**AI tools for cybersecurity**

Because of the capabilities of AI, many cybersecurity professionals are using it as part of their daily work. **AI** refers to computer programs that can complete cognitive tasks typically associated with human intelligence. You can use AI tools to augment and automate general work tasks, such as drafting emails and documents, summarizing information, and helping to analyze data. You can also use it to help complete specific cybersecurity tasks. For example, you might leverage AI tools to:

* **Identify risks and prevent potential threats**:AI tools can analyze network traffic patterns and user behavior to identify unusual activity *before* a cyberattack occurs. This helps you identify threats more efficiently and effectively. AI might also help you identify and analyze system weaknesses so you can fix vulnerabilities before malicious actors exploit them.
* **Automate responses**:AI tools can help automate the actions you take to respond to cybersecurity threats, such as blocking malicious software or suspicious users. This can free up your time to focus on other important tasks, such as staying up to date with the latest news about cybersecurity threats and defenses.
* **Prioritize threats**: AI can assess the severity of security events and help you prioritize your response, allowing you to focus on the most critical threats to your organization. AI tools can also determine your systems’ baselines of safe activity to lower the number of false alarms that slow down security teams.
* **Improve authentication methods**: AI can evaluate factors like type of device, location of user, and usage patterns to confirm a user’s identity in near real-time. This can reduce the number of security alerts legitimate users receive, without sacrificing safety.

As AI systems become more commonly used in professional fields, it will also be part of your job as a cybersecurity professional to keep those systems secure. AI systems are complex and rely on large quantities of high-quality data to operate well. As a result, they can become targets for malicious actors, who often exploit vulnerabilities in new technologies to gain access to valuable information. These individuals may use AI to:

* Conduct more sophisticated or harmful attacks, such as drafting more realistic phishing emails.
* Make attacks more difficult to detect or fix.
* Steal private data.
* Manipulate AI tools.

As you learn about tools, techniques, and best practices for securing systems in your organization, keep in mind that AI tools can help you keep your organization’s systems safe, and that AI systems themselves need to be protected from cybersecurity threats.