Conducting an Azure new user census

Scenario: Active Directory is one of the most important systems for your security posture, and you need to stay on top of events, whether on-premises through regular Active Directory or in the cloud with Azure Active Directory. In particular, you are concerned with attacks such as HAFNIUM, in which new user accounts were created in a domain, giving them the ability to log back into the network using normal authentication rather than use a web shell. You would like a scheduled review of new accounts created in Azure Active Directory each week. You want basic information about each of the new users and their user IDs for further investigation.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Threat hunter
- Technologies:
  - Splunk SOAR
  - Playbook: Azure new user census
- Data: Azure Active Directory

How to use Splunk software for this use case

The playbook starts by listing all users, then filters down to those with the createdDateTime within the last seven days. Next, the playbook queries the Microsoft Graph API to cross-reference the new accounts and make sure that Splunk SOAR has access to investigation and containment actions in Office 365. At the end, the results are saved to artifacts, one for each user, and presented in an analyst note on the investigation page. To use the playbook:

1. Configure the Azure AD Graph app on Splunk SOAR by following the Authentication instructions.
2. Similarly, configure the Microsoft Graph Office 365 app on Splunk SOAR with the Authentication instructions.
3. Configure a new Timer with a new label, such as azure_new_user_census.
   - A once per week schedule might be good to start with.
   - If a different schedule is needed, be sure to change the datetime_modify block in the playbook to look back over the correct number of hours, days, or months.
4. If you haven’t previously used this playbook, configure and activate it:
   1. Navigate to Home>Playbooks and search for azure_new_user_census. If it’s not there, click Update from Source Control and select Community to download new community playbooks.
   2. Click the playbook name to open it.
   3. Resolve the playbook import wizard by selecting the newly created apps.
   4. Set the label to azure_new_user_census or whichever label was created in the timer configuration.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
5. Set the playbook to Active.
6. Save the playbook and then run it.

Results

After this playbook is in use for a few weeks, your security team should have a good understanding of the frequency and common attributes of newly created accounts. After that, if a new account shows up with an irregular field such as a creation time in the middle of the night or an organizational unit that doesn’t make sense, further investigation would be warranted.

Additionally, you can tune and extend this playbook with many variations of logic depending on how you’ve configured your Active Directory deployment and how your organization onboards new users.

- An allowlist could use the presence or value of any Active Directory attribute to filter out new users matching any criteria or automatically disable accounts not matching the necessary criteria.
- This playbook is a good candidate to interface with a ticketing system, messaging platform or email to notify the correct team members or validate information with someone who knows more about the activity.
- If you are using Splunk tools for authentication activity, run a Splunk query from this playbook to check the login history of each account.

Additional resources

These additional Splunk resources might help you understand and implement this use case:

- Blog: Splunk SOAR Playbooks: Conducting an Azure New User Census
- Blog: Detecting HAFNIUM Exchange Server Zero-Day Activity in Splunk
- Tech Talk: Splunk SOAR playbooks: Conducting an Azure new user census