií na základe definovaných bezpečnostných pravidiel alebo detekovaných udalostí.	Výstupné údaje	Bezpečnostný analytik

2. Pravidlá			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Definovanie pravidiel pre upozornenia	Nastavenie podmienok pre generovanie upozornení (napr. kombinácie zdrojov, závažnosť, typ incidentu).	Spracovanie údajov	Bezpečnostný analytik, administrátor

3. Odosielanie notifikácií			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Oznámenia prostredníctvom e-mailu a ďalších kanálov	Odosielanie notifikácií e-mailom, prípadne integráciu s ďalšími notifikačnými kanálmi ako SMS, Slack, MS Teams.	Rozhrania s inými systémami	Administrátor, manažér bezpečnosti

4. Automatické vypĺňanie alertu			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Oznámenia prostredníctvom e-mailu a ďalších kanálov	Automatické generovanie názvu a popisu alertu na základe obsahu incidentu a kontextu (napr. zdroj, cieľ, typ hrozby).	Automatizácia procesov	Bezpečnostný analytik

5. Okamžité upozornenia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora alertov v reálnom čase	Okamžité generovanie a doručovanie alertov v reálnom čase bez oneskorenia, najmä pre kritické incidenty.	Časové požiadavky	SOC operátor

6.2 NEFUNKČNÉ POŽIADAVKY

1. Reálne časy alertov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora real-time notifikácií o incidentoch	Systém musí poskytovať upozornenia okamžite po splnení definovaných podmienok (napr. detekcia hrozby).	Výkon	bezpečnostný analytik, operátor

2. Viackanálové doručenie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Viacero kanálov pre upozornenie (e-mail, syslog, API, webhook, chat)	Alerty musia byť doručiteľné viacerými spôsobmi, podľa typu a úrovne incidentu.	Rozhrania	prevádzkový tím, správca systému

3. Prispôsobenie alertov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť prispôsobiť predmet a obsah notifikácií	Používateľ musí mať možnosť nastaviť, čo sa zobrazí v tele a predmete upozornenia (napr. závažnosť, typ incidentu).	Používateľské požiadavky	analytik, vedúci SOC

4. Eskalačné pravidlá			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora eskalácie podľa definovaných pravidiel (napr. SLA)	Systém má umožniť preposlanie alertu na inú úroveň alebo osobu, ak sa nereaguje v čase.	Správa incidentov	manažér bezpečnosti, SLA operátor

5. Audit alertov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zachytávanie a auditovanie všetkých alertov	Alerty musia byť archivované a dostupné na audit a analýzu spätne.	Bezpečnostné požiadavky	audítor, manažér SOC

6. Podmienkové pravidlá			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora podmieneného generovania alertov (logika „ak-tak“, korelácia)	Alertovanie musí podporovať pokročilé logické podmienky vrátane korelácie z viacerých zdrojov.	výkonnostné požiadavky	bezpečnostný analytik

7. Šifrované alerty

Zameranie	Popis funkcie	ISO/IEC/IEEE 29148:2018 kategória	Rola
abezpečený prenos upozornení (napr. TLS)	Alerty zasielané e-mailom alebo cez sieť musia využívať zabezpečený prenos.	Bezpečnostné požiadavky	správca systému

8. Prepojenie s reakciou			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora integrácie s ticketingom a SOAR	Alerty musia byť schopné automaticky zakladať tikety alebo spúšťať playbooky.	Rozhrania	bezpečnostný analytik, systémový integrátor

7 EDR/XDR

Úloha v SOC (krátky textový opis):

Systém EDR (Endpoint Detection and Response) zohráva v SOC (Security Operations Center) kľúčovú úlohu pri zabezpečení kybernetickej bezpečnosti. EDR neustále monitoruje aktivitu na koncových zariadeniach, ako sú počítače a servery, a zbiera dáta, ktoré môžu indikovať hrozbu. Získané dáta sú analyzované na identifikáciu vzorcov hrozieb, pričom EDR využíva pravidlá a algoritmy na automatické rozpoznanie podozrivej aktivity. Pri identifikácii hrozby môže EDR automaticky reagovať, napríklad izolovať infikované zariadenie alebo eliminovať hrozbu. EDR tiež informuje bezpečnostný tím o identifikovaných hrozbách, čo umožňuje rýchlu reakciu a riešenie incidentov. Okrem toho poskytuje nástroje na podrobnú forenznú analýzu hrozieb a vyšetrenie podozrivej aktivity, čo pomáha pri identifikácii zdroja a rozsahu útoku. Tieto funkcie umožňujú SOC efektívne spravovať kybernetické riziká a chrániť organizáciu pred potenciálnymi útokmi.

7.1 FUNKČNÉ POŽIADAVKY

1. Monitorovanie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Monitorovanie aktivít na koncových zariadeniach	Nepretržité monitorovanie správania a aktivity koncových zariadení (PC, servery, kontajnery) za účelom detekcie podozrivých činností.	Vstupné údaje a zdroje	Bezpečnostný analytik

2. Detekcia hrozieb			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Detekcia a analýza hrozieb na endpointoch	Identifikovanie známej aj neznámej hrozby na základe pravidiel, správania alebo ML modelov, a analyzovať ju.	Spracovanie údajov	SOC analytik, Forenzný analytik

3. Reakcia na incident			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Reakcia na incidenty na koncových zariadeniach	Automatické alebo manuálne vykonanie opatrení ako izolácia zariadenia, ukončenie procesu, odstránenie súboru.	Výstupné údaje	Bezpečnostný analytik

4. Zber auditných údajov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zber a spracovanie auditných údajov	Zber auditných logov, kontrolu integrity súborov (FIM), sieťových pripojení a procesov z endpointov.	Vstupné údaje a zdroje	Bezpečnostný analytik, Administrátor systému

5. Dashboard			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Dashboardy pre vizualizáciu a správu EDR	Prehľadné rozhranie na sledovanie stavu zariadení, incidentov, histórie zásahov a bezpečnostného skóre.	Používateľské rozhranie	SOC operátor, manažér bezpečnosti

6. Preposielanie incidentov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Odozva incidentov do SOC systému	Automatické odoslanie informácie o incidente do centrálneho systému SOC (napr. SIEM, SOAR) vrátane metadát.	Rozhrania s inými systémami	Systémový integrátor

7.2 NEFUNKČNÉ POŽIADAVKY

1. Podpora viacerých prostredí			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora rôznych prostredí (cloud, kontajnery, servery, on-premise)	Riešenie musí byť schopné fungovať na širokom spektre platforiem vrátane hybridných infraštruktúr.	Prispôsobiteľnosť	architekt, správca systému

2. Flexibilný zber dát			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Bezagentový a agentový režim zberu dát	Podpora nasadenia agentov, ale aj zberu bez nutnosti inštalácie podľa typu zariadenia.	Interoperabilita	integrátor, administrátor

3. Viacdátový zber			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zber rôznych typov údajov (logy, metriky, integrita súborov, sieťové dáta)	Riešenie musí vedieť zbierať rôzne bezpečnostné údaje potrebné pre detekciu incidentov a ML analýzu.	Požiadavky na údaje	analytik, ML špecialista

4. Detekcia hrozieber			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Detekcia a klasifikácia malvéru, narušení, podozrivého správania	Musí byť podporovaná schopnosť rozpoznať rôzne typy útokov pomocou pravidiel alebo ML.	Funkčné výkonnostné požiadavky	bezpečnostný analytik

5. Automatická reakcia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Automatizovaná reakcia (napr. izolácia zariadenia, blokovanie procesu)	Možnosť konfigurovať automatické akcie po detekcii hrozby.	Prevádzkové požiadavky	operátor, analytik

6. Vizualizácia EDR dát			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Vizuálne dashboardy pre prehľad a správu incidentov	Prehľadné GUI rozhranie pre správu detekcií, výstrah a incidentov.	Používateľské požiadavky	analytik, operátor

7. Prepojenie s tiketmi			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Notifikácie a integrácia na ticketing systém	EDR systém má posielať alerty a zakladať tikety automaticky alebo poloautomaticky.	Rozhrania	SOC tím, IT podpora

8. Export dát			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť exportu dát pre ďalšie spracovanie (SIEM, ML)	Systém musí podporovať export dát vo formáte vhodnom na koreláciu alebo učenie..	Rozhrania / interoperabilita	ML analytik, integrátor

9. Bezpečné dáta			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zabezpečenie údajov (šifrovanie, prístupové práva)	Všetky prenášané a uchovávané dáta musia byť chránené proti neoprávnenému prístupu.	Bezpečnostné požiadavky	správca, bezpečnostný architekt

8 CYBER THREAT INTELLIGENCE – CTI

Úloha v SOC („krátky“ textový opis)**:**

CTI poskytuje aktuálne informácie o hrozbách, ktoré pomáhajú SOC tímom identifikovať nové a vznikajúce hrozby. Integrácia CTI do bezpečnostných nástrojov umožňuje automatické generovanie upozornení na relevantné hrozby. CTI môže byť integrované do SIEM systémov na obohatenie dát a zlepšenie detekcie hrozieb. SIEM systémy môžu využívať CTI na identifikáciu a koreláciu hrozieb na základe aktuálnych informácií o hrozbách. Kým SIEM sa zameriava na zber a analýzu **logov a udalostí** na identifikáciu bezpečnostných incidentov, CTI sa zameriava na zber a analýzu informácií o **hrozbách** na poskytovanie kontextu a informácií pre lepšiu ochranu pred kybernetickými útokmi. CTI je kľúčovým prvkom pre efektívne fungovanie SOC, pretože poskytuje informácie, ktoré zlepšujú detekciu, reakciu, lov hrozieb, prioritizáciu incidentov a celkovú viditeľnosť hrozieb. Integrácia CTI do SOC umožňuje organizáciám lepšie chrániť svoje IT prostredie a rýchlejšie reagovať na kybernetické útoky.

CTI pomáha odpovedať na otázky:

- Kto predstavuje hrozbu pre moju organizáciu a akými metódami môže vykonať útok?
- Ako ovplyvňujú vektory útokov bezpečnosť mojej organizácie?
- Na čo by mal dohliadať môj SOC tím?
- Ako môžem znížiť riziko kybernetického útoku na moju organizáciu?

Cyber Threat Intelligence (CTI) sa delí na tri hlavné kategórie: strategický CTI, operatívny CTI a taktický CTI.

Strategický CTI poskytuje high level informácie o kybernetickej bezpečnosti, hrozbách, finančnom dopade kybernetických aktivít, trendoch útokov a ich vplyve na obchodné rozhodnutia. Tieto informácie sú určené pre vrcholových manažérov, ako sú CISO, a pomáhajú pri dlhodobom plánovaní a rozhodovaní o rozpočte, zamestnancoch a ochrane kritických aktív

Operatívny CTI sa zameriava na konkrétne informácie o prichádzajúcich útokoch, ako sú taktiky, techniky a postupy (TTP) hrozbových aktérov. Pomáha organizáciám pochopiť rozsah narušenia a pripraviť obranu vopred. Operatívny CTI tiež umožňuje proaktívne vyhľadávanie hrozieb a reakciu na incidenty

Taktický CTI je najzákladnejšou formou CTI a zameriava sa na identifikáciu a analýzu IOC. Slúži primárne na automatizovanú detekciu hrozieb v rámci systémov. Môže byť taktiež využitý na obohatenie bezpečnostných upozornení, napríklad v systémoch SIEM na poskytnutie väčšieho kontextu pre rozhodnutie, ktoré hrozby môžeme bezpečne ignorovať, a pri ktorých je potrebné detailnejšie preskúmanie a aplikovanie komplexnejších bezpečnostných opatrení. A teda môže týmto spôsobom napomáhať pri analýze incidentu analytikom nájsť špecifické artefakty a lepšie ho zdokumentovať. Pre zhrnutie, taktické CTI môže obsahovať napríklad hash súborov, IP adresy, URL adresy a IOC

8.1 FUNKČNÉ POŽIADAVKY

1. Zber dát o hrozbách			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zber a spracovanie hrozieb z viacerých CTI zdrojov	Automatické zhromažďovanie údajov o hrozbách z otvorených, komunitných, platených a interných zdrojov (napr. Abuse.ch, MISP, OTX, VirusTotal, Shodan).	Vstupné údaje a zdroje	CTI analytik, systémový integrátor

2. Normalizácia CTI dát			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Normalizácia a zjednocovanie hrozbových dát	Normalizovanie a zlučovanie CTI údajov z rôznych formátov a zdrojov do jednotnej štruktúry.	Spracovanie údajov	CTI analytik

3. Vytvorenie IOC			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Tvorba a aktualizácia hrozbových indikátorov	Definovanie, správa a distribúcia indikátorov kompromitácie (IOC), ako sú IP adresy, URL, hash hodnoty, domény.	Výstupné údaje	CTI analytik, bezpečnostný analytik

4. SIEM integrácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia CTI so SIEM a firewallom	Priama integrácia CTI informácií do detekčných a korelačných nástrojov ako SIEM, EDR, alebo firewally pre zlepšenie reakcie na incidenty.	Rozhrania s inými systémami	Systémový integrátor

5. Vizualizácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Vizualizácia hrozieb a techník útočníkov	Prehľadné zobrazenie vzťahov medzi útočníkmi, technikami, TTP a IOC prostredníctvom rámcov ako MITRE ATT&CK.	Používateľské rozhranie	CTI analytik, SOC analytik

6. Vytvorenie reakčného scenára			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Tvorba automatizovaných reakčných scenárov (playbookov) na CTI dáta	Spúšťanie reakcií na základe nových hrozbových indikátorov, vrátane skriptovania alebo drag-and-drop nástrojov.	Automatizácia procesov	CTI analytik, DevSecOps

8.2 NEFUNKČNÉ POŽIADAVKY

1. Rozsah CTI vrstiev			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora viacerých typov CTI (strategické, operatívne, taktické)	Riešenie musí vedieť spracovať a uchovávať informácie na rôznych úrovniach abstrakcie, od IOC až po analytické správy.	Požiadavky na údaje	CTI analytik, manažér bezpečnosti

2. Automatizovaný zber CTI			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Automatizované zhromažďovanie údajov zo zdrojov CTI	CTI systém má podporovať zber z komunitných, open-source a platených zdrojov (napr. MISP, OTX, Anomali Limo, VirusTotal).	Rozhrania	integrátor, CTI analytik

3. Štandardný formát CTI			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora normalizácie a štandardizácie formátov (napr. STIX, TAXII)	Všetky CTI údaje musia byť spracované do jednotnej štruktúrovanej formy.	Interoperabilita	systémový integrátor

4. Prepojenie CTI so systémami			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia s inými nástrojmi (SIEM, SOAR, firewall)	Údaje z CTI musia byť použiteľné v reálnom čase pre automatizovanú detekciu a reakciu.	Rozhrania	CTI analytik, integrátor

5. Vizualizácia hrozieb			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť vizualizácie hrozieb (napr. MITRE ATT&CK)	CTI nástroj má zobrazovať aktérov, techniky a vektory útokov v prehľadnej forme s mapovaním na známe rámce.	Používateľské požiadavky	bezpečnostný analytik, vedúci tímu

6. Manuálna validácia CTI			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora manuálnej analýzy a hodnotenia CTI údajov	Riešenie má umožniť analytikom prezerať a manuálne upravovať alebo anotovať informácie o hrozbách.	Použiteľnosť	CTI analytik

7. Bezpečnosť CTI dát			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Bezpečné uchovávanie CTI dát (autentifikácia, prístupové práva)	Prístup k CTI informáciám musí byť riadený na úrovni rolí a logovaný.	Bezpečnostné požiadavky	správca, audítor

8. Real-time obohatenie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora automatického obohacovania dát v reálnom čase	CTI má byť schopný dopĺňať alerty a logy o kontext (napr. reputácia IP, známy hash).	výkonnostné požiadavky	CTI analytik, operátor

9. Automatizované CTI playbooky			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora integrácie playbookov pre CTI spracovanie	Možnosť definovať automatizované akcie pri zistení novej hrozby (napr. blokovanie IP, informovanie analytika).	Prevádzkové požiadavky	bezpečnostný analytik

9 ASSET MANAGEMENT

Úloha v SOC (krátky textový opis):

Správa aktív (softvér, hardvér) a ich bezpečnostných stavov v organizácii.

9.1 FUNKČNÉ POŽIADAVKY

1. Evidencia IT aktív			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Evidencia a správa všetkých aktív v organizácii	Vytváranie, upravovanie a mazanie záznamov o všetkých IT aktívach – hardvér, softvér, virtuálne stroje, cloudové služby.	Vstupné údaje a zdroje	IT administrátor, bezpečnostný analytik

2. Klasifikácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Rozlíšenie aktív podľa typu a kritickosti	Klasifikovanie aktív podľa kategórií (napr. sieťové zariadenia, servery, cloudové služby) a priradenie úrovne dôležitosti či kritickosti.	Spracovanie údajov	Bezpečnostný analytik, manažér IT

3. Integrácia asset databázy			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia asset databázy so skenerom zraniteľností a SIEM	Prepojenie informácií o aktívach s výstupmi zo skenera zraniteľností, SIEM alebo EDR, a tým zabezpečiť lepší kontext pre reakciu na incidenty.	Rozhrania s inými systémami	Systémový integrátor

4. Sledovanie zmien			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Historická evidencia zmien na aktívach	Uchovávanie histórie zmien na jednotlivých aktívach (napr. zmena konfigurácie, stav, zaradenie do VLAN) pre účely auditu a forenznej analýzy.	Bezpečnostné požiadavky	Auditor, administrátor

5. Import/export			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť importu a exportu zoznamu aktív	Import údajov z existujúcich systémov (napr. CSV, API) a export do štandardizovaných formátov pre ďalšie spracovanie.	Výstupné údaje	IT administrátor, systémový integrátor

9.2 NEFUNKČNÉ POŽIADAVKY

1. Typy aktív			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora rôznych typov aktív (hardvér, softvér, cloud, kontajnery, služby)	Riešenie musí byť schopné evidovať všetky relevantné druhy aktív vrátane ich klasifikácie a väzieb.	Požiadavky na údaje	správca infraštruktúry, bezpečnostný analytik

2. Kategorizácia aktív			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť kategorizácie a označenia (tagovanie) aktív	Užívatelia musia mať možnosť triediť a označovať aktíva podľa rôznych kritérií (napr. úroveň rizika, prevádzkovateľ).	Prispôsobiteľnosť	správca systému

3. UX správy aktív			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prehľadné a intuitívne používateľské rozhranie	Evidencia a prehliadanie aktív musí byť dostupné cez prehľadné webové GUI.	Používateľské požiadavky	operátor, administrátor

4. Audit zmien aktív			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Auditovateľnosť zmien a prístupov k záznamom	Každá zmena údajov o aktívach musí byť zaznamenaná (kto, kedy, čo).	Bezpečnostné požiadavky	audítor, manažér bezpečnosti

5. Integrácia s monitoringom			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Napojenie na monitoring a bezpečnostné systémy	Údaje o aktívach musia byť dostupné pre SIEM, EDR, CTI a iné systémy na detekciu a analýzu.	Rozhrania	systémový integrátor, analytik

6. Vyhľadávanie aktív			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora vyhľadávania a filtrovania podľa rôznych parametrov	Rozhranie musí umožňovať pokročilé filtrovanie podľa typu, stavu, triedy alebo značky.	Používateľské požiadavky	analytik, správca

7. Ochrana dát o aktívach			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Bezpečnosť údajov o aktívach (ochrana pred zneužitím, prístupové práva)	Prístup k záznamom o aktívach musí byť kontrolovaný a zabezpečený, v súlade s princípom najmenej potrebných práv.	Bezpečnostné požiadavky	administrátor, audítor

8. Záloha aktív			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora zálohovania databázy aktív	Systém musí umožňovať pravidelné zálohovanie údajov a jednoduché obnovenie.	Udržateľnosť	správca IT infraštruktúry

10 SKENER ZRANITEĽNOSTI

Úloha v SOC (krátky textový opis):

Skener zraniteľností zohráva v SOC (Security Operations Center) dôležitú úlohu pri identifikácii a riešení slabých miest v IT infraštruktúre organizácie. Tento nástroj neustále monitoruje systémy, aplikácie a siete, aby odhalil potenciálne zraniteľnosti, ktoré by mohli byť zneužité útočníkmi. Skener zraniteľností vykonáva pravidelné skenovanie a analýzu, čím poskytuje prehľad o aktuálnom stave bezpečnosti a navrhuje opatrenia na odstránenie identifikovaných rizík. Týmto spôsobom pomáha SOC proaktívne chrániť organizáciu pred kybernetickými útokmi a zabezpečiť súlad s bezpečnostnými štandardmi.

10.1 FUNKČNÉ POŽIADAVKY

1. Detekcia zraniteľností			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Identifikácia zraniteľností v IT infraštruktúre	Automatizované skenovanie aktív za účelom detekcie známych zraniteľností a slabých miest.	Spracovanie údajov	Bezpečnostný analytik

2. Aktualizácia databázy			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Pravidelné aktualizácie databázy zraniteľností	Pravidelné aktualizovanie feed-u zraniteľností (napr. CVE, CPE, EPSS) s podporou komunitných aj podnikových zdrojov.	Vstupné údaje a zdroje	Administrátor, DevSecOps

3. Plánovanie skenovania			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť plánovania a opakovania skenov	Naplánovanie pravidelných skenov alebo ich spustenie na vyžiadanie – manuálne aj automaticky.	Automatizácia procesov	Bezpečnostný analytik, administrátor

4. Prehľad zraniteľností			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zobrazenie výsledkov a prioritizácia zraniteľností	Prehľadné prezentovanie skenovania, vrátane stupňa závažnosti (CVSS/EPSS skóre), odporúčaní na nápravu a triedenia podľa dopadu.	Používateľské rozhranie	Bezpečnostný analytik, manažér bezpečnosti

5. Agentless skenovanie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Skenovanie bez potreby agentov (agentless)	Realizovanie skenov bez potreby inštalácie softvérového agenta na cieľové zariadenia.	Architektúra systému	Systémový architekt, DevOps

6. Reporting			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Export reportov a notifikácie o nálezoch	Export výsledkov skenu do rôznych formátov (napr. CSV, PDF) a zasielanie oznámení o zistených zraniteľnostiach e-mailom alebo cez API.	Výstupné údaje	Bezpečnostný analytik, administrátor

10.2 NEFUNKČNÉ POŽIADAVKY

1. Otvorený nástroj			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora open-source alebo komunitnej verzie (bez licenčných nákladov)	Riešenie musí byť dostupné ako open-source alebo s komunitným prístupom, aby sa minimalizovali náklady.	Ekonomické obmedzenia	správca IT, manažér verejnej inštitúcie

2. Bezagentový sken			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť agentless režimu skenovania	Skener musí fungovať bez nutnosti inštalácie softvéru na skenované zariadenia, ak to architektúra umožňuje.	Interoperabilita	správca systému

3. Plánovanie skenov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora plánovaného aj ad-hoc skenovania	Systém musí umožniť plánovanie pravidelných skenov aj ich manuálne spustenie.	Prevádzkové požiadavky	bezpečnostný analytik

4. Výkonnostný rozsah			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť skenovať minimálne stovky IP adries denne	Nástroj musí byť schopný spracovať aspoň 100 IP adries za 24 hodín.	Výkon	operátor, technik IT

5. Aktualizácia testov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Pravidelne aktualizované databázy zraniteľností (feedy)	Skener musí používať aktualizované signatúry a databázy CVE/CPE, ideálne automaticky.	Udržateľnosť	správca, analytik

6. Použiteľnosť GUI			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zrozumiteľné webové rozhranie s možnosťou exportu výstupov	Rozhranie musí byť prehľadné, dostupné cez prehliadač a podporovať export (napr. CSV, PDF).	Používateľské požiadavky	analytik, audítor

7. Bezpečný prenos			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zabezpečenie komunikácie počas skenovania (napr. TLS)	Všetky dáta počas komunikácie musia byť šifrované a prístup kontrolovaný.	Bezpečnostné požiadavky	správca IT

8. Integrácia výstupov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia výsledkov do SIEM/Ticketing systému	Výstupy musia byť použiteľné ako zdroj pre incident response alebo ďalšiu analýzu.	Rozhrania	integrátor, analytik

9. Podpora súladu			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora politík súladu (GDPR, ISO/IEC, CIS, BSI...)	Skener by mal podporovať štandardné šablóny alebo výstupy pre regulované prostredia.	Právne požiadavky	audítor, bezpečnostný manažér

10. Prioritizácia rizík			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora EPSS a CVSS scoringu	Skener má vyhodnocovať aj pravdepodobnosť zneužitia zraniteľnosti, nie len jej závažnosť.	Výkonnostné hodnotenie	bezpečnostný analytik

11 ZDROJE BEZPEČNOSTNÝCH ÚDAJOV

Úloha v SOC (krátky textový opis):

Zber údajov z endpointov, sieťových zariadení, cloudových služieb atď.

11.1 FUNKČNÉ POŽIADAVKY

1. Zber endpoint logov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zber logov a auditných údajov zo serverov a endpointov	Získavanie systémových, aplikačných a bezpečnostných logov z koncových zariadení a serverov vrátane auditných údajov.	Vstupné údaje a zdroje	Systémový integrátor, bezpečnostný analytik

2. Zber dát z infraštruktúry			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zber sieťových dát z infraštruktúry	Prijímanie dát zo sieťových zariadení cez protokoly ako Syslog, Netflow/IPFIX, SNMP, vrátane podpory pre IPv6.	Vstupné údaje a zdroje	Sieťový administrátor, bezpečnostný analytik

3. Zber logov z bezpečnostných nástrojov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zber logov zo špecializovaných bezpečnostných zariadení	Spracovávanie logov z WAF, IDS/IPS, HIDS systémov (napr. Suricata, Snort, Wazuh) a iných bezpečnostných nástrojov.	Rozhrania s inými systémami	Systémový integrátor

4. Logovací agenti			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora rôznych typov beatov a forwarderov	Nasadenie agentov ako Filebeat, Auditbeat, Metricbeat alebo iných pre efektívny zber a transport logov.	Architektúra systému	DevOps, administrátor systému

5. Normalizácia údajov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Normalizácia zozbieraných údajov	Automatická konverzia údajov do jednotného formátu, aby boli interoperabilné s nástrojmi ako SIEM a ML moduly.	Spracovanie údajov	Bezpečnostný analytik

11.2 NEFUNKČNÉ POŽIADAVKY

1. Podpora typov logov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora rôznych typov logov (systémové, sieťové, aplikačné, bezpečnostné)	Riešenie musí vedieť prijímať logy z rôznych zariadení a softvérových vrstiev, vrátane WAF, IDS/IPS, EDR.	Rozhrania	systémový integrátor, správca IT

2. Normalizované logy			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Štandardizácia a normalizácia formátov údajov	Všetky vstupné dáta musia byť spracované do jednotného formátu použiteľného pre ďalšiu koreláciu a analýzu.	Požiadavky na údaje	bezpečnostný analytik

3. Štandardné protokoly			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora logovania cez štandardné protokoly (syslog, SNMP, IPFIX)	Zber údajov má byť realizovateľný prostredníctvom bežných protokolov a formátov na báze open štandardov.	Interoperabilita	sieťový špecialista

4. Bezpečný zber			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Bezpečný zber údajov (šifrovanie prenosu, autentifikácia prístupu)	Komunikácia medzi zdrojom a zberným komponentom musí byť šifrovaná a overená.	Bezpečnostné požiadavky	bezpečnostný architekt

5. Rozšíriteľnosť zdrojov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť rozšírenia o nové typy zdrojov	Architektúra má byť modulárna, aby umožnila jednoduché pridanie ďalších zdrojov údajov.	Udržateľnosť a rozšíriteľnosť	integrátor, vývojár

6. Podpora agentov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora doplnkových agentov a forwarderov (napr. Filebeat, Auditbeat)	Zber údajov môže byť zabezpečený aj cez špecializované nástroje pre jednotlivé typy údajov.	Výkonové požiadavky	správca systému

7. Validácia logov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť overiť kvalitu a úplnosť zberaných údajov (validácia)	Riešenie musí byť schopné zistiť chyby, výpadky alebo deformácie v prijímaných dátach.	Spoľahlivosť	operátor, kontrolór kvality

8. Archív údajov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zálohovanie a uchovávanie údajov podľa právnych a prevádzkových politík	Musí byť zabezpečené dlhodobé a bezpečné uchovávanie údajov s možnosťou zálohovania a obnovy.	Bezpečnostné / legislatívne požiadavky	správca, audítor

12 KNOWLEDGE BASE

Úloha v SOC (krátky textový opis):

Centrálne úložisko znalostí, dokumentácie a postupov potrebných pre SOC tím.

12.1 FUNKČNÉ POŽIADAVKY

1. Znalostná báza			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Centrálne úložisko znalostí pre SOC tím	Uchovávanie znalostí, dokumentácie, interných procesov, reakčných postupov a iných dôležitých informácií pre SOC tím.	Vstupné údaje a zdroje	Bezpečnostný analytik, manažér SOC

2. Správa záznamov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Tvorba a editácia záznamov v znalostnej báze	Jednoduché vytváranie, upravovanie a organizovanie záznamov v znalostnej báze podľa kategórií, tém alebo incidentov.	Používateľské rozhranie	Analytik, administrátor

3. Vyhľadávanie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Vyhľadávanie v obsahu znalostnej bázy	Rýchle vyhľadávanie na základe kľúčových slov, tagov alebo štruktúrovaných filtrov.	Výstupné údaje	SOC operátor, analytik

4. Riadenie prístupov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prístupové práva k dokumentom podľa roly	Nastavovanie prístupových práv k jednotlivým častiam alebo typom obsahu v znalostnej báze.	Bezpečnostné požiadavky	Administrátor, bezpečnostný architekt

12.2 NEFUNKČNÉ POŽIADAVKY

1. Prehľadná báza znalostí			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prehľadné používateľské rozhranie s vyhľadávaním	Rozhranie má umožňovať jednoduchý prístup ku všetkým záznamom a rýchle vyhľadávanie podľa kľúčových slov.	Používateľské požiadavky	analytik, operátor

2. Tvorba záznamov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť vytvárať, editovať a štruktúrovať záznamy	Systém musí umožniť vytváranie a úpravu článkov, príručiek, SOP (standard operating procedures) a návodov.	Používateľské Požiadavky na údaje	manažér SOC, vedúci tímu

3. História zmien			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť verzovania a ukladania histórie zmien	Každá zmena v zázname musí byť evidovaná s možnosťou návratu k staršej verzii.	Udržateľnosť	audítor, správca znalostí

4. Oprávnenia k znalostiam			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Riadenie prístupov a oprávnení k záznamom	Prístup k jednotlivým dokumentom musí byť riadený na úrovni rolí (napr. len čítanie, editácia, schválenie).	Bezpečnostné požiadavky	správca systému

5. Triedenie záznamov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora kategorizácie obsahu a značiek (tagy, sekcie, témy)	Obsah musí byť možné organizovať do kategórií, sekcií a označovať metadátami pre rýchlejšiu orientáciu.	Prispôsobiteľnosť	editor obsahu

6. Export znalostí			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora exportu záznamov (napr. PDF, HTML)	Obsah by mal byť exportovateľný na offline použitie alebo archiváciu.	Používateľské požiadavky	správca dokumentácie

7. Prepojenie na systémy			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia s ostatnými systémami (napr. ticketing, incident management)	Knowledge base má byť prepojiteľná so systémami, ktoré využívajú jej obsah na odporúčania alebo podporu reakcie.	Rozhrania	systémový integrátor

8. Bezpečnosť databázy znalostí			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zabezpečenie integrity a dostupnosti obsahu (zálohovanie, ochrana)	Obsah musí byť chránený proti strate alebo neoprávneným zmenám, vrátane zálohovania.	Bezpečnostné / udržateľné požiadavky	Bezpečnostné / udržateľné požiadavky

13 TICKETING

Úloha v SOC (krátky textový opis):

Riadenie, sledovanie incidentov prostredníctvom ticketov.

13.1 FUNKČNÉ POŽIADAVKY

1. Vytváranie tiketov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Vytváranie a evidencia ticketov	Ručné alebo automatické vytváranie tiketov pri detekcii incidentu, udalosti alebo potreby zásahu.	Vstupné údaje a správa úloh	SOC operátor, analytik incidentov

2. Stav tiketu			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Editácia a správa stavu tiketu	Zmena stavu (napr. otvorený, v riešení, uzavretý) a sledovanie jeho životného cyklu.	Spracovanie údajov	Riešiteľ incidentov, tímový vedúci

3. Priradenie tiketu			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Priradenie tiketov konkrétnym používateľom	Priraďovanie tiketov konkrétnym riešiteľom podľa ich roly, oblasti zodpovednosti alebo typu incidentu.	Riadenie prístupov a zodpovednosti	Manažér SOC, tímový koordinátor

4. Notifikovanie			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Emailové notifikácie o zmenách v tikete	Odosielanie notifikáciu príslušným osobám cez e-mail alebo iný komunikačný kanál pri akejkoľvek zmene v stave alebo obsahu tiketu.	Výstupné údaje	Riešiteľ incidentov, manažér bezpečnosti

13.2 NEFUNKČNÉ POŽIADAVKY

1. Správa tiketov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť vytvárať a upravovať tikety cez GUI	Systém musí podporovať ručné aj automatizované vytváranie tiketov cez prehľadné webové rozhranie.	Používateľské požiadavky	operátor, IT podpora

2. Stavy tiketov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť zmeny stavu tiketov a workflow spracovania	Každý tiket musí byť spracovávaný podľa definovaných stavov (napr. nové, otvorené, čaká na vstup, vyriešené).	Prispôsobiteľnosť / procesné požiadavky	bezpečnostný analytik, správca incidentov

3. Priradenie riešiteľa			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Priradenie tiketu konkrétnemu používateľovi alebo tímu	Riešiteľ tiketu musí byť identifikovateľný a zmeniteľný v rámci tímovej hierarchie.	Riadenie procesov	manažér tímu

4. Emailové upozornenia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Emailové notifikácie o zmenách stavu alebo komentároch	Systém má informovať príslušné osoby o zmene stavu tiketu alebo pridaní komentára.	Rozhrania / používateľské požiadavky	operátor, analytik

5. Oprávnenia k tiketom			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zabezpečenie prístupu na základe rolí	Prístup k tiketom má byť obmedzený podľa organizačnej štruktúry a rolí.	Bezpečnostné požiadavky	správca systému

6. História spracovania			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť spätnej väzby a audit trail k tiketu	Každý tiket musí obsahovať záznam o všetkých zmenách a zásahoch počas jeho životného cyklu.	Auditovateľnosť	audítor, manažér bezpečnosti

7. Integrácia s reakčnými systémami			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia so SOAR a SIEM systémami	Tikety musia byť zakladateľné automaticky na základe detekcie incidentu v iných komponentoch systému.	Rozhrania	systémový integrátor, bezpečnostný analytik

8. Meranie výkonu riešenia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora SLA a metrík spracovania (napr. doba vyriešenia)	Systém má sledovať časy odozvy a riešenia, v prípade potreby eskalovať porušenie SLA.	Výkonové a prevádzkové požiadavky	manažér služby

14 EVIDENCIA A SPRÁVA INCIDENTOV

Úloha v SOC (krátky textový opis):

Dokumentácia a analýza incidentov pre efektívne riadenie bezpečnosti.

14.1 FUNKČNÉ POŽIADAVKY

1. Evidencia incidentov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zaznamenávanie incidentov s detailnými informáciami	Zaznamenávanie bezpečnostných incidentov s detailmi ako dátum, čas, typ, postihnuté systémy, závažnosť, stav riešenia.	Vstupné údaje	SOC analytik, incident handler

2. Prepojenie incidentov s dátami			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prepojenie incidentov s tiketmi a logmi	Prepojenie incidentov s príslušnými tiketmi, logmi, detekciami zo SIEM alebo EDR, aby bolo možné sledovať ich celý kontext a históriu.	Spracovanie údajov	Bezpečnostný analytik

3. Hodnotenie incidentov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Vyhodnocovanie a klasifikácia incidentov	Kategorizovanie incidentov podľa typu, úrovne rizika, dopadu a odporúčaných reakcií.	Automatizácia procesov	Analytik, manažér bezpečnosti

4. Archivácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Uchovávanie záznamov pre audit a forenzné účely	Dlhodobé uchovávanie incidentov vrátane všetkých súvisiacich údajov pre účely auditu, forenznej analýzy a retrospektívneho hodnotenia.	Bezpečnostné požiadavky	Auditor, bezpečnostný architekt

14.2 NEFUNKČNÉ POŽIADAVKY

1. GUI pre incidenty			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prehľadné rozhranie na správu incidentov	Riešenie musí poskytovať intuitívne a prehľadné rozhranie pre evidenciu, sledovanie a správu incidentov.	Používateľské požiadavky	analytik, operátor SOC

2. Detailný záznam incidentu			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť zaznamenať kompletné detaily incidentu (čas, zdroj, dopad, opatrenia)	Systém musí umožniť záznam kľúčových parametrov incidentu a ich aktualizáciu počas riešenia.	Požiadavky na údaje	bezpečnostný analytik

3. História incidentu			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Verzovanie, komentovanie a časové značky	Evidencia musí uchovávať históriu úprav, komentárov a časových značiek zmien.	Udržateľnosť / auditovateľnosť	audítor, správca incidentov

4. Prepojenie s dôkazmi			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prepojenie na tikety a technické artefakty (logy, IOC, súbory)	Incident musí byť možné prepojiť s inými systémami alebo objektmi (napr. logmi, výstupmi SIEM).	Rozhrania	analytik, vyšetrovateľ incidentov

5. Export incidentov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť exportu incidentu pre report alebo audit (napr. PDF, JSON)	Incidenty musia byť jednoducho exportovateľné na ďalšie použitie alebo archiváciu.	Používateľské požiadavky	manažér bezpečnosti

6. Oprávnenia incidentov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prístupové práva a autorizácia k manipulácii s incidentmi	Len oprávnené osoby môžu upravovať, zatvárať alebo komentovať incidenty.	Bezpečnostné požiadavky	správca systému, vedúci tímu

7. Integrácia incident manažmentu			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia s ticketingom, SIEM, SOAR	Systém má byť schopný automaticky zakladať incidenty alebo ich aktualizovať podľa výstupov iných komponentov.	Rozhrania	integrátor, analytik

8. Kategorizácia incidentov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť klasifikácie a kategorizácie incidentov (napr. podľa typu, závažnosti, služby)	Incidenty musia byť triediteľné pre účely štatistík a prioritizácie.	Prispôsobiteľnosť / procesné požiadavky	bezpečnosti

15 REPORTOVANIE

Úloha v SOC (krátky textový opis):

Generovanie pravidelných a ad-hoc reportov o stave bezpečnosti.

15.1 FUNKČNÉ POŽIADAVKY

1. Bezpečnostný report			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Vytváranie prehľadov o stave bezpečnosti	Vytváranie pravidelných alebo jednorazových prehľadov o bezpečnostnom stave, výskyte incidentov, výkonnosti systémov a zraniteľnostiach.	Výstupné údaje	Manažér bezpečnosti, auditor

2. Export			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť exportu a zdieľania reportov	Vytváranie reportov vo formátoch ako PDF, CSV, HTML a musia byť exportovateľné na lokálne úložisko, sieťový disk alebo emailom.	Výstupné údaje	Analytik, administrátor

3. Automatizácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Automatizované zasielanie reportov podľa harmonogramu	Plánovanie a automatické zasielanie reportov konkrétnym adresátom (napr. denne, týždenne, mesačne).	Automatizácia procesov	Manažér bezpečnosti

4. Filtrovanie obsahu

Zameranie	Popis funkcie	ISO/IEC/IEEE 29148:2018 kategória	Rola
Možnosť filtrovania obsahu reportov podľa typu a rozsahu dát	Prispôsobenie rozsahu údajov v reporte – napr. filtrovať podľa zdroja incidentu, časového obdobia alebo závažnosti.	Používateľské rozhranie	SOC analytik, manažér

15.2 NEFUNKČNÉ POŽIADAVKY

1. Vizualizované reporty			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prehľadné vizuálne reporty dostupné cez web	Reporty musia byť prezentované formou grafov, tabuliek a metrík, čitateľné aj pre manažment.	Používateľské požiadavky	manažér bezpečnosti, zákazník

2. Plánované aj manuálne výstupy			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť generovať pravidelné aj ad-hoc reporty	Užívatelia musia vedieť vytvárať pravidelné reporty (napr. denne, mesačne) aj jednorazové výstupy na požiadanie.	Výkonové požiadavky	analytik, manažér

3. Export reportov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora exportu do bežných formátov (PDF, CSV, JSON)	Výstupy musia byť použiteľné pre interné aj externé účely – tlač, mail, ďalšia analýza.	Rozhrania	správca, analytik

4. Konfigurovateľné výstupy

Zameranie	Popis	ISO/IEC/IEEE 29148:2018 kategória	Rola
Možnosť filtrovať a prispôsobovať obsah reportov	Užívatelia si musia vedieť zvoliť, ktoré údaje sa do reportu zahrnú – podľa typu incidentov, aktív, časového rámca atď.	Prispôsobiteľnosť	analytik, vedúci tímu

5. Riadený prístup k výstupom			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zabezpečený prístup k reportom podľa rolí	K reportom musia mať prístup iba oprávnené osoby podľa prístupových práv.	Bezpečnostné požiadavky	správca systému, audítor

6. Automatická distribúcia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Automatizované zasielanie reportov e-mailom alebo cez API	Systém má podporovať plánované odosielanie reportov na definované adresy alebo systémy.	Prevádzkové požiadavky	správca služby

7. Archív reportov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
História vygenerovaných reportov a možnosť opätovného stiahnutia	Staršie reporty musia byť dohľadateľné v systéme s možnosťou opakovaného zobrazenia alebo exportu.	Udržateľnosť	audítor, manažér služby

16 ADMINISTRATÍVA SYSTÉMU

Úloha v SOC (krátky textový opis):

Správa SOC infraštruktúry, konfigurácia, údržba a aktualizácie.

16.1 FUNKČNÉ POŽIADAVKY

1. Správa prístupov			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Riadenie prístupových práv a rolí používateľov	Správa prístupových práv podľa rolí (napr. analytik, administrátor, manažér), s podporou RBAC (role-based access control).	Bezpečnostné požiadavky	Administrátor systému, bezpečnostný architekt

2. Konfigurácia systému			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Konfigurácia a správa systémových komponentov	Nastavovanie a upravovanie konfigurácie komponentov systému – logovanie, notifikácie, integrácie, šablóny pravidiel.	Spracovanie údajov	DevOps, administrátor

3. Automatizácia			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Automatizované nasadenie infraštruktúry	Sledovanie aktuálnej verzie komponentov, plánovanie a vykonávanie aktualizácií vrátane rollback funkcií.	Údržba systému	Administrátor, DevSecOps

16.2 NEFUNKČNÉ POŽIADAVKY

1. Automatizovaná konfigurácia			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Správa konfigurácie cez automatizačné nástroje (napr. Ansible, Chef)	Konfigurácia systémov musí byť definovateľná ako kód a spustiteľná cez automatizačné platformy.	Prevádzkové požiadavky	devops, správca infraštruktúry

2. Prístup podľa rolí			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Riadenie prístupu na základe rolí (RBAC)	Rôzne úrovne oprávnení pre správu musia byť definované a oddelené (napr. operátor, administrátor, audítor).	Bezpečnostné požiadavky	správca systému

3. Záloha systému			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora zálohovania konfigurácií a obnovy systému	Administrácia musí umožniť pravidelné zálohy konfigurácií a dát s možnosťou obnovy do funkčného stavu.	Udržateľnosť	IT administrátor

4. Správcovské rozhranie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prehľadné GUI pre správu komponentov a služieb	Administrácia musí byť dostupná cez jednotné webové rozhranie, s monitoringom stavu jednotlivých služieb.	Používateľské požiadavky	operátor, správca

5. Audit zmien systému			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Auditovanie zásahov do systému (kto, kedy, čo menil)	Všetky zmeny konfigurácie, oprávnení a stavu služieb musia byť logované.	Auditovateľnosť	audítor, bezpečnostný manažér

6. Aktualizácia systému			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Jednoduchá aktualizácia a upgrade systémových komponentov	Administrátori musia vedieť nasadiť nové verzie komponentov bez výpadku alebo s minimálnym dopadom.	Udržateľnosť	devops, správca

7. Monitorovanie prevádzky			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Integrácia s monitorovacími nástrojmi (napr. Prometheus, Zabbix)	Administrácia musí byť schopná odosielať metriky a stavové informácie do existujúcej monitorovacej platformy.	Rozhrania	správca infraštruktúry

8. Kontajnerové nasadenie			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora nasadzovania v kontajneroch (Kubernetes, Docker)	Systém musí byť pripravený na prevádzku v moderných CI/CD a cloud-native architektúrach.	Inštalačné požiadavky	systémový architekt, devops

17 VOLITEĽNÉ ROZŠÍRENIA

17.1 FUNKČNÉ POŽIADAVKY

1. Forenzná analýza			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Pokročilá forenzná analýza a threat hunting	Vyhľadávanie anomálií, manuálne skúmanie dát, sledovanie správania útočníkov a forenznú analýzu incidentov pomocou viacerých vstupov (logy, pamäť, disk).	Funkčná analytika	Forenzný analytik, SOC špecialista

2. Backup			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zálohovanie a obnova systému	Pravidelné zálohovanie konfigurácie, databáz, logov a iných kritických častí systému, vrátane plánovania a obnovy.	Bezpečnostné a prevádzkové požiadavky	Administrátor systému, DevOps

3. Compliance monitoring			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Compliance manažment (riadenie zhody s normami)	Sledovanie a vyhodnocovanie zhody s bezpečnostnými štandardmi ako GDPR, ISO/IEC 27001, PCI-DSS, NIS2 a ďalšie.	Regulačné a legislatívne požiadavky	Auditor, manažér bezpečnosti

4. SLA monitoring a reporting			
Zameranie	**Popis funkcie**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
SLA monitoring a reporting poskytovaných služieb	Sledovanie úrovne dostupnosti a výkonnosti služieb podľa definovaných SLA, vrátane reportovania incidentov, reakčných časov a nedostupností.	Výkonnostné a prevádzkové požiadavky	Manažér služby, zákazník (tenant)

17.2 NEFUNKČNÉ POŽIADAVKY

1. Prístup k histórii			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Prístup k historickým údajom s presným časovým kontextom	Riešenie musí umožniť rýchle vyhľadávanie a rekonštrukciu udalostí spätne cez časovú os.	Požiadavky na údaje	forenzný analytik

2. Threat hunting režim			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Podpora manuálneho a poloautomatického lovenia hrozieb	Systém musí podporovať aktívne vyhľadávanie anomálií a známok útoku.	výkonnostné požiadavky	SOC analytik

3. Vizualizácia forenzných údajov			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zaznamenávanie a vizualizácia forenzných reťazcov	Analytici musia mať možnosť vizuálne sledovať priebeh útoku (napr. MITRE ATT&CK mapping).	Používateľské požiadavky	bezpečnostný vyšetrovateľ

4. Automatizácia záloh			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť definovať a automatizovať zálohovacie politiky	Riešenie musí podporovať plánovanie a verifikáciu záloh systému a konfigurácií.	Udržateľnosť	správca IT

5. Obnova systému			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Obnova po výpadku bez straty konfigurácie a incidentov	Po výpadku má byť možné obnoviť SOC do plne funkčného stavu vrátane stavu incidentov.	Spoľahlivosť	prevádzkový tím

6. Mapovanie na normy			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Zabezpečenie mapovania bezpečnostných opatrení na normy (GDPR, ISO 27001, NIS2)	Riešenie má podporovať exporty a sledovanie stavu súladu podľa zvolených rámcov.	Právne požiadavky	compliance officer, CISO

7. Kontrola zhody			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Možnosť vyhodnocovania zhody cez kontrolné mechanizmy a checklisty	Systém musí poskytovať nástroje na overenie implementácie požiadaviek a opatrení.	Prispôsobiteľnosť	audítor, bezpečnostný manažér

8. Audítorské výstupy			
Zameranie	**Popis**	**ISO/IEC/IEEE 29148:2018 kategória**	**Rola**
Automatizované reporty a dokumentácia pre audit	Výstupy z compliance manažmentu musia byť automaticky generovateľné a exportovateľné.	Používateľské požiadavky	audítor, manažér kvality

18 TECHNICKÉ POŽIADAVKY – SUMÁRNE

1. Kontajnery			
Zameranie	**Popis**	**Minimálny hardvér pre produkčné prostredie**	**Iné**
Podpora kontajnerov	Každý komponent systému INNOSOC musí byť nasaditeľný ako kontajner (napr. Docker image) a spravovaný pomocou Kubernetes (verzia 1.25 alebo novšia). Musí byť použitá štandardizovaná štruktúra kontajnerov (multi-stage build, zraniteľnostné skeny, podpísané imagy).	Min. 3 fyzické/virtuálne uzly (master + 2 workers) Každý worker: 4 CPU, 8 GB RAM SSD úložisko min. 100 GB na node Gbit sieťová konektivita	Podpora Helm Charts, volume claims (persistent volumes), Ingress Controller.

2. Mikroslužby			
Zameranie	**Popis**	**Minimálny hardvér na službu**	**Iné**
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. REST API musí byť zdokumentované pomocou OpenAPI (Swagger).	1 CPU, 2 GB RAM Zdieľané úložisko: min. 10 GB na službu	

3. CI/CD pipeline			
Zameranie	**Popis**	**Minimálny hardvér pre CI runner**	**Iné**
CI/CD a orchestrácia	Zavedenie pipeline pre build-test-deploy cyklus. Podpora GitOps (ArgoCD), CI (GitLab CI alebo Jenkins), automatizovaný lint, scan, testy, rollout.	2 CPU, 4 GB RAM SSD 50 GB na build artefakty	Prístup k docker registru (lokálnemu alebo vzdialenému)

4. OSS kompatibilita			
Zameranie	**Popis**	**Minimálny hardvér pre Elastic / OpenSearch cluster**	**Iné**
Kompatibilita s OSS	Všetky súčasti systému musia byť postavené na open-source technológiách (preferované: ELK/OpenSearch, Grafana, Fluent Bit, Prometheus, Wazuh). Licencie musia umožňovať úpravy a ďalšie šírenie.	3 uzly: každý min. 4 CPU, 16 GB RAM SSD: 200 GB pre indexy	Oddelený disk pre transakčné logy

5. Štandardné dáta			
Zameranie	**Popis**	**Minimálny hardvér na normalizáciu dát**	**Iné**
Formáty dát	Systém musí spracovávať JSON, YAML, STIX/TAXII (CTI), Syslog, NetFlow/IPFIX. Normalizácia logov musí byť zabezpečená pomocou Fluentd/Logstash.	1 CPU, 2 GB RAM na každý log parser	Voliteľne GPU pre akceleráciu ML parsingu

6. Reverzný proxy a VPN			
Zameranie	**Popis**	**Minimálny hardvér pre edge node**	**Iné**
Prístupová architektúra	Prístup do systému má byť riadený cez NGINX Ingress alebo HAProxy. Pre interný prístup má byť použitý VPN server (napr. WireGuard/OpenVPN). Podporovaná TLS 1.3, forward secrecy.	2 CPU, 4 GB RAM 50 GB SSD na logy	Vverejná IP adresa

7. API zabezpečenie			
Zameranie	**Popis**	**Minimálny hardvér pre API gateway**	**Iné**
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.	2 CPU, 2 GB RAM 100 GB SSD na logy a cache	

8. Audit trail			
Zameranie	**Popis**	**Minimálny hardvér pre auditný uzol**	**Iné**
Auditovateľnosť	Každá zmena konfigurácie, interakcia s API, akcia používateľa a incident musí byť logovaná do centralizovaného auditného úložiska. Uchovávanie logov min. 12 mesiacov, hashovanie a podpisovanie auditných záznamov.	4 CPU, 8 GB RAM 500 GB HDD alebo S3 kompatibilné objektové úložisko	

9. Plugin architektúra			
Zameranie	**Popis**	**Minimálny hardvér na plugin**	**Iné**
Modulárne riešenie	Riešenie musí umožniť dynamické pridávanie plug-inov bez reštartu jadra. Pluginy musia byť izolované (napr. sidecar kontajnery alebo sandboxy).	1 CPU, 1 GB RAM	Dynamické pridelenie podľa potreby služby

10. Multitenancia			
Zameranie	**Popis**	**Minimálny hardvér na jeden tenant**	**Iné**
Multitenantný deployment	Každý tenant musí mať oddelené namespace, databázu, dashboardy a logy. Musí byť možné nakonfigurovať SLA politiky na úrovni tenanta.	2 CPU, 4 GB RAM 100 GB SSD	Možnosť škálovať nezávisle

18.1 BEZPEČNOSTNÉ TECHNICKÉ POŽIADAVKY

1. Šifrovanie komunikácie			
Zameranie	**Popis**	**Minimálny hardvér pre TLS termination**	**Iné**
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.	1 CPU, 1 GB RAM na službu terminujúcu TLS	Použitie hardvérových modulov HSM alebo softvérový vault pre správu kľúčov

2. Prístupové práva			
Zameranie	**Popis**	**Minimálny hardvér pre Identity server**	**Iné**
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.	2 CPU, 2 GB RAM 50 GB SSD pre logy a revokácie	

3. Tajné úložisko			
Zameranie	**Popis**	**Minimálny hardvér pre Vault**	**Iné**
Bezpečná správa tajného úložiska	Heslá, API kľúče, certifikáty a tokeny musia byť uložené v tajnom úložisku (napr. HashiCorp Vault, Kubernetes secrets s podkladom v etcd šifrovanom pri uložení).	2 CPU, 4 GB RAM 100 GB SSD	

4. Bezpečnostné logy			
Zameranie	**Popis**	**Minimálny hardvér pre log server**	**Iné**
Bezpečné logovanie a detekcia anomálií	Systém musí vytvárať bezpečnostné logy, ktoré umožňujú detekciu podozrivého správania (napr. brute force, neobvyklé API prístupy). Požaduje sa integrácia s SIEM.	4 CPU, 8 GB RAM 500 GB SSD, dedikovaný disk pre logy	

18.2 POŽIADAVKY NA ÚLOŽISKO A ZÁLOHOVANIE

1. Úložisko logov			
Zameranie	**Popis**	**Minimálny hardvér**	**Iné**
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.	Min. 1 TB SSD pre SIEM	RAID 10 alebo Ceph na redundanciu

2. Konfiguračné zálohy			
Zameranie	**Popis**	**Minimálny hardvér**	**Iné**
Zálohovanie konfigurácií a dashboardov	Automatické denné zálohovanie konfigurácií, pluginov, playbookov a dashboardov. Obnova musí byť možná do 1 hodiny (RTO ≤ 1h).	Samostatný zálohovací uzol: 2 CPU, 4 GB RAM 2 TB HDD alebo prístup k objektovému úložisku (S3/MinIO)	

3. Archivácia			
Zameranie	**Popis**	**Minimálny hardvér**	**Iné**
Archivácia a dlhodobé uchovanie	Systém musí podporovať automatické presúvanie dát do archívu podľa pravidiel (napr. kompresia, šifrovanie, presun po 90 dňoch).	10 TB kapacita, podpora offline záloh	

18.3 VÝKONNOSTNÉ METRIKY A TECHNICKÉ KPI

1. Horizontálne škálovanie			
Zameranie	**Popis**	**Požiadavky**	**Iné**
Škálovateľnosť systému	Riešenie musí podporovať horizontálne škálovanie jednotlivých komponentov na základe metrík (CPU, RAM, počet logov/min).	Podpora autoscaling cez Kubernetes HPA Clustering pre Elasticsearch, Kafka, Redis	

2. Vysoká dostupnosť			
Zameranie	**Popis**	**Hardvér**	**Iné**
Dostupnosť a odolnosť	Systém musí byť nasadený v režime vysokej dostupnosti (HA) – load balancer, failover, minimálne 2 inštancie kritických služieb.	2+ load balancery (napr. HAProxy)	Oddelené uzly na rôznych fyzických hostoch

3. Výkon spracovania			
Zameranie	**Popis**	**Hardvér na spracovanie logov**	**Iné**
Výkon spracovania dát	Systém musí spracovať minimálne 10 000 logov za sekundu v reálnom čase s oneskorením < 5 sekúnd.	8 CPU, 16 GB RAM na parsing a koreláciu	Možnosť paralelizácie