Incident Response Procedure Format

# Security Event:

Credential Access/Lateral Movement Incident

Date: November 1, 2023 @ 01:19:55

Incident ID: [Auto-generated]

Reported By: [Name/Entity Reporting]

Reporting Date and Time: [Date and Time of Reporting]

# Incident Details:

Target IP Address: 167.71.89.52

Source IP Address: 112.46.22.94

Blacklist Status: Not blacklisted

Handled By SOC Analyst: E1T1JosiUmezur00

System/Hostname: ETTTM-02

MITRE ATT&CK ID: T1021.004

Event of Interest: Attempted login using a non-existent user (check /var/log/auth.log).

Incident Timeline:

Initial Detection: November 1, 2023 @ 01:19:55

Last Detection: November 1, 2023 @ 05:19:53

Incident Description:

< >

**What Happened:** Describe how the incident was detected and its potential impact.

**Evidence:** Mention any suspicious activities, logs, or findings.

**What's Known:** Include details on source and target IP addresses and authentication logs.

**Response Actions:**

*Isolate:* Temporarily disconnect or quarantine the affected system to prevent further spread.

*Gather Data:* Collect logs, system details, and any relevant data about the incident.

Analyze: Investigate the incident to understand its nature and severity. Determine how the attacker attempted to log in.

*Verify User:* Check if the user account exists and confirm if it's a valid login attempt.

*Identify Entry Point:* Determine how the attacker accessed the system and if any vulnerabilities were exploited.

*Mitigate:* Take immediate steps to stop the attack. This may involve disabling accounts, blocking IP addresses, or removing malicious files.

*Notify:* Inform the client, your supervisor, and relevant parties about the incident. Legal and compliance teams may need to be involved.

**Document:** Keep records of actions taken, findings, and any additional incident-related information.

**Classification:** Assign a severity level and priority to the incident.

**Recommendations:** Suggest improvements to prevent future incidents.

**Follow-Up Actions:**

Review: Evaluate existing security measures and apply updates or changes if necessary.

Communication: Keep the affected party informed about the resolution.

Legal: Consider any legal implications or requirements related to the incident.

**Resolution and Closure:**

Describe how the incident was resolved, the final steps taken, and confirmation of closure.

**Incident Review and Lessons Learned:**

Analyze the incident response process and identify areas for improvement or training.

**Additional Comments:**

Include any other relevant information, notes, or feedback related to the incident.

This enhanced form uses plain language and straightforward terms to guide the incident response team through the credential access/lateral movement incident, ensuring that each step is clear and actionable.