

V8 zoznam definovaných kritérií
V8_ML

V8 zoznam definovaných kritérií

KPB3 – Návrh ML algoritmov; typ – zoznam; mesiac odovzdania – M12



PLÁN OBNOVY


 ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

 Zbierka dokumentov v súvislosti
s týmto projektom

BRAIN:IT

V8_ML
Zoznam definovaných kritérií

názov kritéria	stručný popis	vysvetlenie priradenia bodov	rozšírený popis
1 Presnosť detekcie anomálií (Precision, Recall, F1)	Ako presne algoritmus deteguje anomálie bez ohľadu na triedu	1 – F1 pod 0.7; 2 – F1 0.7–0.8; 3 – F1 0.8–0.9; 4 – F1 nad 0.9; 5 – výnimočná presnosť, aj pri neoznačených dátach.	Vyhodnotenie celkovej presnosti pomocou metrik ako Precision, Recall, F1-score alebo AUC-ROC.
2 Miera falošných poplachov (False Positives/Negatives)	Ako často algoritmus generuje falošné pozitíva/negatíva	1 – FP/FN nad 20 %; 2 – FP/FN 10–20 %; 3 – FP/FN 5–10 %; 4 – pod 5 %; 5 – takmer nulové falošné poplachy.	Zníženie miery falošných poplachov je kľúčové pre použiteľnosť v SOC. Ideálne modely majú veľmi nízky počet FP/FN.
3 Podpora učenia bez labelov (unsupervised)	Schopnosť učiť sa zo vstupných dát bez potreby anotácií	1 – iba supervised; 2 – semi-supervised; 3 – základný unsupervised; 4 – pokročilé unsupervised modely; 5 – pokročilé s hybridným prístupom.	Nie všetky modely vyžadujú označené dáta. Unsupervised modely sú výhodné najmä pri veľkých množstvách nelabelovaných údajov.
4 Výpočtová náročnosť (CPU/GPU, pamäť)	Zdroje požadované na tréningovanie a inferenciu modelu	1 – náročné na tréningovanie aj inferenciu; 2 – vysoká záťaž; 3 – stredná; 4 – optimalizované; 5 – ľahký deployment s nízkou záťažou.	Hodnotí sa záťaž na výpočtové zdroje vrátane náročnosti na GPU, RAM a trvanie tréningovania.
5 Rýchlosť inferencie (čas detekcie)	Rýchlosť odozvy pri detekcii v produkcii	1 – vyššie ako 1s; 2 – stovky ms; 3 – desiatky ms; 4 – pod 10ms; 5 – real-time pre veľké objemy.	Ako rýchlo dokáže model poskytnúť výsledok na nové dáta. Kritické pre nasadenie v reálnom čase.
6 Robustnosť voči zmene distribúcie dát (drift, noise)	Odolnosť voči šumu, zmenám v dátach alebo útokom	1 – náchylné na šum; 2 – málo odolné; 3 – priemerná robustnosť; 4 – stabilné; 5 – odolné aj pri adversarial vstupoch.	Model musí byť odolný voči neočakávaným zmenám, fluktuáciám alebo noise, inak prestane fungovať správne.
7 Schopnosť práce s časovo-sekvenčnými dátami	Vhodnosť pre dáta s časovým vývojom (napr. logy, sieťová prevádzka)	1 – nevhodný; 2 – iba cez workaroundy; 3 – zvláda sekvencie; 4 – natívne podporuje časové rady; 5 – optimalizovaný pre sekvencie.	Schopnosť zachytiť dočasné vzory a anomálie v časových radoch. Výhodou sú architektúry ako LSTM, Transformer.
8 Flexibilita vstupných údajov (logy, metriky, tokové dáta)	Koľko typov dát model zvládne bez potreby úpravy architektúry	1 – iba jeden typ; 2 – 2 typy; 3 – základná flexibilita; 4 – viacero typov bez úprav; 5 – univerzálny model.	Model musí vedieť pracovať so štruktúrovanými i neštruktúrovanými vstupmi – logy, metriky, sieťové toky.
9 Možnosť adaptívneho/online učenia	Podpora aktualizácie modelu počas prevádzky bez retrainovania	1 – žiadna možnosť; 2 – cez retraining; 3 – batch-based update; 4 – partial update; 5 – continual learning.	Schopnosť aktualizovať model bez nutnosti úplného retrainovania, napr. pomocou online learningu.
10 Možnosť vysvetliteľnosti modelu (interpretability)	Možnosť vysvetliť výstup detekcie analytikovi	1 – úplne neinterpretovateľné; 2 – slabá vysvetliteľnosť; 3 – čiastočne vysvetliteľný; 4 – dobrá podpora; 5 – vysoko vysvetliteľný s vizualizáciami.	Možnosť poskytnúť analytikovi zrozumiteľné vysvetlenie, prečo bola anomália detegovaná.
11			
12			
13			
14			
15			

Body:

logiku priradovania bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priradovať body od 1 do 5, kde 1 = najnižšia hodnota splnenia kritéria a 5 = úplné splnenie kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha priradená kritériu
1	Presnosť detekcie anomálií (Precision, Recall, F1)	0,07
2	Miera falošných poplachov (False Positives/Negatives)	0,10
3	Podpora učenia bez labelov (unsupervised)	0,10
4	Výpočtová náročnosť (CPU/GPU, pamäť)	0,09
5	Rýchlosť inferencie (čas detekcie)	0,10
6	Robustnosť voči zmene distribúcie dát (drift, noise)	0,09
7	Schopnosť práce s časovo-sekvenčnými dátami	0,10
8	Flexibilita vstupných údajov (logy, metriky, tokové dáta)	0,14
9	Možnosť adaptívneho/online učenia	0,13
10	Možnosť vysvetliteľnosti modelu (interpretability)	0,09
11		
12		
13		
14		
15		
súčet váh:		1,000000001

Priradenie bodov k jednotlivým kritériám

		dostupné riešenia									
		Random Forest	Isolation Forest	Autoencoder	LSTM	Transformer	One-Class SVM	GAN	k-Nearest Neighbors (k-NN)	Naïve Bayes	Decision Tree
Kritériá pre SIEM nástroj	Presnosť detekcie anomálií (Precision, Recall, F1)	4	4	4	4	5	3	4	3	2	3
	Miera falošných poplachov (False Positives/Negatives)	3	4	4	4	5	3	3	2	2	3
	Podpora učenia bez labelov (unsupervised)	1	5	5	3	5	4	5	1	1	1
	Výpočtová náročnosť (CPU/GPU, pamäť)	2	3	3	2	1	3	1	2	2	2
	Rýchlosť inferencie (čas detekcie)	4	4	3	2	2	3	2	2	4	4
	Robustnosť voči zmene distribúcie dát (drift, noise)	3	4	4	4	5	3	4	2	2	2
	Schopnosť práce s časovo-sekvenčnými dátami	2	2	3	5	5	2	3	2	1	2
	Flexibilita vstupných údajov (logy, metriky, tokové dáta)	2	4	4	4	5	2	3	2	1	2
	Možnosť adaptívneho/online učenia	2	2	3	4	5	2	2	2	1	2
	Možnosť vysvetliteľnosti modelu (interpretability)	3	2	2	3	3	2	1	3	3	4

Prepočet so zohľadnením váh jednotlivých kritérií

		dostupné riešenia										
		váhy	Random Forest	Isolation Forest	Autoencoder	LSTM	Transformer	One-Class SVM	GAN	k-Nearest Neighbors (k-NN)	Naïve Bayes	Decision Tree
Kritériá pre SIEM nástroj	Presnosť detekcie anomálií (Precision, Recall, F1)	0,07	0,29	0,29	0,29	0,29	0,36	0,21	0,29	0,21	0,14	0,21
	Miera falošných poplachov (False Positives/Negatives)	0,10	0,30	0,40	0,40	0,40	0,50	0,30	0,30	0,20	0,20	0,30
	Podpora učenia bez labelov (unsupervised)	0,10	0,10	0,50	0,50	0,30	0,50	0,40	0,50	0,10	0,10	0,10
	Výpočtová náročnosť (CPU/GPU, pamäť)	0,09	0,17	0,26	0,26	0,17	0,09	0,26	0,09	0,17	0,17	0,17
	Rýchlosť inferencie (čas detekcie)	0,10	0,40	0,40	0,30	0,20	0,20	0,30	0,20	0,20	0,40	0,40
	Robustnosť voči zmene distribúcie dát (drift, noise)	0,09	0,26	0,34	0,34	0,34	0,43	0,26	0,34	0,17	0,17	0,17
	Schopnosť práce s časovo-sekvenčnými dátami	0,10	0,20	0,20	0,30	0,50	0,50	0,20	0,30	0,20	0,10	0,20
	Flexibilita vstupných údajov (logy, metriky, tokové dáta)	0,14	0,29	0,57	0,57	0,57	0,71	0,29	0,43	0,29	0,14	0,29
	Možnosť adaptívneho/online učenia	0,13	0,26	0,26	0,39	0,51	0,64	0,26	0,26	0,26	0,13	0,26
	Možnosť vysvetliteľnosti modelu (interpretability)	0,09	0,26	0,17	0,17	0,26	0,26	0,17	0,09	0,26	0,26	0,34
výsledný súčet pre dané riešenie			2,51	3,39	3,51	3,54	4,19	2,64	2,79	2,06	1,81	2,44