water
IT Security & Defense

# Data Security - Mythbusting

## Why your biggest data threat is AI-ready inside


Oliver Sahlmann
Solution Lead Data Security Consulting | water



Alex Benoit
CEO | water


Microsoft REGIONAL DIRECTOR

MVP


SwissMicrosoft
SECURITY SUMMIT


scopewyse
we are what's next


Ontinue


INGRAM
MICRO


EPIC FUSION
BRING IT ALL TOGETHER


Microsoft


water
IT Security & Defense


GRABX


Swiss Post
Cybersecurity


techtask


iC CONSULT


Mediawerk

# The world we live in

water

## Data security incidents can happen anytime, anywhere






Sources:
https://cyberscoop.com/hsbc-data-breach-credential-stuffing/
https://ogletree.com/insights-resources/blog-posts/fbi-warns-of-hidden-threats-in-remote-hiring-are-north-korean-hackers-your-newest-employees/
https://blog.kraken.com/news/how-we-identified-a-north-korean-hacker
https://www.scworld.com/news/tesla-says-former-employees-leaked-thousands-of-personal-records-to-german-news-outlet?utm_source=chatgpt.com

# Data exfiltration tactics

water

The threat is already inside – and plugged in

## External risks

- Social Engineering
- Credential theft
- Phishing

## Internal risks

- Former employees
- Inattentive user
- Buy a guy

## Channels

- USB
- Cloud upload
- Email
- Insecure devices

# TOP 6 Data Security Myths

water

## Assumptions that put your data at risk

MYTH 1

You need to know all your data to start with the data security implementation

MYTH 2

Labeling is the answer to everything

MYTH 3

DLP destroys user productivity and kicks off the shit storm

MYTH 4

I trust my employees, I do not need insider risk

MYTH 5

SOC does not need data security insights

MYTH 6

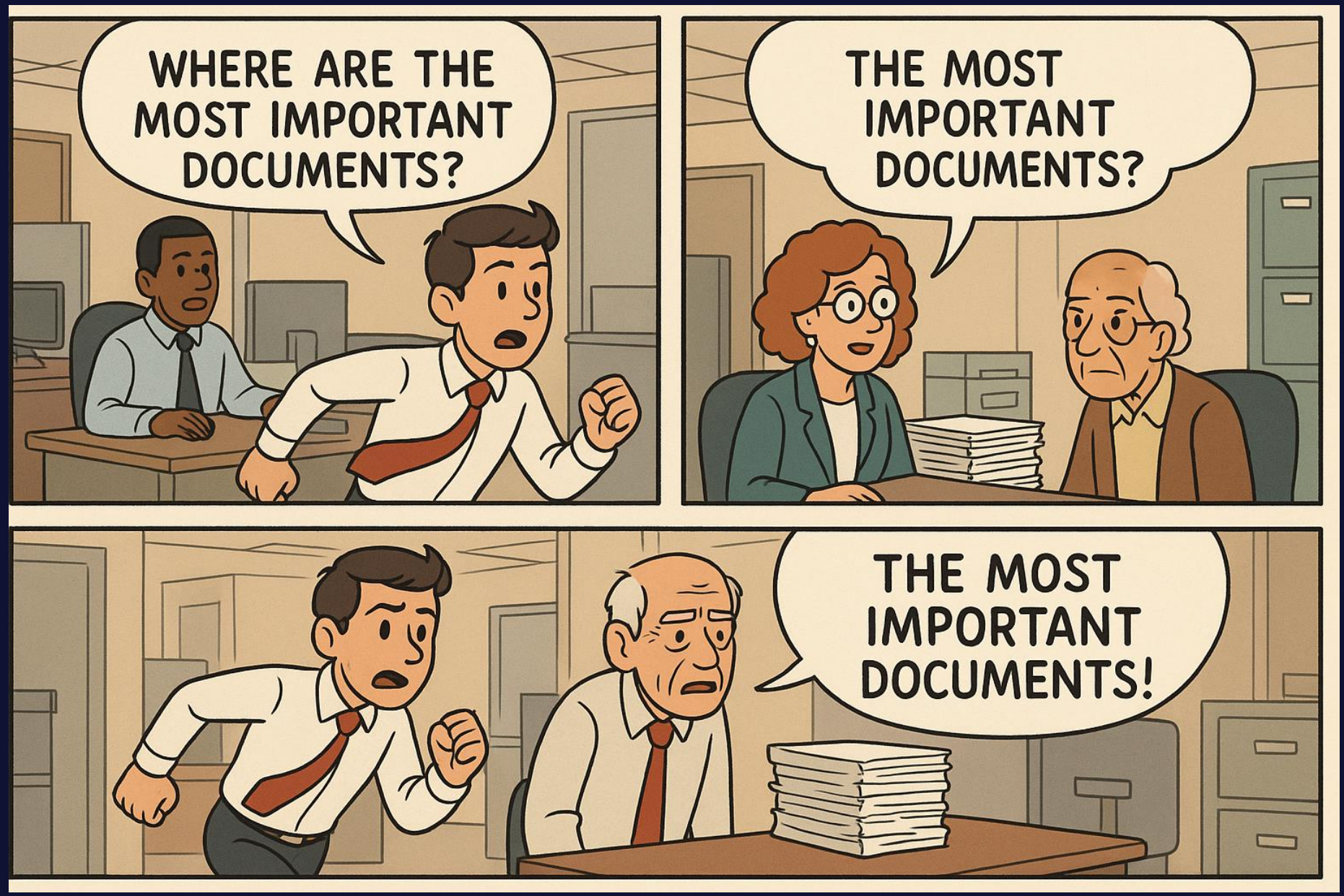
My business will hate the IT for implementing data security

water

MYTH 1

# You need to know all your data to start with the Data Security Implementation

water


WHERE ARE THE MOST IMPORTANT DOCUMENTS?
THE MOST IMPORTANT DOCUMENTS?
THE MOST IMPORTANT DOCUMENTS!

# Let’s focus on what’s really matter

Protect every information if you don’t know it

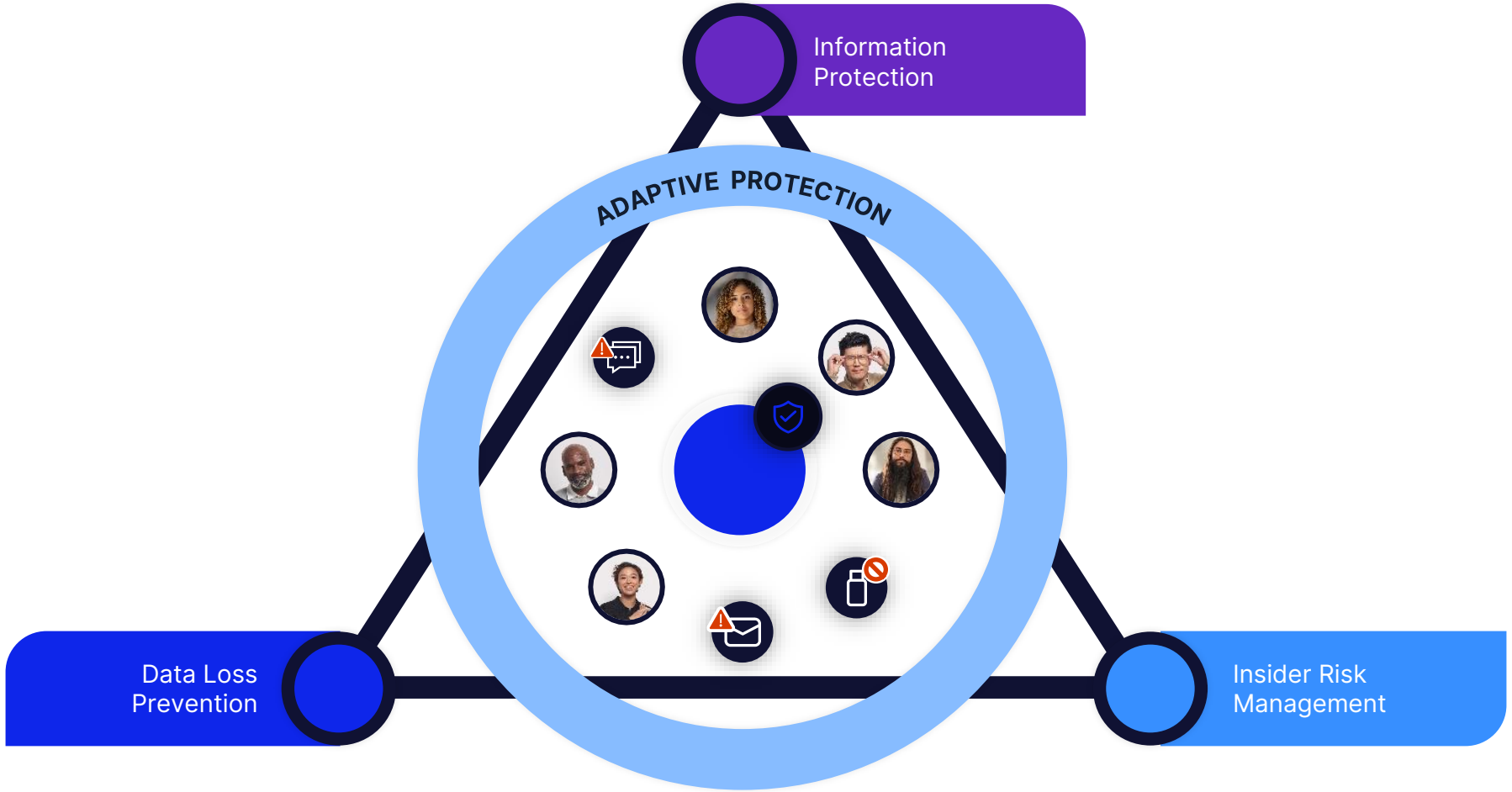

Build a data security MVP

- 3-layer label set
- Control the data flow
- Utilize signals and insights into your strategy

Pareto principle with reasonable default

# Microsoft Data Security toolbox

## The whole is greater than the sum of the parts



water

MYTH 1

# You need to know all your data to start with the Data Security Implementation

BUSTED

MYTH 1

# You need to kn all your data to start with th Data Security Implementation

BUSTED

What if I change my mind on your company data?

- [x] Every Information is valuable
- [x] Share it intentionally

Key Recommendations:

- Move from base to edge – Build your MVP for baseline data protection and iterate through your edge cases based on real use cases

MYTH 2

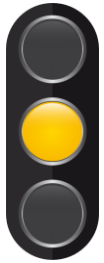
# Labeling is the answer to everything


water

# Traffice light : Make your label taxonomy simple

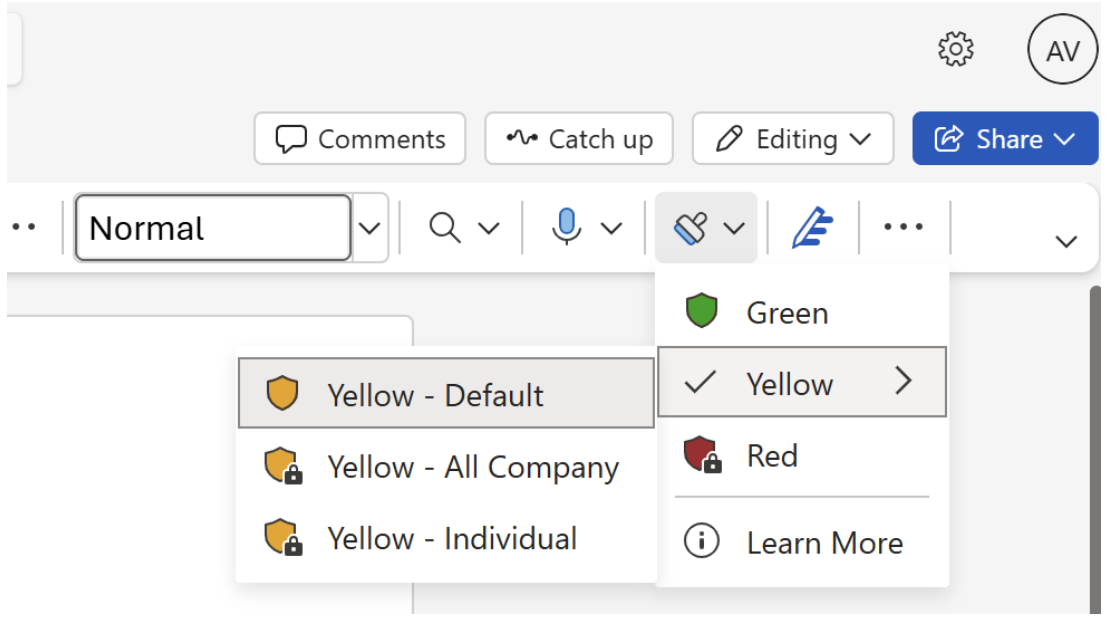
## MVP Label Configuration

Green – No protection, no restrictions



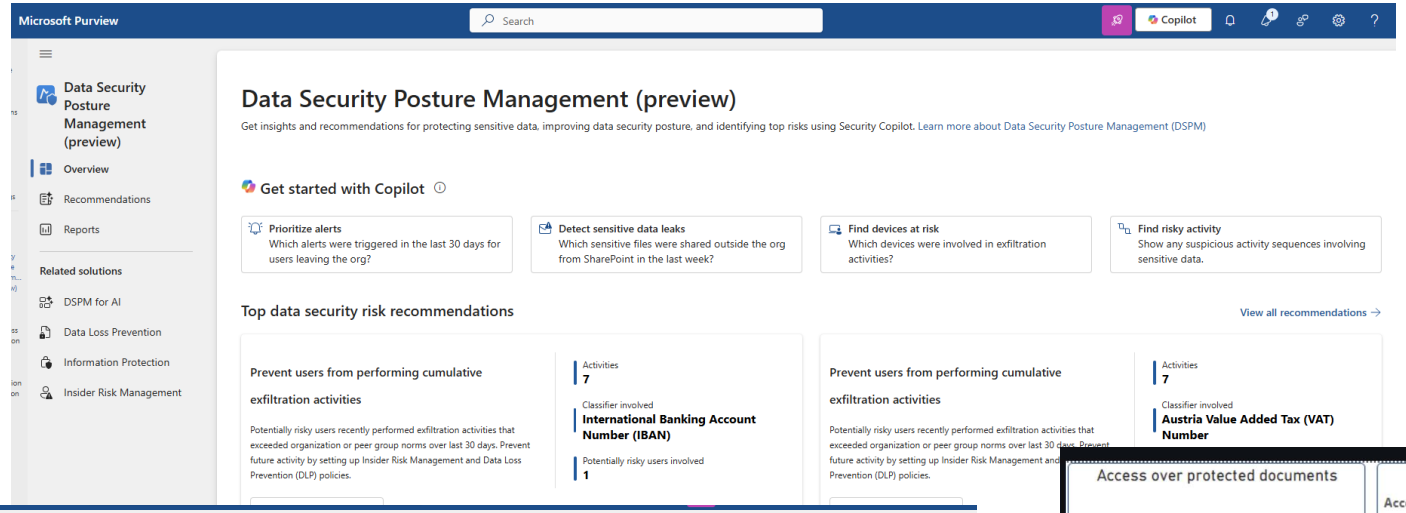
Yellow – Everything you do not know, it should be kept in your company in the first place, but can be shared with good reason

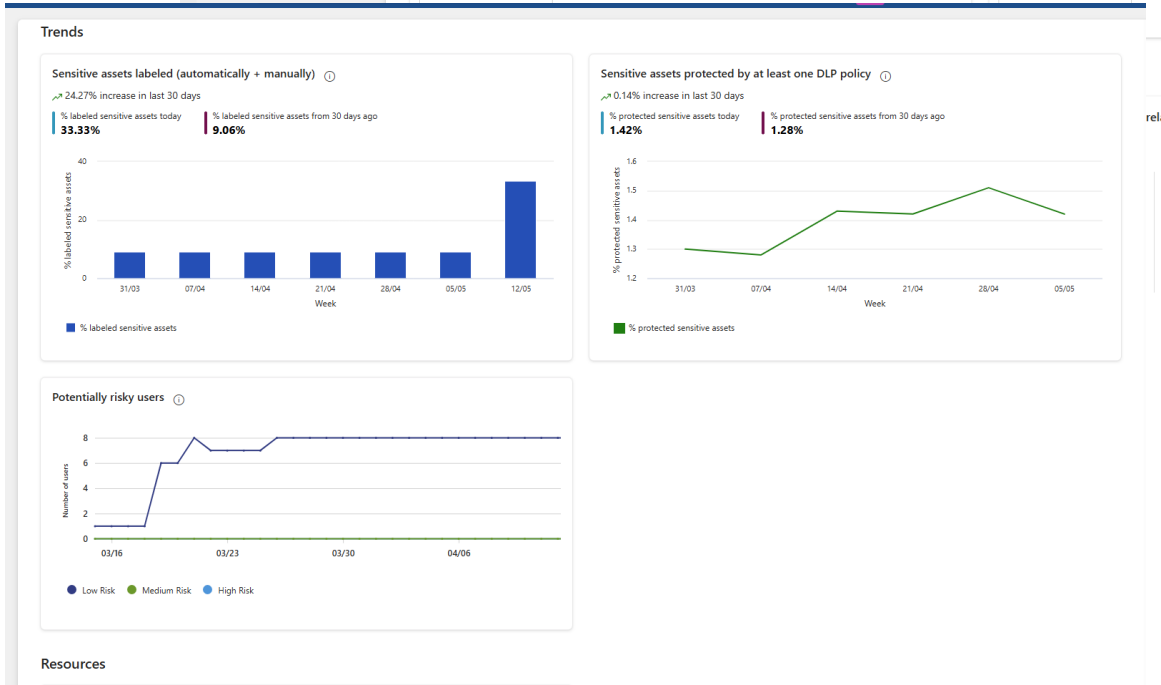
Red – Critical data you either already know and can be addressed by special use cases or a decision of your user to protect it further – Encryption and DLP is need to protected it

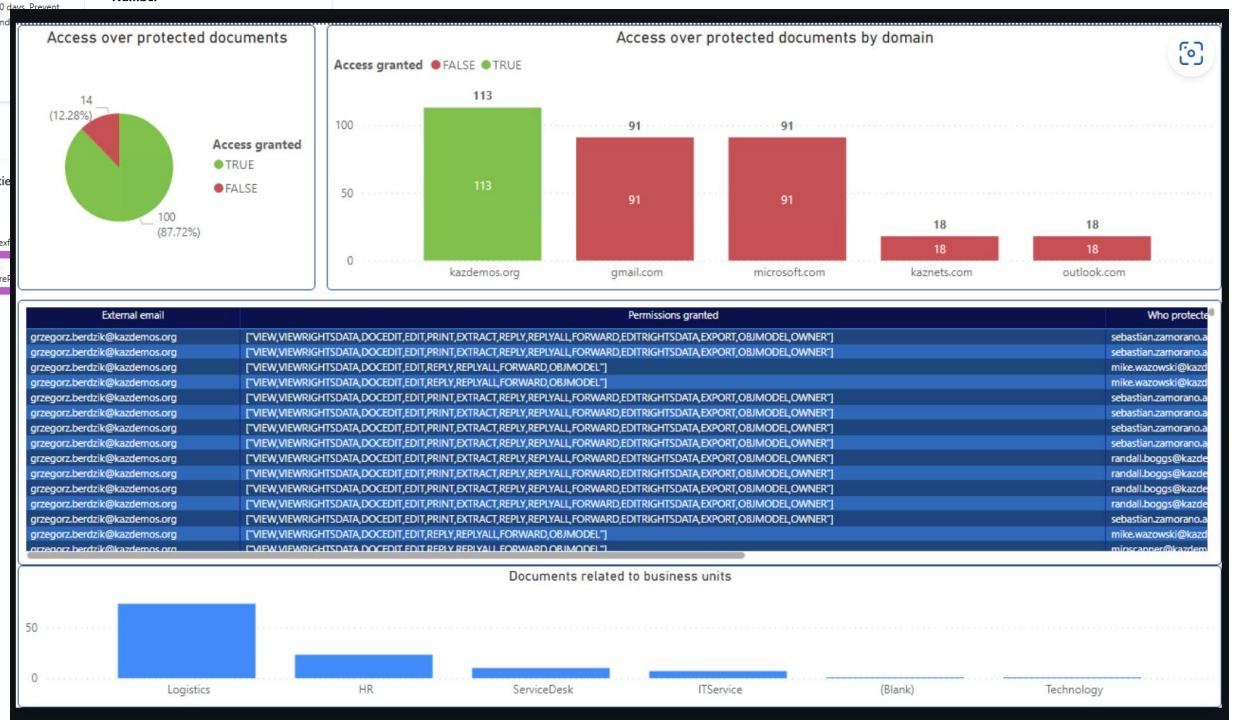


# Know your data and your threats

water




[GitHub - microsoft/Microsoft-Purview-Advanced-Rich-Reports-MPARR-Collector: Repository with all the MPARR components solution]

water

MYTH 2

# Labeling is the answer to everything

BUSTED

MYTH 2

# Labeling is the answer to everything

BUSTED

## Labeling is the foundation of your MVP

- [x] Think about sensitivity
- [x] Educate your users to grow with the MVP
- [x] Don´t make them think

### Key Recommendations:

- Easy to use traffic light taxonomy
- Define a default for new content
- Allow exceptions and monitor usage

water

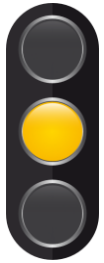
MYTH 3

# DLP destroys user productivity and kicks off the shit storm

# Apply baseline DLP based on your label taxonomy

## MVP DLP Configuration

Green – Block Documents which are shared externally and not labeled



Yellow – Documents which are shared externally and labeled

Red – Critical data which is only available for company internal members. External sharing is blocked without override. Special use cases may apply

| | | | |
|---|---|---|---|
| ☐ | Green - Block Unlabeled | 22 | On |
| ☐ | Yellow - Block Override | 23 | On |
| ☐ | Red - Block External | 24 | On |

| Name | Status |
|---|---|
| Yellow - Block Override Rule | On |

**Conditions**

Content is shared from Microsoft 365 **with people outside my organization**

**And**

Content contains any of these sensitivity labels: **Yellow, Yellow/Yellow - Default, Yellow/Yellow - All Company, Yellow/Yellow - Individual**
Evaluate predicate for **Message or attachment**

**Actions**

Notify users with email and policy tips
Restrict access to the content for external users
Send alerts to Administrator

water

MYTH 3

# DLP destroys user productivity and kicks off the shit storm

MYTH 3

# DLP destroys u
# productivity a
# the shit sion


## DLP that works with you — not against you

- ☑ Smart boundaries, not roadblocks
- ☑ Tailor policies to match your risk tolerance — without slowing down business

## Key Recommendations:

- ☆ Block  Override your “yellow” data
- ☆ Block/override  unlabeled documents
- ☆ Block your “red” data

water

MYTH 4

# I trust my employees, I do not need Insider Risk Management

water

# Detect the unusual & risky pattern

water

# (31ac5f2b) Alert: Confidentiality obligation during departure

Assign | Needs review | Confirm alert to an existing case | Dismiss alert

What will these actions do?

High Risk score: 87/100 Alert created on Feb 22, 2024 (UTC)

## Activity that generated this alert

Reduce alerts for this activity

**Data infiltration: Files downloaded from unallowed site**

87/100 **High severity** | Apr 10, 2024 (UTC)

2 events: Files downloaded from 1 unallowed site

2 events: Files that have labels applied, including: Project Alpha

**Factors that impacted risk score:**

Includes unallowed domains (1 event)

View all activity

## Triggering event

May 28, 2024 (UTC)

An HR connector imported a resignation date for this user.

## User details

**Potential high impact user**

User accessed more content containing sensitive info than other users.

+ 2 more reasons

**Priority user gro**

Project Tiger Tented Project

+ 1 more groups

Anony85KF-34DF

View all details

## User alert history

Last 30 days

No alert history

View full user history

All risk factors | Activity explorer | User activity | Forensic evidence

## All risk factors for this user's activity

### Top exfiltration activities

**1.9K exfiltration activities**

| | |
|---|---|
| Copied to USB | 428 |
| Download from SharePoint | 200 |
| Email sent to external recipient | 1,289 |

View all exfiltration activity

### Cumulative exfiltration activities

**High severity cumulative exfiltration activities detected (Risk score: 82/100)**

User activity detected ranges from 04/09 - 04/10

**All exfiltration activities with prioritized content**
More events than 90% compared to teammates.

| | |
|---|---|
| User | 467 |
| Teammates | 2 |

**Shared SharePoint files externally**
More events than 99% compared to users that access same SharePoint sites.

| | |
|---|---|
| User | 20 |
| Users who access same SharePoi... | 9 |

**All exfiltration activities**
More events than 30% compared to users with similar job title.

| | |
|---|---|
| User | 21 |
| Users with similar job title | 9 |

View all cumulative exfiltration activities

### Sequences of activity

**1 sequence activity**

View all sequence activity

Insider Risk Management alerts page, showing risk factors for user's activity

No activity is considered unusual for this user

No activity includes events with priority content

**2 activities include events with unallowed domains**

# (31ac5f2b) Alert: Confidentiality obligation during departure

Assign | Needs review | Confirm alert to an existing case | Dismiss alert

What will these actions do?

All risk factors | Activity explorer | User activity | Forensic evidence

Filter: Show: All scored activity for this user | Risk category: Any | Activity Type: Any | Reset all

Sort by: Date occured

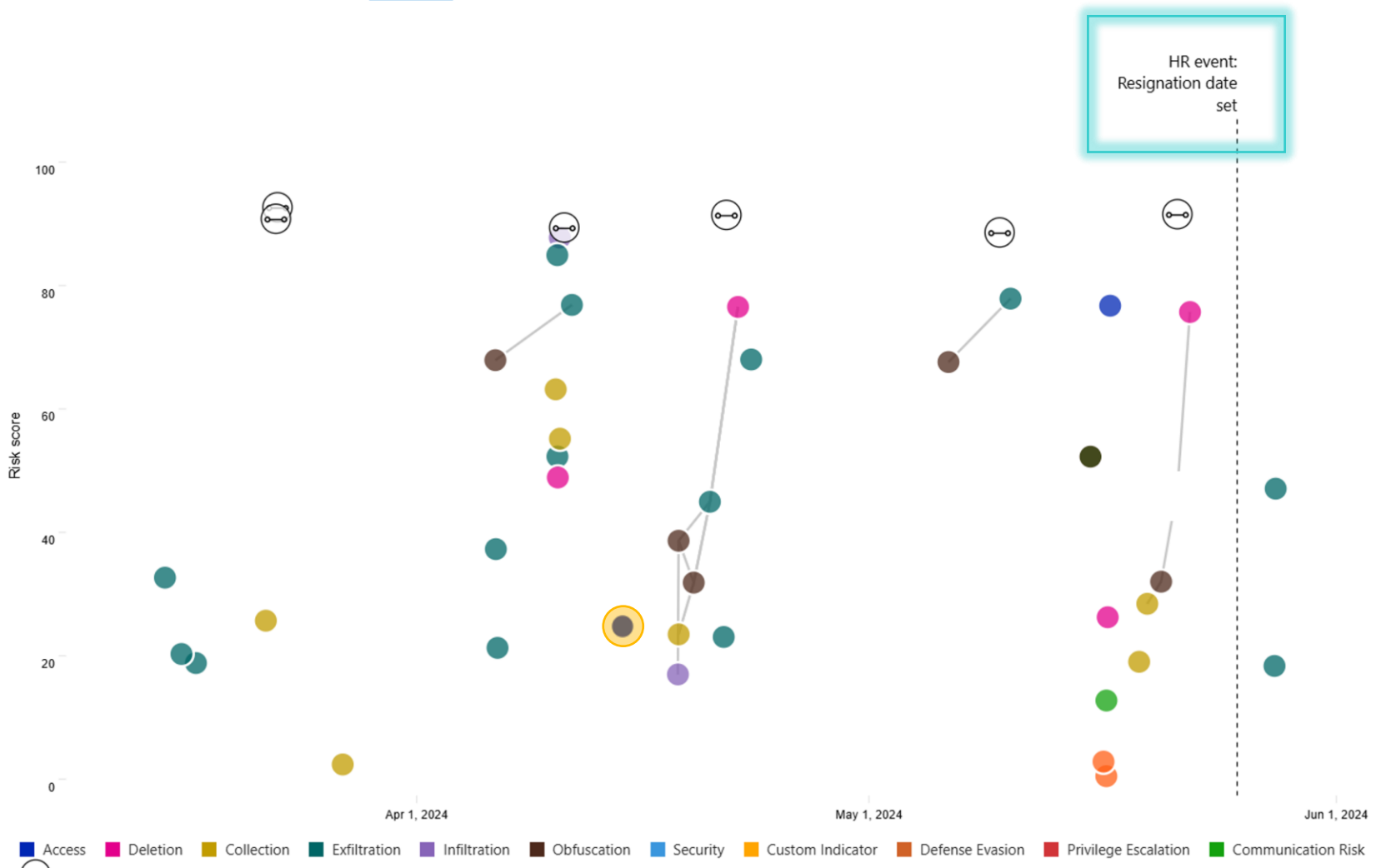
**(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up**
May 19, 2024 - May 22, 2024 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted
5 events: Files that have labels applied, including: Project Obsidian
2 events: Files containing sensitive info, including: Credit Cards
1 event: File sent to 1 unallowed domain
2 events: Files with priority file extensions, including: docx

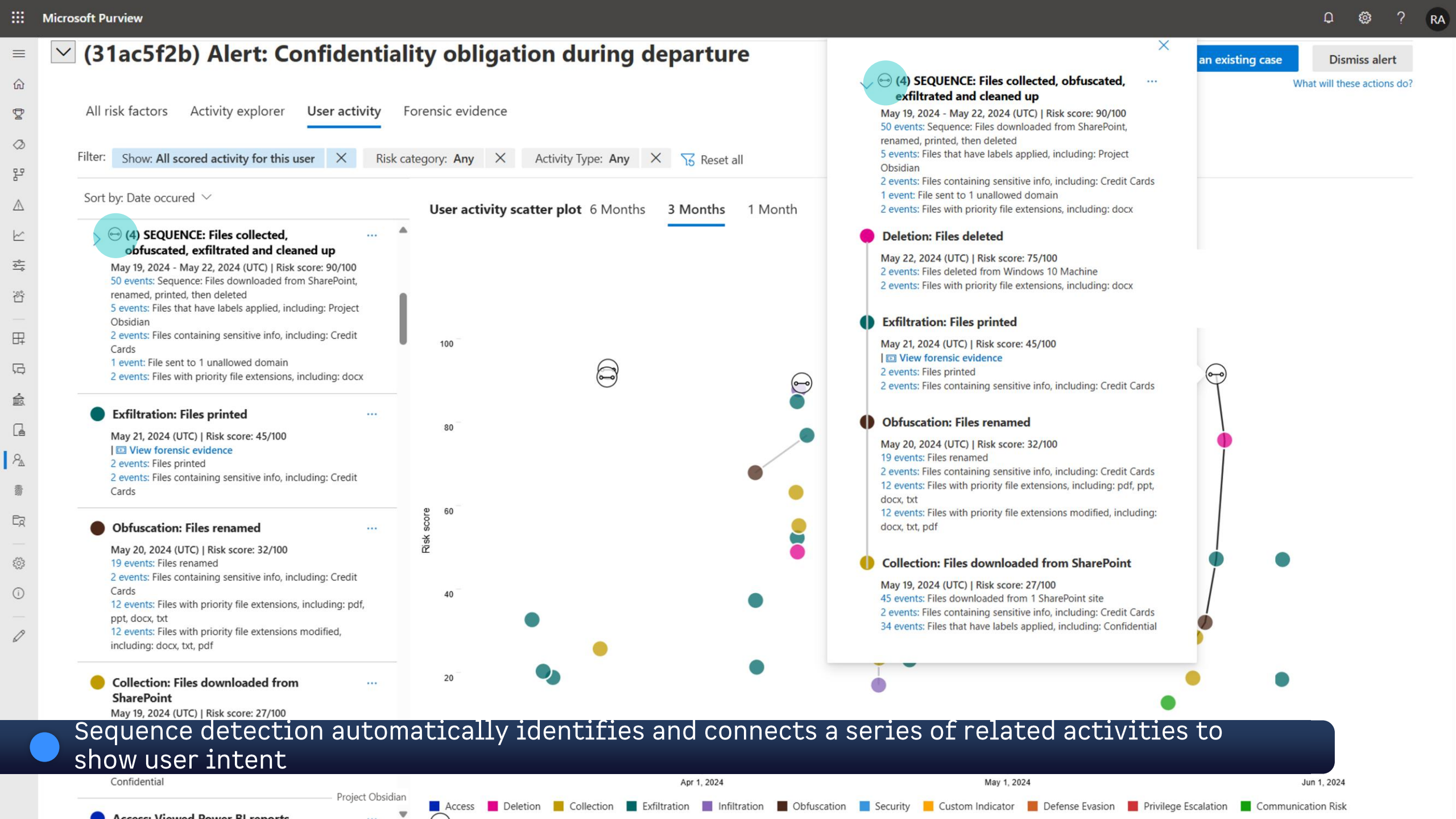
**Exfiltration: Files printed**
May 21, 2024 (UTC) | Risk score: 45/100
| View forensic evidence
2 events: Files printed
2 events: Files containing sensitive info, including: Credit Cards

**Obfuscation: Files renamed**
May 20, 2024 (UTC) | Risk score: 32/100
19 events: Files renamed
2 events: Files containing sensitive info, including: Credit Cards
12 events: Files with priority file extensions, including: pdf, ppt, docx, txt
12 events: Files with priority file extensions modified, including: docx, txt, pdf

**Collection: Files downloaded from SharePoint**
May 19, 2024 (UTC) | Risk score: 27/100
45 events: Files downloaded from 1 SharePoint site
2 events: Files containing sensitive info, including: Credit Cards
34 events: Files that have labels applied, including: Confidential

**User activity scatter plot** 6 Months | 3 Months | 1 Month




Microsoft Purview
RA
(31ac5f2b) Alert: Confidentiality obligation during departure
an existing case
Dismiss alert
What will these actions do?
All risk factors
Activity explorer
User activity
Forensic evidence
Filter:
Show: All scored activity for this user
Risk category: Any
Activity Type: Any
Reset all
Sort by: Date occured
User activity scatter plot
6 Months
3 Months
1 Month
(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up
May 19, 2024 - May 22, 2024 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted
5 events: Files that have labels applied, including: Project Obsidian
2 events: Files containing sensitive info, including: Credit Cards
1 event: File sent to 1 unallowed domain
2 events: Files with priority file extensions, including: docx
Exfiltration: Files printed
May 21, 2024 (UTC) | Risk score: 45/100
View forensic evidence
2 events: Files printed
2 events: Files containing sensitive info, including: Credit Cards
Obfuscation: Files renamed
May 20, 2024 (UTC) | Risk score: 32/100
19 events: Files renamed
2 events: Files containing sensitive info, including: Credit Cards
12 events: Files with priority file extensions, including: pdf, ppt, docx, txt
12 events: Files with priority file extensions modified, including: docx, txt, pdf
Collection: Files downloaded from SharePoint
May 19, 2024 (UTC) | Risk score: 27/100
Deletion: Files deleted
May 22, 2024 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine
2 events: Files with priority file extensions, including: docx
45 events: Files downloaded from 1 SharePoint site
2 events: Files containing sensitive info, including: Credit Cards
34 events: Files that have labels applied, including: Confidential
Risk score
100
80
60
40
20
Apr 1, 2024
May 1, 2024
Jun 1, 2024
Access
Deletion
Collection
Exfiltration
Infiltration
Obfuscation
Security
Custom Indicator
Defense Evasion
Privilege Escalation
Communication Risk
Project Obsidian
Sequence detection automatically identifies and connects a series of related activities to show user intent

water

MYTH 4

# I trust my employees, I do not need Insider Risk Management

MYTH 4

# I trust my emp
# I do not need I
# Management

BUSTED

Insider Risk Management helps you to

- ☑ detect unusual and unexpected behavior
- ☑ identify critical pattern and build a powerful response

## Key Recommendations:

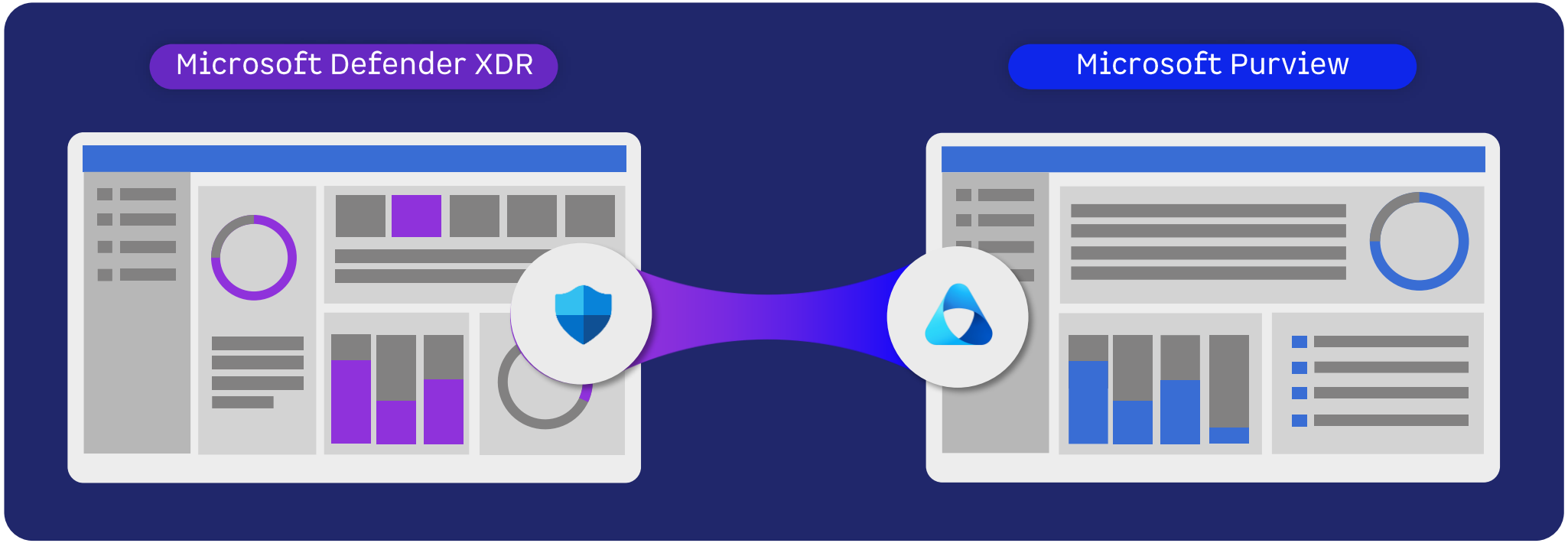
- ☆ Activate Analytics in Insider Risk Management
- ☆ Create a policy for people leaving the company
- ☆ Monitor and investigate incidents in your SOC

water

MYTH 5

# SOC does not need data security insights

# Data security insights for the SOC



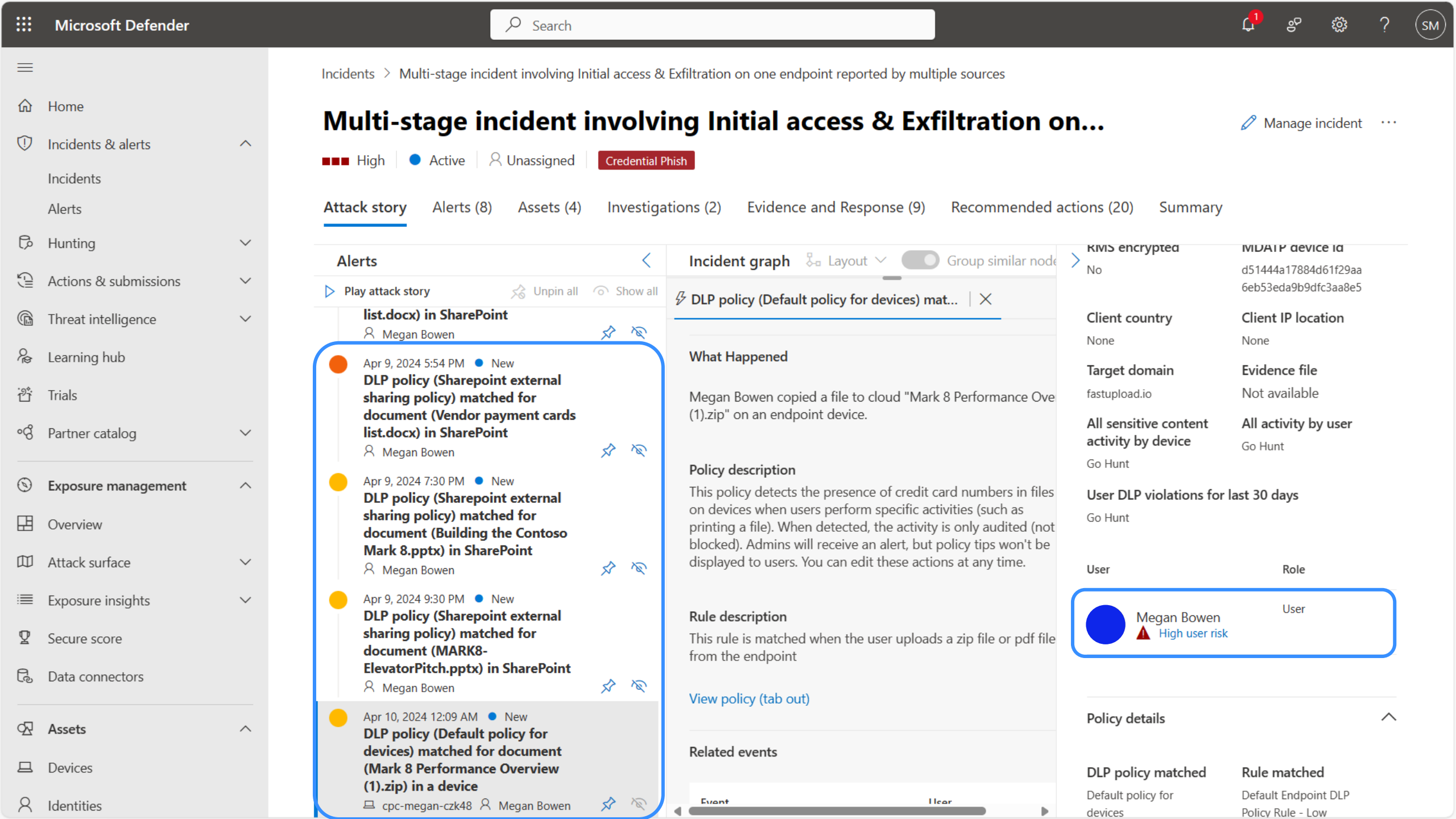
# Data security for SOC scenarios

water

Data security context helping investigation of compromised users

Insider threat investigations in Defender XDR

Defender XDR Advanced Hunting for policy tuning


Microsoft Defender
Search
SM
Home
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Threat intelligence
Learning hub
Trials
Partner catalog
Exposure management
Overview
Attack surface
Exposure insights
Secure score
Data connectors
Assets
Devices
Identities
Incidents > Multi-stage incident involving Initial access & Exfiltration on one endpoint reported by multiple sources
Multi-stage incident involving Initial access & Exfiltration on...
Manage incident
High
Active
Unassigned
Credential Phish
Attack story
Alerts (8)
Assets (4)
Investigations (2)
Evidence and Response (9)
Recommended actions (20)
Summary
Alerts
Play attack story
Unpin all
Show all
list.docx) in SharePoint
Megan Bowen
Apr 9, 2024 5:54 PM New
DLP policy (Sharepoint external sharing policy) matched for document (Vendor payment cards list.docx) in SharePoint
Megan Bowen
Apr 9, 2024 7:30 PM New
DLP policy (Sharepoint external sharing policy) matched for document (Building the Contoso Mark 8.pptx) in SharePoint
Megan Bowen
Apr 9, 2024 9:30 PM New
DLP policy (Sharepoint external sharing policy) matched for document (MARK8-ElevatorPitch.pptx) in SharePoint
Megan Bowen
Apr 10, 2024 12:09 AM New
DLP policy (Default policy for devices) matched for document (Mark 8 Performance Overview (1).zip) in a device
cpc-megan-czk48
Megan Bowen
Incident graph
Layout
Group similar node
DLP policy (Default policy for devices) mat...
What Happened
Megan Bowen copied a file to cloud "Mark 8 Performance Ove (1).zip" on an endpoint device.
Policy description
This policy detects the presence of credit card numbers in files on devices when users perform specific activities (such as printing a file). When detected, the activity is only audited (not blocked). Admins will receive an alert, but policy tips won't be displayed to users. You can edit these actions at any time.
Rule description
This rule is matched when the user uploads a zip file or pdf file from the endpoint
View policy (tab out)
Related events
Event
User
RMS encrypted
No
MDATP device id
d51444a17884d61f29aa6eb53eda9b9dfc3aa8e5
Client country
None
Client IP location
None
Target domain
fastupload.io
Evidence file
Not available
All sensitive content activity by device
Go Hunt
All activity by user
Go Hunt
User DLP violations for last 30 days
Go Hunt
User
Role
Megan Bowen
High user risk
User
Policy details
DLP policy matched
Default policy for devices
Rule matched
Default Endpoint DLP Policy Rule - Low

# Multi-stage incident involving Initial access & Exfiltration on one endpoint report...

Copilot | Manage incident | Tasks | ...

High | Active | abbe33@

Attack story | Alerts (293) | Assets (7) | Investigations (0) | Evidence and Response (11) | Recommended actions (4) | Summary | Similar incidents (1)

Play attack story | Unpin all | Show all

Nov 14, 2024 2:28 PM New
**DLP policy (Default HR & Privacy Info Protection Policy) matched for document (Contoso Background Check Candidates.csv) in OneDrive**
Natasha

Nov 14, 2024 2:28 PM New
**DLP policy (Default Finance Info Protection Policy) matched for document (Acquisition Strategy.docx) in OneDrive**
Natasha

Nov 14, 2024 4:47 PM New
**Endpoint User Behavior Deviation Detection**
CPC-mscot-556 Natasha

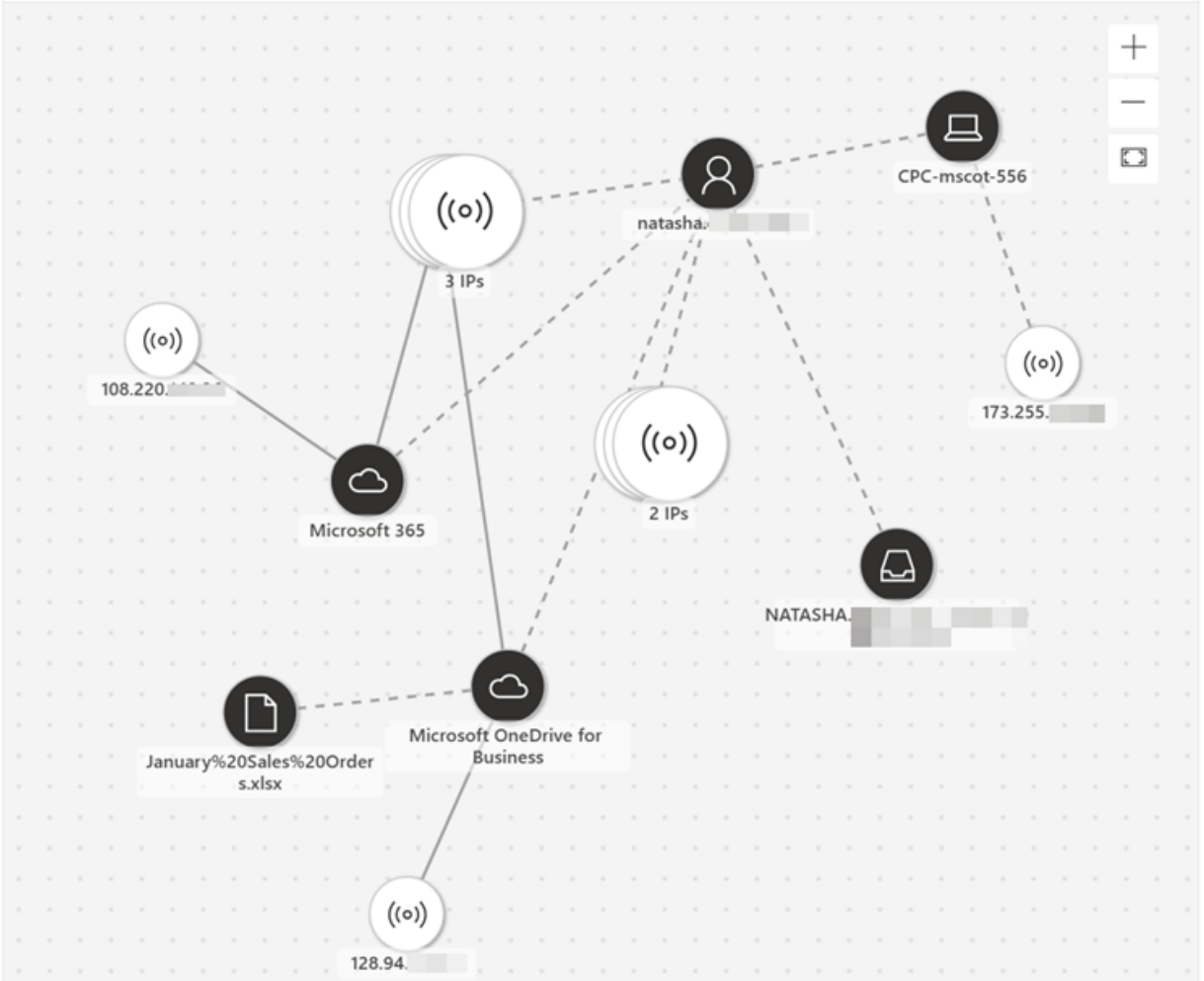
Nov 14, 2024 7:28 PM New
**Purview IRM ('73aad306') Project TNT - Alert**
Natasha

Nov 14, 2024 7:33 PM Resolved
**Purview IRM ('72e4b685') Data leaks quick policy - 1/4/2024**
Natasha

Nov 14, 2024 9:47 PM New
**Endpoint User Behavior Deviation Detection**
CPC-mscot-556 Natasha

Nov 15, 2024 2:47 AM New
**Endpoint User Behavior Deviation Detection**

Incident graph | Layout | Group similar nodes




RELATED THREATS

Threat Overview Profile: Adversary-in-the-middle credential phishing

1129 impacted assets

View threat analytics report

## Incident details

**Assigned to**
abbe33@

**Incident ID**
186975

**Classification**
Not set

**Categories**
Initial access, Defense evasion, Credential access, Exfiltration, Impact, Suspicious activity

**First activity**
Oct 29, 2024 6:47:47 AM

**Last activity**
Jan 6, 2025 4:43:20 PM

## Impacted assets

Devices (1) | Risk Level | Exposure Level

# Advanced hunting

Help resources | Query resources report | Schema reference

New query*

Schema | Functions | Queries

Search

Favorites

Alerts & behaviors

Apps & identities

Data Security

- DataSecurityBehaviors
- DataSecurityEvents
  - Timestamp
  - Application
  - DeviceId
  - DeviceName
  - AadDeviceId
  - IsManagedDevice
  - DlpPolicyMatchInfo
  - DlpPolicyEnforcementMode
  - DlpPolicyRuleMatchInfo
  - FileRenameInfo
  - PhysicalAccessPointId
  - PhysicalAccessPointName

Run query | Custom time range | Save | Share link

Query

```
let InterestedDomains = (DataSecurityEvents
| where ActionType  == "File upload to cloud"
| summarize ConfidentialFileCount = count() by TargetUrlDomain
| sort by ConfidentialFileCount desc
| project TargetUrlDomain, ConfidentialFileCount
| take 5);
let DistinctUserCount = (DataSecurityEvents
| where ActionType == "File upload to cloud"
| summarize DistinctUserCount = dcount(AccountUpn) by TargetUrlDomain
| project TargetUrlDomain, DistinctUserCount);
InterestedDomains
| join kind=innerunique DistinctUserCount on TargetUrlDomain
| project TargetUrlDomain, ConfidentialFileCount, DistinctUserCount
```

Getting started | Results | Query history

Export | Show empty columns | 1 item | Search | 00:00.582 | Low | Chart type | Full screen

Filters: Add filter

| TargetUrlDomain | ConfidentialFileCount | DistinctUserCount |
|---|---|---|
| drive.google.com | 1 | 1 |

water

MYTH 5

# SOC does not need data security insights

MYTH 5

# SOC does not
# security insig

BUSTED

Enable your SOC to

- ☑ get better insights with data context
- ☑ correlate cyber attacks to internal threats

## Key Recommendations:

- ☆ Integrate Insider Risk Management and DLP Alerts into your SOC playbooks
- ☆ Define an investigation process to verify and analyze risky and unusual behavior together with legal and HR

water

MYTH 6

# My business will hate the IT for implementing data security

water

# One team – build upon experts


Success in data security starts with a team that recognizes the challenge and brings diverse perspectives from day one.

water

MYTH 6

# My business will hate the IT for implementing data security

MYTH 6

# My business wi
# IT for impleme
# security

BUSTE

Successful data security projects have

- ☑ Management attention and support
- ☑ Integration of Business and IT
- ☑ User Productivity in mind

Key Recommendations:

- ☆ Data Security is not an IT project
- ☆ Build a interdisciplinary team
- ☆ Let your users grow with the project, start simple, change only with care

water

# Merger and Acquisition project

## From Zero to Hero

### Day 0

**How it starts**

No data security measures in place

IP drained out of the company after the merge with a new company

### Day 10

**Quick Response to tackle the process**

Quick Response by defining the scope of the MVP

Implementing a set of Labels and DLP rules

Activating IRM, for detection and psychological barriers

### Day 45

**MVP Rollout**

Rollout to critical departments of the merged company

Monitor usage and adoption

SOC Playbook to start investigation at SOC lv1; correlate signals and escalate to BU for investigation

### Day 90 and ongoing

**Define edge cases**

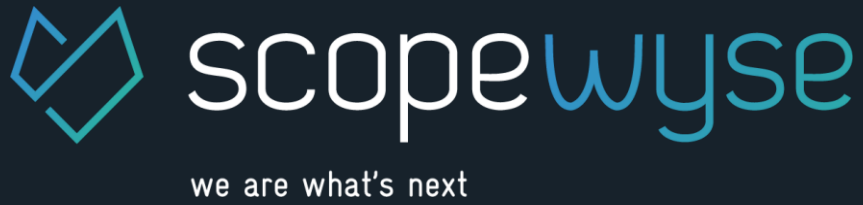
IP content identified which goes beyond the baseline protection

SITs and EDM in combination with DLP to address the risk

water

# Q&A


SwissMicrosoft
SECURITY SUMMIT


scopewyse
we are what's next


Ontinue


INGRAM
MICRO


EPIC FUSION
BRING IT ALL TOGETHER


Microsoft


water
IT Security & Defense


Swiss Post
Cybersecurity


techtask


iC CONSULT


Mediawerk


water
IT Security & Defense