



Cutting through the noise: Jumpstart your insider risk program with Microsoft Purview

Tatu Seppälä



Security & Compliance Architect



★ Data security,
Insider Risk & Compliance

Generative AI
& AI security

Identity & access
management

Power Platform &
Low-code/No-code

Modern work



Mission statement



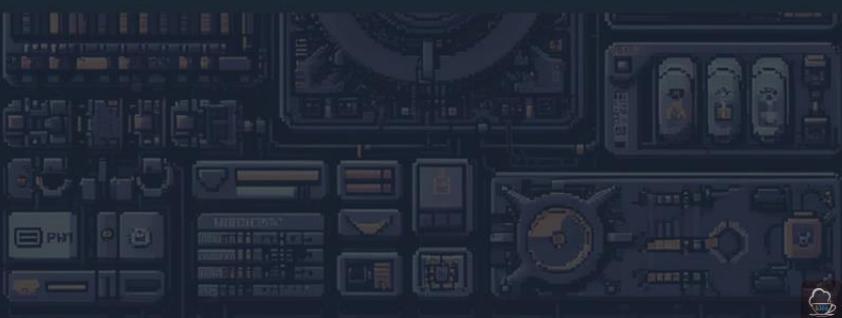
Gathering signals



Assembling a team



Essential configurations



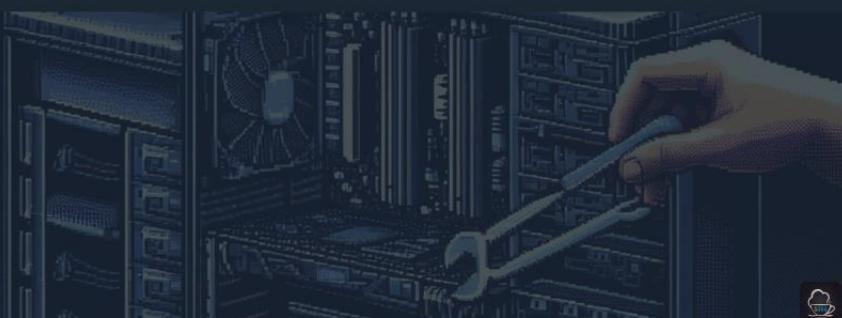
Getting started



Decision points



Fine tuning



Integration



Mission statement



Insider

Any person who has or had **authorized access to** or **knowledge of** an organization's...

- > Information
- > Networks
- > Systems
- > Personnel
- > Facilities
- > Equipment

CISA – "Defining Insider Threats"



Insider risk

The potential for an insider to use their **authorized access or understanding of an organization** to harm that organization.

CISA – “Defining Insider Threats”





Accidental Negligent

- Behavior that violates security policies
- Lack of training or concentration
- Misuse of given tools and resources
- Undesirable behaviour caused by haste or overload



Coerced or malicious

- Unauthorised disclosure of information
- Embezzlement
- Sabotage
- Appropriation of intellectual property
- Corporate espionage



The **signal** is lost in the **noise**



Gathering signals



Indicator

Individual meaningful event



Creating or copying files to USB

Sequence

An interlinked series of meaningful events



Downloading content from SharePoint



Archiving files on a device



Creating or copying files to USB



Deleting files from a device



Indicator source tier list (for getting started)



Device events

Critical

Microsoft 365 / Office events



Defender for Endpoint security events

OK

(Edge & Chrome) Risky browsing events



Defender for Cloud Apps

Situational

Physical access events

Health record events



Device events

Onboard devices to
Microsoft Purview!

- › Creating or copying files to USB
- › Using a browser to upload files to the web
- › Copying files over RDP & Bluetooth
- › Printing documents
- › Deleting files from the endpoint

...

Most data is exfiltrated w/ these



Microsoft 365 / Office events

- › Downloading content from SharePoint / OneDrive
- › Sharing files with externals
- › Downgrading or removing sensitivity labels
- › Accessing sensitive or priority SharePoint sites
- › Sending email with attachments to externals

...

Most **sequences** start with these

Installed extensions / Microsoft Purview Extension



Microsoft Purview Extension

Size < 1 MB Version 1.0.0.71



Description

The Microsoft Purview Extension enables organizations to collect Microsoft Purview Data from the Microsoft Edge browser.



Detected activities

Microsoft Edge

Google Chrome

Files copied to personal cloud storage

Native

Extension

Files printed to local or network devices

Native

Extension

Files transferred or copied to a network share

Extension

Extension

Files copied to USB devices

Extension

Extension

Browsing potentially risky websites

Extension

Extension



Enable MDE-IRM integration



On

Share endpoint alerts with Microsoft Compliance Center

Forwards endpoint security alerts and their triage status to Microsoft Compliance Center, allowing you to enhance [insider risk management](#) policies with alerts and remediate internal risks before they cause harm. Forwarded data is processed and stored in the same location as your Office 365 data.

Security policy violations (preview)

Security policy violations (preview)

Security policy violations by departing users (preview)

Security policy violations by risky users (preview)

Security policy violations by priority users (preview)



Defense evasion - Attempt to bypass security controls



Unwanted software - Unapproved or malicious software

Synergy between your SecOps & Insider Risk teams!

Tip: Create custom variants

Base indicator



Sending email with attachments to recipients outside the organization

+ Custom domain group

Group name	Included domains
Consumer email services	44
Consumer storage services	18

Tip: Create custom **variants**

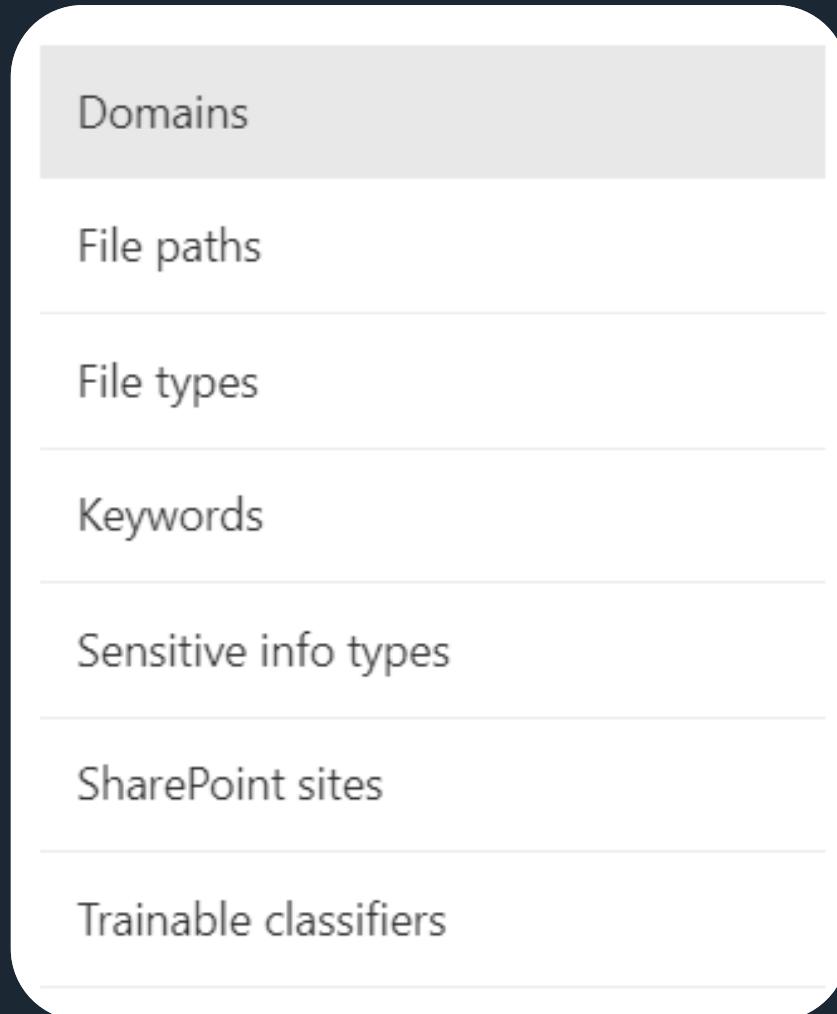
= **Indicator variant** → better signals!



Variant: Sending email with attachments to recipients in consumer email services

Description: Events where email with attachments were sent to recipients in known consumer email services

Tip: Create custom **variants**



Many different types!

Assembling a team



Make HR, Legal & Compliance your allies from the start

- > Identify specific **regulatory and other requirements**
- > Get buy-in from C-levels to resource the insider risk program
- > Build bridges to support future development initiatives
- > Vital in any **true positive** cases



Plan process & roles around IRM RBAC

Management
Insider Risk Admin



Analysis & triage
Insider Risk Analyst



Investigation
Insider Risk Investigator



Auditing
Insider Risk Auditor



Essential configurations





"I never liked that guy.. let's see what he's been up to."

Avoid!





Show anonymized versions of usernames

We'll show an anonymized version of usernames across all insider risk management features (policies, alerts, cases, and so on).

A AnonyIS8-988

Do not show anonymized versions of usernames

We'll show the actual display names for all users who perform activities matching your insider risk policies.

GT Grace Taylor

Pseudoanonymization is essential for privacy & investigation integrity



Past
1-**90** days



Future
1-30 days



Policy trigger

IRM is noisy before fine-tuning

Lower your **alert volume** initially

Alert volume

User activities detected by your policies are assigned a specific risk score, which in turn determines the alert severity (low, medium, high). By default, we'll generate a certain amount of low, medium, and high severity alerts, but you can increase or decrease the volume to suit your needs.

Alert volume

More alerts

You'll see all medium and high severity alerts and most low severity alerts. This might result in more false positives. Review our [alert volume troubleshooting guide](#).

Getting started



Start with Data theft by departing users

Data theft by departing users

Detects data theft by departing users near their resignation or termination date.

Prerequisites

HR data connector OPTIONAL RECOMMENDED

Configure to periodically import resignation and termination date details for your organization. [Set up HR Connector](#)

Devices onboarded OPTIONAL

Physical badging connector OPTIONAL

Physical badging connector configured to periodically import access events to priority physical locations. [Set up badging connector](#)

Triggering event i

- HR data connector imports termination or resignation dates for a user.
- User account deleted from Azure AD.

- User account deleted from Azure AD.
- HR data connector imports termination or resignation dates for a user.

Triggering event i

✓ **Very common real-life stuff for easy wins**

✓ **High true positive %**

✓ **Practice & validate processes**

✓ **Get buy-in for more complex scenarios**



Danger zone



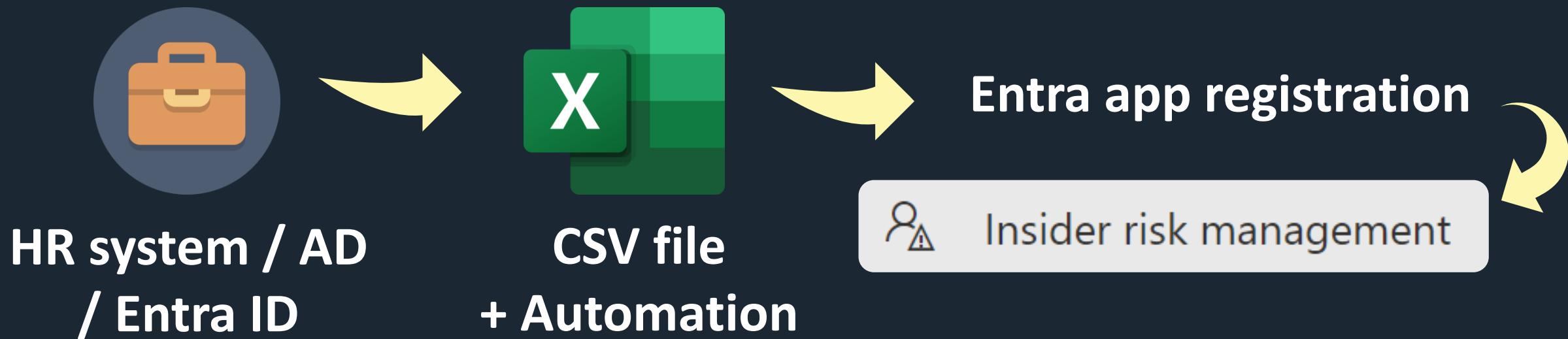
Employment end date set
August 1st 2023



Employment ends
October 31st 2023

Start with Data theft by departing users

- > Usable even without HR connector for pilot & practice
- > **HR connector** is *required* to identify real exfiltration by leavers in time to take action
- > **HR connector** can also work w/ AD or Entra ID data!



Build a routine as early as possible

Every day:

Book at least an hour to triage new alerts & raise cases

Every week:

Go through recent findings with Insider Risk team

Decide on actions to take on raised cases

Every month:

Refine & create policies, custom indicators and variants



Decision points



Alert created



Actions warrant investigation?



Escalate to case & investigate user



Dismiss alert



Accidental?

Improve DLP rules
Provide training

Negligent?

Provide *targeted* training & feedback

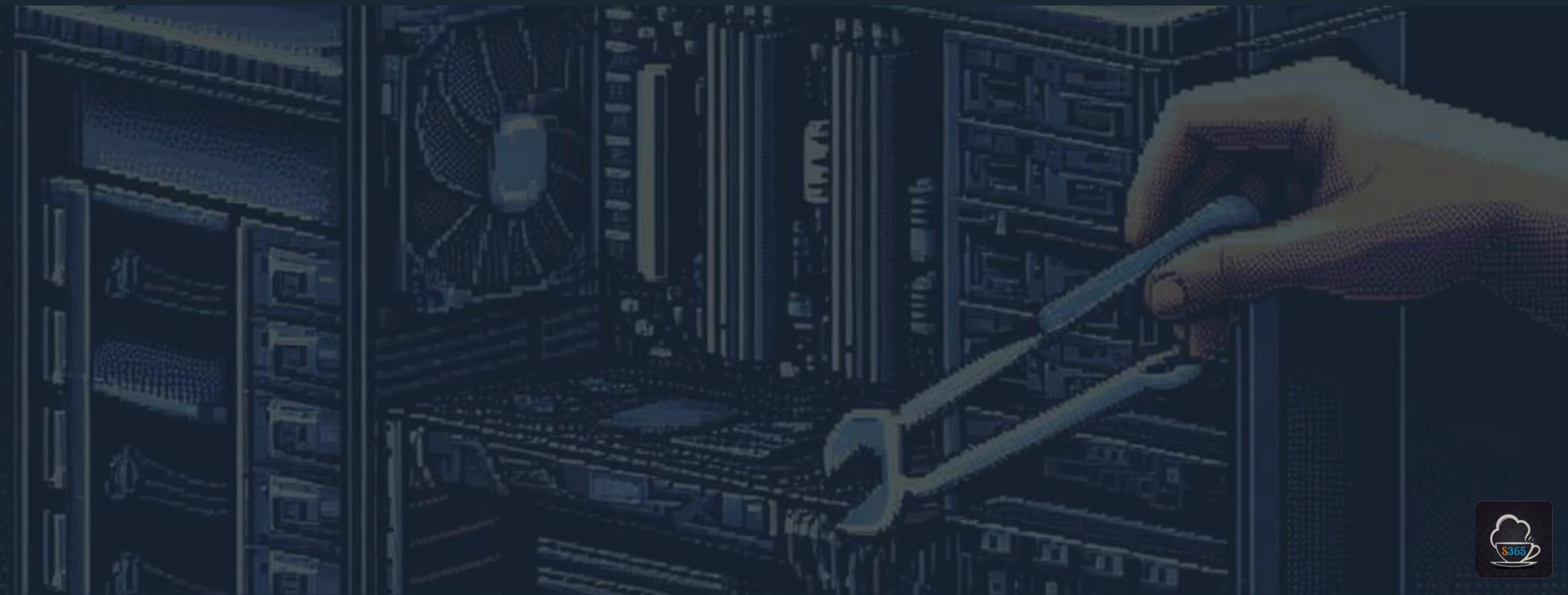
Malicious?

Remove pseudoanon.
Capture forensic evidence
Involve legal & authorities

The hardest part of Insider Risk Management!



Fine tuning



Enable analytics to allow fine-tuning policies

Turn on analytics to scan for potential risks

Scans run daily and provide real-time insights to help detect activity that matters most.



Activity insights over past 10 days (preview)

Insights based on users and activities included in this policy



Approximately 1597 users exceeded lowest daily thresholds for at least one activity

💡 Top 5 activities where users exceeded lowest daily thresholds

Activity	Users
Deleting files from a device	377
Sending email with attachments to recipients outside the orga...	356
Mounting USB to a device	78
Creating or copying files to USB	63

Creating or copying files to USB

⌚ Recommended Thresholds: Low 1511 to 2666, Medium 2666 to 9218, High > 9218

20 ^ ▼ to 40 events per day generates low severity alerts

40 ^ ▼ to 60 events per day generates medium severity alerts

60 ^ ▼ > 60 events per day generates high severity alerts

💡 Approximately **78 users** in this policy exceeded lowest daily thresholds for this activity

Do a fine-tuning pass for each policy & set meaningful thresholds for each indicator

Determine & add priority content to each policy

Trainable classifiers to prioritize

Any activity associated with content that belongs to these trainable classifiers will be assigned a higher risk score.

+ Add or edit trainable classifiers

Trainable classifier

Legal Affairs

M&A Files

Sales and revenue

Strategic planning documents

Legal Agreements



I want to prioritize content

Choose what to prioritize. You'll add the specific items in the next step.

- Sharepoint sites
- Sensitivity labels
- Sensitive info types
- File extensions
- Trainable classifiers

You can create *multiple* IRM policies from the same template w/ differentiated priority content

Integration



Adaptive Protection is easier to use initially with custom risk levels

Define conditions for risk levels

Choose built-in conditions or edit the risk level to create your own.

 Elevated risk level

Custom elevated risk level

Custom risk level

Choose the criteria that the risk level will be based on and then define conditions to control when the risk level is assigned to users.

Risk level based on

- Alert generated or confirmed for a user
- Specific user activity

Alert conditions

Choose the severity for alerts that are generated or confirmed for a user. You can remove a condition if you only want to use one. The risk level will be assigned to a user if the conditions are met.

Severity for confirmed alerts

>=

High

Enhanced DLP auditing, policy tips & controls

User's risk level for Adaptive Protection is Elevated risk level

And

Content contains any of these sensitivity labels: ConfidentialDemo

Recap

- › Craft a clear mission statement
- › Ensure access to key indicators
- › Involve the right stakeholders & establish a routine
- › Pseudoanonymization is critical
- › Start with **data theft by departing employees**
- › The **hardest part** is determining intent
- › Fine-tune your IRM policies!
- › Leverage user risk levels in DLP w/ **Adaptive Protection**

Thank you!

Time for Q&A

Connect with me!

