CYBERAGENT

LIVE THREAT ANALYSIS REPORT

Total Packets Captured

92

Threat Packets

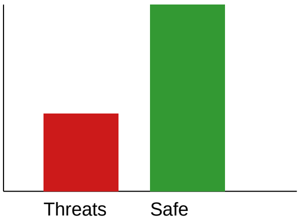
27

Safe Packets: 65

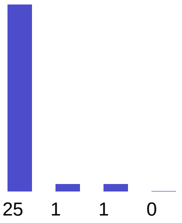
Critical: 25, High: 1, Medium: 1, Low: 0

Threats per Minute: 0

Threat vs Safe Packets



Severity Breakdown



Packet, IP & Dataset Details (recent threats)

Time	Source IP	Dest IP	Port	Severity	Threat Type	Dataset
16:48:56	198.98.45.95	90.95.67.59	53	Critical	SQL Injection	CSE-CIC-IDS 2018 (
16:48:56	184.39.202.218	26.87.245.207	3306	Critical	GraphQL Introspection Abuse	TON_IoT HTTP/REST
16:48:56	229.134.160.92	228.66.211.66	25	Critical	Botnet Activity	HTTP Request Anoma
16:48:56	232.94.111.69	171.175.55.86	445	Critical	HTTP Flood on API Gateway	CSIC 2010 HTTP Web
16:48:56	174.68.214.252	177.230.179.211	445	Critical	SQL Injection	TON_IoT HTTP/REST
16:48:56	226.156.234.229	64.23.178.197	123	Critical	JWT Token Abuse	CIC-IDS 2017 (HTTP
16:48:56	79.246.139.243	181.120.153.83	53	Critical	Mass Assignment in JSON API	CERT Network Flow
16:48:56	198.156.152.3	94.172.226.164	80	High	API Key Leakage	SWaT & WADI ICS HT
16:48:56	42.16.9.136	17.101.112.184	80	Critical	SQL Injection	AWS Open Data – We
16:48:56	233.157.73.203	112.66.211.40	445	Critical	Malware Download	CSE-CIC-IDS 2018 (
16:48:56	206.202.168.102	165.157.8.86	22	Critical	Zero-Day Exploit	SANTA Web Attack D
16:48:56	53.158.212.254	54.156.188.113	123	Critical	Ransomware	Academic WAF Log D
16:48:56	120.232.73.168	81.226.77.195	22	Critical	Phishing	Academic WAF Log D
16:48:56	106.155.174.235	203.92.18.26	25	Critical	REST Endpoint Enumeration	CSE-CIC-IDS 2018 (
16:48:58	221.68.190.9	8.195.44.114	445	Critical	Botnet Activity	OWASP WebGoat Logs
16:48:58	182.59.182.216	14.209.76.61	21	Critical	Ransomware	CERT Network Flow
16:48:58	58.144.15.97	79.7.194.132	445	Critical	Port Scan	SANTA Web Attack D
16:48:58	159.17.248.142	245.19.65.176	123	Medium	HTTP Flood on API Gateway	CSE-CIC-IDS 2018 (
16:48:58	202.148.39.125	59.51.212.191	5432	Critical	REST Endpoint Enumeration	Bot-IoT (API Botne
16:48:58	38.180.199.210	244.244.39.43	25	Critical	Broken Object Level Authorization (BOLA)	AWS Open Data – We
16:48:58	238.52.95.12	30.73.164.53	5432	Critical	HTTP Flood on API Gateway	OWASP WebGoat Logs
16:48:58	187.120.41.47	228.200.226.245	25	Critical	Malware Download	UNSW-NB15 (Modern
16:48:58	156.41.181.106	50.38.73.18	22	Critical	API Key Leakage	CIC-DDoS 2019 (HTT
16:48:58	163.68.101.132	216.144.231.105	53	Critical	Mass Assignment in JSON API	TON_IoT HTTP/REST
16:48:58	47.158.216.61	96.167.200.44	53	Critical	Port Scan	TON_IoT HTTP/REST
16:48:58	151.123.249.244	96.46.132.87	22	Critical	HTTP Flood on API Gateway	CERT Network Flow
16:48:58	54.177.231.37	46.186.201.212	21	Critical	JWT Token Abuse	HTTP Request Anoma

Operational Recommendations

1. Investigate repeated attacks from the same source IPs and block at the perimeter.
2. Review firewall and IDS rules for ports most frequently targeted.
3. Enable deeper logging for critical and high severity events.
4. Correlate these threats with endpoint and SIEM alerts where possible.