Microsoft

Webinar FAQ: What's New with Insider Risk and Communication Compliance

Prepared by:
Microsoft 365 Security & Compliance Team, December 7, 2021

- **View** the Insider Risk and Communication Compliance documentation for additional information: https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-solution-overview?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance-solution-overview?view=o365-worldwide
- **Sign up** for the MIP Preview Program: https://aka.ms/MIP-Preview
- **Follow** us on twitter: twitter.com/MIPnews
- **Watch** previous webinars: http://aka.ms/MIPC/webinars

Commented [CF1]: Can we also promote the Easy Trials? About the Microsoft 365 compliance trial - Microsoft 365 Compliance | Microsoft Docs

Features & Capabilities

Q: What if user has OD or SP or Teams libraries synced to file explorer and then uploads those as attachments into their private email - i.e., signs in to Yahoo or Gmail, uploads files there and send the email to themselves?

A: Depending on if the device is onboarded (and therefore device activities can be captured). Look at the sequence capabilities within Insider Risk as a nice way to see multiple activities that put together show a risky scenario. In Insider Risk Management we generally look at "trends" of insider risk indicators pivoted on individual users, and activity with sensitive content being shared or emailed out certainly falls in that range. https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-policies?view=o365-worldwide#sequence-detection-preview.

You can learn more about browser signal here - https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-browser-support?view=o365-worldwide.

Q: Does the Insider Risk E5 License include the right to onboard an Endpoint?

A: Yes, it does. IR licenses include Endpoint onboarding but not for Endpoint DLP.

Q: Does the healthcare integration with Epic go beyond what we do with Exact Data Match for DLP?

A: It works differently in that we can use Insider Risk Management to look for risk patterns in how patient data in EPIC is being used. While DLP with Exact Data Match can help us detect patient data in unstructured data (say in OneDrive/Data). This integration is more for finding situations where employees are potentially overstepping normal behavior in EPIC itself. An example is noticing that an employee is looking into health records for their family members or neighbors (which the provider wants to investigate), or a higher volume of records per day that you deem above average.

Commented [CF2]: Added another example as this one is more easy to understand and doesn't open up the question 'how do you know who the neighbours are?'

Q: Are we doing an actual integration or is it like what we do with HR data (have to batch it in)?

A: There is a Healthcare connector to bring EPIC use records in a way like the HR Data Connector today. It does come in via batches (but upload times are controllable in the integration). See details here: https://docs.microsoft.com/en-us/microsoft-365/compliance/import-epic-data?view=o365-worldwide

Q: What is the HR connector? How does it work?

A: The HR Connector is a generic connector that provides you the ability to integrate with any HR System (a popular starting point for detecting Insider Risk). Essentially, we use the HR Connector to look for things like resignation signals, or performance improvement signals which often occur near when data theft could occur. In Insider Risk Management this acts as a trigger to monitor the surrounding activity to see if data theft is occurring. More details on setup here: https://docs.microsoft.com/en-us/microsoft-365/compliance/import-epic-data?view=o365-worldwide as well as a video here: https://www.youtube.com/watch?v=FPOnxKuJ9VI

Q: Where will the guides will be located?

A: Look at our One stop Shop website - https://aka.ms/mipc/OSS

Q: Users are anonymized in IRM but viewing audit activity shows the name of the user being reviewed. Is that intentional?

A: Yes this is intentional. While we do allow for anonymization for admins, investigators and reviewers when reviewing alerts and activities there are times we cannot anonymize the names or you may need to take action on some activities which you need to be able to see who the actor is. To maintain referential integrity for users who have insider risk alerts or cases in Microsoft 365 or other systems, anonymization of usernames isn't preserved for exported alerts. Exported alerts will display usernames for each alert.

Q: What happens when you escalate to Advanced eDiscovery?

A: A review set is generated with all the alerts selected for escalation and a case is created. The eDiscovery manager is notified. Be sure to check if you have eDiscovery manager permissions. Also, you might want to give yourself up to 24 hours for the case content to be handed off. *https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-cases?view=o365-worldwide#escalate-for-investigation*