VPN Log Monitoring & Account Misuse Detection

Project Objectives

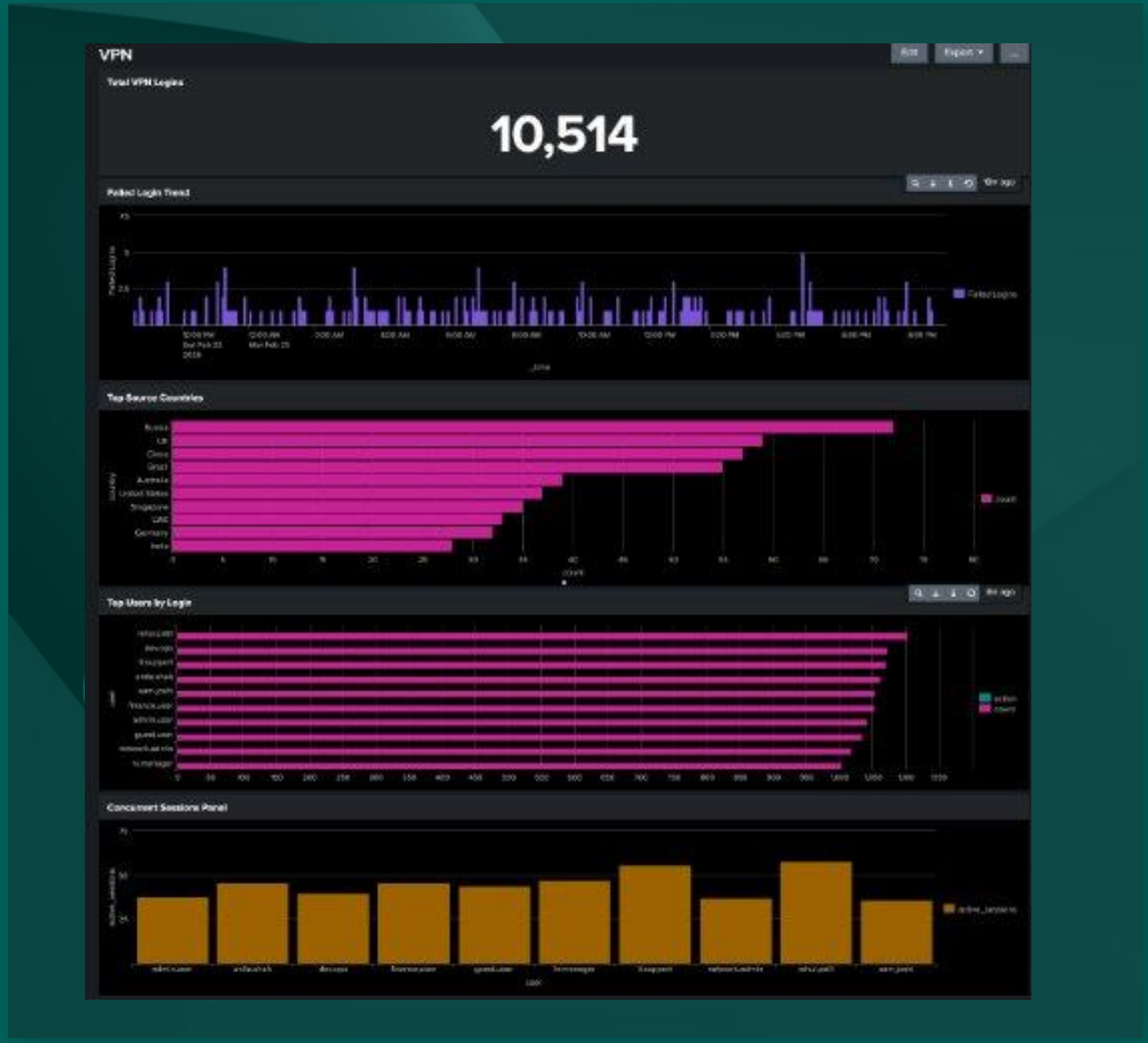
- Monitor VPN authentication logs using Splunk
- Detect account misuse and credential attacks
- Identify anomalous login behavior
- Simulate real-world SOC investigation workflow
- Perform severity classification and escalation

Lab Architecture

- VPN Logs (CSV Dataset)
- Splunk SIEM
- Detection Rules & Alerts
- SOC Investigation
- Incident Escalation

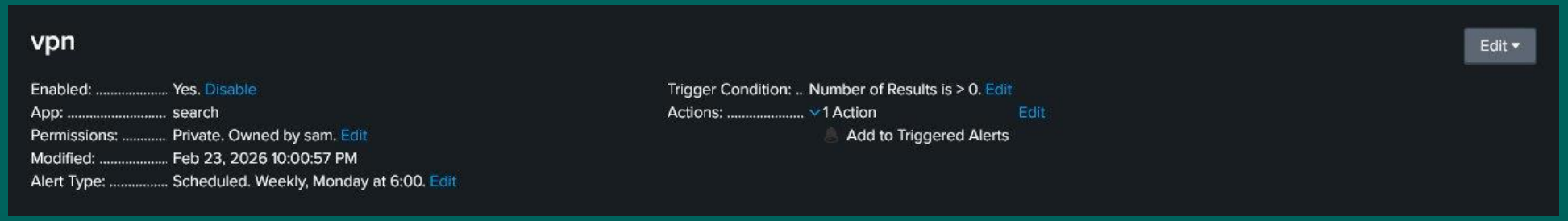
Log Ingestion

- Installed Splunk Enterprise
- Ingested 15,000+ VPN authentication logs
- Parsed fields: user, src_ip, country, action, session_id
- Validated successful & failed login events



VPN Threat Detection Use Cases

- Brute-force login detection
- High-risk country login monitoring
- After-hours login detection
- Impossible travel detection (streamstats logic)
- Concurrent session monitoring



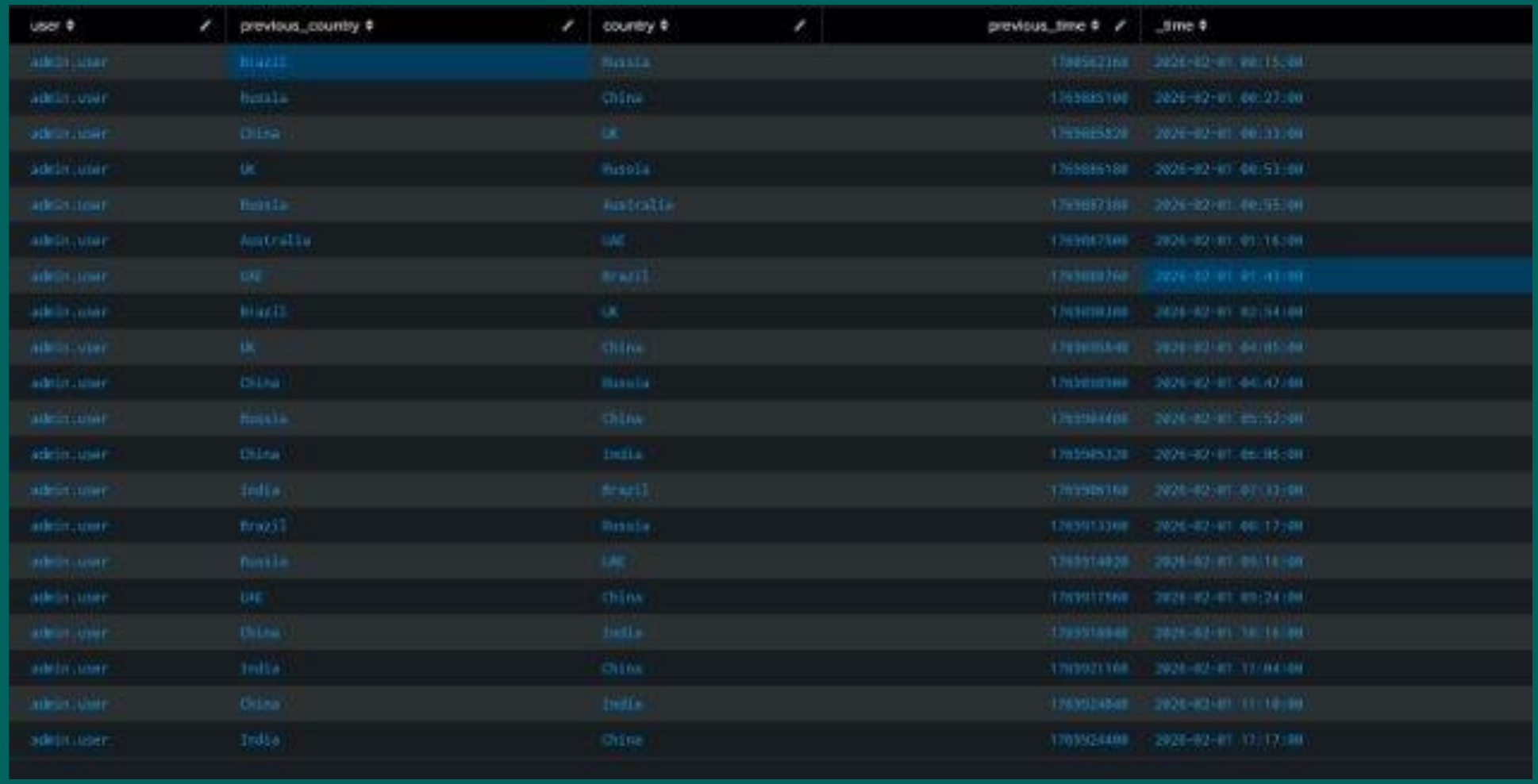
Alert Configuration

- Created **scheduled** alerts in Splunk
- Threshold-based **detection logic**
- Real-time monitoring enabled
- Risk-based severity classification

Incident Case Selection

- Incident ID: VPN-ACCT-001
  Incident Type: Suspicious VPN Login Activity
  Detected By: Splunk SIEM Alert
- Key Indicators:
- Multiple failed attempts
- Login from high-risk country
- After-hours access

Investigation & Evidence



user	previous_country	country	previous_time	_time
admin.user	Brazil	Russia	1765621260	2026-02-01 00:15:00
admin.user	Russia	China	1765885100	2026-02-01 00:27:00
admin.user	China	UK	1765885520	2026-02-01 00:33:00
admin.user	UK	Russia	1765886100	2026-02-01 00:51:00
admin.user	Russia	Australia	1765887160	2026-02-01 00:55:00
admin.user	Australia	UAE	1765887500	2026-02-01 01:16:00
admin.user	UAE	Brazil	1765888760	2026-02-01 01:41:00
admin.user	Brazil	UK	1765890100	2026-02-01 02:54:00
admin.user	UK	China	1765895640	2026-02-01 04:05:00
admin.user	China	Russia	1765898980	2026-02-01 04:47:00
admin.user	Russia	China	1765904400	2026-02-01 05:52:00
admin.user	China	India	1765905120	2026-02-01 06:06:00
admin.user	India	Brazil	1765908760	2026-02-01 07:13:00
admin.user	Brazil	Russia	1765913200	2026-02-01 08:17:00
admin.user	Russia	UAE	1765914820	2026-02-01 08:16:00
admin.user	UAE	China	1765917560	2026-02-01 09:24:00
admin.user	China	India	1765918840	2026-02-01 10:16:00
admin.user	India	China	1765921160	2026-02-01 11:04:00
admin.user	China	India	1765924840	2026-02-01 11:10:00
admin.user	India	China	1765924400	2026-02-01 12:17:00

Severity Classification & Escalation

- Observed:
- ✓ External high-risk IP
  ✓ Multiple failed attempts
  ✓ Suspicious geolocation change
  ✓ After-hours login

1. Final Severity: **HIGH**
2. Escalated to: SOC L2 / Incident Response Team
3. Risk Impact: Potential account compromise

Incident Report & Mitigation

Actions Taken:

- Account locked temporarily
- Password reset enforced
- MFA enabled
- Suspicious IP blocked
- User awareness training recommended

Skills Demonstrated

- Splunk SIEM
- VPN Log Analysis
- Behavioral Detection Engineering
- Impossible Travel Logic (streamstats)
  - Alert Creation & Tuning
- Incident Documentation
- SOC Escalation Workflow

Thank You

Sangram Rajput
Sangramrajput436@gmail.com
https://sangramrajput.netlify.app/