

# CyberSecurity AI SOC Platform

## Incident Response Report

**Prepared By: Harshith Tadikonda**  
**Environment: Demo SOC Lab**  
**Report ID: SOC-202602030955**

Generated: 2026-02-03 09:55:54.560253

### Executive Summary

Total Alerts: 25  
High Severity: 11  
Medium Severity: 10  
Low Severity: 4

### Executive Insights

Top Attack Vector: DDoS  
Highest Risk IP: 218.142.16.155 (Risk 95)  
Peak Activity Time: 2026-02-01 17:49:17.222734

IP Address	Attack Type	Severity	Risk	Timestamp
151.110.247.231	DDoS	High	60	2026-02-01 17:49:17.222734
152.97.113.113	SQLi	Medium	40	2026-02-01 17:49:14.168074
88.21.217.198	DDoS	High	79	2026-02-01 17:49:11.102768
16.55.153.218	DDoS	Low	75	2026-02-01 17:49:08.046023
240.128.16.66	PortScan	High	62	2026-02-01 17:49:04.989643
50.33.132.220	SQLi	Medium	46	2026-02-01 17:49:01.934697
248.191.83.60	DDoS	Low	80	2026-02-01 17:48:58.875663
239.40.237.66	DDoS	Low	52	2026-02-01 17:48:55.824589
143.164.204.25	PortScan	Medium	37	2026-02-01 17:48:52.767144
152.112.73.87	BruteForce	Medium	94	2026-02-01 17:48:49.751666
171.57.97.58	DDoS	Medium	45	2026-02-01 17:48:46.684064
117.62.87.109	PortScan	High	56	2026-02-01 17:48:43.632000
197.186.197.235	BruteForce	Medium	87	2026-02-01 17:48:40.621594
144.232.114.65	PortScan	High	78	2026-02-01 17:48:37.566063
72.32.69.45	PortScan	High	53	2026-02-01 17:48:34.511780
127.59.139.73	DDoS	High	67	2026-02-01 17:48:31.457209
116.35.147.144	DDoS	Medium	81	2026-02-01 17:48:28.405857
5.132.29.158	DDoS	High	54	2026-02-01 17:48:25.347332
207.173.250.205	BruteForce	Medium	94	2026-02-01 17:48:22.333738
10.226.60.164	DDoS	High	51	2026-02-01 17:48:19.280187
223.160.131.234	PortScan	Medium	91	2026-02-01 17:48:16.216115
95.189.142.217	BruteForce	Low	90	2026-02-01 17:48:13.159371
180.118.19.35	SQLi	High	82	2026-02-01 17:48:10.080327
218.142.16.155	DDoS	Medium	95	2026-02-01 17:48:07.008121

IP Address	Attack Type	Severity	Risk	Timestamp
243.205.131.26	PortScan	High	34	2026-02-01 17:48:03.949891

#### Recommended Actions

- Block highest risk IP immediately
- Enable WAF rules for SQL Injection
- Increase firewall sensitivity for PortScan
- Monitor brute-force attempts for next 24 hours
- Review SOC alerts every 30 minutes

Generated by CyberSecurity AI SOC Engine

© 2026 CyberSecurity AI SOC