Objective:

The objective of this experiment is to evaluate the effectiveness of snapshots of identities in Entra Id in the incident respond chain of containment and recovery.

Scenario:

You are an incident responder for a company that uses Azure for its cloud infrastructure. Your company works with only US customers. Your boss informs you there is a threat actor in the environment, and containment needs to be done quickly. You are given an hour to play, hunt, and contain the threat. Your goal is to identify and contain the threat as soon as possible. Please limit your search to the last 2 hours. Since this is a timed experiment, **please pause to check in with the coordinator after identifying and containing.**

1. **Identify**
   - The threat actor
   - Any persistence
   - Pause and check-in with the coordinator to record time
2. **Containment**
   - Disable the threat actor
   - Disable any persistence
   - Pause and check-in with the coordinator
3. **Experiment Complete**

Setup

Log in to the Azure Portal:

- Use the provided credentials to log in to the Azure portal.
    - Url - portal.azure.com
- Setup your account's credentials

Tools

Please ensure that you have access to the following two products before starting

- Microsoft Sentinel Logs
    - SigninLogs
    - AuditLogs
- Entra Id Portal
    - All Users
    - Disable User accounts

Navigate to Microsoft Sentinel

- On the azure portal, use the search bar at the top and type Sentinel.
- You should be given one Sentinel option. Go ahead and open it
- Navigate to logs on the left panel
    - Entra Id portal

Navigate to Entra Id Portal

- On the azure portal, use the search bar at the top and type Entra.
- Click on users on the left
- Click on a random user
- You can disable their accounts on the top menu bar
- Note will not have access to disable any admin coordinator account

Participant Groups

You will be assigned to a participant group by the coordinator. Ensure you have access to the following data sets

Group 1

- Sentinel Logs
    - SigninLogs
    - AuditLogs

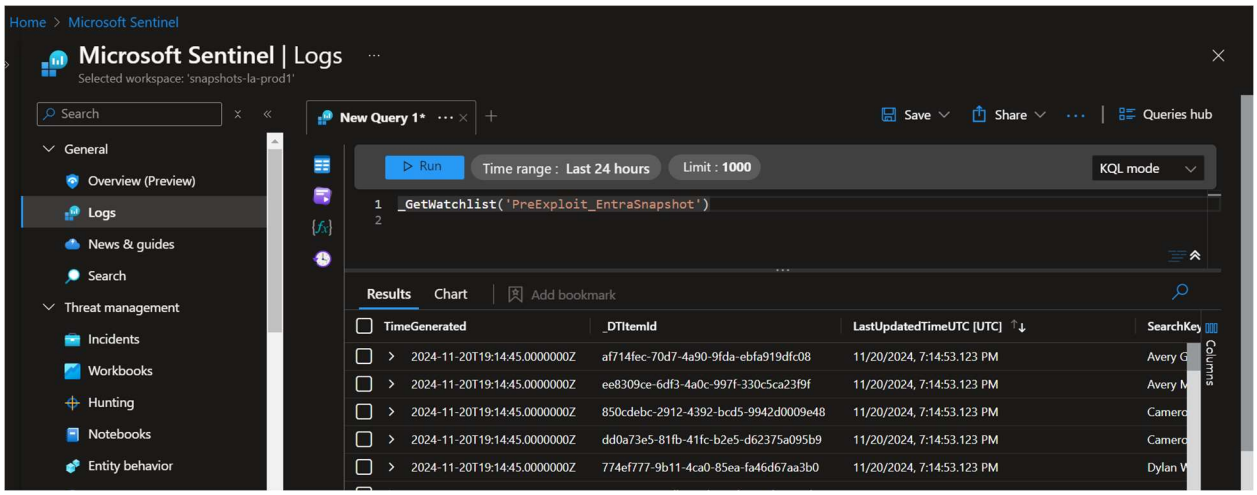
Group 2

- Sentinel Logs
    - SigninLogs
    - AuditLogs
    - _GetWatchlist('PreExploit_EntraSnapshot')
    - _GetWatchlist('PostExploit_EntraSnapshot')

1. **Provide Feedback:**
    - After completing the experiment, provide feedback on the tools and processes used.
    - Suggest any improvements that could be made to enhance the incident response process.

Having trouble?

- Using Sentinel logs, below is an example of one query. Ensure you are in KQL mode so you may type a query



- Sentinel Queries to help with getting started

Look for users named Henry

```
1. SigninLogs
2. | where UserDisplayName has "Henry" //grab user Henry
3. | where TimeGenerated >= ago (2h) // limit search window to the last 2 hours
4. | project-reorder IPAddress,  LocationDetails // move these two columns to the front
```

Look at the list of users before the exploit

```
1. _GetWatchlist('PreExploit_EntraSnapshot')
```

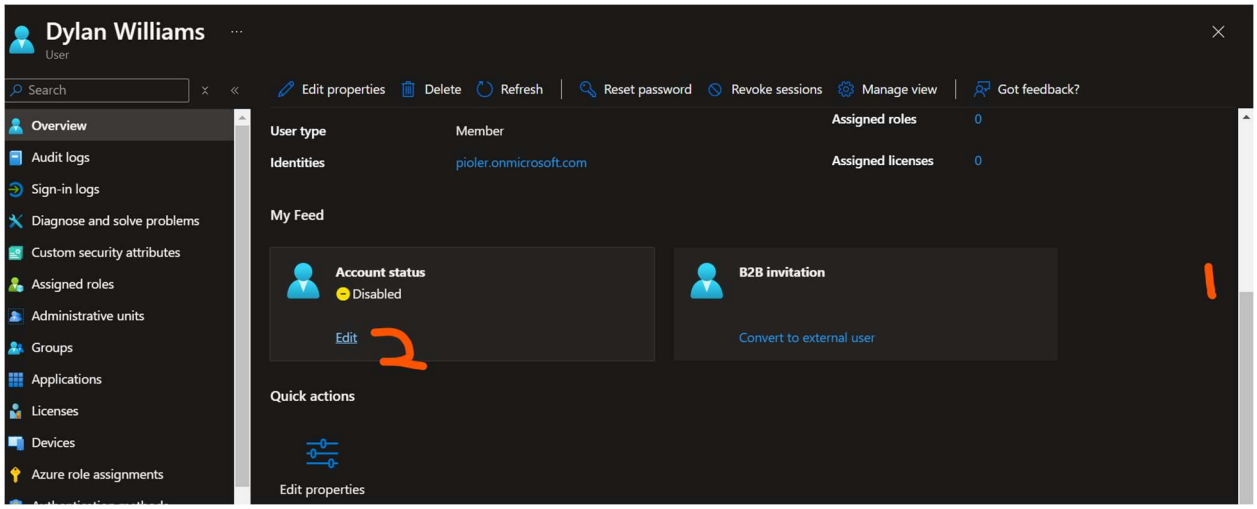
Look for any sign-ins in the last 2 hours for any users named Henry, Apple, or Megaman

```
1. SigninLogs
2. | where TimeGenerated >= ago(2h)
3. | where UserDisplayName has_any ('Henry', 'Apple', 'Megaman')
```

Look for any audit logs related to user Henry in the last 2 hours

```
1. AuditLogs
2. | where TimeGenerated >= ago(2h)
3. | search "Henry"
```

- Disable accounts



Note:

- This is a simulated lab environment. Changes are acceptable. Please limit changes to only disabling accounts.
- If you encounter any issues during the experiment, please contact the experiment coordinator.