Security Event Analysis

Introduction

This analysis investigates security events derived from authentication logs collected across a hybrid Windows/Linux environment. The logs were analyzed for suspicious behavior such as brute-force attacks, logins from high-risk geolocations, and credential anomalies. Cross-correlation of logs enabled detection of sophisticated multi-step intrusion scenarios.

Implementation Steps

1. Log Sources Analyzed

- **Windows Event Logs** (Winlogbeat ingestion)
- **Linux Syslog Authentication Logs** (Filebeat ingestion)
- **Web Access Logs** (mock data for web login simulation)

2. Interpretation Methodology

- Events were parsed into fields: timestamp, event type, username, source IP, geo-location, user-agent, and message.
- Used Kibana and Elasticsearch queries to:
    - Group events by username and source IP.
    - Identify failed and successful authentication patterns.
    - Detect logins from suspicious countries.
    - Analyze anomalies like login attempts with expired credentials or unusual user agents.

Analysis and Findings

Example 1: Authentication Failures (Windows Event Log Analysis)

- **Events Identified**:

- `authentication_failure` for user `it_support` from **North Korea** and **Iran**.

- **Annotated Log Excerpt**:
  `json`
  CopyEdit

```
{
  "timestamp": "2025-04-28T11:51:28.408895Z",
  "event": "authentication_failure",
  "username": "it_support",
  "source_ip": "198.51.100.24",
  "geo_location": "North Korea",
  "message": "Brute-force attack detected"
}
```

- **Interpretation**:
  - Login attempts from sanctioned countries.
  - Pattern indicates brute-force attack attempts, based on rapid and repeated failures.

Example 2: Successful Login from High-Risk Geo (Linux Syslog Analysis)

- **Events Identified**:
  - `authentication_success` for `root` from **Iran** and `guest123` from **China**.

- **Annotated Log Excerpt**:
  `json`
  CopyEdit

```
{
  "timestamp": "2025-04-24T10:04:28.408895Z",
  "event": "authentication_success",
```

```
  "username": "guest123",
  "source_ip": "45.67.23.89",
  "geo_location": "China",
  "message": "Failed login attempt with suspicious user agent"
}
```

- **Interpretation**:
  - Success after a failed attempt hints at a password guess or credential stuffing.
  - Suspicious user-agent (`Windows NT 10.0; Win64; x64`) used during access.

Example 3: Suspicious Web Access (Web Access Logs - Mock Data)

- **Mock Event**:

```
json
CopyEdit
{
  "timestamp": "2025-04-28T12:20:00Z",
  "event": "web_login_attempt",
  "username": "ceo_login",
  "source_ip": "8.8.8.8",
  "geo_location": "Private IP",
  "user_agent": "Python-requests/2.25",
  "message": "Suspicious automated login detected"
}
```

- **Interpretation**:
  - Automated login attempt simulating API exploitation.
  - Originates outside regular VPN/protected infrastructure.

Correlation Between Log Sources

Scenario: Credential Theft Leading to Privileged Access

Timeline	Event
`2025-04-22T05:48:28Z`	Multiple authentication failures for `it_support` from China (Windows logs).
`2025-04-26T13:02:28Z`	Successful login for `it_support` from a different suspicious IP (Linux syslog).
`2025-04-28T01:17:28Z`	Unauthorized privileged access by `root` from North Korea (web access mock).

Conclusion from Correlation:

- Attacker brute-forced user credentials across platforms.
- Later leveraged valid credentials to access root systems across OS types.
- Attack path shows lateral movement from initial phishing/brute-force to root escalation.

Incident Detection Scenario: Full Event Timeline

Attack Chain Reconstruction:

1. **Initial Breach**:
    - Authentication failures targeting `it_support` account from foreign IPs.
2. **Credential Theft**:
    - Successful `it_support` login from untrusted region (Vietnam/China).
3. **Privilege Escalation**:
    - `root` successful login from same IP block used previously for failed attempts.
4. **Command-and-Control Setup (Mock)**:
    - Unusual outbound traffic detected to external IP (noted in separate mock network logs).

Timeline Chart:

```
sql
CopyEdit
Day 1 → Failed logins → Day 2 → Successful suspicious login
→ Day 3 → Root escalation
```

Alert Triage Process

Step	Action
Initial Detection	Detection rule triggered for multiple authentication failures (>5 failures
Severity	HIGH — privileged accounts targeted, logins from blacklisted countries.
False Positive Identification	Cross-checked user location history (user normally operates from US); foreign logins were highly anomalous.
Escalation	Immediate escalation to Tier-2 SOC analysts due to privilege level
Containment	Account lockout initiated, VPN credentials rotated, IP address blacklisting

Conclusion

This investigation utilized multi-source log analysis to detect, correlate, and respond to sophisticated unauthorized access attempts. Proper log correlation between Windows, Linux, and web access environments revealed a coordinated attack chain from brute-force attempts to privilege escalation.
Triage and severity scoring prioritized alerts for swift escalation, minimizing potential impact.