Interactive Guide: Insider Risk Management

Exercise 1 – Day 1 Experience

Objective

In this exercise, you will show how customers can use the scan function to quickly get an understanding of the insider risks an organization is exposed to, show suggested policies, and the ability to customize built-in policies as part of setup/deployment.

The exercise begins in the Microsoft 365 compliance center (https://compliance.microsoft.com), logged in as the administrator of Contoso.

1. Click **Show all** in the left navigation.
2. Select **Insider Risk Management** in the left navigation.
3. On the **Overview** page, click on **Run Scan**.
4. Click on **Run Scan** in the flyout page.
5. Click **Close**.
6. Click on the **View** button under **Risk Scan**.
7. Under **Data Leaks Insight**, click the **View details** button.
8. This page displays a list of the data exfiltration activities that were detected. This page also enables you to quickly begin mitigating these risks by clicking the **Create policy** button. For this exercise, click **Close**.
9. Under **Data Theft Insight**, 5.9% of employees with a resignation date are also showing exfiltration patterns. Click the **View details** button.
10. When you are ready, click **Close**.
11. **Scroll down** to view **Top exfiltration activities**.
12. Under **Employees copying files to USB**, click on the **red bar** to see how many times this activity was detected.
13. Under **Employees emailing external entity**, click on the **red bar** to see how many times this activity was detected.
14. Under **Employees downloading SharePoint files**, click on the **red bar** to see how many times this activity was detected.
15. Under **Top exfiltration activities**, notice the recommendation to monitor the leakage of sensitive data with a General data leaks policy. Click the **View details** button, then click the **Create policy** button.
16. **The General data leaks** template has been automatically selected by the system. Click **Next**.
17. On the **Name your policy** page, click to place focus in the **Name** field and then type **General data leaks policy** and hit **Enter**.
18. Click to place focus in the **Description** field and type **Policy for general data leaks** and hit **Enter**.
19. Click **Next**.
20. On the **Choose users and groups** page, we will keep the default setting **Include all users and groups** and click **Next**.
21. On the **Specify content to prioritize** page, select **I don't want to specify priority content right now**, then click **Next**.
22. On the **Indicators and triggering event for this policy** page, select **Team.Org.Regulatory.US** from the **DLP policy** drop-down list.
23. Under the **Policy indicators** section, **scroll down,** then **scroll down** again and ensure all indicators are selected by default for each category.
24. Click **Next**.
25. Scroll through the **Review settings and finish** page. For this exercise, click the **Cancel** button.

Exercise 2 – Configuring Policies

Objective

In this exercise, you will use the Microsoft 365 compliance center to create an insider risk policy for the data theft by departing employee use case.

1. Starting on the Insider Risk Management Overview page, click the **Policies** tab.
2. To create a policy, click **+ Create Policy.**

3. The **Data theft by departing users** template is selected by default. Review the template's details on the right side of the page, particularly the types of triggering events and indicators specific to this policy. Click **Next**.
4. On the **Name your policy** page, click to place focus in the Name field and then type **Data theft by departing users** and hit **Enter**.
5. Click to place focus in the **Description** field and type **Policy for data theft use case and** hit **Enter**.
6. Click the **Next** button.
7. We can choose one checkbox and have everybody in the organization be in policy or scope it to specific users. In this example, we will keep the default setting to **Include all users and groups** and click **Next**.
8. On the **Specify content to prioritize** page, we can prioritize specific content. A higher priority increases the risk score associated with any activity related to those sites, information types, or labels. Click **Next** to see our options.
9. On the **SharePoint sites to prioritize (optional)** page, click **+ Add or edit SharePoint sites**.
10. On the **Add or edit SharePoint sites** flyout page, select the checkbox for the **group1@contoso.sharepoint.com/sites/group1** SharePoint site, then click **Add**.
11. Click the **Next** button.
12. On the **Sensitive info types to prioritize (optional)** page, click **+ Add or edit sensitive info types**.
13. On the **Add or edit sensitive info types** flyout page, select the checkbox for sensitive info type **type1**, then click **Add**.
14. Click the **Next** button.
15. On the **Sensitivity labels to prioritize (optional)** page, click **+ Add or edit sensitivity labels**.
16. On the **Sensitivity labels to prioritize** flyout page, select the checkbox for sensitivity label **label1**, then click **Add**.
17. Click the **Next** button.
18. Next, we get to choose the triggering events and indicators that define the risk activities we want to detect and investigate. Since we have not yet configured an HR Connector, we will use the second triggering event and click the **User account deleted from Azure AD** checkbox.
19. Under the **Policy indicators** section, **scroll down,** then **scroll down** again and ensure all indicators are selected by default for each category.
20. **Scroll up** back to the **Policy indicators** section.
21. We can use the default thresholds recommended by Microsoft or, if they are too high or low, we can toggle that setting and customize the thresholds to meet the organization's unique requirements. When you are ready, toggle the **Use default thresholds recommended by Microsoft** setting to **OFF.**
22. **Scroll down** to the setting for **Downloading content from SharePoint** and decrease the values to **10**, **25**, and **50**, respectively:
    - Click on **100**, type **10** and hit **Enter**.
    - Click on **250**, type **25** and hit **Enter**.
    - Click on **500**, type **50** and hit **Enter**.
23. Click the **Next** button.
24. Scroll through the **Review settings and finish** page. When you are ready, click **Submit** and then click **Done**.
25. On the **Policies** tab, note that the policy health shown under **Status** for the **Confidentiality obligation during departure** policy displays 3 warnings and 1 recommendation and that the **Policy alert effectiveness** displays 0%.
26. Click the **Confidentiality obligation during departure** policy.
27. Review the warning details and recommendations on the flyout page. One of the items we can immediately address is to add some indicators. Click **Edit policy**.
28. Click **Next**, then click **Next** again.
29. On the **Choose users and groups** page, select **Include all users and groups.** Click **Next**, then click **Next** again**.**
30. On the **Indicators and triggering event for this policy** page, choose **Select all** under **Office indicators**, then click **Next.**
31. On the **Review settings and finish** page, **scroll** down and review the remaining warnings and recommendations that will eventually need to be addressed, then click **Submit**.
32. Click **Done**.

Exercise 3 – Alerts & triage experience

Objective

In this exercise, we will look at the steps involved to triage alerts, investigate to determine the actual event or issue, and drill down to determine validity by creating a case and preparing for remediation.

1. Starting on the Insider Risk Management **Overview** page, click the **Alerts** tab.
2. Click **Filter**.
3. Under **Status**, select **Needs review**.
4. Under **Severity**, select **High**.
5. Click **Apply**.
6. Click on the alert, then click **User activity** on the details page.
7. **Scroll down** through the details of the events and violations that were detected.
8. Cumulative exfiltration anomaly detection or CEAD is a sophisticated machine learning model to analyze user activity over a larger timespan and compare across the organization. This can help identify "low-and-slow drip" exfiltration attempts, for example, where an insider risk actor is slowly stealing or leaking information over a longer period to avoid detection. Click on **Cumulative data exfiltration.**
9. Click on **expanded view** to further analyze the activities.
10. Click on **Open expanded view**.
11. On the **Alert: Confidentiality obligation during departure** page, click the **Activity explorer (preview)** tab.
12. **Activity explorer** provides a microscopic view of the details associated with each activity that was detected. It also lets you slice and dice the data collection to enhance your investigation. For example, select **Printed** from the **Activity** drop-down.
13. Next, click **Filters**, select **File sensitivity label**, then click **Done**.
14. Next, select **Highly Confidential** from the **File Sensitivity Label** drop-down.
15. Select one of the items in the list to open the details pane for that item. Review the information associated with that item, then click **Close**.
16. Click **Confirm all alerts & create case**.
17. Click to place focus in the **Case name** field and type **Case 704: Potential IP Theft**, then hit **Enter**, and click **Create case**.
18. Click **Open the case to investigate and take actions**. We will now open an existing case. Click **Case and** select **Case 449: Potential IP Theft.**
19. On the case overview page, Click the **User activity** tab to see a macro view and sequenced insights of activities over time. Sequencing is the ability to follow file names across a series of actions, which helps reduce the time an analyst takes to triage and raise alerts when these sequences have occurred. In this example, files were downloaded and then emailed.
20. Sequences are a way to provide richer and more sophisticated insider risk detection. We do this by following a trail of activities where the whole is riskier than the sum of the parts. This dramatically improves the fidelity of insider risk detections and reduces investigation time. On the left side of the **User activity** page, select the risk type named "**SEQUENCE: Files exfiltrated and cleaned up**."
21. Click the **Show 4 activities in sequence** link located at the bottom of the activity card.
22. In the chart, you will notice that the activities' sequence is shown via the line connecting the dots. To review details of the specific activity, click on the yellow dot that is the 2nd dot of the sequence)
23. In the detail pane, under **Obfuscation: Files renamed**, click on **2 events: Files renamed.**
24. In the Activity Explorer, we will apply content filters to review what sensitivity labels were applied to the content. Click **Filters** and select **File Sensitivity Label.**
25. Click on File sensitivity label and select **High Confidential.**
26. Click on the **second line item in the list on Jul 14, 2020 at 12:07 PM** and review the details pane.
27. Click on the **X** in the top right to close the details pane.
28. Using Content Explorer, you will examine the emails and files captured by policies. Click on the **Content Explorer** tab**.**
29. First, you will apply a content condition. Click **Condition,** then select **Date**, and click **Add**.
30. Click **Search**.
31. Content can be natively reviewed within Content Explorer using the built-in content viewer. Click **on the first document in the list.**
32. Close the content viewer by clicking on **X**.

Exercise 4 - Remediation

Objective

In this exercise, we will look at available escalation paths, such as inviting others, sending a notice, and escalating to Advanced eDiscovery. We'll also take a quick look at Power Automate, Teams integration, and SIEM integration and see how easy it is to package up relevant details and send to others for review.

The exercise begins on the Case dashboard page.

1. Depending on the nature of the activities, you may determine that there is little risk of malicious intent and that the violations may have been done out of negligence. In this instance, you may notify the user of the violation and point them to standards of business conduct training. Click on **Case 449: Potential IP Theft.**
2. To send the email, click **Send email notice.**
3. From the **Choose a notice template** drop-down list, select **Confidentiality obligation reminder.**
4. Click **Cancel**.
5. The insider risk solution provides different methods for collaborating with others across your organization. One option is to add users as contributors. In the case, click the **Contributors** tab, then click **+ Add contributor.**
6. Click to place focus in the **User** field and then type **Sarah Peterson** and hit Enter.
7. Click on **Sarah Peterson** from the list.
8. Click **Add**.
9. Click the **Case notes** tab, then click **+ Add case note.**
10. Click to place focus in the **Add case note** field and then type **Please review this case**, and hit Enter.
11. Click **Save**.
12. Sometimes a case will need to be investigated by your legal department. Click **Escalate for investigation** to create an Advanced eDiscovery case.
13. On the **Escalate for investigation** window, click to place focus in the **Name** field and then type **Discovery Case 449** and hit Enter.
14. Click **Create case**, then **Done**.
15. When Microsoft Teams is enabled in the Insider Risk Management settings, a Team is automatically created and associated with the case, enabling all analysts, investigators, and contributors to collaborate over a secure channel. You can click on view team to open it. For this guide, go back to the case **overview page** for **Case 449: Potential IP Theft.**
16. Insider Risk Management is integrated with **Power Automate flows,** enabling you to streamline specific actions to help make processes more efficient. When you create a flow, it will appear in the **Automate** drop-down to initiate the workflow. Click **Automate** and observe that two flows have already been created: **Request info from HR or business about a user in an insider risk case** and **Add a calendar reminder to follow-up on an insider risk case**.
17. Click **Manage Power Automate flows**.
18. Review the various available workflow templates. When you are ready, click **X** to close the **Flows** flyout page.

Summary

To learn more and get started go to https://aks.ms/insiderriskdocs and https://aka.ms/insiderriskblog.