

Creating Classifiers from Scratch to Identify Sensitive Data with Microsoft Purview

Myron Helgering

Tech Lead Security

Pink Elephant

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!



Agenda

- Introduction and scenario
- Classifiers
 - Sensitive Information Types
 - Fingerprint SITs
 - Trainable Classifiers
 - Exact Data Match Classifiers
- Classifier Usage
- Takeaways & Q&A

About me

- Technology Lead Security
- Microsoft Security MVP
- Blogger and Speaker
- Huge fantasy geek



Myron Helgering



in/myronhelgering



myronhelgering.com

Meet Minerva McGonagall



- Professor at Hogwarts School
- Chief Information Security Officer (CISO)
- Her goal is to **identify** and **protect** sensitive school data

What does sensitive data look like?

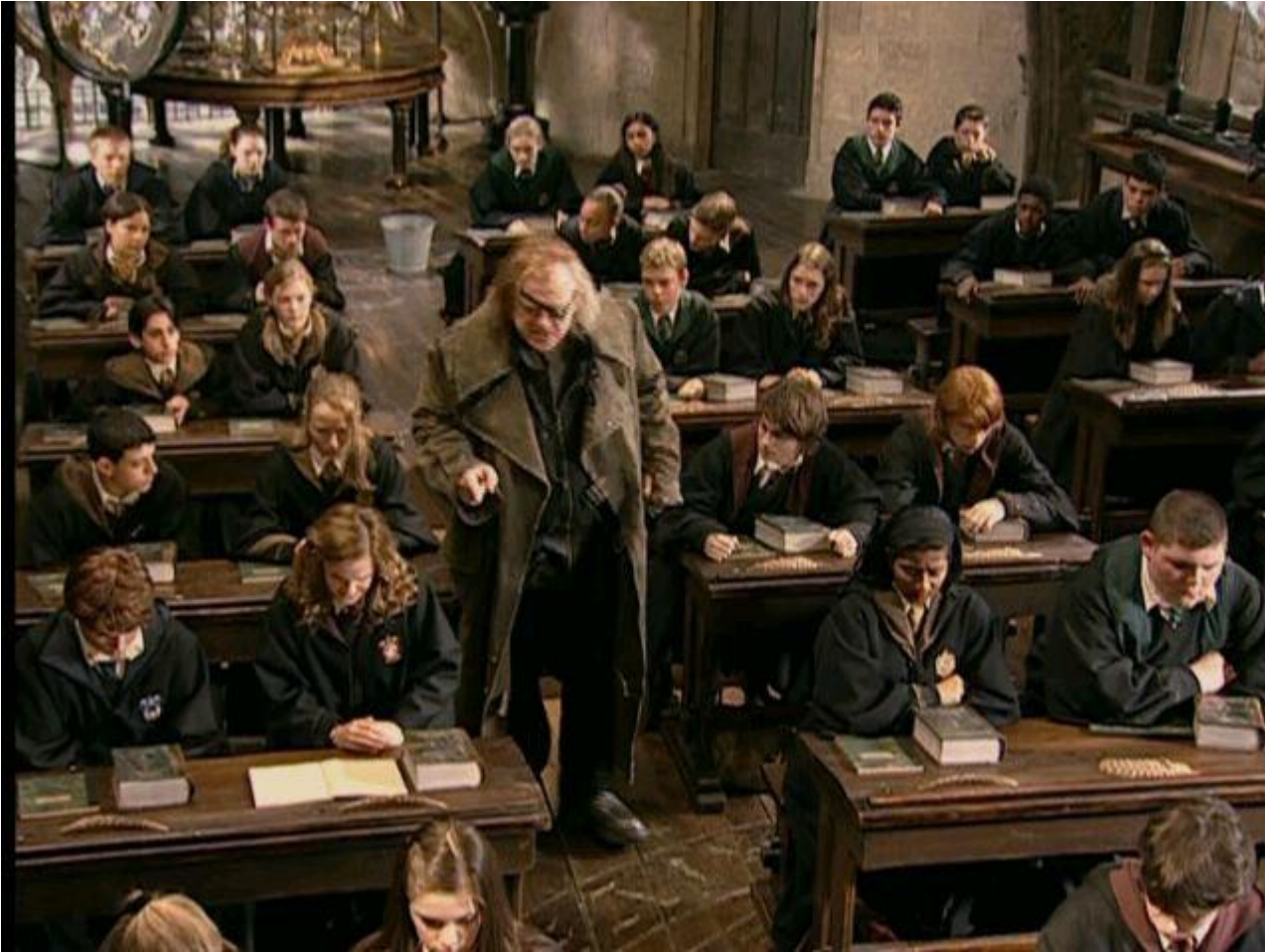


Sensitive information for healthcare

- Patient number
- Insurance number
- Medical record
- Treatment plan
- Lab rapport
- Medical terms



Sensitive information for education



- Student number
- Student PII
- Student grades
- Student database
- Education records
- Class schedules

Don't guess but find out!

- Talk to the security stakeholders
- Talk to the data owners
- Determine your top 5 most sensitive information types
- Ask for examples, formats and templates to work with
- Start creating and finetuning SITs to identify sensitive information

Hogwarts Sensitive Information Types (Top 5)



1. Passport numbers
2. StudentID
3. Student Information Forms
4. Potion Recipes
5. Student Record Database

License and permissions

- Access Data Explorer
 - Access to Endpoint DLP
 - Auto-classify data based on classifiers
 - Use advanced classifiers (e.g. trainable and EDM classifiers)
- 
- M365 E5 or Purview suite
-
- Create classifiers and policies
 - View content in Data Explorer
- 
- Compliance Administrator role
 - Content Explorer Content viewer

Built-in Sensitive Information Types

327 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		
Trainable classifiers	<u>Sensitive info types</u>	EDM classifiers
The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we		
+ Create sensitive info type + Create Fingerprint based SIT Refresh		
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

Overview | Microsoft Purview

https://purview.microsoft.com/informationprotection/purviewmipoverview?tid=97f8ab89-ccf3-4f29-a961-c4e40d453141

Microsoft Purview

Search

Copilot

Home

Solutions

Agents

Learn

Settings

Information Protection

Information Protection

Overview

Reports

Recommendations

Sensitivity labels

Policies

Classifiers

Explorers

Data explorer

Content explorer (classic)

Activity explorer

Diagnostics

Related solutions

Data Lifecycle Management

Data Loss Prevention

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

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](#)

View all 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/>*



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;
-------	--------------

[Continue >](#)

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
```

Text

Tests

1 match (0.6ms)

```
C12345678
```

Tools

Replace

List

Details

Explain



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.

]

Demo: Custom Sensitive Information Types



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

Classifier Simulation Mode

Microsoft Purview: Purview Information Protection | Classifier Simulation Mode (Health Monitoring)

Microsoft Purview

■ □ □ IN DEVELOPMENT

PREVIEW AVAILABLE

October 2026

ROLLOUT START

November 2026

Microsoft Purview introduces the Classifier Simulation Mode, the first phase of the broader Classifier Health Monitoring Platform. This capability enables you to test, analyze, and optimize custom classifiers on production data before publishing them, hence offering a reliable means of verifying the effectiveness of classifiers before committing them to live environments. Custom classifiers are powerful tools but can sometimes include inefficient regex patterns or overly broad logic, leading to Noisy classifier due to high matches, False positives and High scanning latency Simulation Mode mitigates these risks by allowing you to validate classifier quality and performance before publishing, helping ensure healthy, performant, and more precise classification outcomes.

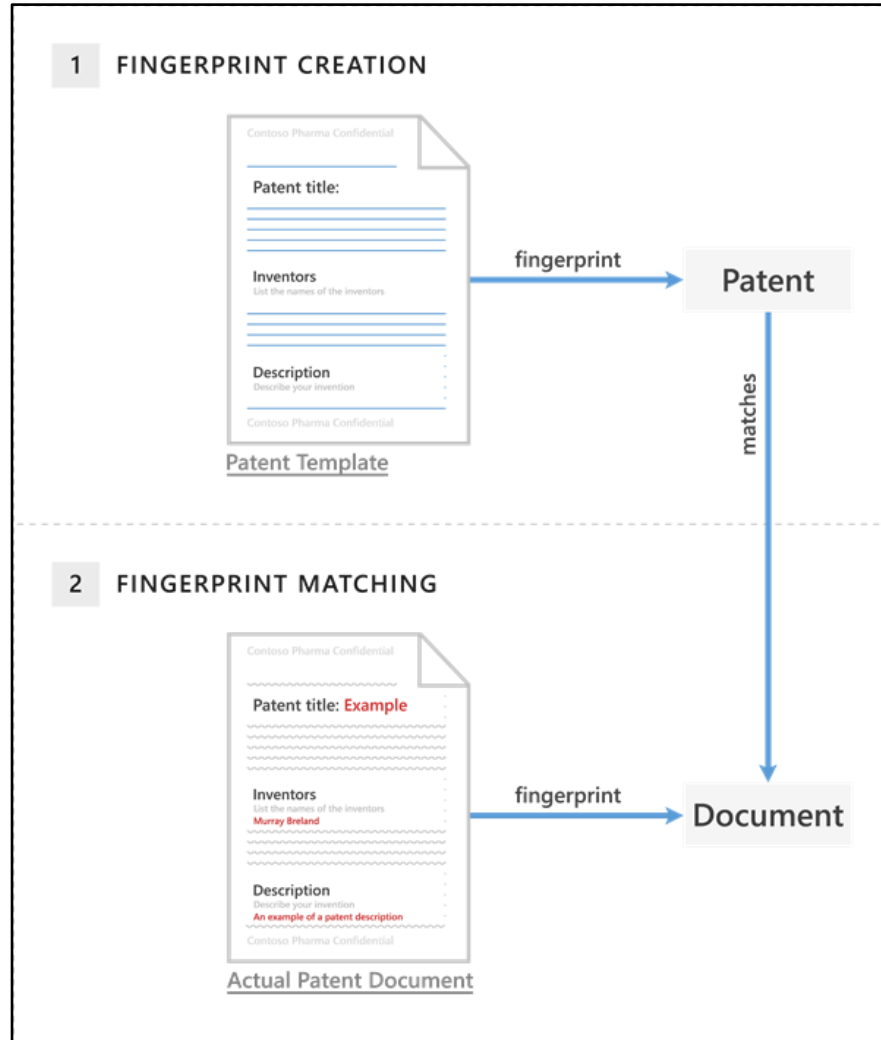
Roadmap ID	Cloud instances(s)	Platform(s)	Release phases(s)
523201	Worldwide (Standard Multi-Tenant)	Web	General Availability

Added to roadmap: 11/05/2025 | Last modified: 07/14/2026

SHARE



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

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 | Microsoft Pu xPotion Recipe Documents (positiv xPotion Recipe Documents (negati x+

https://purview.microsoft.com/informationprotection/dataclassification/trainableclassifiers?tid=97f8ab89-ccf3-4f29-a961-c4e40d453141

Microsoft Purview

Search

Copilot

1

?

Home

Solutions

Agents

Communi... Compliance

eDiscovery

Data Loss Prevention

Information Protection

Compliance Manager

...

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

135 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

Waiting.... (maximum of 48 hours)



Trainable classifiers | Microsoft Pu x

Trainable classifiers | Microsoft Pu x

+

←

↻

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

➤ Send 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 | Microsoft Purview

https://purview.microsoft.com/informationprotection/dataclassification/exactdatamatch?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

Explorers

Diagnostics

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 | Microsoft Purview

https://purview.microsoft.com/informationprotection/dataclassification/exactdatamatch?tid=97f8ab89-ccf3-4f29-a961-c4e40d453141

Microsoft Purview

Search

Copilot

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

Explorers

Diagnostics

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 | Microsoft Purview

https://purview.microsoft.com/informationprotection/dataclassification/exactdatamatch?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

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 of 1 selected

Search

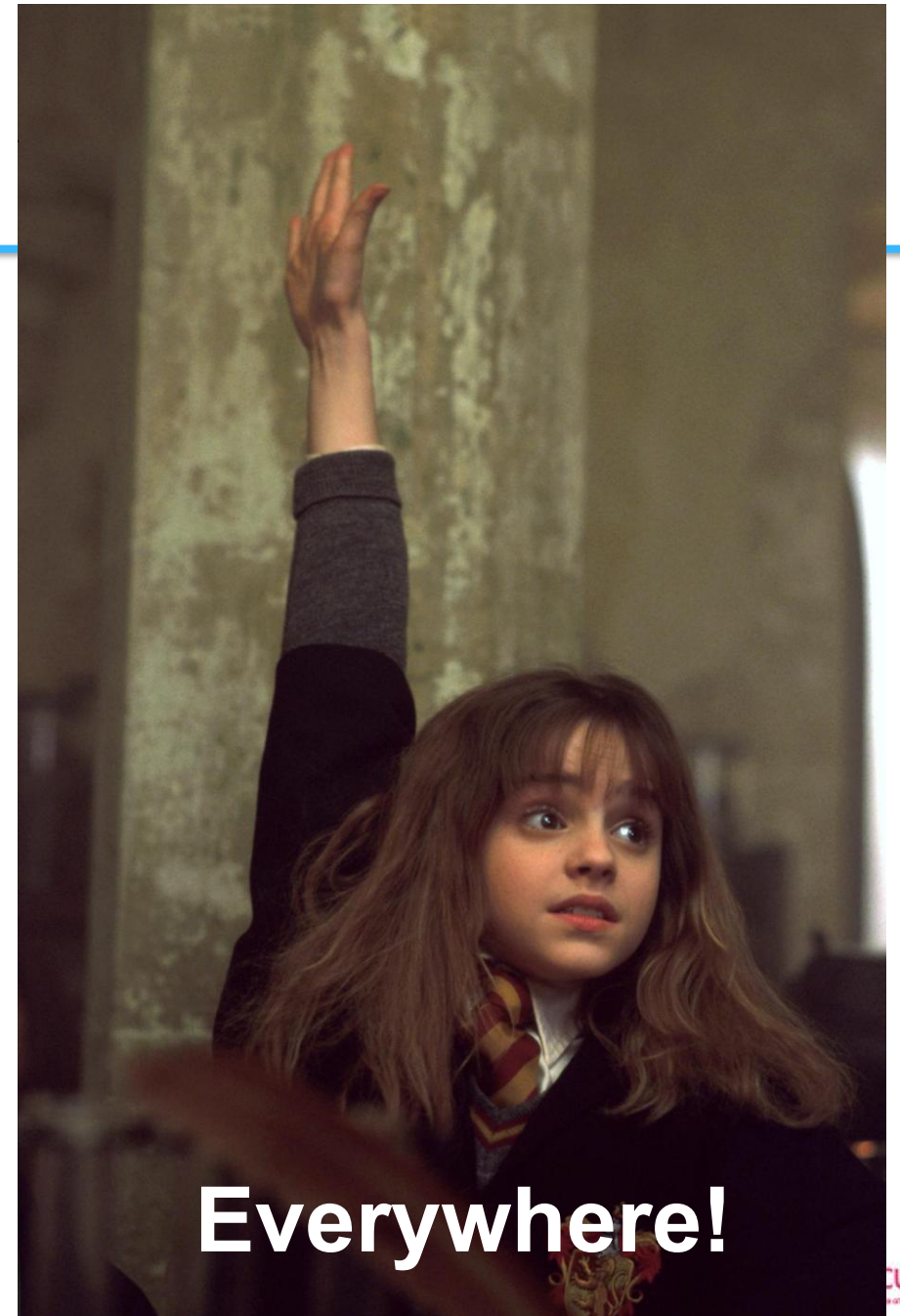
	Name ↑	Created by	Status
☒	Student Database Information	Helgering	Index complete

Goal achieved

1. Identify where passport numbers were 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?



eDiscovery

Cases > Content Search > Searches > Credit Card Numbers Search

[Search](#) [Hold](#) [Review set](#) [Export](#)

Credit Card Numbers Search

[+ Add to review set](#)

[Export](#)

[Process manager](#)

[Delete search](#)

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

[Query](#) [Statistics](#)

[Duplicate search](#)

[Create a hold](#)

[Save as draft](#)

[Discard changes](#)

[Run query](#)

Data sources



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.](#)

[Add sources](#)

[Add tenant-wide sources](#)

Condition builder

Search by file (preview)

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)

[+ Add conditions](#)

[None](#)

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

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  

Add 

 Create group

+ Add condition 

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

- ✓ 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.

+ Add or edit sensitive info types

1 item

Info type ▾



Credit Card Number



Takeaways

- Involve the business before creating classifiers
- Let classifiers be part of your classification process, but don't fully rely on them; 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 @ Cybersecurity Live!

- Tuesday, August 4, 2026
 - Creating Classifiers from Scratch to Identify Sensitive Data with Microsoft Purview **(1:15pm – 2:30pm)**
- Wednesday, August 5, 2026
 - Edge for Business in 2026: Is the Browser Becoming the New Security Perimeter? **(8:00am – 9:15am)**
 - Configuring Cross-Tenant Access for Secure Collaboration **(1:15pm – 1:40pm)**
 - How to Protect Your Business from the Threat of Unmanaged Devices **(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!

