

# MS Copilot for Security

## Get started with Microsoft Copilot for Security

- 7 hr 17 min
- Learning Path

Learn about Microsoft Copilot for Security, an AI-powered security analysis tool that enables analysts to process security signals and respond to threats at a machine speed, and the AI concepts upon which it's built.

## Prerequisites

- Working knowledge of security operations and incident response
  - Working knowledge of Microsoft security products and services
- 

### Fundamental AI Concepts

- 36 min
- Module
- 0 of 10 units completed

With AI, we can build solutions that seemed like science fiction a short time ago; enabling incredible advances in health care, financial management, environmental protection, and other areas to make a better world for everyone.

### Start

#### Overview

- Introduction to AI 2 min
- Understand machine learning 4 min
- Understand computer vision 5 min

- [Understand natural language processing](#)4 min
  - [Understand document intelligence and knowledge mining](#)3 min
  - [Understand generative AI](#)2 min
  - [Challenges and risks with AI](#)3 min
  - [Understand Responsible AI](#)10 min
  - [Knowledge check](#)2 min
  - [Summary](#)1 min
- 

## Introduction to AI

AI enables us to build amazing software that can improve health care, enable people to overcome physical disadvantages, empower smart infrastructure, create incredible entertainment experiences, and even save the planet!

## What is AI?

Simply put, AI is software that imitates human behaviors and capabilities. Key workloads include:

- **Machine learning** - This is often the foundation for an AI system, and is the way we "teach" a computer model to make predictions and draw conclusions from data.
  - **Computer vision** - Capabilities within AI to interpret the world visually through cameras, video, and images.
  - **Natural language processing** - Capabilities within AI for a computer to interpret written or spoken language, and respond in kind.
  - **Document intelligence** - Capabilities within AI that deal with managing, processing, and using high volumes of data found in forms and documents.
  - **Knowledge mining** - Capabilities within AI to extract information from large volumes of often unstructured data to create a searchable knowledge store.
  - **Generative AI** - Capabilities within AI that create original content in a variety of formats including natural language, image, code, and more.
-

# Understand machine learning

Completed 100 XP

- 4 minutes

Machine Learning is the foundation for most AI solutions. Since the 1950's, researchers, often known as *data scientists*, have worked on different approaches to AI. Most modern applications of AI have their origins in machine learning, a branch of AI that combines computer science and mathematics.

Let's start by looking at a real-world example of how machine learning can be used to solve a difficult problem.

Sustainable farming techniques are essential to maximize food production while protecting a fragile environment. *The Yield*, an agricultural technology company based in Australia, uses sensors, data, and machine learning to help farmers make informed decisions related to weather, soil, and plant conditions.

## How machine learning works

So how do machines learn?

The answer is, from data. In today's world, we create huge volumes of data as we go about our everyday lives. From the text messages, emails, and social media posts we send to the photographs and videos we take on our phones, we generate massive amounts of information. More data still is created by millions of sensors in our homes, cars, cities, public transport infrastructure, and factories.

Data scientists can use all of that data to train machine learning models that can make predictions and inferences based on the relationships they find in the data.

Machine learning models try to capture the relationship between data. For example, suppose an environmental conservation organization wants volunteers to identify and catalog different species of wildflower using a phone app. The following animation shows how machine learning can be used to enable this scenario.

1. A team of botanists and scientists collect data on wildflower samples.
2. The team labels the samples with the correct species.

3. The labeled data is processed using an algorithm that finds relationships between the features of the samples and the labeled species.
4. The results of the algorithm are encapsulated in a model.
5. When new samples are found by volunteers, the model can identify the correct species label.

Approaches to AI have advanced to complete tasks of much greater complexity. These complex models form the basis of AI capabilities.

## Machine learning in Microsoft Azure

Microsoft Azure provides the **Azure Machine Learning** service - a cloud-based platform for creating, managing, and publishing machine learning models. **Azure Machine Learning Studio** offers multiple authoring experiences such as:

- **Automated machine learning**: this feature enables non-experts to quickly create an effective machine learning model from data.
  - **Azure Machine Learning designer**: a graphical interface enabling no-code development of machine learning solutions.
  - **Data metric visualization**: analyze and optimize your experiments with visualization.
  - **Notebooks**: write and run your own code in managed Jupyter Notebook servers that are directly integrated in the studio.
- 

## Understand computer vision

Completed 100 XP

- 5 minutes

Computer Vision is an area of AI that deals with visual processing. Let's explore some of the possibilities that computer vision brings.

The **Seeing AI** app is a great example of the power of computer vision. Designed for the blind and low vision community, the Seeing AI app harnesses the power of AI to open up the visual world and describe nearby people, text and objects.



To find out more, check out the [Seeing AI web page](#).

# Computer Vision models and capabilities



Most computer vision solutions are based on machine learning models that can be applied to visual input from cameras, videos, or images. The following table describes common computer vision tasks.

Expand table

Task	Description
Image classification	<div></div> <p>Image classification involves training a machine learning model to classify images based on their contents. For example, in a traffic monitoring solution you might use an image classification model to classify images based on the type of vehicle they contain, such as taxis, buses, cyclists, and so on.</p>
Object detection	<div></div>

Task	Description
	<p>Object detection machine learning models are trained to classify individual objects within an image, and identify their location with a bounding box. For example, a traffic monitoring solution might use object detection to identify the location of different classes of vehicle.</p>
Semantic segmentation	 <p>Semantic segmentation is an advanced machine learning technique in which individual pixels in the image are classified according to the object to which they belong. For example, a traffic monitoring solution might overlay traffic images with "mask" layers to highlight different vehicles using specific colors.</p>
Image analysis	 <p>You can create solutions that combine machine learning models with advanced image analysis</p>



Task	Description
	techniques to extract information from images, including "tags" that could help catalog the image or even descriptive captions that summarize the scene shown in the image.
Face detection, analysis, and recognition	<div data-bbox="579 164 1377 693" data-label="Image"></div> <p>Face detection is a specialized form of object detection that locates human faces in an image. This can be combined with classification and facial geometry analysis techniques to recognize individuals based on their facial features.</p>
Optical character recognition (OCR)	<div data-bbox="579 876 1377 1409" data-label="Image"></div> <p>Optical character recognition is a technique used to detect and read text in images. You can use OCR to read text in photographs (for example, road signs or store fronts) or to extract information from scanned documents such as letters, invoices, or forms.</p>

# Computer vision services in Microsoft Azure

You can use Microsoft's **Azure AI Vision** to develop computer vision solutions. The service features are available for use and testing in the **Azure Vision Studio** and other programming languages. Some features of Azure AI Vision include:

- **Image Analysis**: capabilities for analyzing images and video, and extracting descriptions, tags, objects, and text.
  - **Face**: capabilities that enable you to build face detection and facial recognition solutions.
  - **Optical Character Recognition (OCR)**: capabilities for extracting printed or handwritten text from images, enabling access to a digital version of the scanned text.
- 

## Understand natural language processing

Completed 100 XP

- 4 minutes

Natural language processing (NLP) is the area of AI that deals with creating software that understands written and spoken language.

NLP enables you to create software that can:

- Analyze and interpret text in documents, email messages, and other sources.
- Interpret spoken language, and synthesize speech responses.
- Automatically translate spoken or written phrases between languages.
- Interpret commands and determine appropriate actions.

For example, *Starship Commander* is a virtual reality (VR) game from Human Interact that takes place in a science fiction world. The game uses natural language processing to enable players to control the narrative and interact with in-game characters and starship systems.

## Natural language processing in Microsoft Azure



You can use Microsoft's **Azure AI Language** to build natural language processing solutions. Some features of Azure AI Language include understanding and analyzing text, training conversational language models that can understand spoken or text-based commands, and building intelligent applications.

Microsoft's **Azure AI Speech** is another service that can be used to build natural language processing solutions. Azure AI Speech features include speech recognition and synthesis, real-time translations, conversation transcriptions, and more.

You can explore Azure AI Language features in the **Azure Language Studio** and Azure AI Speech features in the **Azure Speech Studio**. The service features are available for use and testing in the studios and other programming languages.

---

## Understand document intelligence and knowledge mining

Completed 100 XP

- 3 minutes

**Document Intelligence** is the area of AI that deals with managing, processing, and using high volumes of a variety of data found in forms and documents. Document intelligence enables you to create software that can automate processing for contracts, health documents, financial forms and more

### Document intelligence in Microsoft Azure

You can use Microsoft's **Azure AI Document Intelligence** to build solutions that manage and accelerate data collection from scanned documents. Features of Azure AI Document Intelligence help automate document processing in applications and workflows, enhance data-driven strategies, and enrich document search capabilities. You can use prebuilt models to add intelligent document processing for invoices, receipts, health insurance cards, tax forms, and more. You can also use Azure AI Document Intelligence to create custom models with your own labeled datasets. The service features are available for use and testing in the **Document Intelligence Studio** and other programming languages.

Copy 2 -- To Be Filed with Employee's State, City, or Local Income Tax Return.		OMB NO. 1545-0008	
a. Employee's Soc Sec No	1. Wages, tips, other comp.	2. Federal income tax withheld	
123-45-6789	37160.56	4894.54	
b. Employer ID number (EIN)	3. Social security wages	4. Social security tax withheld	
98-7654321	37160.56	2301.95	
	5. Medicare wages and tips	6. Medicare tax withheld	
	37160.56	538.83	
c. Employer's name, address and ZIP code			
CONTOSO LTD 123 MICROSOFT WAY REDMOND, WA 98765			
d. Control Number			
000086242			
e. Employee's name, address, and ZIP code			
ANGEL BROWN 4567 MAIN STREET BUFFALO, WA 12345			
7. Social security tips	8. Allocated tips	9.	
00280	874.20		
10. Dependent care benefits	11. Nonqualified plans	12a. Code See inst. for box 12	
8073.20	DISINS	01	5939.68
13. Statutory employee	14. Other	12b. Code	
<input checked="" type="checkbox"/>	DISINS 170.85	0	5494.00
Retirement plan		12c. Code	
<input checked="" type="checkbox"/>		1	87680
Third-party sick pay		12d. Code	
<input checked="" type="checkbox"/>		0	12880
PA 87654321	37160.56		1135.65
WA 12345678	9631.20		
15. State Employer's state ID number	16. State wages, tips, etc.	17. State income tax	
18. Local wages, tips, etc.	19. Local income tax	20. Locality name	
37160.56	51.00	Camberland Vly/Mddl	
37160.56	594.54	E. Pennsboro/E. Pnns	

Fields	Result	Code
AllocatedTips #1	874.2	99.90%
ControlNumber #1	000086242	99.90%
DependentCareBenefits #1	9873.2	99.90%
Employee #1	Address	99.90%
	4567 MAIN STREET BUFFALO, WA 12345	
	HouseNumber	
	4567	
	Road	
	MAIN STREET	
	PostalCode	
	12345	

This example shows information extracted from a tax form using Azure AI Document Intelligence.

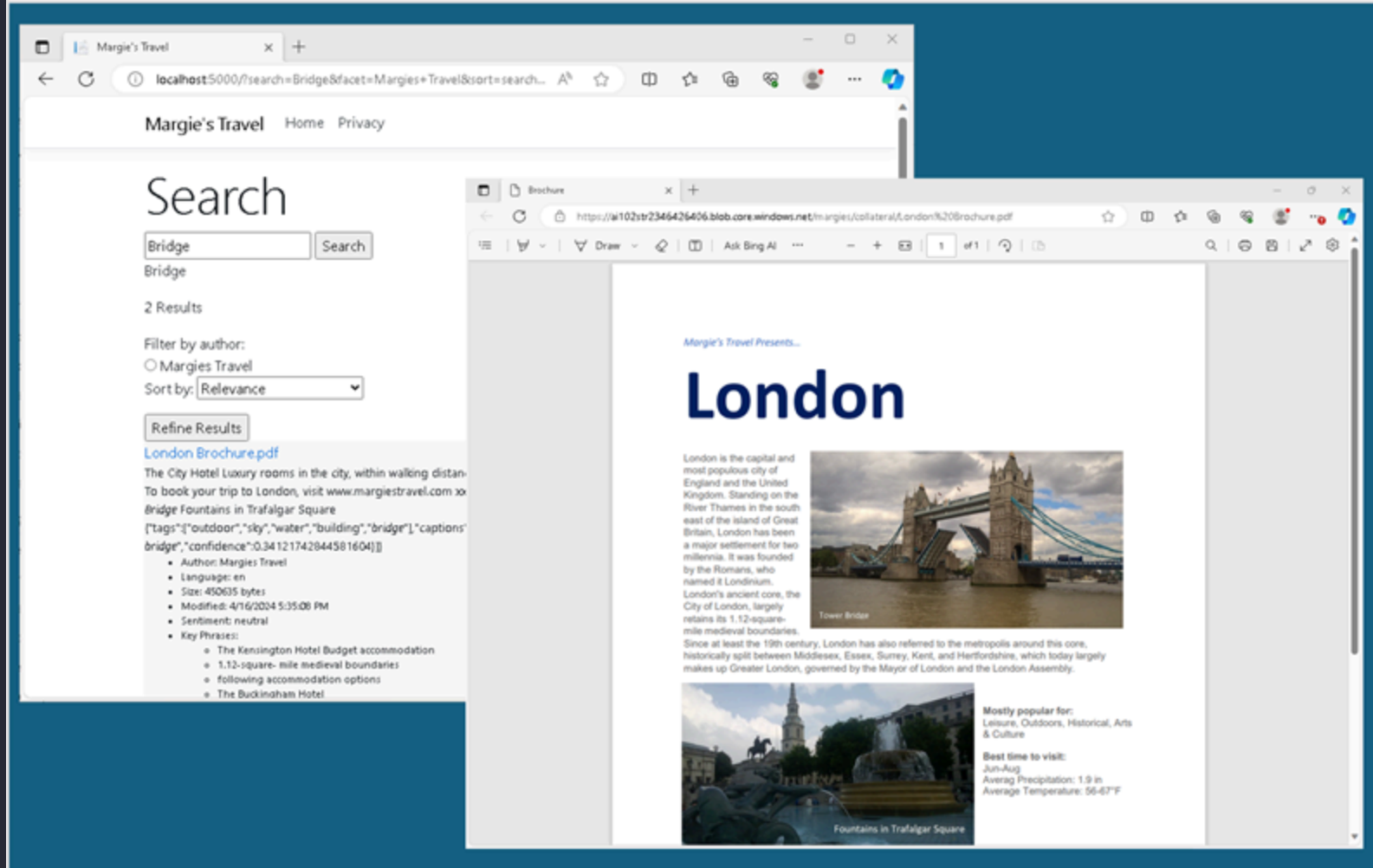
## Knowledge Mining

**Knowledge mining** is the term used to describe solutions that involve extracting information from large volumes of often unstructured data to create a searchable knowledge store.

## Knowledge mining in Microsoft Azure

One Microsoft knowledge mining solution is **Azure AI Search**, an enterprise, search solution that has tools for building indexes. The indexes can then be used for internal only use, or to enable searchable content on public facing internet assets.

Azure AI Search can utilize the built-in AI capabilities of Azure AI services such as image processing, document intelligence, and natural language processing to extract data. The product's AI capabilities makes it possible to index previously unsearchable documents and to extract and surface insights from large amounts of data quickly.



In this example, a travel web site uses Azure AI Search to power searching for information about destinations based on information extracted from images or text using AI services.

### Tip

Learn how a global engineering company uses knowledge mining to create more accurate bid proposals and reclaim the time it would take to manually compile them in this [case study](#)

## Understand generative AI

Completed 100 XP

- 2 minutes

Generative AI describes a category of capabilities within AI that create original content. People typically interact with generative AI that has been built into chat applications. Generative AI applications take in natural language input, and return appropriate responses in a variety of formats including natural language, image, code, and audio.

## Generative AI in Microsoft Azure

**Azure OpenAI Service** is Microsoft's cloud solution for deploying, customizing, and hosting generative AI models. It brings together the best of OpenAI's cutting edge models and APIs with the security and scalability of the Azure cloud platform.

Azure OpenAI Service supports many generative model choices that can serve different needs. You can use **Azure AI Studio** to create generative AI solutions, such as custom *copilot* chat-based assistants that use Azure OpenAI Service models



[Employer's Name]  
[Company Name]  
[Company Address]  
[City, State, Zip Code]

Dear [Employer's Name],

I am writing to express my interest in the software developer position at [Company Name], as advertised. With a strong background in computer science and extensive experience in software development, I am confident in my ability to contribute to your team and help [Company Name] achieve its goals.

I am a highly skilled software developer with a passion for creating innovative and user-friendly applications. My technical expertise includes proficiency in programming languages such as Java, C++, and Python, as well as experience with database management and web development. I am also well-versed in software engineering principles and best practices, and I

Write a cover letter for a resume to use in an application for a role as a software developer.

In this example, an Azure OpenAI Service model is used to power a copilot application that can be used to generate original content in response to user *prompts*, such as a request to write a cover letter.

Tip

Learn how a large manufacturing company uses Azure OpenAI to foster better communication and collaboration in this [case study](#)



# Challenges and risks with AI

Completed100 XP

- 3 minutes

Artificial Intelligence is a powerful tool that can be used to greatly benefit the world. However, like any tool, it must be used responsibly.

The following table shows some of the potential challenges and risks facing an AI application developer.

Expand table

Challenge or Risk	Example	
Bias can affect results	A loan-approval model discriminates by gender due to bias in the data with which it was trained	
Errors may cause harm	An autonomous vehicle experiences a system failure and causes a collision	
Data could be exposed	A medical diagnostic bot is trained using sensitive patient data, which is stored insecurely	
Solutions may not work for everyone	A home automation assistant provides no audio output for visually impaired users	
Users must trust a complex system	An AI-based financial tool makes investment recommendations - what are they based on?	
Who's liable for AI-driven decisions?	An innocent person is convicted of a crime based on evidence from facial recognition – who's responsible?	

---

## Understand Responsible AI

Completed100 XP

- 10 minutes

At Microsoft, AI software development is guided by a set of six principles, designed to ensure that AI applications provide amazing solutions to difficult problems without any unintended negative consequences.

## Fairness

AI systems should treat all people fairly. For example, suppose you create a machine learning model to support a loan approval application for a bank. The model should predict whether the loan should be approved or denied without bias. This bias could be based on gender, ethnicity, or other factors that result in an unfair advantage or disadvantage to specific groups of applicants.

Azure Machine Learning includes the capability to interpret models and quantify the extent to which each feature of the data influences the model's prediction. This capability helps data scientists and developers identify and mitigate bias in the model.

Another example is Microsoft's implementation of [\*Responsible AI with the Face service\*](#), which retires facial recognition capabilities that can be used to try to infer emotional states and identity attributes. These capabilities, if misused, can subject people to stereotyping, discrimination or unfair denial of services.

## Reliability and safety

AI systems should perform reliably and safely. For example, consider an AI-based software system for an autonomous vehicle; or a machine learning model that diagnoses patient symptoms and recommends prescriptions. Unreliability in these kinds of systems can result in substantial risk to human life.

AI-based software application development must be subjected to rigorous testing and deployment management processes to ensure that they work as expected before release.

## Privacy and security

AI systems should be secure and respect privacy. The machine learning models on which AI systems are based rely on large volumes of data, which may contain personal details that must be kept private. Even after the models are trained and the system is in production, privacy and security need to be considered. As the system uses new data to make predictions or take action, both the data and decisions made from the data may be subject to privacy or security concerns.

## Inclusiveness

AI systems should empower everyone and engage people. AI should bring benefits to all parts of society, regardless of physical ability, gender, sexual orientation, ethnicity, or other factors.

## Transparency

AI systems should be understandable. Users should be made fully aware of the purpose of the system, how it works, and what limitations may be expected.

## Accountability

People should be accountable for AI systems. Designers and developers of AI-based solutions should work within a framework of governance and organizational principles that ensure the solution meets ethical and legal standards that are clearly defined.

The principles of responsible AI can help you understand some of the challenges facing developers as they try to create ethical AI solutions.

## Further resources

For more resources to help you put the responsible AI principles into practice, see <https://www.microsoft.com/ai/responsible-ai-resources>.

To see these policies in action you can read about [Microsoft's framework for building AI systems responsibly](#).

---

## Summary

Completed 100 XP

- 1 minute

Artificial Intelligence enables the creation of powerful solutions to many kinds of problems. AI systems can exhibit human characteristics to analyze the world around them, make predictions or inferences, and act on them in ways that we could only imagine a short time ago.

With this power, comes responsibility. As developers of AI solutions, we must apply principles that ensure that everyone benefits from AI without disadvantaging any individual or section of society.

---

Keep up the great work!



Fundamental AI Concepts

You have earned an achievement!

Congratulations, but what should you do next?