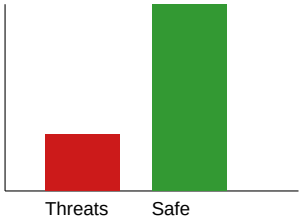
CYBERAGENT
LIVE THREAT ANALYSIS REPORT

Total Packets Captured
43

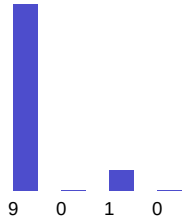
Threat Packets
10

Safe Packets: 33
Critical: 9, High: 0, Medium: 1, Low: 0
Threats per Minute: 0

Threat vs Safe Packets



Severity Breakdown



Packet & IP Details (recent threats)

Time	Source IP	Dest IP	Port	Severity	Threat Type
17:14:22	101.14.165.17	177.111.73.177	8080	Medium	Man-in-the-Middle
17:14:22	245.51.236.202	68.16.165.167	5432	Critical	SQL Injection
17:14:22	72.201.46.255	188.224.106.111	25	Critical	Mass Assignment in JSON API
17:14:22	132.38.226.34	191.156.240.250	443	Critical	Malware Download
17:14:22	25.74.214.7	62.106.49.3	25	Critical	XSS Attempt
17:14:22	253.16.18.35	59.236.221.102	5432	Critical	JWT Token Abuse
17:14:22	231.203.37.185	112.26.12.77	3306	Critical	Privilege Escalation
17:14:22	202.175.236.100	73.6.31.71	8080	Critical	API Authentication Brute Force
17:14:22	133.205.126.214	39.142.148.174	445	Critical	Privilege Escalation
17:14:22	82.150.33.242	133.15.68.99	3306	Critical	XSS Attempt

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.