How does Endpoint Detection use the MITRE ATT&CK Framework? (Supplementary Materials)

Apurva Virkud, Muhammad Adil Inam, Andy Riddle, Jason Liu, Gang Wang, Adam Bates
University of Illinois Urbana-Champaign
{avirkud2, mainam2, rriddle2, jdliu2, gangw, batesa}@illinois.edu

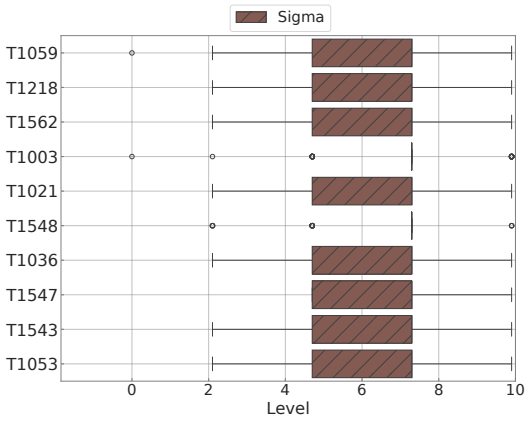

Figure 1: **Criticality Level For Top Techniques:** Qualitative criticality levels are mapped to numeric values based on the CVSS scale. The top 10 techniques across all four rulesets are shown.

A Sigma Criticality Level

We observe fairly consistent criticality within the Sigma ruleset across the top techniques, as shown in Figure 1.

B Malicious Entities Across Rulesets

The 37 malicious entities that appear in at least two of the three commercial rulesets—Carbon Black (CB), Splunk (S), and Elastic (E)—are enumerated in Table 1. The table values indicate the number of unique technique labels in each ruleset as well as in the intersections between them. The table is sorted in descending order by the number of agreeing technique labels.

	CB	S	E	CB ∩ S	CB ∩ E	S ∩ E	CB ∩ S ∩ E
ps1	2	20	15	1	1	7	1
nobelium	16	9	2	4	2	2	2
trickbot	2	13	8	2	1	4	1
sunburst	15	4	5	2	2		
ryuk	1	14	4			2	
solarwinds	12	1	5	1	1		
cve-2022-30190	3	3		2			
wiper	1	27		1			
icedid		15	1			1	
revil		11	1			1	
hafnium		9	1			1	
conti		5	4			1	
fin6		1	5			1	
meterpreter	1	3	1		1		
cve-2021-34527		3	1			1	
cve-2021-4034	1	1	2			1	
cve-2021-42278		1	2			1	
cve-2021-26857		1	1			1	
fin7	2	9	3				
solorigate	6	2					
maze		3	4				
shlayer	6		1				
emotet	3	3					
raindrop	3	2					
apt29	1		3				
doublepulsar	2	2					
teardrop	2	2					
bad rabbit	2	1					
coinminer	1	2					
njrat	2	1					
plugx	2		1				
teamtnt		1	2				
cve-2021-41379		1	1				
kinsing	1	1					
mespinoza		1	1				
pysa		1	1				
qakbot	1	1					

Table 1: **Comparing ATT&CK Technique Labels for Common Malicious Entities**