S-HOLMES Threat & Benign Scores

Table I and Table II show the measurements of S-HOLMES in terms of threat and benign scores calculated as per every attack stage for DARPA attack scenarios and the two public APT attacks respectively. As S-HOLMES follows the original HOLMES design, threat and benign scores do not change when there is no adversarial activities per the corresponding attack stage.

Table I
S-HOLMES Evaluation on DARPA Attack Scenarios. Threat and Benign Scores are calculated per every attack stage (S1, S2, ..., S7).

Scenario No.	Measurements	S-HOLMES						
		S1	S2	S3	S4	S5	S6	S7
1	Threat Score	13	108	108	1987	1987	55342	1163881
	Benign Score	13	108	108	1328	1328	1328	1328
2	Threat Score	13	108	108	1988	1988	55379	55379
	Benign Score	13	108	108	1331	1331	1331	1331
3	Threat Score	13	108	108	1987	1987	55342	1163881
	Benign Score	13	29	298	298	298	298	298
4	Threat Score	2	5	74	903	903	25153	25153
	Benign Score	7	62	638	638	638	638	638
5	Threat Score	13	29	432	7946	7946	221381	4648997
	Benign Score	7	60	897	16504	16504	16504	16504
6	Threat Score	7	17	247	4530	4530	126199	2653973
	Benign Score	7	60	897	16504	16504	16504	16504
7	Threat Score	13	29	297	5466	96092	96092	96092
	Benign Score	13	108	1110	13650	13650	13650	13650
8	Threat Score	13	108	1110	20414	20414	568743	568743
	Benign Score	13	13	108	1615	19844	19844	19844

Table II
S-HOLMES Evaluation on Public Attacks.

APTs	CTI Report	Report Year	Measurements	S-HOLMES						
				S1	S2	S3	S4	S5	S6	S7
APT41	FireEye [2]	2019	Threat Score	2	18	18	226	226	9002	308730
			Benign Score	2	18	18	338	338	338	338
APT35	Darktrace [1],	2021	Threat Score	7	62	62	1133	1133	45089	948268
	FireEye [3]	2019	Benign Score	10	85	85	1039	1039	1039	1039

References

[1] Darktrace.

[2] FireEye, “Special Report: Double Dragon APT41, a dual espionage and cyber crime operation,” https://content.fireeye.com/apt-41/rpt-apt41, 2019.

[3] FireEye-Mandiant, “M-Trends 2018 report,” https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf, 2018.