Tanner Wale

## **AI in Cybersecurity: The Impact of AI on the Future of Cybersecurity Careers**

## **How Does AI Impact Cybersecurity in the Future?**

The impact of Artificial Intelligence (AI) in cybersecurity careers will be instrumental in successfully defending against attacks. AI will transform the industry by being able to resolve help desk tickets, and monitor networks. To aid people beginning their cybersecurity careers.

One of the ways AI provides support with network monitoring is automation. Automation is the process of not needing human interaction to complete a task or project. Organizations can depend on AI to complete their network analysis without needing manual intervention. Completing important tasks such as traffic pattern analysis, log analysis, protocol analysis, and many more. Without having to worry about human error that could later lead to an attack on the organization. Companies will trust AI much more than humans.

There is worry that AI will take away more jobs for future cybersecurity professionals. However, this is not the case, as AI is doing the easy part of cybersecurity. Humans can focus on much more complex projects to push forward innovation in the cybersecurity field. This innovation creates new jobs for AI to be used and managed correctly. Jobs created such as AI Security Analyst, Machine Learning Security Engineer, AI Security Architect, AI Forensics Expert, and Ethical AI Auditor (Vaishnavi, 2025).

Combining AI with humans for the benefit of defense to cybersecurity teams in organizations. Will make for better defense in areas that could be considerably weak to begin with. AI is not taking jobs from cybersecurity professionals. As AI continues to evolve it will need more testing and improvement from real-case scenarios. Humans drive this testing and improvement as AI with a bad database can be harmful. Instead AI is changing what the workforce may need out of candidates. Providing support for advanced threat detection, automation of security operations, behavioral analytics, real-time monitoring, data analysis, and simulations. Let's first look at how AI is shaping some of the current cybersecurity landscape. To later, understand the future of cybersecurity knowledge that will be useful for your cybersecurity careers.

## **Advanced Threat Detection**

AI will help humans in advanced threat detection by monitoring networks, systems, and user behavior twenty-four seven. A human cannot do these processes all day and all night without fatigue. Leading to missing important signs of an attack that AI wouldn’t miss due to lack of sleep. Trying to spot anomalies in this data. That accumulates rapidly faster than a human can get through one report. For humans to be consistent in this type of environment, human error would have to be removed. Finding potential threats through humans is not good for any security architecture.

Now adding another factor to this. Is to spot these attacks early, so that the attack will be stopped before it costs the organization. The costs accumulate from repairs, reputation (loss of customers), or in some cases fines for not adhering to data protection requirements. The organization can also move resources around if they know where their vulnerability is. To better defend against a malicious threat AI does this at a higher rate compared to humans. A human cannot get through all these monitoring activities without making countless errors. That would cost the organization later; it is just too much information for a human to efficiently detect potential threats.

AI uses a large amount of data for the monitoring activities of the networks, systems, and user behavior to give reports to humans. This is done through automation by creating baselines (acceptable behavior of the network, systems, and users). Humans can find these anomalies through reports from AI automation. AI is looking through all of its large data sets to spot signs of anomalies. These data sets of AI, are compared to the baseline, created by humans.

This makes the employees in the cybersecurity field more productive. By not having to manually look for anomalies in large datasets, or taking part in repetitive tasks. As this is a less efficient use of employee’s time. Also, as we have established, humans cannot thoroughly look for signs of a possible attack in large data sets of network activity. Without committing a human error in the thousands of network logs and scanning reports that must be vetted. These are the building blocks of a secure and safe network.

A next-generation firewall can use AI to make security more robust. It does this though using real-time monitoring, threat detection, and automation of incident response. AI is able to use customer data to gain insight whether there is a possible threat. Attacks on AI models can happen. This is because AI uses data to learn how to detect and find signs of potential threats. This data can be altered by malicious users. To skew the data for finding and detecting threats. Attackers can go undetected and exploit vulnerabilities of an organization’s network without being detected.



Photo by Tara Winstead: <https://www.pexels.com/photo/robot-pointing-on-a-wall-8386440/>

ALT Text: Robot pointing on a wall

## **Log Analysis Automation**

Log analysis and vulnerability scanning being automated using AI provides a better outcome for security processes. Log analysis is crucial to security for watching out for potential threats. As we mentioned earlier, the large amounts of data employees must go through to protect their organization from malicious threats.

Log analysis requires humans to find patterns, outliers, and suspicious activity in these large data sets. Potential patterns AI can find, to gain insight into how an attacker might have gained unauthorized access. AI provides root cause analysis from multiple log files. Showing the history of the same issues, to troubleshoot ways to protect from threats better.

AI creates a risk matrix that sorts the priority of threats in alerts such as low, medium, high, or critical alert. This helps employees of an organization sort out better alerts to respond and give focus to first. Organizations would love to maintain their network with one hundred percent uptime to make the most profit they can. In theory this is possible, by making updates to servers, and turning on other servers to handle network traffic. This is not possible, due to not only updates of their systems to protect against threats. Also, attacks that leave an organization with no other choice but to turn off their systems (critical alert).

Also, another factor in the downtime of an organization could be a system failure to the servers. AI can help by providing real-time monitoring of user behavior, network activity, and systems reports. To spot threats that could affect the organization's uptime. Another AI benefit is predictive analysis. Generative AI is used to predict if systems could have failure, far before it does by monitoring systems closely.

Analysis of this data Generative AI collects. Will lead to less downtime and faster fixes of important systems, giving organizations more uptime. These insights provided by AI help keep the organization’s cybersecurity team up to date. With the latest risk matrix of critical alerts. So they can be solved in time to keep customers’ access to the organization safe and secure. Providing more revenue to the organization by having longer uptime.

## **Vulnerability Scanning Automation**

AI is better than humans at vulnerability scanning with large amounts of data. This is due to the speed of AI scanning through large amounts of data with no human errors. AI is more accurate than humans in vulnerability scanning, meaning less false positives. AI can scan faster and find vulnerabilities more efficiently than humans. Leaving less time for malicious attackers to execute a successful attack on an organization. AI has a risk matrix that sets alerts and scans for the highest risks to the organization's network. The organization, through using AI to scan for these vulnerabilities. Can get reports back in real-time from large data sets. Allowing a cybersecurity team to focus on higher profile risks that pose a greater threat to the organization’s architecture.

Cybersecurity teams can handle important risks because AI can scan for vulnerabilities using automation. The critical risks can be handed out to cybersecurity teams to collaborate on how to mitigate the critical risks. Through using better security policies, procedures, or security design principles.

AI automation for vulnerability scanning is more beneficial to the organization’s cost of fixing security issues. AI can spot these vulnerabilities and make predictions faster than humans. Predictions such as when an attack might occur. Which saves money for the organization, by mitigating more of the attack than previously possible. Securing the vulnerabilities and making them harder for attackers to exploit.

Another area in which AI shines is false positives. AI has fewer false positives than humans, due to human error. A false positive occurs in vulnerability scanning with AI models. When AI thinks it has identified a threat, but in reality, it has not. The issue with too many false positives is that each one must be looked at, for the possibility of a real threat. This takes time away from real threats to the organization. Contributing to more burnout and a greater risk of human error among employees working with real threats.



Photo by Ron Lach : <https://www.pexels.com/photo/person-facing-a-big-screen-with-numbers-9783346/>

ALT Text: Person facing big screen with numbers floating

## **Continuous Improvements from AI**

AI will continue to adapt to find new emerging threats. Also, signs of possible attacks using vulnerability scanning and log analysis. Along with making simulations for employees to go through response procedures to these new emerging threats. AI can create a sandbox environment so that the response procedure can be practiced in a safe environment. The fastest response time can be reached by trainees and they will be ready for a real attack. All employees will know what to do when this new threat is used on the organization.

Employees will learn what is detrimental in these simulations. Such as who to contact, how to write the report, and what to include in the report. This is important as information needs to be moved along to different departments. To collect critical information and only the information that is important. If employees are putting nonrelevant information in these reports, it can take longer to mitigate the threat. When moving the information along with the correct information, the threat can be handled effectively.

After employees get used to this, the response procedure will have fewer accidents. Less chance of derailing the response procedure. Which is all thanks to the AI’s simulations.

## **Technical Skills for Future Cybersecurity Professionals**

## **Adversary Mindset**

The focus of what to learn as we lean into the future of AI’s help in cybersecurity. Is understanding AI usefulness and its capabilities. This is because AI is being used in security environments to help with detection and response to cyber attacks. Attackers will try to find ways to exploit AI to their advantage.

Understanding how AI is tested, built, used, and areas of the network they are deployed, are ways for an attacker to exploit AI. A future job as an AI Security Analyst will be validating AI’s detection and response measures. To ensure no false positives of potential attacks are found by AI. This leaves the real attacks undetected, leading to revenue loss to the organization. This type of attack is known as data poisoning. Which is an attack on AI models data sets using false data entered by the attacker. That leads to false positives of log analysis and vulnerability scanning. As attackers gain access to data, they can input into AI’s detection for potential attacks. Malicious attackers can have AI detect legitimate traffic as an attack. While also allowing AI to detect malicious traffic as legitimate traffic. This lets the attack pass through to the organization’s network without being detected. To successfully launch an attack. These hidden vulnerabilities the attacker uses to exploit AI. Such as gaining access to the data, AI uses to analyze large data sets. Will be detrimental to the protection of AI.

To understand how paramount the security of these AI data set models are to the public. Let's look at a case study that occurred earlier this year in January 2025.

When Natural Medicine researchers showcased how much a data poisoning attack. Will have to affect a large data set, in order for the attack to be successful (Traynor, 2025). The case study tested a model trained to find lung diseases in patients. According to (Traynor, 2025), the result of this study found just an attack on 0.001% of the large dataset. Will show false positives or not detect lung disease in patients who have it. The AI’s data set model was affected by approximately 0.001% (Traynor, 2025). mThis was enough to make the model untrustworthy in diagnosing patients with lung disease.

As you can see from the case study, there is a very thin line of error when it comes to protecting these large datasets. Data poisoning attacks according to (Traynor, 2025) are very hard to detect due to certain security baselines of data poisoning. Being able to detect 0.001% (Traynor, 2025) of data poisoning in a large data set is very difficult. This is why before using AI models, they should always be tested. This leads to our next section, Testing, and Deployment of AI Models.



Photo by Pavel Danilyuk: <https://www.pexels.com/photo/robot-picking-a-chess-piece-8438945/>

ALT Text: Robot picking a chess piece on a chessboard

## **Testing and Deployment of AI Models**

Employees should know how to test and deploy AI models for certain security conditions. Such as what scenarios to use AI endpoint security models and AI incident response models to be most effective. Asking questions such as what AI models can find root cause analysis faster and more efficiently. Also, what models can detect and respond to zero-day attacks best. The AI security Analyst will have their hands full.

Launching an AI model that has not been tested for detecting threats in log analysis could be catastrophic. If the AI model is unable to detect these threats due to being under attack previously from data poisoning. This will cause even easily detected attacks to go through and launch successfully. Resulting in massive revenue loss, potential fines, loss of customers and customer's trust in the organization’s security.

By being able to test AI models before being used by the public. You can spot false positives or inconsistencies in data. AI models must be able to operate without clear vulnerabilities that attackers can take advantage of. AI must be tested for data bias by the organization before being deployed. To get back useful unbiased conclusions from data that the AI model can use to predict attacks.

Biased conclusions from data can open the company up to more revenue loss. As customers will lose trust in the organization, by poorly structured analysis. Examples of biased conclusions are overlooking threats, insider threat detection, and incorrectly classifying networking protocols. Furthermore, issues with biased conclusions can also lead to legal fines. The organization will have to pay for not doing their due diligence before the deployment of an AI model. Therefore, legal requirements of proper testing, deployment procedures, and policies must be in place for the organization to protect itself from legal fines.

## **AI Data Science**

Learning data science to use AI more effectively can help your organization protect against threats. Learning how to build AI models to detect and protect incident response procedures against malware, viruses, or vulnerabilities. In real time without needing human intervention to solve the problem. This can be done using AI automation. Large datasets of information to identify potential threats and respond to threats; are trained by these large data sets. This is done through recognizing patterns within these large data sets of information. As using this data is helpful, the data also has to be cleaned, so that the AI model can be trusted to function properly.

Data cleaning is checking for attacks on data input from users. This is another area where automation can be used. To analyze large data sets to complete tasks that would take too long for humans. Also, having human error involved in these areas is dangerous and can lead to attacks on AI models. Analysis of large data sets using AI is a huge plus for an organization. As humans would struggle to connect the present trends, patterns, and anomalies from the past. To learn the most efficient ways to defend against a certain attack. Automation can be done using a variety of ways, like scripting.

This creates a more efficient cybersecurity team for your organization. By focusing on more important tasks. Such as improvements to be made to respond faster to sophisticated attacks like zero-day attacks (critical risk). Learning data science to build AI models for future attacks will always be beneficial for solving the newest attacks on an organization.



Photo by Pavel Danilyuk: <https://www.pexels.com/photo/scientists-testing-a-device-8438994/>

ALT Text: Scientists testing a device with AI capabilities

## **Automation**

Although we talked about scripting AI for automation. It is important to know all possible ways to do this task, so you can find one that fits you. There are other scripting options available now. Such as Visual Workflow Builders, Natural Language Processing (NLP), Robotic Process Automation, and Automated Connectors. Visual workflow builders allow users to not need to know any programming skills. Instead users use drag-and-drop pre-programmed or visual workflows to automate AI for what is needed. Natural Processing Language (NLP) is unique, in the fact that it can take a set of instructions typed by the user. To make automation tasks to complete for the user. The user does not need to know any scripting languages for this. The user just simply types in what they need (a set of instructions), and NLP will create the automation from the user's instructions. Robotic Process Automation (RPA) uses visual user interfaces and automation from workflows to create the automation of tasks. Automated Connectors use AI models instead of scripting, to automate processes and data flows. This is done by connecting through apps with pre-built templates so that users can customize to fit their needs. Examples of Automated Connectors are Zapier and Make.

If you are not comfortable with scripting, these are great options as moving forward with AI at the helm. These tools will become more and more common. Making yourself familiar with these tools to use for automation is another advantage you can have. Traditional scripting is still useful to learn but could fade out as time goes on due to human error in scripting. These tools offer pre-built services and visual interfaces users can interact with or give a set of instructions to. Which can be automated to complete those sets of instructions, limiting human error.



Photo by Hyundai Motor Group : <https://www.pexels.com/photo/boston-dynamics-robot-in-a-car-factory-19319639/>

ALT Text: Boston dynamics robot in a car factory

## **AI Outlook**

AI is now being utilized in technology, medical fields, finance, education, and other fields more and more. This is because of the tremendous upside of AI. Which enhances an organization's effectiveness in completing tasks. Employers in the future of cybersecurity will look for candidates who have related expertise with AI. To use that to their advantage for the organization.

Employers will look for work experience but also AI-related certifications. Such as Azure AI Engineer Associate, Microsoft AI Fundamentals, and AWS Certified AI Practitioner. These are just some relevant certifications to AI. More will become available in the near future. As more of a demand for skills in AI continues to grow.

As of this writing, cybersecurity needs employees who understand the traditional scripting language for automation. As for now, this is still widely used. Employees who can understand the automation processing, testing, and deploying. As well as adversary mindset, and use cases of AI models. Also, identifying common attack vectors, malicious attackers will try to exploit AI through.

Cybersecurity will continue to increase the usage of AI because the pros outweigh the cons. Data breaches are less frequent due to AI being able to analyze all traffic in real time to find potential threats. This allows cybersecurity professionals to work on critical issues and find innovative solutions for critical risks. There are still areas of concern when it comes to AI. As mentioned earlier, 0.001% (Traynor, 2025) of a large data set AI model was affected by a data poisoning attack. Will create more false positives and make the AI model ineffective. Future cybersecurity professionals will need to solve this so that diseases can be caught and treated.

There will need to be better ways to detect these attacks on AI models by extensive testing policies and procedures before deployment. More will be done with AI models to get better detection of data poisoning to aid in fewer false positives. Unbiased data sets for AI models, to use to find attacks will also need more security to avoid a catastrophe.

The future of AI in cybersecurity careers is just beginning to grow and we are seeing greater security results compared to before. Fewer data breaches are happening compared to before AI was in use. Better vulnerability scanning, improved log analysis, automation of repetitive tasks, and more AI helps with. It will be exciting to see where AI takes us next to improve cybersecurity.



Photo by Pavel Danilyuk: <https://www.pexels.com/photo/a-robot-holding-a-wine-8439094/>

ALT Text: Robot holding a wine glass filled with wine

## **References**

1. Traynor, O. (2025, April 24). *Data & Model Poisoning [Exploring Threats to AI Systems]*. CybelAngel.<https://cybelangel.com/data-model-poisoning/>
2. Vaishnavi. (2025, March). *AI and the Future of Cybersecurity Jobs | How Automation is Reshaping the Industry*. WebAsha Technologies.<https://www.webasha.com/blog/ai-and-the-future-of-cybersecurity-jobs-how-automation-is-reshaping-the-industry>
3. <https://www.sentinelone.com/cybersecurity-101/cybersecurity/ai-vulnerability-management/>
4. <https://www.advantage.tech/role-ai-next-gen-vulnerability-scanning/>
5. <https://www.paloaltonetworks.com/cyberpedia/ai-risks-and-benefits-in-cybersecurity>
6. <https://binaryit.com.au/top-10-benefits-of-ai-in-cybersecurity/>
7. <https://www.legitsecurity.com/blog/role-of-ai-in-cybersecurity>
8. <https://www.cyberdefensemagazine.com/transforming-security-testing-with-ai-benefits-and-challenges/>
9. <https://www.techtarget.com/searchsecurity/tip/How-AI-will-transform-vulnerability-management-for-the-better>
10. <https://testgrid.io/blog/scriptless-test-automation/>
11. <https://kobiton.com/blog/scriptless-test-automation-tools-for-mobile-application-testing/>
12. <https://www.leapwork.com/blog/what-is-scriptless-test-automation>
13. <https://www.reddit.com/r/DigitalMarketing/comments/1e9q9y0/what_ai_and_automation_tools_can_you_not_live/>
14. <https://zapier.com/blog/best-ai-productivity-tools/>
15. <https://smartbear.com/blog/no-code-no-problem-ai-powered-automation-for-manual-testers/>
16. <https://moz.com/blog/ai-tools-for-automation-productivity>
17. <https://www.secureworld.io/industry-news/ai-future-of-work-cybersecurity-beyond>
18. <https://securing.ai/ai-security/adversarial-attacks-ai/>
19. <https://www.excelsior.edu/article/ai-in-cybersecurity/>
20. <https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity>
21. <https://logz.io/blog/ai-log-analysis/>