Microsoft

Insider Risk Management

Lab Guide

Updated: November 15th June 2020

Table of Contents

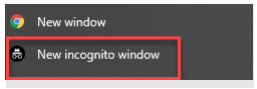
Before you begin

Pre-requisites

Before you start you should have completed the "Getting started with Microsoft 365 Compliance Master Class Labs". If you have not completed this you will not be able to do this lab. You can find this document which you can download from https://aka.ms/m365masterclass-labs Each tenant will take 24 hours to provision so its important that you complete this prior to Tuesday when the event starts.

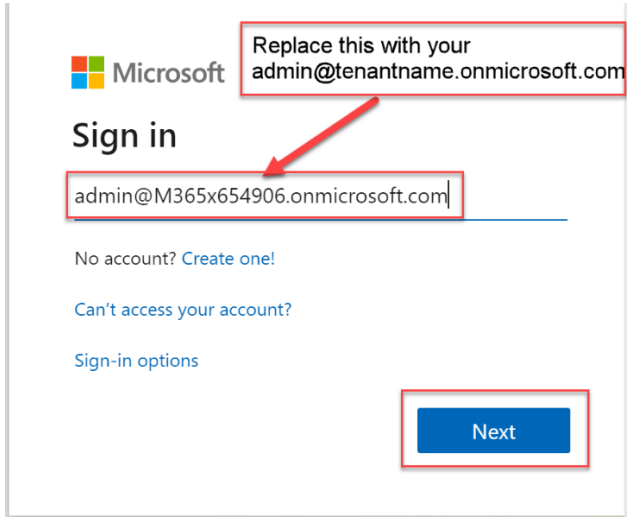
User accounts

Open an In-private browser (Edge) 

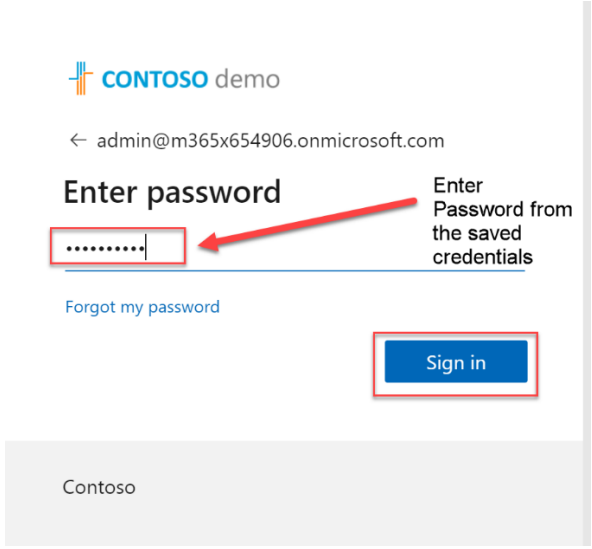
or New in-Cognito (Chrome) 

on your machine and then go to https://df.protection.office.com/insiderriskmgmt?viewid=overview&flight=enablem365compliancecenter,enableinsiderriskmgmt,enableinsiderriskservice,EnableFakeData

a) Enter the admin account username that you saved in "Getting started with Microsoft 365 Compliance Master Class Labs" to gain credentials.
b) Enter your admin credentials in the sign in as below and click NEXT



c) Enter the password and then click "Sign in"



Insider Risk Management Demo

The world of the modern workplace offers innovative technology that employees love, empowering them to communicate, collaborate, and produce with agility. In this world, trusting your employees is the key to creating a dynamic, inclusive workplace and increasing productivity.

But, with trust also comes risk. Risk that an employee may negligently breach that trust by inadvertently leaking confidential information in corporate communications channels. Or risk that an employee maliciously breaches that trust by stealing intellectual property.

In fact, a survey by Crowd Research Partners indicates that 90% of organizations feel vulnerable to insider attacks, and 53% confirmed insider attacks against their organization in the previous 12 months.

We know from our own experience that it's hard to maintain trust without the right visibility, processes and control. However, the effort required to identify these risks and violations is not trivial. Think about the number of people accessing resources and communicating with each other, as well as the natural cycle of people entering and leaving the company. How do you quickly determine risk that is intentional vs. unintentional at scale? And how do you achieve this level of visibility, while aligning to the cultural, legal and privacy requirements in your environment? For example, truly malicious insiders do things, such as intentionally stealing your intellectual property, turning off security controls or harassing others at work. But there are many more situations in which an insider might not even know they are causing a risk to the organization or violating your policies, like when they're excited about something new they're working on and send files or photos to tell others about it.

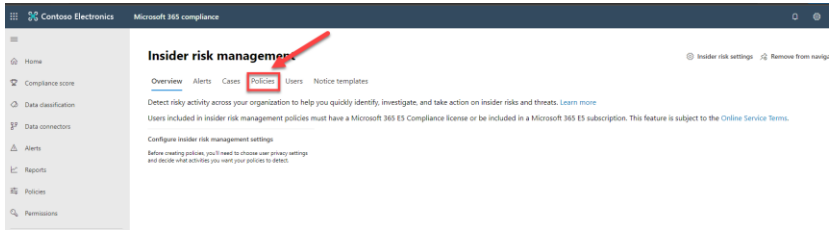
Ultimately, it's important to see the activities and communications that occurred in the context of intent, in order to take the correct course of action. The only way to do this efficiently and at scale is by leveraging intelligence and machine learning, as human driven processes can't keep up and aren't always that accurate. Furthermore, a holistic solution to this problem requires effective collaboration across Security, HR and Legal and Compliance, as well as a balanced approach across privacy and risk management.

Lab steps

Insider Risk Management

NOTE – It take a while for a tenant to have enough data to generate alerts to use in an Insider risk Demo. Therefore this lab will just show you how to create a Policy and an overview.

Creating an insider risk policy

What to say	What to show
Introduction A new solution, Insider Risk Management, uniquely positions Microsoft 365 to help organizations quickly identify and remediate insider risks. This solution was incubated in Microsoft's internal digital security and risk engineering (DSRE) organization and then brought to scale by the Microsoft 365 engineering team. The ability to quickly identify risks from insiders (employees or contractors with corporate access) and act in collaboration with HR and Legal to minimize the negative impact on corporate policy compliance, competitive business position and brand reputation, is a priority for organizations worldwide.	1. Navigate to https://df.protection.office.com/insiderriskmgmt?viewid=overview&flight=enablem365compliancecenter,enableinsiderriskmgmt,enableinsiderriskservice,EnableFakeData browser tab, and login using your demo tenant credentials. See User accounts
Creating a policy Now for the implementers, let us review how to create a policy, used to start reviewing this content and triggering alerts. You begin creating a policy by clicking **Add policy**. First, give the policy a name and description and select a playbook. As the playbook name implies, these contain a preconfigured set of detections focused on a given insider risk	2. On the top page navigation, Click **Policies** tab. 

type. After entering a name, I'll select **Departing employee data theft**.

On the **Users** page I can scope the policy to groups or specific users in my tenant or all users. Given the importance of privacy, Microsoft has developed this experience as an explicit opt-in experience meaning you have to add the users for a given policy.

Here I assign content priority, because not all content is created equal.

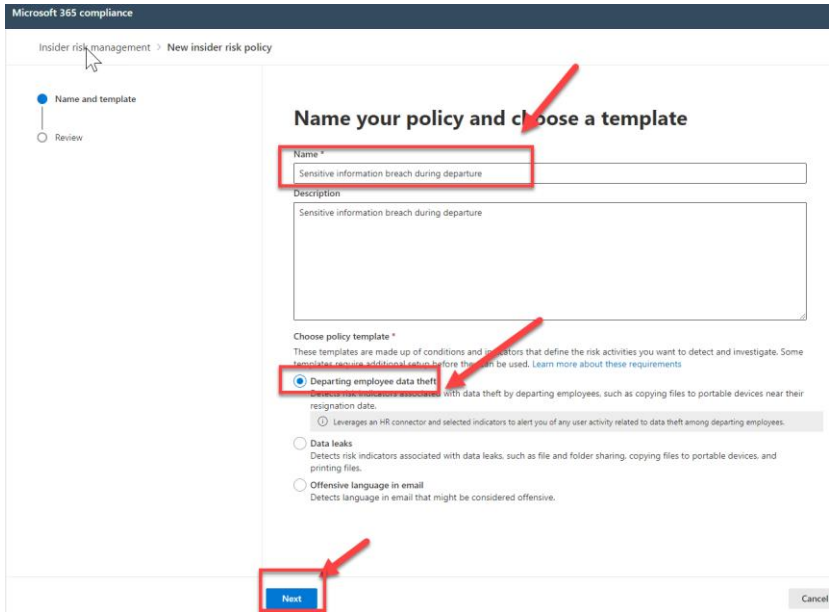
As an example, creating a policy for a sales team and knowing that the most important sales documents are stored in a specific SharePoint site, I can define that SharePoint Online site as a content priority for the given policy.

I can also select sensitive information types such as credit card number, banking information or sensitive labels. Those are ways I can use to prioritize the important content for this policy.

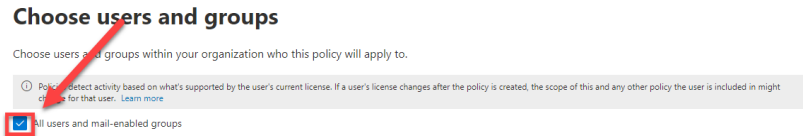
Next, I select relevant alert indicators. For example, to capture events from your HR system using the HR connector, I select **HR events**. I can select other signal types as well. The more indicators selected, the richer the policy matches will be.

The Anomalous activity indicator enables the system to verify if an individual's activity is considered anomalous against their historical activity pattern using machine learning.

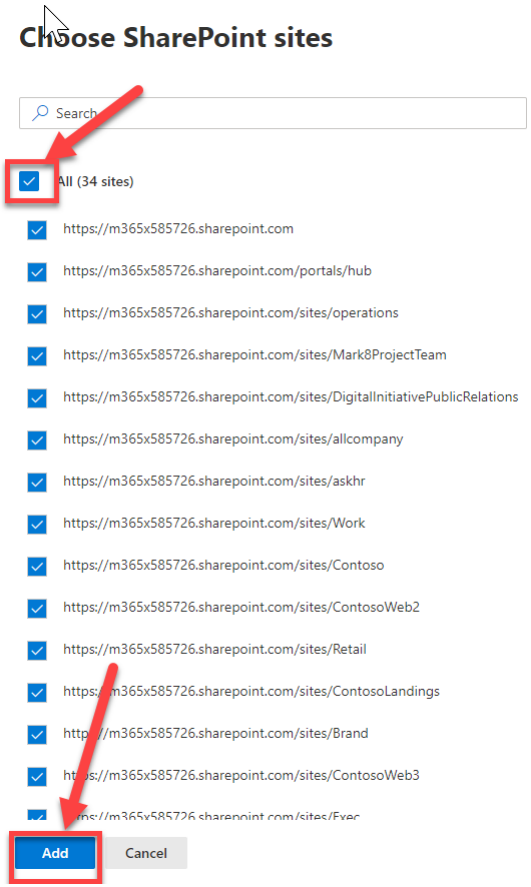
3. Click Add policy.
4. In the Create insider risk policy wizard, under Name type Sensitive information breach during departure, and then under Select policy template, click Departing employee data theft.

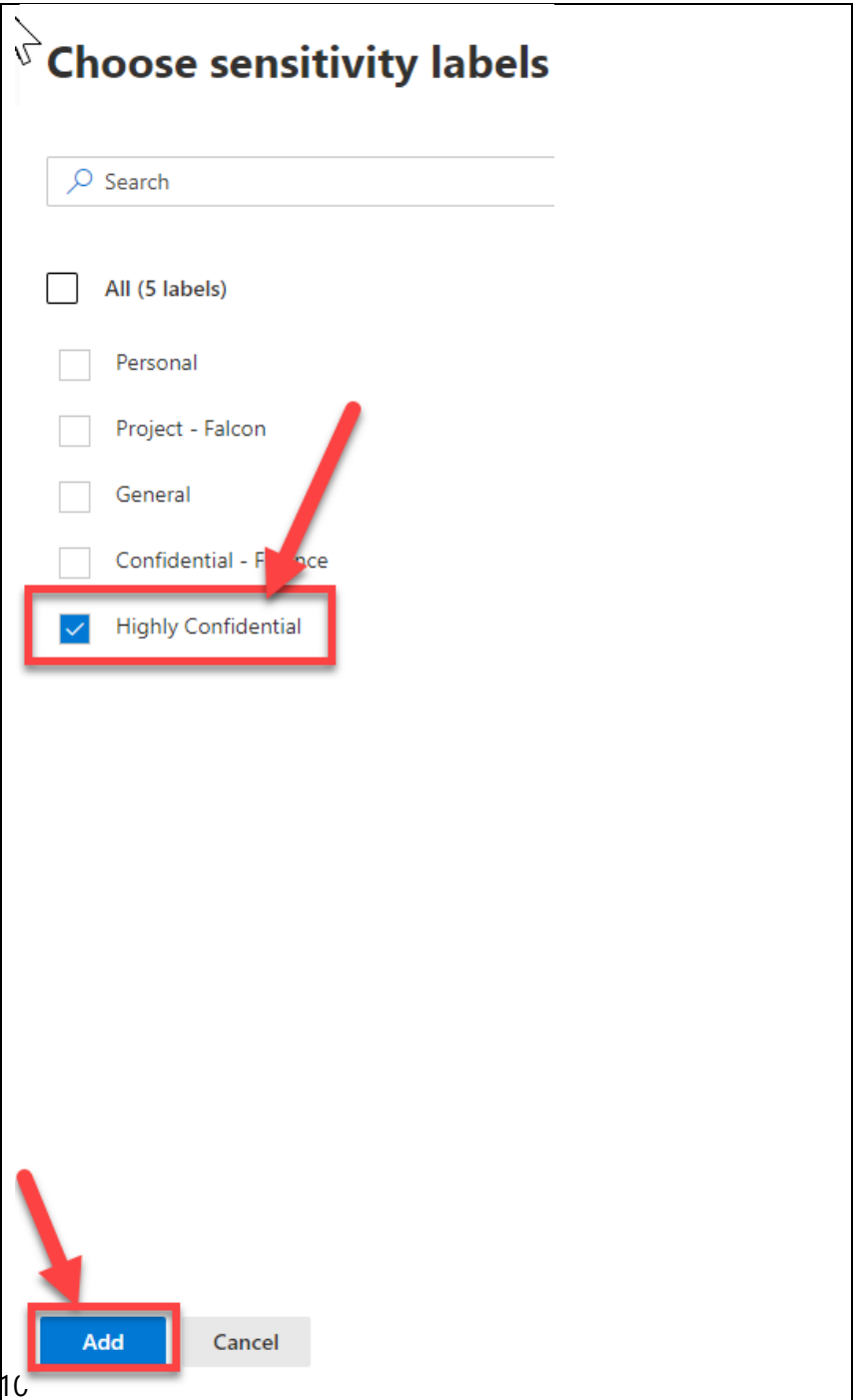


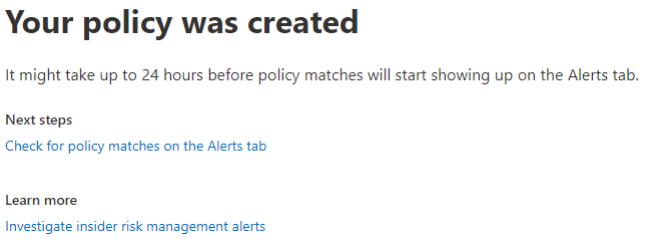
5. Click **Next**.
6. On the Users page, click All users and mail-enabled groups and then click Next.



7. On the Specify what content to prioritize (optional) page, Add Choose SharePoint site.

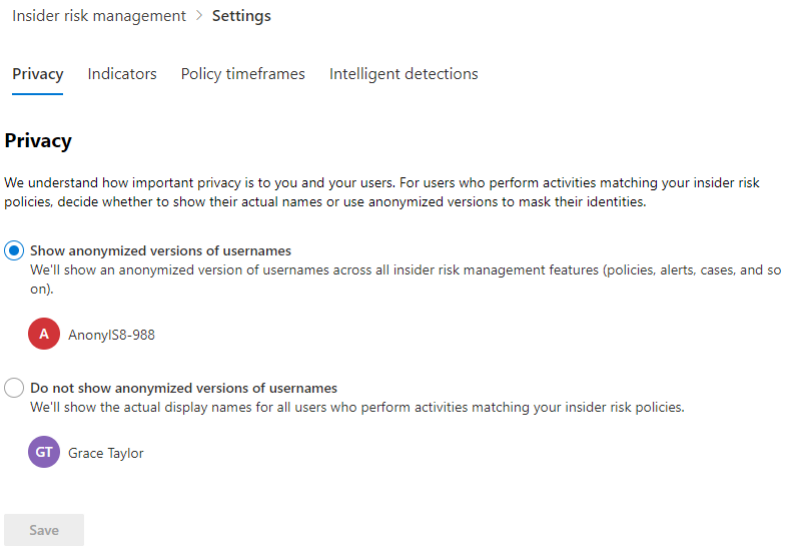
Next, I select a monitoring window. I can configure various parameters to indicate how long I want a potential user to be in scope for policy evaluation. I will leave the default parameters and click **Next**. Clicking **Submit**, this policy, scope and alert indicators will start generating alerts to review as suspicious activities are found. This could take a few days or more depending on your environment and user activity.	8. On the **Search** pane, review the **SharePoint sites** and then Select All and Add  9. On the Specify what content to prioritize (optional) page, click Choose sensitivity Labels 10. On the **Search** pane, review the sensitive information types choose **Highly confidential and click Add**


Choose sensitivity labels
Search
All (5 labels)
Personal
Project - Falcon
General
Highly Confidential
Add
Cancel

	11. click Next. 12. On the **Alert indicators** page, review the alert signals available and then click **Next**. 13. On the **Policy timeframes** page, review the configurable timeframes, and then click **Next**. 14. On the **Review** page, review the policy options, and then click **Submit**  15. Return to the portal in 24hours to see what it has found.

What to say	What to show
IN THIS SECTION WILL ALL DATA AND ALERTS WILL BE BLANK IN A DEMO TENANT	
Dashboard The Insider risk management dashboard displays an overview of **Alerts needing review**, **Active cases**, **Users**, and **Policies with most activity**.	16. This will be BLANK in your demo tenant but you can see the interface. 17. On the **Overview** tab for **Insider risk management**, review the Insider risk management dashboard. Once you have data you could see : • Alerts needing review • Active cases

What to say	What to show
There are tabs for **Alerts**, **Cases**, **Policies**, **Users**, and **Notices**. The display names for users can be pseudo-anonymized to prevent conflicts of interest, maintain privacy and enable bias-control ensuring you are not purposefully overlooking a relative, friend or your boss on the list. While user information is anonymized in the UI, the original user information is stored in the backend to enable further investigation if an issue is found. Clicking **Alerts** displays a list of alerts based on different risk types. On the Alerts tab, you can view basic statistics and how alerts are trending over time. Clicking an alert displays additional information, such as any associated case, the user activity leading to the alert and the anonymized user information. You can view a detailed timeline of events on the **User Activity** tab. A curated list of the history of recent user activity is displayed in a timeline view. Clicking **Cases** displays a list of cases, statistics and status of cases that have been created.	• Users • Policies with most activity • Pseudonymize toggle 18.On the dashboard, click **Alerts** tab. 19.Review **Alerts** and point out: • Alerts needing review • Open alerts over time • Statistics • Policy match alert 20.Click User activity. 21.In the upper right corner, click **X** to close the pane. 22.Click **Cases** tab and point out: • Active cases • Cases over time • Statistics • Case name 23.Click **Policies** tab and review the existing policies. 24.Click **Alerts** tab.

What to say	What to show
The **Policy** tab displays the list of policies that exist and are being enforced to check for violations.	
If the **Pseudonymize** option was off, information from Azure AD would be displayed including the user's full name, email address, title, department, and manager name under the "User profile" tab. This toggle is only off for those users with the highest level of permissions for Insider rights management, which in most organization is limited to members of their legal or compliance group.	To view these **Pseudonymize** options - On the main dashboard click Insider Risk settings  See the privacy Tab below to show the options 

Conclusion

What to say	What to show
Insider Risk Management leverages the Microsoft Graph to obtain real-time native signals across Office, Windows, and Azure, including file activity and abnormal user behaviors.	No click steps.

Additional 3rd party signals from HR systems and desktop agents can be included via an API level integration. A robust set of configurable playbooks tailored specifically for digital IP theft, confidentiality breach and offensive communication use machine learning and intelligence to correlate the signals to identify hidden patterns and risks that traditional or manual methods might miss. A comprehensive 360° view provides a curated and easy-to-understand visual summary of individual risks within your organization. This view includes an historical timeline of all activities and trends associated with each identified threat. Finally, end-to-end integrated workflows, including 'Notice/education' and 'escalate for further investigation,' ensure that the right people across Security, HR, Legal and Compliance are involved to quickly investigate and take action once a risk has been identified.	