**Key takeaways from AI for cybersecurity**

In this lesson, you learned about AI and how it can help you as a cybersecurity professional. Then, you practiced prompting a generative AI tool to generate useful output.

Continue to experiment with generative AI tools to brainstorm ideas, boost your productivity, help you avoid mistakes, and aid in your decision-making process. Throughout the Google Cybersecurity Certificate and beyond, consider experimenting with Gemini to find out more about these topics and continue your AI learning journey.

**Key takeaways**

**AI in cybersecurity**

AI is rapidly changing the cybersecurity domain. As a cybersecurity professional, you can boost your career by understanding this powerful technology and how to leverage it in your daily work. While you continue to develop expertise in this profession, remember that:

* Understanding and using AI is important for your future success as a cybersecurity professional, as AI tools become more commonly used in the field.
* AI tools can help you perform tasks such as identifying risks, automating responses, and prioritizing threats.
* You may be involved in securing AI systems in your organization.

**Generative AI in cybersecurity**

Generative AI is a type of AI that’s capable of creating new content. You can leverage generative AI tools to complete practical and creative tasks. As a cybersecurity professional, you might use generative AI tools to:

* Create content, like lists of cybersecurity best practices for members of your organization to reference.
* Analyze and summarize large amounts of information, like security reports.
* Answer questions you have about common cybersecurity threats.
* Simplify daily tasks, like determining whether an email shows signs of phishing.

**Use AI responsibly**

AI tools have their share of limitations. To use AI responsibly, ensure that you:

* Review AI outputs carefully.
* Disclose your use of AI.
* Consider the privacy and security implications of using AI.
* Consider the effects of using AI.

**Resources for more information**

If you’re interested in learning more, please visit the following resources:

* [**All Things Generative AI**](https://generativeai.net/)**:** Delve into a more comprehensive introduction to generative AI, along with links to a few other popular generative AI tools.
* [**Global Trends 2040: A More Contested World**](https://www.dni.gov/index.php/gt2040-home/gt2040-structural-forces/technology)**:** Investigate how technological trends, including AI, are expected to transform the world over the next 20 years in this publication from the U.S. Office of the Director of National Intelligence.
* [**Introducing Google’s Secure AI Framework**](https://blog.google/technology/safety-security/introducing-googles-secure-ai-framework/)**:** Explore key elements of Google’s Secure AI Framework (SAIF) and how Google uses and supports SAIF.
* [**Science & Tech Spotlight: Generative AI**](https://www.gao.gov/products/gao-23-106782)**:** Discover why generative AI systems matter in today’s world in this article by the U.S. Government Accountability Office (GAO).
* [**There’s More to AI Bias Than Biased Data, NIST Report Highlights**](https://www.nist.gov/news-events/news/2022/03/theres-more-ai-bias-biased-data-nist-report-highlights#:~:text=Bias%20in%20AI%20systems%20is,systemic%2C%20institutional%20biases%20as%20well.)**:** Examine the risks involved when bias is present in AI data and recommendations for mitigating these risks, based on research performed by the National Institute of Standards and Technology (NIST), U.S. Department of Commerce.