

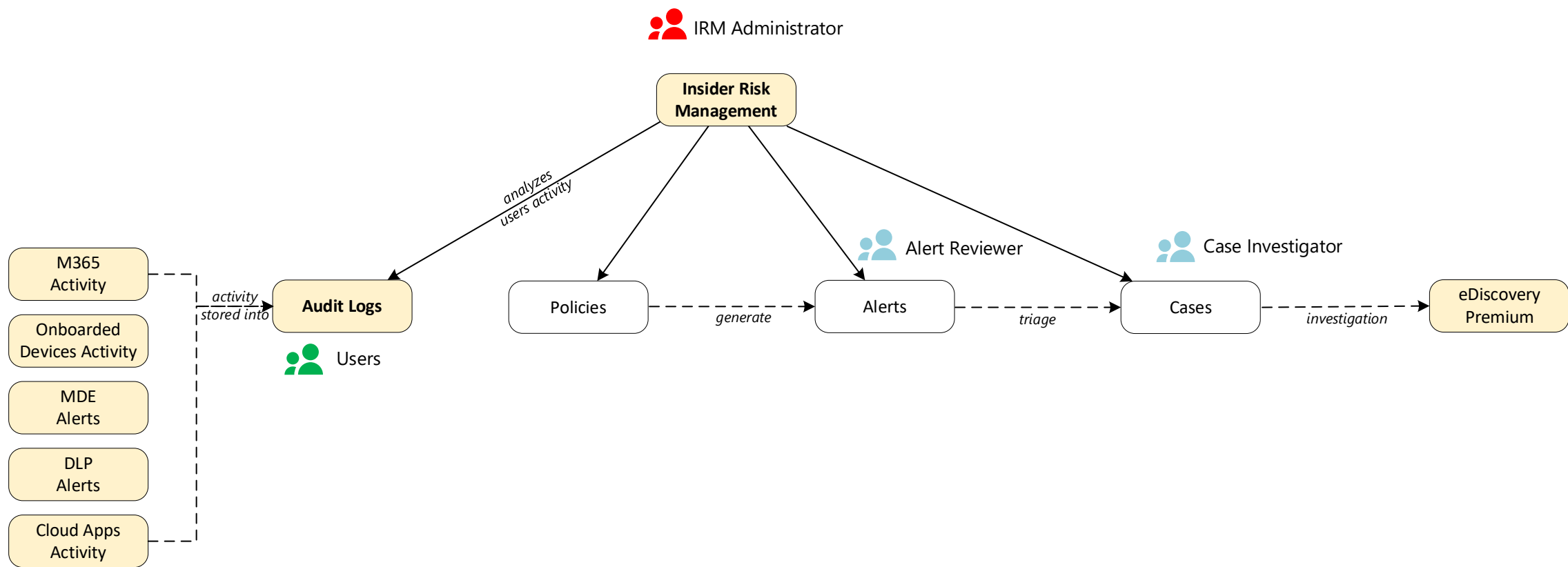


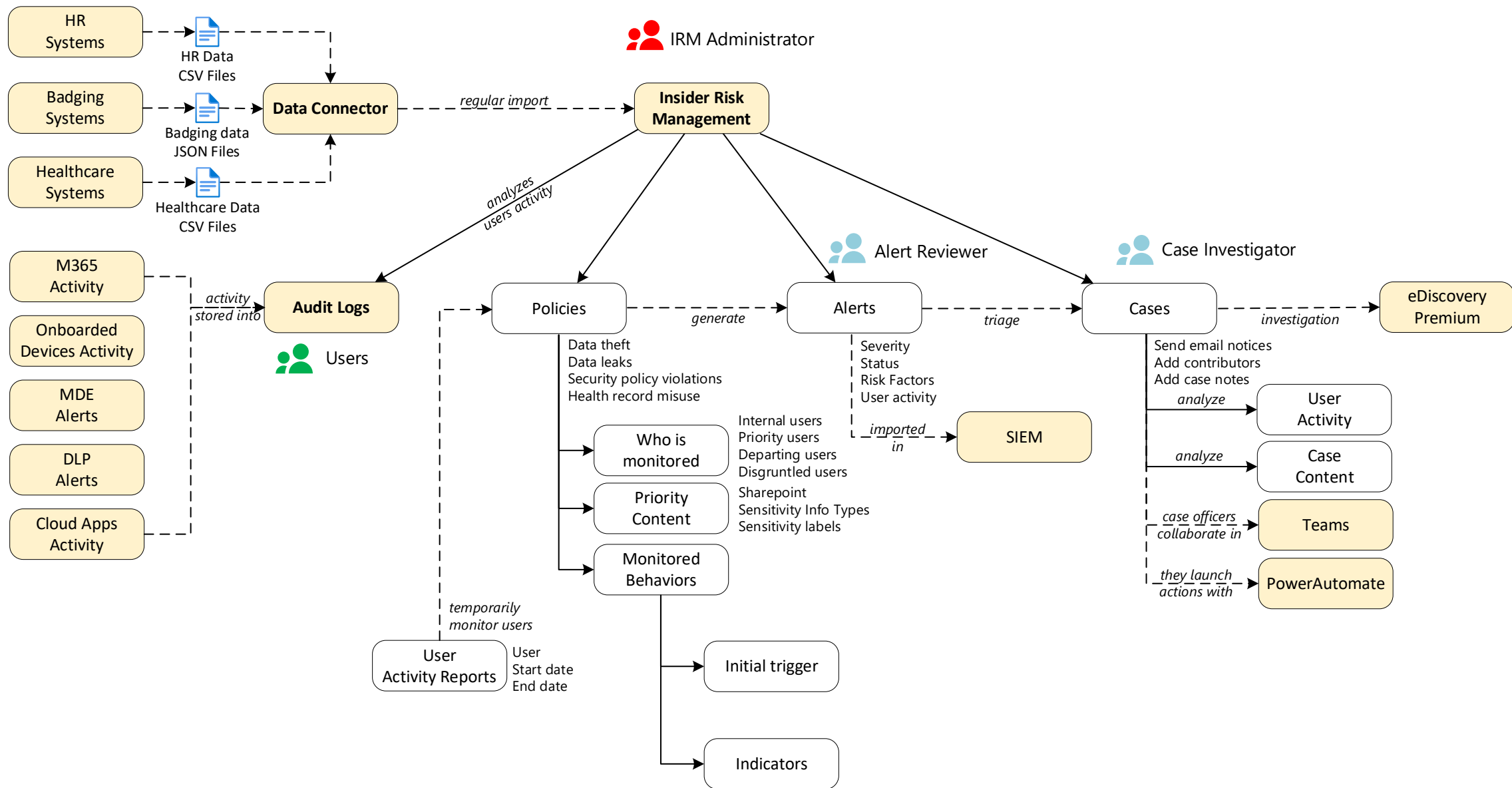
# Vision Diagrams Series

## Insider Risk Management

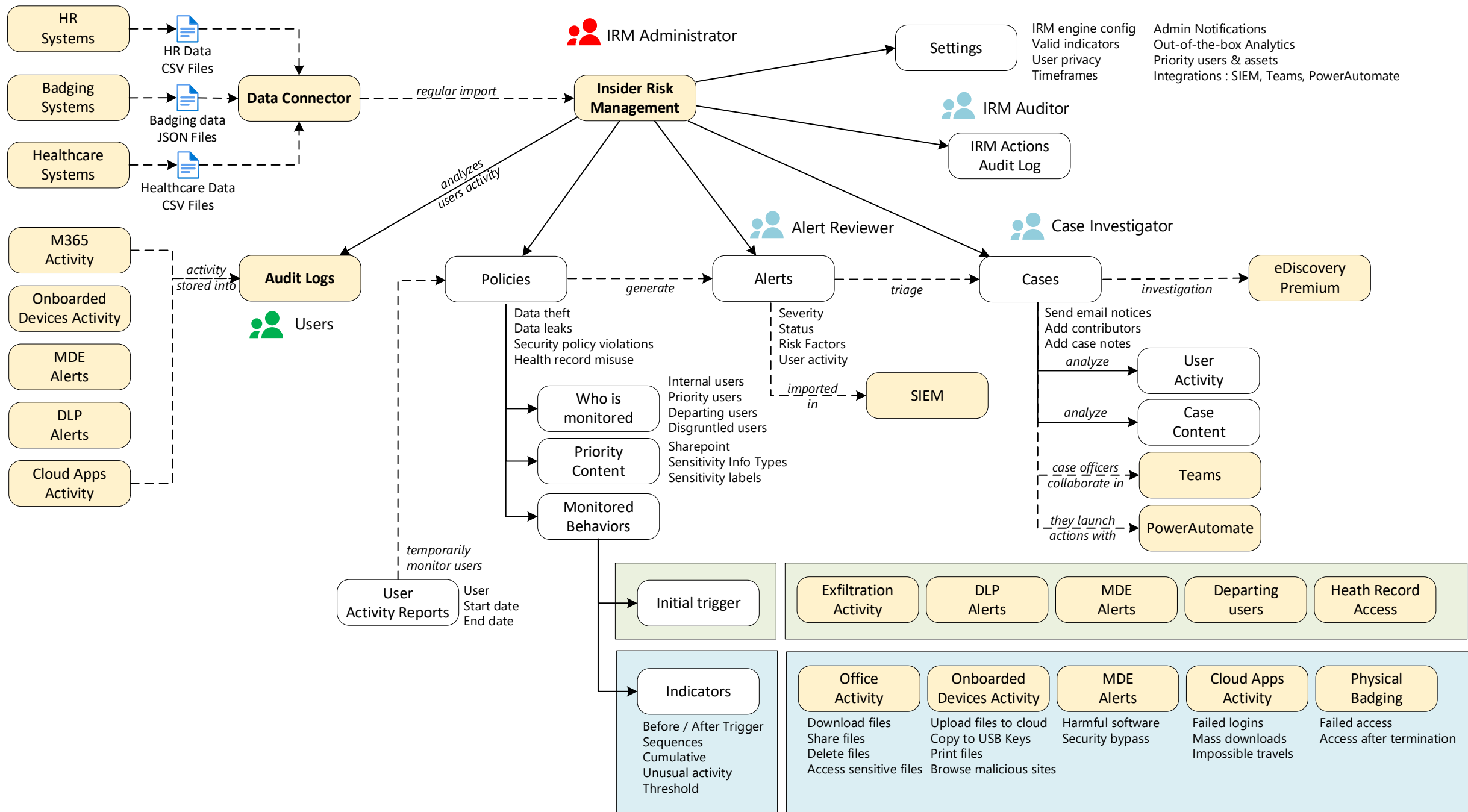
Thierry Matusiak - Data Protection & Compliance - Technical Specialist

*Insider Risk Management  
monitors internal users activity  
to identify suspicious behaviors*





# Insider Risk Management – Even More Details





# Vision Diagrams Series Insider Risk Management

Thierry Matusiak - Data Protection & Compliance - Technical Specialist

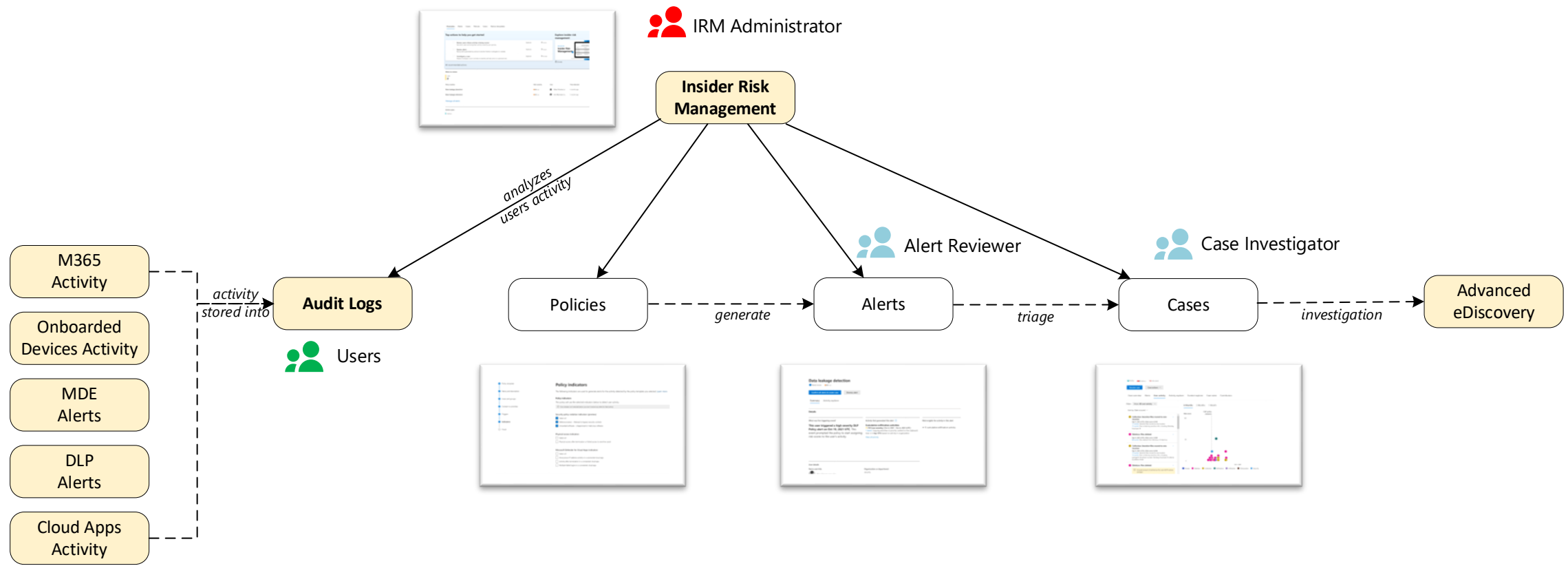







Conclusion



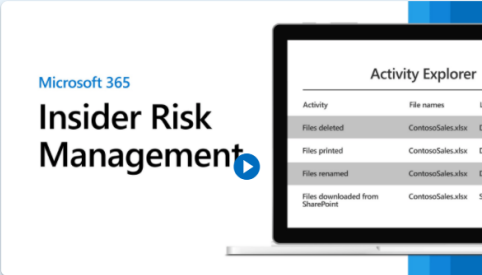




## Top actions to help you get started

<input type="radio"/>	<b>Review users whose activity is being scored</b> See which users are having their activity scored by your policies.	Optional	 5 min
<input type="radio"/>	<b>Review alerts</b> Review alerts generated by policies to decide if further investigation is needed.	Optional	 5 min
<input type="radio"/>	<b>Investigate a case</b> Deeply investigate a user's activities to identify and take action on potential risks.	Optional	 10 min

## Explore insider risk management



 4 min



## All recommended actions

### Alerts to review

Low

2

### Policy matches

	Alert severity	User	Time detected
Data leakage detection	<div><div></div><div></div><div></div>Low</div>	 Nina Simone (s...	2 months ago
Data leakage detection	<div><div></div><div></div><div></div>Low</div>	 Jim Morrison (s...	3 months ago

[Manage all alerts](#)

### Active cases

Active

4


- ✓ Policy template
- ✓ Name and description
- ✓ Users and groups
- ✓ Content to prioritize
- ✓ Triggers
- Indicators**
- Finish

## Policy indicators

The following indicators are used to generate alerts for the activity detected by the policy template you selected. [Learn more](#)

### Policy indicators

This policy will use the selected indicators below to detect user activity.

 If an indicator isn't selected below, you won't receive any alerts for that activity.

### Security policy violation indicators (preview)

- ☒ Select all
- ☒ Defense evasion - Attempt to bypass security controls
- ☒ Unwanted software - Unapproved or malicious software

### Physical access indicators

- ☐ Select all
- ☐ Physical access after termination or failed access to sensitive asset

### Microsoft Defender for Cloud Apps indicators

- ☐ Select all
- ☐ Anonymous IP address activity in a connected cloud app
- ☐ Activity after termination in a connected cloud app
- ☐ Multiple failed logins in a connected cloud app

Back

Next

# Data leakage detection

● Needs review ■ ■ ■ Low

Confirm all alerts & create case

Dismiss alert

Summary    Activity explorer

## Details

What was the triggering event?

**This user triggered a high severity DLP Policy alert on Oct 19, 2021 UTC.** This event prompted the policy to start assigning risk scores to the user's activity.

Activity that generated this alert ⓘ

**Cumulative exfiltration activities**  
**17/100 Low severity** | Oct 4, 2021 - Oct 4, 2021 (UTC)  
**1 event:** Copying sensitive or priority content to the clipboard:  
User is in **top 13%** based on activity in organization  
[View all activity](#)

Risk insights for activity in this alert

- **1** cumulative exfiltration activity

## User details

Name and title



Nina Simone (security)

Organization or department

security

# TMK - JBaker Case

Active Medium 54 risk score

Resolve case

Case actions

- Case overview
- Alerts
- User activity
- Activity explorer
- Content explorer
- Case notes
- Contributors

Filter: Show: All user activity

Sort by: Date occurred

<div>Collection: Sensitive files moved to new location</div> <div>Sep 9, 2021 (UTC)   Risk score: 0/100</div> <div>11 events: Sensitive files moved to new location</div> <div>11 events: Files containing sensitive info, including: Workday Employee ID</div>
<div>Deletion: Files deleted</div> <div>Sep 9, 2021 (UTC)   Risk score: 5/100</div> <div>89 events: Files deleted from Windows 10 Machine</div>
<div>Collection: Sensitive files moved to new location</div> <div>Sep 8, 2021 (UTC)   Risk score: 0/100</div> <div>13 events: Sensitive files moved to new location</div> <div>13 events: Files containing sensitive info, including: [gulagach] Employee number, Workday Employee ID, [Benlc] Ip address finder</div>
<div>Deletion: Files deleted</div> <div><div><div>i</div><div>Unusual amount of activity by this user (657% above average)</div></div></div> <div>Sep 8, 2021 (UTC)   Risk score: 20/100</div> <div>477 events: Files deleted from Windows 10 Machine</div>

6 Months 3 Months 1 Month

