

Project 6

Gerrell Bones

03 NOV 2023

CNT 4403

Project 6

Required Challenges (Required)

Item #1: A screenshot of your Splunk Malware case in Catalyst:

The screenshot displays the Splunk Malware case interface in Catalyst. The main header shows the incident title "Incident #2668: classical macaw" and a search icon. Below the header, there is a section for "Details" with a "CHANGE TEMPLATE" button. The "Severity" is set to "Medium" and the "TLP" is set to "TLP". A red error message "This information is required" is visible below the TLP field. The "Description" field is also empty, with a red error message "This information is required" below it. A "SAVE DETAILS" button is located at the bottom right of the form. The left sidebar shows a navigation menu with options like "Open", "Details", "Severity", and "Log". The right sidebar shows a list of related items, including "Owne", "Playbo", "Phis", "Refer", "argue", "insura", "count", "Artifa", and "Relate".

Item #2: At least one artifact and notes from an external source:

1. **Artificat: 192.168.10.25 and the external source comes from the link :**
<http://www.investorcutting-edge.info/niches/markets>

Item #3: A brief write-up of your findings and Lessons Learned:

The classical Macaw is based on a phishing email from a malicious user. Phishing emails are typically deceptive messages sent by malicious actors with the intent of tricking individuals into revealing sensitive information such as usernames,

passwords, or financial details. If there's a specific phishing campaign named "Macaw," understanding its characteristics, tactics, and techniques would be crucial for devising effective countermeasures or protection strategies. Always exercise caution and employ cybersecurity best practices to avoid falling victim to phishing attacks.