Enterprise Firewall Threat Hunting & Detection Engineering Using Splunk

Prepared by: Sangram Rajput

Project Overview

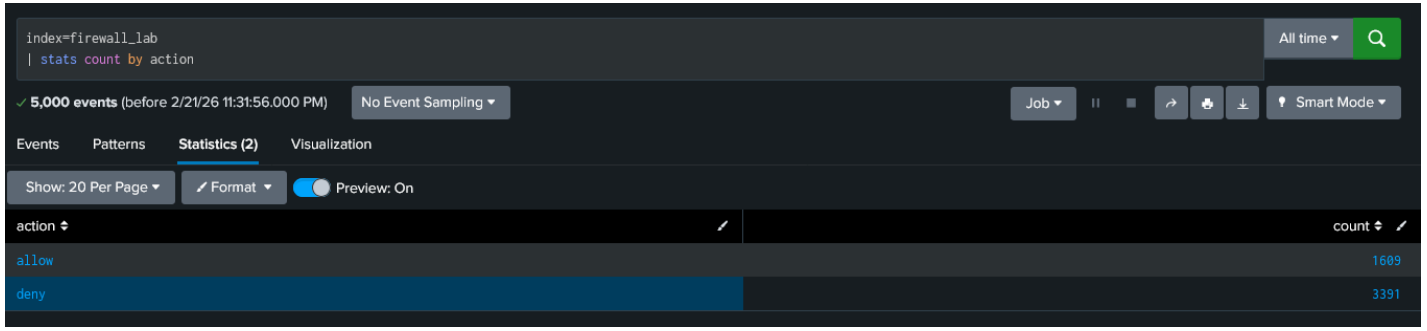
- Objective: Detect reconnaissance & lateral movement using firewall logs
  - Platform: Splunk Enterprise
  - Dataset: 5,000 simulated FortiGate-style firewall events
  - Detection Engineering + Threat Hunting approach

Log Structure

- Fields analyzed:
  - src_ip, dest_ip, dest_port
  - action (allow/deny), protocol, country
  - bytes_sent, bytes_received

Baseline Analysis

- Total Events: 5,000
  - Allow: 1,609
  - Deny: 3,391
  - TCP dominant protocol traffic



Port Scan Detection Logic

- Used distinct port count (dc(dest_port))
  - Identified multiple IPs scanning 14 unique ports
  - Detected both external and internal scanning behavior

src_ip	unique_ports	count
1.1.1.1	14	136
10.0.0.5	14	344
103.25.45.8	14	645
172.16.0.12	14	164
185.243.115.10	14	1159
192.168.1.200	14	134
198.51.100.7	14	133
203.0.113.5	14	147
45.77.12.33	14	141
77.88.55.44	14	134
8.8.8.8	14	148
91.189.88.152	14	106

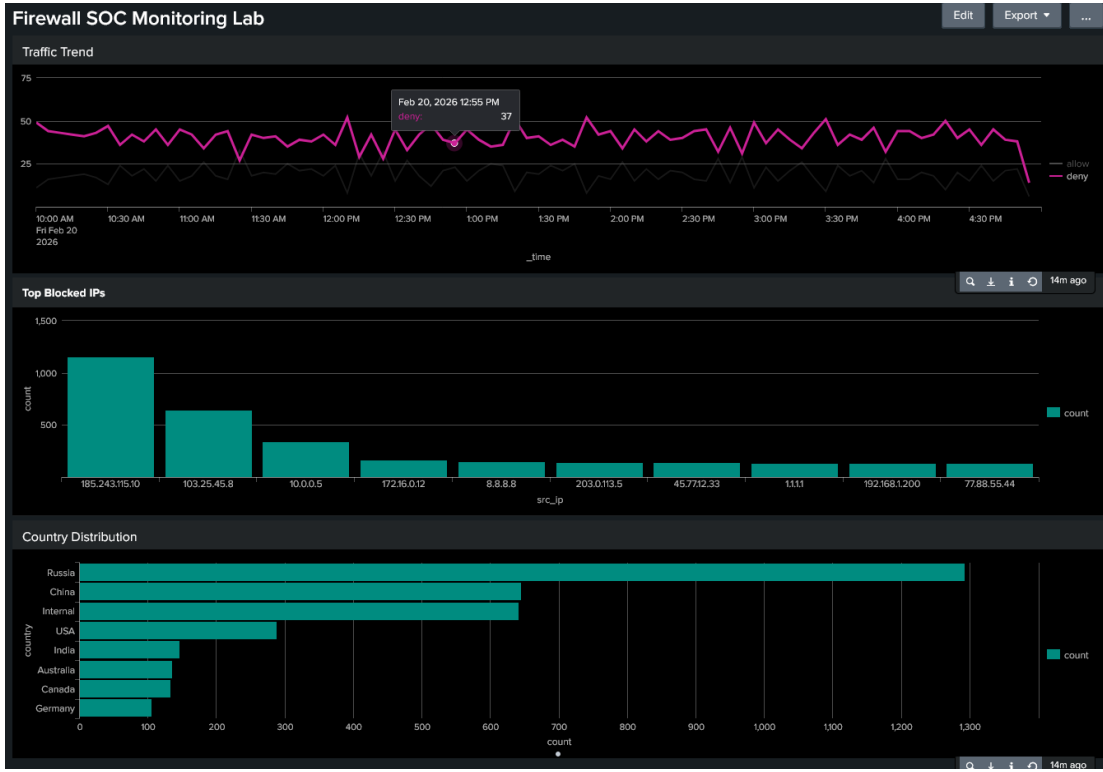
Sensitive Port Monitoring (RDP Exposure)

- Identified 3389 (RDP) as exposed service
- External IP 91.189.88.152 showed highest allowed connections

src_ip	count
91.189.88.152	18
8.8.8.8	16
10.0.0.5	15
198.51.100.7	14
185.243.115.10	13
45.77.12.33	12
192.168.1.200	11
77.88.55.44	11
172.16.0.12	10
103.25.45.8	8
1.1.1.1	7
203.0.113.5	7

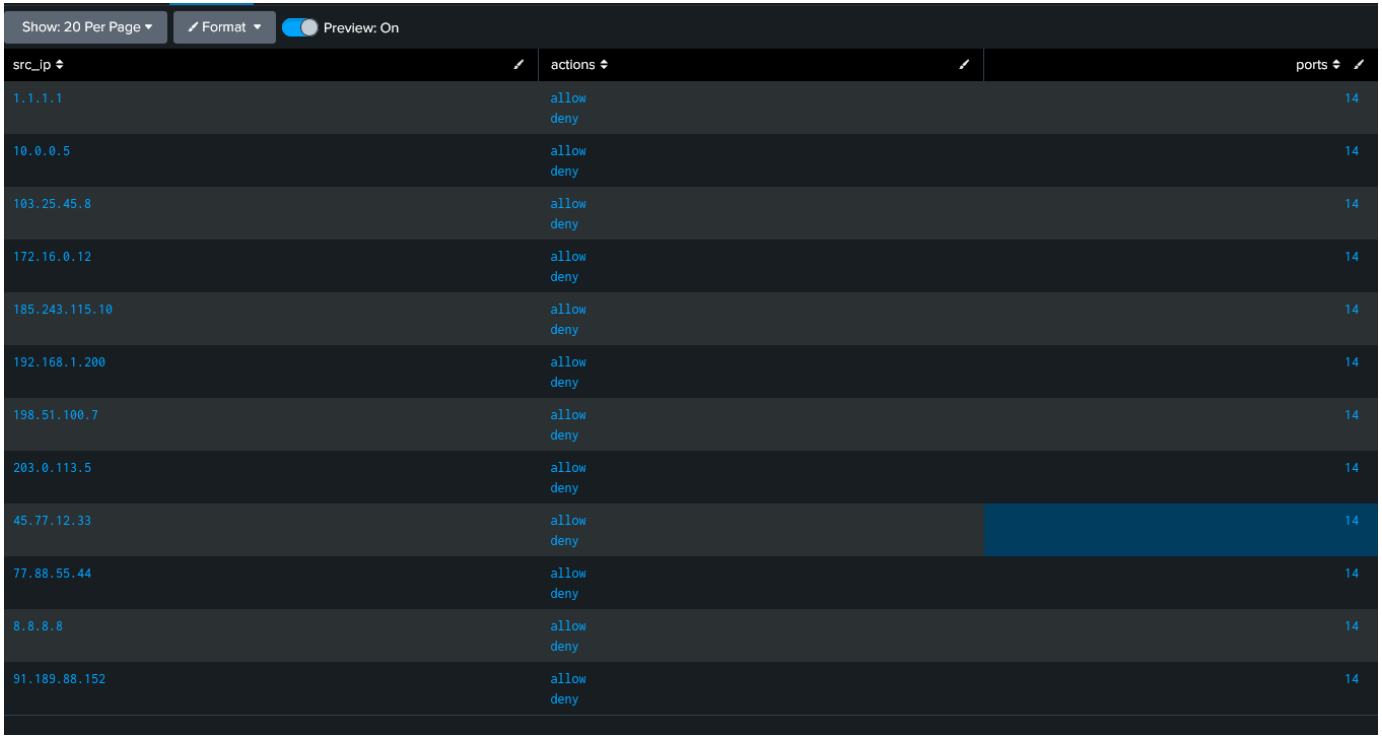
Key Findings

- External IP 91.189.88.152 showed highest successful connection attempts after scanning behavior.
  - Repeated RDP (3389) targeting observed
  - Internal IP 10.0.0.5 scanning 14 ports (possible lateral movement)
  - Top deny countries: Russia, China

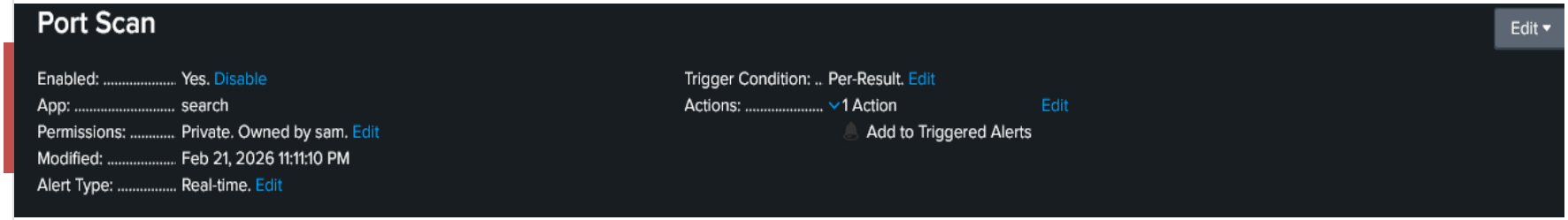


Advanced Correlation Detection

- Identified IPs with both allow + deny traffic
  - Simulated attacker probing then successful connection
  - Created real-time alert for port scanning activity



src_ip	actions	ports
1.1.1.1	allow deny	14
10.0.0.5	allow deny	14
103.25.45.8	allow deny	14
172.16.0.12	allow deny	14
185.243.115.10	allow deny	14
192.168.1.200	allow deny	14
198.51.100.7	allow deny	14
203.0.113.5	allow deny	14
45.77.12.33	allow deny	14
77.88.55.44	allow deny	14
8.8.8.8	allow deny	14
91.189.88.152	allow deny	14



- **Detection Logic:**
  - Trigger when dc(dest_port) > 5
  - Identify IPs scanning multiple services

- **Alert Type:**
  - Real-time monitoring
  - Per-result trigger

- **SOC Action:**
  - Generate triggered alert
  - Escalate for investigation
  - Block malicious IP at firewall

Risk Classification Logic

- High Risk: 3389 (RDP), 445 (SMB)
  - Medium Risk: 22 (SSH)
  - Low Risk: 80 (HTTP)
  - Custom risk-based monitoring logic implemented

SOC Response & Mitigation

- Block malicious external IPs at firewall
  - Investigate exposed RDP services
  - Endpoint investigation for internal host 10.0.0.5
  - Continuous monitoring via Splunk alerts

Conclusion

- Demonstrated enterprise-level firewall monitoring, detection engineering, correlation analysis, and incident response simulation using Splunk.
  - Built dashboards, alerts, and correlation logic
  - Simulated enterprise firewall threat hunting scenario
  - Project ready for GitHub & LinkedIn portfolio

Thank You !

For queries or walk-through, feel free to ask

Prepared by: Sangram Rajput