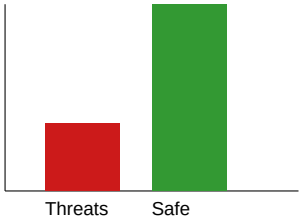
CYBERAGENT
LIVE THREAT ANALYSIS REPORT

Total Packets Captured
124

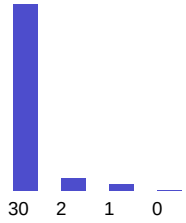
Threat Packets
33

Safe Packets: 91
Critical: 30, High: 2, 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
19:26:24	52.77.213.190	242.105.131.193	3306	Critical	Botnet Activity
19:26:24	2.110.79.164	214.174.17.9	80	Critical	Brute Force
19:26:24	86.210.192.166	107.78.65.150	21	Critical	DNS Tunneling
19:26:24	244.137.44.89	169.186.69.140	3306	Critical	Botnet Activity
19:26:24	191.240.57.225	153.231.252.38	25	Critical	DNS Tunneling
19:26:24	90.74.211.13	180.232.254.135	80	High	Ransomware
19:26:24	98.204.32.235	121.8.145.187	123	Critical	Brute Force
19:26:24	26.241.219.220	132.240.145.129	5432	Critical	Botnet Activity
19:26:24	74.164.224.192	90.214.239.137	22	Critical	XSS Attempt
19:26:24	186.37.203.81	166.138.230.226	3306	Critical	Zero-Day Exploit
19:26:24	114.55.155.15	26.230.164.189	443	Critical	Data Exfiltration
19:26:24	84.48.30.59	95.183.172.164	123	Critical	DNS Tunneling
19:26:26	217.120.65.168	73.232.109.90	123	Critical	Privilege Escalation
19:26:26	48.216.50.86	229.229.38.179	80	High	Malware Download
19:26:26	248.98.253.98	231.113.139.174	80	Critical	SQL Injection
19:26:26	87.50.24.213	23.246.210.243	22	Critical	Port Scan
19:26:26	98.149.135.72	183.222.45.167	80	Critical	Ransomware
19:26:26	232.10.201.17	64.203.75.211	53	Critical	Data Exfiltration
19:26:26	14.206.141.253	239.78.49.180	53	Critical	Ransomware
19:26:26	228.45.14.139	225.229.175.242	8080	Critical	DDoS Attack
19:26:28	30.90.67.18	196.216.241.16	123	Critical	Data Exfiltration
19:26:28	9.48.161.210	111.92.126.10	8080	Critical	Brute Force
19:26:28	250.137.90.212	157.13.167.248	5432	Critical	Port Scan
19:26:28	55.86.198.116	237.18.207.52	139	Critical	Man-in-the-Middle
19:26:28	221.120.123.238	246.64.27.209	445	Medium	SQL Injection
19:26:28	250.75.139.93	194.243.74.50	445	Critical	XSS Attempt
19:26:28	43.251.242.97	126.16.58.34	5432	Critical	Malware Download
19:26:28	212.216.189.235	192.149.78.198	80	Critical	Ransomware
19:26:28	222.213.50.211	117.8.155.129	21	Critical	Brute Force
19:26:28	229.163.143.228	48.103.14.206	8080	Critical	Phishing
19:26:28	209.244.226.80	254.27.161.111	139	Critical	Data Exfiltration
19:26:28	219.106.114.147	138.254.194.242	25	Critical	DNS Tunneling
19:26:28	23.176.118.8	194.46.172.252	25	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.