Building Playbooks in Google SecOps Workshop: Exercise Guide

Background: The extraction of the ntds.dit file from an organization can have a devastating impact on the organization's security and operations.
Compromised user accounts:

- Pass-the-hash attacks: The ntds.dit file stores the password hashes for all users in the Active Directory domain. By extracting these hashes, attackers can use tools like Mimikatz to impersonate any user, including privileged accounts like Domain Administrators. This grants them access to sensitive data and resources.
- Offline password cracking: Attackers can attempt to crack the password hashes using tools like Hashcat to obtain the cleartext passwords. Once they have the passwords, they can log in as any user and wreak havoc on the organization's systems.

Loss of data and functionality:

- The ntds.dit file also contains other critical information about the Active Directory domain, such as user accounts, groups, group memberships, and computer objects. With this information, attackers can:
  - Delete or modify user accounts and groups
  - Create new accounts with administrative privileges
  - Disable security measures
  - Disrupt essential services and functionality
  - Access confidential information

Part 1

Goal: Build a playbook for the alert wmic_ntds_dit_t1003_003_cisa_report and test it using the playbook Simulator.

The playbook should contain the following steps. If time permits, additional steps can be added in, but please start with these.

- Trigger: Add a custom trigger based on the aforementioned alert to start the playbook
  - Find the field ***Alert.Name*** in the Insert Placeholder list
- Block: Add the block named ***Playbook Workshop - Prep Block***. This block contains the following actions and has been built in lieu of creating individual actions and can be re-used in other playbooks if desired.
  - Assigns the alert and its case the priority of critical
  - Marks the case as Important
  - Sets an Alert SLA for the alert

    - Adds a description to the case that includes the principal hostname of the impacted system
    - Adds MITRE ATT&CK Technique details by using the detection outcome of MITRE ATT&CK Technique ID with the External ID identifier type
    - Add MITRE ATT&CK Technique mitigations by retrieving json results from the previous step and using the external_attack_id identifier type
    - Changes the case’s stage to investigation
- Action: Assign the case using the Siemplify integration to the user you are logged in as (soar-user-xx)
- Action: Tag the case using the MITRE ATT&CK Technique details json results to apply the external_id as the tag

With the basic information around the alert and case set, let’s add a multiple choice question for the analyst to answer.

- Do you want to check VirusTotal for IOCs from the alert?
    - Yes/No
    - Check the sub-tab for settings on this multiple choice question and assign it to a user who will answer it
- If the analyst responds yes
    - Action: Enrich the Hash using VirusTotal
        - Set the engine threshold to 20
    - Action: Get related IPs from VirusTotal
        - Only get entities that are marked as suspicious
    - Action: Get related URLs from VirusTotal
        - Only get entities that are marked as suspicious
    - Action: Use the Siemplify Utility Query Joiner to build a query that can be used in Chronicle UDM search (in the next step)
        - Values can be constructed using the Insert Placeholder - Playbooks and selecting the action for the VirusTotal Get Related IPs json results and selecting the IPs expression.
        - Query field is ip (this is the name of the grouped field in Chronicle), operator is OR and add double quotes
    - Action: Chronicle Execute UDM Search
        - Query can be constructed using the Insert Placeholder - Playbooks and selecting the Siemplify Utility Query Joiner.query from the previous step.
        - To ensure the query is properly constructed, running the simulator and viewing the json results is a good idea
        - Time frame for the search should be the past week.
- If the analyst responds no
    - Action: Case Comment that analyst declined to research VirusTotal

The next set of actions are the same whether the response was yes or no, so these two paths will merge once this action has been created.

- Action: List assets in Chronicle for internal entities for the past 72 hours
    - When merging two paths back into a single action, dragging an action block from one path onto a ***"Drag a step over here"*** of the other path will link those divergent paths back together on that same action block.
- Action: Add a Flow instruction
    - Assign it to your user (in a multi-user environment, this would be another team, but since we have a single user, we will just use that one today)
    - Add a message for the user to review the information gathered
    - Set a time to respond of 5 minutes
    - Provide instructions around what the potential next steps should be
        - If this is a true positive, escalate to tier3

Once the analyst has performed the instruction, add a multiple choice question for the analyst to answer

- Does this need to be escalated for incident response and remediation?
    - Yes/No
    - Check the sub-tab for settings on this multiple choice question and assign it to a user who will answer it
- If the analyst responds yes
    - Action: Change the stage of the case to incident
    - Action: Siemplify Assign Case to the tier3 group
    - Action: Add a comment to the case that the case has been escalated and include the principal hostname of the system to the comment
- If the analyst responds no
    - Action: Change the stage of the case to assessment

Hints

- Make sure the playbook is turned off, but simulator mode is turned on
- Use the search at the top of the step selection to find specific actions
- The block that has already been built and is used in the playbook has some examples already built into it, including how to add an event field name into a comment using a placeholder as well as an example of taking a json result from one action block and using it in another. Having this block open in another tab can be a handy reference.
- Right clicking on steps and the line and dot that connects each step will provide cut/copy/paste/delete type options.
- Save and test your playbook frequently
- Review the simulator events at the bottom of the screen to validate the playbook is running as expected

Part 2

Goal: Build an alert view to accompany the playbook for the alert wmic_ntds_dit_t1003_003_cisa_report.

In the playbook, click Add View to create a new view. Specify a name for the view and the roles that can observe the view. For this exercise, we will assign all roles and click add.

Use both general and predefined widgets to enhance the view the analyst would see for this alert. Suggested widgets to add to this view include:

- Pending Actions (General)
- Events Table (General)
- Insights (General)
- Entities Highlights (General)
- MITRE ATT&CK (Predefined)
- VirusTotal (Predefined)
- Chronicle (Predefined)

Modify the Events Table widget to include the following field values. Use a descriptive name for the column name. Values need to be enclosed in square brackets:

- Event.event_principal_hostname
- Event.event_principal_user_userid
- Event.event_principal_process_file_sha256
- Event.event_principal_process_commandLine
- Event.event_target_process_commandLine
- Event.event_target_process_file_sha256

For an additional challenge, add a HTML widget to the view

- Name the widget something descriptive
- Assign the preset to be a Number (you will need to click ***Show More*** in the Presets to find that preset)
- Scroll to the bottom of the configuration to find the HTML editor and click the expand button
- Modify the three lines of HTML code after: **/*Update below variable value with placeholder*/**

```
          var field1 = [GoogleChronicle_List Assets_1.JsonResult|
"EntityResult.assets" | count()];
          var field2 = 'Related Assets';
          var field3 = 'Total Related Assets found in Chronicle over
the past 72 hours';
```

- Save the widget

Once you are satisfied with your alert view, turn simulator mode off (click confirm), enable the playbook and save the playbook.

To run our completed playbook against an alert

- Open the alert associated with the playbook
- Click Manual Action on the Alert sub-tab
- Select ***Siemplify - Attach Playbook to Alert*** and specify the specific alert and playbook to run and click Execute

Notice the alert view will change to add the widgets identified in the alert view associated with the playbook. As additional steps are executed within the playbook, additional information will become available.

As user prompts are introduced, click the refresh case button (it will turn yellow when it needs to be refreshed) to see updates to the alerts. Refreshing the pending actions widget as well is a good idea because there are three specific actions that are defined that the analyst needs to respond to. Because we added the Pending Actions widget to our alert, we don’t need to go to the case view or the workdesk to perform these actions.

Once the playbook has completed, review the alert and its associated widgets. Look at the case wall and adjust the playbook if needed. To re-run the playbook against the alert, we can use the manual action to kick this off, we will just continue to build up more actions on our case wall. If we run into an error that we didn’t uncover during our testing, the case wall is a good place to review this information.