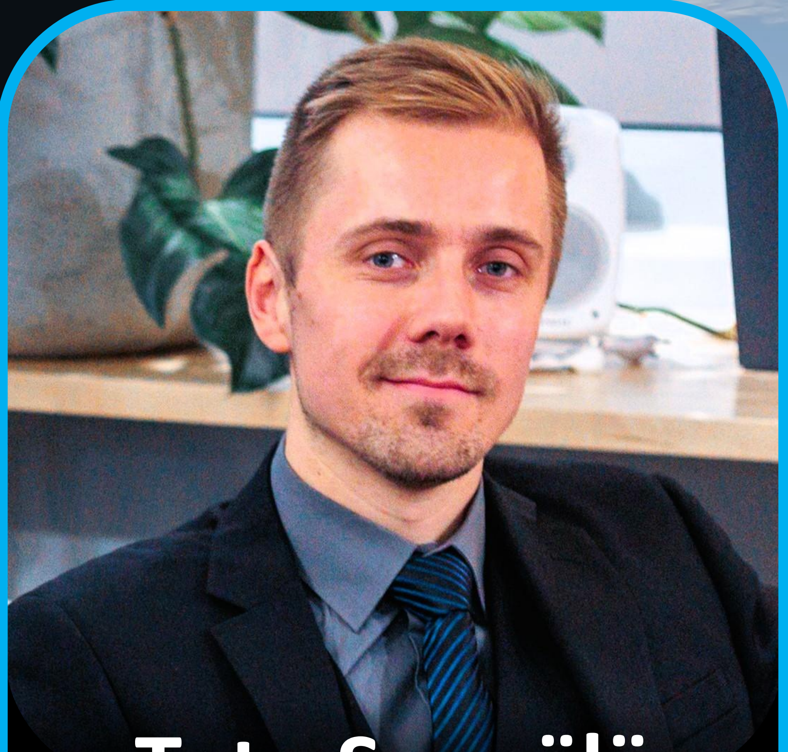
Insider threat:
First Aid for a Misunderstood Risk Vector

Tatu Seppälä

- ⭐ Data security
- ⭐ Insider risk
- Power Platform
- Governance
- IAM / Entra ID
- Generative AI

SULAVA
CREATING BETTER WORKLIFE

The Digital
Neighborhood



Tatu Seppälä

Security & Compliance Architect

MVP Microsoft® Most Valuable Professional

By **2027**,

70% of organizations will combine **data loss prevention and insider risk management disciplines with IAM context** to identify suspicious behavior more effectively.

Gartner, 3/2024

Agenda

- Insider risk vs. insider threat
- It’s all about indicators
- The intentional insider
- Connecting the dots
- The unintentional insider
- What’s next?

Insider risk vs. insider threat

What is an ‘insider’?

- Any person who **has** or **previously had..**
- ..authorized **access to** or **knowledge of..**
- the organization’s resources, including **people**, **processes**, **information**, **technology** and **facilities**.

⚠️ Insider risk

- The ***potential*** for any individual..
- ..who **has or previously had..**
- **..**authorized **access to or knowledge of** an organization's assets..
- ..to act (or not act), **either maliciously or unintentionally..**
- ..in a way that could cause harm or loss to an organization.

💣 Insider threat

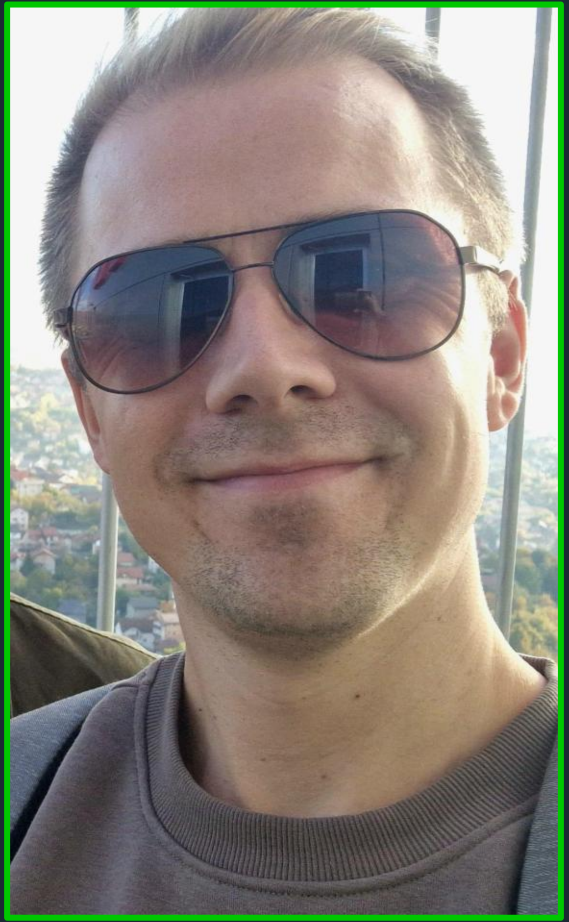
- An insider, or group of insiders, that either **intends to** or **is likely to** cause harm or loss to the organization.

The typical threat

- ♂️ Male
- 👨 31-45yo
- 🎓 University graduate
- 💼 Permanent staff – not C-level
- Customer service, security or financial dept.
- Employed for <5y
- Self-initiated: identified opportunity *after* being hired
- Threat activity ongoing for <1y when detected

The typical threat

- ♂ Male
- 👨 31-45yo
- 🎓 University***(ish)*** graduate
- 💼 Permanent staff – not C-level ***(yet..)***
- Customer service, security or financial dept.
- Employed for <5y
- Self-initiated: identified opportunity *after* being hired
- Threat activity ongoing for <1y when detected



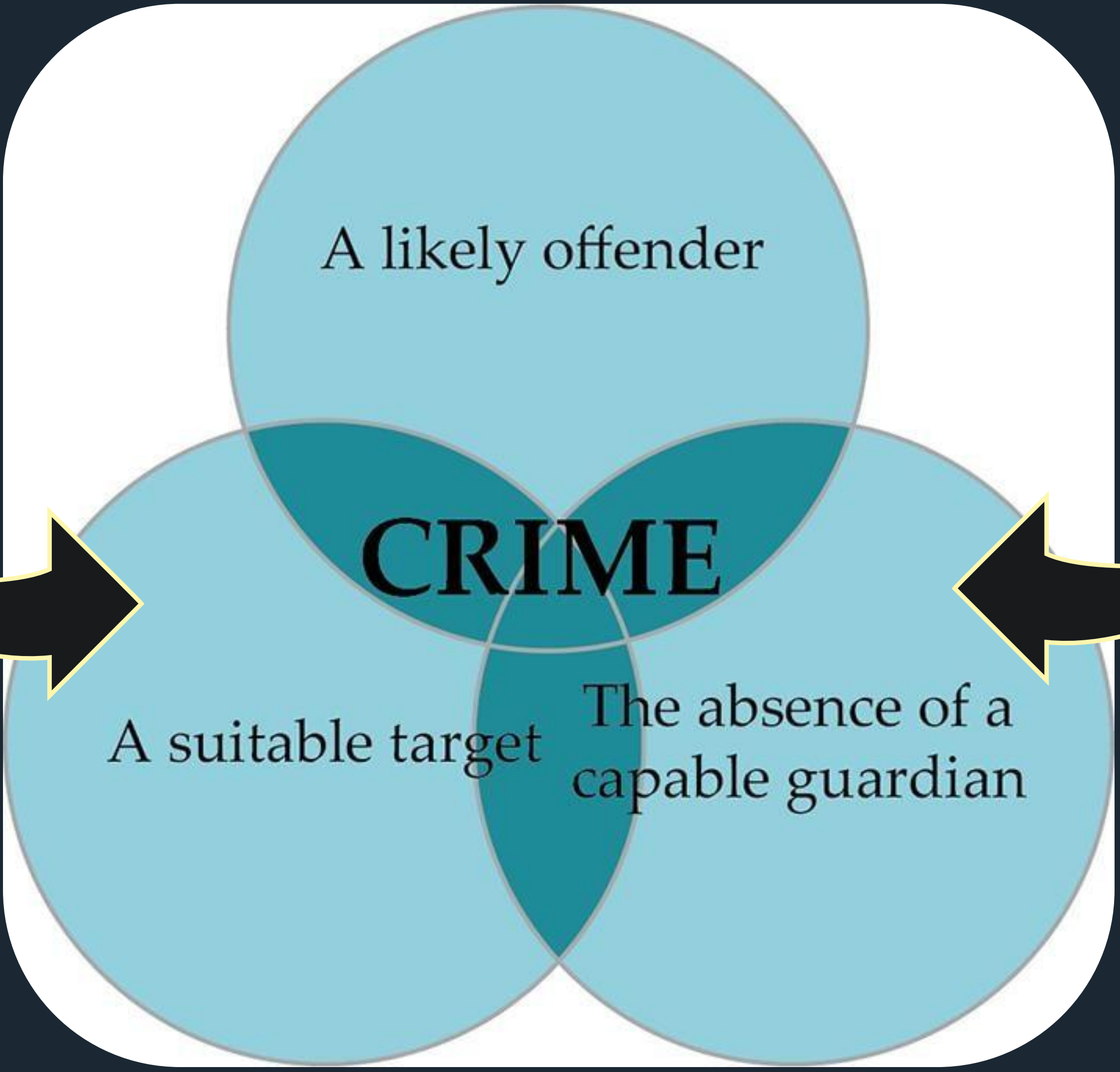
The intentional insider

Topics: The intentional insider

- 🐀 RAT & the criminology angle
- Motivators, triggers and threat activities
- Case examples & first aid

🐀 Routine Activities Theory

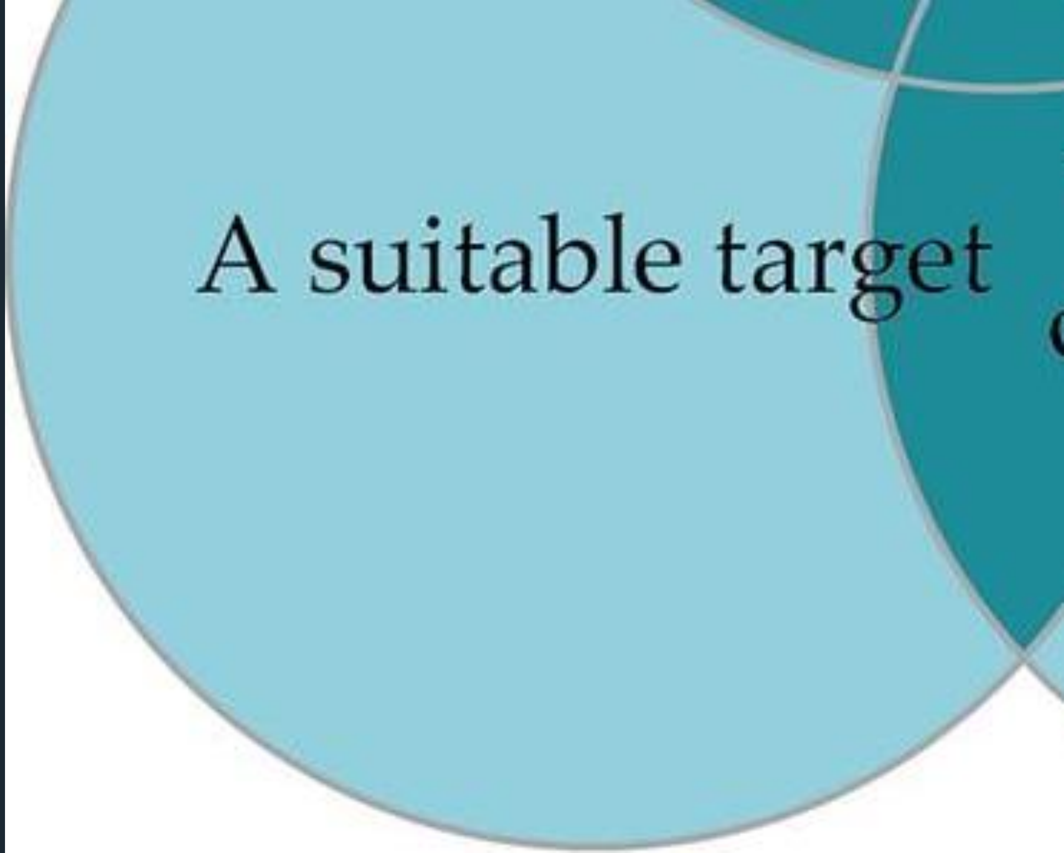
Partly our job



Our job

The VIVA model

- **Value** – target desirability
- **Inertia** – how simple target is to take
- **Visibility** – how noticeable target is
- **Access** – how easy target is to get to

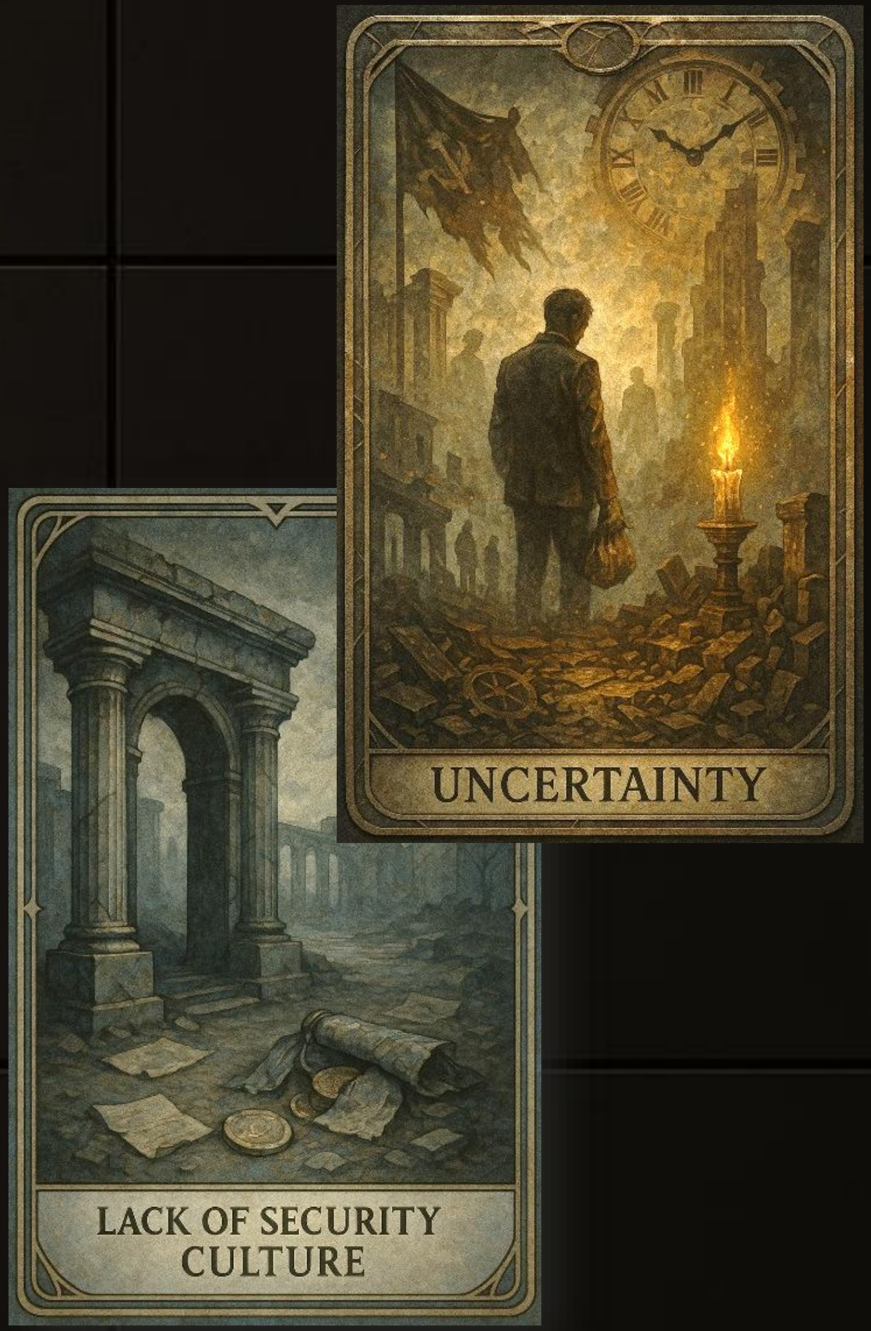


Motivators

GREED
EGO
IDEOLOGY
OPPORTUNITY
REVENGE

Triggers

ISOLATION
PERSONAL DISSATISFACTION
STRESS AND LIFE EVENTS
FINANCIAL PROBLEMS


LACK OF SECURITY CULTURE
UNCERTAINTY

Threat activities

UNAUTH. ACCESS
UNAUTH. DISCLOSURE
PROCESS CORRUPTION
IT / PHYSICAL SABOTAGE
FACILITATION OF 3P ACCESS

Predisposing factors for motivations

- **Dark triad personality traits**
  - **Narcissism** → Ego, Revenge
  - **Machiavellianism** → Greed, Opportunity
  - **Psychopathy** → Greed, Opportunity, Revenge
- **Impulsiveness** → Opportunity
- **Vengefulness** → Revenge
- **Over-achievement** → Ego
- Paranoia
- …

Ephialtes of Trachis

- Battle of Thermopylae (480BCE)
- Betrayed the Greek army, revealing a flanking path to the Persians
- Primary motivator: **Greed** - hoped for a monetary reward

⛔ Didn’t get paid

🎬 Got into a movie though

Assassination of Julius Caesa

- Rome (44BCE)
- Two insiders close to Julius Caesar organized his assassination
- Presented act as defense of the republic against tyranny
- Primary motivator: **Ideology**

👉 Ideological rationalization lets people justify extreme insider acts

Tim Lloyd
& Omega engineering

- 1996, Newark New Jersey
- Programmer & network admin activated pre-prepared software time bomb three weeks after being fired
- Deleted all design and production software, caused $10 million in damages
- Also stole $50k in equipment
- Primary motivator: **Revenge**

💊 First aid

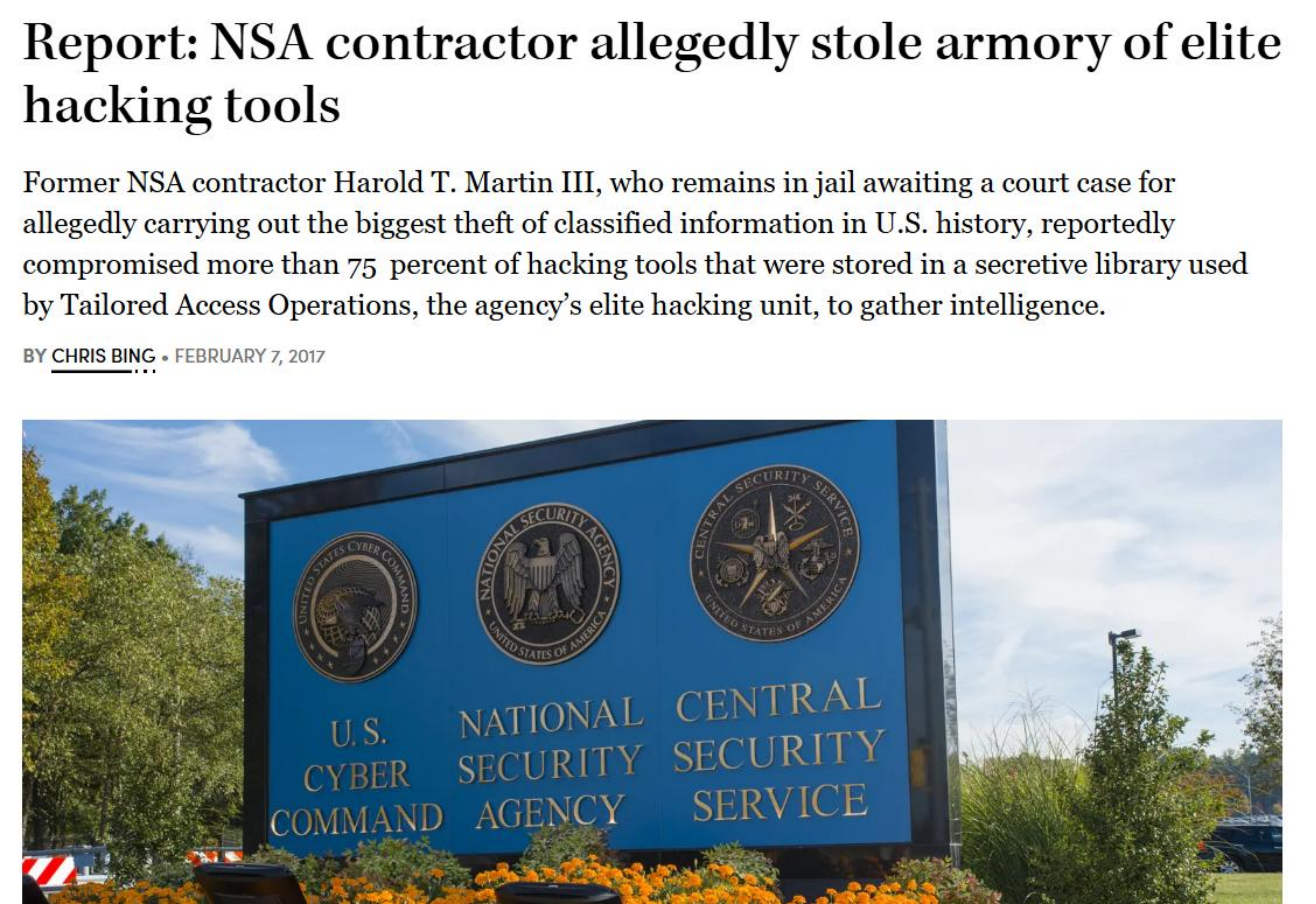
- IAM hygiene on termination
- Review automations built by / changed by user
- Require managed, compliant device

Terry Childs and the San Francisco Fib

- Engineer locked admins out of network for 12 days, “hijacked” both the network passwords and the backup configurations
- Triggers:
  - Concerned about threat of layoff
  - City discovered his lies about his criminal background
- Incident cost: $866000
- Ultimately drew attention to ineffective security controls
- Primary motivator: **Ego**

💊 First aid

- Implement PIM, remove standing GA privileges
- Follow least privilege, limit admin rights consolidation
- Critical admin tasks only from Privileged Access Workstations
- Offboarding playbook for individuals with privileged access
- Screening for privileged roles



Report: NSA contractor allegedly stole armory of elite hacking tools

Former NSA contractor Harold T. Martin III, who remains in jail awaiting a court case for allegedly carrying out the biggest theft of classified information in U.S. history, reportedly compromised more than 75 percent of hacking tools that were stored in a secretive library used by Tailored Access Operations, the agency's elite hacking unit, to gather intelligence.

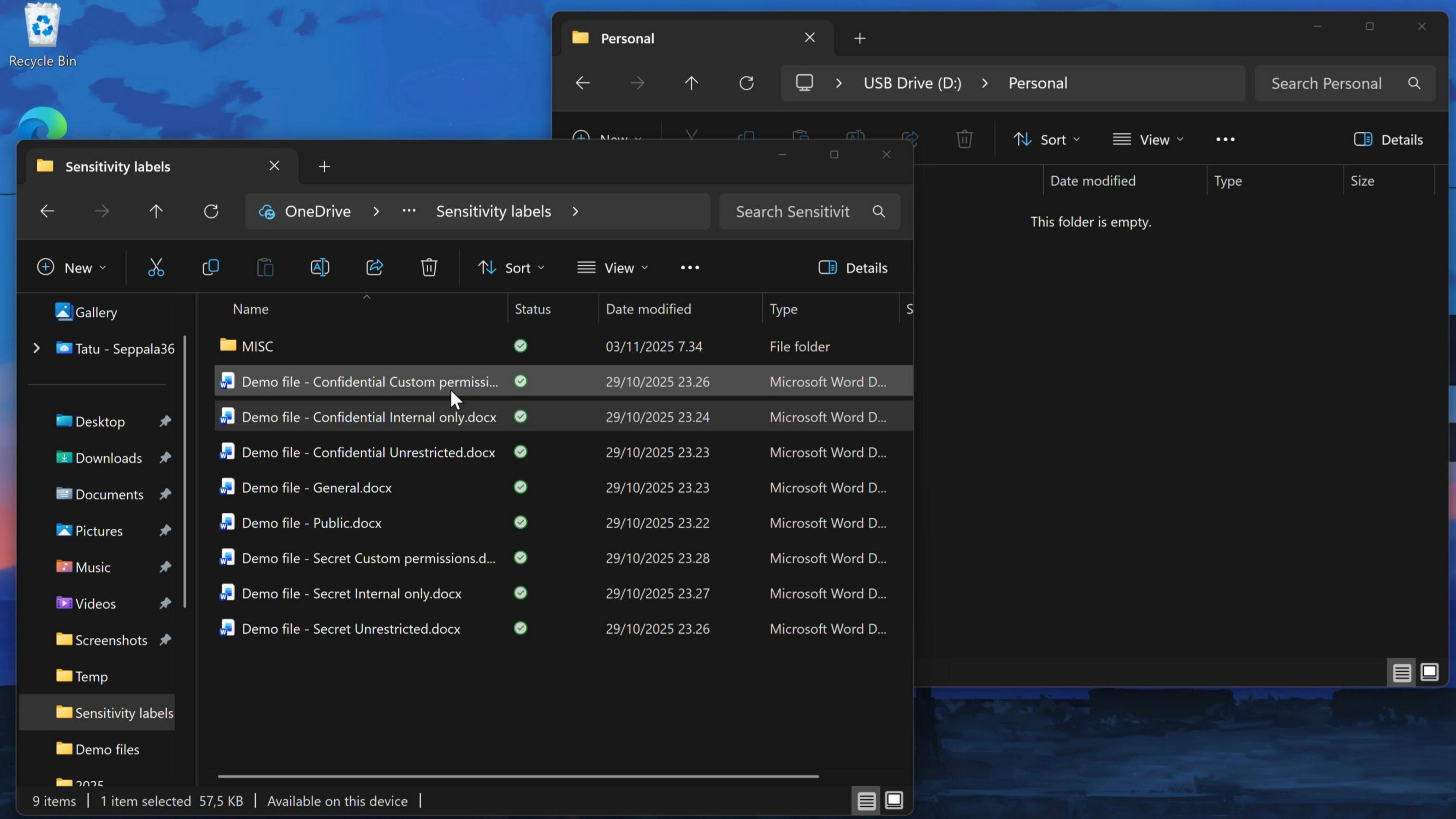
BY CHRIS BING • FEBRUARY 7, 2017

UNITED STATES CYBER COMMAND
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
CENTRAL SECURITY SERVICE UNITED STATES OF AMERICA
U.S. CYBER COMMAND
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

Harold T. Martin III & the NSA

- Contractor accumulated sensitive NSA data over 20 years, total >50TB, of which dozens were secret documents
- Driven by **curiosity** and hoarding tendencies, rather than profit or malice
- Data included >75% of all hacking tools of the TAO (Tailored Access Operations) unit
- Enabled by poor access management practices and security controls on data
- Primary motivator: **Opportunity**

Endpoint DLP restrictions



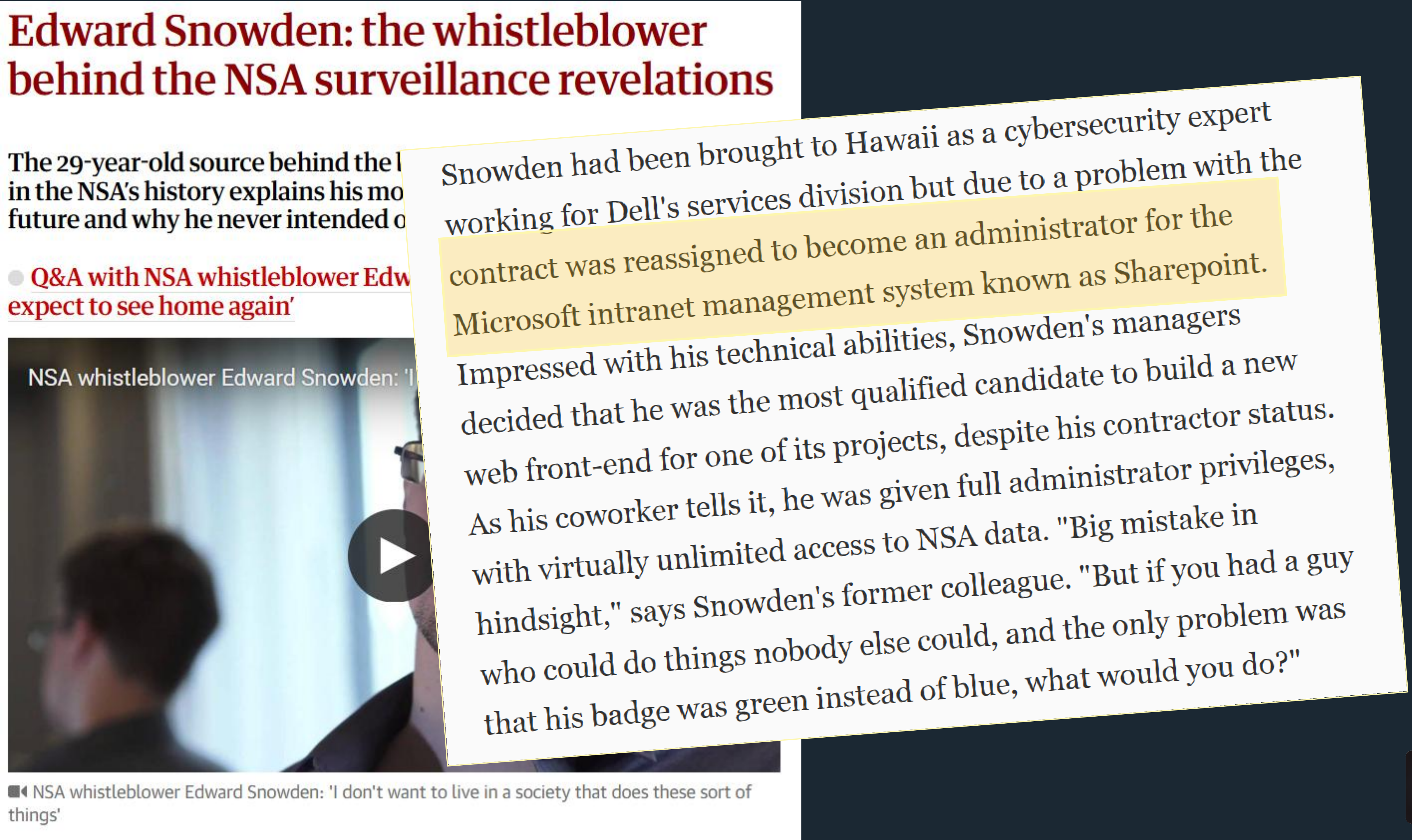
This folder is empty.

Name	Status	Date modified	Type
MISC	✓	03/11/2025 7.34	File folder
Demo file - Confidential Custom permissi...	✓	29/10/2025 23.26	Microsoft Word D...
Demo file - Confidential Internal only.docx	✓	29/10/2025 23.24	Microsoft Word D...
Demo file - Confidential Unrestricted.docx	✓	29/10/2025 23.23	Microsoft Word D...
Demo file - General.docx	✓	29/10/2025 23.23	Microsoft Word D...
Demo file - Public.docx	✓	29/10/2025 23.22	Microsoft Word D...
Demo file - Secret Custom permissions.d...	✓	29/10/2025 23.28	Microsoft Word D...
Demo file - Secret Internal only.docx	✓	29/10/2025 23.27	Microsoft Word D...
Demo file - Secret Unrestricted.docx	✓	29/10/2025 23.26	Microsoft Word D...

9 items | 1 item selected 57,5 KB | Available on this device |

💊 First aid

- Protect and track critical documents with Purview sensitivity labels and encryption
- Make exfiltration louder with Data Loss Prevention guardrails in M365 and endpoints
- Discover “slow drip” cumulative exfiltration patterns with Insider Risk Management
- Use Entra ID Access Packages to provide time-based access to sensitive materials



Edward Snowden: the whistleblower behind the NSA surveillance revelations

The 29-year-old source behind the b
in the NSA's history explains his mo
future and why he never intended o

Q&A with NSA whistleblower Edw
expect to see home again'

NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'

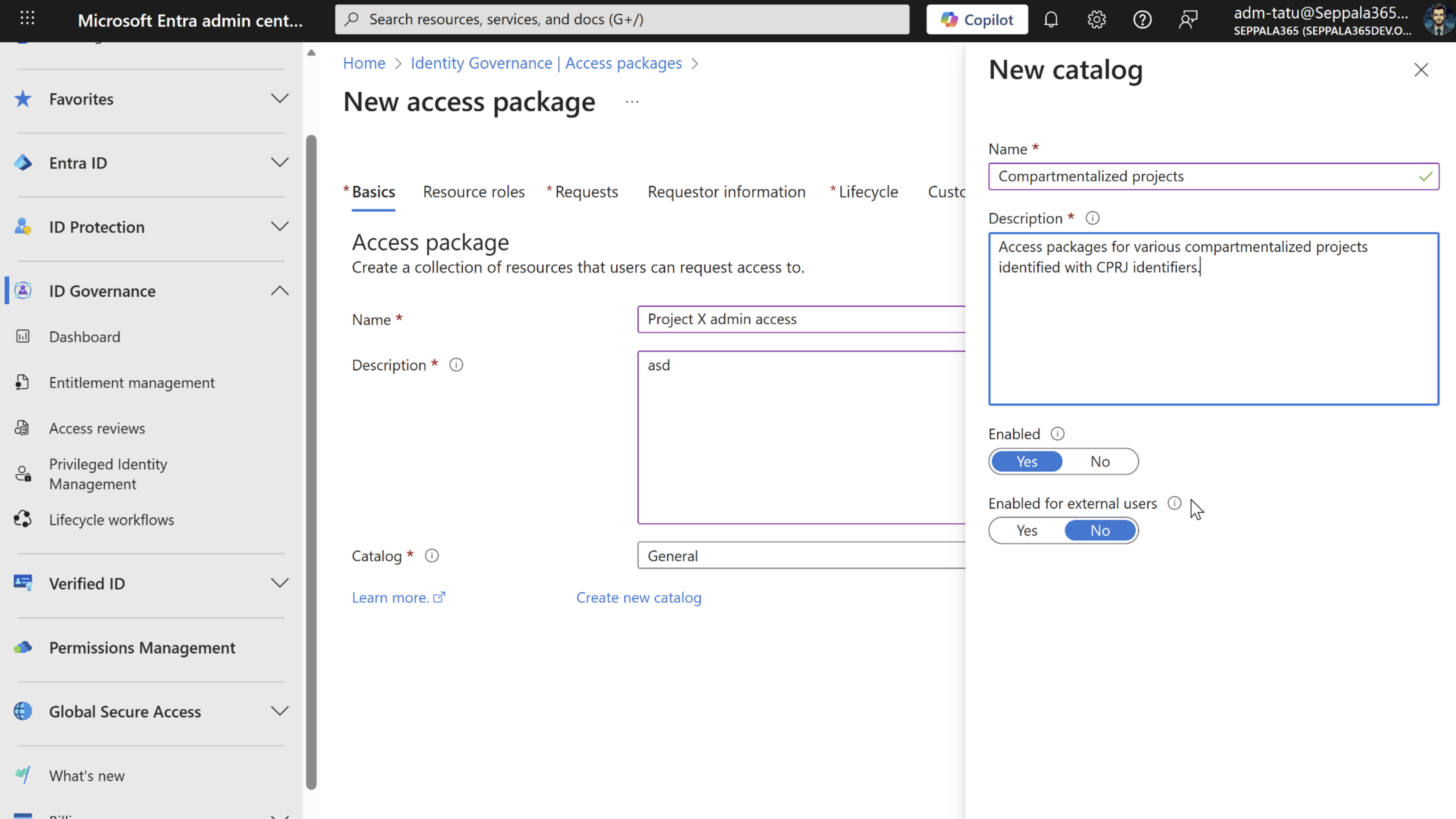
Snowden had been brought to Hawaii as a cybersecurity expert working for Dell's services division but due to a problem with the contract was reassigned to become an administrator for the Microsoft intranet management system known as Sharepoint. Impressed with his technical abilities, Snowden's managers decided that he was the most qualified candidate to build a new web front-end for one of its projects, despite his contractor status. As his coworker tells it, he was given full administrator privileges, with virtually unlimited access to NSA data. "Big mistake in hindsight," says Snowden's former colleague. "But if you had a guy who could do things nobody else could, and the only problem was that his badge was green instead of blue, what would you do?"

Edward Snowden & the NSA (2013)

- NSA contractor turned whistleblower, disclosed sensitive information about global surveillance programs
- Worked as **SharePoint admin** for servers used broadly by NSA analysts
- Had access to 1,7 million documents, shared up to 200,000+ with reporters
- Incl. Top Secret & Special Intelligence info
- Primary motivator: **Ideology**

🔎 Ability to detect cumulative exfiltration was missing for compartmentalized information

Entitlement management



New access package

Access package

Create a collection of resources that users can request access to.

Name * Project X admin access

Description * asd

Catalog * General

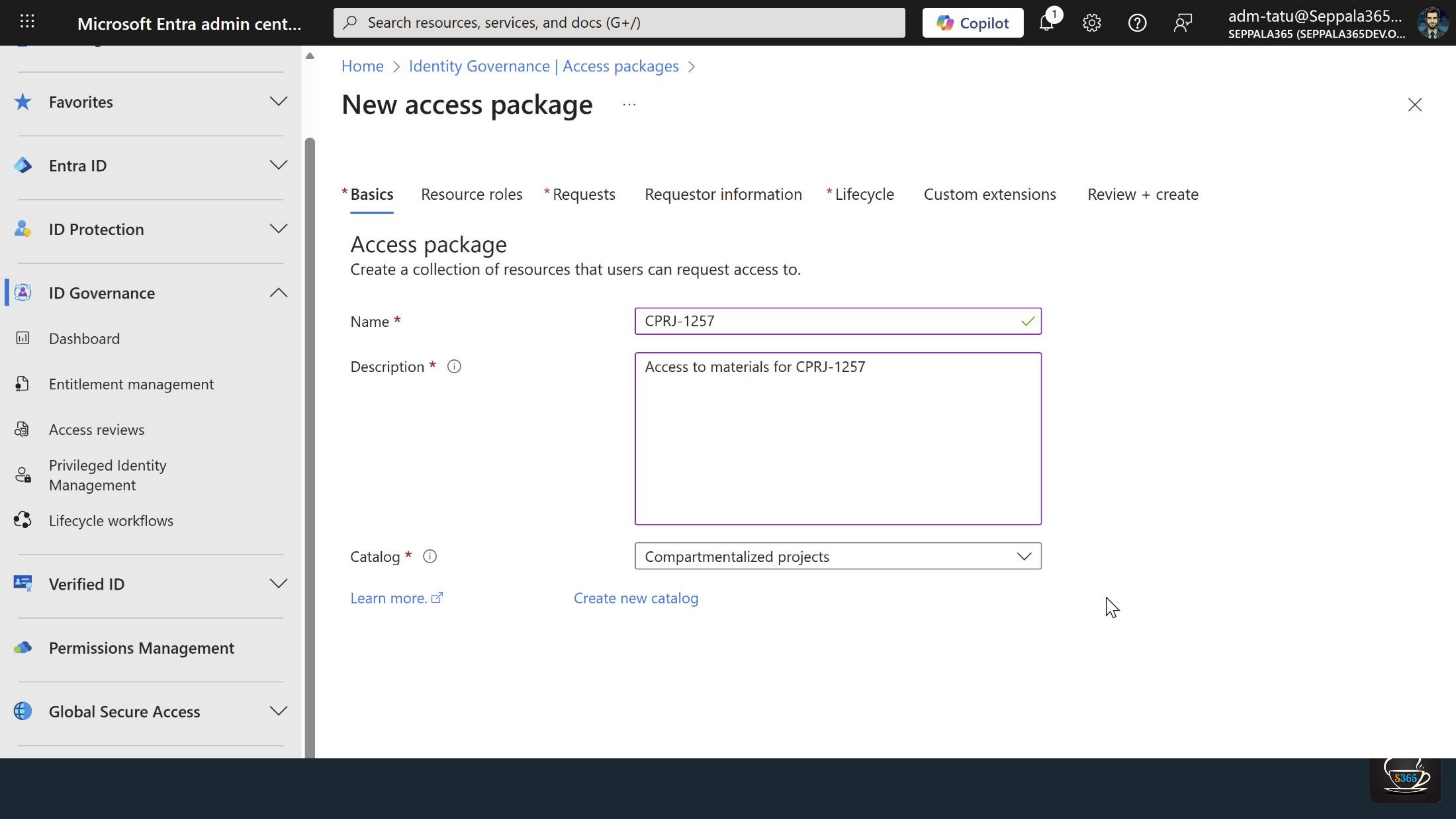
New catalog

Name * Compartmentalized projects

Description * Access packages for various compartmentalized projects identified with CPRJ identifiers.

Enabled: ● Yes ○ No

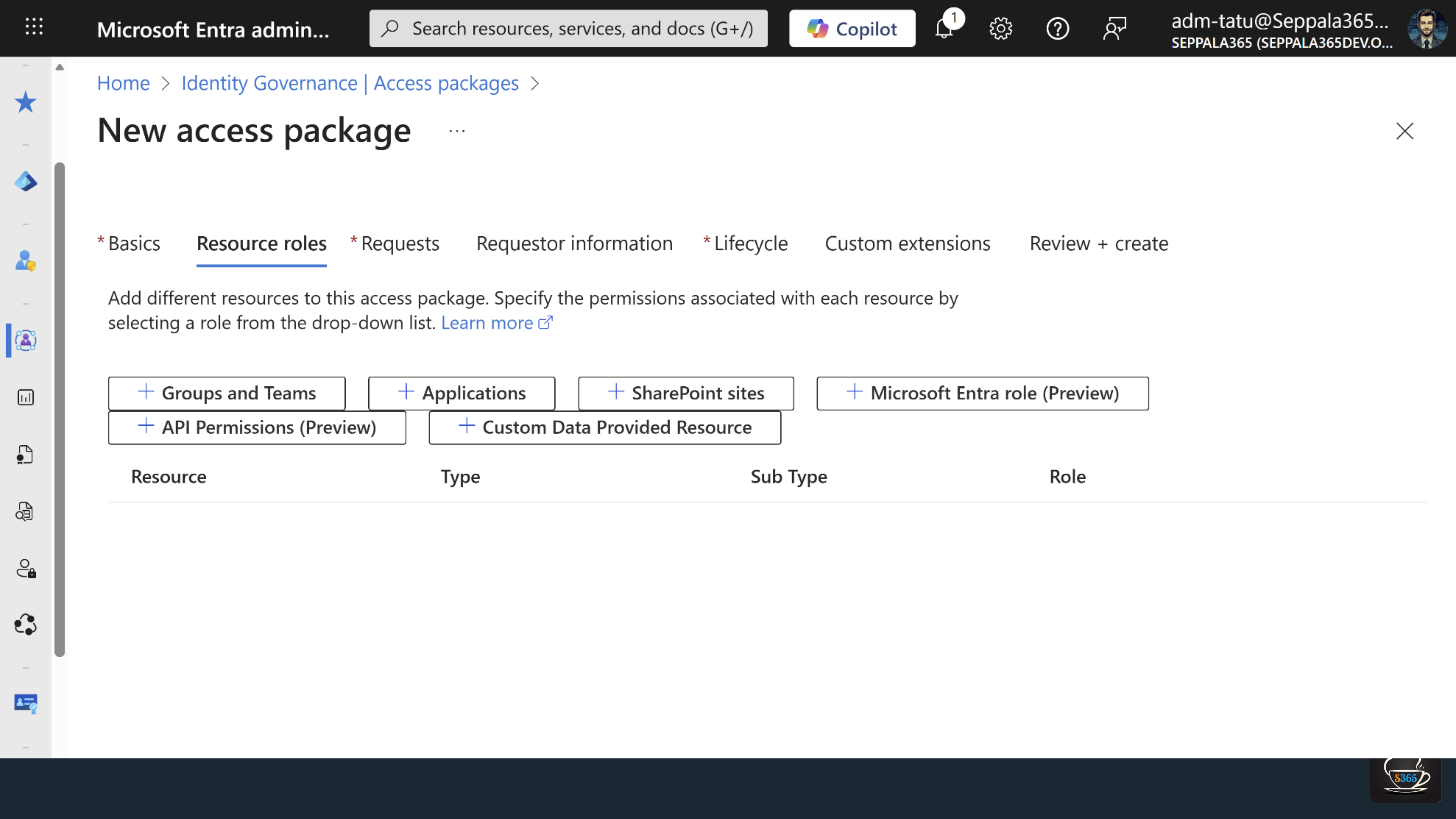
Enabled for external users: ○ Yes ● No



Access package

Create a collection of resources that users can request access to.

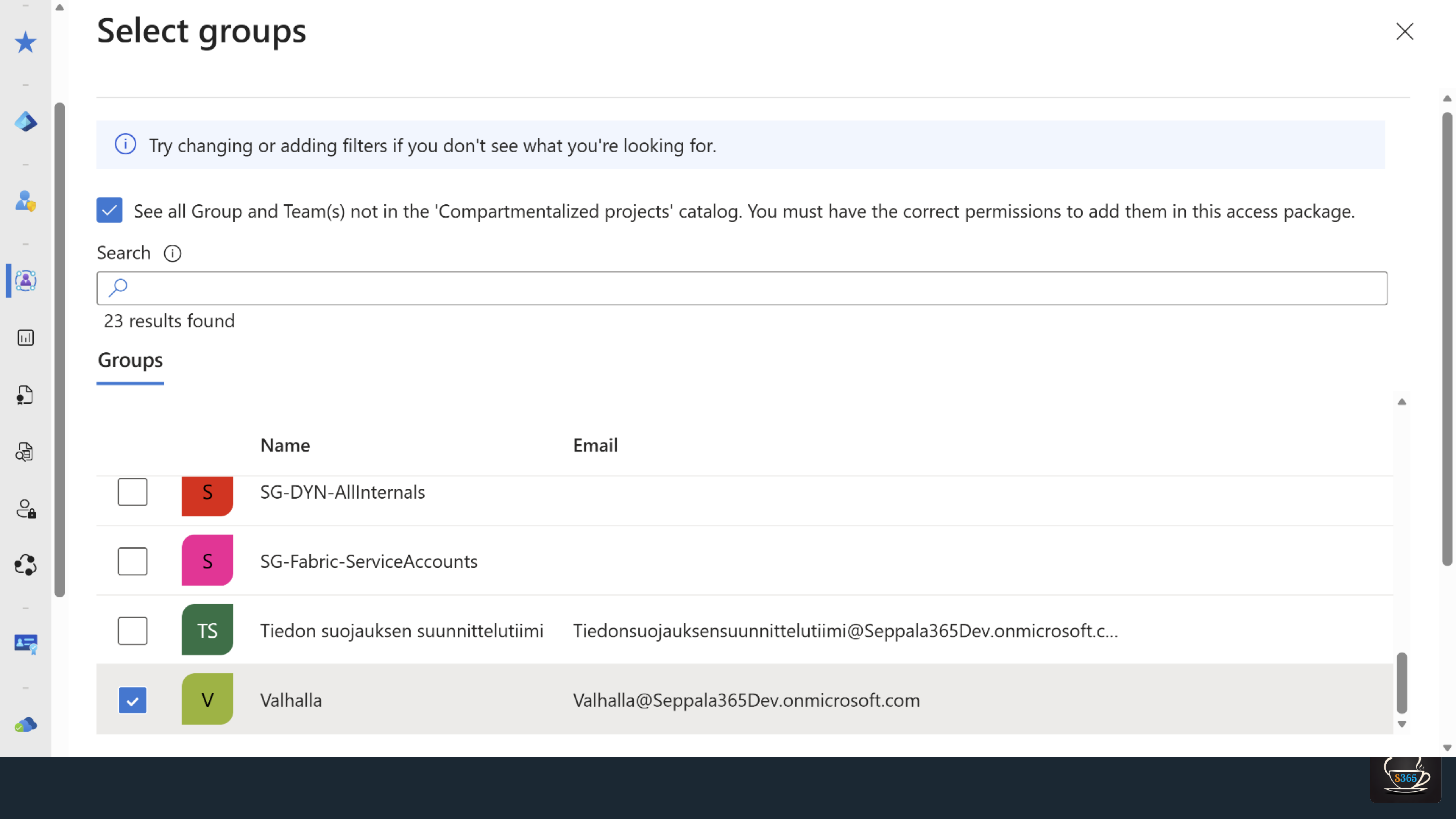
Name *	CPRJ-1257
Description *	Access to materials for CPRJ-1257
Catalog *	Compartmentalized projects


Microsoft Entra admin...
Search resources, services, and docs (G+/)
Copilot
1
adm-tatu@Seppala365...
SEPPALA365 (SEPPALA365DEV.O...
Home > Identity Governance | Access packages >
...
* Basics
Resource roles
* Requests
Requestor information
* Lifecycle
Custom extensions
Review + create
+ Groups and Teams
+ Applications
+ SharePoint sites
+ Microsoft Entra role (Preview)
+ API Permissions (Preview)
+ Custom Data Provided Resource
S365

New access package

Add different resources to this access package. Specify the permissions associated with each resource by selecting a role from the drop-down list. Learn more

Resource	Type	Sub Type	Role



Select groups

Try changing or adding filters if you don't see what you're looking for.

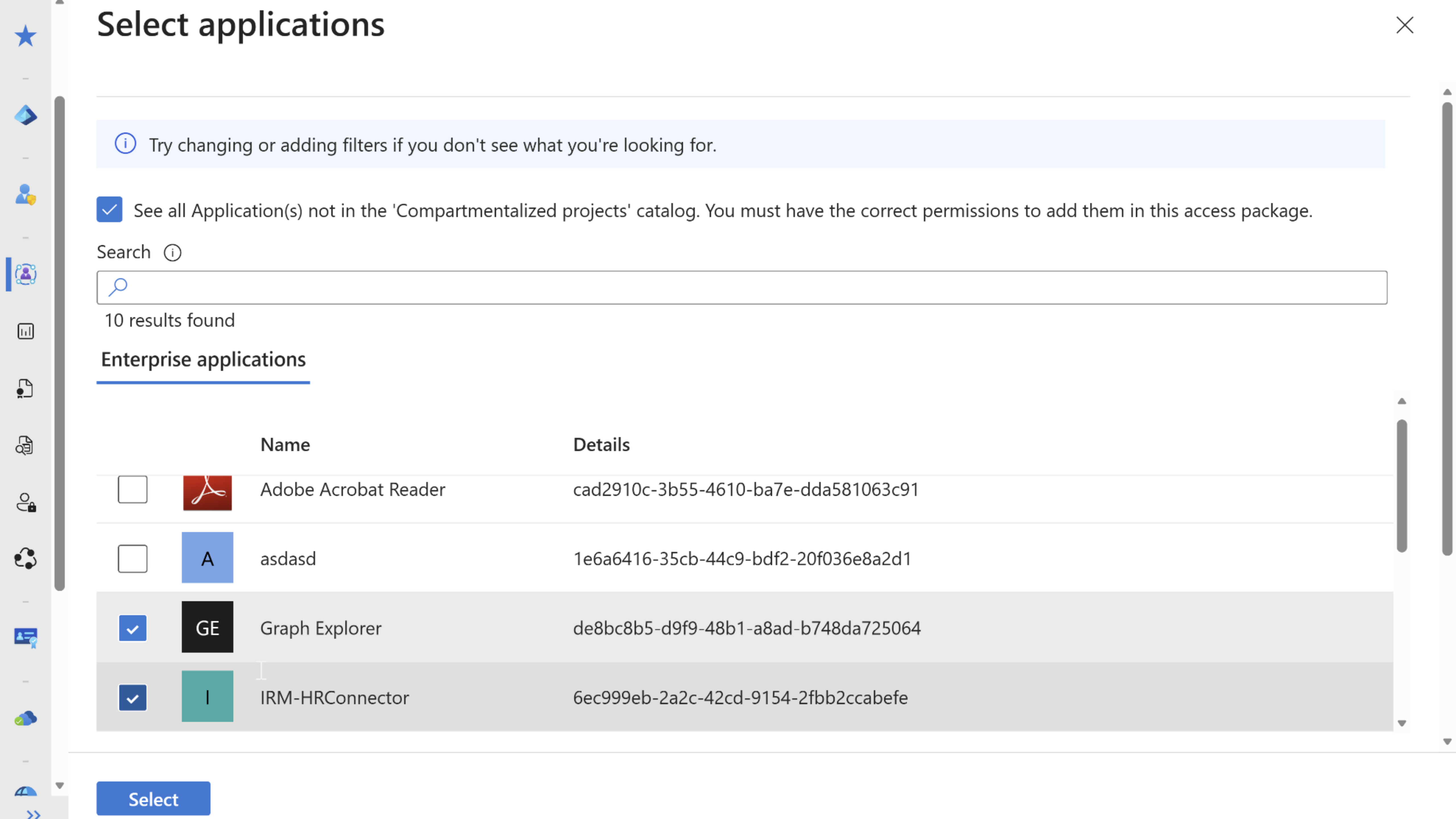
☑ See all Group and Team(s) not in the 'Compartmentalized projects' catalog. You must have the correct permissions to add them in this access package.

Search

23 results found

Groups

		Name	Email
□	S	SG-DYN-AllInternals	
□	S	SG-Fabric-ServiceAccounts	
□	TS	Tiedon suojauksen suunnittelutiimi	Tiedonsuojauksensuunnittelutiimi@Seppala365Dev.onmicrosoft.c...
☑	V	Valhalla	Valhalla@Seppala365Dev.onmicrosoft.com



Select applications

Try changing or adding filters if you don't see what you're looking for.

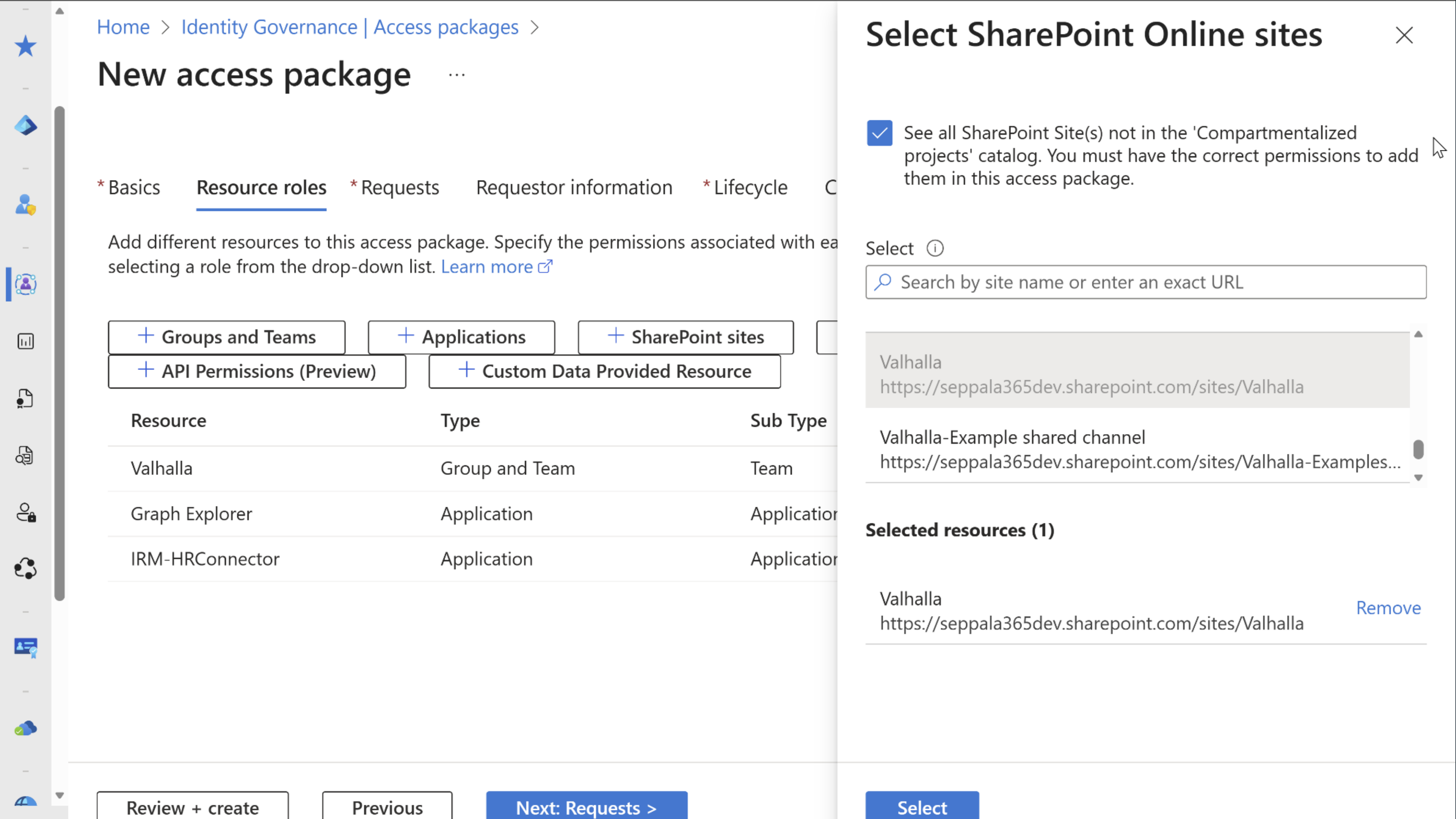
☑ See all Application(s) not in the 'Compartmentalized projects' catalog. You must have the correct permissions to add them in this access package.

Search

10 results found

Enterprise applications

		Name	Details
□		Adobe Acrobat Reader	cad2910c-3b55-4610-ba7e-dda581063c91
□	A	asdasd	1e6a6416-35cb-44c9-bdf2-20f036e8a2d1
☑	GE	Graph Explorer	de8bc8b5-d9f9-48b1-a8ad-b748da725064
☑	I	IRM-HRConnector	6ec999eb-2a2c-42cd-9154-2fbb2ccabefe



Home > Identity Governance | Access packages >

New access package ...

* Basics | Resource roles | * Requests | Requestor information | * Lifecycle | C

Add different resources to this access package. Specify the permissions associated with ea
selecting a role from the drop-down list. Learn more

Resource	Type	Sub Type
Valhalla	Group and Team	Team
Graph Explorer	Application	Applicatior
IRM-HRConnector	Application	Applicatior

Select SharePoint Online sites

☑ See all SharePoint Site(s) not in the 'Compartmentalized projects' catalog. You must have the correct permissions to add them in this access package.

Select ⓘ

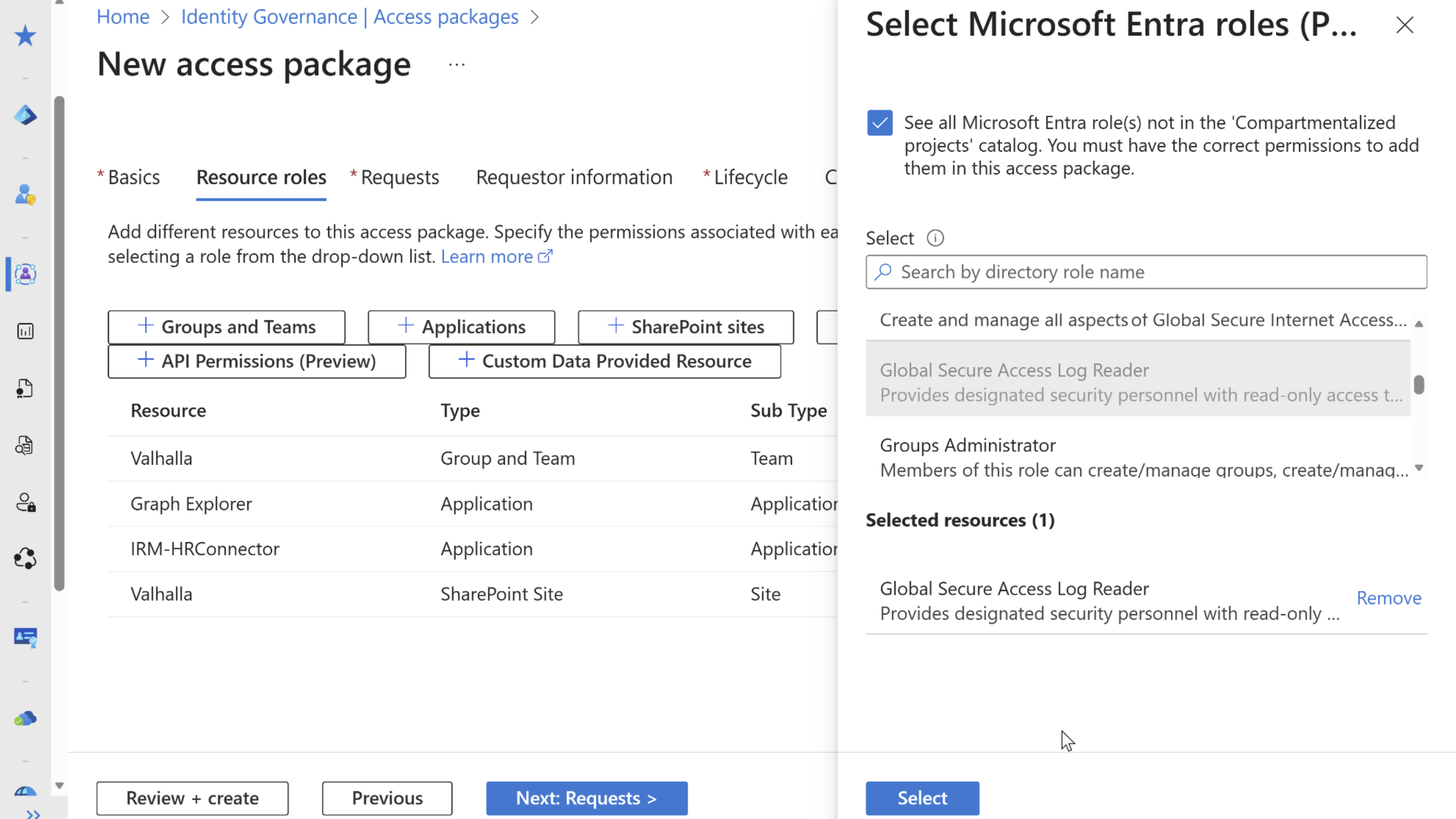
Search by site name or enter an exact URL

Valhalla
https://seppala365dev.sharepoint.com/sites/Valhalla

Valhalla-Example shared channel
https://seppala365dev.sharepoint.com/sites/Valhalla-Examples...

Selected resources (1)

Valhalla
https://seppala365dev.sharepoint.com/sites/Valhalla
Remove



Add different resources to this access package. Specify the permissions associated with ea selecting a role from the drop-down list. Learn more

Resource	Type	Sub Type
Valhalla	Group and Team	Team
Graph Explorer	Application	Applicatior
IRM-HRConnector	Application	Applicatior
Valhalla	SharePoint Site	Site

☑ See all Microsoft Entra role(s) not in the 'Compartmentalized projects' catalog. You must have the correct permissions to add them in this access package.

Select ⓘ

Search by directory role name

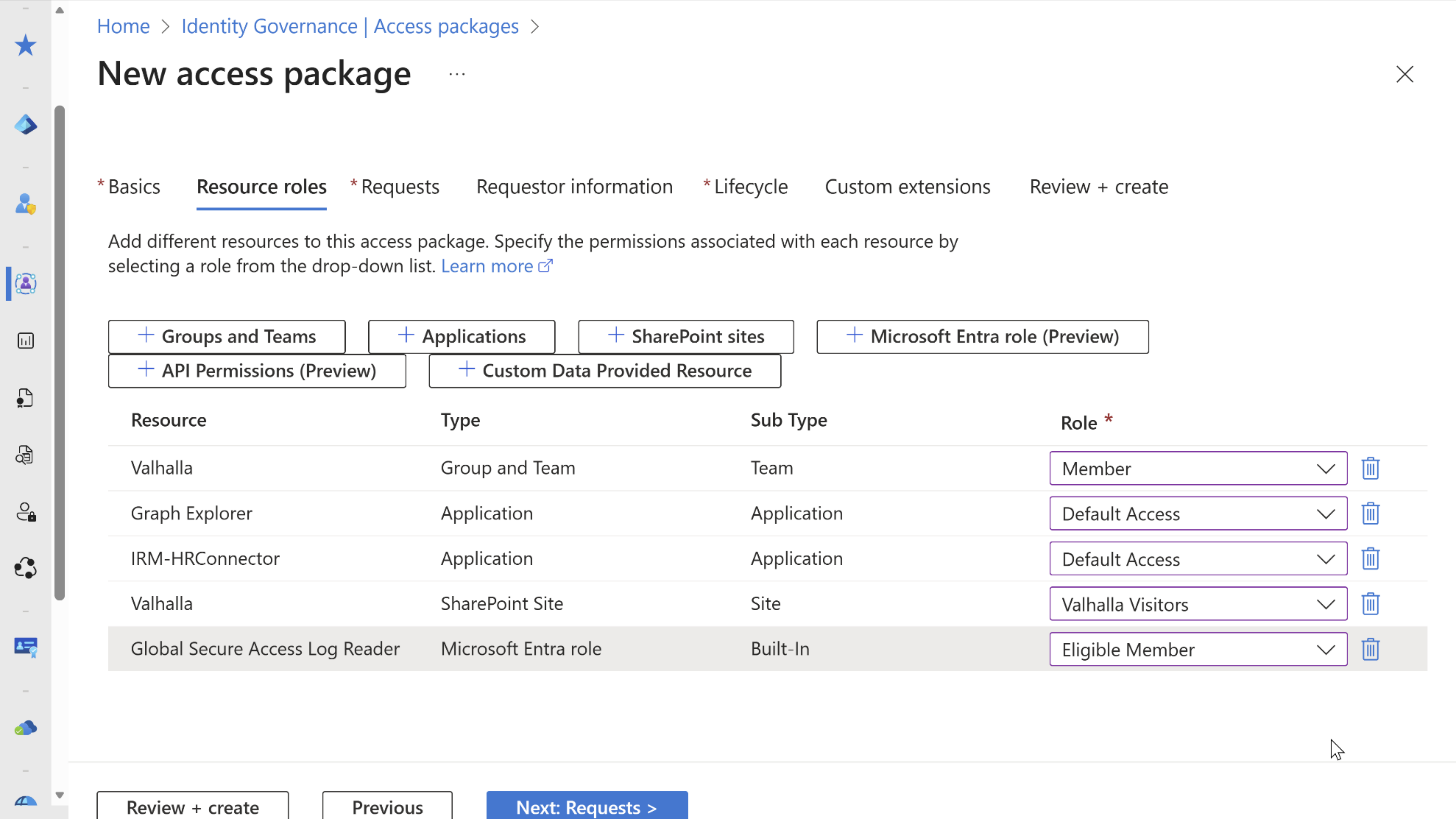
Create and manage all aspects of Global Secure Internet Access...

Global Secure Access Log Reader
Provides designated security personnel with read-only access t...

Groups Administrator
Members of this role can create/manage groups, create/manag...

Selected resources (1)

Global Secure Access Log Reader
Provides designated security personnel with read-only ...

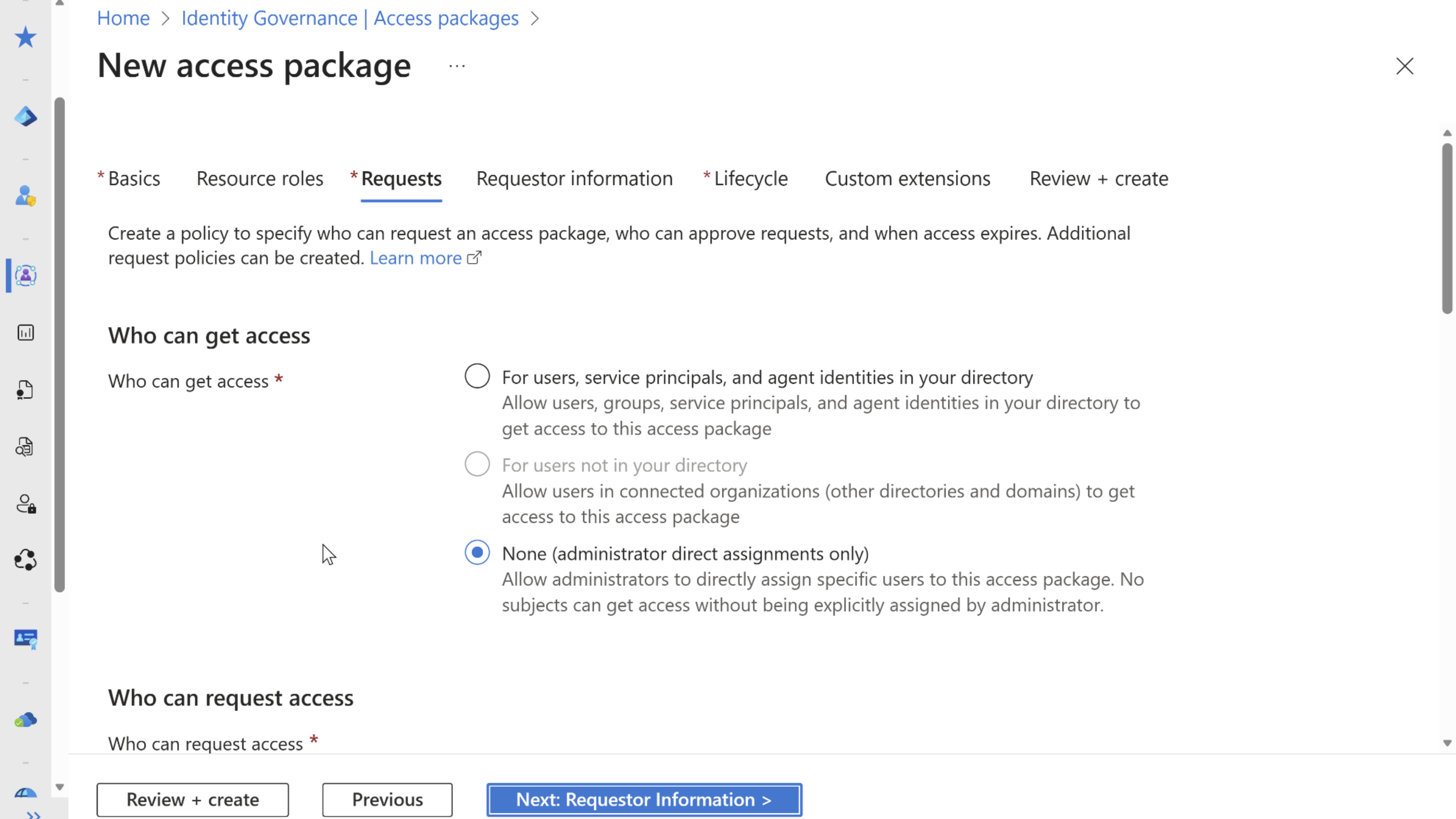


New access package

Add different resources to this access package. Specify the permissions associated with each resource by selecting a role from the drop-down list. Learn more

+ Groups and Teams
+ Applications
+ SharePoint sites
+ Microsoft Entra role (Preview)
+ API Permissions (Preview)
+ Custom Data Provided Resource

Resource	Type	Sub Type	Role *
Valhalla	Group and Team	Team	Member
Graph Explorer	Application	Application	Default Access
IRM-HRConnector	Application	Application	Default Access
Valhalla	SharePoint Site	Site	Valhalla Visitors
Global Secure Access Log Reader	Microsoft Entra role	Built-In	Eligible Member



Home > Identity Governance | Access packages >

New access package ···

* Basics | Resource roles | * **Requests** | Requestor information | * Lifecycle | Custom extensions | Review + create

Create a policy to specify who can request an access package, who can approve requests, and when access expires. Additional request policies can be created. Learn more

Who can get access

Who can get access *

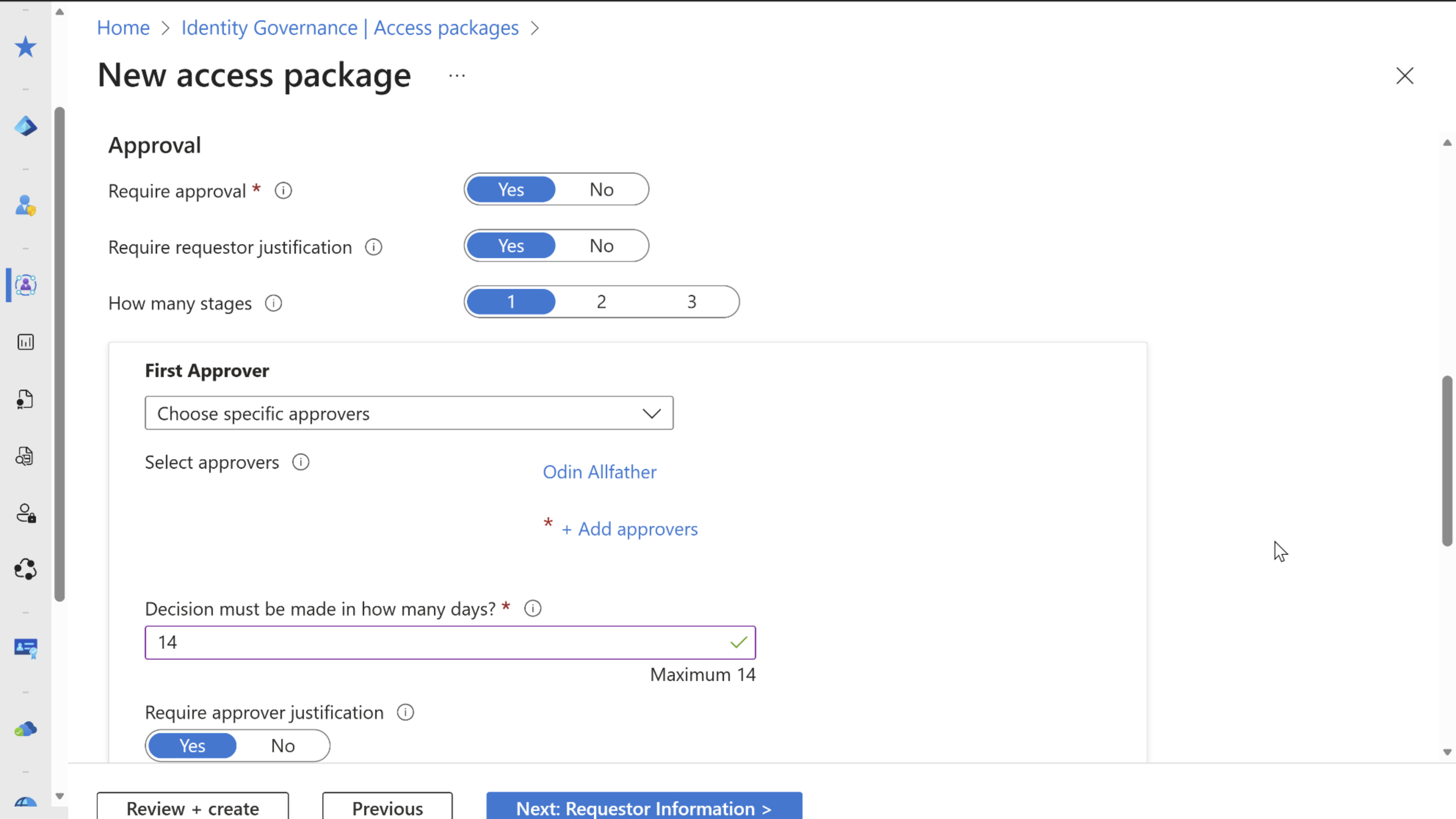
○ For users, service principals, and agent identities in your directory
Allow users, groups, service principals, and agent identities in your directory to get access to this access package

○ For users not in your directory
Allow users in connected organizations (other directories and domains) to get access to this access package

● None (administrator direct assignments only)
Allow administrators to directly assign specific users to this access package. No subjects can get access without being explicitly assigned by administrator.

Who can request access

Who can request access *


Home > Identity Governance | Access packages >

New access package

Approval

Require approval * ● Yes ○ No

Require requestor justification ● Yes ○ No

How many stages ● 1 ○ 2 ○ 3

First Approver

Choose specific approvers

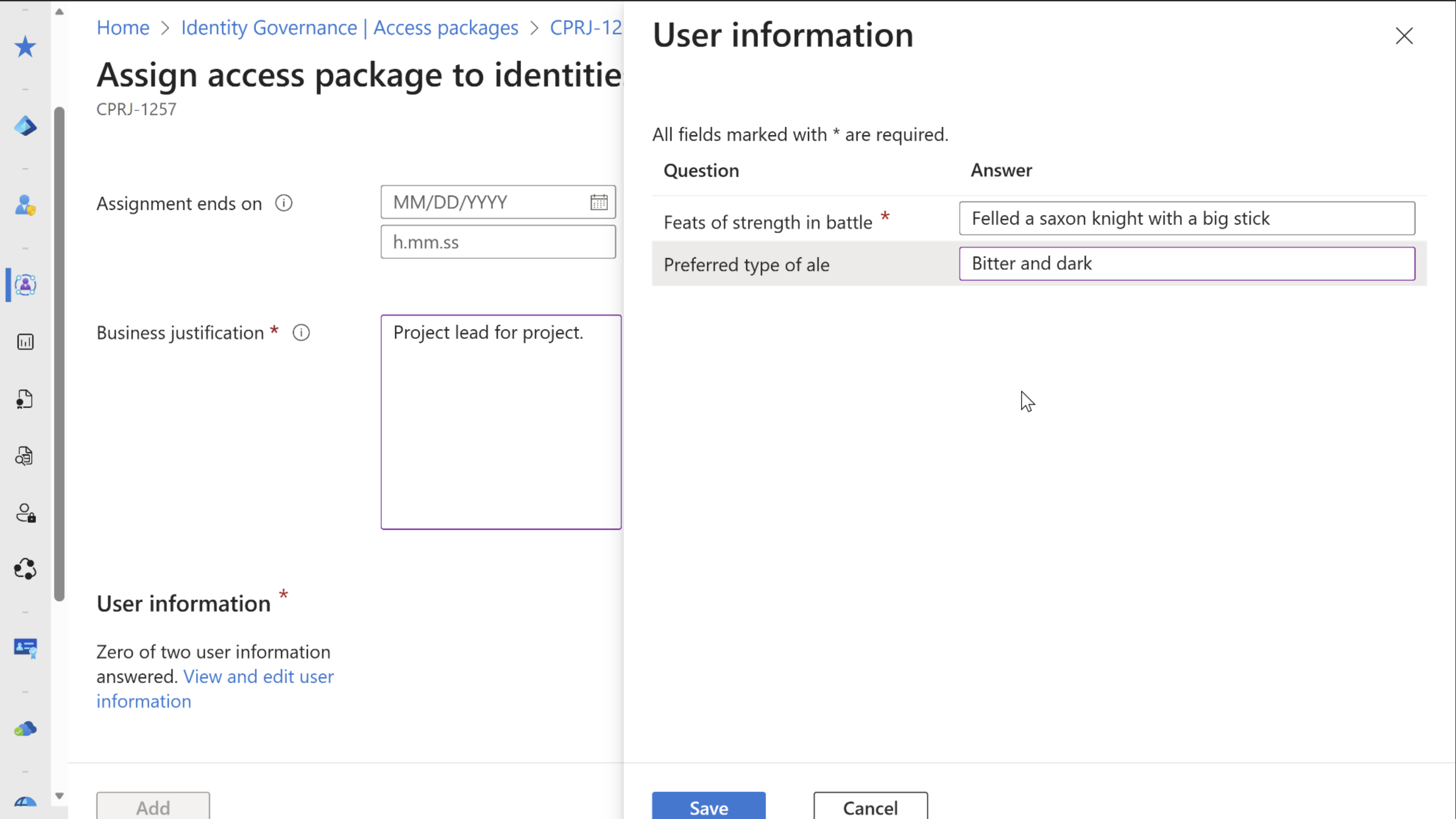
Select approvers: Odin Allfather

Decision must be made in how many days? * 14

Maximum 14

Require approver justification ● Yes ○ No

Review + create
Previous
Next: Requestor Information >



Assign access package to identitie

CPRJ-1257

Assignment ends on: MM/DD/YYYY, h.mm.ss

Business justification *: Project lead for project.

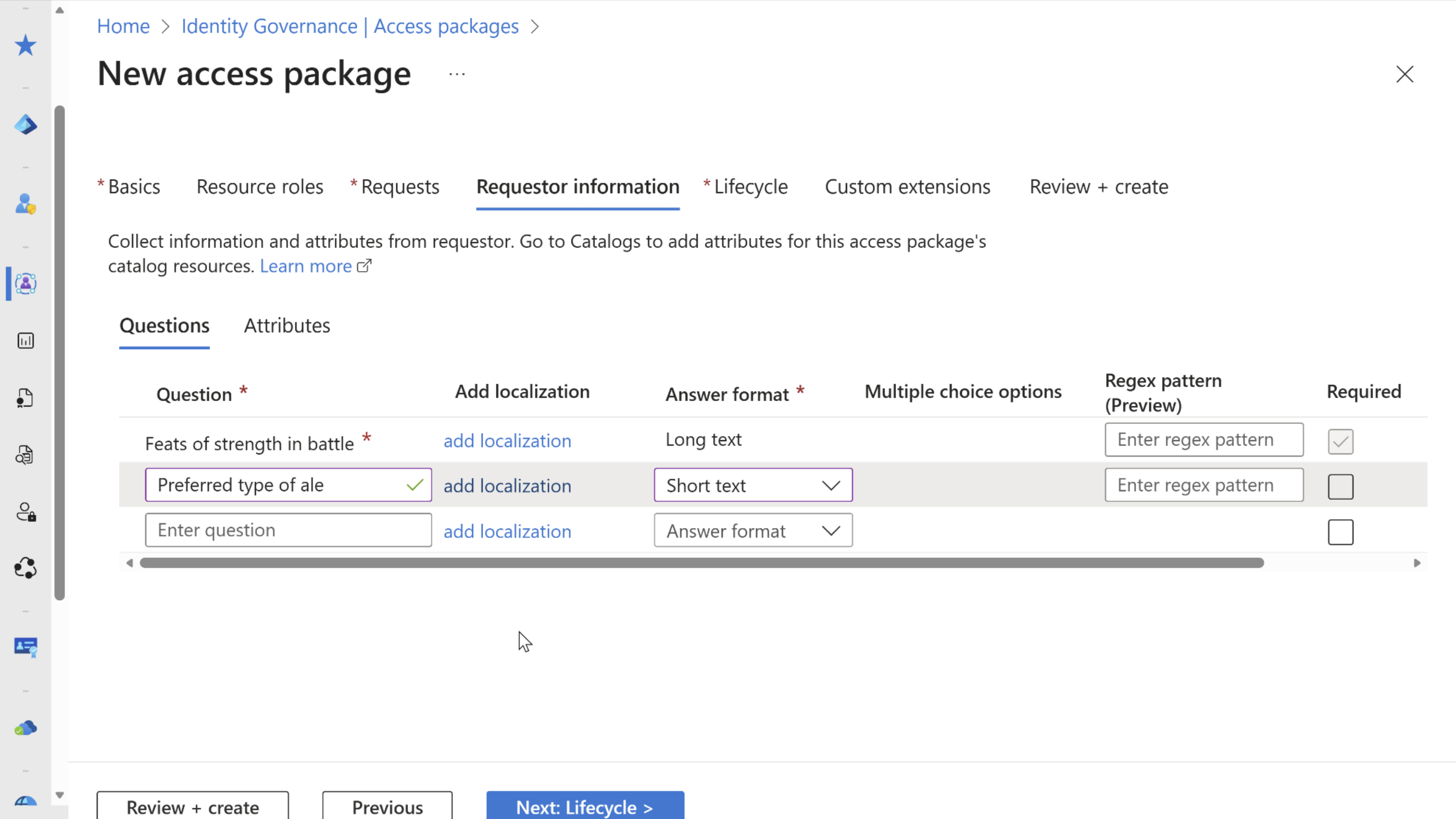
User information *

Zero of two user information answered. View and edit user information

User information

All fields marked with * are required.

Question	Answer
Feats of strength in battle *	Felled a saxon knight with a big stick
Preferred type of ale	Bitter and dark



Home > Identity Governance | Access packages >

New access package ···

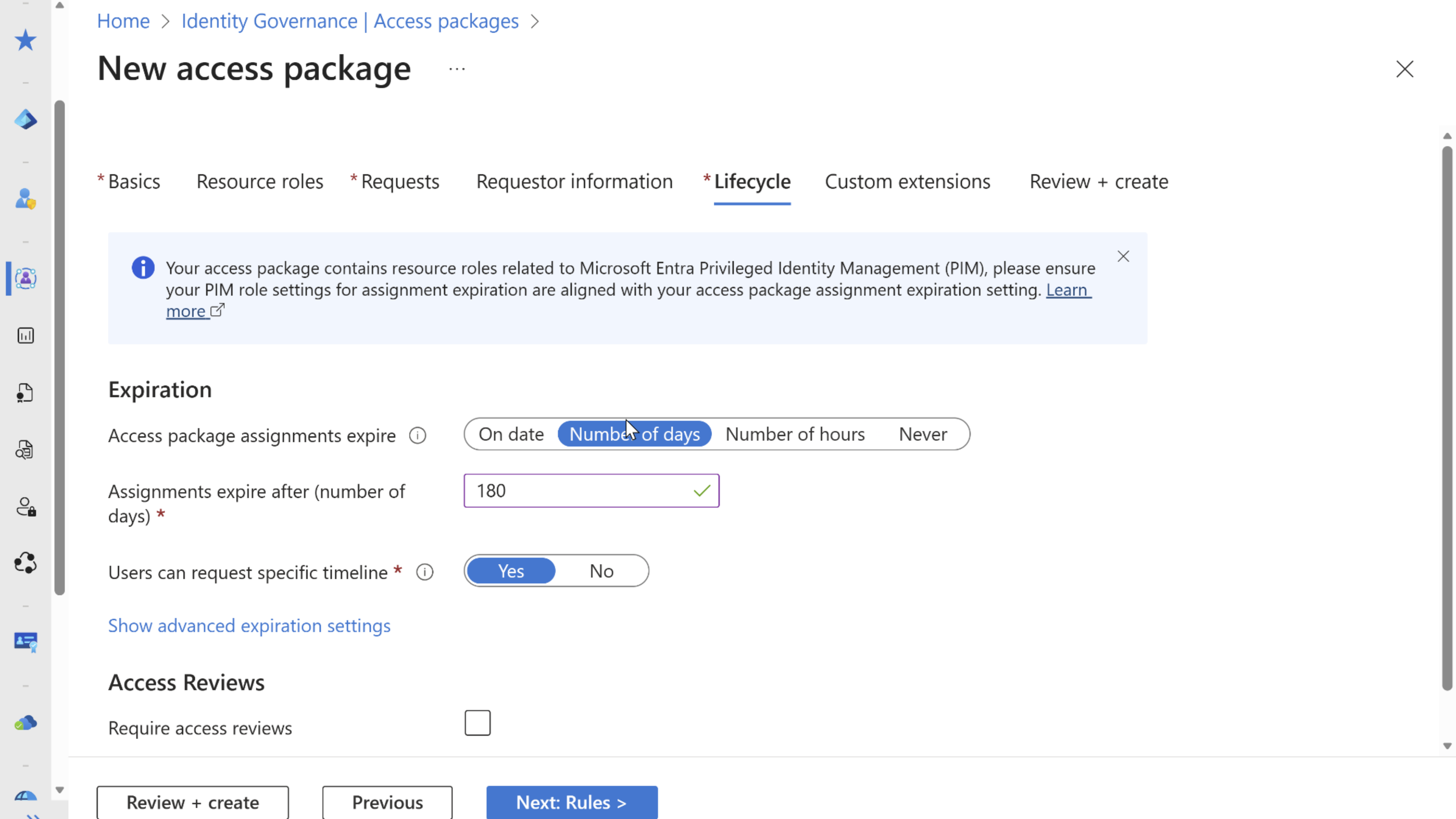
* Basics | Resource roles | * Requests | **Requestor information** | * Lifecycle | Custom extensions | Review + create

Collect information and attributes from requestor. Go to Catalogs to add attributes for this access package's catalog resources. Learn more

Questions | Attributes

Question *	Add localization	Answer format *	Multiple choice options	Regex pattern (Preview)	Required
Feats of strength in battle *	add localization	Long text		Enter regex pattern	☑
Preferred type of ale ✓	add localization	Short text ⌄		Enter regex pattern	□
Enter question	add localization	Answer format ⌄			□

Review + create | Previous | Next: Lifecycle >



Home > Identity Governance | Access packages >

New access package ···

* Basics | Resource roles | * Requests | Requestor information | * **Lifecycle** | Custom extensions | Review + create

Your access package contains resource roles related to Microsoft Entra Privileged Identity Management (PIM), please ensure your PIM role settings for assignment expiration are aligned with your access package assignment expiration setting. Learn more

Expiration

Access package assignments expire: On date [✓ Number of days] Number of hours Never

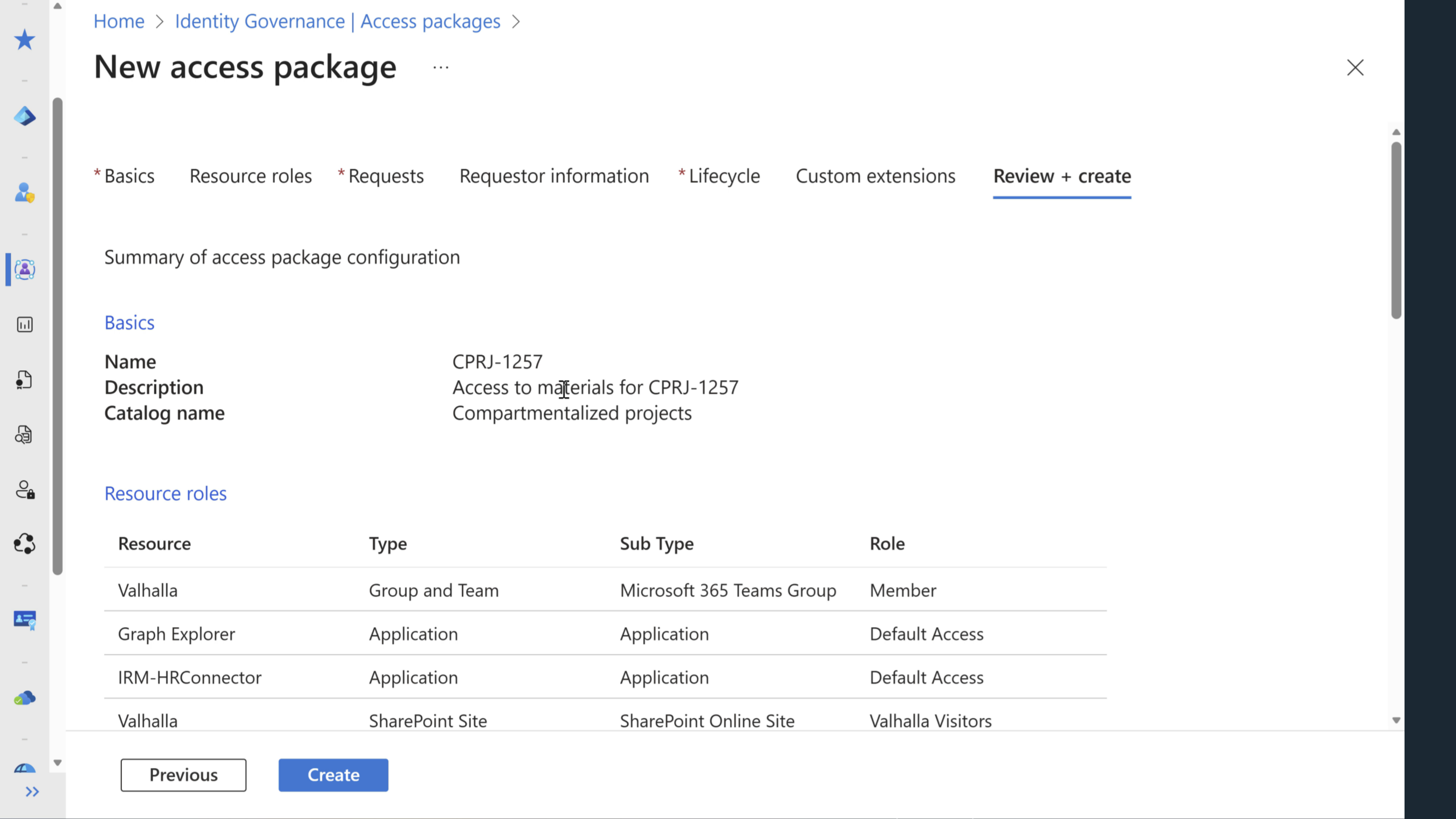
Assignments expire after (number of days) *: 180 ✓

Users can request specific timeline *: [✓ Yes] No

Show advanced expiration settings

Access Reviews

Require access reviews ☐



New access package

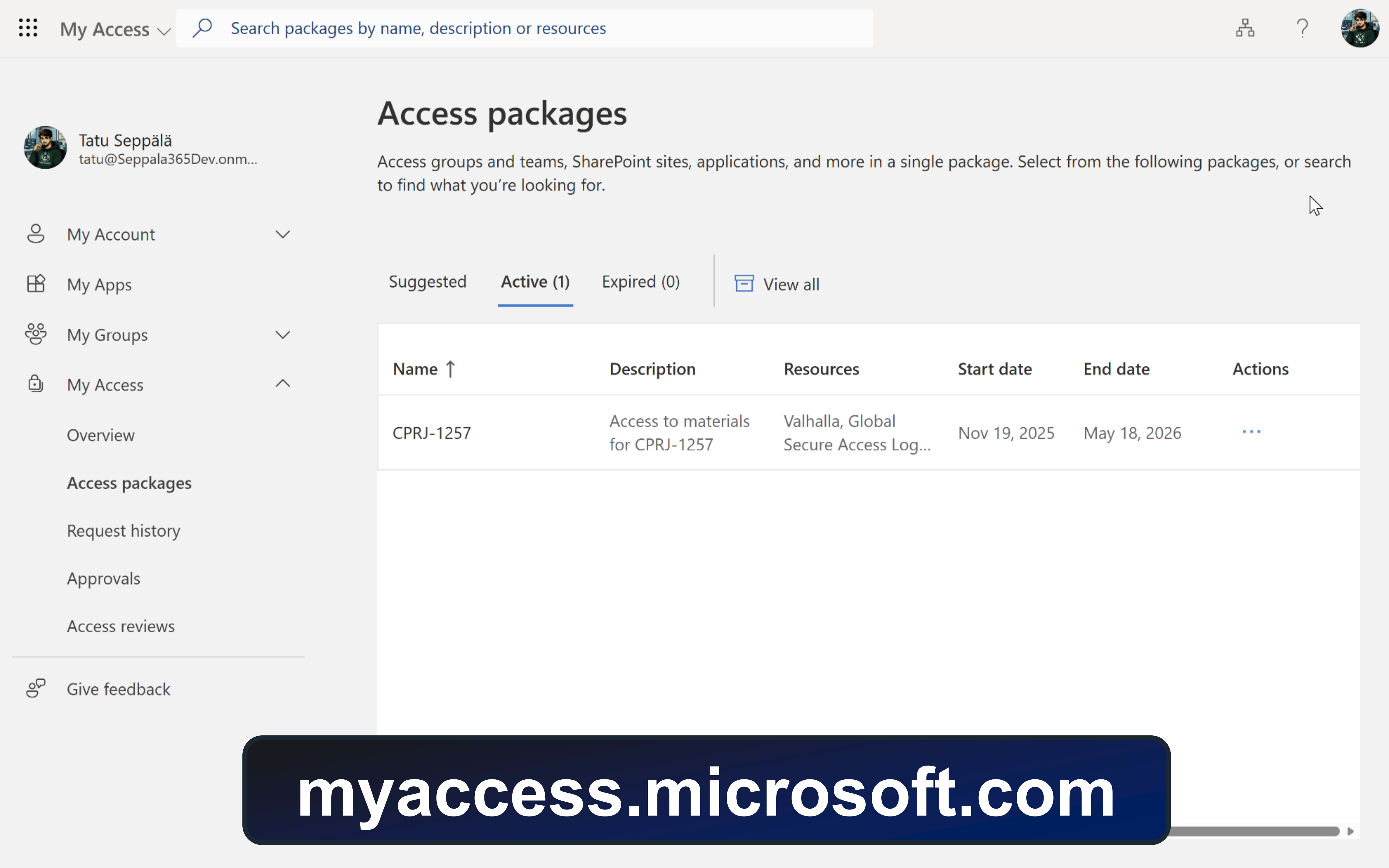
Summary of access package configuration

Basics

Name	CPRJ-1257
Description	Access to materials for CPRJ-1257
Catalog name	Compartmentalized projects

Resource roles

Resource	Type	Sub Type	Role
Valhalla	Group and Team	Microsoft 365 Teams Group	Member
Graph Explorer	Application	Application	Default Access
IRM-HRConnector	Application	Application	Default Access
Valhalla	SharePoint Site	SharePoint Online Site	Valhalla Visitors

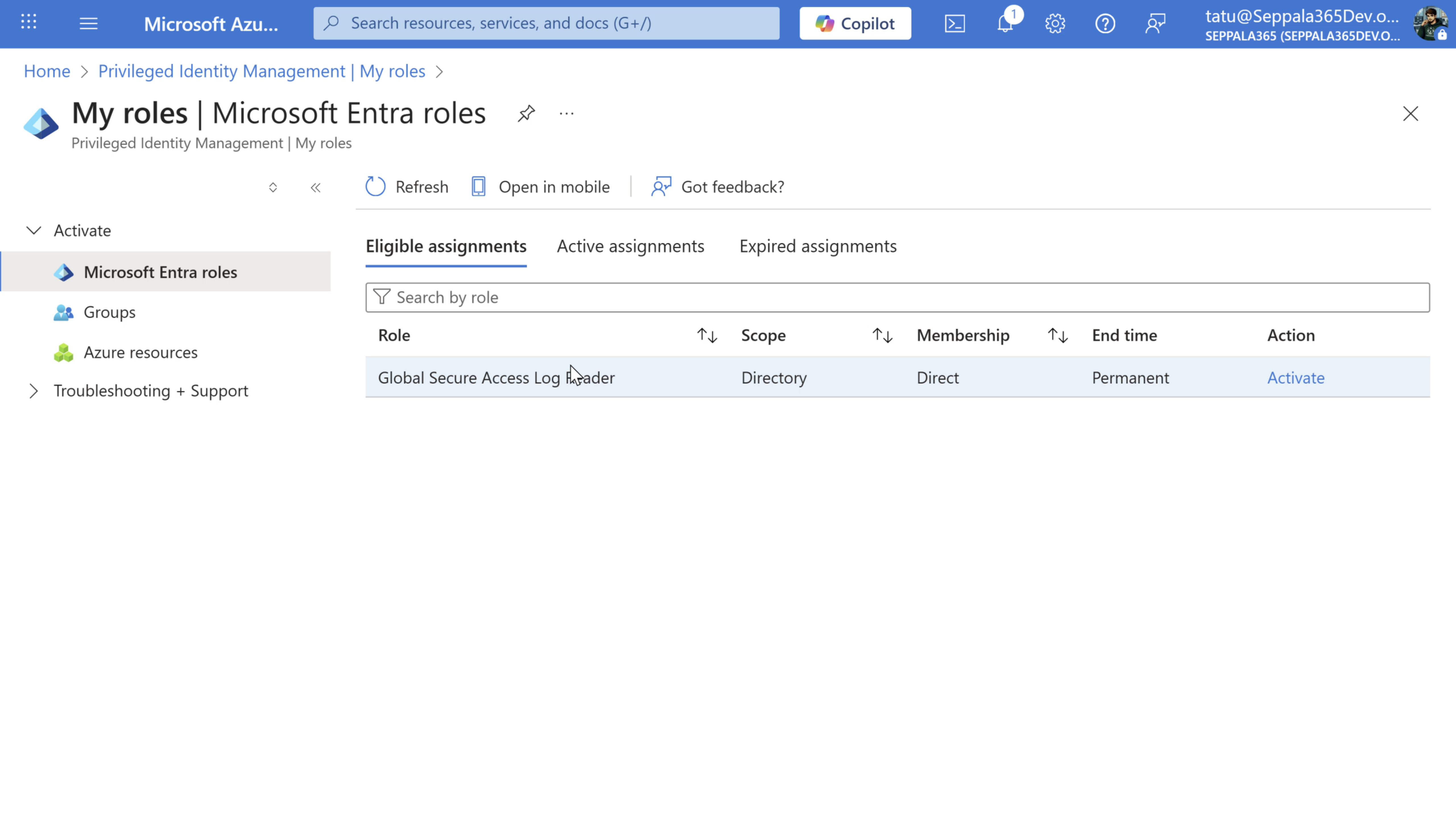


Access packages

Access groups and teams, SharePoint sites, applications, and more in a single package. Select from the following packages, or search to find what you're looking for.

Name ↑	Description	Resources	Start date	End date	Actions
CPRJ-1257	Access to materials for CPRJ-1257	Valhalla, Global Secure Access Log...	Nov 19, 2025	May 18, 2026	···

myaccess.microsoft.com



My roles | Microsoft Entra roles

Privileged Identity Management | My roles

Role	Scope	Membership	End time	Action
Global Secure Access Log Reader	Directory	Direct	Permanent	Activate

💊 First aid

- Limit access to compartmentalized information with **access packages** and encrypting **sensitivity labels**
- Mandate monitored **Privileged Access Workstations** for admin tasks
- Deploy **Insider Risk Management** to detect and investigate anomalous content access and collection patterns

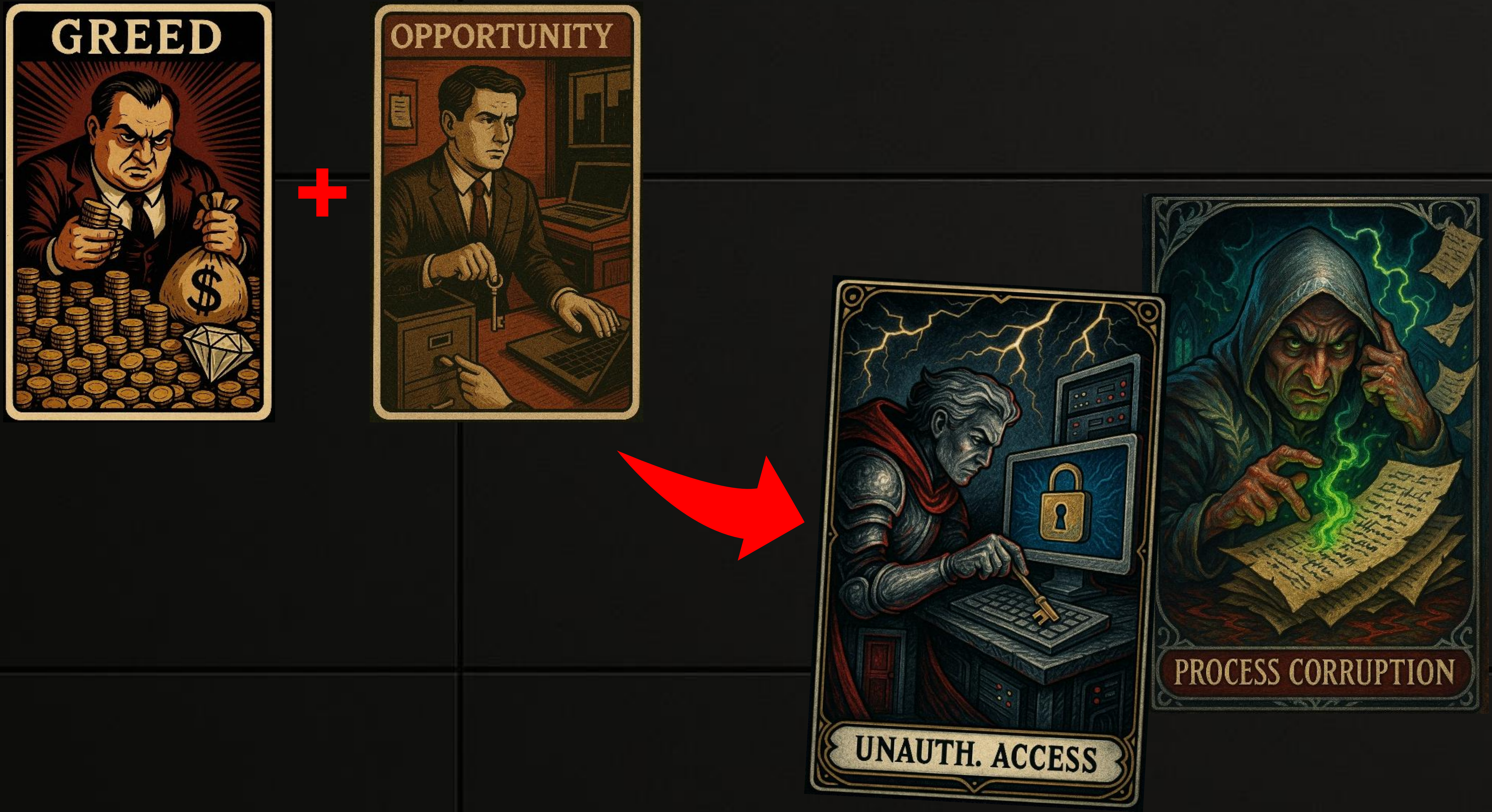
CrowdStrike (11/25)

- Company insider shared screenshots on internal Okta systems with threat actor *Scattered Lapsus$ Hunters*
- Initial info says threat actor offered $25,000 to the insider to provide access to Crowdstrike network
- Threat actor received SSO auth cookies from insider but they had already been detected & access had been removed
- Primary motivator: **Greed?**

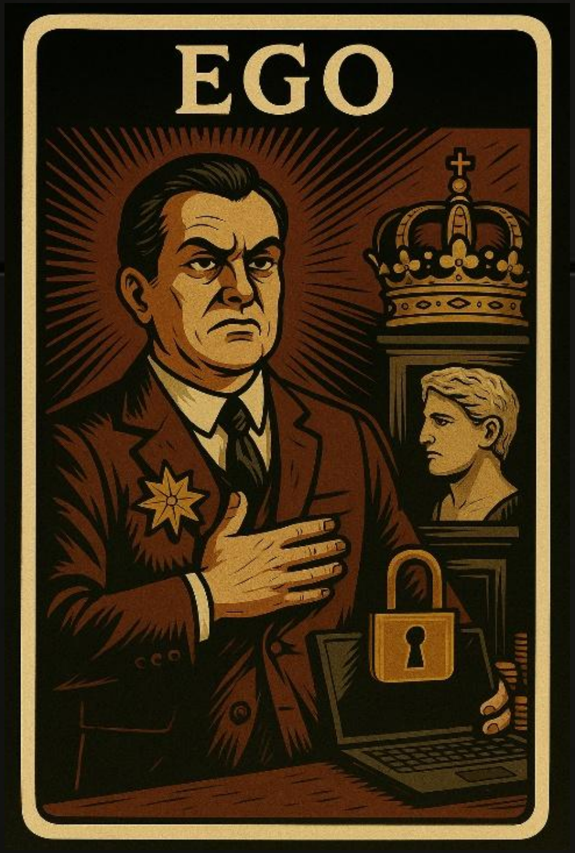
“We made a critical mistake. We assumed that outsider external threats were different in kind than insider threats.

My view today is they are exactly the same.”

Chris Inglis
Former deputy director, NSA


GREED
+
OPPORTUNITY
UNAUTH. ACCESS
PROCESS CORRUPTION

IDEOLOGY



EGO

UNAUTH. DISCLOSURE

EGO
+
REVENGE
FACILITATION OF 3P ACCESS
IT / PHYSICAL SABOTAGE

Connecting the dots 🕵️

It’s all about 🔎 indicators

Technical

- Mass download / exfiltration of sensitive data
- Unjustified escalation of privileges
- Anomalous access patterns
- Physical access attempts after termination or job level change

Behavioral

- Excessive absences
- Anomalous working hours
- Anti-social behavior
- Bypassing instructions
- Poor performance
- Untruthfulness / lies

Audit logging

Indicator event source tier list

Device events

Microsoft 365 / Office events

Critical

Defender for Endpoint security events

Power BI & Fabric events

OK

Defender for Cloud Apps
Risky browsing
Physical access
Health record access

Situational

Device events

Onboard devices to Microsoft Purview!

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

...

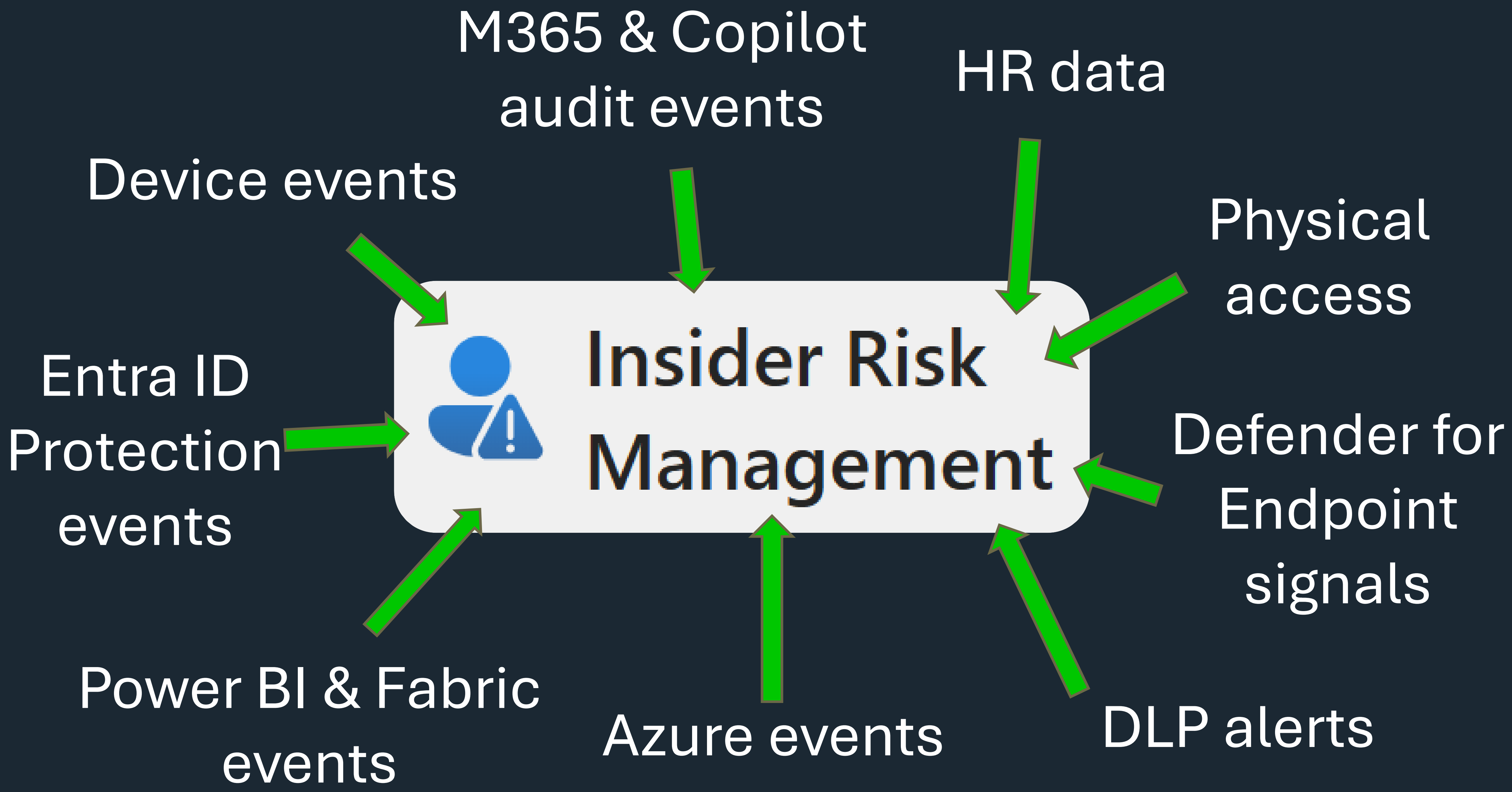
Most data is exfiltrated w/ these

Microsoft 365 / Office events

- Downloading content from SharePoint / OneDrive
  - Especially to unmanaged devices
- Downgrading or removing sensitivity labels
- Accessing sensitive documents
- Sending email with attachments to personal accts.

…

Most exfil sequences start w/ these



Insider Risk Management

M365 & Copilot audit events

HR data

Physical access

Defender for Endpoint signals

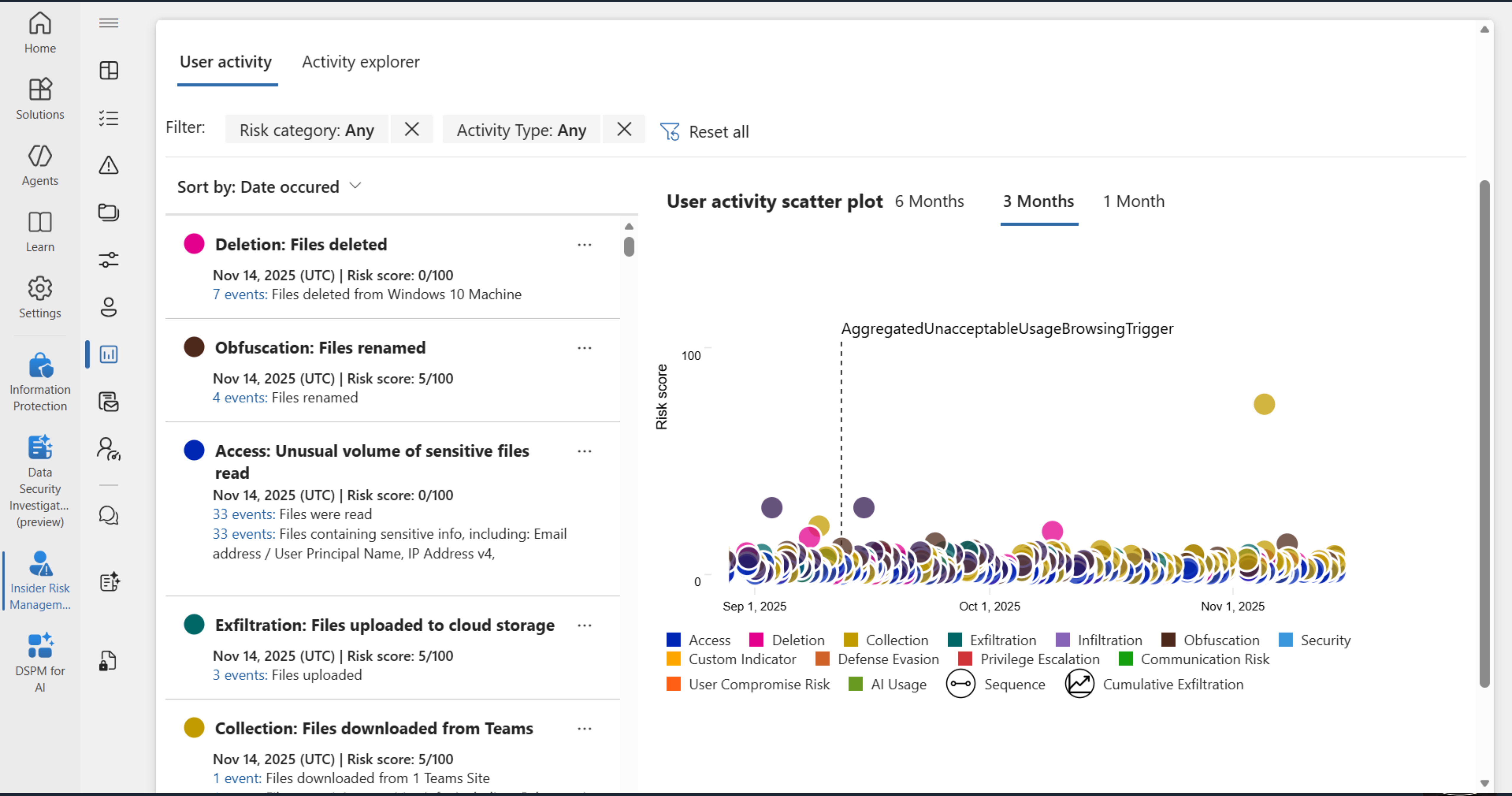
DLP alerts

Azure events

Power BI & Fabric events

Entra ID Protection events

Device events



User activity | Activity explorer

Filter: Risk category: Any ✕ | Activity Type: Any ✕ | Reset all

Sort by: Date occured

● **Deletion: Files deleted**
Nov 14, 2025 (UTC) | Risk score: 0/100
7 events: Files deleted from Windows 10 Machine

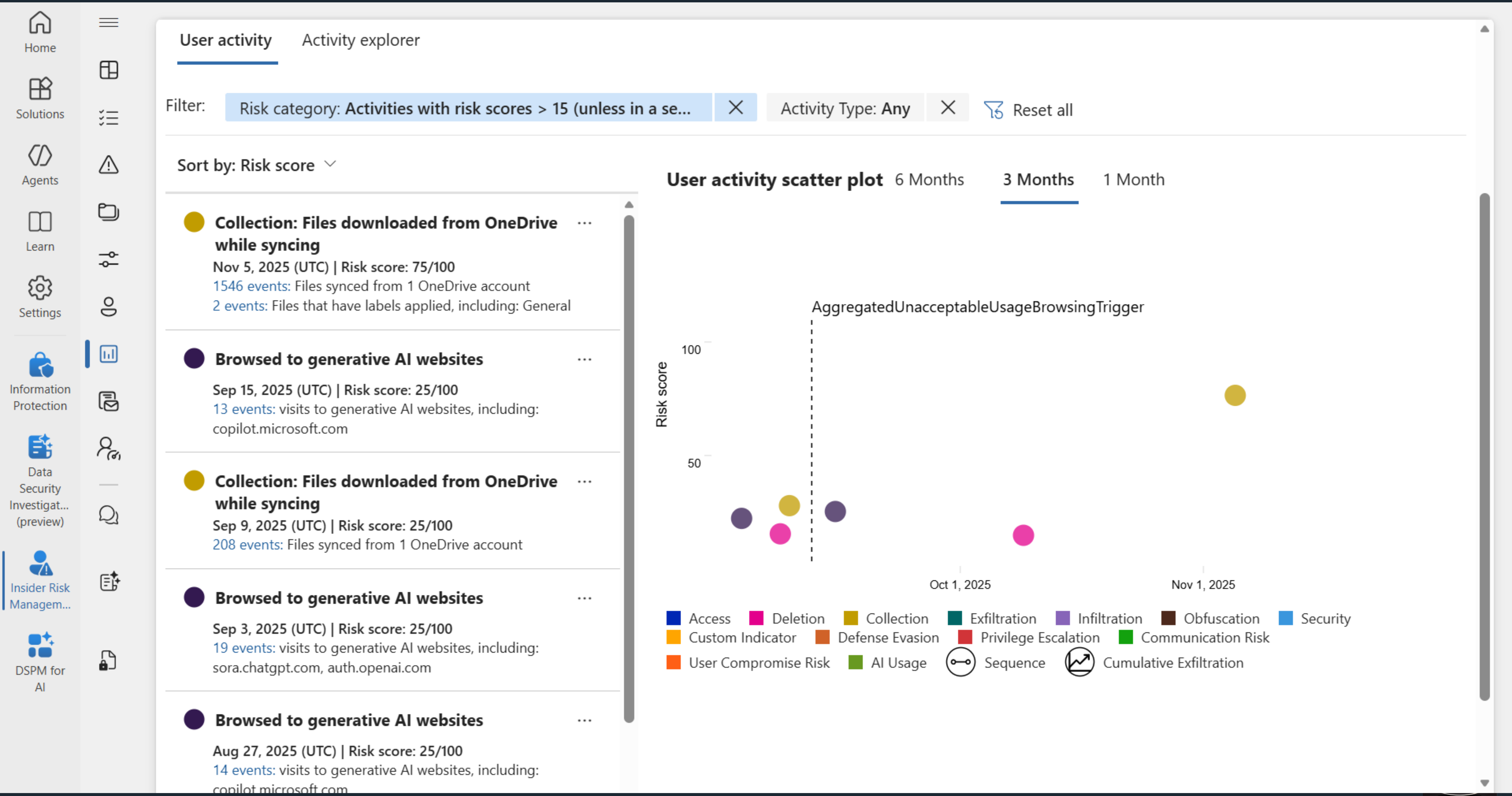
● **Obfuscation: Files renamed**
Nov 14, 2025 (UTC) | Risk score: 5/100
4 events: Files renamed

● **Access: Unusual volume of sensitive files read**
Nov 14, 2025 (UTC) | Risk score: 0/100
33 events: Files were read
33 events: Files containing sensitive info, including: Email address / User Principal Name, IP Address v4,

● **Exfiltration: Files uploaded to cloud storage**
Nov 14, 2025 (UTC) | Risk score: 5/100
3 events: Files uploaded

● **Collection: Files downloaded from Teams**
Nov 14, 2025 (UTC) | Risk score: 5/100
1 event: Files downloaded from 1 Teams Site

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



User activity | Activity explorer

Filter: Risk category: **Activities with risk scores > 15 (unless in a se...** ✕ | Activity Type: **Any** ✕ | Reset all

Sort by: Risk score ⌄

● **Collection: Files downloaded from OneDrive while syncing** ···
Nov 5, 2025 (UTC) | Risk score: 75/100
1546 events: Files synced from 1 OneDrive account
2 events: Files that have labels applied, including: General

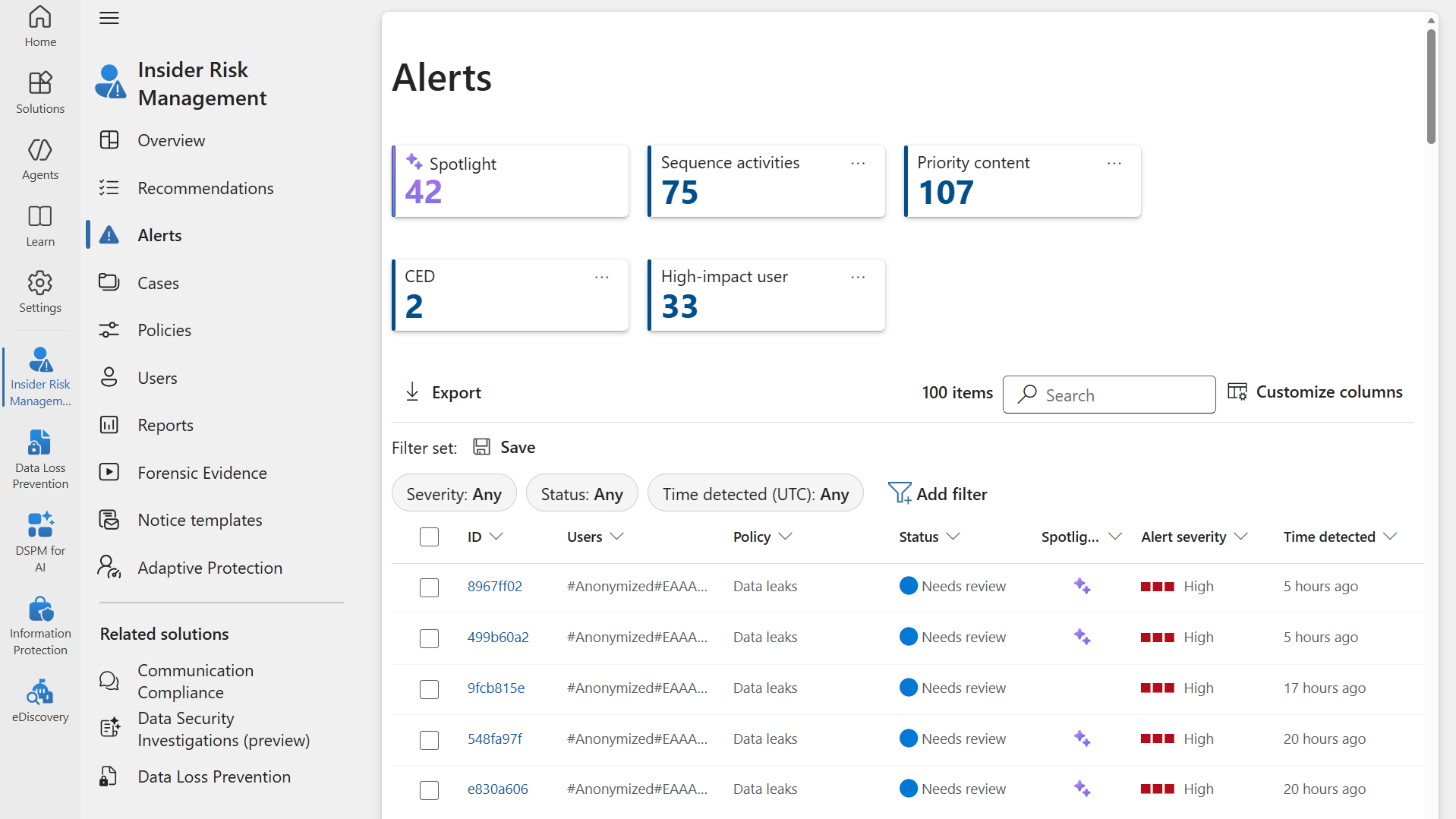
● **Browsed to generative AI websites** ···
Sep 15, 2025 (UTC) | Risk score: 25/100
13 events: visits to generative AI websites, including: copilot.microsoft.com

● **Collection: Files downloaded from OneDrive while syncing** ···
Sep 9, 2025 (UTC) | Risk score: 25/100
208 events: Files synced from 1 OneDrive account

● **Browsed to generative AI websites** ···
Sep 3, 2025 (UTC) | Risk score: 25/100
19 events: visits to generative AI websites, including: sora.chatgpt.com, auth.openai.com

● **Browsed to generative AI websites** ···
Aug 27, 2025 (UTC) | Risk score: 25/100
14 events: visits to generative AI websites, including: copilot.microsoft.com

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



Insider Risk Management

- Overview
- Recommendations
- Alerts
- Cases
- Policies
- Users
- Reports
- Forensic Evidence
- Notice templates
- Adaptive Protection

Related solutions

- Communication Compliance
- Data Security Investigations (preview)
- Data Loss Prevention

Alerts

Spotlight	42
Sequence activities	75
Priority content	107
CED	2
High-impact user	33

Export

100 items

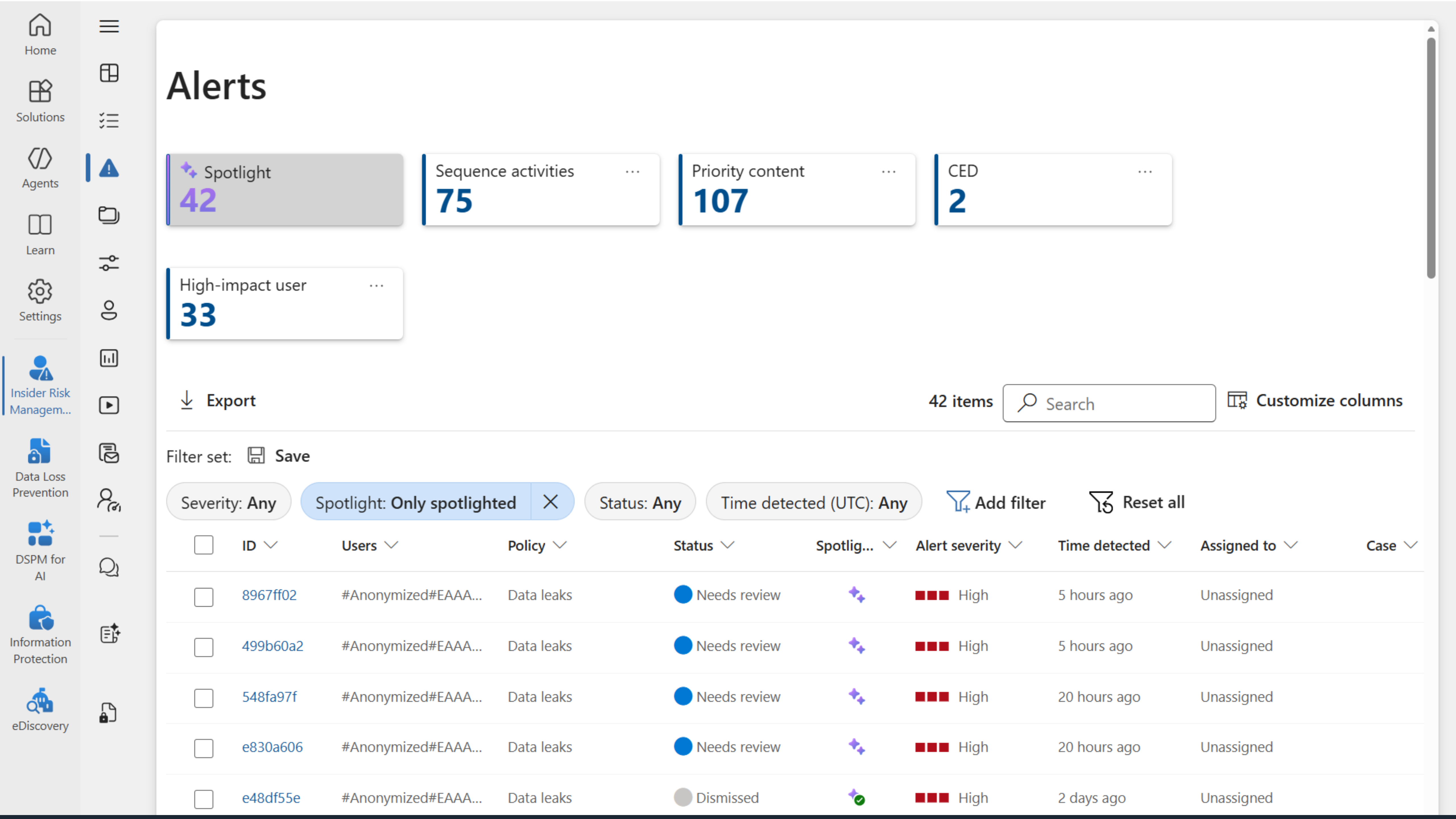
Search

Customize columns

Filter set: Save

Severity: Any | Status: Any | Time detected (UTC): Any | Add filter

□	ID	Users	Policy	Status	Spotlig...	Alert severity	Time detected
□	8967ff02	#Anonymized#EAAA...	Data leaks	● Needs review	✦	■■■ High	5 hours ago
□	499b60a2	#Anonymized#EAAA...	Data leaks	● Needs review	✦	■■■ High	5 hours ago
□	9fcb815e	#Anonymized#EAAA...	Data leaks	● Needs review		■■■ High	17 hours ago
□	548fa97f	#Anonymized#EAAA...	Data leaks	● Needs review	✦	■■■ High	20 hours ago
□	e830a606	#Anonymized#EAAA...	Data leaks	● Needs review	✦	■■■ High	20 hours ago



Alerts

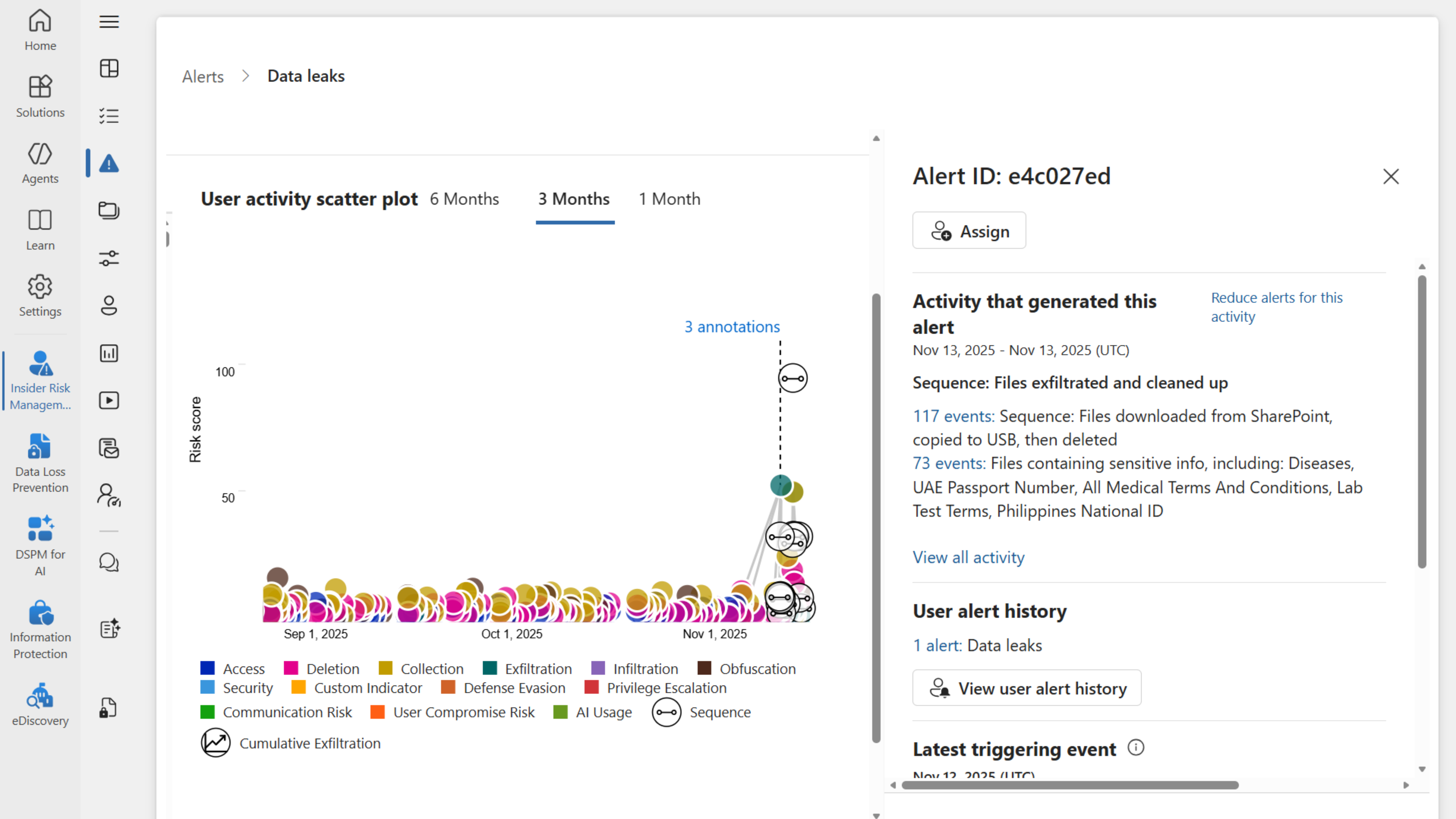
Spotlight 42	Sequence activities 75	Priority content 107	CED 2	High-impact user 33

42 items

Filter set:

Severity: Any | Spotlight: Only spotlighted ✕ | Status: Any | Time detected (UTC): Any

☐	ID	Users	Policy	Status	Spotlig...	Alert severity	Time detected	Assigned to	Case
☐	8967ff02	#Anonymized#EAAA...	Data leaks	● Needs review	✦	🟥🟥🟥 High	5 hours ago	Unassigned	
☐	499b60a2	#Anonymized#EAAA...	Data leaks	● Needs review	✦	🟥🟥🟥 High	5 hours ago	Unassigned	
☐	548fa97f	#Anonymized#EAAA...	Data leaks	● Needs review	✦	🟥🟥🟥 High	20 hours ago	Unassigned	
☐	e830a606	#Anonymized#EAAA...	Data leaks	● Needs review	✦	🟥🟥🟥 High	20 hours ago	Unassigned	
☐	e48df55e	#Anonymized#EAAA...	Data leaks	● Dismissed	✦✓	🟥🟥🟥 High	2 days ago	Unassigned	



Alert ID: e4c027ed

Assign

Activity that generated this alert

Reduce alerts for this activity

Nov 13, 2025 - Nov 13, 2025 (UTC)

Sequence: Files exfiltrated and cleaned up

117 events: Sequence: Files downloaded from SharePoint, copied to USB, then deleted

73 events: Files containing sensitive info, including: Diseases, UAE Passport Number, All Medical Terms And Conditions, Lab Test Terms, Philippines National ID

View all activity

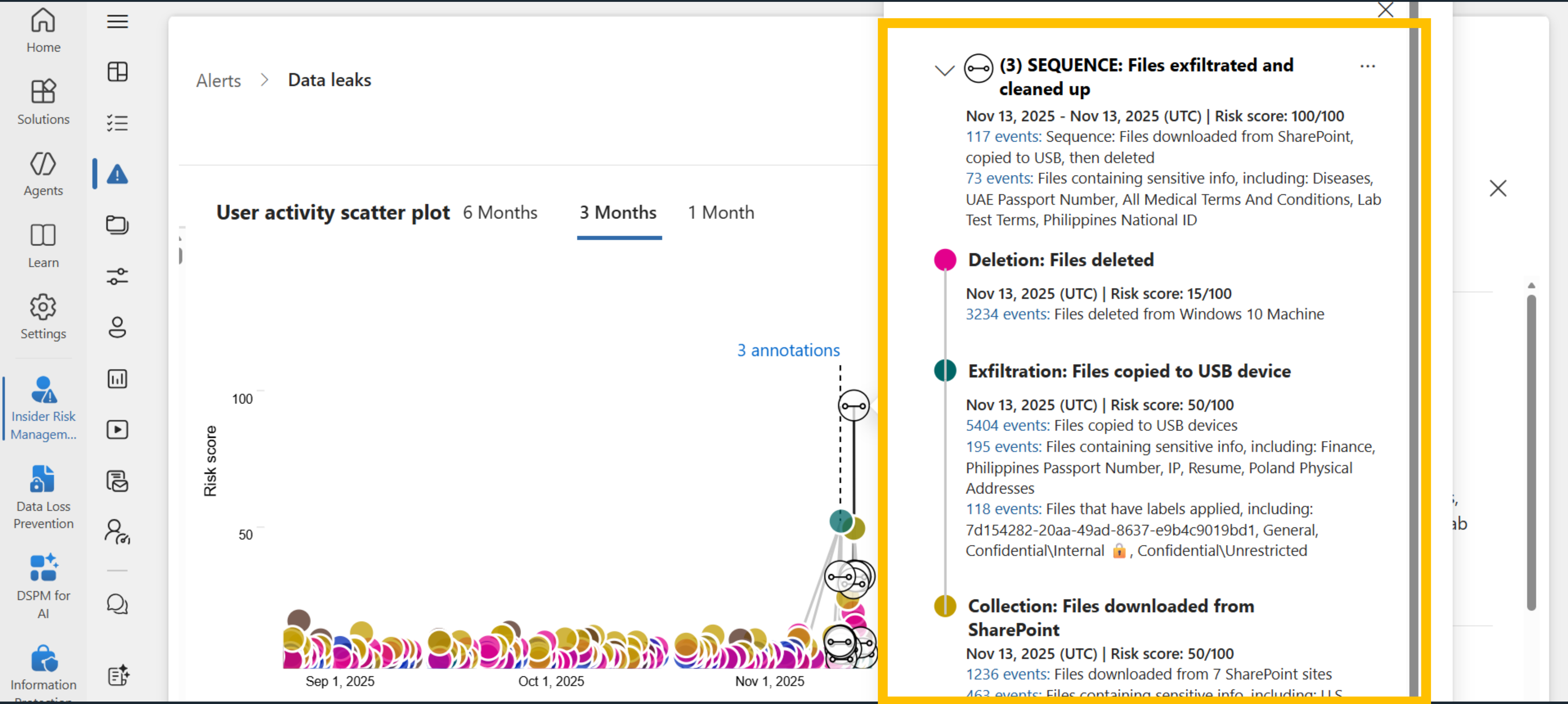
User alert history

1 alert: Data leaks

View user alert history

Latest triggering event ⓘ

Nov 13, 2025 (UTC)



(3) SEQUENCE: Files exfiltrated and cleaned up

Nov 13, 2025 - Nov 13, 2025 (UTC) | Risk score: 100/100
117 events: Sequence: Files downloaded from SharePoint, copied to USB, then deleted
73 events: Files containing sensitive info, including: Diseases, UAE Passport Number, All Medical Terms And Conditions, Lab Test Terms, Philippines National ID

Deletion: Files deleted

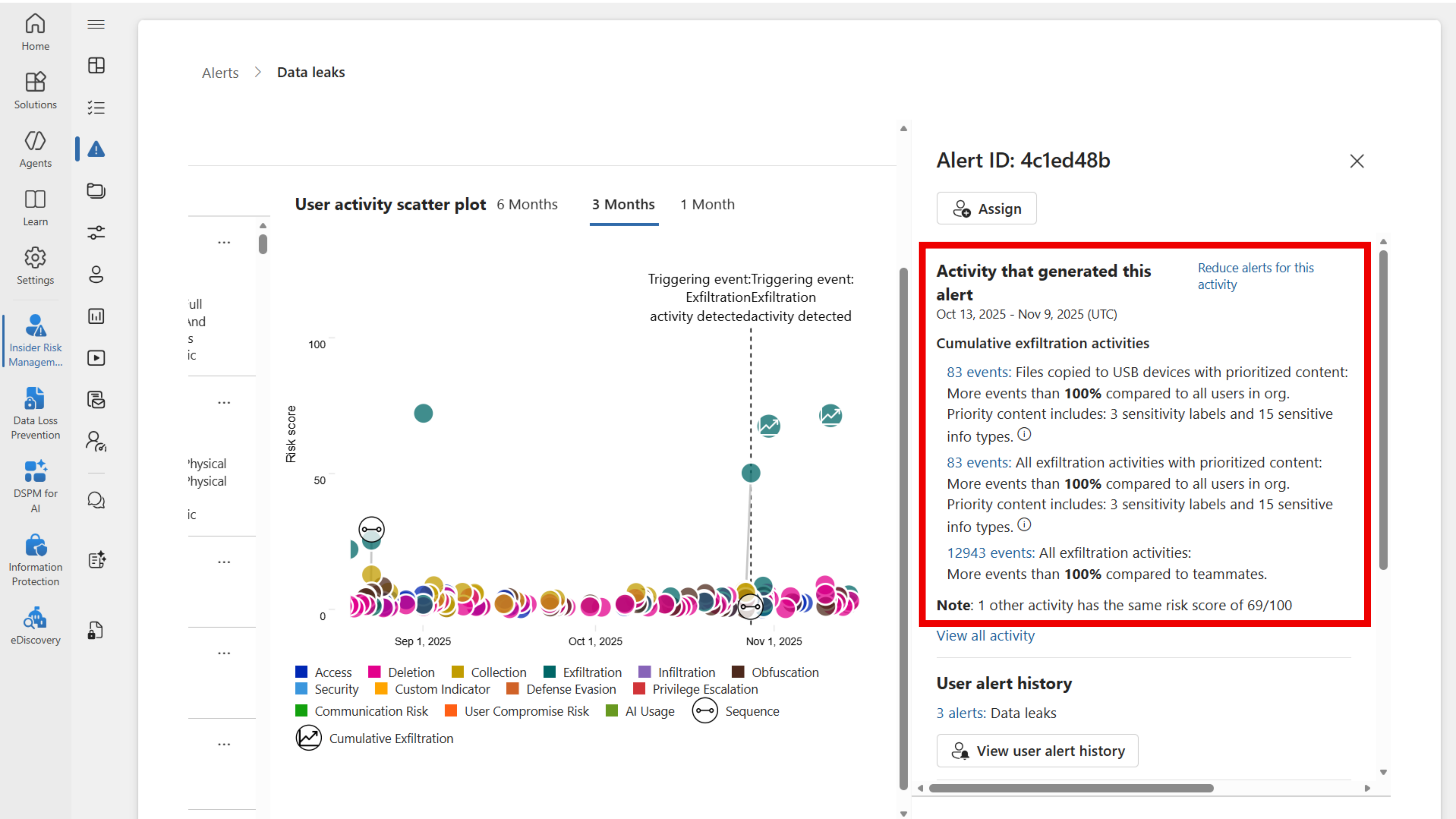
Nov 13, 2025 (UTC) | Risk score: 15/100
3234 events: Files deleted from Windows 10 Machine

Exfiltration: Files copied to USB device

Nov 13, 2025 (UTC) | Risk score: 50/100
5404 events: Files copied to USB devices
195 events: Files containing sensitive info, including: Finance, Philippines Passport Number, IP, Resume, Poland Physical Addresses
118 events: Files that have labels applied, including: 7d154282-20aa-49ad-8637-e9b4c9019bd1, General, Confidential\Internal 🔒, Confidential\Unrestricted

Collection: Files downloaded from SharePoint

Nov 13, 2025 (UTC) | Risk score: 50/100
1236 events: Files downloaded from 7 SharePoint sites
463 events: Files containing sensitive info, including: U.S.



Alert ID: 4c1ed48b

Assign

Activity that generated this alert

Reduce alerts for this activity

Oct 13, 2025 - Nov 9, 2025 (UTC)

Cumulative exfiltration activities

83 events: Files copied to USB devices with prioritized content: More events than **100%** compared to all users in org. Priority content includes: 3 sensitivity labels and 15 sensitive info types. ⓘ

83 events: All exfiltration activities with prioritized content: More events than **100%** compared to all users in org. Priority content includes: 3 sensitivity labels and 15 sensitive info types. ⓘ

12943 events: All exfiltration activities: More events than **100%** compared to teammates.

Note: 1 other activity has the same risk score of 69/100

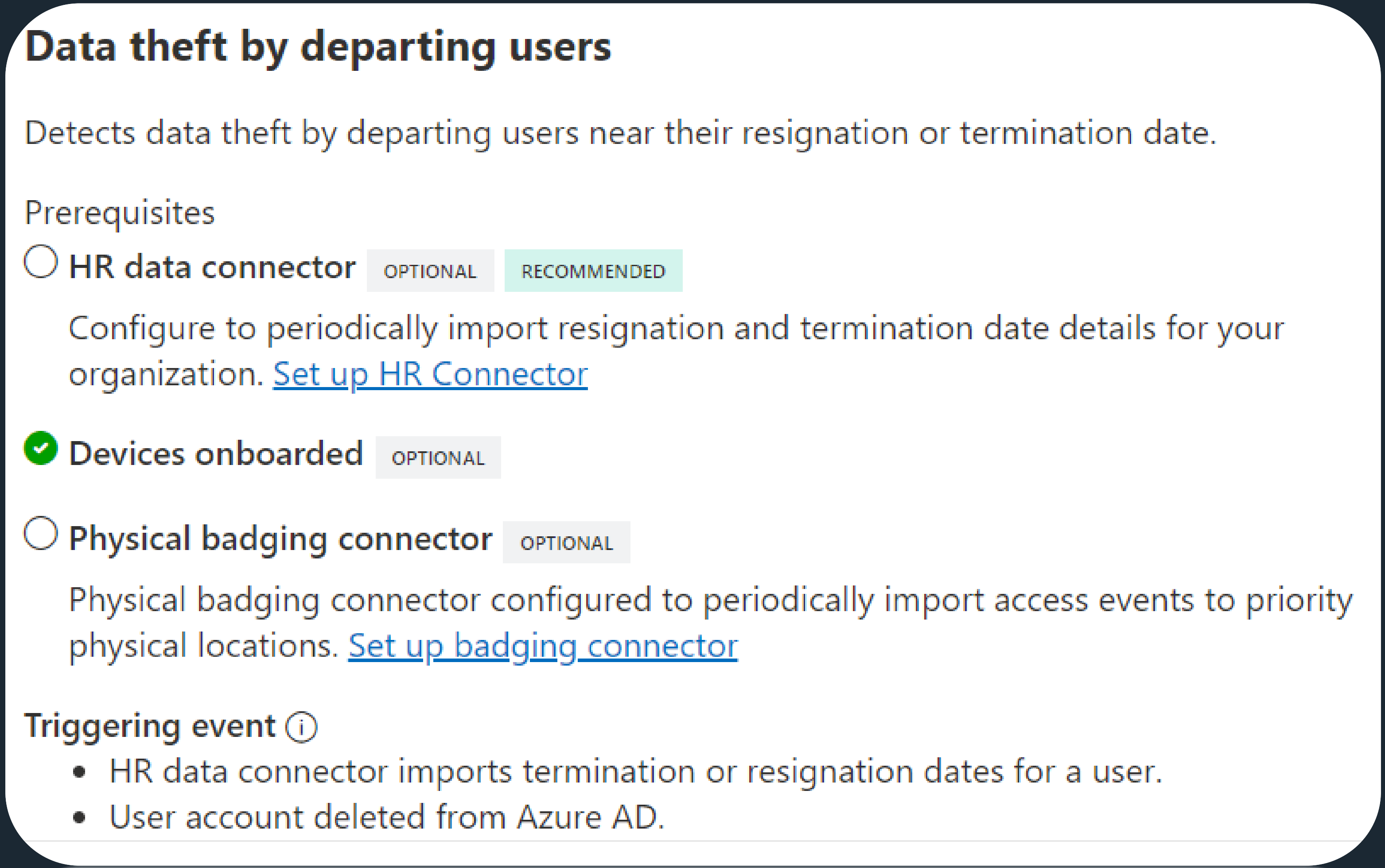
View all activity

User alert history

3 alerts: Data leaks

View user alert history

Start with ”Data theft by departing users”



Data theft by departing users

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

Prerequisites

○ **HR data connector** OPTIONAL RECOMMENDED

Configure to periodically import resignation and termination date details for your organization. Set up HR Connector

✓ **Devices onboarded** OPTIONAL

○ **Physical badging connector** OPTIONAL

Physical badging connector configured to periodically import access events to priority physical locations. Set up badging connector

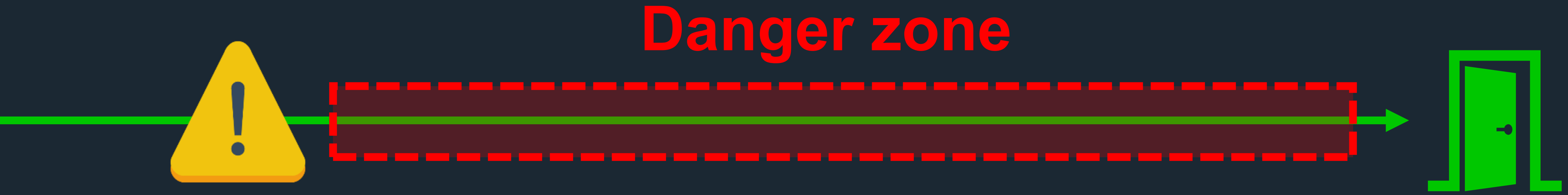
Triggering event ⓘ

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

✓ **High true positive %**

✓ **Practice & validate processes**

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



Danger zone

Employment end date set
October 1st

Employment ends
December 31st

The unintentional or careless insider

”That which is **easy** to do will be done frequently, **whether it should be or not**”

The underestimated threat

- Imminently more problematic because of **scale**
- Negligence, misunderstood role or unclear rules
- Lack of clear behavioral indicators
- Enabled by lack of security culture and secure management practices
- Carelessness – people do what they think is useful or important, but in the wrong ways

LACK OF SECURITY CULTURE
UNAUTH. DISCLOSURE

Samsung engineers & ChatGPT (2023)

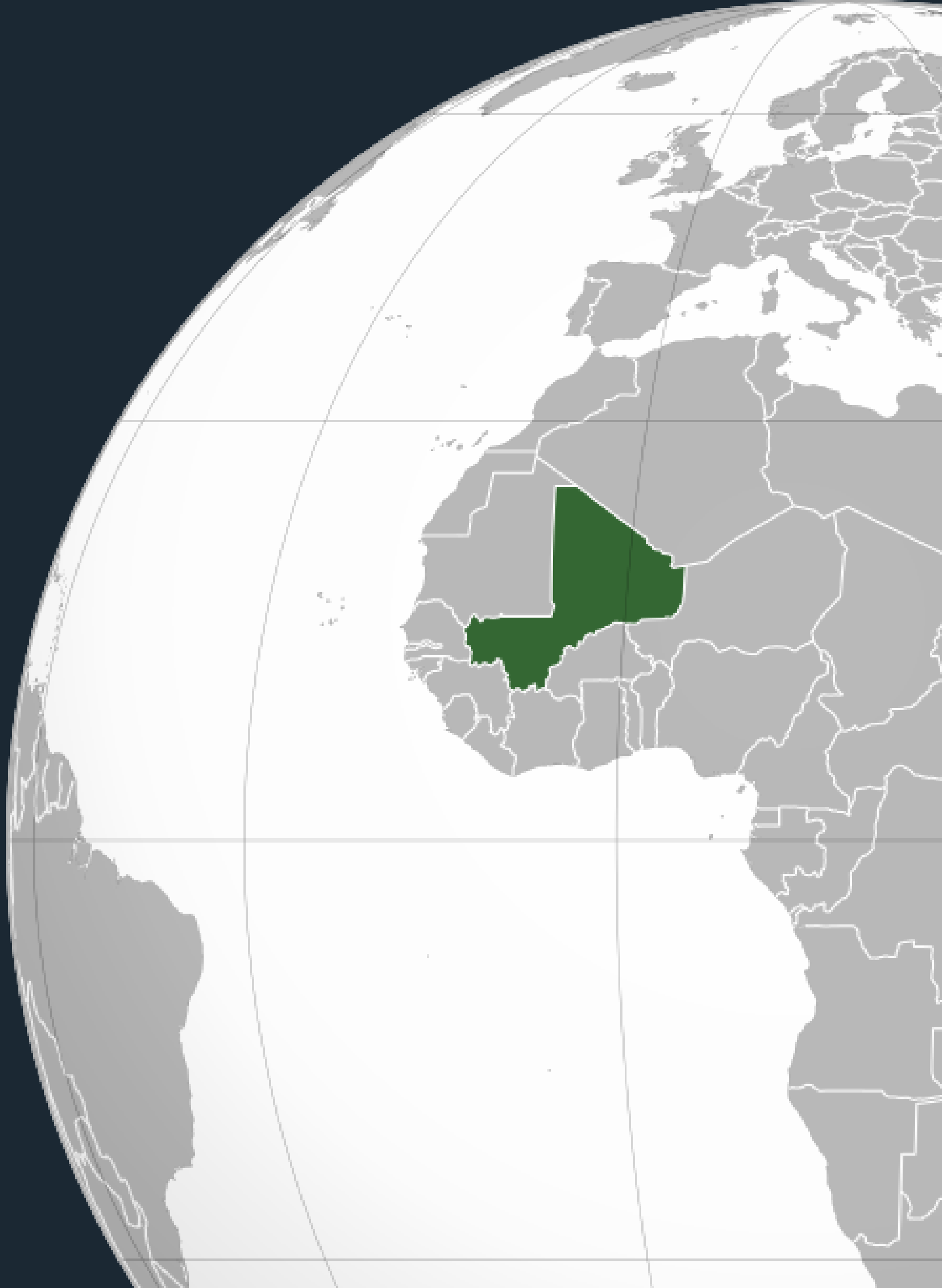
- Samsung engineers pasted source code & secret internal meeting notes into consumer ChatGPT
- Tried to get help optimizing test sequences for identifying faults in chips, turn meetings notes into PPTX
- Led to trade secret exposure – OpenAI retains prompts for model training
- Samsung then developed in-house LLM / AI solution
- **Classic careless insider threat**

City of Calgary privacy breach (2015)

- City employee shared private info of **3700+** other employees with recipient from another municipality
- Info sent **unencrypted** to both professional **and personal** address of recipient
- Sharing was for purposes of "receiving technical assistance"
- Led to **$92,9 million** class-action suit
- No malicious intent - lack of training, lack of guardrails

From .MIL to Mali

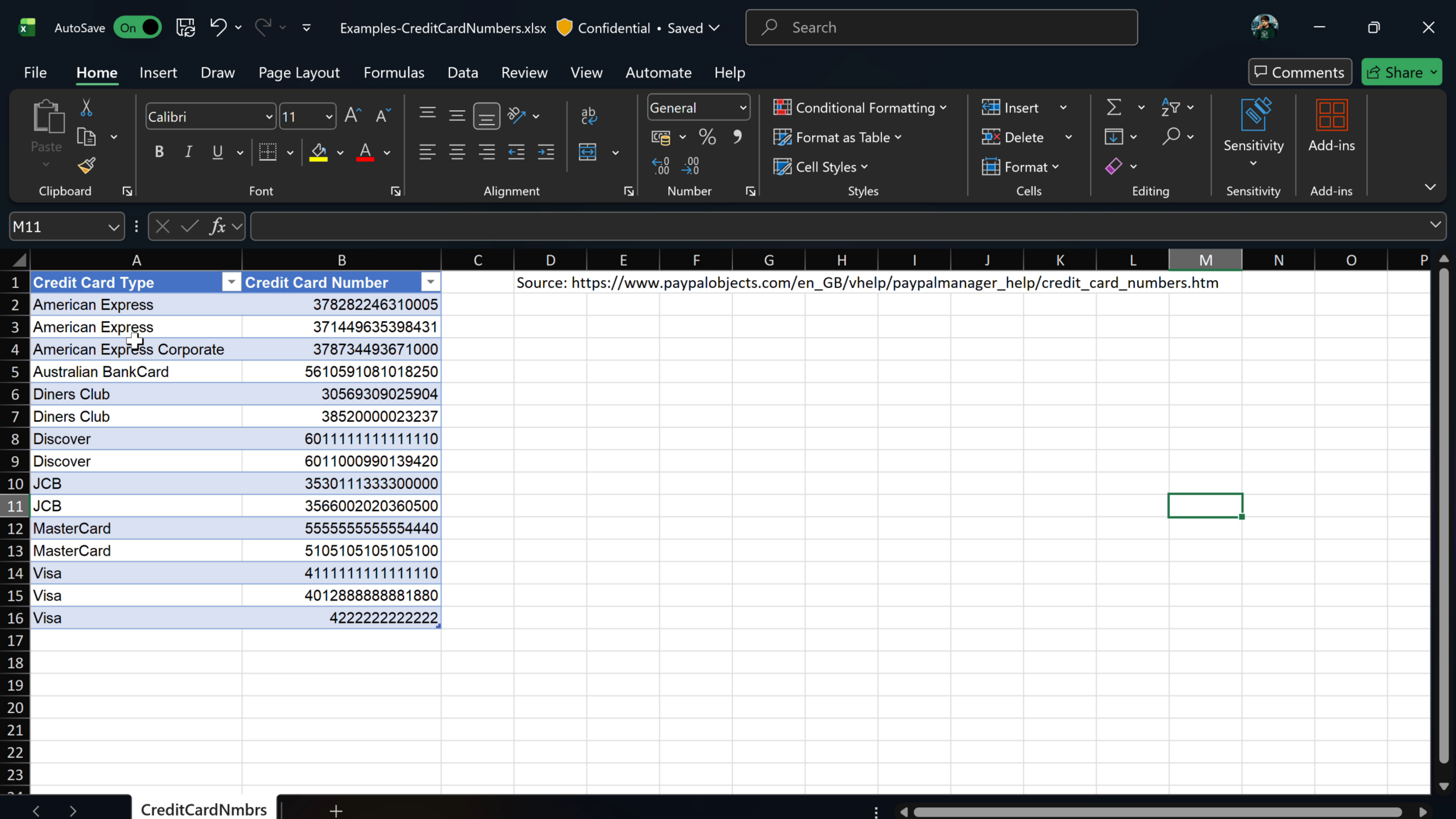
- US military email addresses end in **.MIL**
- The country of Mali has a domain, **.ML**
- US military has been accidentally sending internal email to .ML addresses for years – a “typo leak”
- Discovered in 2013 by Dutch businessman contracted to manage Mali’s domain
- Mali has warmed its relation to Russia – oops!
- **The real issue:** Lack of guardrails



First aid for unintentional insider risk

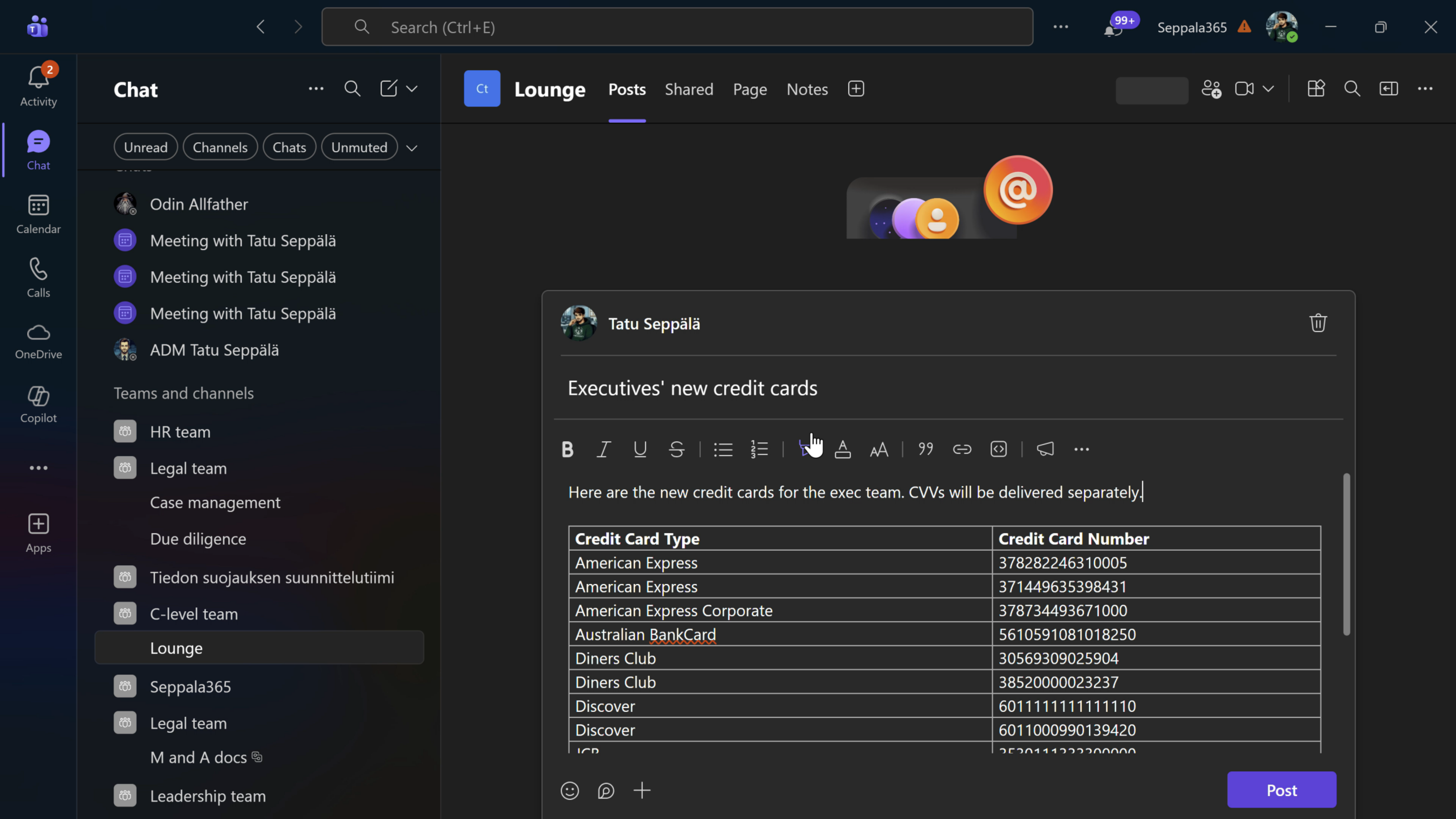
- **Sensitivity labels & DLP** turn policy into guardrails
  - Make anomalies **louder**
- **Audit logs** correlated by **Insider Risk Management** help identify persistent risky data handling
  - Identify bigger context & repeat offenders

Data Loss Prevention



Credit Card Type	Credit Card Number
American Express	378282246310005
American Express	371449635398431
American Express Corporate	378734493671000
Australian BankCard	5610591081018250
Diners Club	30569309025904
Diners Club	38520000023237
Discover	6011111111111110
Discover	6011000990139420
JCB	3530111333300000
JCB	3566002020360500
MasterCard	5555555555554440
MasterCard	5105105105105100
Visa	4111111111111110
Visa	4012888888881880
Visa	4222222222222

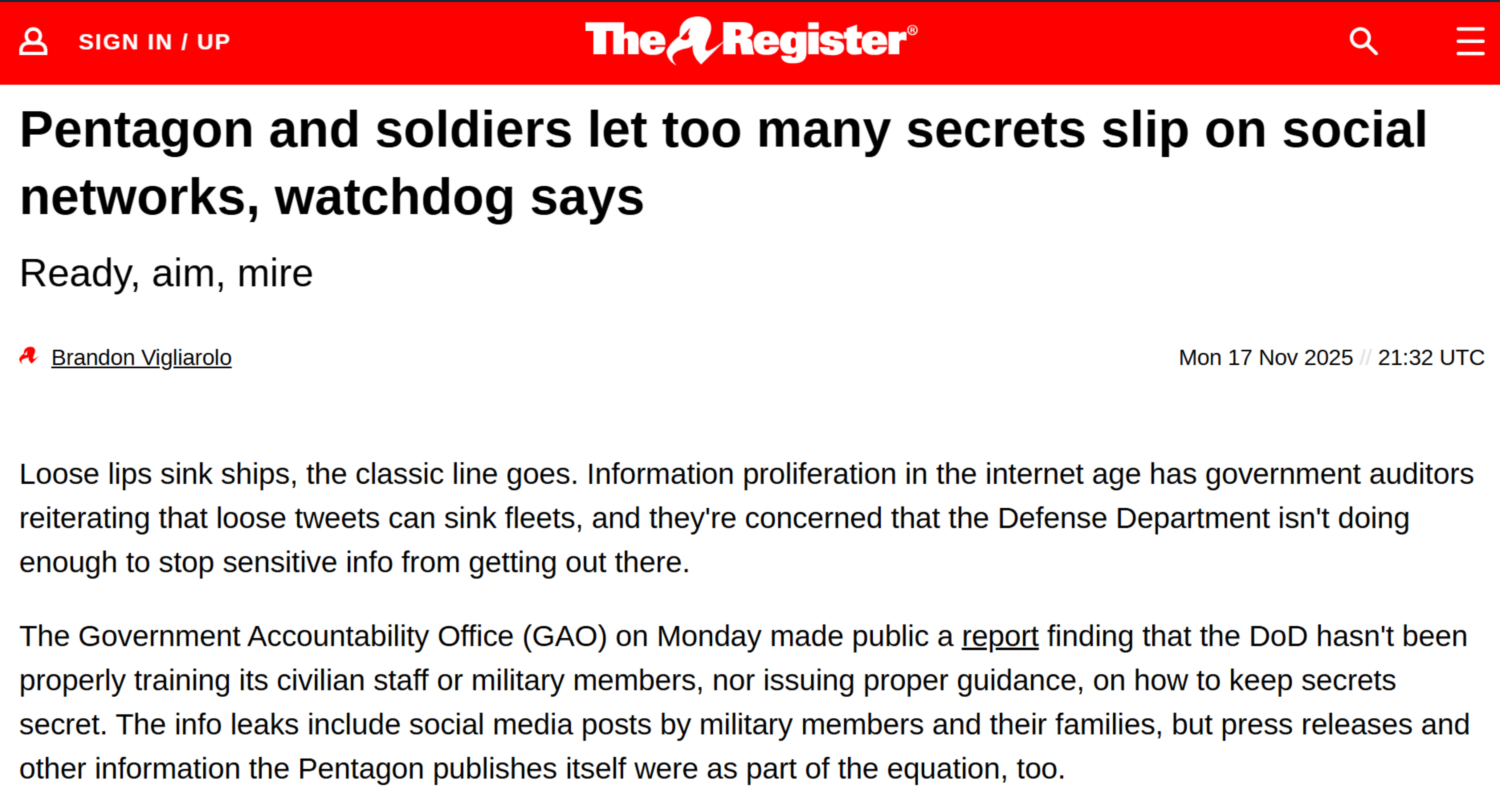
Source: https://www.paypalobjects.com/en_GB/vhelp/paypalmanager_help/credit_card_numbers.htm



Executives' new credit cards

Here are the new credit cards for the exec team. CVVs will be delivered separately.

Credit Card Type	Credit Card Number
American Express	378282246310005
American Express	371449635398431
American Express Corporate	378734493671000
Australian BankCard	5610591081018250
Diners Club	30569309025904
Diners Club	38520000023237
Discover	6011111111111110
Discover	6011000990139420
JCB	3530111333300000



Pentagon and soldiers let too many secrets slip on social networks, watchdog says

Ready, aim, mire

Brandon Vigliarolo

Mon 17 Nov 2025 // 21:32 UTC

Loose lips sink ships, the classic line goes. Information proliferation in the internet age has government auditors reiterating that loose tweets can sink fleets, and they're concerned that the Defense Department isn't doing enough to stop sensitive info from getting out there.

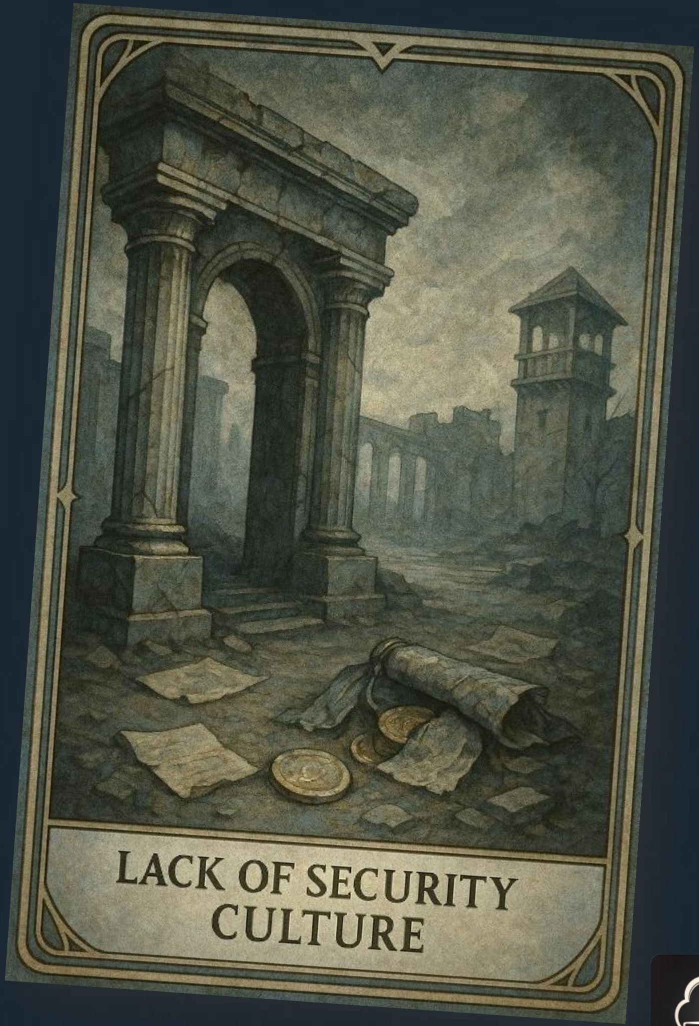
The Government Accountability Office (GAO) on Monday made public a report finding that the DoD hasn't been properly training its civilian staff or military members, nor issuing proper guidance, on how to keep secrets secret. The info leaks include social media posts by military members and their families, but press releases and other information the Pentagon publishes itself were as part of the equation, too.

First aid for unintentional insider risk

- Unchecked use of personally-owned devices and 24/7 social media blur boundaries between work & private life → costly mistakes!
- Increasing volume of unstructured data in M365 magnifies accidental exposure likelihood & impact

Reinforcing security culture

- Poor security culture manifests as general disregard for security practices, no personal ownership for security
- Countermeasures: Peers acting as security champions, training, consistent enforcement of policies and positive reinforcement
- **The job of security: enable business to work in a secure, sustainable manner**



#Naas
No as a Service

Next up?

- **Nation-states** like China, Russia are now using non-state actors to identify & target vulnerable insiders
- Most at-risk industries: AI, quantum, biotech, defense

Microsoft

Microsoft Digital Defense Report 2025

Lighting the path to a secure future

A Microsoft Threat Intelligence report

“The critical element is not the source of a threat, but its **potential for damage.**

Evaluating threats from that perspective, it becomes obvious that although most attacks might come from outside the organization, **the most serious damage is done with help from the inside.**”

- Eric Cole

Former SANS faculty fellow

Former CTO @ McAfee

Former Chief scientist @ Lockheed Martin

Comments or questions?

Connect with me!