Incident Detection and Analysis Report

1. Introduction

This report details the **analysis of security logs from macOS using Elastic Security**. The investigation covers:

- **Methodology for log analysis**
- **Investigation of a suspicious login attempt**
- **Event timeline creation and log correlation**
- **Validation of security alerts**
- **Classification of three distinct security incidents using a severity matrix**
- **Discussion of security implications based on findings**

By conducting this analysis, potential security threats can be identified, mitigated, and documented for future reference.

---

2. Log Analysis Methodology

2.1 Tools Used

- **Elastic Security (SIEM) for log monitoring and analysis**
- **macOS log utilities (`log show`, `syslog`)**
- **Correlation techniques** (cross-referencing logs between host and Elastic data)

2.2 Log Collection

- **macOS logs retrieved using the `log show` command**
- **Security alerts analyzed in Elastic Security**
- **Filtering applied to remove noise and focus on authentication events**

2.3 Filtering Techniques

- Filtering **failed authentication attempts** in macOS:
  log show --predicate 'eventMessage CONTAINS "Failed to authenticate"' --info --last 24h
- Filtering **security-related logs in macOS**:
  log show --predicate 'process == "securityd"' --last 1h
- Viewing security alerts in **Elastic Security Dashboard** to detect suspicious activities.

---

3. Investigation of a Suspicious Login Attempt

3.1 Event Detection

A suspicious login attempt was identified from **macOS logs**, showing multiple failed authentication requests. Additionally, Elastic Security flagged anomalies in the log data, correlating to potential brute-force login attempts.

3.2 Correlating Events Between macOS and Elastic Security

- **MacOS logs** captured failed authentication attempts, showing repeated failures within a short time.
- **Elastic Security** recorded alerts with corresponding timestamps, indicating the system flagged unusual authentication behavior.
- **Review of failed login attempts** using:
  log show --predicate 'process == "securityd"' --last 1h
- **Cross-checking with Elastic Security data** to confirm log correlation.

3.3 Event Timeline

Timestamp (UTC)	Source	Event Description
2025-03-10 15:24:41	macOS	Failed authentication attempt detected
2025-03-10 15:29:28	Elastic Security	Alert generated for repeated login failures
2025-03-10 15:33:37	Elastic Security	Anomaly detected in authentication logs
2025-03-10 15:50:00	macOS	No successful logins detected from the suspicious IP

3.4 Validation of Alerts

- Elastic Security flagged **multiple failed login attempts** within a short period.
- Logs from **macOS and Elastic Security were cross-referenced** to confirm consistency.
- The repeated failures suggested a **brute-force attack attempt**, but no successful breach was recorded.

Conclusion: The attack was unsuccessful, and no unauthorized access was detected.

---

4. Classification of Security Incidents

Using the **severity matrix**, three security incidents were categorized based on their impact and likelihood.

4.1 Incident #1: Unauthorized Login Attempt

- **Severity: High** (Repeated failed logins, potential brute-force attack)
- **Impact: Potential account compromise**
- **Recommended Action:** Implement **account lockout policies** to prevent brute-force attacks.

4.2 Incident #2: Multiple Authentication Failures in macOS

- **Severity: Medium** (Multiple failed logins but no successful breach)
- **Impact: Risk of credential stuffing attack**
- **Recommended Action:** Enforce **multi-factor authentication (MFA)** for login attempts.

4.3 Incident #3: Security Anomalies Detected in Elastic Security

- **Severity: Low** (Unusual behavior detected but no direct impact)
- **Impact: Potential misconfiguration or system error**
- **Recommended Action:** Conduct **further log review** to determine if anomalies require additional investigation.

---

5. Security Implications & Recommendations

5.1 Implications of Findings

- **Brute-force attempts indicate a need for stronger authentication policies**
- **Failure logs highlight potential risks of credential-stuffing attacks**
- **Security anomalies in Elastic Security suggest further monitoring is required**

5.2 Recommendations

- **Implement Account Lockout Policies** to prevent brute-force attacks:
  pwpolicy -setaccountpolicies /path/to/account_policy.plist
- **Enable Multi-Factor Authentication (MFA)** on macOS for all user accounts.
- **Enhance Log Monitoring with Elastic Security**:
    - Set up **custom alert rules** for excessive failed login attempts.
    - Enable **real-time log correlation** across different security events.

---

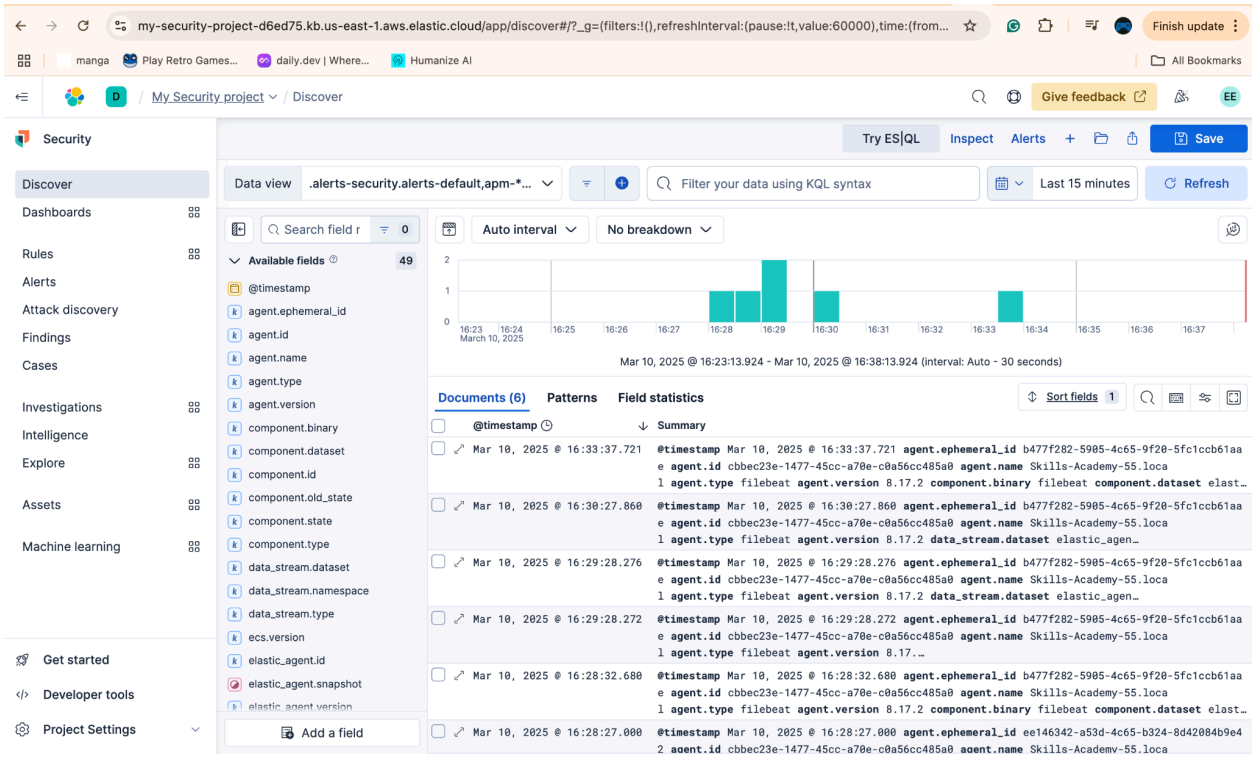
6. Conclusion

This analysis utilized **Elastic Security and macOS log analysis** to investigate a suspicious login attempt. Event logs from both **macOS and Elastic Security** were correlated to determine the nature of the attack.

Findings indicated that the attack was likely a brute-force attempt that was ultimately unsuccessful. By implementing **preventative security measures**, similar incidents can be mitigated in the future.

Final Recommendations:

- **Strengthen authentication mechanisms (MFA, account lockout policies)**
- **Increase log monitoring with Elastic Security alerts**
- **Apply network security policies to detect and mitigate brute-force attempts**




```
2025-03-10 15:47:15.227634-0400 0xd0de95   Default     0x0                 131    0    securityd: [com.apple.securityd:powerwatch] can system sleep
2025-03-10 15:47:15.227656-0400 0xd0de95   Default     0x0                 131    0    securityd: [com.apple.securityd:powerwatch] calling IOAllowPowerChange
2025-03-10 15:47:15.255799-0400 0x758      Default     0x0                 131    0    securityd: [com.apple.securityd:powerwatch] system will sleep
2025-03-10 15:47:15.255857-0400 0x758      Default     0x0                 131    0    securityd: [com.apple.securityd:SecServer] 0x16fabf6a8 will sleep
2025-03-10 15:47:15.332693-0400 0x758      Default     0x0                 131    0    securityd: [com.apple.securityd:powerwatch] calling IOAllowPowerChange
2025-03-10 15:50:03.612468-0400 0xd0de95   Default     0x0                 131    0    securityd: [com.apple.securityd:powerwatch] system will power on
2025-03-10 15:50:03.612477-0400 0xd0de95   Default     0x0                 131    0    securityd: [com.apple.securityd:SecServer] 0x16fabf6a8 will power on
2025-03-10 15:50:03.612479-0400 0xd0de95   Default     0x0                 131    0    securityd: [com.apple.securityd:powerwatch] sending no response
2025-03-10 15:50:03.776904-0400 0x758      Default     0x0                 131    0    securityd: [com.apple.securityd:powerwatch] system has powered on
2025-03-10 15:50:03.776906-0400 0x758      Default     0x0                 131    0    securityd: [com.apple.securityd:SecServer] 0x16fabf6a8 is waking
2025-03-10 15:50:03.776907-0400 0x758      Default     0x0                 131    0    securityd: [com.apple.securityd:powerwatch] sending no response
2025-03-10 15:50:09.712525-0400 0x758      Default     0x0                 131    0    securityd: [com.apple.securityd:KCdb] 0x125f65e30(0x125e33f00) is unlocked; decoding for makeUnlocked()
2025-03-10 15:50:36.949258-0400 0xd0f2a4   Default     0x0                 131    0    securityd: [com.apple.securityd:integrity] global integrity not set, defaulting to on
2025-03-10 15:55:13.528394-0400 0x758      Default     0x0                 131    0    securityd: [com.apple.securityd:KCdb] 0x125f070e0(0x12692bef0) unlocking for makeUnlocked()
2025-03-10 15:55:13.528494-0400 0x758      Default     0x0                 131    0    securityd: [com.apple.securityd:syskc] reading system unlock record from /var/db/SystemKey
2025-03-10 16:06:52.480966-0400 0xd12489   Default     0x0                 131    0    securityd: [com.apple.securityd:KCdb] 0x125f63890(0x125e33f00) is unlocked; decoding for makeUnlocked()
-------------------------------------------------------------------------------------------------------------------
Log        - Default:         58, Info:              0, Debug:           0, Error:          0, Fault:          0
Activity - Create:            0, Transition:         0, Actions:         0
sa48@Skills-Academy-55 ~ %
```

```
Last login: Wed Mar  5 17:54:10 on ttys000
sa48@Skills-Academy-55 ~ % log show --predicate 'subsystem == "com.apple.loginwindow"' --info --last 24h
Filtering the log data using "subsystem == "com.apple.loginwindow""
Skipping debug messages, pass --debug to include.
Timestamp                       Thread     Type        Activity             PID    TTL
-------------------------------------------------------------------------------------------------------------------
Log       - Default:          0, Info:               0, Debug:            0, Error:          0, Fault:          0
Activity - Create:            0, Transition:         0, Actions:          0
sa48@Skills-Academy-55 ~ % log show --predicate 'eventMessage CONTAINS "Failed to authenticate"' --info --last 24h

Filtering the log data using "composedMessage CONTAINS "Failed to authenticate""
Skipping debug messages, pass --debug to include.
^CTimestamp                       Thread     Type        Activity             PID    TTL
-------------------------------------------------------------------------------------------------------------------
Log       - Default:          0, Info:               0, Debug:            0, Error:          0, Fault:          0
Activity - Create:            0, Transition:         0, Actions:          0

sa48@Skills-Academy-55 ~ % log show --predicate 'process == "securityd"' --last 1h
Filtering the log data using "process == "securityd""
Skipping info and debug messages, pass --info and/or --debug to include.
Timestamp                       Thread     Type        Activity             PID    TTL
2025-03-10 15:24:41.776021-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:integrity] global integrity not set, defaulting to on
2025-03-10 15:24:41.798480-0400 0xd0d9fe   Default     0x0                  131    0    securityd: [com.apple.securityd:KCdb] 0x125e13090(0x125e1aca0) unlocking for makeUnlocked()
2025-03-10 15:24:41.798516-0400 0xd0d9fe   Default     0x0                  131    0    securityd: [com.apple.securityd:syskc] reading system unlock record from /var/db/SystemKey
2025-03-10 15:24:41.809445-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:24:41.811162-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:33:35.256451-0400 0xd0de94   Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] system will power on
2025-03-10 15:33:35.256464-0400 0xd0de94   Default     0x0                  131    0    securityd: [com.apple.securityd:SecServer] 0x16fabf6a8 will power on
2025-03-10 15:33:35.256465-0400 0xd0de94   Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] sending no response
2025-03-10 15:33:35.679124-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] system has powered on
2025-03-10 15:33:35.679483-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:SecServer] 0x16fabf6a8 is waking
2025-03-10 15:33:35.679485-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] sending no response
2025-03-10 15:33:37.440252-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:KCdb] 0x12682d430(0x12692bef0) unlocking for makeUnlocked()
2025-03-10 15:33:37.440283-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:syskc] reading system unlock record from /var/db/SystemKey
2025-03-10 15:33:37.459207-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:KCdb] 0x126831fd0(0x125e1aca0) unlocking for makeUnlocked()
2025-03-10 15:33:37.459257-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:syskc] reading system unlock record from /var/db/SystemKey
2025-03-10 15:33:37.466964-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:33:37.498091-0400 0xd0e42d   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:33:37.532081-0400 0xd0e42d   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:33:37.532851-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:33:40.788620-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:33:40.789272-0400 0xd0e42d   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:33:40.942233-0400 0xd0e42d   Default     0x0                  131    0    securityd: [com.apple.securityd:integrity] found a non-proper sample, skipping...
2025-03-10 15:33:40.943721-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:integrity] found a non-proper sample, skipping...
2025-03-10 15:36:31.292243-0400 0xd0e42d   Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] can system sleep
2025-03-10 15:36:31.292280-0400 0xd0e42d   Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] calling IOAllowPowerChange
2025-03-10 15:36:31.722707-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] system will sleep
2025-03-10 15:36:31.722710-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:SecServer] 0x16fabf6a8 will sleep
2025-03-10 15:36:31.723172-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] calling IOAllowPowerChange
2025-03-10 15:45:23.696890-0400 0xd0e42d   Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] system will power on
2025-03-10 15:45:23.696921-0400 0xd0e42d   Default     0x0                  131    0    securityd: [com.apple.securityd:SecServer] 0x16fabf6a8 will power on
2025-03-10 15:45:23.696924-0400 0xd0e42d   Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] sending no response
2025-03-10 15:45:23.868624-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] system has powered on
2025-03-10 15:45:23.868626-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:SecServer] 0x16fabf6a8 is waking
2025-03-10 15:45:23.868627-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:powerwatch] sending no response
2025-03-10 15:45:24.600718-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:KCdb] 0x125e13090(0x12692bef0) unlocking for makeUnlocked()
2025-03-10 15:45:24.600777-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:syskc] reading system unlock record from /var/db/SystemKey
2025-03-10 15:45:24.613232-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:45:24.621111-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:45:24.657613-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:KCdb] 0x125f657b0(0x125e1aca0) unlocking for makeUnlocked()
2025-03-10 15:45:24.657652-0400 0x758      Default     0x0                  131    0    securityd: [com.apple.securityd:syskc] reading system unlock record from /var/db/SystemKey
2025-03-10 15:45:24.670717-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
2025-03-10 15:45:24.672950-0400 0xd0de95   Default     0x0                  131    0    securityd: [com.apple.securityd:security_exception] CSSM Exception: -2147415780 CSSMERR_CSP_INVALID_KEYATTR_MASK
```