

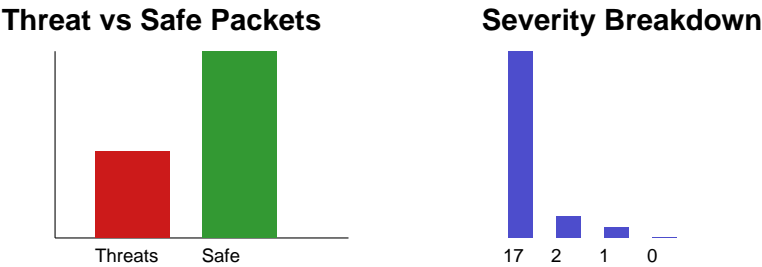
Total Packets Captured

63

Threat Packets

20

Safe Packets: 43
Critical: 17, High: 2, Medium: 1, Low: 0
Threats per Minute: 0



Packet & IP Details (recent threats)

Time	Source IP	Dest IP	Port	Severity	Threat Type
17:05:48	146.206.254.41	36.171.170.240	139	Critical	SQL Injection
17:05:48	241.40.191.98	35.185.40.98	443	Critical	HTTP Flood on API Gateway
17:05:48	246.227.45.28	123.136.117.63	25	Critical	DDoS Attack
17:05:48	92.155.199.160	57.111.142.131	8080	Critical	Broken Object Level Authorizatio...
17:05:48	194.67.206.203	241.175.228.122	8080	Critical	API Key Leakage
17:05:48	207.48.213.206	67.128.19.217	443	Critical	Port Scan
17:05:48	51.174.234.252	144.119.176.131	21	Critical	Mass Assignment in JSON API
17:05:48	140.129.66.9	135.41.195.246	22	Critical	Phishing
17:05:48	58.81.62.170	170.200.209.39	21	Critical	Zero-Day Exploit
17:05:48	196.91.88.101	140.100.212.10	53	Critical	Ransomware
17:05:48	254.217.160.69	222.11.167.121	80	Critical	API Key Leakage
17:05:48	214.36.137.188	247.145.13.51	139	High	Mass Assignment in JSON API
17:05:48	48.179.28.130	30.224.223.247	3306	High	DDoS Attack
17:05:50	75.119.93.52	154.164.160.181	443	Medium	Malware Download
17:05:50	26.166.112.178	101.91.73.59	3306	Critical	HTTP Flood on API Gateway
17:05:52	11.213.162.134	230.2.223.73	3306	Critical	Malware Download
17:05:52	242.125.244.48	180.218.53.173	445	Critical	XSS Attempt
17:05:52	193.52.166.101	34.115.61.250	443	Critical	Mass Assignment in JSON API
17:05:52	152.168.162.197	119.194.153.139	3306	Critical	Malware Download
17:05:52	199.225.18.95	199.190.216.49	8080	Critical	Data Exfiltration

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.