Automated Data Security: Identifying Sensitive Data with Microsoft Purview

Myron Helgering

Level: Intermediate

Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!

LIVE! 360

TECH EVENTS WITH PERSPECTIVE

About me

- Solution Lead @ Pink Elephant
- Microsoft Security MVP
- Blogger and Speaker
- Fantasy geek

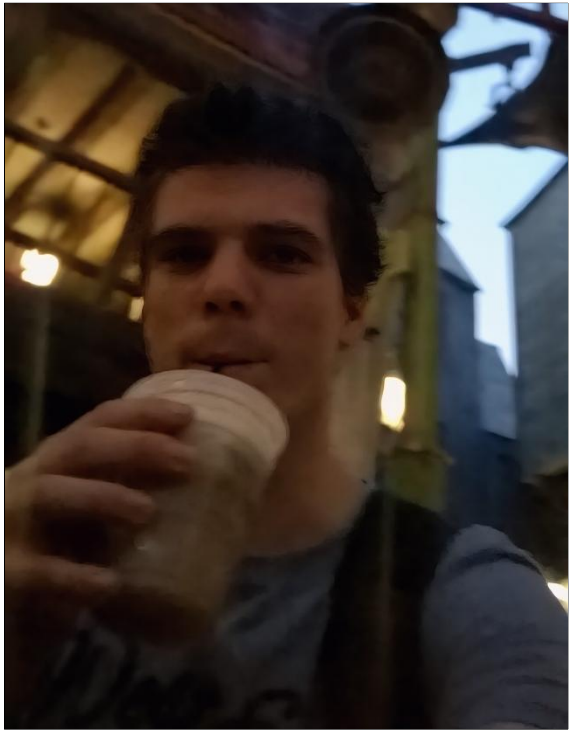
Myron Helgering

in/myronhelgering   myronhelgering.com

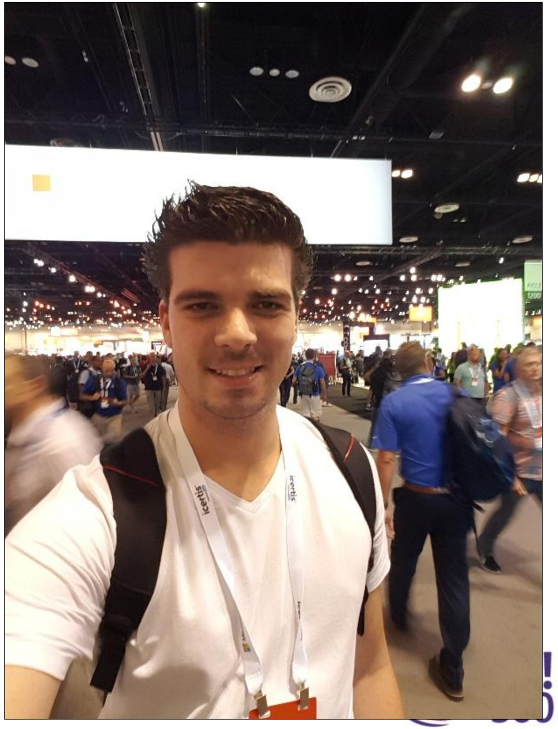
I 💘 Orlando

2007

2016



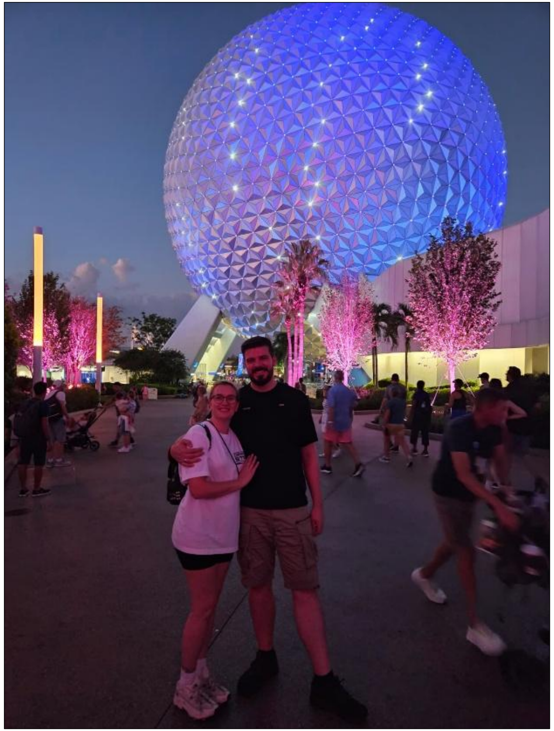
2018



I 💘 Orlando

2019

2024



2025

LIVE! 360
TECH CON 2025
ORLANDO
FLORIDA
Cybersecurity & Ransomware LIVE!
Banda Sea 2
Cybersecurity & Ransomware Live! Pre-Con Hands-On Lab: Sunday, Nov 16
9:00 AM - 6:00 PM CRHOL01 Hands-On Lab: Protect, Detect, Respond with Microsoft Defender XDR - Stefan Schörling & Mattias Borg
Cybersecurity & Ransomware Live! Pre-Con Workshops: Monday, Nov 17
8:30 AM - 5:30 PM CRM01 Workshop: Designing a Privileged Access Management Solution - Sami Laiho
Cybersecurity & Ransomware Live! Day 1: Tuesday, November 18
8:00 AM - 9:00 AM Cybersecurity & Ransomware Live! Keynote: 2026 Ransomware State of the Union - Sami Laiho, Chief Research Officer, Adminize
9:15 AM - 10:30 AM CRT02 Using Security Copilot and Defender XDR to Streamline Your SOC - John O'Neill Sr.
1:30 PM - 1:50 PM CRT04 Fast Focus: Connect Securely to Your Home Network Without a Single Firewall Port Open - Sami Laiho
2:00 PM - 2:20 PM CRT06 Fast Focus: Elevate to Admin on Demand - Sami Laiho
2:45 PM - 4:00 PM CRT08 When Hackers Collide – Unleashing Sticky Data Protection - Andy Malone
4:15 PM - 5:30 PM CRT10 Unlocking Next-Gen Cloud Security: What's New in Microsoft Defender for Cloud - Markus Lintuala
Cybersecurity & Ransomware Live! Day 2: Wednesday, November 19
8:00 AM - 9:15 AM CRW02 What Security Engineers and Developers Must Know About Azure AI Solutions - Markus Lintuala
9:30 AM - 10:45 AM CRW04 Automated Data Security: Identifying Sensitive Data with Microsoft Purview - Myron Helgering
2:00 PM - 3:15 PM CRW06 Improve Your Resilience with Cybersecurity Table-top Exercises - Stefan Schörling & Mattias Borg
4:00 PM - 5:15 PM CRW08 BYOAI: Bring Your Own AI to the Cybersecurity Fight - Michael Van Horenbeeck
Cybersecurity & Ransomware Live! Day 3: Thursday, November 20
8:00 AM - 9:15 AM CRH01 Securing, Managing and Hacking Microsoft Copilot - Stephen L. Rose
9:30 AM - 10:45 AM CRH03 Building a Resilient Incident Response Team: Beyond Playbooks and Tools - John O'Neill Sr.
11:00 AM - 12:00 PM Cybersecurity & Ransomware Live! Panel Discussion: How to Not Get Hacked in 2026 - Sami Laiho (moderator) Erica Burgess, Michael Niehaus, Stefan Schörling, & Michael Van Horenbeeck
1:00 PM - 2:15 PM CRH05 Six Methods to Protect Your Business From the Threat of Unmanaged Devices - Myron Helgering
2:30 PM - 3:45 PM CRH07 Why Domain Tiering is Critical to Prevent Ransomware - Sami Laiho

Agenda

01 Introduction

02 Sensitive Information Types

03 Fingerprint SITs

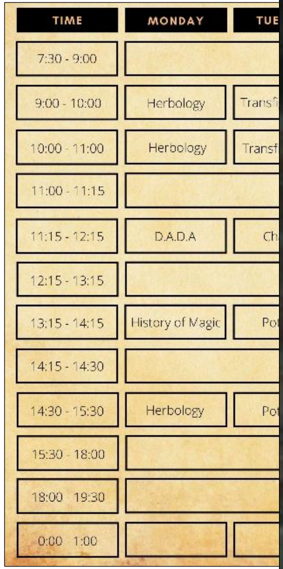
04 Trainable Classifiers

05 Exact Data Match Classifiers

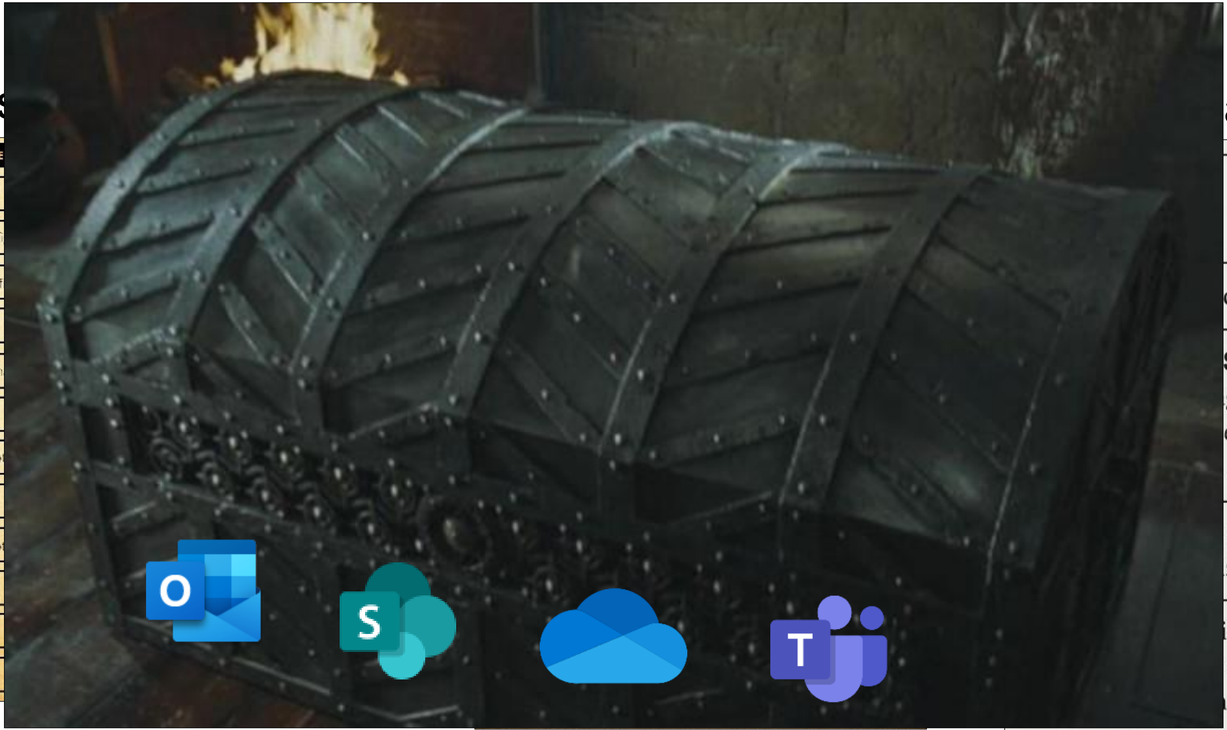
06 Classifier Usage, Takeaways & Q&A

Why is classifying your sensitive data important?

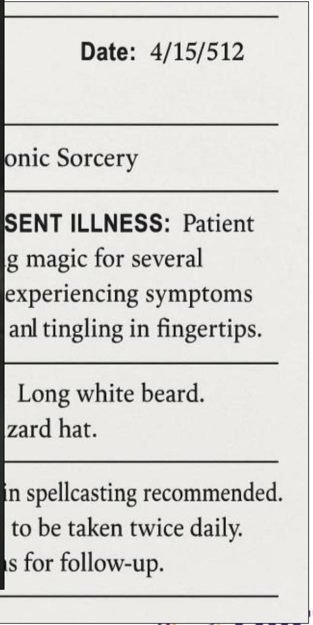
Class



TIME	MONDAY	TUE
7:30 - 9:00		
9:00 - 10:00	Herbology	Transf
10:00 - 11:00	Herbology	Transf
11:00 - 11:15		
11:15 - 12:15	D.A.D.A	Ch
12:15 - 13:15		
13:15 - 14:15	History of Magic	Po
14:15 - 14:30		
14:30 - 15:30	Herbology	Po
15:30 - 18:00		
18:00 - 19:30		
0:00 - 1:00		



al Records



Date: 4/15/512

onic Sorcery

SENT ILLNESS: Patient
g magic for several
experiencing symptoms
anl tingling in fingertips.

Long white beard.
zard hat.

in spellcasting recommended.
to be taken twice daily.
s for follow-up.

LIVE! 360
TECH EVENTS WITH PERSPECTIVE

Which data is sensitive or important enough?

- Intellectual property
- Medical information
- Personal information
- Pricing lists
- Customer information
- Business processes
- Financial data
- Or any other type of data

Who will classify sensitive data?

Manually

Automagically

Meet Minerva McGonagall

- Professor at Hogwarts School
- Chief Information Security Officer (CISO)

🎯 Her goal is to identify, classify and protect sensitive school data.

License and permissions

- Access Data Explorer
- Apply protection automatically based on classifiers
- Use advanced classifiers (e.g. trainable and EDM classifiers)

→

- M365 E5 or E5 add-on license

- Create classifiers and policies
- View content in Data Explorer

→

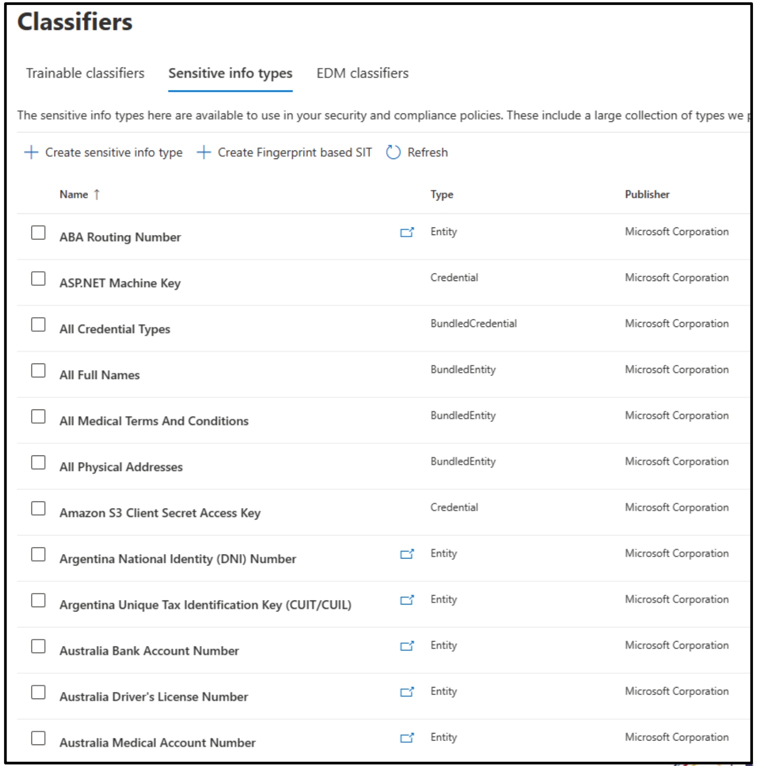
- Compliance Administrator role
- Content Explorer Content viewer

TECH EVENTS WITH PERSPECTIVE

Built-in Sensitive Information Types

311 Built-in SITs to classify specific sensitive information;

- Credit card
- Passport number
- National Insurance number (UK)
- SSN number (USA)
- Physical address
- Ip-address
- Driver’s license number
- Password

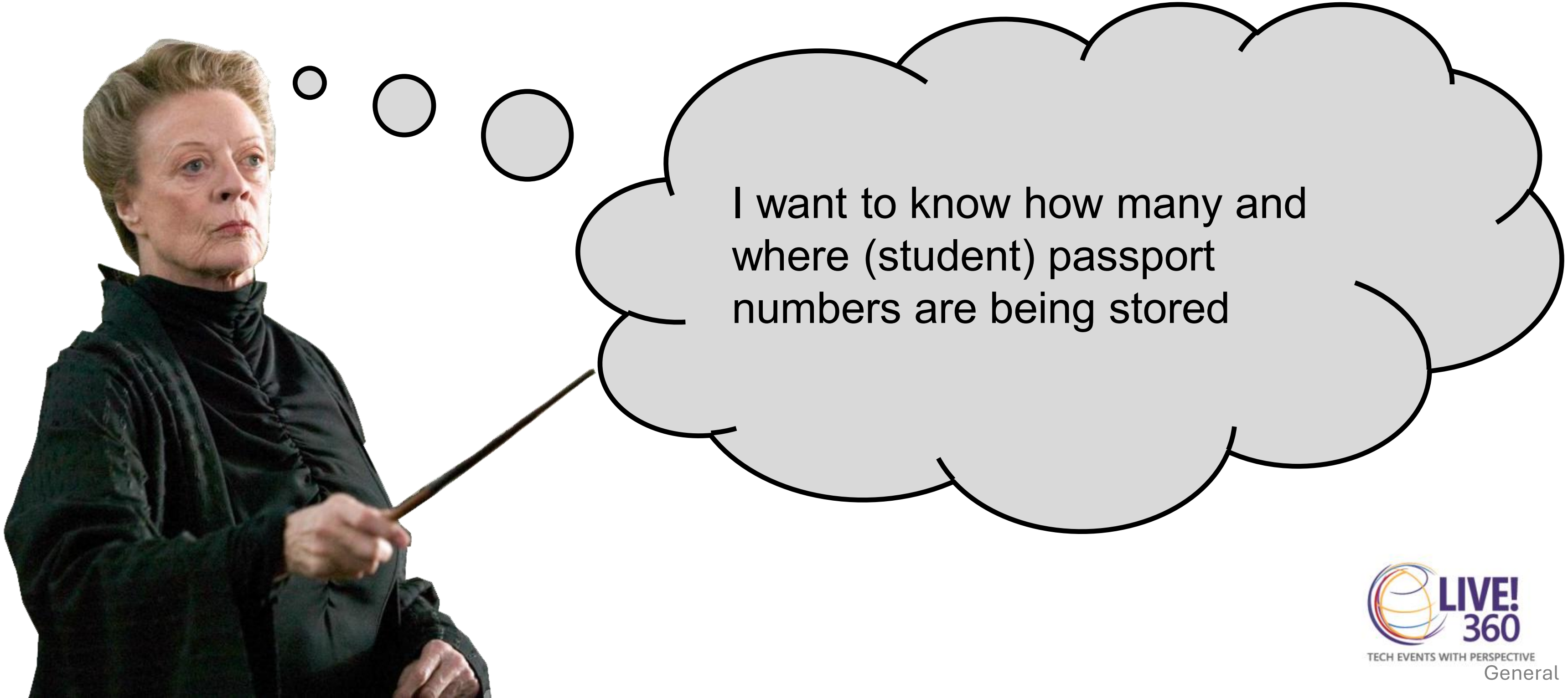


Classifiers

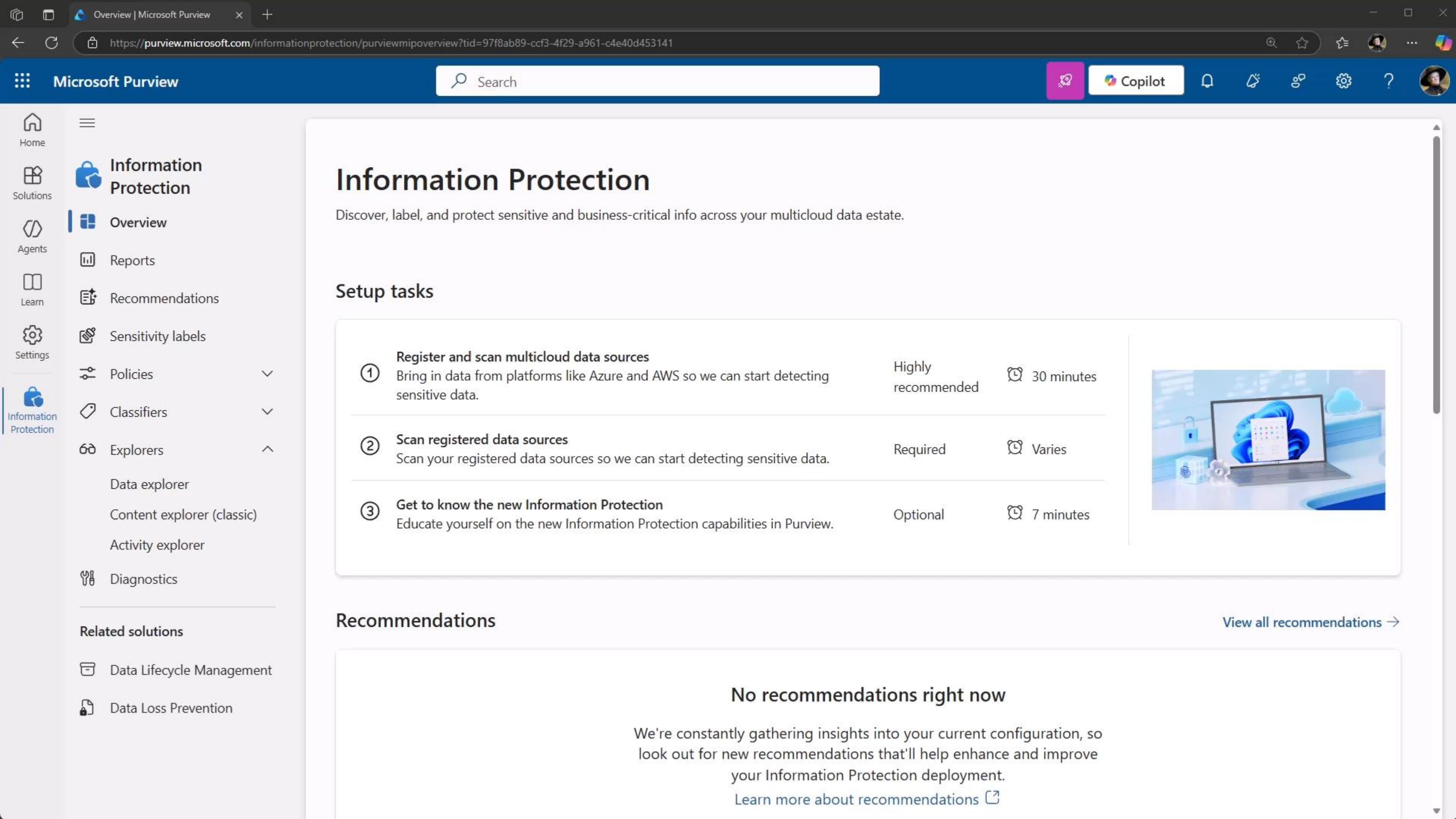
The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we

	Name ↑	Type	Publisher
□	ABA Routing Number	Entity	Microsoft Corporation
□	ASP.NET Machine Key	Credential	Microsoft Corporation
□	All Credential Types	BundledCredential	Microsoft Corporation
□	All Full Names	BundledEntity	Microsoft Corporation
□	All Medical Terms And Conditions	BundledEntity	Microsoft Corporation
□	All Physical Addresses	BundledEntity	Microsoft Corporation
□	Amazon S3 Client Secret Access Key	Credential	Microsoft Corporation
□	Argentina National Identity (DNI) Number	Entity	Microsoft Corporation
□	Argentina Unique Tax Identification Key (CUIT/CUIL)	Entity	Microsoft Corporation
□	Australia Bank Account Number	Entity	Microsoft Corporation
□	Australia Driver's License Number	Entity	Microsoft Corporation
□	Australia Medical Account Number	Entity	Microsoft Corporation

Demo: Sensitive Information Types



I want to know how many and where (student) passport numbers are being stored



Information Protection

Discover, label, and protect sensitive and business-critical info across your multicloud data estate.

Setup tasks

1	**Register and scan multicloud data sources** Bring in data from platforms like Azure and AWS so we can start detecting sensitive data.	Highly recommended	30 minutes
2	**Scan registered data sources** Scan your registered data sources so we can start detecting sensitive data.	Required	Varies
3	**Get to know the new Information Protection** Educate yourself on the new Information Protection capabilities in Purview.	Optional	7 minutes

Recommendations

View all recommendations →

No recommendations right now

We're constantly gathering insights into your current configuration, so look out for new recommendations that'll help enhance and improve your Information Protection deployment.

Learn more about recommendations

Custom Sensitive Information Types

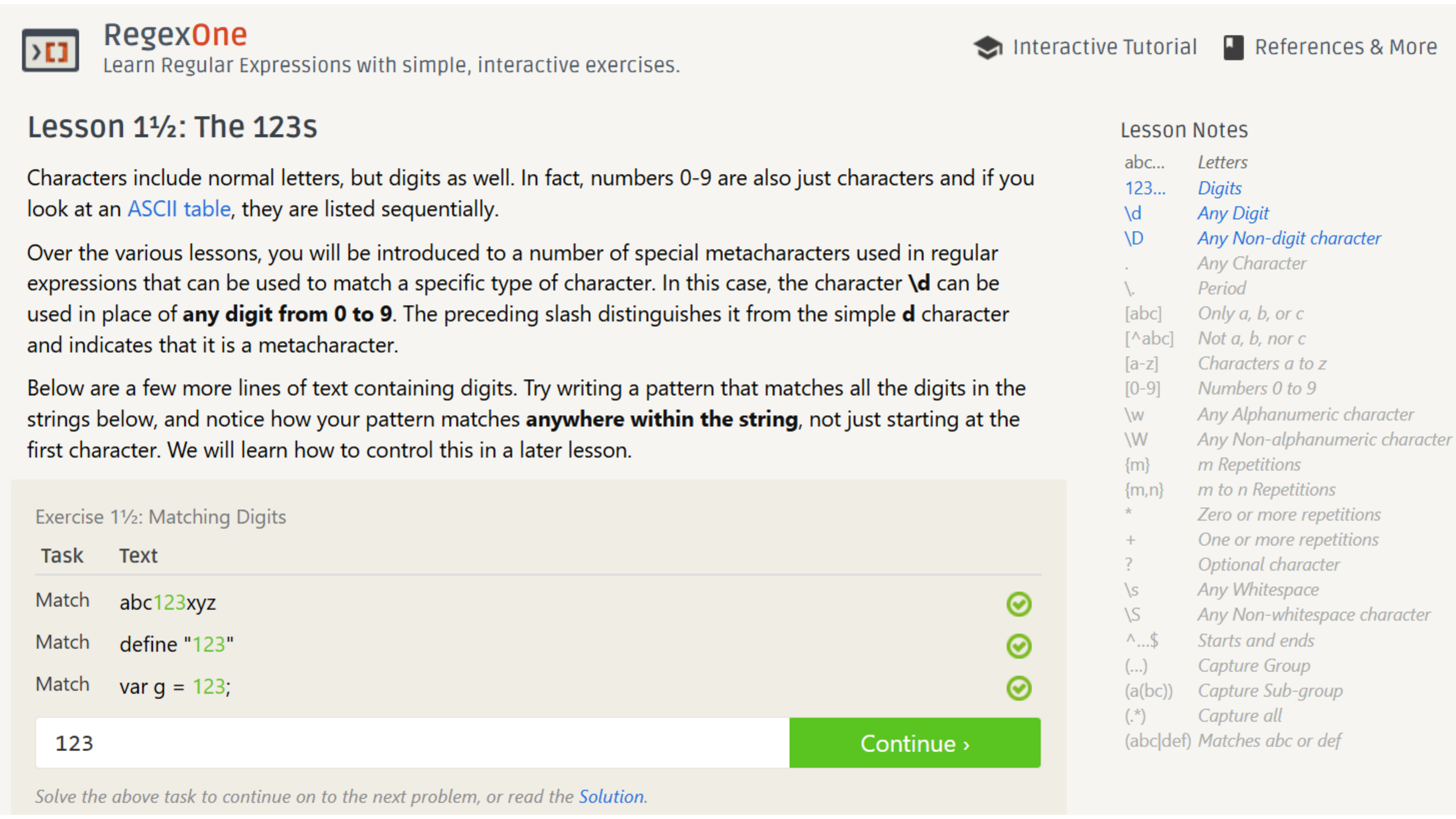
StudentID numbers

- Number format is 1234-5678
- Wordlist contains StudentID

Doc 1: Harry has **ID** number 389-9468

Doc 2: Harry has **StudentID** number 0397-3845

Learn the basics Regular Expressions https://regexone.com/
Test and create Regular Expressions https://regexr.com/



RegexOne
Learn Regular Expressions with simple, interactive exercises.

Lesson 1½: The 123s

Characters include normal letters, but digits as well. In fact, numbers 0-9 are also just characters and if you look at an ASCII table, they are listed sequentially.

Over the various lessons, you will be introduced to a number of special metacharacters used in regular expressions that can be used to match a specific type of character. In this case, the character **\d** can be used in place of **any digit from 0 to 9**. The preceding slash distinguishes it from the simple **d** character and indicates that it is a metacharacter.

Below are a few more lines of text containing digits. Try writing a pattern that matches all the digits in the strings below, and notice how your pattern matches **anywhere within the string**, not just starting at the first character. We will learn how to control this in a later lesson.

Exercise 1½: Matching Digits

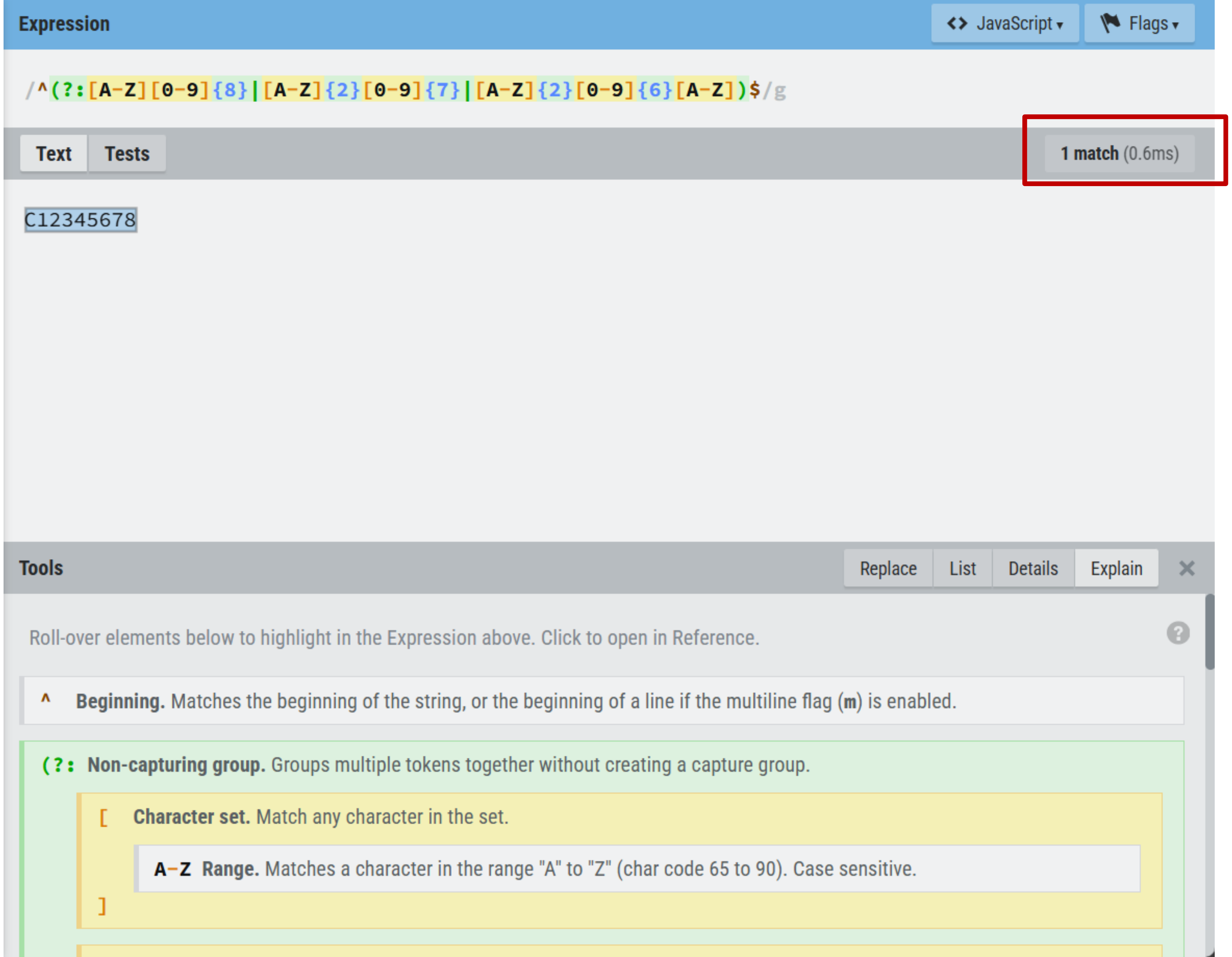
Task	Text	
Match	abc123xyz	✓
Match	define "123"	✓
Match	var g = 123;	✓

123

Solve the above task to continue on to the next problem, or read the Solution.

Lesson Notes

abc…	*Letters*
123…	*Digits*
\d	*Any Digit*
\D	*Any Non-digit character*
.	*Any Character*
\.	*Period*
[abc]	*Only a, b, or c*
[^abc]	*Not a, b, nor c*
[a-z]	*Characters a to z*
[0-9]	*Numbers 0 to 9*
\w	*Any Alphanumeric character*
\W	*Any Non-alphanumeric character*
{m}	*m Repetitions*
{m,n}	*m to n Repetitions*
*	*Zero or more repetitions*
+	*One or more repetitions*
?	*Optional character*
\s	*Any Whitespace*
\S	*Any Non-whitespace character*
^…$	*Starts and ends*
(…)	*Capture Group*
(a(bc))	*Capture Sub-group*
(.*)	*Capture all*
(abc|def)	*Matches abc or def*



```
/^(?:[A-Z][0-9]{8}|[A-Z]{2}[0-9]{7}|[A-Z]{2}[0-9]{6}[A-Z])$/g
```

1 match (0.6ms)

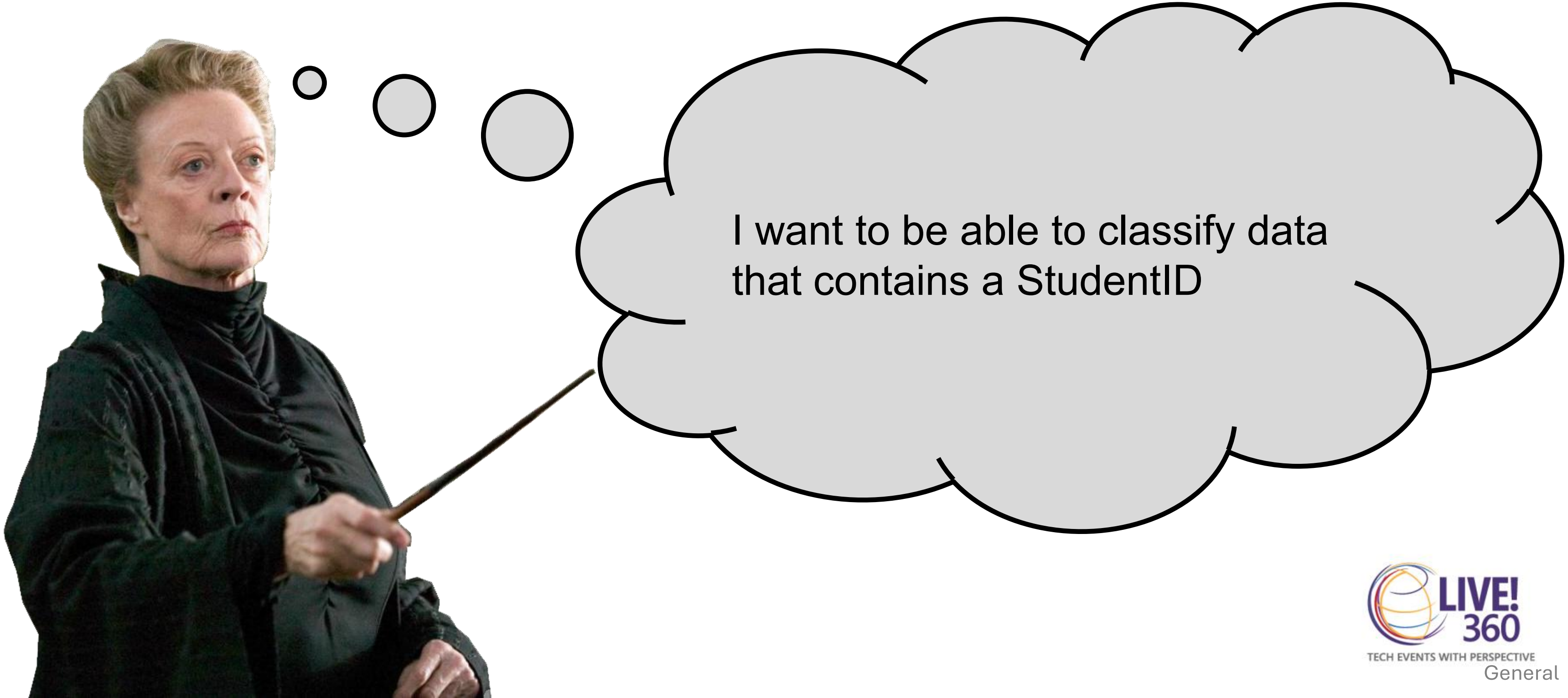
```
C12345678
```

Roll-over elements below to highlight in the Expression above. Click to open in Reference.

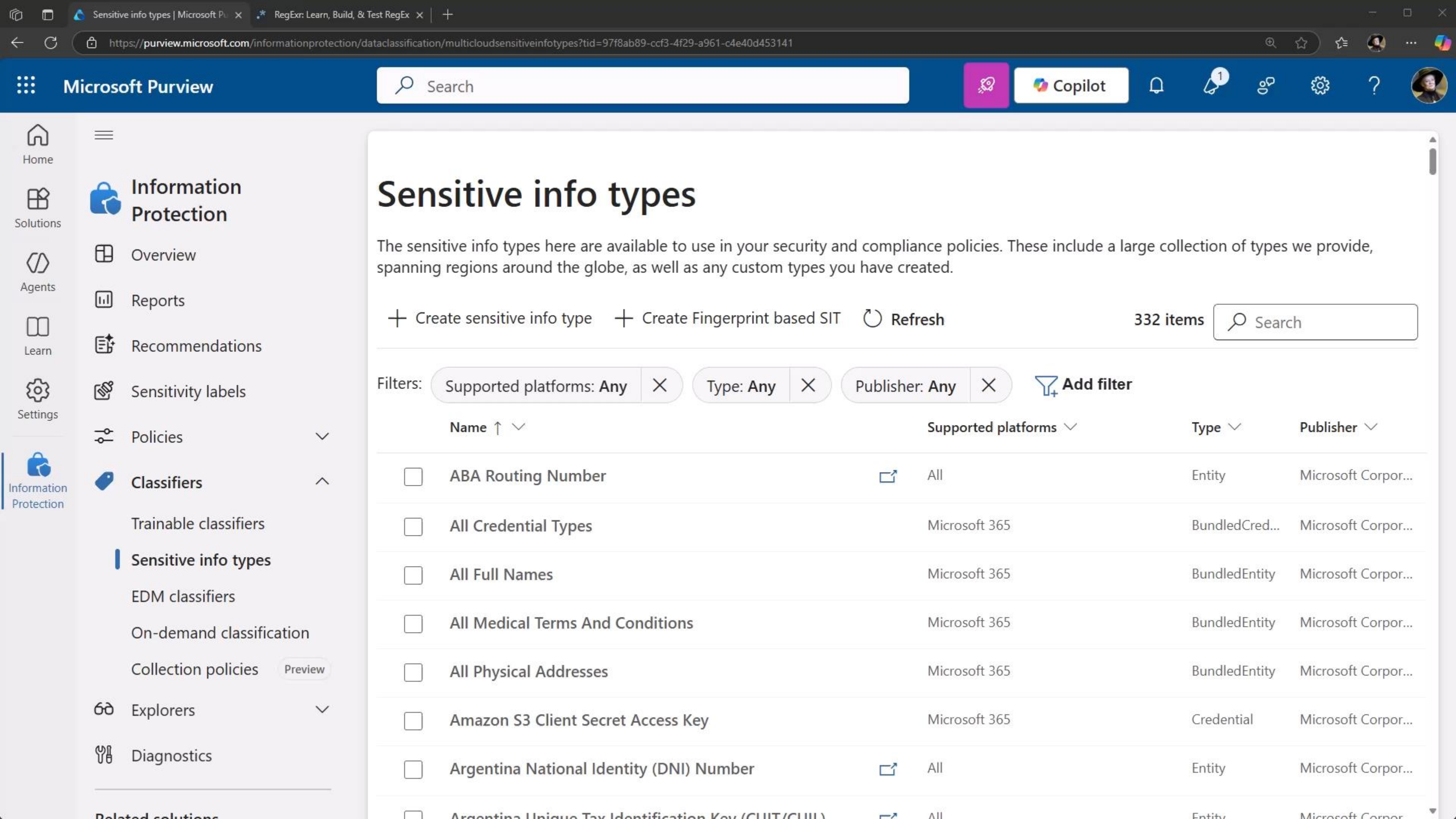
- `^` **Beginning.** Matches the beginning of the string, or the beginning of a line if the multiline flag (**m**) is enabled.
- `(?:` **Non-capturing group.** Groups multiple tokens together without creating a capture group.
  - `[` **Character set.** Match any character in the set.
    - `A-Z` **Range.** Matches a character in the range "A" to "Z" (char code 65 to 90). Case sensitive.
  - `]`

LIVE! 360
TECH EVENTS WITH PERSPECTIVE

Demo: Custom Sensitive Information Types



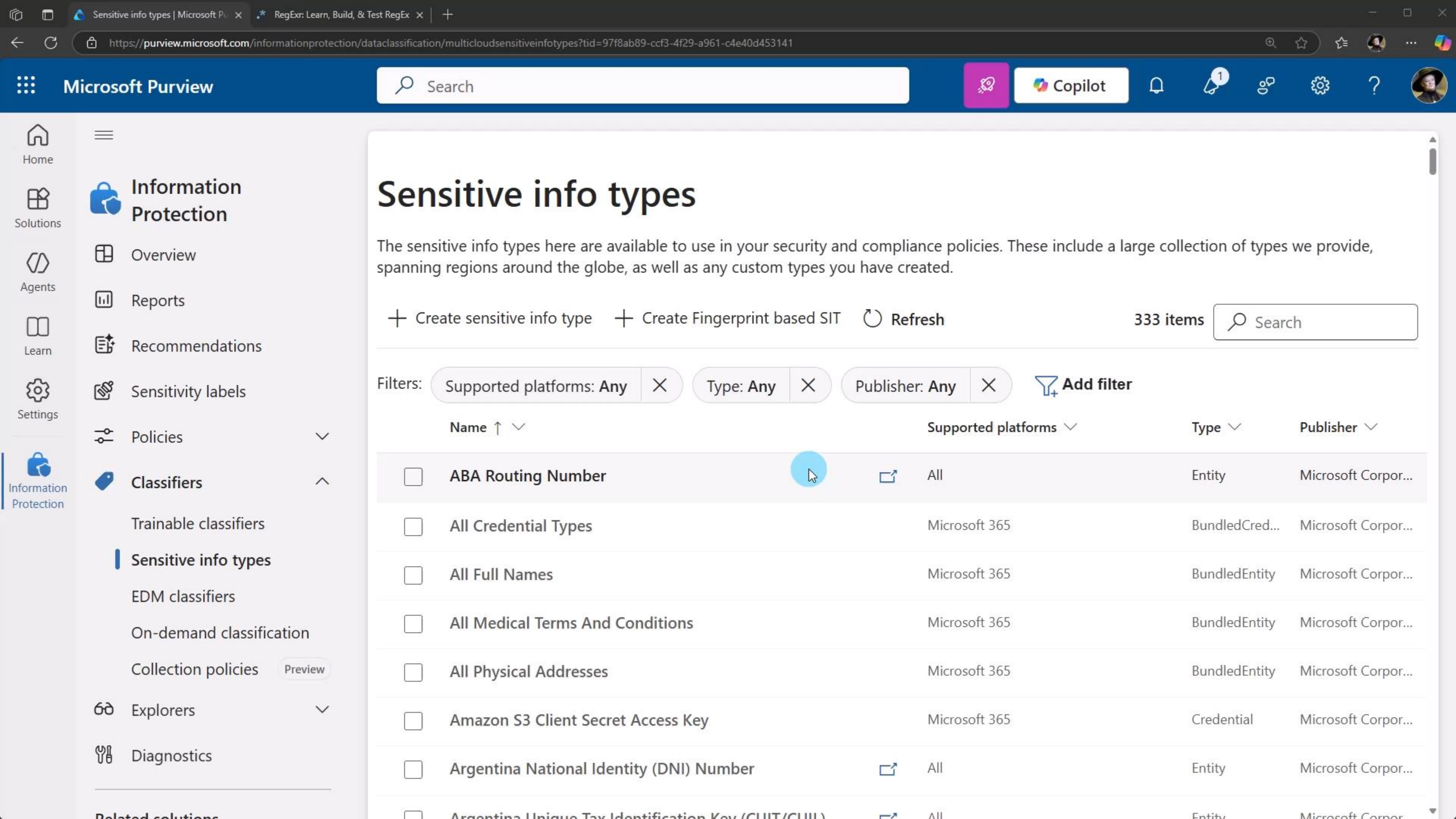
I want to be able to classify data that contains a StudentID



Sensitive info types

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

	Name ↑		Supported platforms	Type	Publisher
□	ABA Routing Number	↗	All	Entity	Microsoft Corpor...
□	All Credential Types		Microsoft 365	BundledCred...	Microsoft Corpor...
□	All Full Names		Microsoft 365	BundledEntity	Microsoft Corpor...
□	All Medical Terms And Conditions		Microsoft 365	BundledEntity	Microsoft Corpor...
□	All Physical Addresses		Microsoft 365	BundledEntity	Microsoft Corpor...
□	Amazon S3 Client Secret Access Key		Microsoft 365	Credential	Microsoft Corpor...
□	Argentina National Identity (DNI) Number	↗	All	Entity	Microsoft Corpor...
□	Argentina Unique Tax Identification Key (CUIT/CUIL)	↗	All	Entity	Microsoft Corpor...

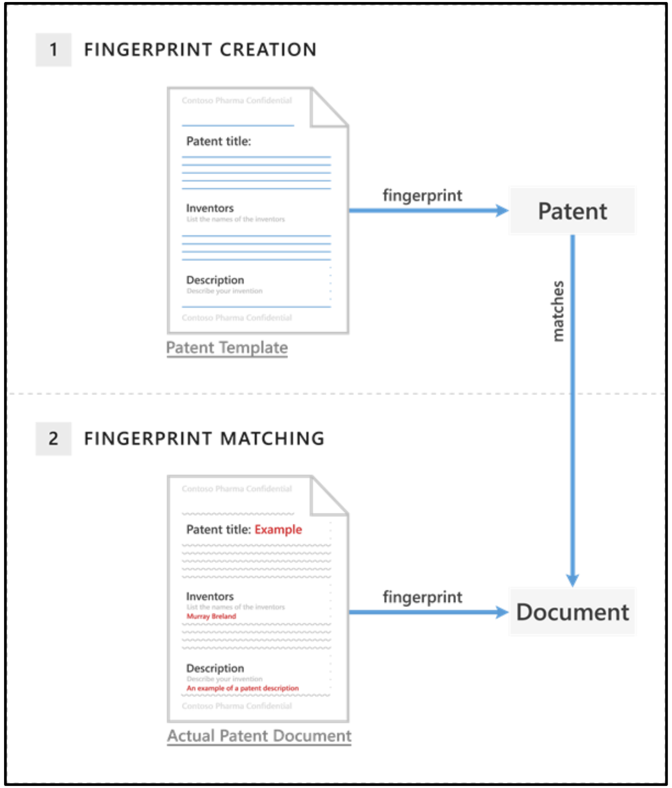


Sensitive info types

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

	Name ↑	Supported platforms	Type	Publisher
□	ABA Routing Number	All	Entity	Microsoft Corpor...
□	All Credential Types	Microsoft 365	BundledCred...	Microsoft Corpor...
□	All Full Names	Microsoft 365	BundledEntity	Microsoft Corpor...
□	All Medical Terms And Conditions	Microsoft 365	BundledEntity	Microsoft Corpor...
□	All Physical Addresses	Microsoft 365	BundledEntity	Microsoft Corpor...
□	Amazon S3 Client Secret Access Key	Microsoft 365	Credential	Microsoft Corpor...
□	Argentina National Identity (DNI) Number	All	Entity	Microsoft Corpor...
□	Argentina Unique Tax Identification Key (CUIT/CUIL)	All	Entity	Microsoft Corpor

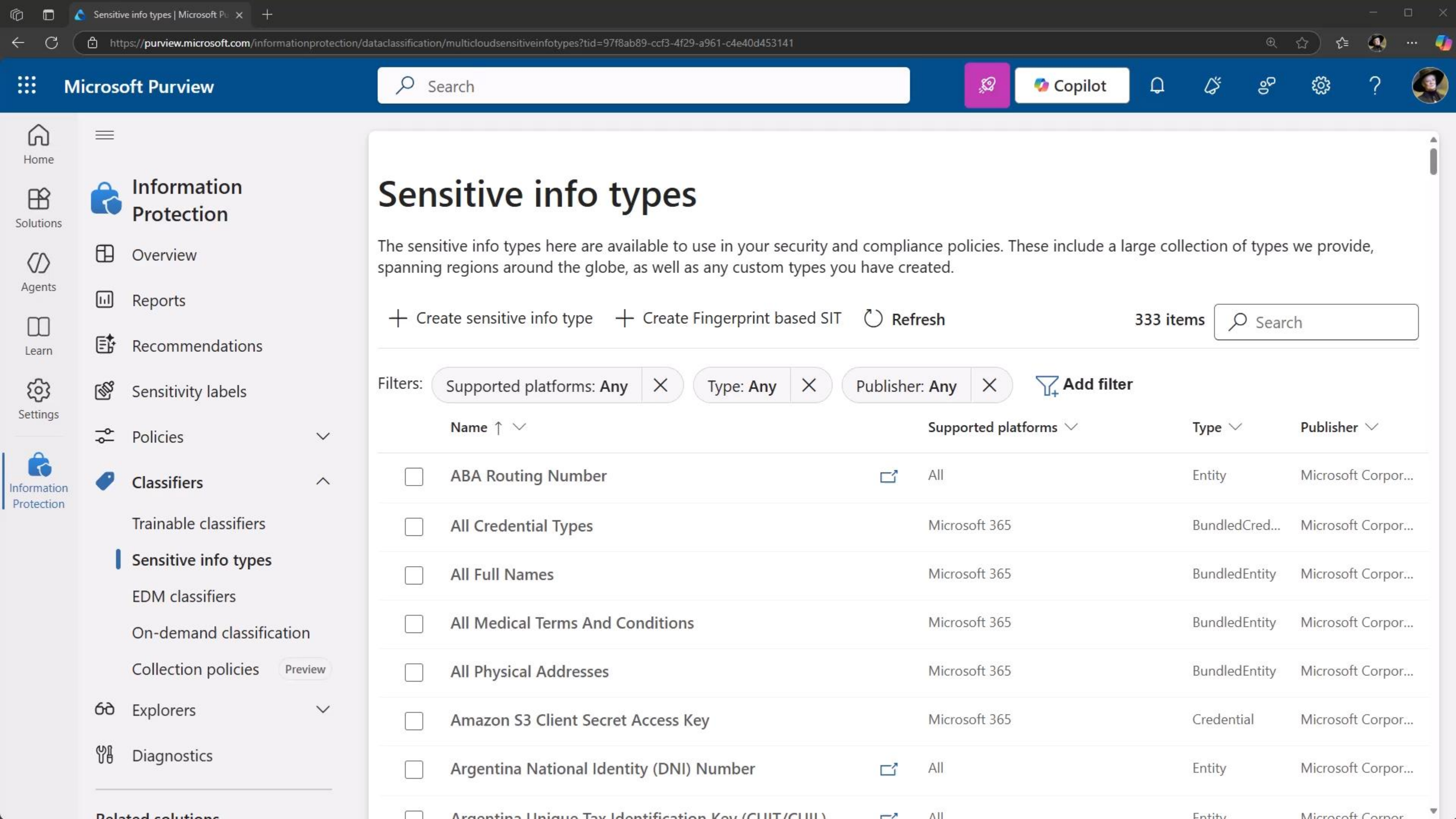
Fingerprint Sensitive Information Types



- Employee information forms
- Customer information forms
- Medical records
- Contracts
- Invoices
- Non-Disclosure Agreements (NDA)
- Or any other custom template file

Demo: Fingerprint Sensitive Information Types

I want to be able to classify Student Information Forms



Sensitive info types

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

	Name ↑		Supported platforms	Type	Publisher
□	ABA Routing Number	↗	All	Entity	Microsoft Corpor...
□	All Credential Types		Microsoft 365	BundledCred...	Microsoft Corpor...
□	All Full Names		Microsoft 365	BundledEntity	Microsoft Corpor...
□	All Medical Terms And Conditions		Microsoft 365	BundledEntity	Microsoft Corpor...
□	All Physical Addresses		Microsoft 365	BundledEntity	Microsoft Corpor...
□	Amazon S3 Client Secret Access Key		Microsoft 365	Credential	Microsoft Corpor...
□	Argentina National Identity (DNI) Number	↗	All	Entity	Microsoft Corpor...
□	Argentina Unique Tax Identification Key (CUIT/CUIL)	↗	All	Entity	Microsoft Corpor...

Built-in Trainable Classifiers

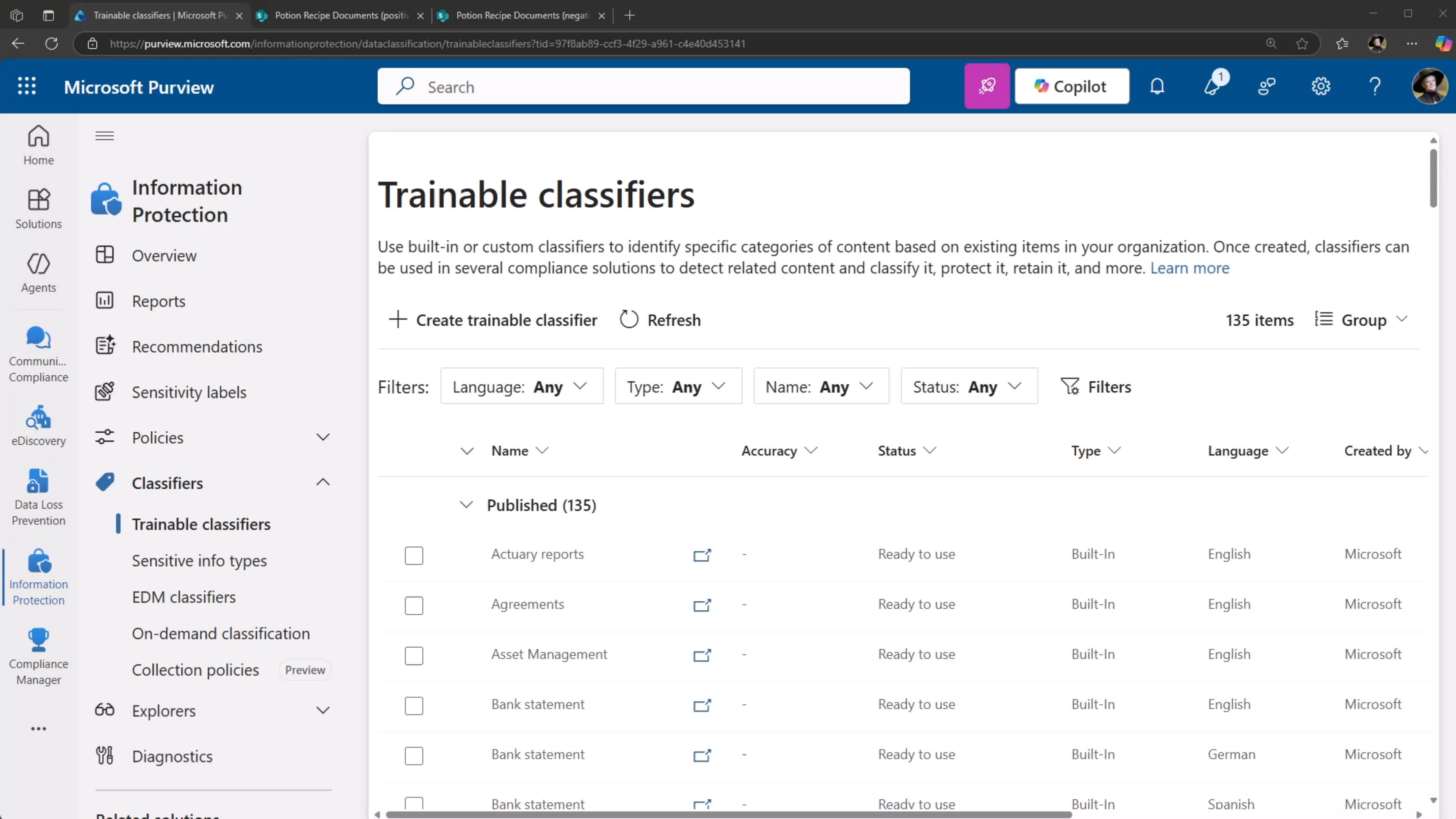
- Trainable classifiers identify a “type” of content
- 134 pre-trained classifiers are ready-to-use
- 14 different languages

Custom Trainable Classifiers

1. 50-500 positive and negative samples (English only)
2. Microsoft trains the classifier
3. Review false negatives
4. Retrain for higher accuracy
5. Publish, test and use the classifier

Demo: Custom Trainable Classifiers

I want to be able to classify potion recipes



Trainable classifiers

Use built-in or custom classifiers to identify specific categories of content based on existing items in your organization. Once created, classifiers can be used in several compliance solutions to detect related content and classify it, protect it, retain it, and more. Learn more

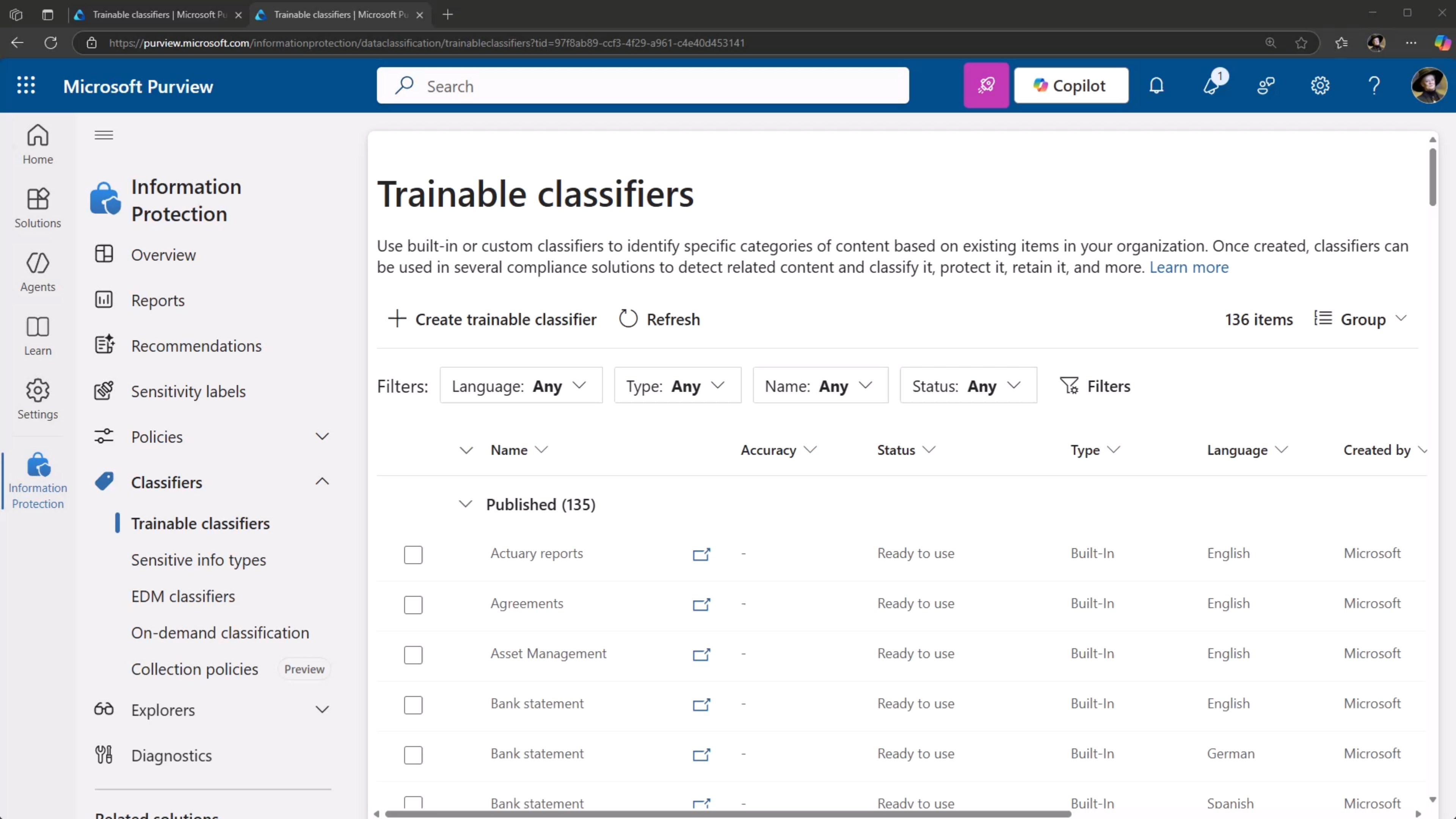
Filters: Language: **Any** Type: **Any** Name: **Any** Status: **Any** Filters

Published (135)

	Name		Accuracy	Status	Type	Language	Created by
□	Actuary reports	↗	-	Ready to use	Built-In	English	Microsoft
□	Agreements	↗	-	Ready to use	Built-In	English	Microsoft
□	Asset Management	↗	-	Ready to use	Built-In	English	Microsoft
□	Bank statement	↗	-	Ready to use	Built-In	English	Microsoft
□	Bank statement	↗	-	Ready to use	Built-In	German	Microsoft
□	Bank statement	↗	-	Ready to use	Built-In	Spanish	Microsoft

Waiting….. (maximum of 48 hours)

TECH EVENTS WITH PERSPECTIVE



Trainable classifiers | Microsoft Pu
Trainable classifiers | Microsoft Pu
https://purview.microsoft.com/informationprotection/dataclassification/trainableclassifiers?tid=97f8ab89-ccf3-4f29-a961-c4e40d453141
Microsoft Purview
Search
Copilot
1
Home
Solutions
Agents
Learn
Settings
Information Protection

Information Protection

- Overview
- Reports
- Recommendations
- Sensitivity labels
- Policies
- Classifiers
  - Trainable classifiers
  - Sensitive info types
  - EDM classifiers
  - On-demand classification
  - Collection policies Preview
- Explorers
- Diagnostics

Trainable classifiers

Use built-in or custom classifiers to identify specific categories of content based on existing items in your organization. Once created, classifiers can be used in several compliance solutions to detect related content and classify it, protect it, retain it, and more. Learn more

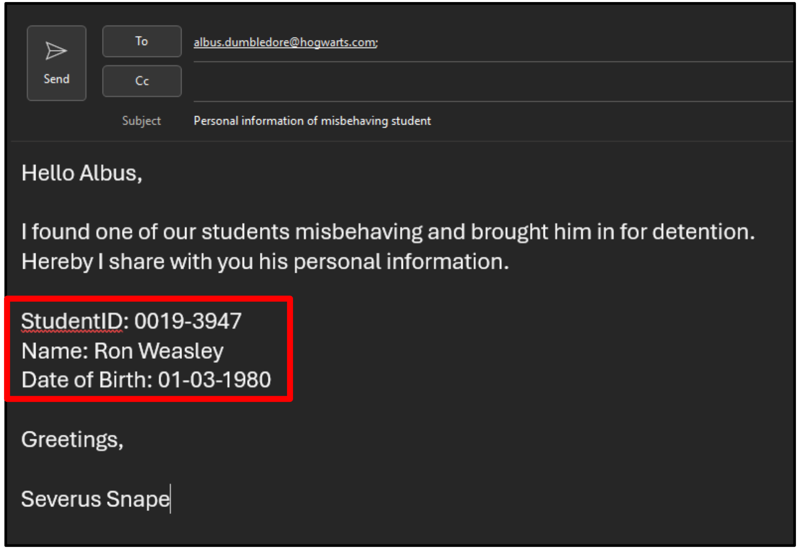
+ Create trainable classifier   Refresh   136 items   Group

Filters: Language: **Any**   Type: **Any**   Name: **Any**   Status: **Any**   Filters

Name	Accuracy	Status	Type	Language	Created by
Published (135)					
□ Actuary reports	-	Ready to use	Built-In	English	Microsoft
□ Agreements	-	Ready to use	Built-In	English	Microsoft
□ Asset Management	-	Ready to use	Built-In	English	Microsoft
□ Bank statement	-	Ready to use	Built-In	English	Microsoft
□ Bank statement	-	Ready to use	Built-In	German	Microsoft
□ Bank statement	-	Ready to use	Built-In	Spanish	Microsoft

Exact Data Match Classifiers

StudentID	First name	Last name	Date of Birth
0019-3947	Ron	Weasley	01-03-1980
0010-2394	Harry	Potter	31-06-1980
0015-5934	Hermione	Granger	19-09-1979



To: albus.dumbledore@hogwarts.com;

Cc:

Subject: Personal information of misbehaving student

Hello Albus,

I found one of our students misbehaving and brought him in for detention. Hereby I share with you his personal information.

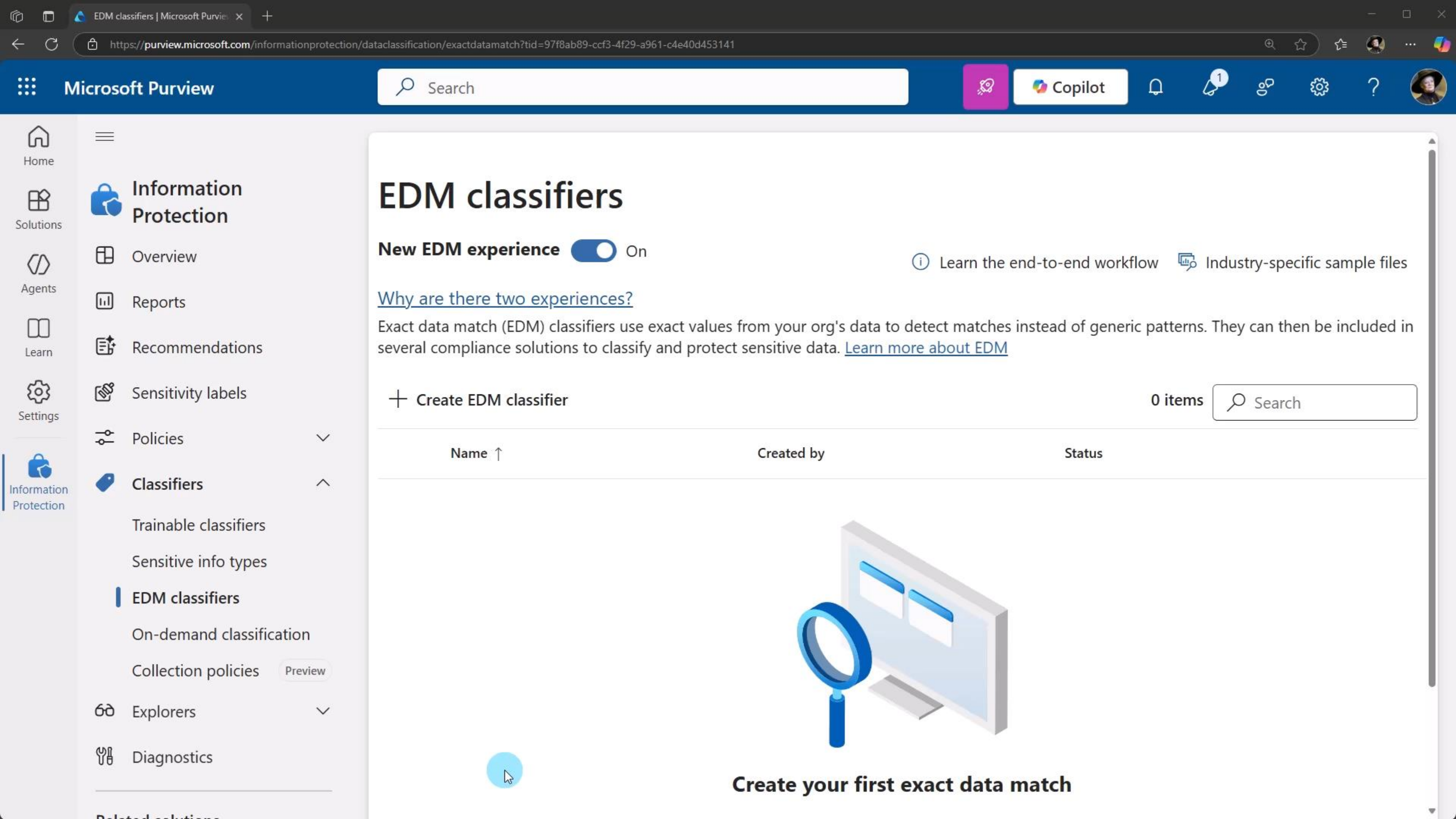
StudentID: 0019-3947
Name: Ron Weasley
Date of Birth: 01-03-1980

Greetings,

Severus Snape

Demo: Exact Data Match Classifiers

I want to be able to classify data that exactly matches the student record database



EDM classifiers

New EDM experience On

Learn the end-to-end workflow

Industry-specific sample files

Why are there two experiences?

Exact data match (EDM) classifiers use exact values from your org's data to detect matches instead of generic patterns. They can then be included in several compliance solutions to classify and protect sensitive data. Learn more about EDM

+ Create EDM classifier

0 items

Search

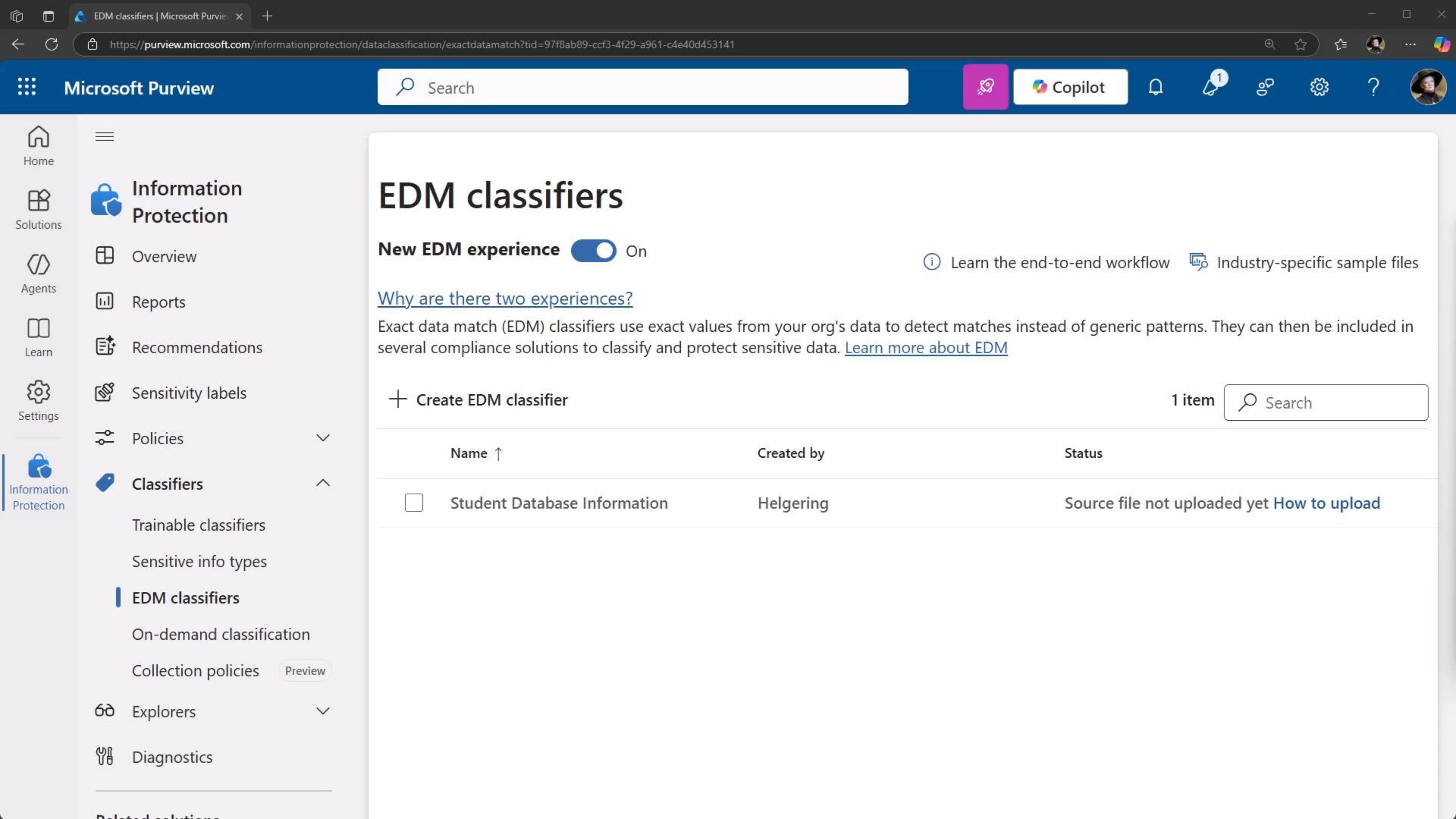
Name ↑	Created by	Status

Create your first exact data match

Preparation for next step

- Create the “EDM_DataUploaders” security group
- Install the Exact Data Match (EDM) agent
- Separate the hashing and uploading process
- Automate the process of uploading live data

Create exact data match sensitive information type in the New Experience workflow



EDM classifiers

New EDM experience On

Learn the end-to-end workflow

Industry-specific sample files

Why are there two experiences?

Exact data match (EDM) classifiers use exact values from your org's data to detect matches instead of generic patterns. They can then be included in several compliance solutions to classify and protect sensitive data. Learn more about EDM

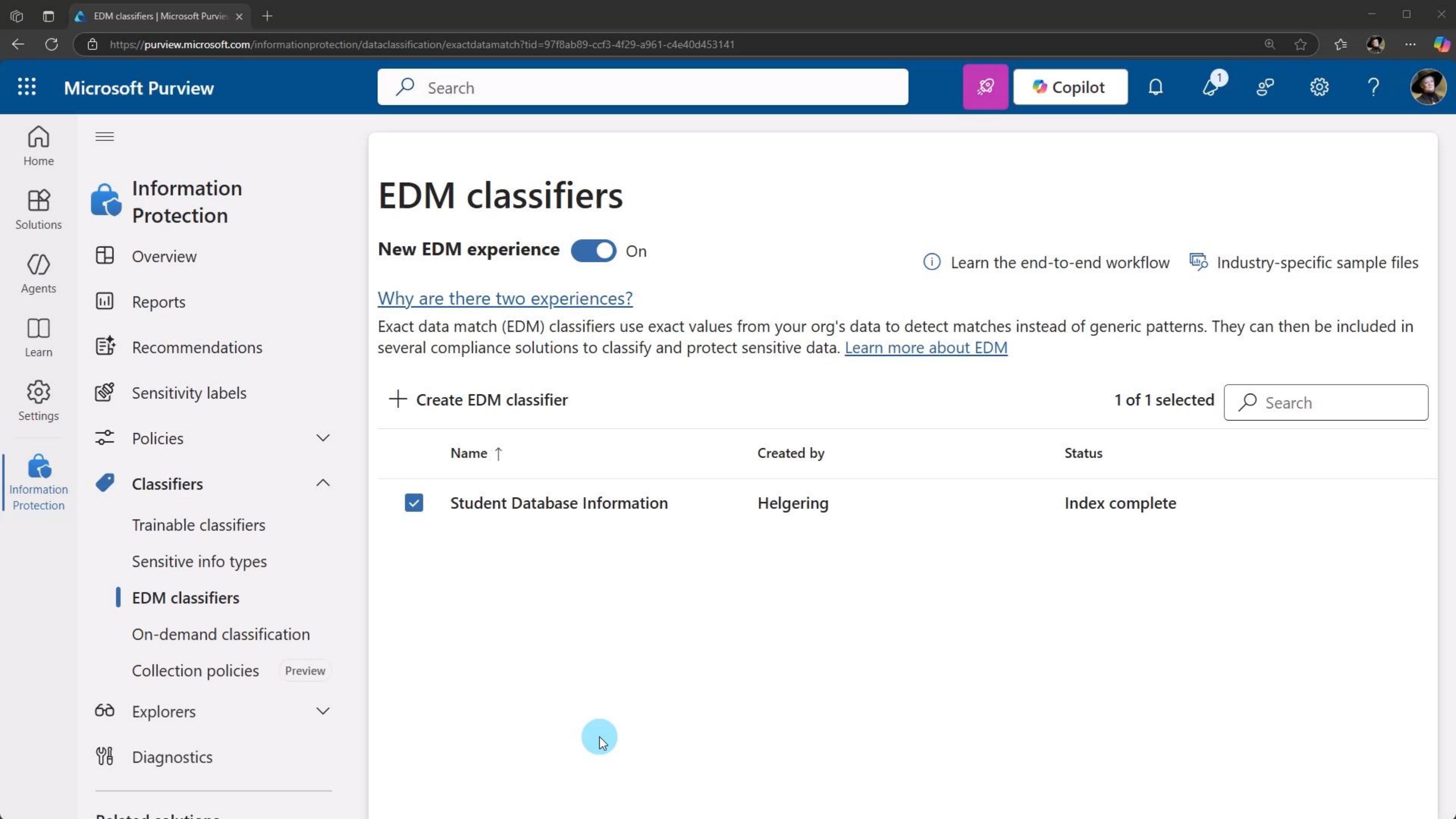
+ Create EDM classifier

1 item

Search

	Name ↑	Created by	Status
□	Student Database Information	Helgering	Source file not uploaded yet How to upload

Waiting….. (maximum of 1 hour)



EDM classifiers

New EDM experience On

Why are there two experiences?

Exact data match (EDM) classifiers use exact values from your org's data to detect matches instead of generic patterns. They can then be included in several compliance solutions to classify and protect sensitive data. Learn more about EDM

1 of 1 selected

	Name ↑	Created by	Status
☑	Student Database Information	Helgering	Index complete

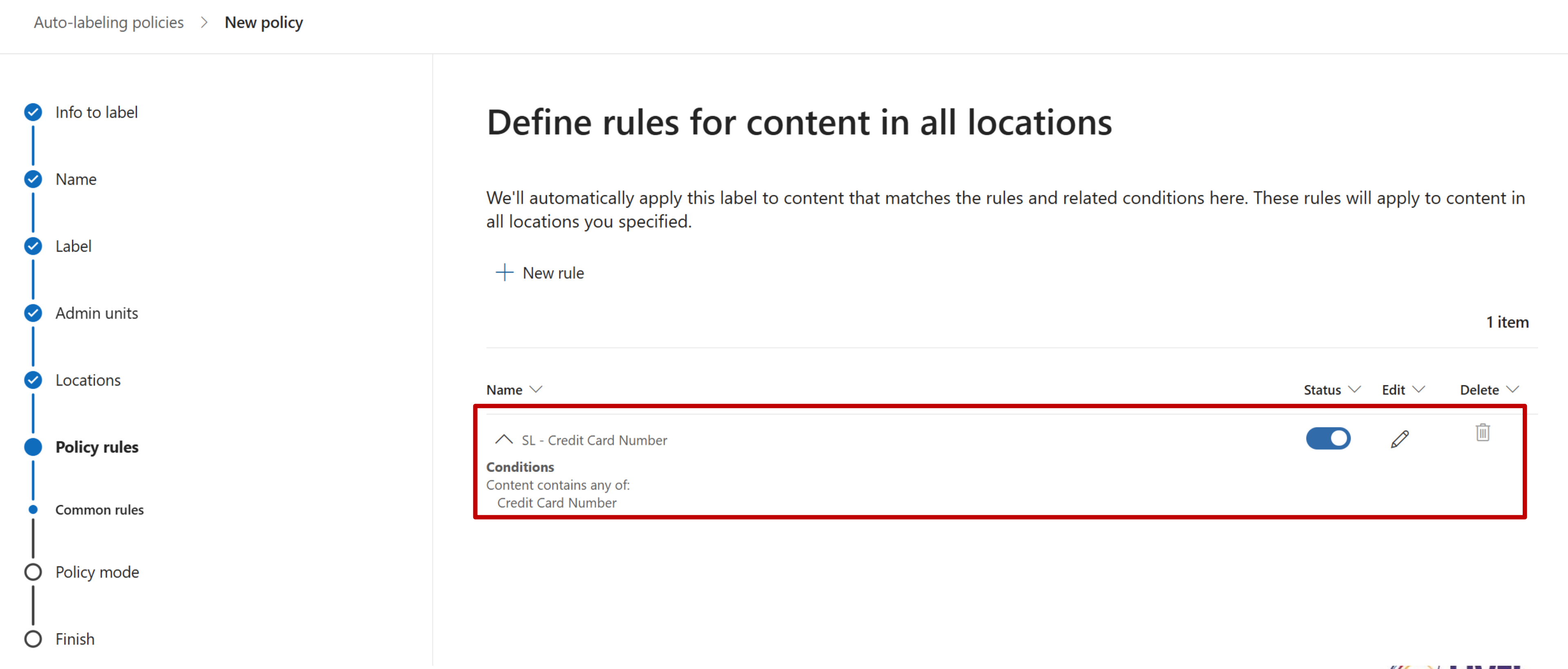
Goal achieved

1. Identify where sensitive information is stored with the Data Explorer
2. Classify data that contains a StudentID with a Custom SIT
3. Classify student information forms with a Fingerprint SIT
4. Classify potion recipes with a Trainable Classifier
5. Classify data containing information that exactly matches the student record database with an Exact Data Match Classifier

Where can we use Classifiers in Purview?

LIVE! 360 TECH EVENTS WITH PERSPECTIVE

Information Protection



Auto-labeling policies > **New policy**

- ✓ Info to label
- ✓ Name
- ✓ Label
- ✓ Admin units
- ✓ Locations
- ● **Policy rules**
- • Common rules
- ○ Policy mode
- ○ Finish

Define rules for content in all locations

We'll automatically apply this label to content that matches the rules and related conditions here. These rules will apply to content in all locations you specified.

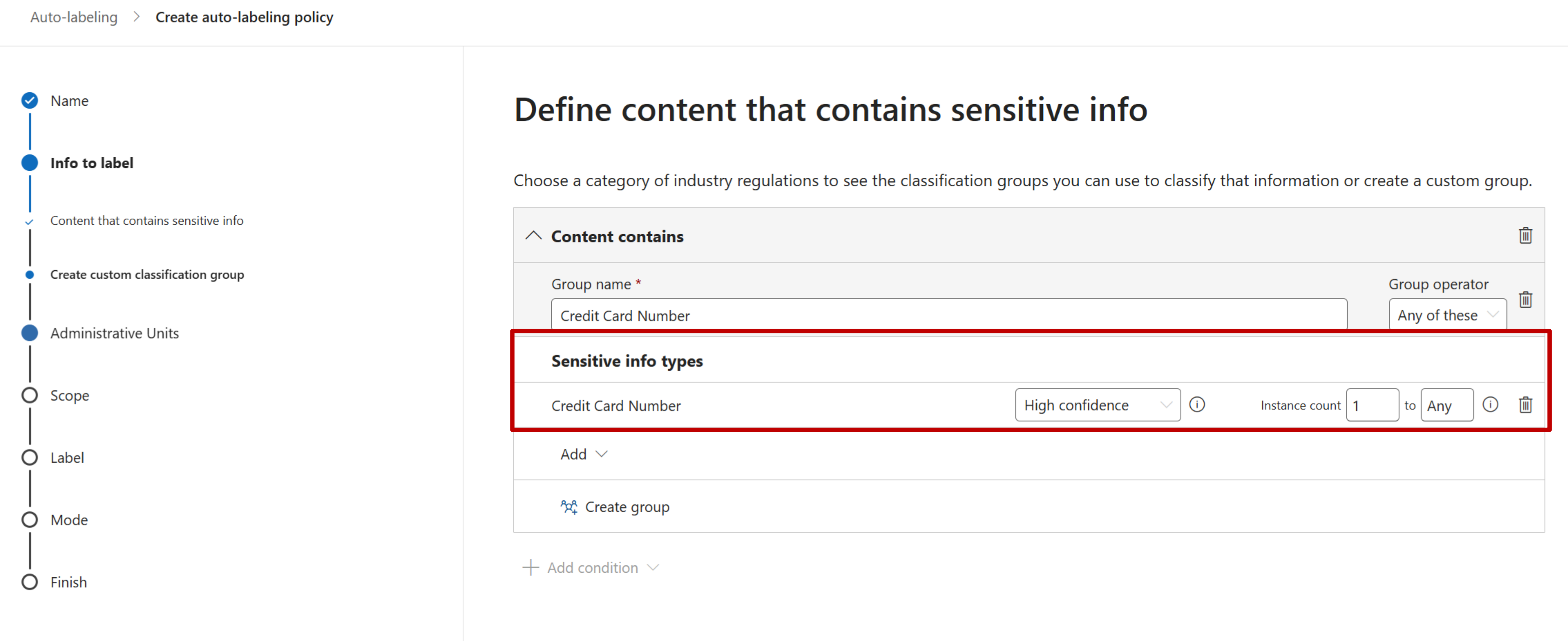
+ New rule

1 item

Name	Status	Edit	Delete
SL - Credit Card Number	●	✎	🗑

Conditions
Content contains any of:
Credit Card Number

Data Lifecycle Management



Auto-labeling > **Create auto-labeling policy**

- ● Name
- ● **Info to label**
- ✓ Content that contains sensitive info
- ● **Create custom classification group**
- ● Administrative Units
- ○ Scope
- ○ Label
- ○ Mode
- ○ Finish

Define content that contains sensitive info

Choose a category of industry regulations to see the classification groups you can use to classify that information or create a custom group.

Content contains

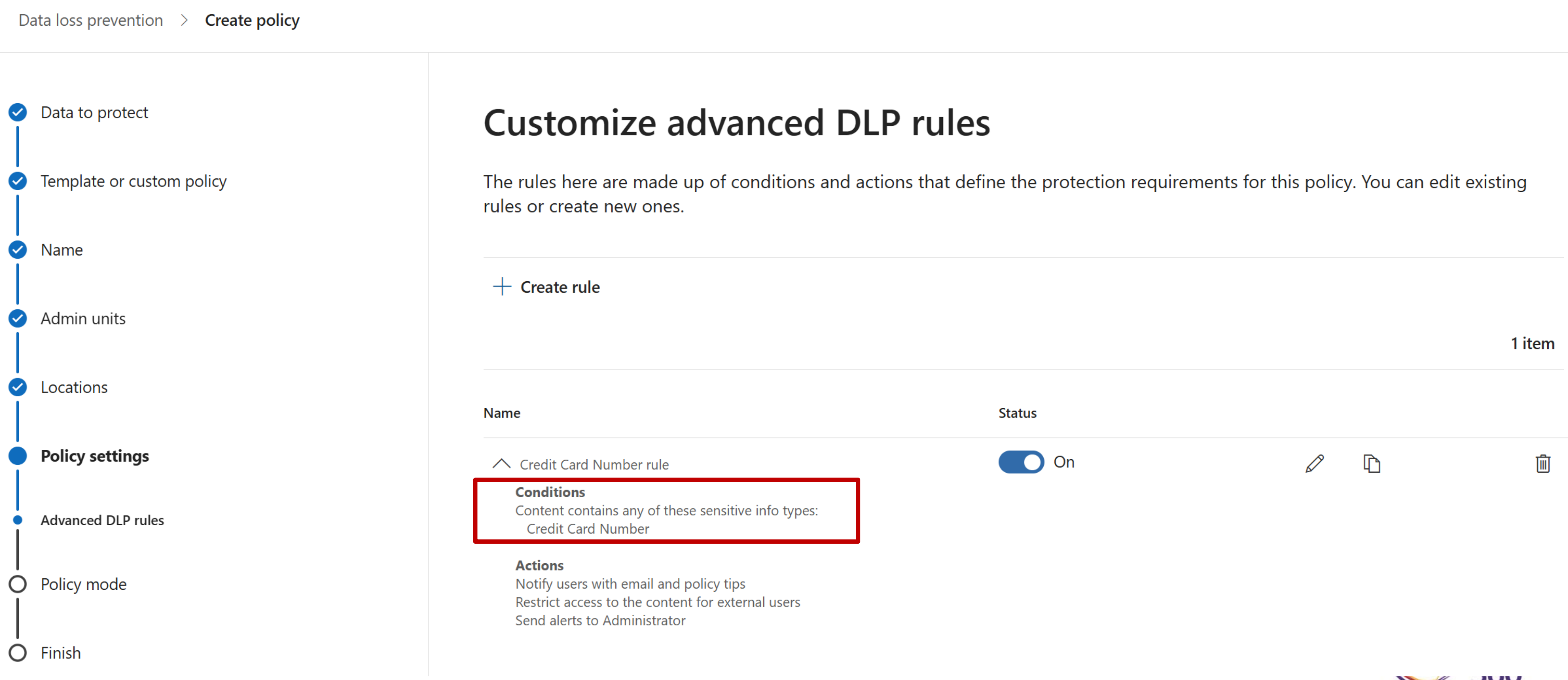
Group name *: Credit Card Number

Group operator: Any of these

Sensitive info types

Credit Card Number | High confidence | Instance count 1 to Any

Data Loss Prevention



Data loss prevention > **Create policy**

- ✓ Data to protect
- ✓ Template or custom policy
- ✓ Name
- ✓ Admin units
- ✓ Locations
- ● **Policy settings**
- • **Advanced DLP rules**
- ○ Policy mode
- ○ Finish

Customize advanced DLP rules

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones.

+ Create rule

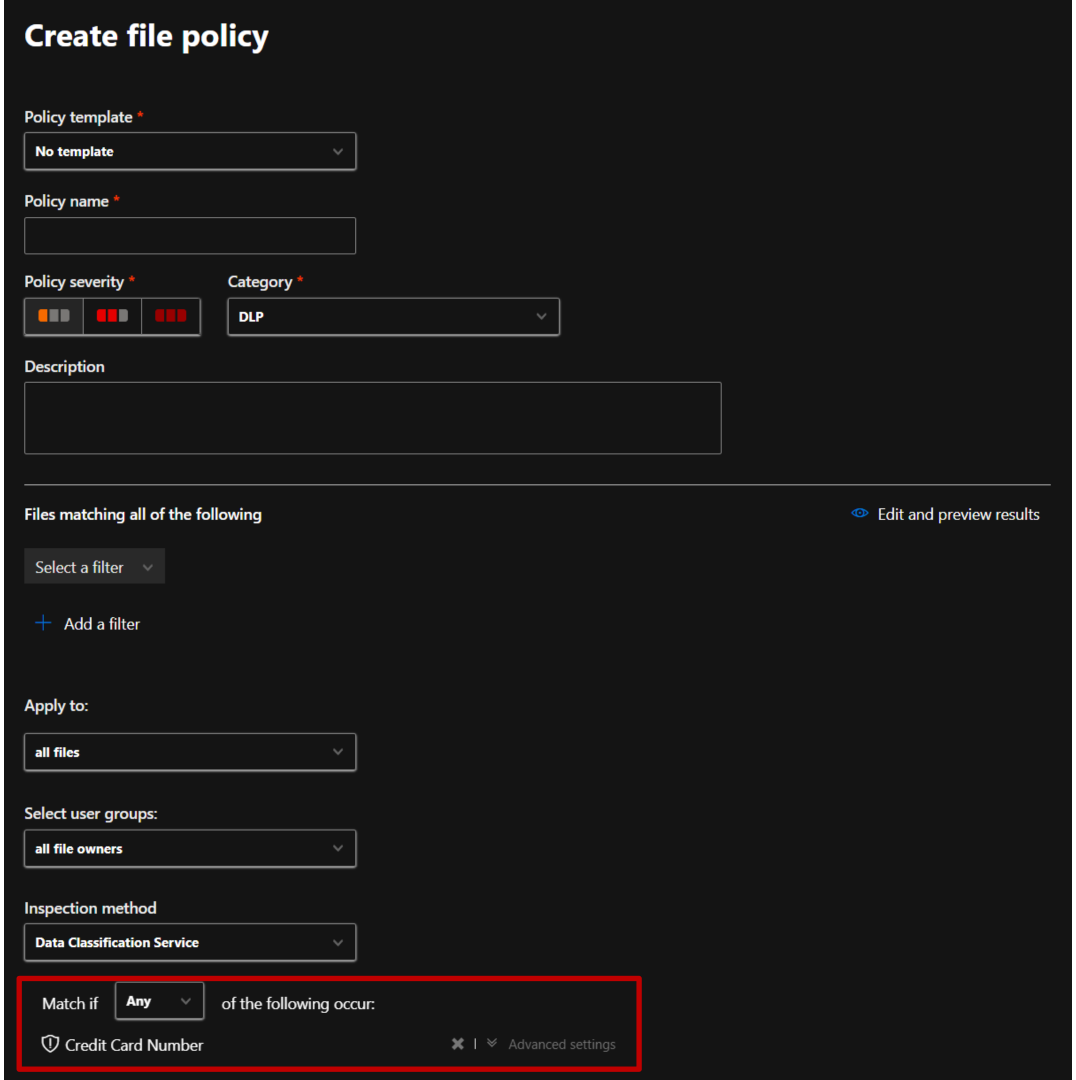
1 item

Name	Status
Credit Card Number rule	On

Conditions
Content contains any of these sensitive info types:
Credit Card Number

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

Defender for Cloud Apps



Create file policy

Policy template *

No template

Policy name *

Policy severity *

Category *

DLP

Description

Files matching all of the following

Edit and preview results

Select a filter

+ Add a filter

Apply to:

all files

Select user groups:

all file owners

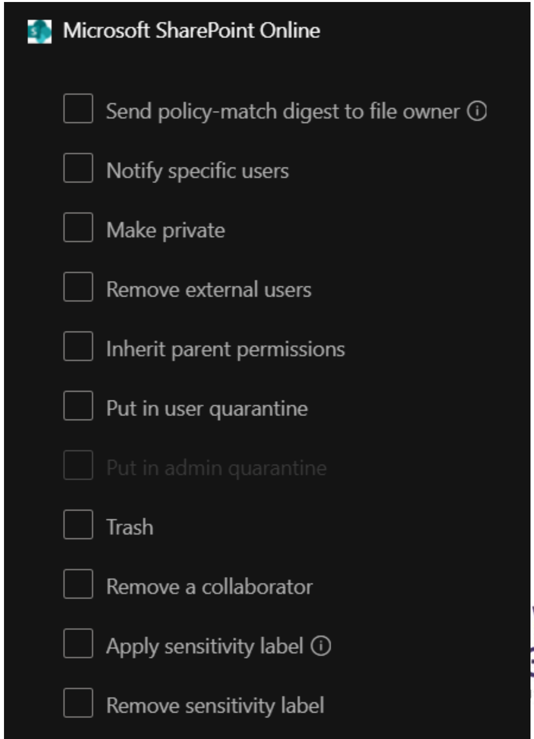
Inspection method

Data Classification Service

Match if Any of the following occur:

Credit Card Number

Advanced settings



Microsoft SharePoint Online

□ Send policy-match digest to file owner ⓘ

□ Notify specific users

□ Make private

□ Remove external users

□ Inherit parent permissions

□ Put in user quarantine

□ Put in admin quarantine

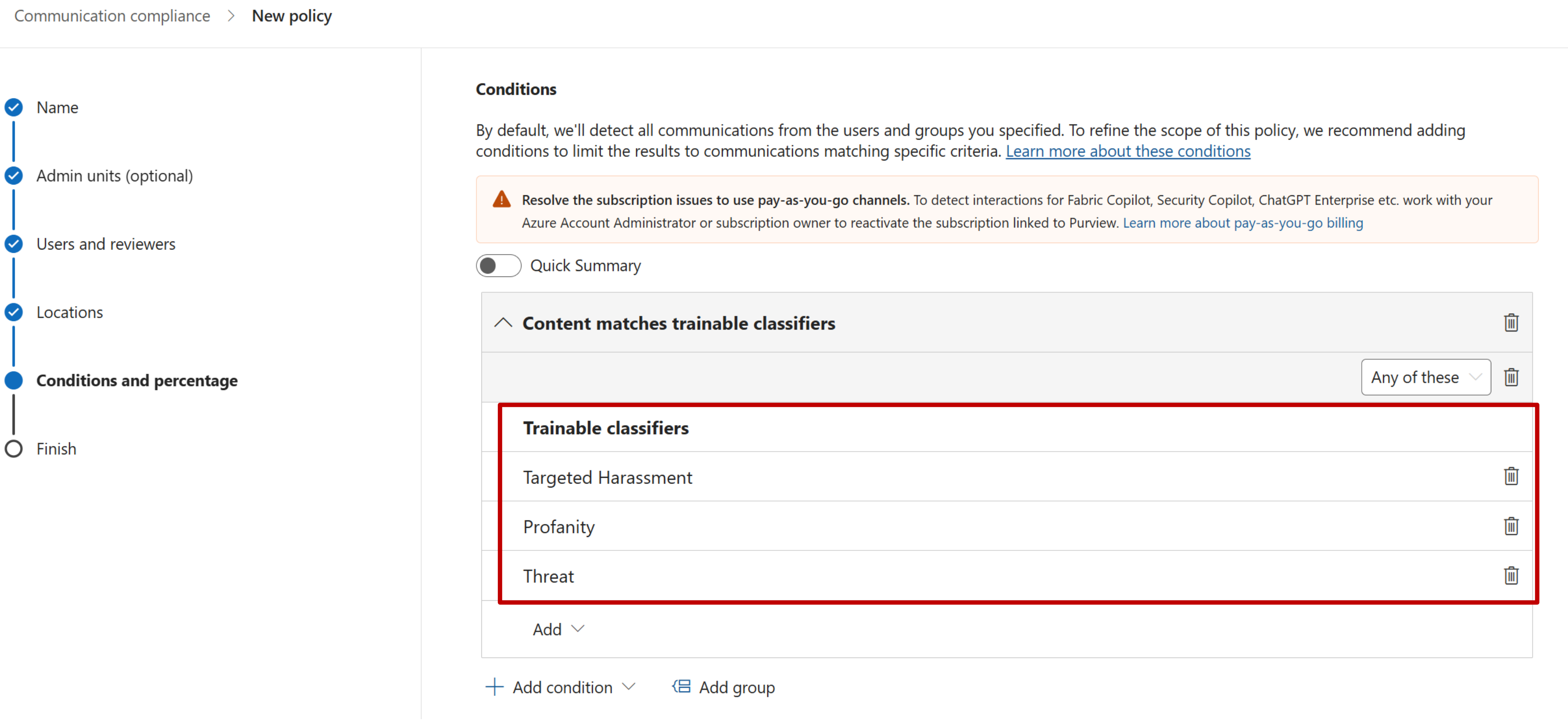
□ Trash

□ Remove a collaborator

□ Apply sensitivity label ⓘ

□ Remove sensitivity label

Communication Compliance



Communication compliance > **New policy**

- ✓ Name
- ✓ Admin units (optional)
- ✓ Users and reviewers
- ✓ Locations
- ● **Conditions and percentage**
- ○ Finish

Conditions

By default, we'll detect all communications from the users and groups you specified. To refine the scope of this policy, we recommend adding conditions to limit the results to communications matching specific criteria. Learn more about these conditions

⚠ **Resolve the subscription issues to use pay-as-you-go channels.** To detect interactions for Fabric Copilot, Security Copilot, ChatGPT Enterprise etc. work with your Azure Account Administrator or subscription owner to reactivate the subscription linked to Purview. Learn more about pay-as-you-go billing

○ Quick Summary

Content matches trainable classifiers

Any of these

Trainable classifiers

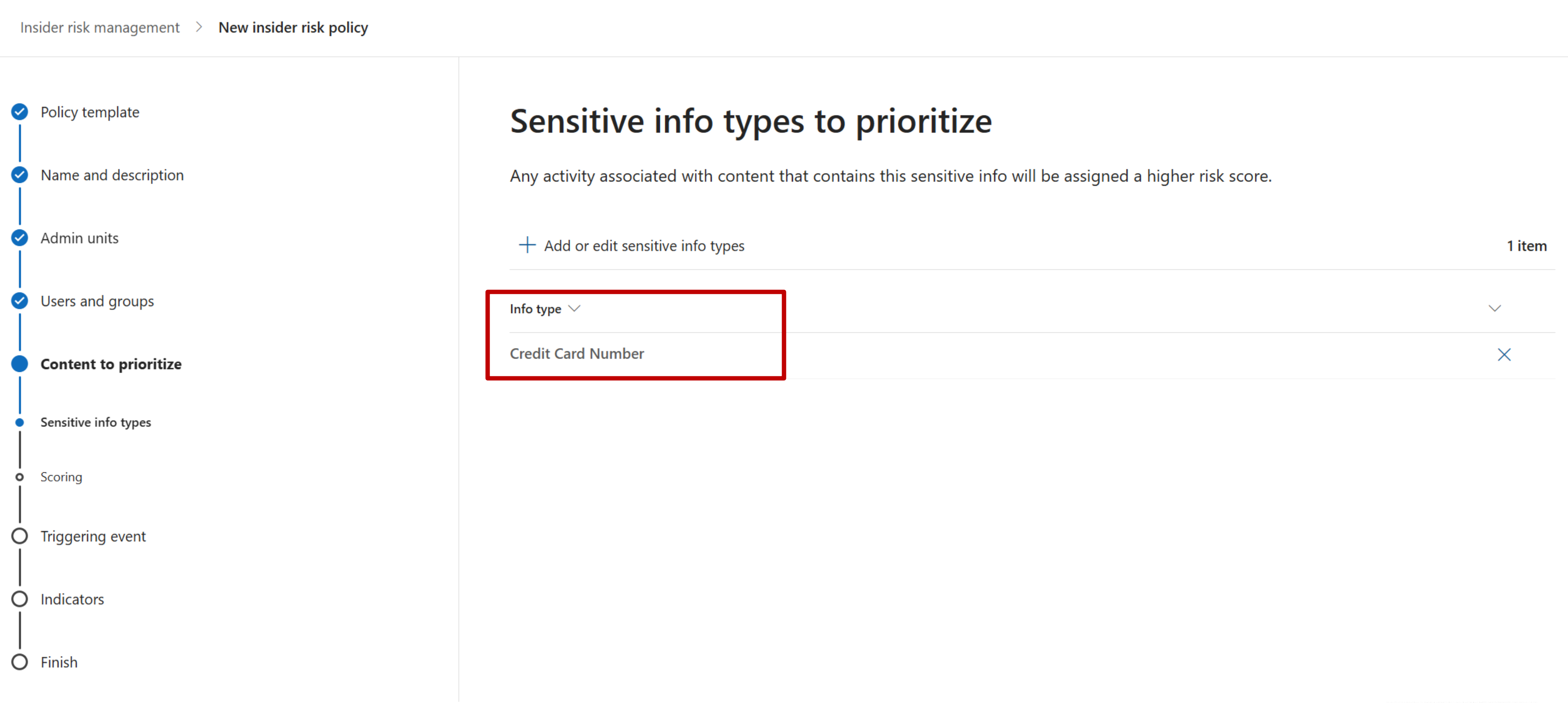
- Targeted Harassment
- Profanity
- Threat

Add

+ Add condition

Add group

Insider Risk Management



Insider risk management > New insider risk policy

- ● Policy template
- ● Name and description
- ● Admin units
- ● Users and groups
- ● **Content to prioritize**
  - **Sensitive info types**
  - Scoring
- ○ Triggering event
- ○ Indicators
- ○ Finish

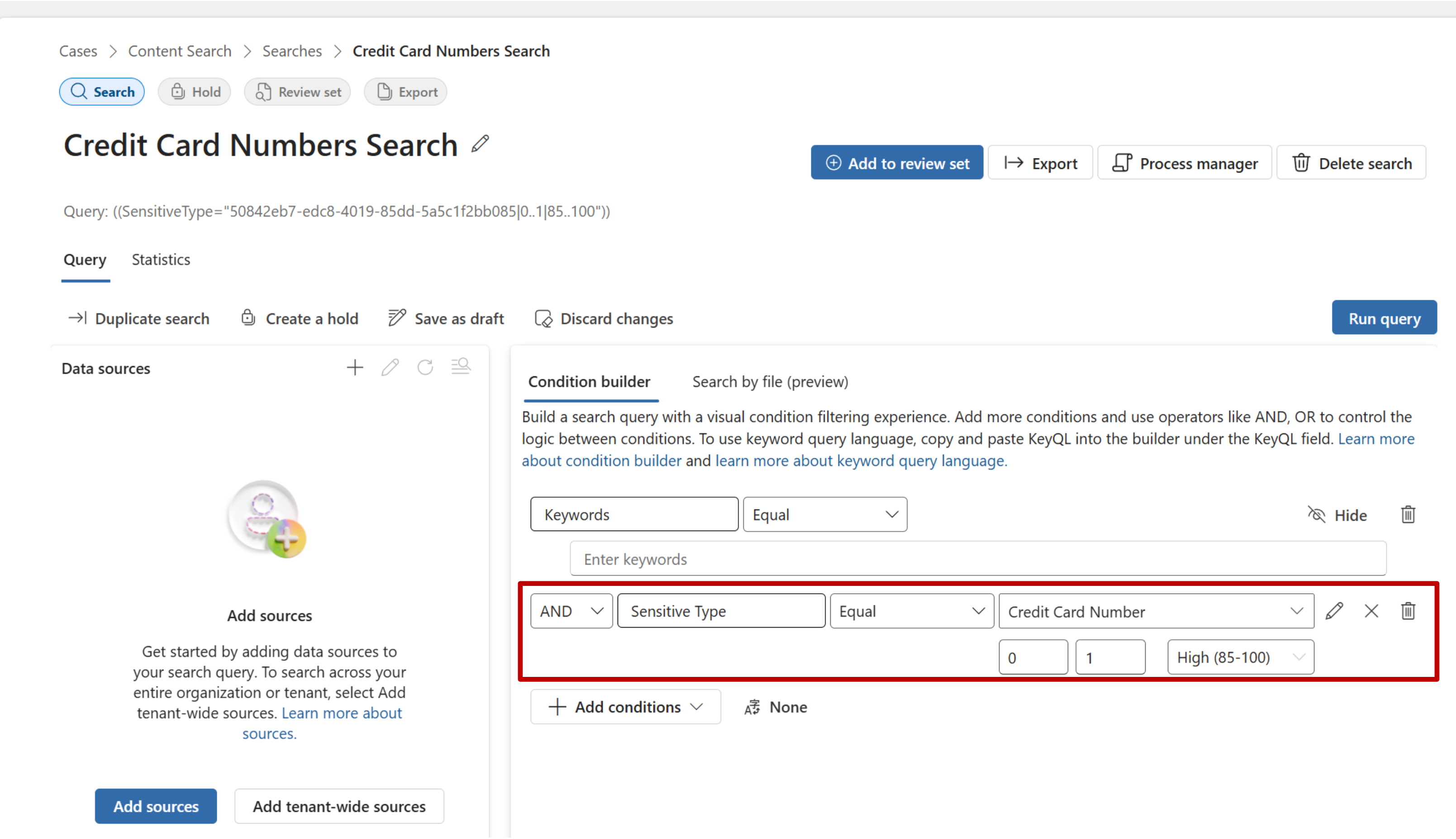
Sensitive info types to prioritize

Any activity associated with content that contains this sensitive info will be assigned a higher risk score.

1 item

Info type
Credit Card Number

eDiscovery



Cases > Content Search > Searches > Credit Card Numbers Search

Credit Card Numbers Search

Query: ((SensitiveType="50842eb7-edc8-4019-85dd-5a5c1f2bb085|0..1|85..100"))

Add sources

Get started by adding data sources to your search query. To search across your entire organization or tenant, select Add tenant-wide sources. Learn more about sources.

Build a search query with a visual condition filtering experience. Add more conditions and use operators like AND, OR to control the logic between conditions. To use keyword query language, copy and paste KeyQL into the builder under the KeyQL field. Learn more about condition builder and learn more about keyword query language.

Keywords | Equal | Hide

Enter keywords

AND | Sensitive Type | Equal | Credit Card Number

0 | 1 | High (85-100)

Takeaways

- Let classifiers be part of your classification process
- Don’t rely on automation alone; involve your users
- Use a classifier that fits the type of data
- The task of managing classifiers is never done

in/myronhelgering myronhelgering.com

Time for questions!

Other sessions @ Live! 360

- Wednesday, November 19, 2025
  - Automated Data Security: Identifying Sensitive Data with Microsoft Purview **(9:30am – 10:45am)**
- Thursday, November 20, 2025
  - Six Methods to Protect your Business from the Threat of Unmanaged Devices **(1:00pm – 2:15pm)**
  - The Challenge of Providing Secure Access to External Admins **(2:30pm – 3:45pm)**

Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!

Thank you!