Ashley Furr raised this request via **Jira**

Description:

On July 9 at 2:59pm, there was an alert raised by Stellar. This was due to an **Internal User Login Failure Anomaly** and an **Internal Brute-Forced Successful User Login**. These alerts raise concerns as it shows successful login activity following previous login failures from the same source IP.

Internal User Login Failure Anomaly:

- "[redacted] has **43** outgoing login failures related to [redacted] (failure percent rate: 91%) within **5 minutes**"

Internal Brute-Forced Successful User Login:

- "In internal traffic, the source "[redacted]" that was previously observed having a large number of login failures from the account with [redacted]", username "[redacted]" has had a successful login of type [redacted]".

To better understand the incident, we would appreciate your assistance with the following questions:

- Are you aware of any recent changes or configurations that might explain the high number of failed login attempts and subsequent successful login?

- Have there been any unusual activities or suspicious behaviors reported by the affected account "[redacted]"?

Recommendations:

- Conduct a thorough investigation into the internal host with the IP address [redacted] to determine the cause of the login failures and subsequent successful login.

- Monitor the affected account "[redacted]" for any further abnormal activities and consider resetting its credentials if necessary.

- Implement network and system security best practices, such as strong password policies, account lockout mechanisms, and multi-factor authentication.

Alert Info:

Internal Brute-Forced Successful User Login

Internal User Login Failure Anomaly

Source Hosts:

[redacted]

Destination Hosts:

[redacted]