In this lesson, you learned about AI and how it can help you as a cybersecurity professional. Then, you practiced prompting a generative AI (gen AI) tool to produce useful outputs. It’s helpful to use the TCREI (task, context, references, evaluate, and iterate) framework to guide your prompts. When you Thoughtfully Create Really Excellent Inputs, you’re more likely to get results that work for you!

Keep experimenting with generative AI tools to spark ideas, enhance your productivity, minimize errors, and support your decision-making. Practice with Gemini or other tools to explore these topics further and apply your Google Cybersecurity Certificate knowledge to your work—or use them outside of work to continue your AI learning journey.

**Key takeaways**

**The growing role of AI in cybersecurity**

AI is rapidly changing the cybersecurity domain. As a cybersecurity professional, you can help boost your career by understanding this powerful technology and how to use it effectively 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.

**How cybersecurity professionals can use generative AI to work smarter and faster**

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

* Create content, like lists of cybersecurity best practices that members of your organization can 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.

**Basic guidelines for responsible use of generative AI**

AI tools have their share of limitations. To use generative AI responsibly, make sure to:

* Review generative AI outputs carefully for accuracy and usefulness.
* Disclose your use of generative AI.
* Consider the privacy and security implications of using generative AI, and avoid entering sensitive information.
* Apply a human-in-the-loop approach, as AI should always serve as a complement to our human skills and abilities.

**Note:** This list is not exhaustive. Be sure to check your company’s policies on the use of generative AI.

**AI in action: real-world applications in cybersecurity**

In the videos, you learned how a real cybersecurity professional harnesses AI technology in their role at Google. Luis shared how gen AI tools like Gemini can:

* Help cybersecurity professionals understand, navigate, and adopt complex security frameworks.
* Scan code for common errors, vulnerabilities, and potential performance bottlenecks.
* Make suggestions to update and improve code written in Python or other programming languages.
* Describe common security vulnerabilities, their potential impact, and how to mitigate them.
* Assist security professionals with key detection and response tasks, such as investigating alerts.

Try these examples out yourself using Gemini or another generative AI tool, and keep experimenting to uncover new ways to apply AI to your role and responsibilities. With help from AI, you can spend less time on repetitive, routine tasks and devote more of your energy and attention to keeping people, organizations, and data safe—the work you’re uniquely qualified to do as a cybersecurity professional.

**Resources for more information**

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

* [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.