

Brandon Rollinson Jr

7/27/2026

CyberQRT

Reflection 3

During this stage of my CyberQRT internship, my primary responsibility was researching topics related to artificial intelligence and machine learning and understanding how these technologies are being used in cybersecurity. I spent time reading peer reviewed research papers, technical articles, and industry resources that explained different AI models, machine learning techniques, and their real world applications. My goal was to build a stronger foundation in AI while learning how these technologies can improve security operations, automate tasks, and help organizations defend against cyber threats.

Throughout the week, I focused on understanding the different types of machine learning, including supervised, unsupervised, and reinforcement learning. I learned how each type of learning is used depending on the problem being solved and how models are trained using large amounts of data. I also studied neural networks, deep learning, feature engineering, and the importance of selecting quality datasets when developing machine learning models. These concepts helped me understand what happens behind the scenes when an AI system is trained to recognize patterns or make predictions.

A large part of my research focused on how AI and machine learning are applied within cybersecurity. I learned how organizations use machine learning models to detect malicious network traffic, identify phishing emails, classify malware, detect insider threats, and recognize abnormal user behavior. Many of the papers I reviewed explained how AI can analyze thousands of events much faster than a human analyst, making it easier for security teams to identify potential threats before they become

major incidents. Learning about these real world applications helped me connect my cybersecurity coursework to technologies that are currently being used across the industry.

As I worked through each research paper, I took detailed notes and summarized the main ideas in a way that made them easier to understand. Instead of simply reading the material, I focused on understanding the researchers objectives, the methods they used, the datasets they trained their models on, and the results they achieved. I compared different approaches and looked at why certain models performed better than others. This process improved my ability to analyze technical documentation and think critically about how research can be applied to practical cybersecurity problems.

One of the biggest things I learned was that building an effective AI model involves much more than choosing an algorithm. The quality of the data, the preprocessing steps, feature selection, training process, and evaluation methods all have a major impact on how well a model performs. I also learned about common evaluation metrics such as accuracy, precision, recall, and F1 score. Understanding these metrics helped me see how researchers determine whether a model is reliable enough to be used in real world environments where accuracy is critical.

This experience also strengthened my research and analytical skills. Some of the papers included technical language and complex concepts that required me to slow down, reread sections, and conduct additional research to fully understand them. Although challenging at times, this process improved my ability to interpret technical information and break down complex topics into concepts that were easier to understand. As I continued reading more papers, I became more comfortable recognizing common machine learning terminology and understanding how different AI models are designed and evaluated.

Beyond the technical knowledge, this experience taught me the importance of continuous learning in cybersecurity. Artificial intelligence and machine learning continue to evolve, and new research is constantly being published. Staying current with emerging technologies is an important part of becoming a successful cybersecurity professional because attackers are also beginning to use AI to develop more

advanced attacks. Learning how defenders can use the same technology to improve threat detection and incident response showed me how important AI will continue to be in the future of cybersecurity.

Next week, I will begin creating a project based on everything I have researched during this phase of my internship. Instead of only studying existing research, I will apply the concepts I have learned by designing and developing a project that demonstrates the use of AI and machine learning to solve a cybersecurity related problem. This will require me to think through the entire development process, including selecting an appropriate dataset, preparing the data, choosing a machine learning model, evaluating its performance, and making improvements based on the results. I am excited to transition from research into development because it will allow me to gain practical experience while reinforcing everything I have learned.

Overall, this stage of my internship has been extremely valuable for my professional growth. It has strengthened my understanding of artificial intelligence, machine learning, cybersecurity research, and technical problem solving while improving my ability to read and analyze technical literature. It has also shown me how research plays an important role in developing innovative cybersecurity solutions. As I continue my internship, I look forward to building my project, expanding my technical skills, and gaining a deeper understanding of how AI and machine learning can be applied to solve real world cybersecurity challenges. This experience is helping prepare me for a future career in cybersecurity by giving me exposure to emerging technologies and teaching me how research can be transformed into practical solutions.