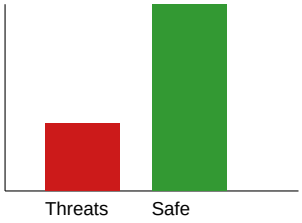
CYBERAGENT
LIVE THREAT ANALYSIS REPORT

Total Packets Captured
105

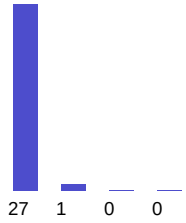
Threat Packets
28

Safe Packets: 77
Critical: 27, 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
17:01:57	180.234.9.195	165.47.119.175	8080	Critical	REST Endpoint Enumeration	OWASP WebGoat Logs Dataset
17:01:57	73.38.196.155	34.180.244.12	22	Critical	REST Endpoint Enumeration	SANTA Web Attack Dataset
17:01:57	246.157.82.44	192.251.191.243	25	Critical	JWT Token Abuse	CIC-IDS 2017 (HTTP & Web Attacks)
17:01:57	194.244.7.149	132.55.169.135	123	Critical	Mass Assignment in JSON API	SWaT & WADI ICS HTTP/API Traces
17:01:57	101.164.111.203	102.135.105.70	5432	Critical	JWT Token Abuse	AWS Open Data – Web & API Logs
17:01:59	198.221.67.231	26.11.53.243	123	Critical	Ransomware	CSIC 2010 HTTP Web Attack Dataset
17:01:59	94.11.206.68	95.4.149.56	123	Critical	Brute Force Login	CIC-BELL-DNS 2021 (DNS Abuse & Routing)
17:01:59	219.110.43.164	153.22.163.202	22	Critical	Data Exfiltration	SWaT & WADI ICS HTTP/API Traces
17:01:59	196.244.40.84	185.240.75.188	53	Critical	Man-in-the-Middle	AWS Open Data – Web & API Logs
17:01:59	52.197.70.86	196.53.175.245	5432	Critical	Ransomware	CERT Network Flow Data (API Misuse)
17:01:59	230.178.107.221	193.135.179.41	443	High	Port Scan	Bot-IoT (API Botnet & Anomalies)
17:01:59	132.240.213.184	205.213.115.81	22	Critical	Port Scan	CIC-BELL-DNS 2021 (DNS Abuse & Routing)
17:01:59	145.233.253.139	10.36.147.42	443	Critical	XSS Attempt	SANTA Web Attack Dataset
17:01:59	175.11.44.92	197.151.184.172	8080	Critical	Privilege Escalation	CSE-CIC-IDS 2018 (Enterprise API/Web ...
17:01:59	120.89.81.99	43.209.23.216	21	Critical	JWT Token Abuse	SWaT & WADI ICS HTTP/API Traces
17:01:59	5.111.7.150	48.222.128.244	8080	Critical	API Key Leakage	CSE-CIC-IDS 2018 (Enterprise API/Web ...
17:01:59	242.138.103.136	69.160.250.140	123	Critical	Zero-Day Exploit	UNSW-NB15 (Modern Web & App Attacks)
17:01:59	134.72.87.195	29.226.97.225	445	Critical	GraphQL Introspection Abuse	CIC-BELL-DNS 2021 (DNS Abuse & Routing)
17:02:01	37.44.169.209	25.107.103.78	123	Critical	API Key Leakage	SANTA Web Attack Dataset
17:02:01	175.172.123.131	124.45.174.72	123	Critical	DDoS Attack	SWaT & WADI ICS HTTP/API Traces
17:02:01	16.38.144.183	223.171.167.229	123	Critical	SQL Injection	CIC-DDoS 2019 (HTTP Floods)
17:02:01	34.87.83.45	93.142.163.195	22	Critical	Man-in-the-Middle	CSIC 2010 HTTP Web Attack Dataset
17:02:01	156.212.180.4	118.157.225.182	53	Critical	DNS Tunneling	HTTP Request Anomaly Research Datasets
17:02:01	200.73.9.36	216.193.5.51	123	Critical	JWT Token Abuse	HTTP Request Anomaly Research Datasets
17:02:01	216.8.242.50	58.250.222.196	21	Critical	JWT Token Abuse	CSE-CIC-IDS 2018 (Enterprise API/Web ...
17:02:01	118.207.179.82	124.252.91.22	443	Critical	Brute Force Login	SANTA Web Attack Dataset
17:02:01	54.156.54.221	111.24.104.218	25	Critical	Insecure Direct Object Re	SWaT & WADI ICS HTTP/API Traces
17:02:01	3.192.1.3	16.62.241.169	22	Critical	REST Endpoint Enumeration	HTTP Request Anomaly Research Datasets

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.