podklady ku V10 - Zoznam funkčných a nefunkčných požiadaviek a V11 – Biznis architektúra
previazané na KPB4

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY | ŽILINSKÁ UNIVERZITA V ŽILINE Fakulta riadenia a informatiky | BRAIN:IT

Use Case

Rola			
prevádzkovateľ platformy	SIEM	nefunkčné	Nasaditeľnosť v kontajneroch

Rola			
Správca infraštruktúty	Spracovanie logov	nefukčné	Kontajnerizovateľnosť
	Asset management	nefukčné	Typy aktív
	Administratíva systému	nefukčné	automatizovaná konfigurácia
			monitorovanie prevádzky

Rola			
Incident handler	SOAR	funkčné	kategorizácia
	Evidencia a správaincidentov	funkčné	evidencia incidentov

Rola			
DevSecOps	SOAR	funkčné	playbook
	CTI	funkčné	vytvorenie reakčného scenára
	Skener zraniteľnosti	funkčné	aktualizácia databázy
	administratíva systému	funkčné	automatizácia

Rola			
Poskytovateľ služby	SIEM	Nefunkčné	Mulitenancia

Rola			
Prevdzkovateľ platformy	SIEM	Nefunkčné	Mulitenancia

Rola			
Data Scientist	detekcia pomocou ML	funkčné	Detekcia anomálií
			Aktualizácia ML
			Hodnotenie modelov

Rola			
ML špecialista	detekcia pomocou ML	nefunkčné	Presnosť detekcie
			Modulárne modely
	EDR/XDR	nefunkčné	Viacdátový zber

Rola			
ML inžinier	detekcia pomocou ML	nefunkčné	rýchlosť reakcie
			škálovateľnosť výpočtov
			pipeline pre učenie

Rola			
Architekt	Detekcia pomocou ML	nefuknčné	hodnotenie modelov
			správa modelov
	EDR/XDR	nefuknčné	podpora viacerých prostredí

Rola			
Vedúci tímu SOC	vizualizácia dát	nefunkčné	konfigurovateľné dashboardy

Rola			
prevádzkovateľ	vizualizácia dát	nefunkčné	jednotné prihlásenie

Rola			
prevádzkový tím	alertovanie	nefunkčné	viackanálové doručenie
	voliteľné rozšírenia	nefunkčné	obnova systému

Rola			
Vedúci SOC	alertovanie	nefunkčné	prispôsobenie alertov

Rola			
SOC operátor	alertovanie	funkčné	okamžité upozornenia
		nefunkčné	reálne časy alertov
	EDR/XDR	funkčné	dashboard
	knowledge base	funkčné	vyhľadávanie
	ticketing	funkčné	vytváranie tiketov

Rola			
SLA operátor	alertovanie	nefunkčné	eskalačné pravidlá

Rola			
SOC analytik	EDR/XDR	funkčné	detekcia hrozieb
	CTI	funkčné	vizualizácia
	evidencia a správa incidentov	funkčné	evidencia incidentov
	reportovanie	funkčné	filtrovanie obsahu
	voliteľné rozšírenia	nefunkčné	threat hunting režim

Rola			
forenzný analytik	voliteľné rozšírenia	funkčné	forenzná analýza
	EDR/XDR	nefunkčné	prístup k histórií
		funkčné	detekcia hrozieb

Rola

Systémový integrátor	SIEM	Funkčné	Zber logov bezpečnostných údajov
			Integrácia systémov
		Nefukčné	OS kompatiblita
	Spracovanie logov	Funkčné	zber logov
			rozšírenia
		Nefukčné	Viaczdrojý zber
			Prepojenie so SIEM
	SOAR		
		Funkčné	orchestrácia procesov
		Nefunkčné	automatizované scenáre
			API rozhranie
			integrácia s ekosystémom
	Detekcia pomocou ML		
		nefunkčné	Viaczdrojové dáta
			Integrácia výstupov ML
	Vizualizácia dát	Funkčné	SIEM integrácia
		Nefunkčné	dynamická aktualizácia
			Prepojenie dát
	Alertovanie		
		nefunčné	prepojenie s reakciou
	EDR/XDR		
		Funkčné	Preposielanie incidentov
		nefunkčné	
			flexibilný zber dát
	CTI	Funkčné	Zber dát o hrozbách
			SIEM integrácia
		Nefunkčné	Automatizovaný zber CTI
			Prepojenie CTI so systémami
			Štandardný formát CTI
	Asset management		
		Funkčné	Integrácia asset databázy
			import/export
		Nefunkčné	Integrácia s monitoringom
	Skener zraniteľnosti	nefunkčné	integrácia výstupov
	Zdroje bezpečnostných údajov		
		Funkčné	Zber endpoint logovb
			zber logov z bezpečnostných nástrojov
		Nefunkčné	rozšíriteľnosť zdrojov
			podpora typov logov
	Knowedge base		
		Nefunkčné	Prepojenie na systémy
	Ticketing	Nefunkčné	Integrácia s reakčnými systémami
	Evidencia a správa incidentov	nefunkčné	Integrácia incident manažmentu

Rola			
Koncový používateľ	Vizualizácia dát	nefunkčné	jazyková lokalizácia

Rola

manažer	SIEM	nefunkčné	podpora OSS
	Detekcia pomocou ML	nefunkčné	vysvetliteľnosť modelu
	vizualizácia dát	nefunkčné	vizualizačné šablóny
	alertovanie	nefunkčné	audit alertov
	Asset management	funkčné	klasifikácia
	skener zraniteľnosti	nefunkčné	otvorený nástroj
	knowledge base	funkčné	znalostná báza
		nefunkčné	tvorba záznamov
	Ticketing	funkčné	priradenie tiketu
		nefunkčné	priradenie riešiteľa
			meranie výkonu riešenia
	Reportovanie		
		funkčné	filtrovanie obsahu
		nefunkčné	plánované aj manuálne výstupy
	Voliteľné rozšírenia	funkčné	SLA monitoring a reporting
		nefunkčné	audítorské výstupy

Rola

Administrátor	SIEM	nefunkčné	UX správy aktív
			riadenie prístupu
			správa dát
			aktualizácia a konfigurácia
	Spracovanie logov		
		funkčné	vizualizácia
		nefunkčné	normalizácia logov
			archivácia logov
	Vizualizácia dát		
		funkčné	prihlásenie
		nefunkčné	záloha vizualizácie
	Alertovanie	funkčné	pravidlá
			odosielanie notifikácií
	EDR/XDR		
		Funkčné	zber auditných údajov
		nefunkčné	flexibilný zber dát
	Asset management		
		Funkčné	evidencia IT aktív
			sledovanie zmien
			import/export
		nefunkčné	UX správy aktív
			ochrana dát o aktívach
	Skener zraniteľnosti		
		funkčné	aktualizácia databázy
			plánovanie skenovania
			reporting
	Zdroje bezpečnostných údajov	funkčné	zber endoint logov

Rola

analytik	Spracovanie logov	funkčné	Vizualizácia
		nefunkčné	Vizualizačná kompatibilita
	SOAR		
		nefunčné	reverzná reakcia
	Detekcia pomocou ML		
		Funkčné	predikcia incidentov
	Vizualizácia dát	Nefunkčné	dynamická aktualizácia
			Konfigurovateľné dashboardy
			Vizualizačné šablóny
	Alertovanie		
		Nefunkčné	Prispôsobenie alertov
	EDR/XDR	Nefunkčné	viacdátový zber
			automatická reakcia
			vizualizácia EDR dát
	Asset management		
		nefunkčné	Integrácia s monitoringom
			Vyhľadávanie aktív
	Skener zraniteľnosti		
		nefunkčné	aktualizácia testov
			použiteľnosť GUI
			integrácia výstupov
	knowledge base		
		funkčné	správa záznamov
			vyhľadávanie
		nefunkčné	prehľadná báza znalostí
	Evidencia a správa incidentov		
		Funkčné	Hodnotenie incidentov
		nefunkčné	GUI pre incidenty
			prepojenie s dôkazmi
			integrácia incidentov manažmentu
	Reportovanie		
		funkčné	Export
		nefunkčné	plánovanie aj manuálne výstupy
			export reportov
			konfigurovateľné výstupy

Rola

Manažér bezpečnosti	SIEM	Funkčné	Dashboard
			Reporting
		Nefunčná	Regulačná zhoda
	SOAR		
		Funkčné	Evidencia
		Nefunkčné	audit činností
	Detekcia pomocou ML		
		Funkčné	Predikcia incidentov
	Vizualizácia dát		
		Funkčné	Dashboard
	Alertovanie		
		Funkčné	Odosielanie notifikácií
		Nefunkčné	Eskalačné pravidlá
	EDR/XDR		
		Funkčné	Dashboard
	CTI		
		Nefunkčné	Rozsah CTI vrstiev
	Asset management		
		Nefunkčné	Audit zmien aktív
	Skener zraniteľnosti		
		Funkčné	Prehľad zraniteľnosti
		Nefunkčné	Podpora súladu
	Ticketing		
		Funkčné	Notifikovanie
		Nefunkčné	História spracovania
	Evidencia a správa incidentov		
		Funkčné	Hodnotenie incidentov
		Nefunkčné	Export incidentov
	Reportovanie		
		Funkčné	Bezpečnostný report
			Automatizácia
		Nefunkčné	Vizualizované reporty
	Asministratíva systému		
		Funkčné	Audit zmien systému
	Voliteľné rozšírenia		
		Funkčné	Compliance monitoring
		Nefunkčné	Kontrola zhody

Rola

Bezpečnostný analytik	SIEM	Funkčné	Korelácia udalostí	Korelácia bezpečnostných udalostí
			Detekcia hrozieb	Detekcia hrozieb v reálnom čase
			Dashboard	Prehľadné vizualizácie a dashboardy
		Nefunkčné	Integrácia s nástrojmi	Integrácia s inými nástrojmi (napr. XDR, vizualizačné nástroje)
			Korelácia udalostí	Analytické schopnosti a korelácia dát (Korelácia dát)
			Užívateľské rozhranie	Používateľské rozhranie a UX (GUI)
	Spracovanie logov			
		Funkčné	Filtrovanie	Normalizácia a filtrovanie logo
			Vyhľadávanie	Vyhľadávanie v zozbieraných logoch
		Nefunkčné	Normalizácia logov	Podpora normalizácie logov
			Vyhľadávanie logov	Výkonné vyhľadávanie a filtrovanie záznamov
	SOAR			
		Funkčné	Automatizácia	Automatizácia reakcií na bezpečnostné incidenty
			Kategorizácia	Kategorizácia a triedenie incidentov
			Playbook	Tvorba a úprava playbookov
		Nefunkčné	Automatizované scenáre	Podpora workflow a playbookov (automatizované scenáre reakcie)
			Konfigurovateľné playbooky	Flexibilita v konfigurácii scenárov
			Kategorizácia incidentov	Možnosť kategorizácie incidentov a pravidiel ich riešenia
	Detekcia pomocou ML			
		Funkčné	Detekcia anomálií	Detekcia sieťových a operačných anomálií pomocou ML
		Nefunkčné	Presnosť detekcie	Presnosť detekcie anomálií (napr. sieťových, phishing, spam, malware)
			Pipeline pre učenie	Zber a príprava dát pre trénovanie modelov (data pipeline)
			Vysvetliteľnosť modelu	Možnosť vysvetlenia výsledku ML modelu (explainability)
	Vizualizácia dát			
		Funkčné	Dashboard	Tvorba interaktívnych dashboardov
			Šablóna	Podpora šablón pre rôzne typy vizualizácií
			Korelácia	Korelácia dát vo vizualizáciách
		Nefunkčné	Grafické rozhranie	Grafické používateľské rozhranie (GUI)
			Korelačné vizualizácie	Korelačné pravidlá a ich vizualizácia
	Alertovanie			
		Funkčné	Automatizácia	Generovanie notifikácií o bezpečnostných udalostiach
			Pravidlá	Definovanie pravidiel pre upozornenia
			Automatické vyplňanie alertu	Oznámenia prostredníctvom e-mailu a ďalších kanálov
		Nefunkčné	Reálne časy alertov	Podpora real-time notifikácií o incidentoch
			Podmienkové pravidlá	Podpora podmieneného generovania alertov (logika „ak-tak“, korelácia)
			Prepojenie s reakciou	Podpora integrácie s ticketingom a SOAR
	EDR/XDR			
		Funkčné	Monitorovanie	Monitorovanie aktivít na koncových zariadeniach
			Reakcia na incident	Reakcia na incidenty na koncových zariadeniach
			Zber auditných údajov	Zber a spracovanie auditných údajov
		Nefunkčné	Detekcia hrozieb	Detekcia a klasifikácia malvéru, narušení, podozrivého správania
	CTI			
		Funkčné	Vytvorenie IOC	Tvorba a aktualizácia hrozbových indikátorov
		Nefunkčné	Vizualizácia hrozieb	Možnosť vizualizácie hrozieb (napr. MITRE ATT&CK)
			Automatizované CTI playbooky	Podpora integrácie playbookov pre CTI spracovanie
	Asset management			
		Funkčné	Evidencia IT aktív	Evidencia a správa všetkých aktív v organizácii
			Klasifikácia	Rozlíšenie aktív podľa typu a kritickosti
		Nefunkčné	Typy aktív	Podpora rôznych typov aktív (hardvér, softvér, cloud, kontajnery, služby)
	Skener zraniteľnosti			
		Funkčné	Detekcia zraniteľností	Identifikácia zraniteľností v IT infraštruktúre
			Plánovanie skenovania	Možnosť plánovania a opakovania skenov
			Prehľad zraniteľností	Zobrazenie výsledkov a priorizácia zraniteľností
			Reporting	Export reportov a notifikácie o nálezoch
		Nefunkčné	Plánovanie skenov	Podpora plánovaného aj ad-hoc skenovania
			Prioritizácia rizík	Podpora EPSS a CVSS scoringu
	Zdroje bezpečnostntných údajov			
		Funkčné	Zber endpoint logov	Zber logov a auditných údajov zo serverov a endpointov
			Zber dát z infraštruktúry	Zber sieťových dát z infraštruktúry
			Normalizácia údajov	Normalizácia zozbieraných údajov
		Nefunkčné	Normalizované logy	Štandardizácia a normalizácia formátov údajov
	Knowledge base	Funkčné	Znalostná báza	Centrálne úložisko znalostí pre SOC tím
	Ticketing	Nefunkčné	Stavy tiketov	Možnosť zmeny stavu tiketov a workflow spracovania
			Integrácia s reakčnými systémami	Integrácia so SOAR a SIEM systémami
	Evidencia a správa incidentov			
		Funkčné	Prepojenie incidentov s dátami	Prepojenie incidentov s tiketmi a logmi
			Archivácia	Uchovávanie záznamov pre audit a forenzné účely
		Nefunkčné	Detailný záznam incidentu	Možnosť zaznamenať kompletné detaily incidentu (čas, zdroj, dopad, opatrenia)
			Kategozácia incidentov	Možnosť klasifikácie a kategorizácie incidentov (napr. podľa typu, závažnosti, služby)

Rola

Správca systému	SOAR	nefunkčné	Bezpečné akcie
	Vizualizácia dát	nefunkčné	jednotné prihlásenie
	alertovanie	nefunkčné	viackanálové doručenie
			šifrované alerty
	EDR/XDR	nefunkčné	podpora viacerých prostredí
	Asset management	nefunkčné	kategorizácia aktív
	Skener zraniteľností	nefunkčné	bezagentový sken
	Zdroje bezpečnostných údajov	nefunkčné	podpora agentov
	Knowledge base	nefunkčné	oprávnenia k znalostiam
	Ticketing	nefunkčné	oprávnenia k tiketom
	Evidencia a správa incidentov	nefunkčné	oprávnenia incidentov
	Reportovanie	nefunkčné	riadený prístup k výstupom
			Export reportov
	Administratíva systému	nefunkčné	prístup podľa rolí

Rola

Operátor	vizualizácia dát	nefunkčné	dynamická aktualizácia
			grafické rozhranie
	alertovanie	nefunkčné	reálne časy alertov
	EDR/XDR	nefunkčné	automatická reakcia
			vizualizácia EDR Dát
	CTI	nefunkčné	Real time obohatenie
	asset management	nefunkčné	ux správy aktív
	skener zraniteľnosti	nefunkčné	výkonnostný rozsah
	zdroje bezpečnostných údajov	nefunkčné	validácia logov
	knowledge base	nefunkčné	prehľadná báza znalostí
	ticketing	nefunkčné	správa tiketov
			emailové upozornenia
	administratíva systému	nefunkčné	správcovské rozhranie

Rola

Auditor	SIEM	Funkčné	Dashboard
			Reporting
		Nefunkčné	Regulačná zhoda
			Správa dát
			Nasaditeľnosť v kontajneroch
	SOAR	Funkčné	Evidencia
		Nefunkčné	Audit činností
	Asset management		
		Funkčné	Sledovanie zmien
	Evidencia a správa incidentov		
		Funkčné	Archivácia
	Reportovanie		
		Funkčné	Bezpečnostný report
	Voliteľné rozšírenia		
		Funkčné	Compliance monitoring
	Administratíva systému		
		Nefunkčné	Autid zmien systému
	CTI	Nefunkčné	Bezpečnosť CTI dát
	Alertovanie	Nefunkčné	audit alertov

Architekt riešenia	SIEM	Funkčné	Spracovanie údajov
		Nefunkčné	škálovanie systému
	Spracovanie logov		
		Nefunkčné	Vizualizačná kompatibilita
			archivácia logov

Rola

Vývojár	SIEM	Funkčné	Rozšírenia
		Nefunkčné	Integrácia s nástrojmi
	SOAR		
		Nefunkčné	API rozhranie
	Detekcia pomocou ML		
		Funkčné	Knižnice ML
		Nefunkčné	Viaczdrojové dáta
			Modulárne modely
			Správa modelov
	Zdroje bezpečnostných údajov		
		Funkčné	Rozšíriteľnosť zdrojov

Rola

DevOps	SIEM	Funkčné	Rozšírenia
			Nasadenie
		Nefunkčné	Aktualizácie a konfigurácia
			Nasaditeľnosť v kontajneroch
	Spracovanie logov		
		Nefunkčné	škálovanie spracovania
			Kontajnerizovateľnosť
	Detekcia pomocou ML		
		Funkčné	Aktualizácia ML
		Nefunkčné	škálovateľnosť výpočtov
	Skener zraniteľnosti		
		Funkčné	Agentless skenovanie
	Zdroje bezpečnostných údajov		
		Funkčné	Logovací agenti
	Administratíva systému		
		Funkčné	Konfigurácia systému
		Nefunkčné	Automatizovaná konfigurácia
			Aktualizácia systému
			Kontajnerové nasadenie
	Voliteľné rozšírenia		
		Funkčné	Backup

Rola

Bezpečnostný architekt	SIEM	Funkčné	Zabezpečenie údajov
		Nefunkčné	Šifrovanie dát
	SOAR		
		Nefunkčné	Bezpečné akcie
	Detekcia pomocou ML		
		Funkčné	Hodnotenie modelov
	Vizualizácia dát		
		Funkčné	Prihlásenie
	EDR/XDR		
		Nefunkčné	Bezpečné dáta
	Zdroje bezpečných údajov		
		Nefunkčné	Bezpečný zber
	Knowledge base		
		Funkčné	Riadenie prístupu
	Evidencia a správa incidentov		
		Funkčné	Archivácia
	Administratíva systému		
		Funkčné	Správa prístupov

Rola

Systémový architekt	SIEM	Nefunkčné	Podpora OSS
			Nasaditeľnosť v kontajneroch
	Spracovanie logov		
		Funkčné	škálovanie spracovania
	SOAR		
		Nefunkčná	reverzná reakcia
	Detekcia pomocou ML		
		Nefunkčné	rýchlosť reakcie
	Skener zraniteľnosti		
		Funkčné	Agentless skenovanie
	Aministratíva systému		
		Nefunkčné	Kontajnerové nasadenie