Managing Insider Risk Investigations

LIGHTHOUSE

Graham Hosking – Director, Advisory

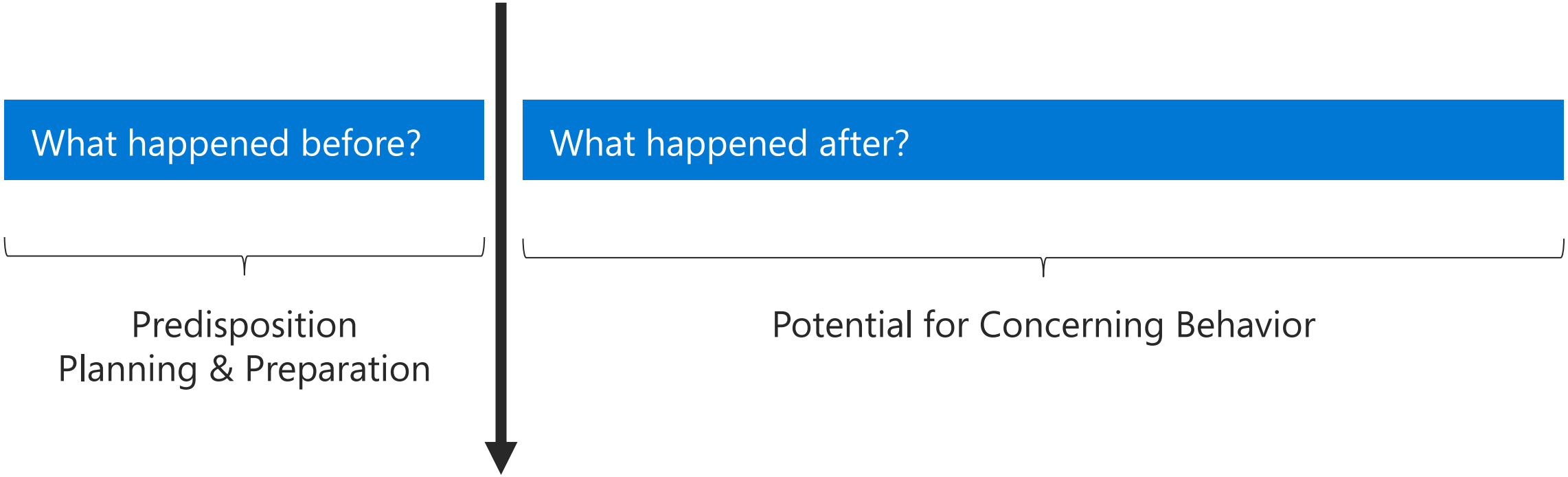
Critical Concept: Events and Data Enrichment

Stressor

Someone receives a performance improvement plan…

In this case, the stressor is something that happens to the person.

In some cases, it may be something like a resignation where they plan the event and take early steps to prepare.



Critical Concept: Events and Data Enrichment

Each element which informs the alert “enriches” the context…
….The system can make a more accurate confidence decision
… The analyst can make an alert triage determination

HR Connector

Someone receives a performance improvement plan…

What happened before?

6 days before:
Accessed OneDrive
Downloaded 10 files…

OneDrive

Information Protection

5 files labeled strictly confidential
7 files meet classifier ‘account number’
7 files meet classifier ‘US Credit Card Number’

2 hours before:
Downloaded 5 files…

2 files labeled “Project Contoso”

What happened after?

Accessed SharePoint
Downloaded 35 files…

SharePoint

5 files labeled strictly confidential

Endpoint DLP indicates a write of 50 files to an external device.

Endpoint DLP

10 files labeled strictly confidential
7 files meet classifier ‘account number’
7 files meet classifier ‘US Credit Card Number’
2 files labeled “Project Contoso”

Exchange exfiltration - Audit framework use case

Exchange Online Platform

Email system for 1:1/1:M outbound sharing of content and/or Attachments both physically attached or via modern attachments (sharing links).

- SIEM
- M365 Audit Logs
- DLP Alerts
- Exchange logs
  Azure AD audit

Modern attachment - Audit framework use case

M365 Service

Sharing from any Microsoft application is possible, which in turn creates a sharing link. Data is stored within the M365 tenant, but access granted with permissions.

App/Service

Sharing link Added to email

Data loss policy check

External recipient

Understanding recipient, access to sensitive data.

M365 tenant

Data accessed

External accesses sensitive data – rights to edit/view

User account is used to access services

Recipient accessed?

SOC Team

Investigate logs to determine timeline of events, and if sensitive data was authorised.

Data loss audit reports/logs

Using a combination of SIEM / M365 DLP logs to view potential triggers/content.

Identity – Log check

Azure AD audit logs
O365 audit logs

Teams Meeting - Audit framework use case

1 **Microsoft Teams federation file share**

Sharing content via chat during a federated connection

2 **Microsoft Teams 1:1/1:M/Meeting**

Sharing data via a desktop/app screenshare is possible.

M365 tenant

Data accessed

External **accesses** sensitive data – rights to edit/view

File Shared during chat

Sharing link created and presented in chat

Data loss policy check

External recipient

Understanding recipient, access to sensitive data.

User account is **used to access MS Team**

Screen share performed

Data loss audit reports/logs

Using a combination of SIEM / M365 DLP logs to view potential triggers/content.

MS Teams logs

Access to the MS Teams admin portal to investigate activities conducted. E.g. Screenshare started.

Recipient accessed?

SOC Team

Investigate logs to determine timeline of events, and if sensitive data was authorised.

Identity – Log check

Azure AD audit logs
O365 audit logs

Data Search/Export - Audit framework use case

User account is **used to access eDiscovery tools**

eDiscovery
Multiple tools to run tenant wide search and export data.

Search run
Search on tenant data. Subset or all

Export request
Export job created ready for download

Data downloaded
Once job is complete zip file used to download to local machine.

Local Machine

Data accessed

Local access now available which now **unaudited**.

- Identity – what machine? Browser?
- Permissions
- M365 audit – search run
- M365 – Export
- Managed device?
- Tenant restrictions
- Conditional access

Data loss audit reports/logs

Using a combination of SIEM / M365 DLP logs to view potential triggers/content.

Alert setup to email all global admins.

SOC Team
Investigate logs to determine timeline of events, and if sensitive data was authorised.

Identity – Log check

Azure AD audit logs
O365 audit logs

Customers face a broad range of Insider risks

Data spillage
People overshare data and don't remove access rights after valid access.

IP theft
People go to the competition and take data with them for an advantage.

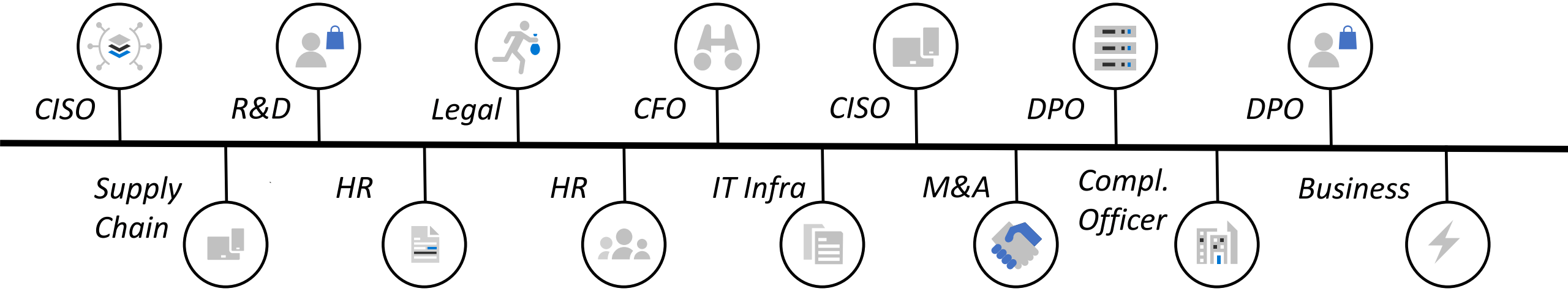
Illicit Activity
Corporate Fraud, Blackmail, and other Illegal activities.

Insider trading
Only the need-to-know should have access to critical financial data.

Leaks of sensitive data
M&A activities, Marketing strategies, Financial results, R&D results.

Data Loss
Mobile devices get stolen, lost and forgotten. Records get deleted without recovery options

"The right to be forgotten"
Registered consumers might request to be removed, as per Privacy regulations.



Leaks of sensitive 3rd party data
Supplier prices, competitor information, etc.

Confidentiality Violations
Unintentional sharing of confidential information.

Workplace violence and harassment
Company culture violations due to bad language and abuse.

Data Proliferation
Many tools can be used on various devices and in multiple locations, companies lose oversight.

Conflicts of Interest
People act in their own interest rather than in the companies' interest.

Regulatory compliance violations
Many new regulations and updates every day.

Accidental data leakage
Information which is derived through technological functions leads to a breach. (Autocomplete, for example)

Microsoft **Insider Risk Management** : How everything works together

Trainable Classifiers

- Targeted Harassment
- Discrimination
- Offensive Language
- Profanity
- 7- Languages
- Custom Document Models

Sensitive info Types

Out of Box
- Credit Card
- SSN
- License
- More

Custom
- RegEx
- Dictionary
- Fingerprint
- EDM

Connectors

- Human Resources
- Registration date
- Performance
- Physical Badge Access

Cloud App Security

- Mass Download
- Mass Sharing
- Activity After Termination
- Failed Logins

Microsoft Information Protection

- Classified Content
- Protected Content - Decrypt

Defender Sensor

- Cloud Upload
- App Control
- USB Drive
- Network
- Print
- Clipboard
- Defense Evasion
- Unwanted Software

Azure Active Directory

- Activity log – accessed, logon times, locations, risk level etc

365 Audit Log

- Activity log – accessed files, moved, re-named, deleted, etc

Informed by Stack

Insider risk analytics

Logic apps

- Transpose audit logs
- Extract IRM only alerts

365 Audit Log

- Activity log – logs IRM alerts
- O365 Management API

Insider Risk Management Service

Azure Sentinel

- Incident management
- Advanced hunting
- Machine learning analytics

Logic Apps

- Trigger automation
- Automatic remediation
- Alerting & notification
- Auto incident creation for ITSM

Permissions
- RBAC:
- IRM / Sentinel
- Content / Activity Explorer

Policies

Categories
- Data theft
- Data leaks
- Security policy violations

Data leaks/Security templates
- General data leaks
- General security violations
- By priority users
- By disgruntled users
- By departing users

Alerts

- Alert management / Triage
- Review summary/activity
- Create case
- Dismiss alerts

Power Automate

- Add calendar reminders
- Notify manager
- Request info from HR
- Custom flows

Notify User

- **Action**:
- Templated email notices
- Anonymized user entity

Cases

- **Investigation** - User activity
- Activity/content explorers
- Case notes
- Contributors- HR/Legal/Sec
- Close case

Escalation

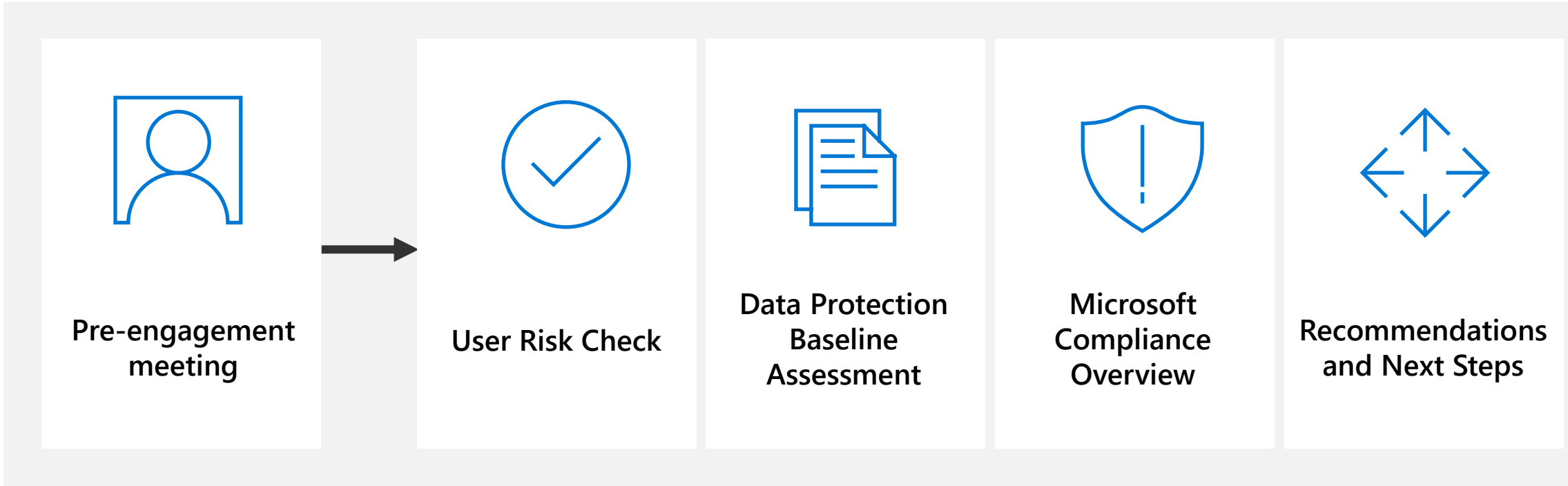
- **Action**:
- Hand-off to Advanced eDiscovery
- Case creation

Created by G.Hosking 9/2021

Investigations and Discussion

Review
Triage
Who’s watching the watchers?
Forensics
Legal Action
Sentinel

The Manage and Investigate Risk Kick Off



Out-of-box sensitive info types

Microsoft 365 includes 200+ sensitive info types

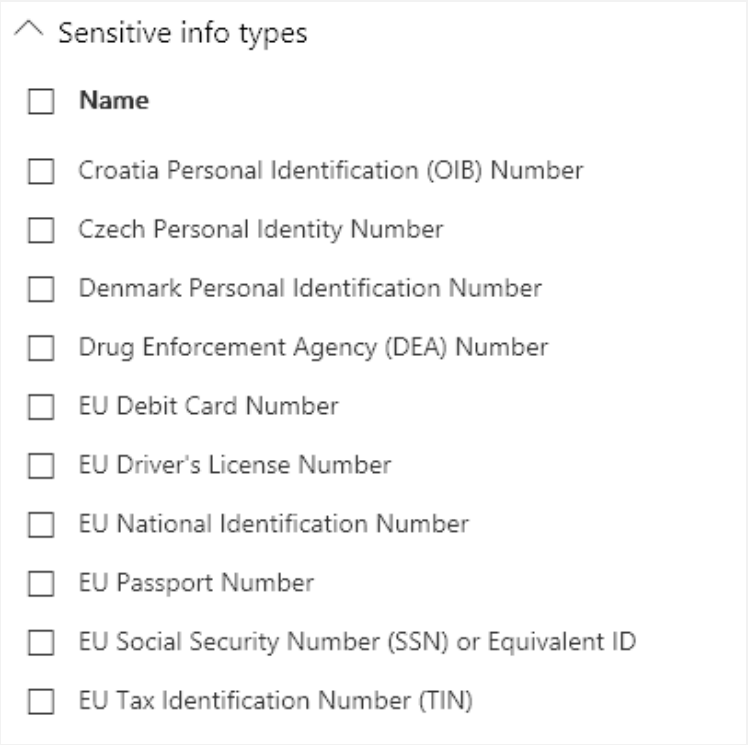
For different countries, industries, or by information type

Sensitive information comes in many forms

Financial data, Personally Identifiable Information (PII)

Examples

- Croatia Personal Identification (OIB) Number
- EU Debit Card Number
- EU Passport Number
- US Drivers License Number
- Social Security Number



Customer-specific sensitive info types

Business intellectual property
Business plans, product designs, confidential projects

Employee or customer information
HR Information, resumés, employment records, salary information

Highly confidential information
Mergers and Acquisition, workforce reduction

Examples

- Employee or customer numbers — *Technology: RegEx*
  - <EMP-nnnnn>
  - <CUST-nnnnnn-NL>
- Specific keywords — *Technology: Static Keywords*
  - <Project Enigma>
  - <Highly Confidential>
  - <Internal only>

Module -Insider Risk Discovery

Activity overview

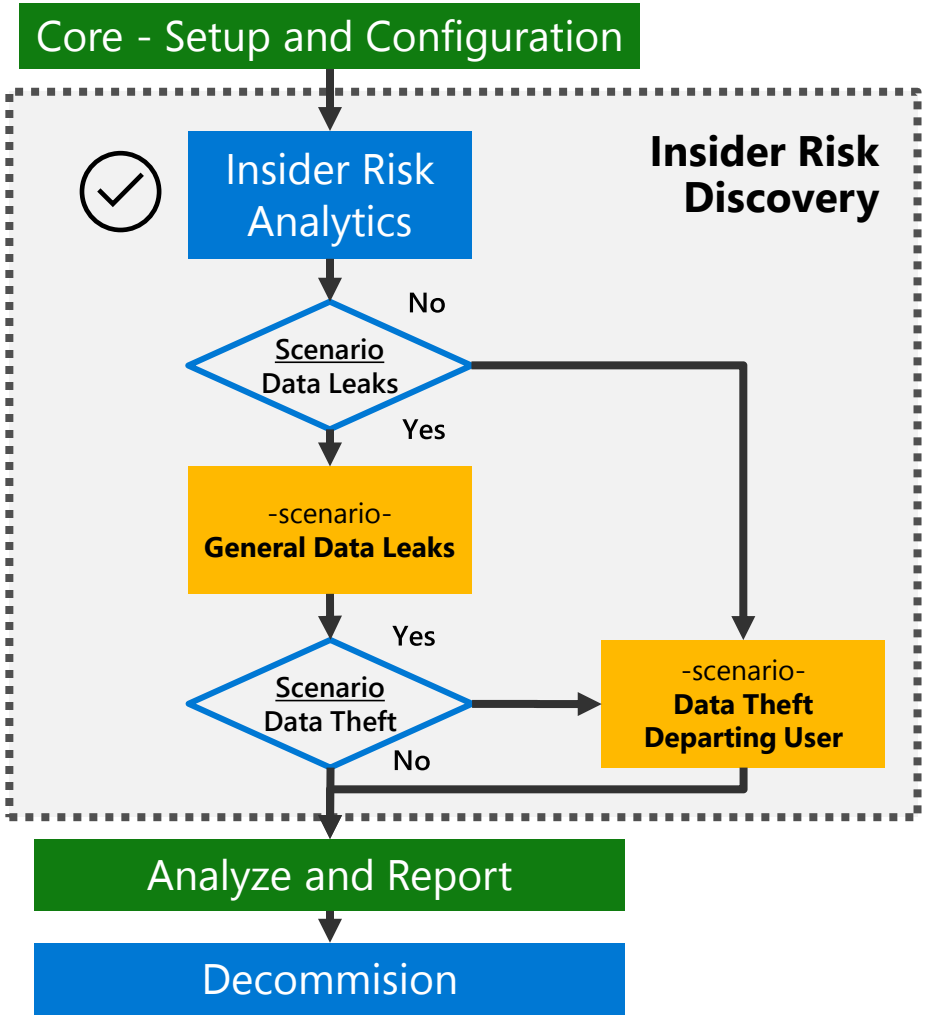
Detect malicious and inadvertent activities in the organization by enabling Insider Risk Management and configuring policies that will define the types of risks to identify and detect.

Insider Risk Analytics

- The first activity for Insider Risk Management

Choose at least one of the additional scenarios:

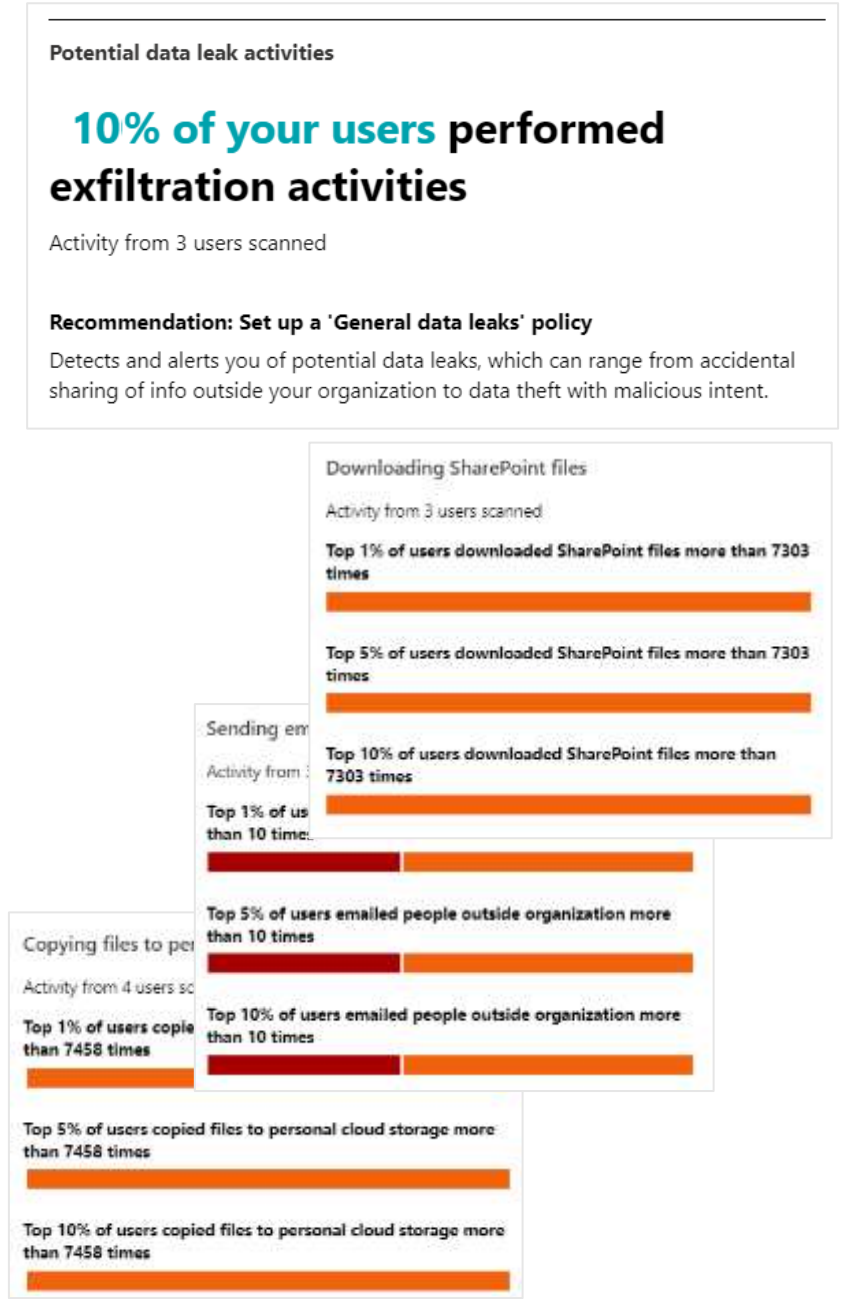
- General data leaks
- Data theft by departing user



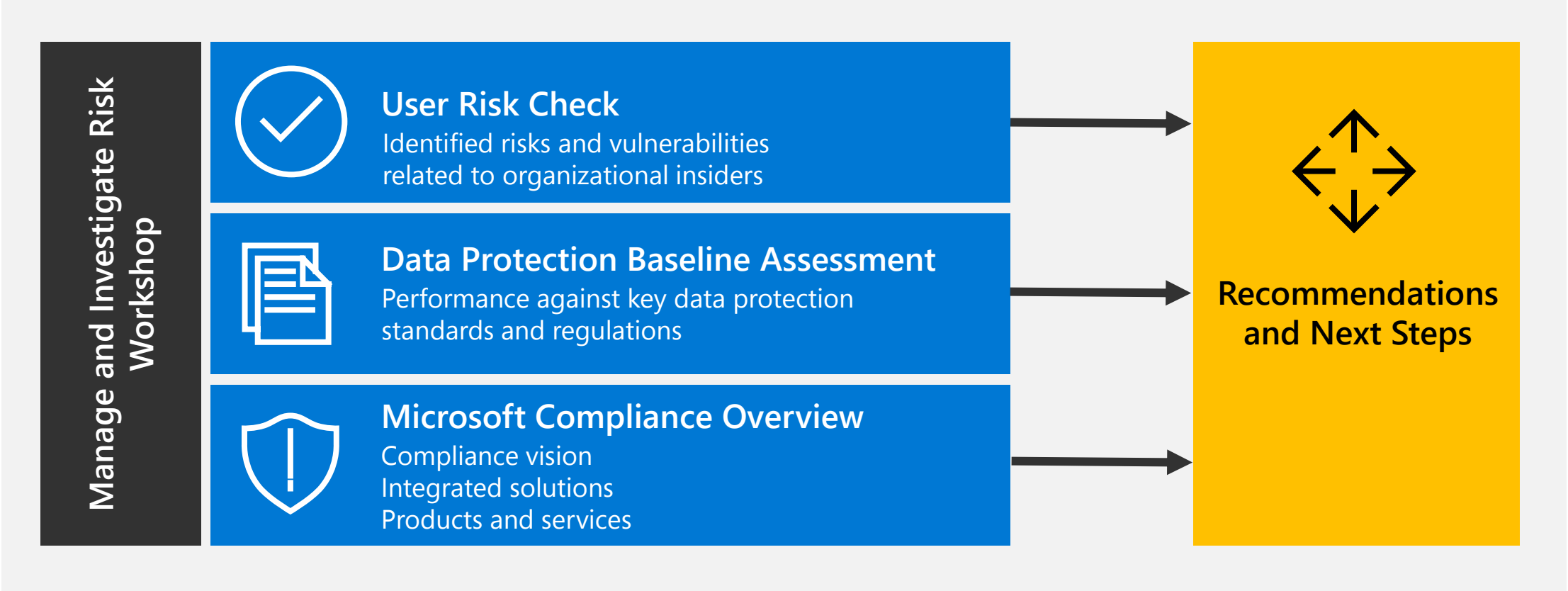
Insider Risk Analytics

Evaluation of potential insider risks

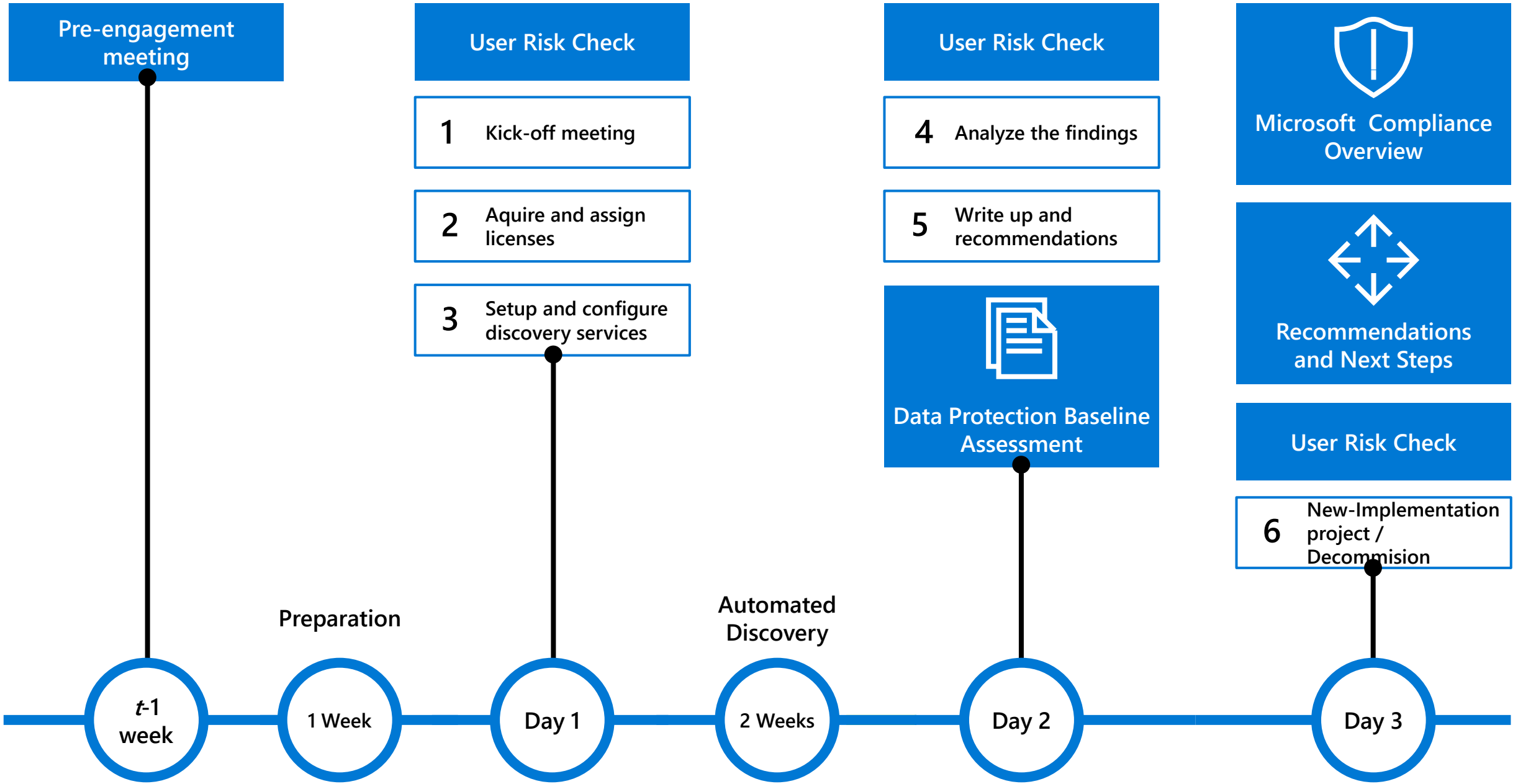
- First activity for Insider Risk Discovery
- Insights based on same signals used by insider risk management
- Works out of the box without configuring policies
- Identify potential areas of high user risk
- Help determine type and scope for policies to consider



Recommendations and next steps



Workshop timeline



Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings

Insider risk management

Overview | Alerts | Cases | Policies | Users | Notice templates

Top actions to help you get started

✓	**Turn on auditing** Start recording user and admin activity to the audit log.	Required	2 min
✓	**Get permissions to use insider risk management.** Assign yourself to an insider risk management role group.	Required	2 min
✓	**Choose policy indicators** Choose the user activities you want your policies to detect.	Required	2 min
✓	**Scan for potential insider risks** Run an analytics scan to identify potential risks in your org.	Optional	5 min
○	**Assign permissions to others** Assign other admins to an insider risk management role group.	Optional	5 min
✓	**Create your first policy** Use predefined templates to detect risk activities, such as data theft.	Required	5 min

Explore insider risk management

4 min

All recommended actions

Alerts to review

High	Medium	Low
10	5	3

Policy matches	Alert severity	User	Time detected
Departing Employee Theft	High	#Anonymized#...	4 months ago
Corp. Terms Data Leak	High	#Anonymized#...	4 months ago

Active cases

Active
4

Case name	Status	User	Case last updated
IRM003	Active	#Anonymized#...	10 months ago
IRM005	Active	#Anonymized#...	10 months ago

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings

Alerts to review

High	Medium	Low
10	5	3

Policy matches	Alert severity	User	Time detected
Departing Employee Theft	High	#Anonymized#...	4 months ago
Corp. Terms Data Leak	High	#Anonymized#...	4 months ago

Manage all alerts

Active cases

Active
4

Case name	Status	User	Case last updated
IRM003	Active	#Anonymized#...	10 months ago
IRM005	Active	#Anonymized#...	10 months ago

Manage all cases

Users

Display name	Risk level	Case
#Anonymized#EAAAALz0miRg3YamuZXgheRwGt5MTTJFOc...	High	IRM007
#Anonymized#EAAAAI3gtsInqaWBBTWfYWp+/2XzUYcBY+2...	High	IRM005
#Anonymized#EAAAAPOwMJ4UhxzTBNKqZwRki+UyDhaHu...	High	
#Anonymized#EAAAAF0I9iw2cDTKIW6oiFgGJFz5ZEIJDP5H...	High	

View all users

Policies with most activity

Policy name	Active alerts	Confirmed alerts
GDPR Data Leaks	5	4
Corp. Terms Data Leak	5	4
PCI Data Leaks	4	4
Departing Employee Theft	2	6

Manage all policies

Insider risk analytics (preview)

Activities detected and ready to review

Analytics scan is complete. Review the anonymized results to identify potential risks and determine which policies to set up.

View results

User activity reports (preview)

Investigate user activity

Search for any user's recent activity, regardless of whether they're already included in a policy or an alert. Review the results in a detailed report to help you quickly identify potential risks.

Manage reports

Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources
Customize navigation

Results from the last scan for risk activities

The insights below provide a summary of anonymized user activities detected. Activities scanned are the same ones detected by insider risk policies. After reviewing the insights, view their details to drill down further and set up a recommended policy to address potential risks.

Insights from September 18 - September 27

Potential data leak activities

20% of your users performed exfiltration activities

Activity from 5 users scanned

20% of users performed activities involving sensitive info
20% of users downloaded SharePoint files

Recommendation: Set up a 'General data leaks' policy

Detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

View details

Top exfiltration activities

Recommendation

Set up a 'General data leaks' policy
Create a policy that detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

Downloading SharePoint files

Activity from 3 users scanned

Top 1% of users downloaded SharePoint files more than 179 times

Top 5% of users downloaded SharePoint files more than 179 times

Top 10% of users downloaded SharePoint files more than 179 times

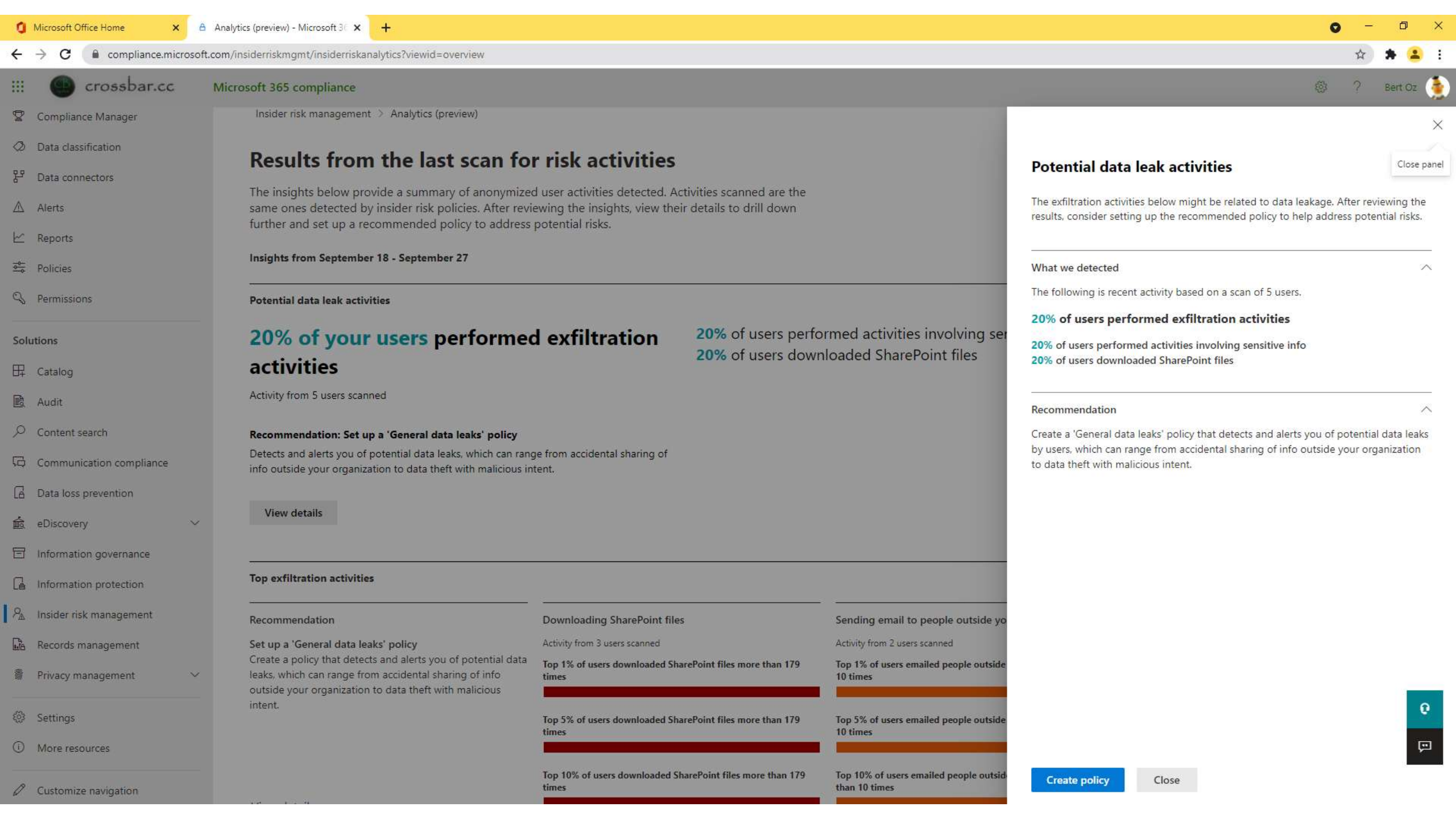
Sending email to people outside your organization

Activity from 2 users scanned

Top 1% of users emailed people outside organization more than 10 times

Top 5% of users emailed people outside organization more than 10 times

Top 10% of users emailed people outside organization more than 10 times


Microsoft Office Home
Analytics (preview) - Microsoft
compliance.microsoft.com/insiderriskmgmt/insiderriskanalytics?viewid=overview
crossbar.cc
Microsoft 365 compliance
Bert Oz
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings
More resources
Customize navigation
Insider risk management > Analytics (preview)
Results from the last scan for risk activities
The insights below provide a summary of anonymized user activities detected. Activities scanned are the same ones detected by insider risk policies. After reviewing the insights, view their details to drill down further and set up a recommended policy to address potential risks.
Insights from September 18 - September 27
Potential data leak activities
20% of your users performed exfiltration activities
Activity from 5 users scanned
Recommendation: Set up a 'General data leaks' policy
Detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.
View details
20% of users performed activities involving ser
20% of users downloaded SharePoint files
Top exfiltration activities
Recommendation
Set up a 'General data leaks' policy
Create a policy that detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.
Downloading SharePoint files
Activity from 3 users scanned
Top 1% of users downloaded SharePoint files more than 179 times
Top 5% of users downloaded SharePoint files more than 179 times
Top 10% of users downloaded SharePoint files more than 179 times
Sending email to people outside yo
Activity from 2 users scanned
Top 1% of users emailed people outside 10 times
Top 5% of users emailed people outside 10 times
Top 10% of users emailed people outsid than 10 times
Close panel
Potential data leak activities
The exfiltration activities below might be related to data leakage. After reviewing the results, consider setting up the recommended policy to help address potential risks.
What we detected
The following is recent activity based on a scan of 5 users.
20% of users performed exfiltration activities
20% of users performed activities involving sensitive info
20% of users downloaded SharePoint files
Recommendation
Create a 'General data leaks' policy that detects and alerts you of potential data leaks by users, which can range from accidental sharing of info outside your organization to data theft with malicious intent.
Create policy
Close

Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings
More resources
Customize navigation

Results from the last scan for risk activities

The insights below provide a summary of anonymized user activities detected. Activities scanned are the same ones detected by insider risk policies. After reviewing the insights, view their details to drill down further and set up a recommended policy to address potential risks.

Insights from September 18 - September 27

Potential data leak activities

20% of your users performed exfiltration activities

Activity from 5 users scanned

Recommendation: Set up a 'General data leaks' policy

Detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

View details

20% of users performed activities involving ser
20% of users downloaded SharePoint files

Top exfiltration activities

Recommendation

Set up a 'General data leaks' policy
Create a policy that detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

View details

Downloading SharePoint files

Activity from 3 users scanned

Top 1% of users downloaded SharePoint files more than 179 times

Top 5% of users downloaded SharePoint files more than 179 times

Top 10% of users downloaded SharePoint files more than 179 times

Sending email to people outside yo

Activity from 2 users scanned

Top 1% of users emailed people outside 10 times

Top 5% of users emailed people outside 10 times

Top 10% of users emailed people outsid than 10 times

Exfiltration insights

After reviewing the exfiltration activities we detected below, consider setting up the recommended policy to help address potential risks.

What we detected

The following is recent exfiltration activity from users in your organization.

Top 1% of users downloaded SharePoint files more than 179 times

Top 1% of users emailed people outside organization more than 10 times

Recommendation

Create a 'General data leaks' policy that detects and alerts you of potential data leaks by users, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

Create policy | Close

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings

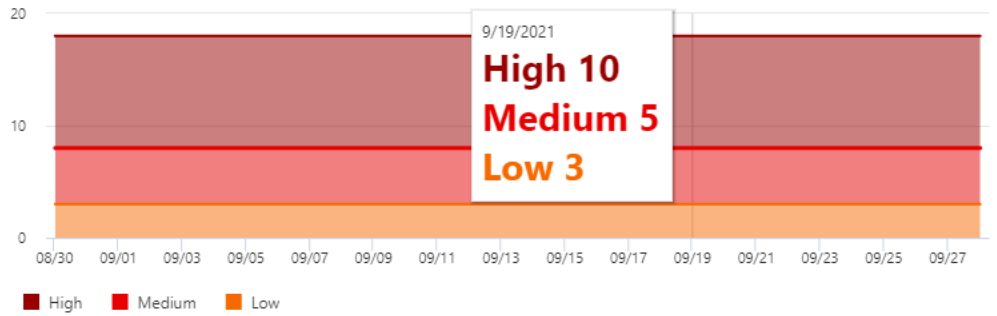
Insider risk management

Overview | Alerts | Cases | Policies | Users | Notice templates

Total alerts that need review

High	Medium	Low
10	5	3

Open alerts over past 30 days



Average time to resolve alerts

High severity alerts
Resolution time not available

Medium severity alerts
Resolution time not available

Low severity alerts
Resolution time not available

Export | 43 items | Search | Filter

Users	Alert	Status	Alert severity	Time detected	Case	Case status
#Anonymized#EAAAAOAQcAZvPVVaK2AB38FHzkNfrJcQEoogDy+EUpUkayd5vK6c2...	Corp. Terms Data Leak	Needs review	Low	a month ago		No case
#Anonymized#EAAAAPydsTOW18pCia7/7/IKY4BSM+Ie0YIOV7tzpK02B+4+cKDhSqT...	GDPR Data Leaks	Needs review	Low	a month ago		No case
#Anonymized#EAAAABBxihjZ0c/U5h9Uw05kouWdRG+Kkiyw1Ileu/+fXjv45K2x2uQm...	Corp. Terms Data Leak	Needs review	Medium	2 months ago		No case
#Anonymized#EAAAANg87qWC47kIYAWqbnRe9Bu56rtJqENmpUeMpuZpJY0M6WD...	PCI Data Leaks	Needs review	Medium	2 months ago		No case
#Anonymized#EAAAABfAhJNj0Dq6XrgTYftbTs3EExQAz6nP4HfbM3DdWxz+5J6yBR6...	GDPR Data Leaks	Needs review	Medium	2 months ago		No case
#Anonymized#EAAAAGzUs5kxIEMThUggboD1LAbWI854GQkShla+4e81BBol4BbnoO...	Departing Employee Theft	Needs review	High	4 months ago		No case

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings

Departing Employee Theft

Needs review ■■■ High

Confirm all alerts & create case | Dismiss alert

Summary | Activity explorer

Details

Activity that generated this alert

Data exfiltration: Files downloaded from SharePoint
75/100 **High severity** | Mar 11, 2021 (UTC)
335 events: Files downloaded from 1 SharePoint site
296 events: Files containing sensitive info, including: EU Debit Card Number, Taiwan Passport Number, Italy Passport Number, EU Social Security Number (SSN) or Equivalent ID, EU Tax Identification Number (TIN)
30 events: Files that have labels applied, including: General, Confidential
Factors that impacted risk score:
Includes priority content (24 events)

Risk insights for activity in this alert

- **4** activities are considered unusual for the user
- **11** activities include events with priority content
- **2** sequence activities

User details

Name and title

A #Anonymized#EAAAAMZYmQFOo7WeVFhtMprx2Oj80CB2RsrhVUEltoozTcyztMycMauiN5sDvpfWX9tXng==

Alert details

Policy matches
Departing Employee Theft

Case
None

Time detected
12:00 AM UTC on Mar 11, 2021

Other alerts for this user
High severity (Needs review)
Disgruntled Users Data Leak
11 June 2021
4 more alerts

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings

Departing Employee Theft

Needs review ■■■ High

Confirm all alerts & create case | Dismiss alert

Summary | Activity explorer

Filter:

Show: All scored activity for this u...

Risk insight: Any

Sort by

Access: Unusual volume of sensitive files read
Sep 10, 2021 (UTC) | Risk score: 0/100
4 events: Files were read
4 events: Files containing sensitive info, including: Trading Analysis slang terms, New Zealand Inland Revenue number, Credit Card Number copy, U.S. Bank Account Number, EU Debit Card Number

Deletion: Files deleted
Sep 10, 2021 (UTC) | Risk score: 10/100
26 events: Files deleted from Windows 10 Machine

Collection: Sensitive files moved to new location
Aug 26, 2021 (UTC) | Risk score: 0/100
1 event: Sensitive files moved to new location
1 event: Files containing sensitive info, including: Hungarian Social Security Number (TAJ), EU Tax Identification Number (TIN), Credit Card Number copy, EU Debit Card Number, U.S. Bank Account Number
1 event: Files that have labels applied, including: Confidential

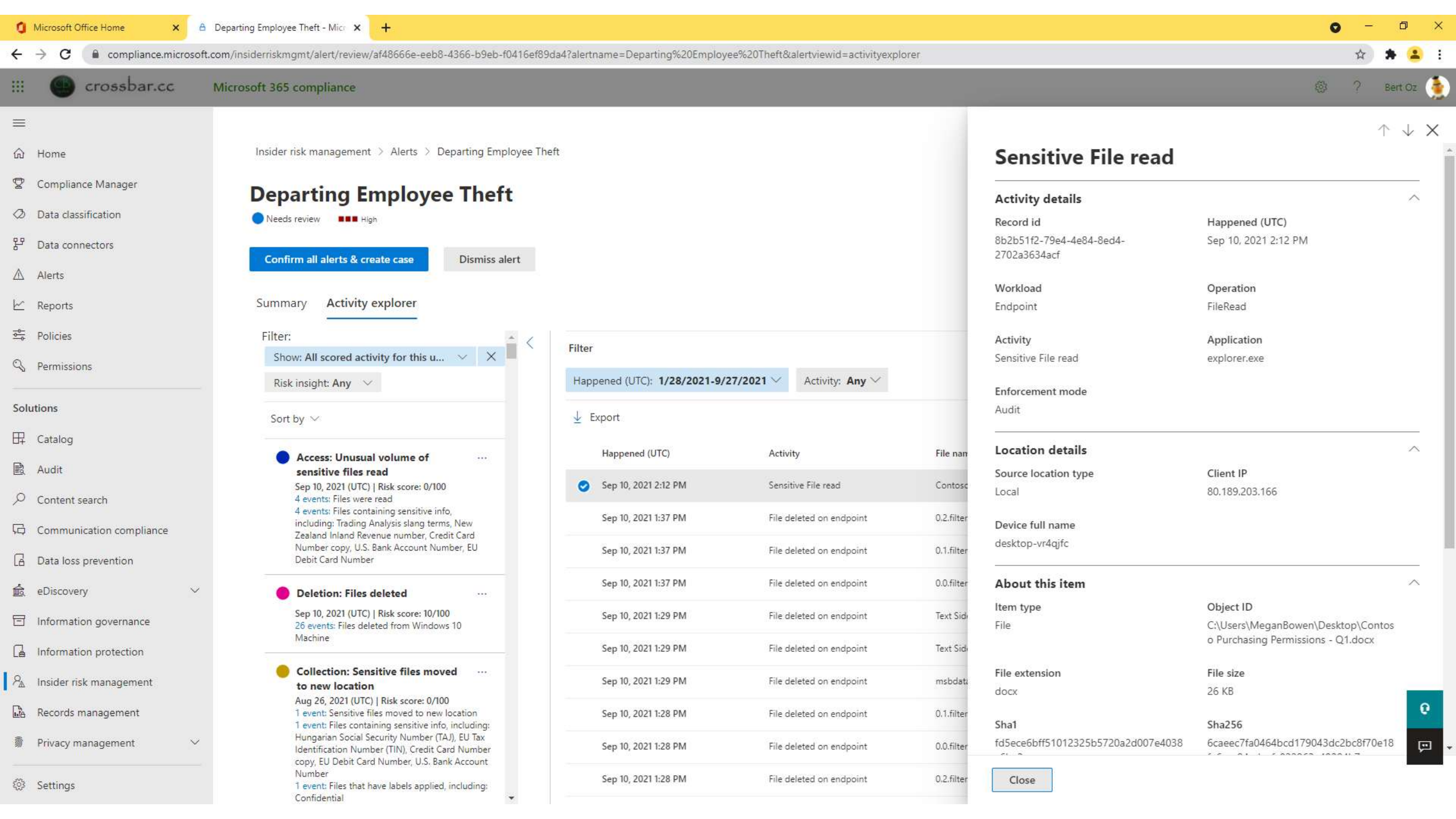
Filter

Clear all | Filters

Happened (UTC): 1/28/2021-9/27/2021 | Activity: Any

Export | 11478 items | Restore default columns | Customize columns

Happened (UTC)	Activity	File name	Object ID	Workload	Item type
Sep 10, 2021 2:12 PM	Sensitive File read	Contoso Purchasing Permissi...	C:\Users\MeganBowen\Desktop\Cont...	Endpoint	File
Sep 10, 2021 1:37 PM	File deleted on endpoint	0.2.filtertrie.intermediate.txt	C:\Users\MeganBowen\AppData\Loca...	Endpoint	File
Sep 10, 2021 1:37 PM	File deleted on endpoint	0.1.filtertrie.intermediate.txt	C:\Users\MeganBowen\AppData\Loca...	Endpoint	File
Sep 10, 2021 1:37 PM	File deleted on endpoint	0.0.filtertrie.intermediate.txt	C:\Users\MeganBowen\AppData\Loca...	Endpoint	File
Sep 10, 2021 1:29 PM	File deleted on endpoint	Text Sidebar (Annual Report ...	C:\Users\MeganBowen\AppData\Loca...	Endpoint	File
Sep 10, 2021 1:29 PM	File deleted on endpoint	Text Sidebar (Annual Report ...	C:\Users\MeganBowen\AppData\Loca...	Endpoint	File
Sep 10, 2021 1:29 PM	File deleted on endpoint	msbdata_edba8fd44a91665b...	C:\Users\MeganBowen\AppData\Loca...	Endpoint	File
Sep 10, 2021 1:28 PM	File deleted on endpoint	0.1.filtertrie.intermediate.txt	C:\Users\MeganBowen\AppData\Loca...	Endpoint	File
Sep 10, 2021 1:28 PM	File deleted on endpoint	0.0.filtertrie.intermediate.txt	C:\Users\MeganBowen\AppData\Loca...	Endpoint	File
Sep 10, 2021 1:28 PM	File deleted on endpoint	0.2.filtertrie.intermediate.txt	C:\Users\MeganBowen\AppData\Loca...	Endpoint	File


Microsoft Office Home
Departing Employee Theft - Micr
compliance.microsoft.com/insiderriskmgmt/alert/review/af48666e-eeb8-4366-b9eb-f0416ef89da4?alertname=Departing%20Employee%20Theft&alertviewid=activityexplorer
crossbar.cc
Microsoft 365 compliance
Bert Oz
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings
Insider risk management > Alerts > Departing Employee Theft
Departing Employee Theft
Needs review
High
Confirm all alerts & create case
Dismiss alert
Summary
Activity explorer
Filter:
Show: All scored activity for this u...
Risk insight: Any
Sort by
Access: Unusual volume of sensitive files read
Sep 10, 2021 (UTC) | Risk score: 0/100
4 events: Files were read
4 events: Files containing sensitive info, including: Trading Analysis slang terms, New Zealand Inland Revenue number, Credit Card Number copy, U.S. Bank Account Number, EU Debit Card Number
Deletion: Files deleted
Sep 10, 2021 (UTC) | Risk score: 10/100
26 events: Files deleted from Windows 10 Machine
Collection: Sensitive files moved to new location
Aug 26, 2021 (UTC) | Risk score: 0/100
1 event: Sensitive files moved to new location
1 event: Files containing sensitive info, including: Hungarian Social Security Number (TAJ), EU Tax Identification Number (TIN), Credit Card Number copy, EU Debit Card Number, U.S. Bank Account Number
1 event: Files that have labels applied, including: Confidential
Filter
Happened (UTC): 1/28/2021-9/27/2021
Activity: Any
Export
Happened (UTC)
Activity
File nam
Sep 10, 2021 2:12 PM
Sensitive File read
Contosc
Sep 10, 2021 1:37 PM
File deleted on endpoint
0.2.filter
Sep 10, 2021 1:37 PM
File deleted on endpoint
0.1.filter
Sep 10, 2021 1:37 PM
File deleted on endpoint
0.0.filter
Sep 10, 2021 1:29 PM
File deleted on endpoint
Text Sid
Sep 10, 2021 1:29 PM
File deleted on endpoint
Text Sid
Sep 10, 2021 1:29 PM
File deleted on endpoint
msbdata
Sep 10, 2021 1:28 PM
File deleted on endpoint
0.1.filter
Sep 10, 2021 1:28 PM
File deleted on endpoint
0.0.filter
Sep 10, 2021 1:28 PM
File deleted on endpoint
0.2.filter
Sensitive File read
Activity details
Record id
8b2b51f2-79e4-4e84-8ed4-2702a3634acf
Happened (UTC)
Sep 10, 2021 2:12 PM
Workload
Endpoint
Operation
FileRead
Activity
Sensitive File read
Application
explorer.exe
Enforcement mode
Audit
Location details
Source location type
Local
Client IP
80.189.203.166
Device full name
desktop-vr4qjfc
About this item
Item type
File
Object ID
C:\Users\MeganBowen\Desktop\Contoso Purchasing Permissions - Q1.docx
File extension
docx
File size
26 KB
Sha1
fd5ece6bff51012325b5720a2d007e4038
Sha256
6caeec7fa0464bcd179043dc2bc8f70e18
Close

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings

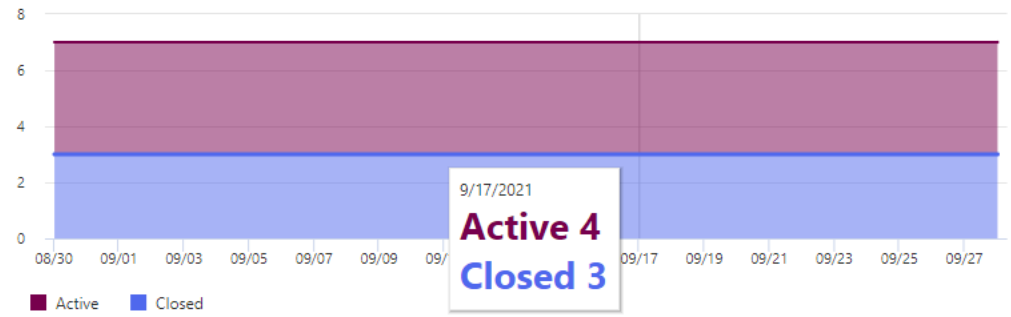
Insider risk management

Overview | Alerts | **Cases** | Policies | Users | Notice templates

Active cases **4**

Closed cases **3**

Cases over past 30 days



Statistics

Average time cases are active
7 months

Export

4 items Search Filter

Filters: Status: Active

Case name	Status	User	Time case opened	Total policy alerts	Content load progress	Content last updated	Case last updated	Last updated by
IRM007	Active	#Anonymi...	4 months ago	5	Complete	Aug 6, 2021 (UTC)	4 months ago	Bert Oz
IRM006	Active	#Anonymi...	7 months ago	5	Complete	May 25, 2021 (UTC)	7 months ago	Bert Oz
IRM005	Active	#Anonymi...	10 months ago	5	Complete	Sep 22, 2021 (UTC)	10 months ago	Bert Oz
IRM003	Active	#Anonymi...	10 months ago	7	Complete	Jun 24, 2021 (UTC)	10 months ago	Bert Oz

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings

IRM005

Active High 100 risk score

Resolve case | Case actions

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

About this case

Case information

Status
Active

Case created on
30/11/2020, 16:29:35

Microsoft Team
FailedToGet

User details

User's risk score
100/100

Email
#Anonymized#EAAAAFbaYeqm5r2Vq+Dz/TnqRj3bfjnaGzAX

Organization or department

Manager name

Manager email

Alerts

Policy matches	Status	Severity	Time detected
Departing Employee Theft	Confirmed	High	4 months ago
Disgruntled Users Data Leak	Confirmed	High	6 months ago
Corp. Terms Data Leak	Confirmed	High	10 months ago
PCI Data Leaks	Confirmed	High	a year ago

Content detected

Top labels

1.2K with sensitivity labels

Label	Number of activities
bdf2a4eb-b756-48f1-880c-b6f2...	985
Confidential	215
General	12

Top sensitive info types

7.1K with sensitive info types

Sensitive info type	Number of activities
Defence Terms	2850
Pharma Data	2450
Project Codenames	1821

Top Keywords

560 with keywords detected

Keyword	Number of instances
purchasing	211
crossbar	180
employee	169

Top SharePoint sites

15.9K with SharePoint sites

Site name	Number of activities
https://m365x764095.sharepoi...	15151
https://m365x764095.sharepoi...	781

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings

IRM005

Active | High | 100 risk score

Resolve case | Case actions

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

Export

5 items | Search | Filter

Filters: Time detected: 9/28/2011-9/28/2021

Alert	Status	Severity	Time detected
Departing Employee Theft	Confirmed	High	4 months ago
Disgruntled Users Data Leak	Confirmed	High	6 months ago
Corp. Terms Data Leak	Confirmed	High	10 months ago
PCI Data Leaks	Confirmed	High	a year ago
GDPR Data Leaks	Confirmed	High	a year ago

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings

IRM005

Active High 100 risk score

Resolve case | Case actions

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

Filter: Show: All user activity

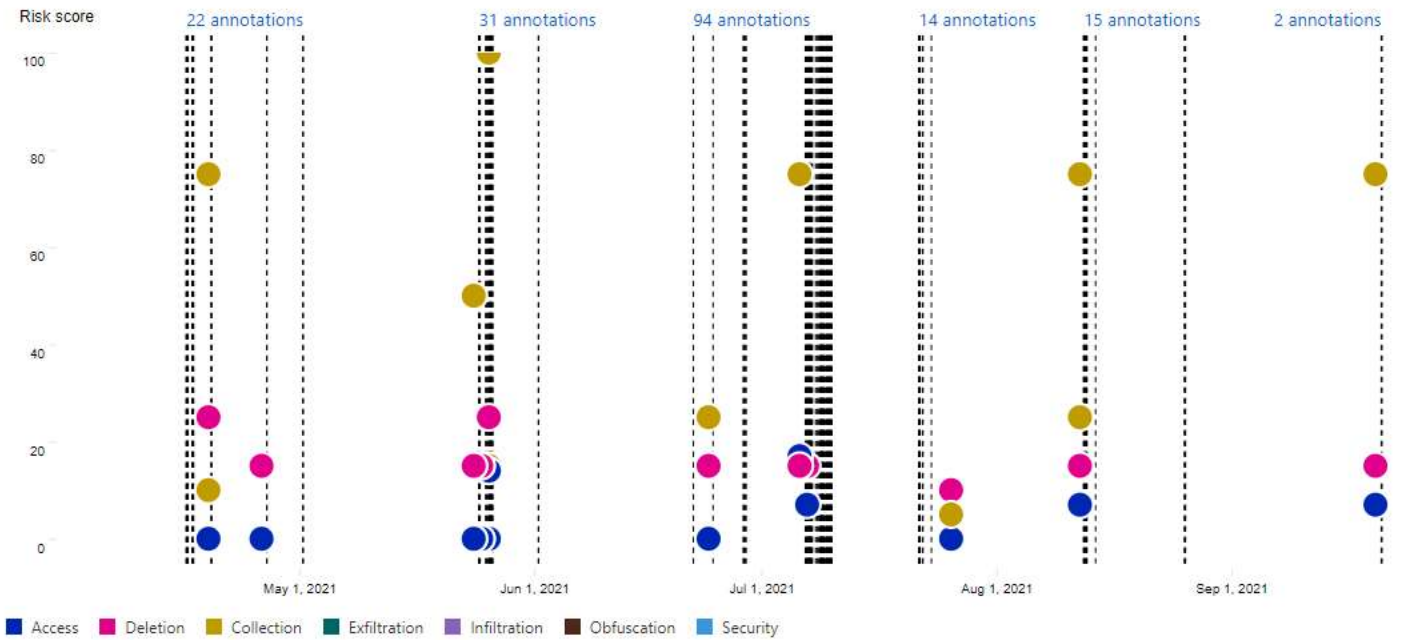
Sort by: Date occured

Access: Unusual volume of sensitive files read
Sep 20, 2021 (UTC) | Risk score: 7/100
51 events: Files were read
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential

Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine

Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied, including: Confidential, General (Explore content)

6 Months | 3 Months | 1 Month



Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings

IRM005

Active High 100 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 occured

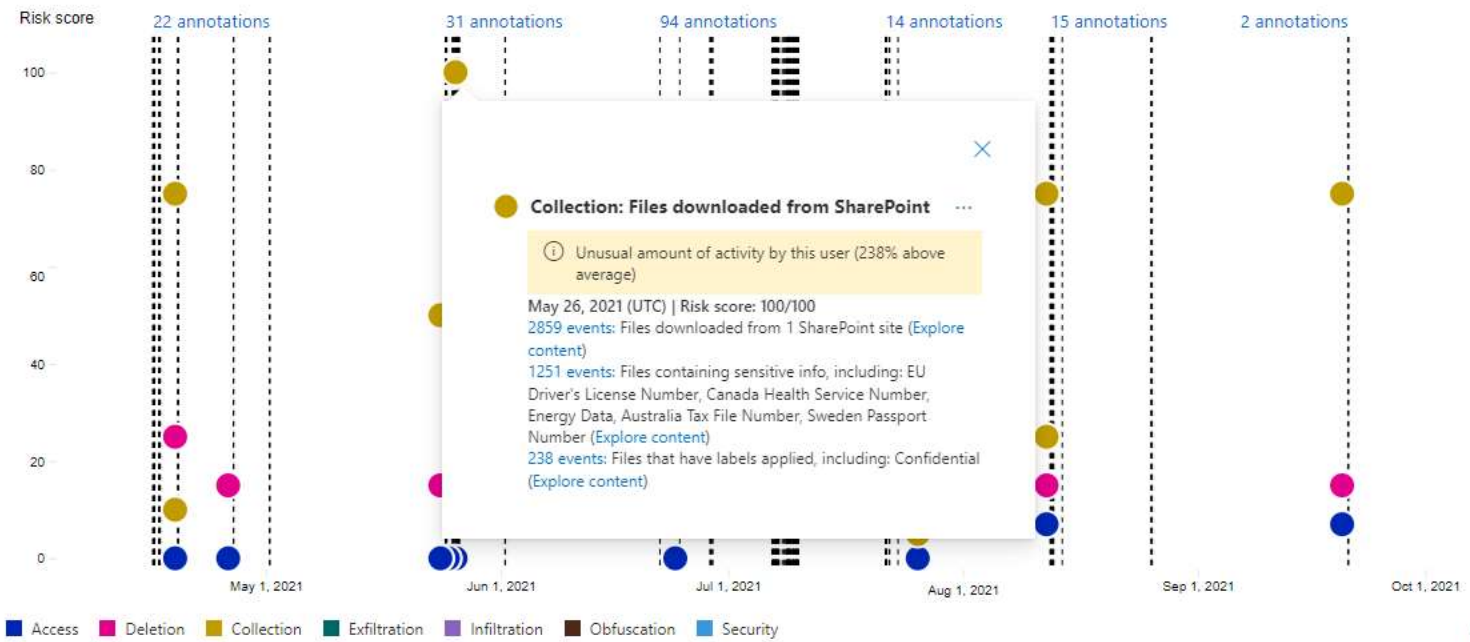
Access: Unusual volume of sensitive files read
Sep 20, 2021 (UTC) | Risk score: 7/100
51 events: Files were read
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential

Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine

Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied, including: Confidential, General (Explore content)

Collection: Sensitive files moved to new location
Unusual amount of activity by this user (130% above average)
Aug 12, 2021 (UTC) | Risk score: 25/100

6 Months | 3 Months | 1 Month



Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings

IRM005

Active High 100 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 occured

Access: Unusual volume of sensitive files read

Unusual amount of activity by this user (497% above average)

Jul 6, 2021 (UTC) | Risk score: 17/100
215 events: Files were read
191 events: Files containing sensitive info, including: Portugal Tax Identification Number, Ireland Passport Number, EU Driver's License Number, Romania Passport Number, U.S. Social Security Number (SSN)
35 events: Files that have labels applied, including: Confidential, General

Deletion: Files deleted

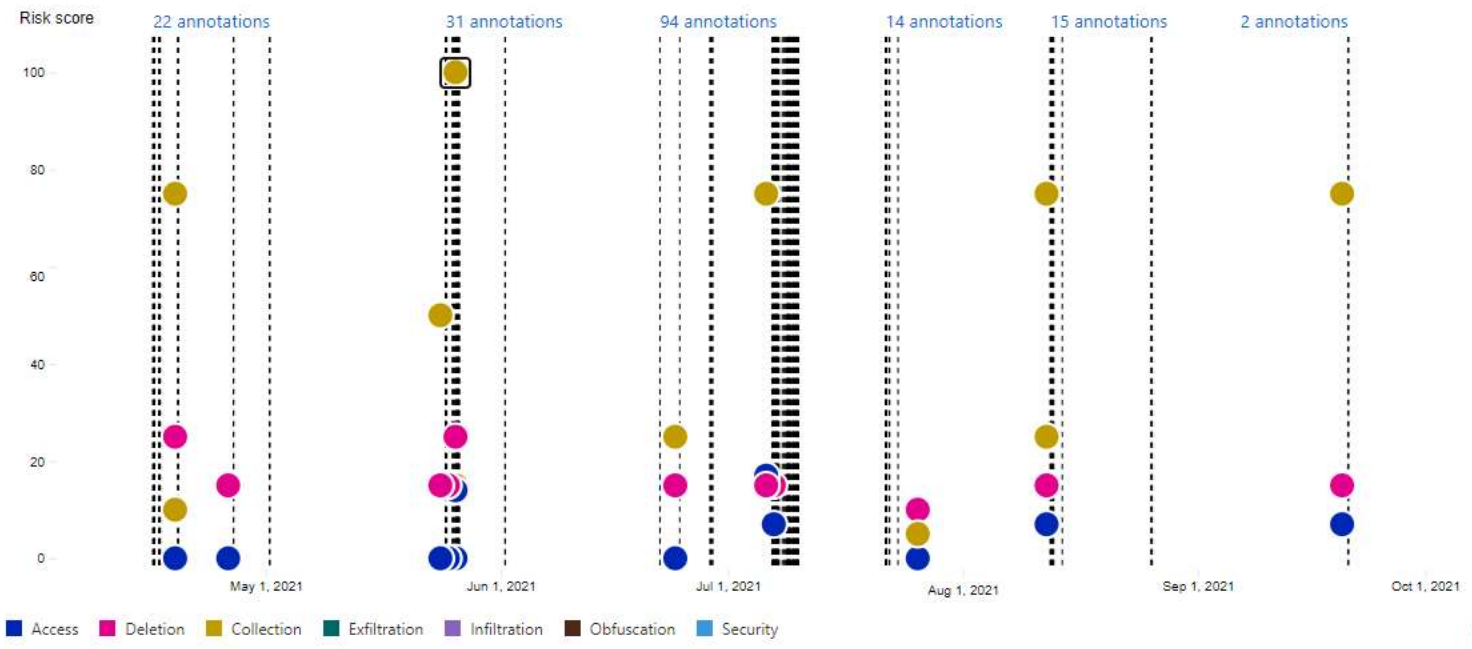
Jul 6, 2021 (UTC) | Risk score: 15/100
565 events: Files deleted from Windows 10 Machine

Collection: Files downloaded from SharePoint

Jul 6, 2021 (UTC) | Risk score: 75/100
476 events: Files downloaded from 2 SharePoint sites (Explore content)
459 events: Files containing sensitive info, including: Australia Bank Account Number, Project Codenames, EU Passport Number, Brazil National ID Card (RG), Hungarian Social Security Number (TAJ) (Explore content)
100 events: Files that have labels applied, including: Confidential, General (Explore content)

Collection: Sensitive files moved to new location

6 Months | 3 Months | 1 Month



Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings

IRM005

Active High 100 risk score

Resolve case | Case actions

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

Filter: Risk insight: Any

Sort by

Access: Unusual volume of sensitive files read
Sep 20, 2021 (UTC) | Risk score: 7/100
51 events: Files were read
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential

Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine

Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied,

Filter

Clear all | Filters

Happened (UTC): 1/28/2021-9/27/2021 | Activity: Any

Export | 40499 items | Restore default columns | Customize columns

Happened (UTC)	Activity	File name	Object ID	Workload	Item type
Sep 20, 2021 1:48 PM	Sensitive File read	050177.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050197.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050200.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050202.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050203.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050204.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050205.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050206.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050209.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050208.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File

Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources
Customize navigation

IRM005

Active | High | 100 risk score

Resolve case | Case actions

Case overview | Alerts | User activity | **Activity explorer** | Content explorer | Case notes | Contributors

Filter: Risk insight: Any

- Unusual activity
- Includes event with priority content
- Includes event with unallowed domain
- Sequence activities
- Cumulative exfiltration activities

Sort by

A
Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential

Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine

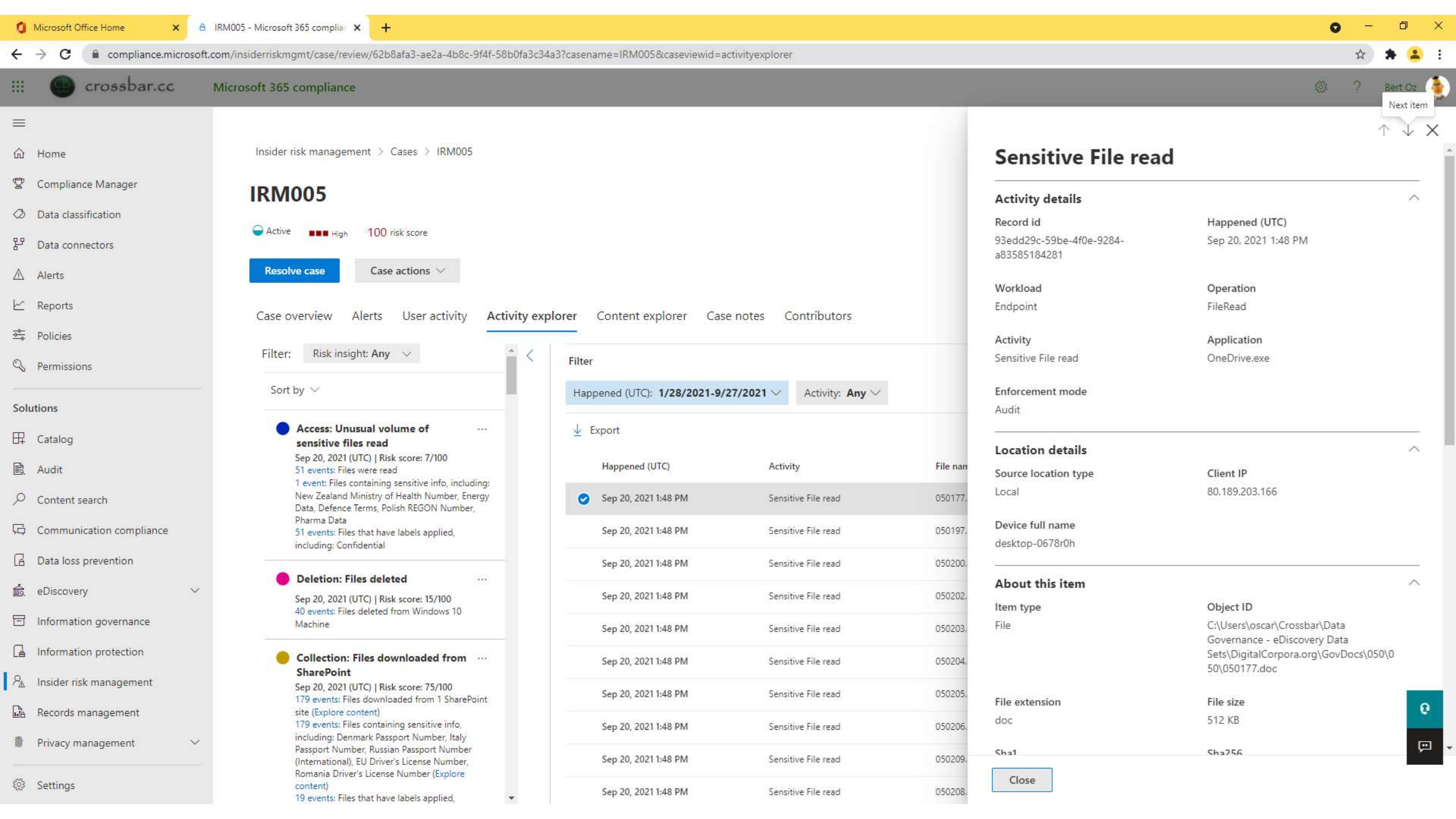
Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied,

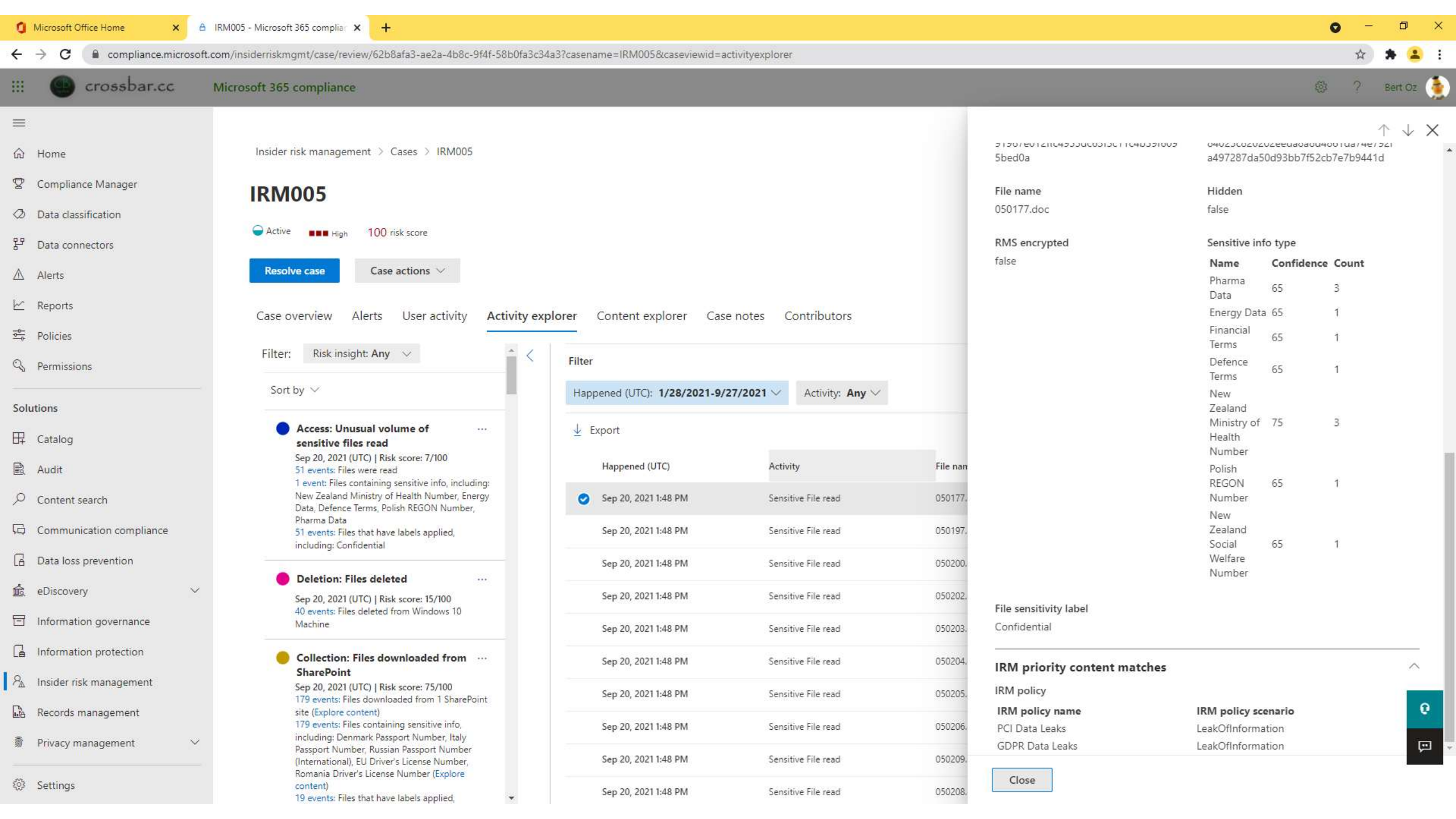
Filter | Clear all | Filters

Happened (UTC): 1/28/2021-9/27/2021 | Activity: Any

Export | 40499 items | Restore default columns | Customize columns

Happened (UTC)	Activity	File name	Object ID	Workload	Item type
Sep 20, 2021 1:48 PM	Sensitive File read	050177.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050197.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050200.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050202.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050203.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050204.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050205.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050206.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050209.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050208.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File


Microsoft Office Home
IRM005 - Microsoft 365 compliar
compliance.microsoft.com/insiderriskmgmt/case/review/62b8afa3-ae2a-4b8c-9f4f-58b0fa3c34a3?casename=IRM005&caseviewid=activityexplorer
crossbar.cc
Microsoft 365 compliance
Bert Oz
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings
Insider risk management > Cases > IRM005
IRM005
Active
High
100 risk score
Resolve case
Case actions
Case overview
Alerts
User activity
Activity explorer
Content explorer
Case notes
Contributors
Filter:
Risk insight: Any
Sort by
Access: Unusual volume of sensitive files read
Sep 20, 2021 (UTC) | Risk score: 7/100
51 events: Files were read
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential
Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine
Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied,
Filter
Happened (UTC): 1/28/2021-9/27/2021
Activity: Any
Export
Happened (UTC)
Activity
File nam
Sep 20, 2021 1:48 PM
Sensitive File read
050177.
Sep 20, 2021 1:48 PM
Sensitive File read
050197.
Sep 20, 2021 1:48 PM
Sensitive File read
050200.
Sep 20, 2021 1:48 PM
Sensitive File read
050202.
Sep 20, 2021 1:48 PM
Sensitive File read
050203.
Sep 20, 2021 1:48 PM
Sensitive File read
050204.
Sep 20, 2021 1:48 PM
Sensitive File read
050205.
Sep 20, 2021 1:48 PM
Sensitive File read
050206.
Sep 20, 2021 1:48 PM
Sensitive File read
050209.
Sep 20, 2021 1:48 PM
Sensitive File read
050208.
Next item
Sensitive File read
Activity details
Record id
93edd29c-59be-4f0e-9284-a83585184281
Happened (UTC)
Sep 20, 2021 1:48 PM
Workload
Endpoint
Operation
FileRead
Activity
Sensitive File read
Application
OneDrive.exe
Enforcement mode
Audit
Location details
Source location type
Local
Client IP
80.189.203.166
Device full name
desktop-0678r0h
About this item
Item type
File
Object ID
C:\Users\oscar\Crossbar\Data Governance - eDiscovery Data Sets\DigitalCorpora.org\GovDocs\050\050\050177.doc
File extension
doc
File size
512 KB
Sha1
Sha256
Close


Microsoft Office Home
IRM005 - Microsoft 365 compliar
compliance.microsoft.com/insiderriskmgmt/case/review/62b8afa3-ae2a-4b8c-9f4f-58b0fa3c34a3?casename=IRM005&caseviewid=activityexplorer
crossbar.cc
Microsoft 365 compliance
Bert Oz
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings
Insider risk management > Cases > IRM005
IRM005
Active
High
100 risk score
Resolve case
Case actions
Case overview
Alerts
User activity
Activity explorer
Content explorer
Case notes
Contributors
Filter:
Risk insight: Any
Sort by
Access: Unusual volume of sensitive files read
Sep 20, 2021 (UTC) | Risk score: 7/100
51 events: Files were read
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential
Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine
Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied,
Filter
Happened (UTC): 1/28/2021-9/27/2021
Activity: Any
Export
Happened (UTC)
Activity
File nam
Sep 20, 2021 1:48 PM
Sensitive File read
050177.
Sep 20, 2021 1:48 PM
Sensitive File read
050197.
Sep 20, 2021 1:48 PM
Sensitive File read
050200.
Sep 20, 2021 1:48 PM
Sensitive File read
050202.
Sep 20, 2021 1:48 PM
Sensitive File read
050203.
Sep 20, 2021 1:48 PM
Sensitive File read
050204.
Sep 20, 2021 1:48 PM
Sensitive File read
050205.
Sep 20, 2021 1:48 PM
Sensitive File read
050206.
Sep 20, 2021 1:48 PM
Sensitive File read
050209.
Sep 20, 2021 1:48 PM
Sensitive File read
050208.
5bed0a
a497287da50d93bb7f52cb7e7b9441d
File name
050177.doc
Hidden
false
RMS encrypted
false
Sensitive info type
Name
Confidence
Count
Pharma Data
65
3
Energy Data
65
1
Financial Terms
65
1
Defence Terms
65
1
New Zealand Ministry of Health Number
75
3
Polish REGON Number
65
1
New Zealand Social Welfare Number
65
1
File sensitivity label
Confidential
IRM priority content matches
IRM policy
IRM policy name
IRM policy scenario
PCI Data Leaks
LeakOfInformation
GDPR Data Leaks
LeakOfInformation
Close

Microsoft Office Home | IRM005 - Microsoft 365 compliance

compliance.microsoft.com/insiderriskmgmt/case/review/62b8afa3-ae2a-4b8c-9f4f-58b0fa3c34a3?casename=IRM005&caseviewid=contentexplorer

crossbar.cc | Microsoft 365 compliance | Bert Oz

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions

Solutions

- Catalog
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery
- Information governance
- Information protection
- Insider risk management
- Records management
- Privacy management

- Settings
- More resources
- Customize navigation

Insider risk management > Cases > IRM005

IRM005

Active | High | 100 risk score

Resolve case | Case actions

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

Examine the emails and files captured by the policies included in this case. Learn more

Last Updated Sep 22, 2021 (UTC)

Filter | Reset | Filters

Group | Customize columns | Export all file names | 1 of 114790 selected

Subject/Title	Date (UTC)	File class	Sender/Author	Recipients	Sensitivity Labels	Sensitive info types
056172.ppt		Document				
063500.ppt		Document				
088769.doc		Document				
		Document				
096031.ppt		Document				
098228.xls	Oct 30, 2003 11:35 ...	Document	Oscar Grouch			
062960.ppt		Document				
067005.ppt		Document				
060150.ppt		Document				
085268.ppt		Document				
074251.ppt		Document				
125559.doc		Document				
079880.ppt		Document				
075454.ppt		Document				
070369.ppt		Document				

098228.xls

Source

Excel 098228 - View-only | Search | bert@crossbar.cc

File | Home | Insert | Draw | Page Layout | Formulas | Data | Review | View | Search

N38 | agreed

Key:

Categories: 1 - Job complete or complete by end of shutdown, 2 - Job in process, 3 - Job just starting, 4 - Jobs approved but not started, 5 - Jobs pending revie

System: B=Booster; CKM=CKM; EC=Electron Cooling; E907=Experiment 907; FMI=FMI; Gen=BD General Use; L=Linac; MB=MiniBooNE; NM=NuMI; P=P-bar;

Job Number: TD Number for Tracking Jobs

Priority: (Determined by BD) 1=Impacts BD Schedule or No Spare; 2=Does Not Impact BD Schedule; 3=Fill-in Work.

Beams Division Tasks as of 14-Oct-2003

Category	System	Job No.	Task Name	Scope of Work	Priority	TD Contact	BD Contact	Units Req'd	Units Comp	Project	Tas
			cooling								
5	P	0223	Additional LQD quadrupole	Fabricate one LQD quadrupole to		Harding	D Vander				

Joblist | Closed Jobs

Workbook Statistics | Give Feedback to Microsoft | 100%

Microsoft Office Home | IRM005 - Microsoft 365 compliance

compliance.microsoft.com/insiderriskmgmt/case/review/62b8afa3-ae2a-4b8c-9f4f-58b0fa3c34a3?casename=IRM005&caseviewid=contentexplorer

crossbar.cc | Microsoft 365 compliance

Bert Oz

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources
Customize navigation

Insider risk management > Cases > IRM005

IRM005

Active | High | 100 risk score

Resolve case | Case actions

Case overview | Alerts | User activity | Activity explorer | **Content explorer** | Case notes | Contributors

Examine the emails and files captured by the policies included in this case. Learn more

Filter | Reset | Filters

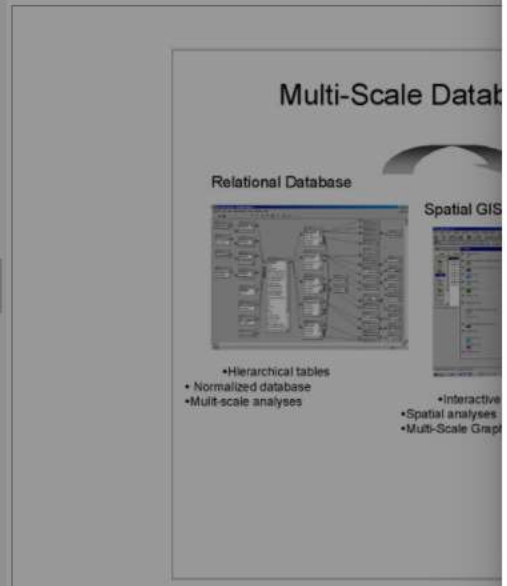
Sender: Any

Group | Customize columns | Export all file names | 1 of 114790 selected

Subject/Title	Date (UTC)	File class	Sender/Author	Recipients	Sensitivity Labels	Sensitive info types
065485.ppt		Document				
122346.ppt		Document				
085267.ppt		Document				
082757.ppt		Document				
060297.ppt		Document				
124569.doc	Jan 9, 2006 6:27 PM	Document	Oscar Grouch			
124569.doc	Jul 7, 2005 5:28 PM	Document				
124569.doc	Jul 7, 2005 5:24 PM	Document				
124569.doc		Document				
124569.doc		Document				
124569.doc	Jul 7, 2005 5:16 PM	Document				
124569.doc		Document				
124569.doc		Document				

image5.jpg

Source



Filter

You can customize the filter, choose filter sets, and save them as the default filter.

- [ ] Bcc
- [ ] CC
- [ ] Compliance label
- [ ] Content source
- [ ] Created Time (UTC)
- [ ] Date (UTC)
- [ ] File Extension
- [ ] Has Attachment
- [ ] Is Email Attachment
- [ ] Is Embedded Document
- [ ] Is Inline Attachment
- [ ] Last Modified Date (UTC)
- [ ] Recipient Domains
- [ ] Recipients
- [x] Sender
- [ ] Sender domain
- [ ] Sender/Author
- [ ] Source
- [ ] Subject/Title
- [ ] To
- [ ] User activity events

Done

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings

IRM005

Active High 100 risk score

Resolve case | Case actions

Case overview | Alerts | User activity | Activity explorer | Content explorer | **Case notes** | Contributors

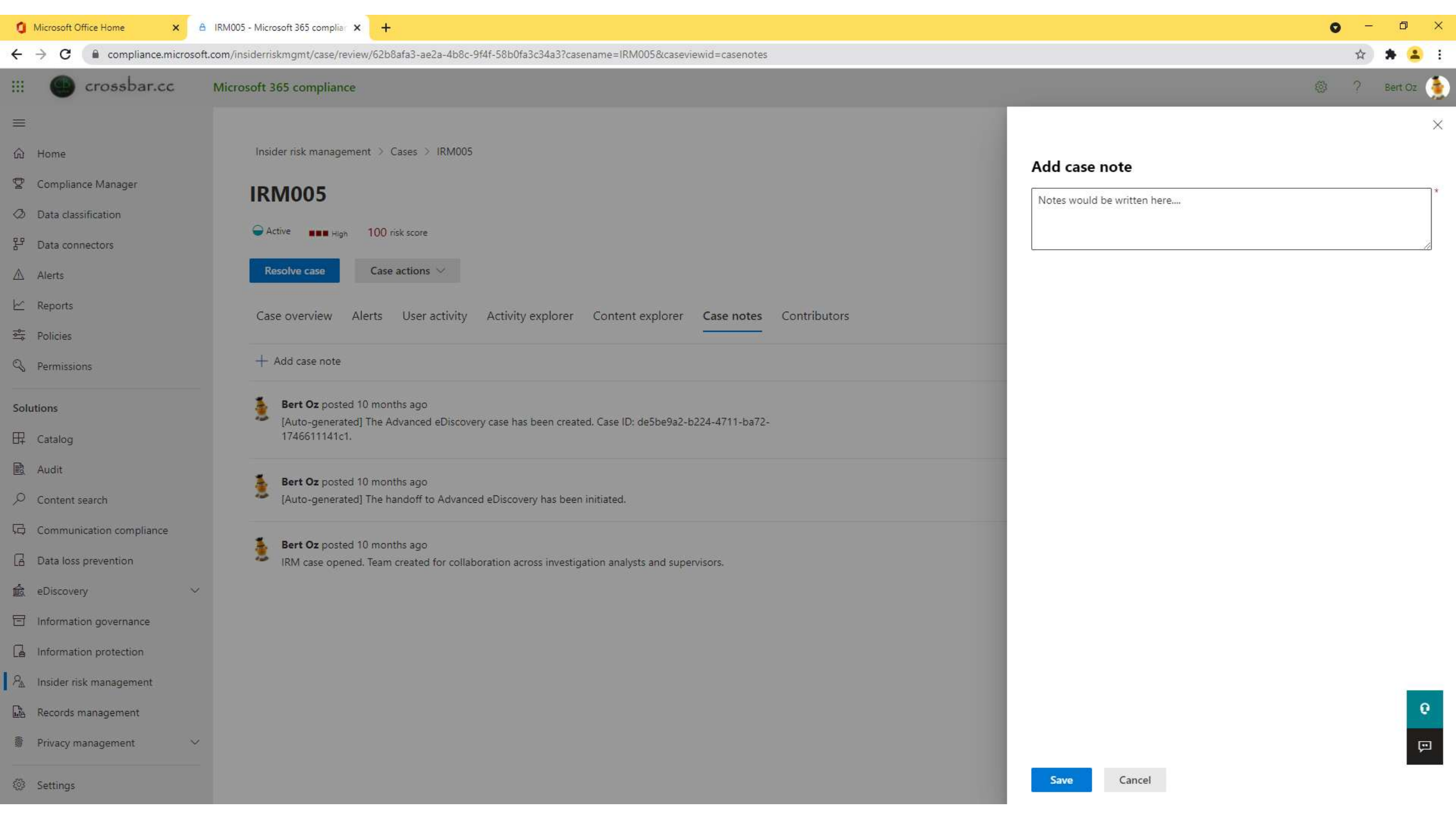
Add case note

3 items Search

Bert Oz posted 10 months ago
[Auto-generated] The Advanced eDiscovery case has been created. Case ID: de5be9a2-b224-4711-ba72-1746611141c1.

Bert Oz posted 10 months ago
[Auto-generated] The handoff to Advanced eDiscovery has been initiated.

Bert Oz posted 10 months ago
IRM case opened. Team created for collaboration across investigation analysts and supervisors.


Microsoft Office Home
IRM005 - Microsoft 365 compliar
compliance.microsoft.com/insiderriskmgmt/case/review/62b8afa3-ae2a-4b8c-9f4f-58b0fa3c34a3?casename=IRM005&caseviewid=casenotes
crossbar.cc
Microsoft 365 compliance
Bert Oz
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings
Insider risk management > Cases > IRM005
IRM005
Active
High
100 risk score
Resolve case
Case actions
Case overview
Alerts
User activity
Activity explorer
Content explorer
Case notes
Contributors
Add case note
Bert Oz posted 10 months ago
[Auto-generated] The Advanced eDiscovery case has been created. Case ID: de5be9a2-b224-4711-ba72-1746611141c1.
Bert Oz posted 10 months ago
[Auto-generated] The handoff to Advanced eDiscovery has been initiated.
Bert Oz posted 10 months ago
IRM case opened. Team created for collaboration across investigation analysts and supervisors.
Add case note
Notes would be written here....
Save
Cancel

Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources

Customize navigation

IRM005

Active High 100 risk score

Resolve case | Case actions

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

Add contributor | Copy case link | Refresh | 4 items

Name	Email
Bert Oz	bert@crossbar.cc
Megan Bowen	MeganB@crossbar.cc
Insider Risk Management	
Insider Risk Management Admins	

Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources
Customize navigation

IRM005

Active High 100 risk score

Resolve case | Case actions

- Send email notice
- Escalate for investigation
- Automate
- Share
- Create Microsoft team
- Manage pseudonymize
- Learn more about insider risk cases

Case overview | lorer | Content explorer | Case notes | Contributors

Filter: Risk insig

Sort by

Access: Unu... sensitive file
Sep 20, 2021 (U...
51 events: Files...
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential

Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine

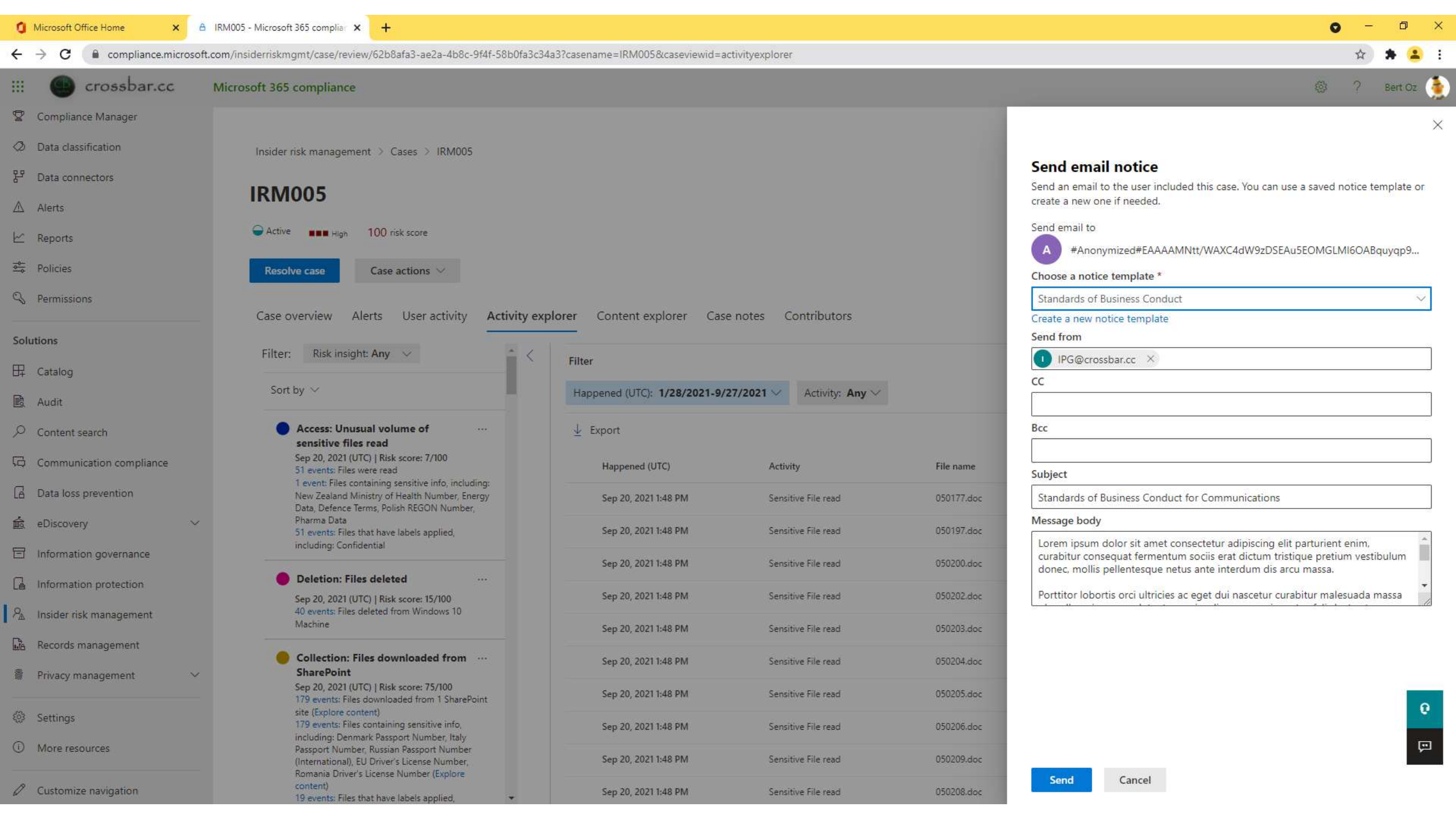
Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied,

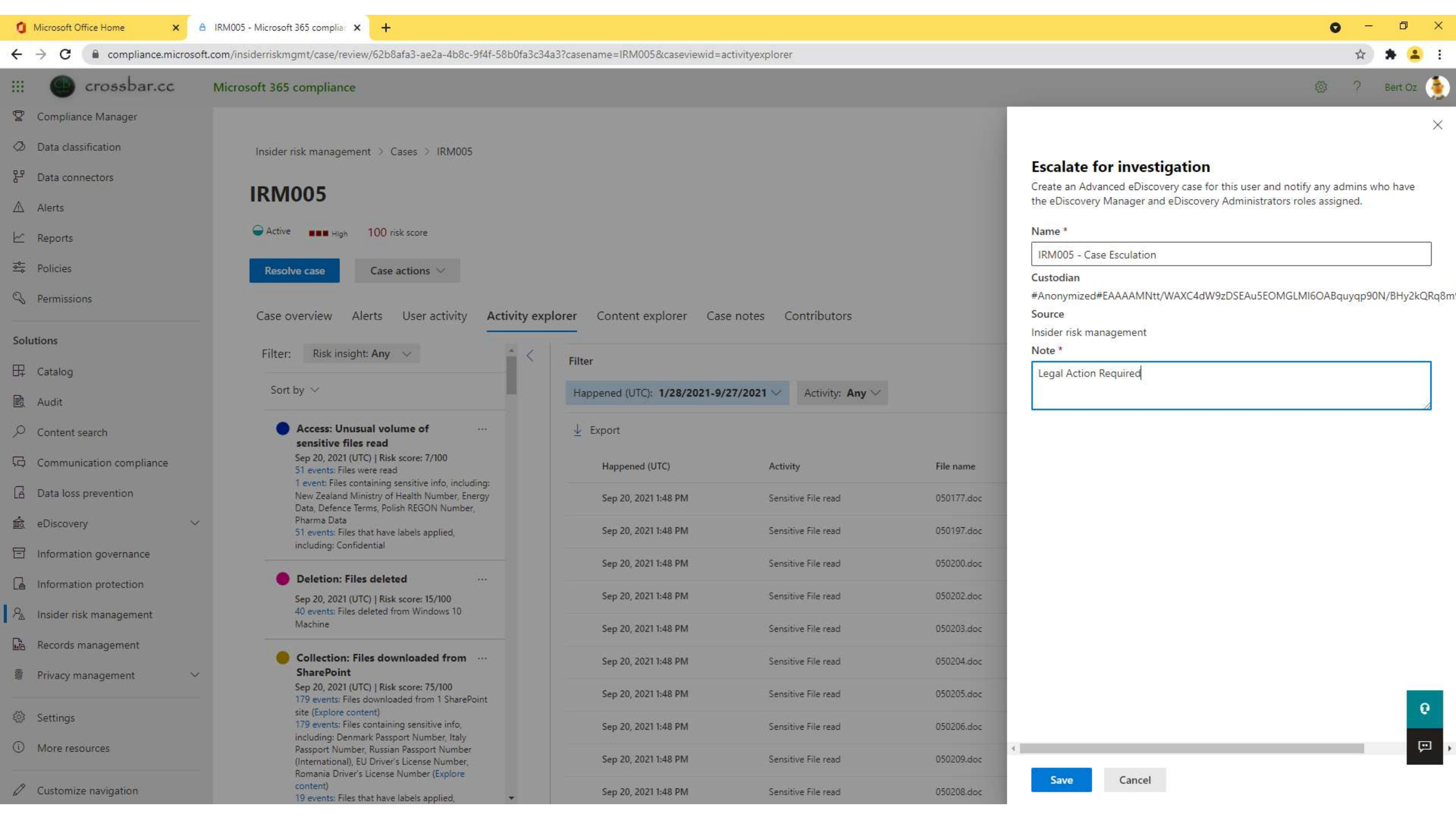
Filter | Clear all | Filters

Happened (UTC): **1/28/2021-9/27/2021** | Activity: **Any**

Export | 40499 items | Restore default columns | Customize columns

Happened (UTC)	Activity	File name	Object ID	Workload	Item type
Sep 20, 2021 1:48 PM	Sensitive File read	050177.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050197.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050200.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050202.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050203.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050204.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050205.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050206.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050209.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050208.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File


Microsoft Office Home
IRM005 - Microsoft 365 compliar
compliance.microsoft.com/insiderriskmgmt/case/review/62b8afa3-ae2a-4b8c-9f4f-58b0fa3c34a3?casename=IRM005&caseviewid=activityexplorer
crossbar.cc
Microsoft 365 compliance
Bert Oz
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings
More resources
Customize navigation
Insider risk management > Cases > IRM005
IRM005
Active
High
100 risk score
Resolve case
Case actions
Case overview
Alerts
User activity
Activity explorer
Content explorer
Case notes
Contributors
Filter:
Risk insight: Any
Sort by
Access: Unusual volume of sensitive files read
Sep 20, 2021 (UTC) | Risk score: 7/100
51 events: Files were read
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential
Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine
Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied,
Filter
Happened (UTC): 1/28/2021-9/27/2021
Activity: Any
Export
Happened (UTC)
Activity
File name
Sep 20, 2021 1:48 PM
Sensitive File read
050177.doc
050197.doc
050200.doc
050202.doc
050203.doc
050204.doc
050205.doc
050206.doc
050209.doc
050208.doc
Send email notice
Send an email to the user included this case. You can use a saved notice template or create a new one if needed.
Send email to
#Anonymized#EAAAAMNtt/WAXC4dW9zDSEAu5EOMGLMI6OABquyqp9...
Choose a notice template *
Standards of Business Conduct
Create a new notice template
Send from
IPG@crossbar.cc
CC
Bcc
Subject
Standards of Business Conduct for Communications
Message body
Lorem ipsum dolor sit amet consectetur adipiscing elit parturient enim, curabitur consequat fermentum sociis erat dictum tristique pretium vestibulum donec, mollis pellentesque netus ante interdum dis arcu massa.
Porttitor lobortis orci ultricies ac eget dui nascetur curabitur malesuada massa
Send
Cancel


Microsoft Office Home
IRM005 - Microsoft 365 compliar
compliance.microsoft.com/insiderriskmgmt/case/review/62b8afa3-ae2a-4b8c-9f4f-58b0fa3c34a3?casename=IRM005&caseviewid=activityexplorer
crossbar.cc
Microsoft 365 compliance
Bert Oz
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings
More resources
Customize navigation
Insider risk management > Cases > IRM005
IRM005
Active
High
100 risk score
Resolve case
Case actions
Case overview
Alerts
User activity
Activity explorer
Content explorer
Case notes
Contributors
Filter:
Risk insight: Any
Sort by
Access: Unusual volume of sensitive files read
Sep 20, 2021 (UTC) | Risk score: 7/100
51 events: Files were read
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential
Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine
Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied,
Filter
Happened (UTC): 1/28/2021-9/27/2021
Activity: Any
Export
Happened (UTC)
Activity
File name
Sep 20, 2021 1:48 PM
Sensitive File read
050177.doc
050197.doc
050200.doc
050202.doc
050203.doc
050204.doc
050205.doc
050206.doc
050209.doc
050208.doc
Escalate for investigation
Create an Advanced eDiscovery case for this user and notify any admins who have the eDiscovery Manager and eDiscovery Administrators roles assigned.
Name *
IRM005 - Case Esculation
Custodian
#Anonymized#EAAAAMNtt/WAXC4dW9zDSEAu5EOMGLMI6OABquyqp90N/BHy2kQRq8m
Source
Insider risk management
Note *
Legal Action Required
Save
Cancel

Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources
Customize navigation

IRM005

Active High 100 risk score

Resolve case | Case actions

- Send email notice
- Escalate for investigation
- Automate
  - Add a calendar reminder to follow-up on an insider risk case
  - Notify manager of insider risk alerts for user
  - Request info from HR or business about a user in an insider risk case
  - Manage Power Automate flows
- Share
- Create Microsoft team
- Manage pseudonymize
- Learn more about insider risk cases

Case overview | lorer | Content explorer | Case notes | Contributors

Filter: Risk insig | Clear all | Filters

Sort by

Access: Unu... sensitive fil...
Sep 20, 2021 (U...
51 events: Files...
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential

Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine

Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied,

40499 items | Restore default columns | Customize columns

Happened (UTC)	Activity	File name	Object ID	Workload	Item type
Sep 20, 2021 1:48 PM	Sensitive File read	050177.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050197.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050200.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050202.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050203.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050204.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050205.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050206.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050209.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050208.doc	C:\Users\oscar\Crossbar\Data Govern...	Endpoint	File

Microsoft Office Home | IRM005 - Microsoft 365 compliance

compliance.microsoft.com/insiderriskmgmt/case/review/62b8afa3-ae2a-4b8c-9f4f-58b0fa3c34a3?casename=IRM005&caseviewid=activityexplorer

crossbar.cc | Microsoft 365 compliance | Bert Oz

- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions

Solutions

- Catalog
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery
- Information governance
- Information protection
- Insider risk management
- Records management
- Privacy management

- Settings
- More resources
- Customize navigation

Insider risk management > Cases > IRM005

IRM005

Active | High | 100 risk score

Resolve case | Case actions

- Send email notice
- Escalate for investigation
- Automate
- Share
- Create Microsoft team
- Manage pseudonymize
- Learn more about insider risk cases

Case overview | Timeline explorer | Content explorer | Case notes | Contributors

Filter: Risk insig

Sort by

Access: Unu… sensitive file
Sep 20, 2021 (U…
51 events: Files…
1 event: Files containing sensitive info, including: New Zealand Ministry of Health Number, Energy Data, Defence Terms, Polish REGON Number, Pharma Data
51 events: Files that have labels applied, including: Confidential

Deletion: Files deleted
Sep 20, 2021 (UTC) | Risk score: 15/100
40 events: Files deleted from Windows 10 Machine

Collection: Files downloaded from SharePoint
Sep 20, 2021 (UTC) | Risk score: 75/100
179 events: Files downloaded from 1 SharePoint site (Explore content)
179 events: Files containing sensitive info, including: Denmark Passport Number, Italy Passport Number, Russian Passport Number (International), EU Driver's License Number, Romania Driver's License Number (Explore content)
19 events: Files that have labels applied,

Filter | Clear all | Filters

Happened (UTC): 1/28/2021-9/27/2021 | Activity: Any

Export | 40499 items | Restore default columns | Customize columns

Happened (UTC)	Activity	File name	Object ID	Workload	Item type
Sep 20, 2021 1:48 PM	Sensitive File read	050177.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050197.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050200.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050202.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050203.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050204.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050205.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050206.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050209.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File
Sep 20, 2021 1:48 PM	Sensitive File read	050208.doc	C:\Users\oscar\Crossbar\Data Govern…	Endpoint	File

Who’s watching the watchers?

Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources

Customize navigation

Insider risk audit log

Review activity in this log to stay informed about the actions that were taken on insider risk features. Activity here was performed by users who are assigned to one or more insider risk management roles, and you can filter on activity related to settings, policies, alerts, cases, and more. Learn more about the insider risk audit log

Export Refresh 100 items Search Customize columns

Filter Reset Filters

Category: **Any** Activity performed by: **Any** Date range: **Any**

Activity	Category	Activity performed by	Date
Viewed case notes in "IRM005"	Cases	Bert Oz	Sep 28, 2021 3:41 PM
Viewed case notes in "IRM005"	Cases	Bert Oz	Sep 28, 2021 3:38 PM
Viewed user activity in "IRM005"	Cases	Bert Oz	Sep 28, 2021 3:30 PM
Viewed case alerts in "IRM005"	Cases	Bert Oz	Sep 28, 2021 3:30 PM
Viewed user activity in "IRM005"	Cases	Bert Oz	Sep 28, 2021 3:30 PM
Viewed case alerts in "IRM005"	Cases	Bert Oz	Sep 28, 2021 3:29 PM
Viewed user activity in "IRM007"	Cases	Bert Oz	Sep 16, 2021 2:55 PM
Viewed user profile in "PCI Data Leaks"	Alerts	Bert Oz	Sep 16, 2021 2:53 PM
Viewed user activity in "IRM007"	Cases	Bert Oz	Sep 16, 2021 11:27 AM
Viewed user activity in "IRM006"	Cases	Bert Oz	Sep 16, 2021 11:26 AM
Viewed user profile in "PCI Data Leaks"	Alerts	Bert Oz	Sep 16, 2021 11:25 AM