V8 zoznam definovaných kritérií

KPIS – Nákup ML algoritmov, typ – zoznam; meniac sám zdroja – M12

V8_ML

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov	realizácia popis
1	Presnosť detekcie anomálií (Precision, Recall, F1)	Ako presne algoritmus dokazuje anomálie bez chýbania na triedu	1 – F1 pod 0.5; 2 – F1 0.5–0.6; 3 – F1 0.6–0.7; 4 – F1 0.7–0.8; 5 – F1 > 0.8 – výnimočná presnosť, aj pri nevyrovnaných dátach	Vyhodnotenie celkovej presnosti pomocou metrík ako Precision, Recall, F1-score alebo AUC-ROC.
2	Miera falošných pozitívov (False Positive/Negatives)	Ako často algoritmus generuje falošné poplachy/chýbajúce	1 – FPR/FNR nad 20 %; 2 – FPR/FN 10–20 %; 3 – FPR/FN 5–10 %; 4 – pod 5 %; 5 – takmer nulové falošné poplachy	Analýza miery falošných pozitívov je kľúčová pre akceptovateľnosť v SOC. Iba/len modely majú veľmi nízke FPR/FN sú vhodné.
3	Podpora učenia bez štítkov (unsupervised)	Schopnosť učiť sa bez označených dát bez potreby ground	1 – iba supervised; 2 – semi-supervised; 3 – polovičný unsupervised; 4 – plnohodný unsupervised modely; 5 – kombinácia s kvalitnou unsupervised	Ak nie všetky modely, vyhodnotiť vyváženie dát. Unsupervised/semi-supervised, ak výrobné signály pri veľkých množinách a kvalitnom unsupervised.
4	Výpočtová náročnosť (CPU/GPU, pamäť)	Zdroje pri/ako/ako na trénovanie a inferenciu modelu	1 – náročné na trénovanie aj inferenciu; 2 – vysoká náročnosť na GPU; RAM a trvanie trénovania; 3 – ľahký model, ale pomalá inferencia; 4 –	Hodnotí sa zdroje na výpočtové zdroje vrátane náročnosti na GPU, RAM a trvania trénovania.
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 predpovedať 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 dátovej	1 – náchylné na šum; 2 – mało odolné; 3 – priemerná robustnosť; 4 – dobrá; 5 – odolné aj pri adversariálnych útokoch	Model musí byť odolný voči nestabilnosťam v dátach. Robustnosť alebo noise, ak prestane fungovať bez tréningu.
7	Schopnosť práce s časovo-sekvenčnými dátami	Vhodnosť pre série v časovom vývojom (napr. logy, sekvencie prevádzky)	1 – nevhodné pre časové série; 2 – mało vhodné; 3 – priemerné; 4 – dobré; 5 – optimálne pre sekvenčné	Vhodnosť pre časové série alebo sekvencie. Ak model nezvládne časovosť, ak prestane fungovať bez tréningu.
8	Flexibilita vstupných zdrojov (logy, metriky, takmer dáta)	Koľko typov dát model zvládne bez potreby úpravy architektúry	1 – len jeden typ; 2 – 2 typy; 3 – obmedzená flexibilita; 4 – zvládne typov bez úpravy; 5 – univerzálny model.	Model musí vedieť pracovať so štruktúrovanými/ne-sekvenčnými vstupmi – logy, metriky, takmer dáta.
9	Možnosť adaptovateľnosti/online učenia	Podpora aktualizácie modelu počas prevádzky bez obnovovania	1 – žiadna možnosť; 2 – len retraining; 3 – batch-based update; 4 – partial update; 5 – continual learning.	Schopnosť aktualizovať model bez nutnosti úplného obnovovania, napr. pomocou online learning.
10	Možnosť vysvetliteľnosti modelu (interpretability)	Možnosť vysvetliť výstup detekcie analytikovi	1 – úplne nevysvetliteľné; 2 – veľmi vysvetliteľné; 3 – čiastočne vysvetliteľné; 4 – dobrá podpora; 5 –	Možnosť poskytnúť analytikovi zrozumiteľné vysvetlenie, prečo bola anomália detegovaná.
11				
12				
13				
14				
15				

Body:
Iniciálne priradenie bodov pre všetky kritériá je potrebné nastaviť tak, aby bolo možné priraďovať body od 1 do 5, kde 1 = najnižšia hodnota a/alebo kritéria a 5 = najlepšie a/alebo kritéria.

Priradenie váh k jednotlivým kritériám

	názov kritéria	váha jednotlivého kritéria
1	Presnosť detekcie anomálií (Precision, Recall, F1)	0,07
2	Miera falošných pozitívov (False Positive/Negatives)	0,10
3	Podpora učenia bez štítkov (unsupervised)	0,10
4	Výpočtová náročnosť (CPU/GPU, pamäť)	0,08
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 zdrojov (logy, metriky, takmer dáta)	0,14
9	Možnosť adaptovateľnosti/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

		Kritériá pre nákladný ML														
		Presnosť detekcie anomálií (Precision, Recall, F1)	Miera falošných pozitívov (False Positive/Negatives)	Podpora učenia bez štítkov (unsupervised)	Výpočtová náročnosť (CPU/GPU, pamäť)	Rýchlosť inferencie (čas detekcie)	Robustnosť voči zmene distribúcie dát (drift, noise)	Schopnosť práce s časovo-sekvenčnými dátami	Flexibilita vstupných zdrojov (logy, metriky, takmer dáta)	Možnosť adaptovateľnosti/online učenia	Možnosť vysvetliteľnosti modelu (interpretability)	0	0	0	0	0
Hodnotené riešenia	Random Forest	4	4	3	3	3	4	2	3	2	2					
	Isolation Forest	4	4	5	4	4	4	2	4	3	3					
	Autoencoder	5	5	5	2	2	5	3	5	4	2					
	LSTM	5	5	4	2	2	5	5	4	4	2					
	Transformer	5	5	4	1	1	5	5	5	3	2					
	One-Class SVM	3	3	3	3	3	3	2	2	2	3					
	LOF	3	3	3	3	3	3	2	2	2	3					
	K-Means	2	2	5	4	4	2	2	2	3	4					
	Nearest Neighbors (k-NN)	3	3	1	2	2	3	2	2	1	3					
	Naive Bayes	2	2	1	4	4	2	1	1	2	4					
	Decision Tree	3	3	1	4	4	3	2	2	2	4					

Prepočet na zohľadnenie váh jednotlivých kritérií

		Kritériá pre nákladný ML															
		Presnosť detekcie anomálií (Precision, Recall, F1)	Miera falošných pozitívov (False Positive/Negatives)	Podpora učenia bez štítkov (unsupervised)	Výpočtová náročnosť (CPU/GPU, pamäť)	Rýchlosť inferencie (čas detekcie)	Robustnosť voči zmene distribúcie dát (drift, noise)	Schopnosť práce s časovo-sekvenčnými dátami	Flexibilita vstupných zdrojov (logy, metriky, takmer dáta)	Možnosť adaptovateľnosti/online učenia	Možnosť vysvetliteľnosti modelu (interpretability)	0	0	0	0	0	výsledný súčet pre danú riešenie
	váha	0,07	0,10	0,10	0,08	0,10	0,09	0,10	0,14	0,13	0,09	0,00	0,00	0,00	0,00	0,00	
Hodnotené riešenia	Random Forest	0,28	0,30	0,10	0,17	0,40	0,26	0,20	0,29	0,26	0,09						2,01
	Isolation Forest	0,28	0,40	0,50	0,25	0,40	0,36	0,20	0,57	0,39	0,27						3,37
	Autoencoder	0,35	0,45	0,50	0,16	0,20	0,45	0,30	0,57	0,52	0,18						3,37
	LSTM	0,35	0,45	0,40	0,16	0,20	0,45	0,50	0,57	0,52	0,18						3,54
	Transformer	0,35	0,50	0,40	0,08	0,10	0,45	0,50	0,71	0,39	0,18						3,56
	One-Class SVM	0,21	0,30	0,30	0,24	0,30	0,27	0,20	0,29	0,26	0,27						2,64
	LOF	0,21	0,30	0,30	0,24	0,30	0,27	0,20	0,29	0,26	0,27						2,64
	K-Means	0,14	0,20	0,50	0,32	0,40	0,18	0,20	0,29	0,39	0,36						2,76
	Nearest Neighbors (k-NN)	0,21	0,30	0,10	0,16	0,20	0,27	0,20	0,29	0,13	0,27						1,93
	Naive Bayes	0,14	0,20	0,10	0,32	0,40	0,18	0,10	0,14	0,26	0,36						1,81
	Decision Tree	0,21	0,30	0,10	0,32	0,40	0,27	0,20	0,29	0,26	0,36						2,83