Incident Response Report

Incident Type: Insider Misuse

Severity: Low-Medium

Confidence: 0.47

Situation Assessment

Incident Response Situation Assessment

Incident Identification

* Incident ID: [Insert ID]
* Incident Type: Potential Insider Misuse
* Incident Time: 12:30 AM
* Affected System: File Server

Situation Assessment

1. Why this activity is noteworthy

The observed repeated authentication attempts on a file server at 12:30 AM, originating from a valid internal user account, warrant attention due to the unusual timing and potential implications for sensitive directories. This activity deviates from the expected minimal legitimate system activity during non-business hours, indicating a possible anomaly that requires further investigation.

2. Key risk factors in this context

* **Unusual timing**: The activity occurred outside normal business hours, increasing the likelihood of malicious intent.
* **Access to sensitive directories**: The user account in question has access to sensitive directories, which could be compromised if the account is compromised or used maliciously.
* **Potential insider misuse**: The predicted incident type is Insider Misuse, which could result in unauthorized access, data theft, or other malicious activities.

3. Factors that limit certainty or reduce risk

* **Classification confidence**: The classification confidence is 0.47, indicating a moderate level of uncertainty regarding the incident type.
* **Similarity to historical incidents**: The similarity to historical incidents such as Phishing (0.35 and 0.34) and Data Breach (0.32) suggests possible alternative explanations for the observed activity.
* **Lack of additional context**: Insufficient information is available to fully understand the user's intentions, motivations, or potential vulnerabilities exploited.

4. What assumptions should NOT be made yet

* **Malicious intent**: It is premature to assume that the user's actions are malicious or intentional.
* **Compromised account**: The account in question may not be compromised, and the user may have legitimate reasons for accessing sensitive directories during non-business hours.
* **Specific incident type**: The predicted incident type of Insider Misuse should be treated as a hypothesis, and further investigation is required to confirm or rule out this classification.

Recommendations

Based on the current situation assessment, further investigation is required to determine the root cause of the observed activity and to assess the potential risks and impacts.

Response Plan

IR-ID-01 (Identification) - Relevance: 100.0%

IR-ID-02 (Identification) - Relevance: 15.6%

IR-CON-02 (Containment) - Relevance: 51.8%

IR-CON-03 (Containment) - Relevance: 32.7%

IR-CON-01 (Containment) - Relevance: 32.0%

IR-ERAD-01 (Eradication) - Relevance: 29.2%

IR-POST-01 (Post-Incident) - Relevance: 79.0%

Evidence

[Phishing] similarity=0.352
forwarded by john j lavorato cal ect on pm tim heizenrader am to john j lavorato cal ect ect cc tim belden hou ect ect subject west power fundamentals site i ve established an account for you on the west power fundamentals website the url for the site is your username is jlavora your password is calgx this password is different than your normal enron nt password because of authentication requirements of our server and you may need to enter it or times per session depending on how many areas of o

[Phishing] similarity=0.336
john please be advised that effective monday december you will need to access dynegydirect with the following log in user id jarnold password enron please note that these are case sensitive your current log in will no longer be available on monday thank you stephanie sever x

[Data Breach] similarity=0.32
i tried to get into the reports viewer and noted that changes have been made as i am the director responsible for the dpr i need access to all reports please let me know when you have given me access again regards shona x christa winfrey ect pm to brad mckay hou ect ect greg mcclendon hou ect ect peter f keavey hou ect ect larry may corp enron enron mike grigsby hou ect ect sandra f brawner hou ect ect kristin albrecht enron communications enron communications eugenio perez hou ect ect shona wil

[Insider Misuse] similarity=0.309
policy malek attempts then choose sir beating meeting annually against rule attacked time community six under minutes observed parties vast reopened students south complying urdu along line

[Data Breach] similarity=0.305
please set randy janzen up for sap access thanks lynn blair original message from tow eva on behalf of sap security sent friday august pm to cherry paul cc janzen randy blair lynn subject fw randy janzen sap security request form eva randy janzen is requesting access to the below role s and its pending your approval please email your response to sap security if you have any questions please let me know financial accounting roles add fn ar accounts receivable management ets user s current access