Introduction to artificial intelligence

Previously, you explored different tools that cloud security analysts use throughout their careers. Tools help analysts perform their job more efficiently. Artificial intelligence (AI) and machine learning (ML) are modern technologies that analysts can use as additional tools to improve workflow and the security of systems.

In this reading, you'll learn about AI and ML, explore generative artificial intelligence (GenAI), and learn how security professionals use it.

Artificial intelligence

AI is the theory and development of computer systems that are able to perform tasks that normally require human intelligence. AI can be used as an assistive technology for a variety of tasks, like converting speech to text, or even translating languages. This aspect is especially useful in the cybersecurity field, where AI can independently monitor networks for suspicious activity, or detect threats.

AI is a broad field made up of several subfields, including:

- Machine learning (ML)
- Deep learning
- Large language models (LLMs)
- Generative artificial intelligence (GenAI)

Machine learning (ML)

ML is a subfield of AI that uses algorithms to train data to make useful predictions without explicit programming. An algorithm is a set of instructions that a computer follows to perform a task. Training data is the process of teaching an algorithm to create a model from existing content. A model is a program that can identify patterns and form predictions. ML uses artificial neural networks to classify data. A neural network is like a human brain; it connects and analyzes data using artificial neurons. The more information the algorithm is provided, the more accurate it becomes when making predictions.

ML uses different methods to train data, like supervised or unsupervised learning. Supervised learning uses labeled data that helps neural networks learn the basic concepts of a task. Labeled data contains tags that categorize the data as a name, type, or number. For example, to train a model to identify dogs, a person would provide it with pictures labeled as dogs. In contrast, unsupervised ML uses unlabeled data that doesn't have tags. Instead, unsupervised ML learns from the unlabeled data in order to categorize it. Unlabeled data helps neural

networks generalize to new examples. This means an unsupervised ML model can sort through pictures of dogs and cats, and correctly identify dogs.

Deep learning

Deep learning, a subset of ML, uses several layers of artificial neural networks, allowing the networks to process more complex problems than traditional ML. Because of the increased amount of artificial neural networks, the model can analyze a greater volume of data and form more accurate predictions.

Deep learning also uses semisupervised learning as a method to train models. Semisupervised learning trains models on a small amount of labeled data, and a large amount of unlabeled data.

Large Language Models (LLMs)

LLMs are a subset of deep learning that help solve language problems, like answering questions, summarizing documents, and classifying or generating text. LLMs contain an enormous amount of training data. They can be pretrained with a large amount of data or fine-tuned to specific domains. A pretrained model uses previously established data to complete a task. A fine-tuned model adapts to a new domain or set of custom use cases by training the LLM on new data. For example, as new threats emerge in cybersecurity, security analysts can fine-tune their data to identify new attack patterns.

LLMs are beneficial because practitioners don't need to be an expert or know how to train a model to use the technology. Instead, they just need a clearly defined prompt for the model to use to accomplish tasks. The LLM creates content that is mathematically predicted to be accurate based on its training. For example, security analysts can ask–or prompt–the LLM to list the top 10 cybersecurity threats to stay current with evolving trends.

Generative artificial intelligence (GenAI)

GenAI is another subset of deep learning that uses artificial neural networks to produce various types of content, like text, imagery, audio, and simulated data. It's a type of AI that creates new content based on what it has learned from existing content. It uses this trained data to create a model. When prompted, GenAI uses this model to predict a response, which generates new content.

Chatbots are a common example of GenAI. Imagine you're contacting customer service using the chat feature. Before you're connected to a representative, the chatbot asks questions to determine why you're contacting customer service. The chatbot uses its trained data to predict and respond to your request, and to connect you to the appropriate customer service department.

There are different types of GenAI models, including:

- **Text-to-text:** Produces text output from text input, for example, translating a language
- **Text-to-image:** Generates an image from a large pool of captioned images
- **Text-to-video or 3D:** Generates a video or 3D object using a description, sentence, or script
- **Text-to-task:** Performs an action based on text input, for example, updating a document
- **Foundation model:** Adapts to performing different tasks by using a vast amount of data that can be tuned for specific purposes, for example, tuning a model with legal or compliance data
- **Multimodal:** Converts one input type, like text, into a different output type, like an image

GenAI in security

An increasing number of organizations are adopting AI to improve business processes and customer relations. And, cloud security analysts increasingly use tools or processes that involve AI. For example, imagine an analyst has been tasked to create shell scripts to monitor their system's resources. They can use GenAI to generate examples of code that they can use and then modify to meet their system's specific configuration.

Pro tip: It's important to remember that while GenAI can produce helpful content, security analysts must still verify and modify the content to meet specific organizational requirements. A blend of security and AI knowledge is helpful for getting the best results from a GenAI toolset.

In another example, security analysts can use GenAI to analyze large volumes of data specific to vulnerabilities, attack patterns, and threats. For example, analysts can use GenAI to identify and then output patterns in network traffic during a security incident. As an added feature, GenAI can then interpret and summarize the data.

Key takeaways

AI and ML are important technologies in modern computing, with GenAI evolving as an important subset of deep learning. GenAI's ability to generate a multitude of content types makes it a useful solution for creating text and images, and even performing actions. LLMs' extensive data pools help inform the content that GenAI generates. As GenAI becomes more widely adopted in the workplace, security analysts engage with this technology to help improve efficiency of tasks and bolster system security.

Resources for more information

These resources provide additional information about GenAI:

- Learn more about GenAI by taking Google's free Cloud Skills Boost course: Introduction to Generative AI
- Discover different GenAI uses cases with Google