CYBERAGENT

LIVE THREAT ANALYSIS REPORT

Total Packets Captured

65

Threat Packets

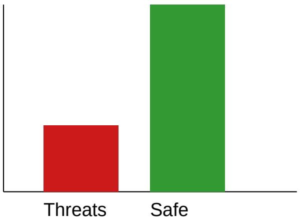
17

Safe Packets: 48

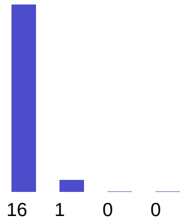
Critical: 16, High: 1, Medium: 0, Low: 0

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
16:48:40	30.44.7.252	93.3.143.13	3306	Critical	Ransomware	Bot-IoT (API Botne
16:48:40	150.212.171.137	42.158.141.109	123	Critical	HTTP Flood on API Gateway	Bot-IoT (API Botne
16:48:40	126.195.207.184	205.79.153.197	8080	Critical	API Authentication Brute Force	TON_IoT HTTP/REST
16:48:40	233.255.133.222	201.79.64.207	21	Critical	Man-in-the-Middle	CSIC 2010 HTTP Web
16:48:40	139.179.3.228	70.109.55.184	80	Critical	Port Scan	UNSW-NB15 (Modern
16:48:40	168.184.254.86	108.171.76.41	21	Critical	API Authentication Brute Force	Academic WAF Log D
16:48:40	64.87.186.211	203.149.104.149	8080	Critical	Mass Assignment in JSON API	CSE-CIC-IDS 2018 (
16:48:40	50.108.243.57	22.252.81.207	22	Critical	GraphQL Introspection Abuse	HTTP Request Anoma
16:48:40	101.157.44.234	51.57.60.132	25	Critical	JWT Token Abuse	Bot-IoT (API Botne
16:48:40	208.34.97.145	80.17.19.182	5432	Critical	Botnet Activity	Academic WAF Log D
16:48:40	233.49.206.47	252.237.54.219	25	Critical	API Authentication Brute Force	UNSW-NB15 (Modern
16:48:40	63.154.143.243	88.156.115.180	123	Critical	Mass Assignment in JSON API	CSE-CIC-IDS 2018 (
16:48:42	66.114.229.58	98.110.102.186	139	Critical	REST Endpoint Enumeration	CSE-CIC-IDS 2018 (
16:48:42	227.102.83.71	201.94.113.38	5432	Critical	Phishing	OWASP WebGoat Logs
16:48:42	62.117.25.99	71.84.50.88	21	Critical	SQL Injection	CIC-BELL-DNS 2021
16:48:42	214.205.84.228	158.113.89.170	139	High	JWT Token Abuse	CIC-BELL-DNS 2021
16:48:42	109.99.230.31	46.170.141.120	443	Critical	HTTP Flood on API Gateway	TON_IoT HTTP/REST

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.