Part 6b – Insider Risk Management Settings

(Insider Risk Management)

Contents

Before we start, please not that if you want to see a table of contents for all the sections of this blog and their various Purview topics, you can locate the in the following link:

Microsoft Purview- Paint By Numbers Series (Part 0) - Overview - Microsoft Tech Community

Disclaimer

This document is not meant to replace any official documentation, including those found at docs.microsoft.com. Those documents are continually updated and maintained by Microsoft Corporation. If there is a discrepancy between this document and what you find in the Compliance User Interface (UI) or inside of a reference in docs.microsoft.com, you should always defer to that official documentation and contact your Microsoft Account team as needed. Links to the docs.microsoft.com data will be referenced both in the document steps as well as in the appendix.

All of the following steps should be done with test data, and where possible, testing should be performed in a test environment. Testing should never be performed against production data.

Target Audience

The Insider Risk Management section of this blog series is geared toward Security and Compliance officers who need to monitor users behavior when it comes to compliance data.

Document Scope

This document is meant to guide an administrator who is "net new" to Microsoft E5 Compliance through the use of Insider Risk Management (IRM).

It is presumed that you already data to search inside your tenant.

We will only step through a basic eDiscovery case (see the Case section).

This part of the blog will cover the Settings for IRM, the Indicators it tracks, the Overview tab and Analytics available withing the Overview tab.

Out-of-Scope

This document does not cover any other aspect of Microsoft E5 Compliance, including:

- Sensitive Information Types
- Exact Data Matching
- Data Protection Loss (DLP) for Exchange, OneDrive, Devices
- Microsoft Cloud App Security (MCAS)
- Records Management (retention and disposal)
- Overview of Advanced eDiscovery (AeD)
- Reports and Analytics available in of Advanced eDiscovery (AeD)

It is presumed that you have a pre-existing of understanding of what Microsoft E5 Compliance does and how to navigate the User Interface (UI).

It is also presumed you are using an existing Information Types (SIT) or a SIT you have created for your testing.

As it relates to Insider Risk Management we will not be covering:

- Permissions
- Alerts
- Cases (investigations)
- Users
- Notifications
- Creation of Advanced eDiscovery Cases from IRM

If you wish to set up and test any of the other aspects of Microsoft E5 Compliance, please refer to Part 1 of this blog series (listed in the link below) for the latest entries to this blog. That webpage will be updated with any new walk throughs or Compliance relevant information, as time allows.

Microsoft Compliance - Paint By Numbers Series (Part 1) - Sensitive Information Types - Microsoft Tech Community

Use Case

There are many use cases related to accessing and sharing of sensitive data. One example is – A user is accessing and sharing sensitive data on a regular bass and management needs to know if there are any spikes in access or sharing of that information that might coordinate with negative HR reports, resignations, etc.

Overview of Document

This part of the blog will cover the Settings for IRM, the Indicators it tracks, the Overview tab and Analytics available withing the Overview tab.

Here are the parts of the settings that we will cover:

- Anonymization
- Policy Indicators
- Priority User Groups
- Analytics
- Overview/Analytics – Activities detected and ready to review
- Overview/Analytics – User Activity Reports

Definitions

- Data Theft – This means data taken/stolen by departing users near their resignation or termination date.
- Data Leakage – Data leaks can range from accidental oversharing of information outside your organization to data theft with malicious intent.
- Indicators – Indicators included in insider risk management policies used to determine a risk score for an in-scope user. These policy indicators are only activated after a triggering event occurs for a user.
- Thresholds – Each indicator uses default thresholds that influences an activity's risk score, which in turn determines whether an alert's severity is low, medium, or high. The threshold is based on the number of events recorded for an activity per day.
- Triggers – Triggering events determine when a policy will begin to assign risk scores to a user's activity.
- Anonymization – Masking a user's name and account information to prevent bias from investigators
- Telemetry – data from the M365 Audit log (ex. deletions, changes, label modifications, uploads, etc),
- Risk Score – Insider Risk Management leverages a score system to track how low or high a risk an activity is 100/100 is the highest risk possible. 0/100 is the lowest risk possible.

Notes

None

Pre-requisites

If you have performed parts 1-3 of this blog series, then you have everything you need to run this . If you have not done those parts of the blog, you will need to populate your test environment with test data for the steps to follow.

You must have enabled at least 1 Insider Risk Management license.

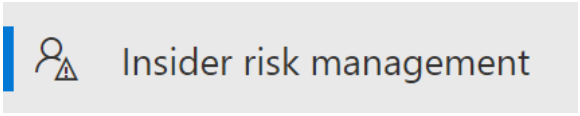
It is recommended you have completed Part 3a DLP for Endpoint, or at the least, that you have on-boarded a minimum of one Windows 10/11 device to test the collection of Endpoint DLP policies into Insider Risk management (IRM).

You have loaded an Insider Risk Management (IRM) licensing for at least 1 week in order to collect as much telemetry as possible. That you have run Sensitivity and DLP testing during that 1 week, again, to add telemetry information to your IRM console.

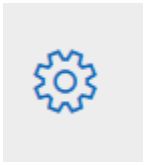
You should have done steps 6-6a in this series.

Part 1 - Settings

1. Go to the **Insider Risk Management** section in the left-hand side of the Compliance portal.

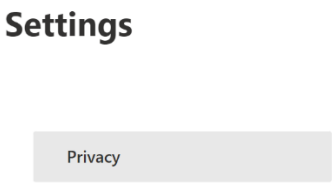


2. Click on the Settings icon in the top right corner

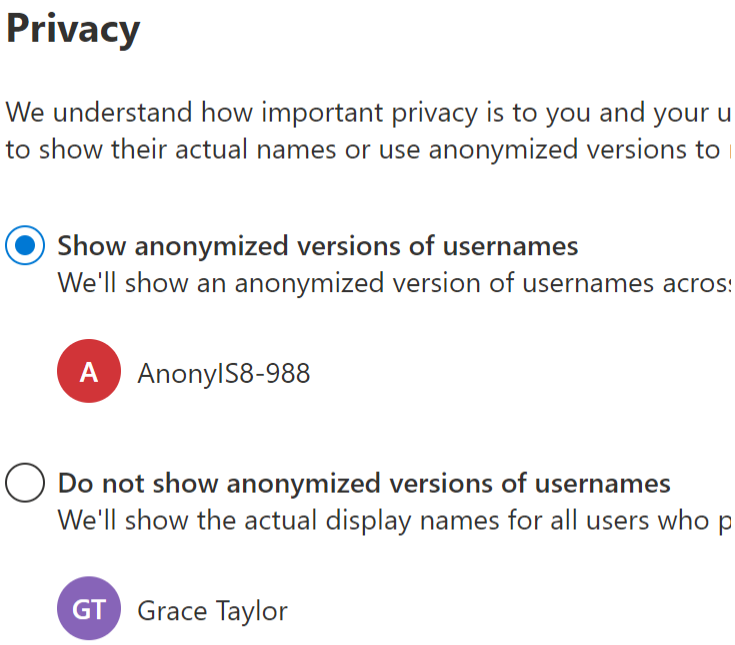


Part 1a - anonymization

1. Click the **Privacy** option



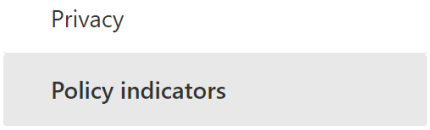
2. On the right, see the option to turn and off Anonymization of users in Insider Risk Management



Part 1b – Policy Indicators

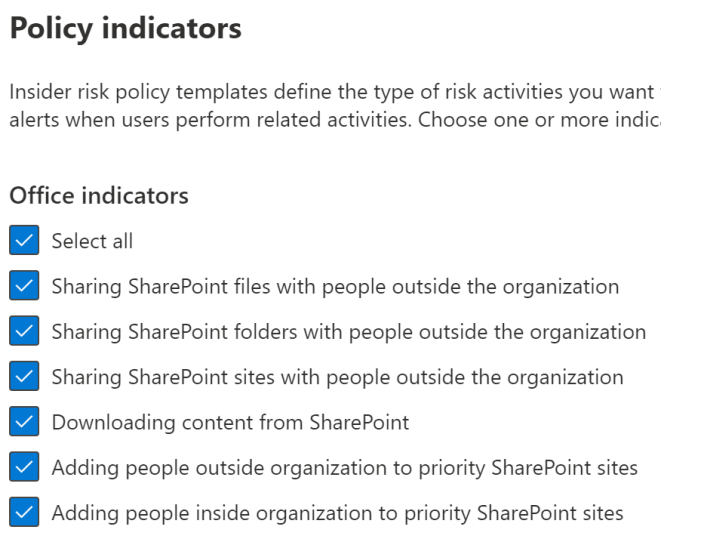
Policy indicators take a subset of the telemetry from the Audit log. It takes the telemetry related to data (ex. deletions, changes, label modifications, uploads, etc), and feeds that into a single console.

1. Stay in settings and click on **Policy Indicators.**

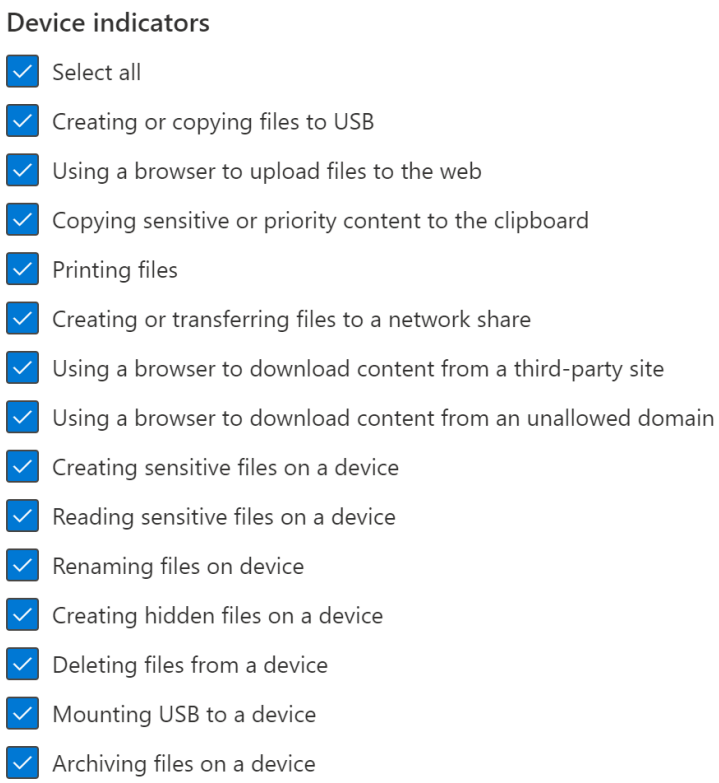


2. On the right-hand side you will see all the different indicators available. In settings you can turn this on/off, but in an individual IRM policy, you determine the level what is acceptable versus not acceptable. This will be explained more further down when we review an individual policy.

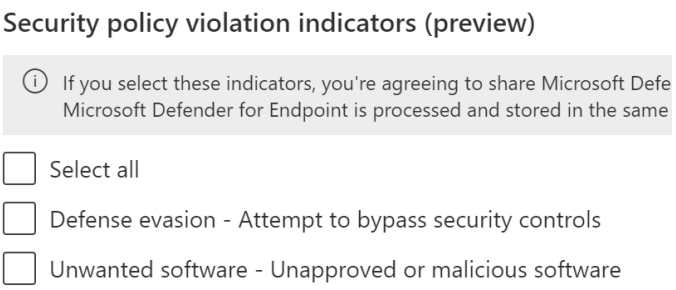
3. Office Indicators – These indicators are focused on telemetry related to access and user interactions with data located int SharePoint, Teams, and emails.



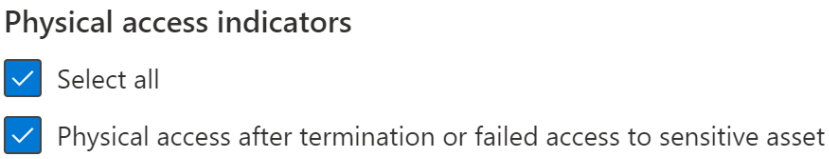
4. Device Indicators – These indicators are focused on telemetry related to data flowing to, thru, and from Endpoint devices.



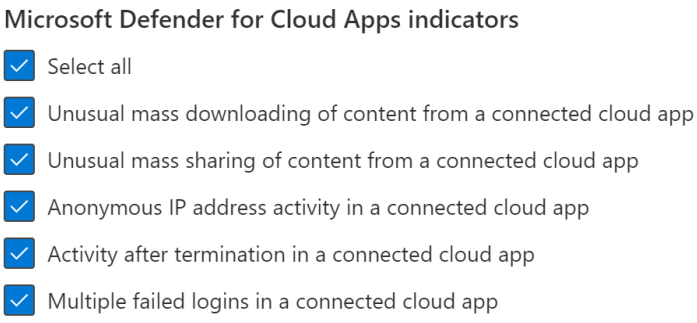
5. Security policy violation indicators – These indicators are focused on telemetry related to security violations related to the security side of Microsoft Defender for Endpoint (MDE). These indicators are currently in preview as of the writing of this blog entry. We will NOT be covering this as part of this blog series.



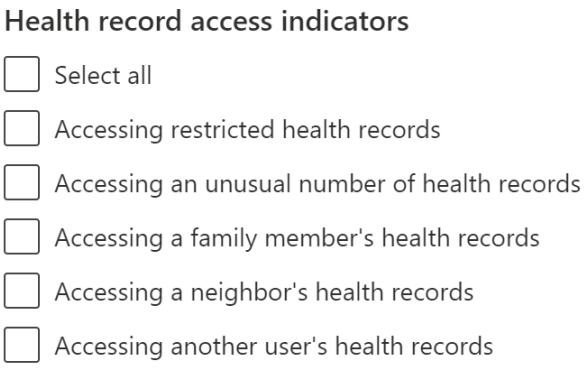
6. Physical access indicators – These indicators are focused on telemetry related primarily to badging systems. We will NOT be covering this as part of this blog series.



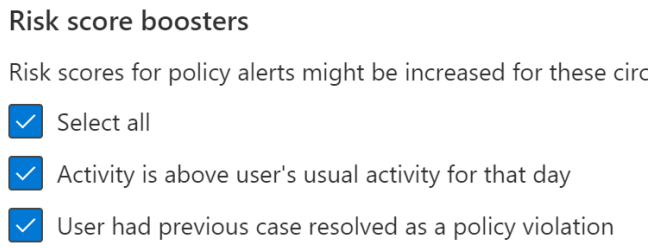
7. Microsoft Defender for Cloud Apps Indicators – These indicators are focused on telemetry related to our CASB tool which covers conditional access, Data Loss Prevention to third part cloud apps. We will NOT be covering this as part of this blog series.



8. Health record access indicators – These indicators are focused on telemetry related to Electronic Message Record (EMR) systems. We will NOT be covering this as part of this blog series.



9. Risk Score boosters – These allows you to modify the Risk Score of activities in each of the policies you create. We will NOT be covering this as part of this blog series.



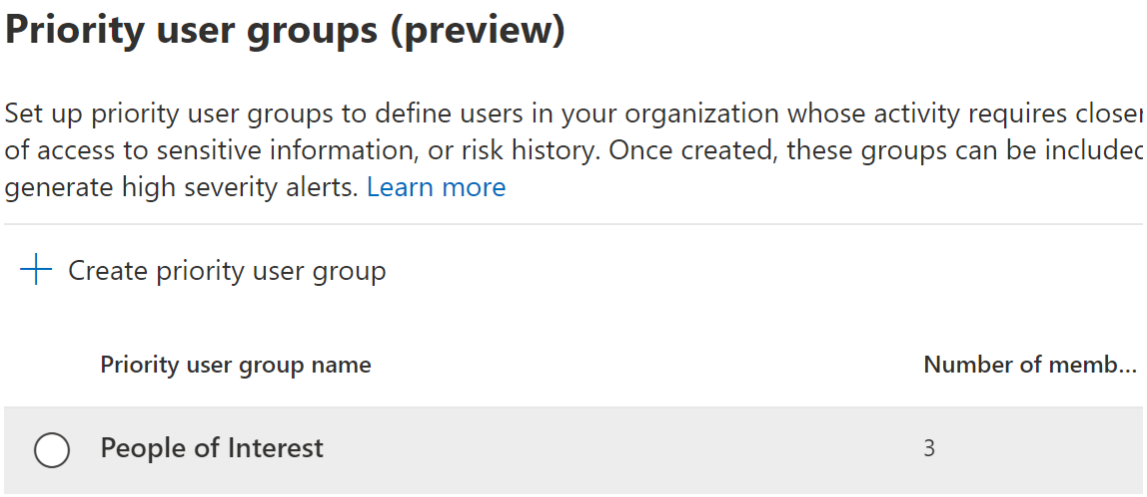
10. Leave all indicators at their default selections.

11. You can now move to the next section of the Settings.

Part 1c – Priority User Groups

1. Another item that might be of interest, is the ability to set the priority of groups and individuals and groups for tracking within the IRM tool. You find this under Priority User Groups.

2. You can then Create a group and add individuals to that group.

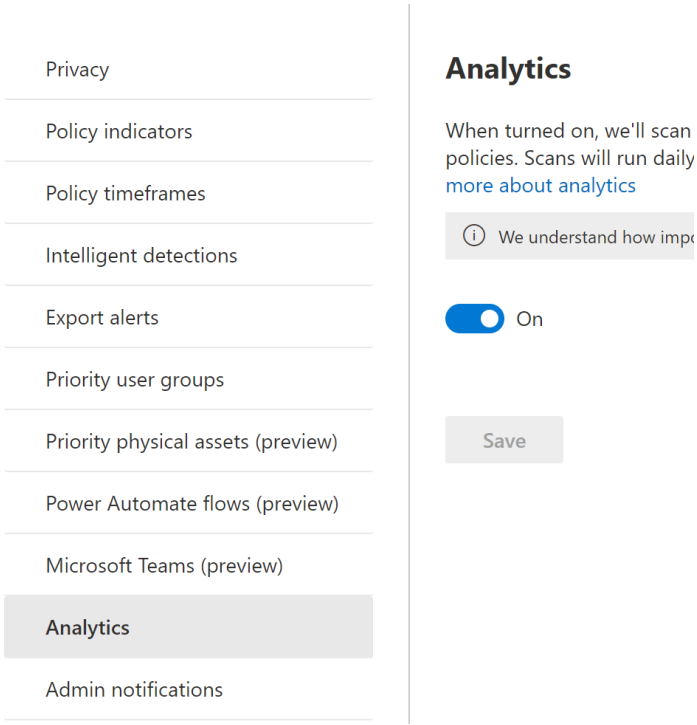


3. We will not be creating a priority group at this time. Return to the **Overview** tab.

Part 1d – Analytics

Analytics is an optional configuration. To turn on Analytics, you need at least one Insider Risk Management license.

1. Next, go to the Analytics tab on the left of the **Settings** tab and on the right side, click **On**.



2. Now wait at least a week (7 days) to let the analytics engine collect data. If you are not running your Insider Risk Management test in production (which is not recommended) OR in a QA tenant with active DLP testing, you will need to go to part 3 of this blog series (Data Loss Prevention) to generate material for your testing in later parts of the Insider Risk Management section of the blog

Part 2 –Analytics Reports

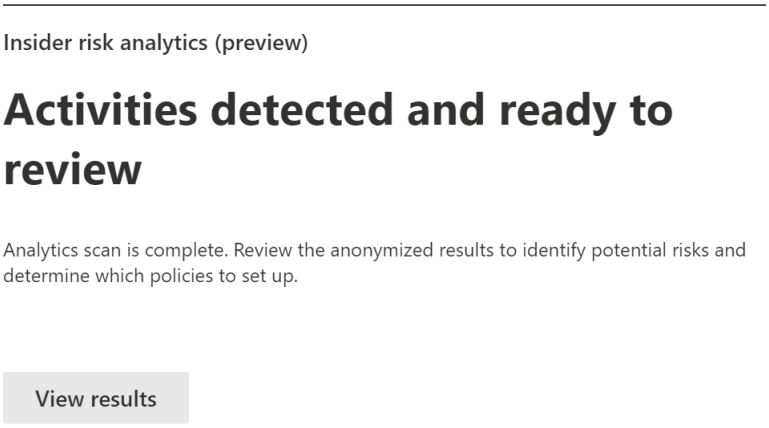
On the **Overview** tab, go to the bottom to see the **Insider risk analytics** from the last week. Here you will find the two analytics:

- Analytics detected and ready to review
- User Activity Reports

Let's look at what these two reports provide.

Part 2a – Activities detected and ready to review (preview)

1. On the **Overview** tab, go to the bottom to see the **Insider risk analytics** section. Click on **Activities detected and ready to review** from the last week (or more). Click **View results**.



1. **Activities detected and ready to review** is general as to what it's seeing in your tenant. This is different than **Investigate user activity** allows you to run reports on specific users or groups.

2. On the details page, you will see sections of information such as "Potential data leak activities" and "Top exfiltration activities".

3. You will also see Insider Risk Management's "Recommendations" under each section

4. To get more details for each of the above, click on **View Details** that corresponds with that section.

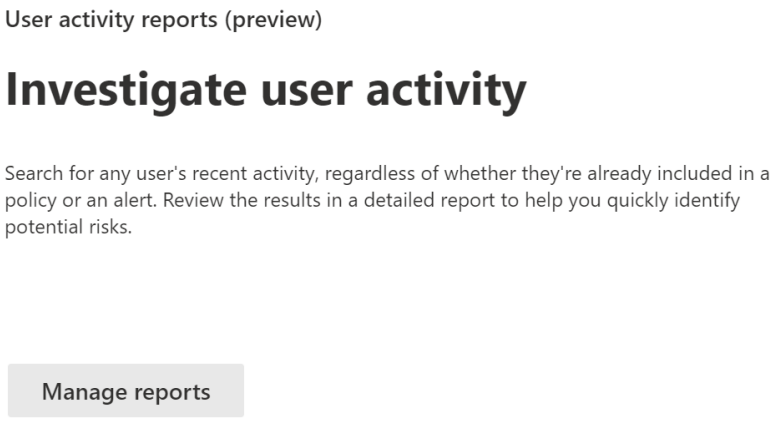
5. If you click on the View Details, you will see a popup to the right. This will let you see the details, again give you recommendations and even give you the option to jump in and click **Create Policy** based on what you are seeing. Do not click **Create Policy** at this time, as we will create a Policy in the next section of this blog.

6. Do not click **Create Policy** at this time, as we will create a Policy in the next section of this blog.

7. Click **Close** and return to the root of the Insider Risk Management tools.

Part 2b – User Activity Reports

1. On the **Overview** tab, go to the bottom to see the **Insider risk analytics** section. Click on **Investigate user activity** from the last week (or more). Click **Manage Reports**.

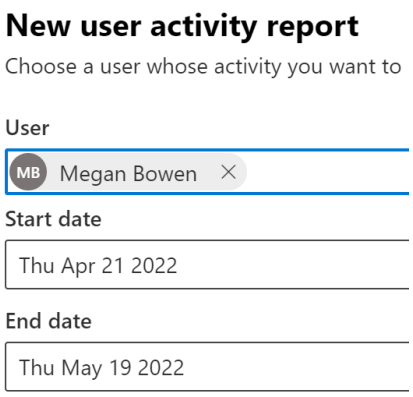


2. **Investigate user activity** allows you to run reports on specific users or groups, which is different than the **Activities detected and ready to review**. That report is more general as to what it's seeing in your tenant.

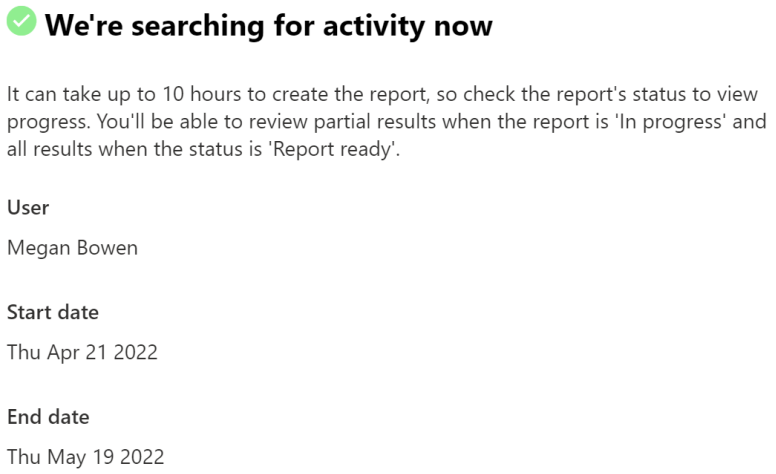
3. Click on **Create user activity report**.

4. On the left, a pop-up will appear. You can enter the user you want a report on and the dates you want to search. Please note that you can only run a report for the previous 30 days.

5. I will select my users Megan Bowen and click **Create Report**.

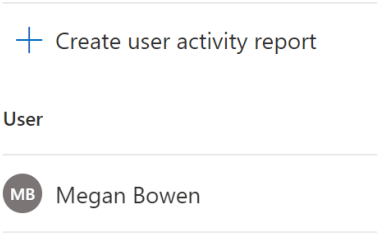


6. Note that it will take several hours (up to 10) for the report to be generated.

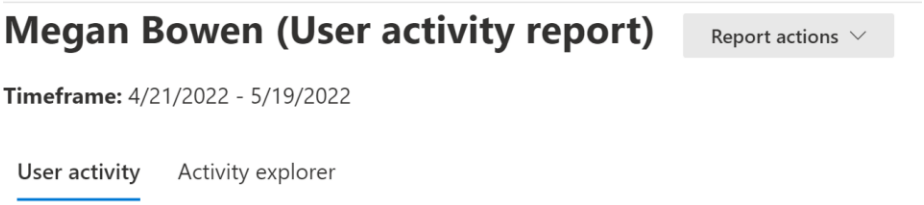


7. Click **Close** and return to this webpage in the next day or two.

8. When you return, you should see a report similar to the one below.



9. Double click on it to see your report

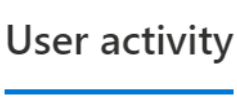


10. The Report will show you the **User Activity** and **Activity Explorer** for the time period selected
    a. Note – My tenant is new and therefore has very little date being driving through it or my test user of Megan

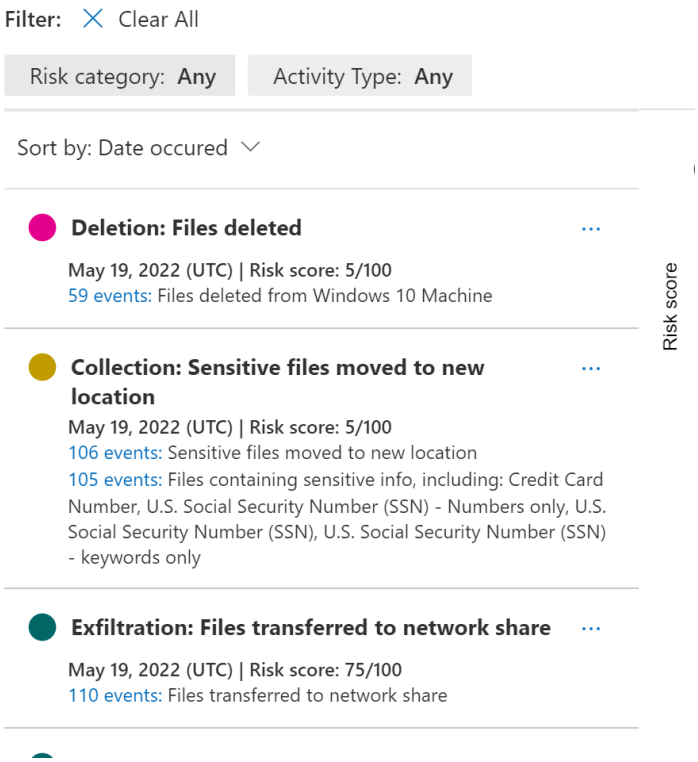
11. You can now move to the **User Explorer** tab

Part 2c – User Explorer

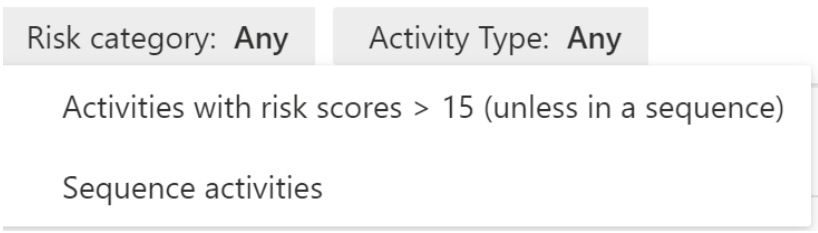
1. Click on **Activity Explorer** tab at the top.



2. On the left-hand side you can **Filter** by **Risk Category** and/or **Activity Type**.

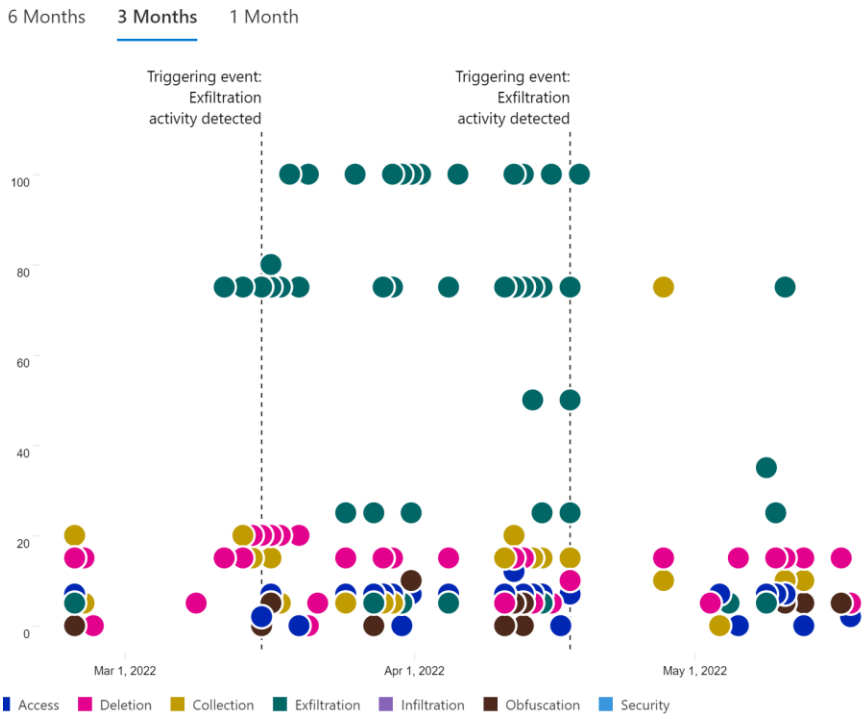


3. Under **Risk categories** you will see these two options. Remember **Risk Scores** is between 0/100 (lowest risk) and 100/100 (highest risk).



4. Under Activity Type, you will see the following options related to data creation, movement and disposal:

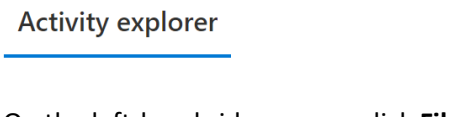
5. On the right-hand side you will see a graphical representation of what has happened over the period selected.



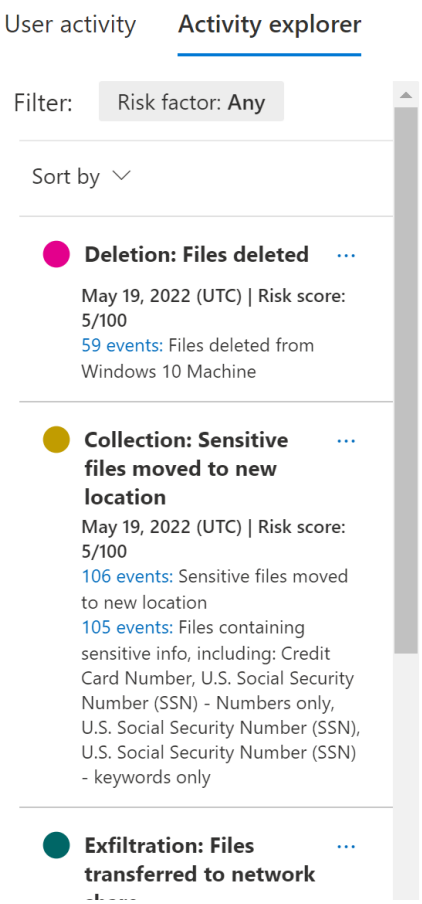
6. You are now down with this section

Part 2d – Activity Explorer

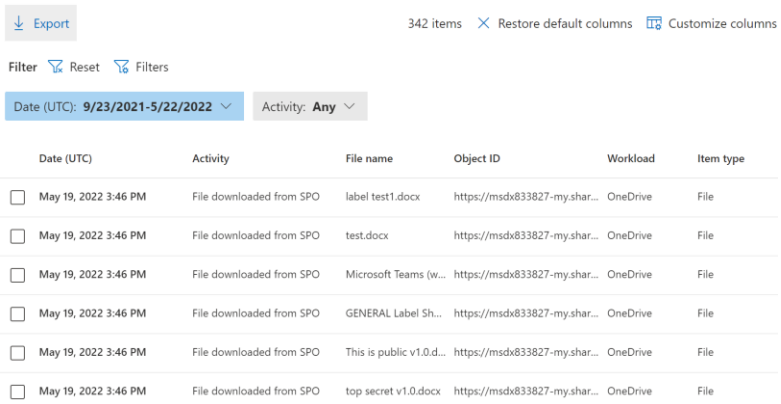
1. Click on **Activity Explorer** tab



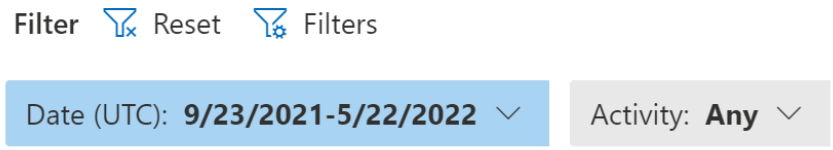
2. On the left-hand side you can click **Filter** to see all the ways you can sift through this data.



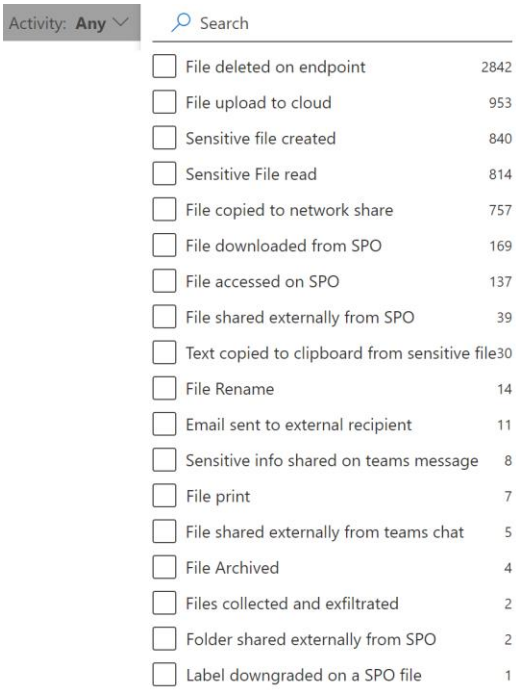
3. The right-hand side lets you look at the list of activities associated with this alert.



4. At the top are filters that let you more easily sift through the data. The default Activity is **Any**,



5. Click on **Activity** to see what the options are you can choose.



6. We are done with this section.

Appendix and Links

[Learn about insider risk management - Microsoft 365 Compliance | Microsoft Docs]

[Investigate insider risk management activities - Microsoft 365 Compliance | Microsoft Docs]

[Insider risk management cases - Microsoft 365 Compliance | Microsoft Docs]

Insider risk management policies - Microsoft 365 Compliance | Microsoft Docs

Insider risk management notice templates - Microsoft 365 Compliance | Microsoft Docs

Insider risk management settings - Microsoft 365 Compliance | Microsoft Docs

Note: This solution is a sample and may be used with Microsoft Compliance tools for dissemination of reference information only. This solution is not intended or made available for use as a replacement for professional and individualized technical advice from Microsoft or a Microsoft certified partner when it comes to the implementation of a compliance and/or advanced eDiscovery solution and no license or right is granted by Microsoft to use this solution for such purposes. This solution is not designed or intended to be a substitute for professional technical advice from Microsoft or a Microsoft certified partner when it comes to the design or implementation of a compliance and/or advanced eDiscovery solution and should not be used as such. Customer bears the sole risk and responsibility for any use. Microsoft does not warrant that the solution or any materials provided in connection therewith will be sufficient for any business purposes or meet the business requirements of any person or organization.