CYBERAGENT

LIVE THREAT ANALYSIS REPORT

Total Packets Captured

47

Threat Packets

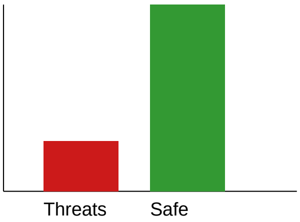
10

Safe Packets: 37

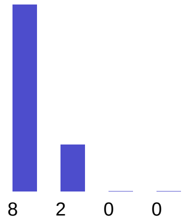
Critical: 8, High: 2, Medium: 0, Low: 0

Threats per Minute: 0

Threat vs Safe Packets



Severity Breakdown



Packet & IP Details (recent threats)

Time	Source IP	Dest IP	Port	Severity	Threat Type
17:05:36	120.124.248.191	101.129.154.47	139	Critical	REST Endpoint Enumeration
17:05:36	41.107.145.148	87.152.16.172	139	Critical	REST Endpoint Enumeration
17:05:36	187.216.190.95	69.216.214.189	5432	High	SQL Injection
17:05:36	111.101.255.158	216.178.10.80	443	Critical	Mass Assignment in JSON API
17:05:36	170.30.95.114	104.5.158.38	53	Critical	Port Scan
17:05:38	135.36.36.78	118.189.187.181	5432	Critical	Broken Object Level Authorizatio...
17:05:38	221.210.49.28	193.16.85.105	139	High	XSS Attempt
17:05:38	163.185.147.33	227.82.42.73	53	Critical	DNS Tunneling
17:05:38	63.156.70.218	8.115.133.249	53	Critical	Mass Assignment in JSON API
17:05:38	98.167.138.184	37.102.142.67	3306	Critical	Ransomware

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.