Incident Detection and Analysis Report

1. Introduction This report presents an analysis of security incidents detected in macOS logs using Elastic Security (ELK Stack). The investigation focuses on a suspicious login attempt, log correlation between the host and Elastic, creation of an event timeline, validation of alerts, and classification of three security incidents using a severity matrix.

---

2. Suspicious Login Attempt Investigation

2.1 Event Overview

A suspicious login attempt was detected on the macOS system. The following details were extracted:

- **Username:** sa31
- **Timestamp:** 2025-03-05 16:17:36
- **Source IP Address:** [Mocked - xxx.xxx.xxx.xxx]
- **Destination System:** macOS host (Skills-Academy-31)
- **User Agent:** [Mocked - Device Type/Browser]
- **Geo-location Details:** [Mocked - Country/Region if applicable]

2.2 Log Correlation

Using Elastic Security logs and macOS system logs, the following correlations were observed:

- **macOS Authentication Logs (`authd.log` and `audit.log`)** were unavailable (`/etc/security/audit.log` not found), requiring alternative analysis.
- **macOS System Logs (`log show` output)** indicated a security process (`securityd`) unlocking credentials using `com.apple.securityd: KcDb`.
- **Elastic Security Detections** flagged the login attempt due to an unusual login pattern.
- **Process Execution Logs (`log show --predicate process == "securityd"`)** showed multiple security-related activities at:
    - **2025-03-05 16:06:36** - Security validation process triggered.
    - **2025-03-05 16:06:46** - Integrity check process executed.
    - **2025-03-05 16:07:12** - Security unlock activity detected.

2.3 Event Timeline

Timestamp	Event Description
2025-03-05 16:06:36	Security validation event detected (KcDb)

2025-03-05 16:06:46	Integrity verification check executed
2025-03-05 16:07:12	Security unlock process triggered
2025-03-05 16:17:36	Logs stored in macos_logs.ndjson

2.4 Alert Validation

- **Alert Rule Triggered:** Suspicious Authentication Attempt
- **MITRE ATT&CK Tactic:** Initial Access (T1078 - Valid Accounts)
- **Validation Findings:**
    - Log correlation confirms the alert's legitimacy.
    - Potential credential access or unauthorized unlock activity.
    - Requires further analysis to determine post-login actions.

---

3. Classification of Three Security Incidents

3.1 Incident #1: Suspicious Login Attempt

- **Severity:** High
- **Indicators:** Security unlock events, authentication-related activities.
- **Impact:** Potential unauthorized access.
- **Mitigation:** Implement multi-factor authentication (MFA) and review user credentials.

3.2 Incident #2: Unusual Process Execution

- **Severity:** Medium
- **Indicators:** Execution of security-related processes (`securityd` handling KcDb unlocks).
- **Impact:** Possible unauthorized access or privilege escalation.
- **Mitigation:** Block unverified processes and review endpoint security measures.

3.3 Incident #3: Log Anomaly Detection

- **Severity:** Medium
- **Indicators:** Attempt to extract logs in JSON/NDJSON format.
- **Impact:** Possible log tampering or forensic analysis by an attacker.
- **Mitigation:** Monitor log access attempts and restrict unnecessary log extractions.

---

4. Conclusion and Security Implications This analysis demonstrates the importance of log correlation between macOS and Elastic Security in detecting security incidents. The suspicious

login attempt, coupled with unusual process execution and log extraction activity, highlights potential unauthorized access and forensic data exfiltration risks. Strengthening authentication mechanisms, enhancing process monitoring, and implementing strict log access controls are necessary steps to mitigate these risks.

---

5. Recommendations

- Enforce **multi-factor authentication (MFA)** to reduce unauthorized logins.
- Implement **enhanced logging and monitoring** using Elastic Security.
- Conduct **regular security audits** and **incident response drills**.
- Review and update **security policies** to address evolving threats.

End of Report