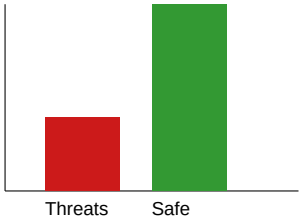
CYBERAGENT
LIVE THREAT ANALYSIS REPORT

Total Packets Captured
85

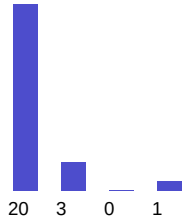
Threat Packets
24

Safe Packets: 61
Critical: 20, High: 3, Medium: 0, Low: 1
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
17:01:39	124.103.168.30	28.240.108.13	22	Critical	Malware Download	TON_IoT HTTP/REST Dataset
17:01:39	34.147.179.85	194.61.187.244	5432	Critical	DNS Tunneling	UNSW-NB15 (Modern Web & App Attacks)
17:01:39	62.250.206.96	16.123.59.99	53	Critical	Phishing	TON_IoT HTTP/REST Dataset
17:01:41	148.166.193.31	8.37.85.12	22	Critical	JWT Token Abuse	CSIC 2010 HTTP Web Attack Dataset
17:01:41	60.90.177.47	208.124.44.58	443	Critical	DNS Tunneling	CIC-DDoS 2019 (HTTP Floods)
17:01:41	117.3.139.125	163.178.125.76	22	Critical	SQL Injection	CERT Network Flow Data (API Misuse)
17:01:41	41.59.147.236	183.245.126.223	5432	Critical	API Key Leakage	CIC-BELL-DNS 2021 (DNS Abuse & Routing)
17:01:41	103.26.30.39	217.93.4.44	123	Critical	Mass Assignment in JSON API	TON_IoT HTTP/REST Dataset
17:01:41	157.166.51.224	189.135.239.16	8080	High	Malware Download	CERT Network Flow Data (API Misuse)
17:01:41	69.190.24.95	47.84.230.82	22	Critical	Zero-Day Exploit	CERT Network Flow Data (API Misuse)
17:01:41	3.96.191.131	9.81.55.91	445	Critical	Broken Object Level Auth...	CSE-CIC-IDS 2018 (Enterprise API/Web ...
17:01:41	242.219.55.182	225.218.29.207	8080	High	Ransomware	Bot-IoT (API Botnet & Anomalies)
17:01:41	163.91.236.127	240.199.221.152	443	High	HTTP Flood on API Gateway	OWASP WebGoat Logs Dataset
17:01:41	144.187.13.24	216.43.225.159	22	Critical	Malware Download	OWASP WebGoat Logs Dataset
17:01:41	188.92.118.1	199.43.86.221	25	Critical	HTTP Flood on API Gateway	OWASP WebGoat Logs Dataset
17:01:41	232.21.221.97	77.114.239.37	139	Critical	Privilege Escalation	CIC-BELL-DNS 2021 (DNS Abuse & Routing)
17:01:41	127.124.88.181	72.226.149.180	5432	Critical	Privilege Escalation	Academic WAF Log Datasets (Sanitized)
17:01:43	44.117.120.86	73.176.203.157	21	Critical	API Key Leakage	SWaT & WADI ICS HTTP/API Traces
17:01:43	26.4.114.13	170.40.37.242	22	Low	API Authentication Brute ...	CIC-BELL-DNS 2021 (DNS Abuse & Routing)
17:01:43	187.234.223.30	24.234.105.13	8080	Critical	Brute Force Login	AWS Open Data – Web & API Logs
17:01:43	42.169.255.16	81.216.146.53	5432	Critical	Insecure Direct Object Re...	OWASP WebGoat Logs Dataset
17:01:43	11.244.72.108	163.162.15.23	3306	Critical	GraphQL Introspection Abuse	AWS Open Data – Web & API Logs
17:01:43	125.104.155.9	145.103.230.71	123	Critical	JWT Token Abuse	CSE-CIC-IDS 2018 (Enterprise API/Web ...
17:01:43	84.38.2.140	187.43.95.171	22	Critical	Privilege Escalation	UNSW-NB15 (Modern Web & App Attacks)

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.