

## **CYSE 368: Final Paper**

Bailey Williams

Usable Machines, Inc. (dba Kindo)

CYSE 368: Cybersecurity Internship

December 1, 2024; Fall 2024 Term

## Table of Contents

<b>Introduction.....</b>	<b>3</b>
<b>Beginning of Internship.....</b>	<b>4</b>
Overview of Kindo.....	4
Description of Kindo at the start of my internship.....	4
Description of Kindo at the end of my internship.....	4
Overview of Kindo Products.....	5
Initial Orientation & Training.....	6
<b>Management Environment.....</b>	<b>7</b>
<b>Internship Duties.....</b>	<b>8</b>
Creating Tutorial Videos.....	8
Discord Management.....	8
Writing Content.....	9
Cybersecurity Conferences.....	11
<b>Usage of Cybersecurity Skills and Knowledge.....</b>	<b>13</b>
<b>Connections between the ODU Curriculum and the Internship.....</b>	<b>13</b>
<b>Fulfillment of Learning Objectives.....</b>	<b>14</b>
<b>Motivating &amp; Exciting Aspects.....</b>	<b>15</b>
<b>Discouraging Aspects.....</b>	<b>16</b>
<b>Challenging Aspects.....</b>	<b>16</b>
<b>Recommendations for Future Interns.....</b>	<b>17</b>
<b>Conclusion.....</b>	<b>17</b>
<b>References.....</b>	<b>19</b>
<b>Appendix.....</b>	<b>20</b>
Figure 1.....	20
Figure 2.....	20
Figure 3.....	21
Figure 4.....	21
Figure 5.....	22
Figure 6.....	23

## Introduction

My relationship with Kindo began in the summer of 2023 when I interned as a Customer Support Representative. This was towards the beginning of the company's existence, and much of my work entailed helping early users get the most out of the product and creating FAQ documentation. Due to my performance that summer, I was asked to return in May 2024, this time as a Cybersecurity Intern. I chose to return to Kindo as a Cybersecurity Intern because I enjoyed the work environment and felt there was no better way to stay on top of Artificial Intelligence (AI) trends and how they impact cybersecurity than to work for an AI platform tailored for DevSecOps.

While my official Cybersecurity Intern role began in May 2024, my original contract ended at the beginning of August. Due to my performance over the summer, my manager offered me the opportunity to remain at Kindo on a part-time basis (approximately 10 hours per week) this semester. My new contract, and the focus of this reflection, began on August 26, 2024.

At the beginning of the semester, I set four learning objectives:

1. Develop educational content on using AI in cybersecurity tasks.
2. Gain confidence to give talks on AI in cybersecurity at cybersecurity conferences.
3. Research open-source AI tool-use projects focusing on cybersecurity.
4. Integrate WhiteRabbitNeo, a red-team open-source AI model, into these AI tool-use programs.

These learning objectives were chosen based on the description of my internship responsibilities presented by my manager when I was asked to work part-time during the semester.

## **Beginning of Internship**

### **Overview of Kindo**

At the start of the semester, Kindo marketed itself as a secure AI management platform, designed to help all employees in enterprises to integrate AI into their workflows. Right before Thanksgiving, Kindo rebranded itself to focus on marketing AI to help automate DevSecOps workflows.

### ***Description of Kindo at the start of my internship***

Kindo is a secure AI management platform designed to provide enterprises with a way to adapt and manage AI usage safely across the company. Kindo supports any AI model and grants enterprise users data controls that allow them to maintain compliance with GDPR, HIPAA, and other industry compliance standards (*Kindo Features*, n.d.). The startup was founded in 2022 and is headquartered in Venice Beach, California (*Kindo AI About*, n.d.). Recently, Kindo raised over \$20 million to close out its Series A round (Takahashi, 2024).

Kindo's target customer demographic is mid-range enterprises looking to integrate AI into their employee's workflow. Kindo allows these entrepreneurs to ensure their employees are using AI safely and securely, rather than employees having unrestricted access to AI or banning AI completely in the organization.

### ***Description of Kindo at the end of my internship***

After the acquisition of WhiteRabbitNeo, described in the next section, Kindo began slowly shifting its focus toward DevSecOps. DevSecOps, or Development, Security, and Operations, means that security is a concern at every step of the software engineering process, with the end goal of reducing code vulnerabilities (*What Is Devsecops?*, n.d.). Right before the company took off for Thanksgiving, Kindo rolled out

a rebranded website, changing its marketing to target enterprises looking to add generative AI to its DevSecOps practices.

While products and services offered by Kindo remained the same following the rebrand, the sales strategy has shifted from targeting enterprises looking to integrate AI into all of their processes to those looking to integrate AI specifically into DevSecOps uses.

### ***Overview of Kindo Products***

The two major products at Kindo are its Agents and Secure Coding plugin. The Agents are on the Kindo product site, [app.kindo.ai](https://app.kindo.ai), while the plugin is offered through Continue on Visual Studio Code and JetBrains IDE. Agents allow users to automate tasks using any AI model. Kindo is a provider for the Continue extension on Visual Studio and JetBrains. The plugin allows users to customize which models they use in their Integrated Development Environment (IDE), picking from the models offered by Kindo or adding their own. All requests made in the Kindo provision are sent through the same servers as requests made on the product site, meaning they have the same level of privacy controls. Both Agents and the plugin are protected by Kindo's privacy filters, which enterprises can customize to filter out sensitive information before the AI receives it.

While most of the AI models supported by Kindo are from other companies, Kindo acquired WhiteRabbitNeo in May 2024. WhiteRabbitNeo is an open-source, uncensored, AI model. It has a software engineering foundational model trained on red-team-specific and general cybersecurity data. The advantage of an uncensored model, particularly in offensive cybersecurity, is that you do not have to trick it into helping you like you have to with other models to avoid ethical constraints. New

WhiteRabbitNeo models are released roughly every quarter, and the foundational model changes depending on what model is currently scoring the highest on code evaluations. This coding expertise combined with cybersecurity knowledge makes WhiteRabbitNeo very effective at analyzing code to identify vulnerabilities and suggest ways to make it more secure. Other applications of WhiteRabbitNeo include log analysis, teaching cybersecurity concepts, and creating custom hacking tools.

### **Initial Orientation & Training**

As a remote employee at a primarily in-person company, my orientation looked a little different than most. It involved ensuring I had access to the work Slack and my email account, as well as getting set up with payroll. I had to choose my health insurance and other policy opt-ins from my work benefits and set up my 401(k) plan. I was then given a checklist of accounts to ensure I had access to so that I could complete my work tasks. Kindo sent me a MacBook so that I could run some of the more resource-intensive AI tasks, so I had to set it up and configure the security controls per company policy. I also had an introductory meeting with my supervisor and informal meetings with many coworkers over Slack. After I was onboarded, I familiarized myself with the Kindo platform, learning how to work with the coding plugin and build my own Agents.

Overall, I was very impressed by how welcoming everyone at Kindo is, and how willing they were to help with any questions I had. Although most of the staff is based on the West Coast, they are good at getting back to me promptly. The difference in time zones also grants me more flexibility with my working times, which I enjoy. My supervisor especially was focused on assigning me tasks that allow me to get what I want out of the internship, and build upon my strengths. Although the first week was very slow as I was focused on onboarding tasks and ensuring everything was set up properly,

I am excited to get started on my internship and know that I will be able to get a lot out of it.

### **Management Environment**

The management environment at Kindo is similar to how I imagine many West Coast tech startups are. In general, the management structure is fairly relaxed, with the majority of employees reporting directly to the Vice President (VP) of the department they work for. The only exception I am aware of is that the engineering department has its own structure with different levels of engineers and supervisor positions.

In my experience at Kindo, supervision entailed weekly meetings with my manager, where we discussed where I am on my current projects and she assigned me more projects as I finished ones. My supervisor is also the primary editor of my content, so as I finish rough drafts of blog posts I send them to her for review. In addition to weekly meetings, the marketing team, where my role resides, has experimented with different project management systems, including Notion, Workday, and Asana, which we currently use to keep track of our projects and event planning.

I feel that this style of supervision is very effective for my internship. Since I only work an average of 10 hours per week and complete my work whenever I find time during the week, it can be difficult to connect with my coworkers, especially since many of them are in different time zones. By having weekly meetings with my manager, I can stay connected with my team and ensure that I am up to date with the various projects going on at work. These meetings also make it easy to communicate with my manager when I need to reduce my workload to focus on schoolwork, which my manager is very supportive of.

## **Internship Duties**

I have had many internship duties throughout the semester, including managing a Discord server, writing content, and applying to speak at cybersecurity conferences.

### **Creating Tutorial Videos**

One of my first projects this semester was to create tutorial videos on how to use different aspects of the Kindo product site and secure coding plugin with an emphasis on WhiteRabbitNeo and cybersecurity-related examples. These videos included how to use the chat by itself or with one or more files, different ways to create automated Agents with varying degrees of complexity, downloading and configuring the secure coding plugin, and how to optimize WhiteRabbitNeo using the plugin (see Appendix, Figure 1).

The creation of these tutorial videos is necessary to Kindo because these videos show users how to get the most out of the Kindo products. The secure coding plugin videos in particular are important because it provides a visual representation of the written configuration instructions, which may be easier for some customers to follow. These videos also serve as a repository for the Customer Support team to direct customers to as needed.

### **Discord Management**

Throughout the semester, my ongoing project at Kindo was managing our Discord server for the WhiteRabbitNeo community. Unlike our product customer support channel, the server is geared towards people running WhiteRabbitNeo locally on their systems. I am responsible for interacting with members and helping to answer any questions they may have about using WhiteRabbitNeo (see Appendix, Figure 2). Oftentimes I have to reach out to coworkers on Slack to answer more technical



questions members may have. I also record the metrics for the server every week, noting how many people join the server, how many messages are sent, and if any notable events may have encouraged more interaction, among other things.

The server had minimal interaction rates when I began to actively manage it, so one of my main goals was to encourage more interaction, especially from new members. To accomplish this, I spearheaded a project where I found an outside contractor experienced with Discord to create a bot that automatically messages new members to ask if they would like help getting started (see Appendix, Figure 3). This bot has increased the number of people asking questions on the server. In addition to the bot, the contractor organized the channels and roles to be more easily navigable and created a new channel that automatically responds to FAQs with pre-programmed responses. One of my responsibilities is ensuring that the bot and FAQ channel are functioning properly and remain up to date.

My management of the WhiteRabbitNeo Discord server is necessary to Kindo because it helps to maintain our brand image in the open-source community. It also gives Kindo a way to better understand what the needs of the community are, so that future WhiteRabbitNeo models and educational content can be tailored to address those needs.

## **Writing Content**

Creating educational content about WhiteRabbitNeo has been the primary focus of my internship for the past four months. So far, my content has been primarily driven by questions from Discord community members. Many members have asked for help locally hosting WhiteRabbitNeo in Ollama and on other platforms, which inspired a

three-part series detailing how to locally host WhiteRabbitNeo and the hardware requirements to locally host different-sized models.

While none of these posts have been officially published yet, the drafts have been shared on the WhiteRabbitNeo server many times. Part of my responsibility is completing technical reviews of blog posts to ensure the instructions are accurate and comprehensive. During a technical review of the post detailing how to locally host in Ollama, I realized that the newest Python update causes errors in the commands, which made me spend a few hours researching the commands and finding a workaround until the newest Python version is supported in the programs used to locally host (see Appendix, Figure 4).

While researching different local host systems mentioned by the community, I realized that some are better suited for use with WhiteRabbitNeo than others, which has made me more informed when new members ask for help.

In addition to the local host blog series, I have interviewed different Kindo employees to get information for future blog posts. So far, I have interviewed the Chief Security Officer about how he uses WhiteRabbitNeo in his own life and the Chief Technology Officer about how RAG works as a search option in AI and how to use RAG within Kindo products. Due to my minimal work hours, I have not been able to complete these posts yet, but they will be part of my workload in the future. I am also about to start a content series covering how to use WhiteRabbitNeo on the Nvidia Orin, starting with a piece on how to configure WhiteRabbitNeo to run on the Orin. Finally, I was also asked to write a press release announcing Kindo becoming SOC 2 Type II compliant, which will be published soon. As the posts related to my interviews and the press release

have not been distributed or published yet, I am unable to attach any appendices that display these items.

My favorite part of writing content is that it introduces me to topics that I otherwise would know nothing about. The local hosting series in particular has taught me a lot about how AI models are run locally and has given me more command-line experience. I have also gained hands-on experience in how different local host systems work throughout this process. By interviewing senior employees at Kindo, I have not only learned more about the topic of the interviews but have also gained experience in conducting interviews and leading meetings with people higher up.

My creation of educational content is necessary to Kindo because it generates more exposure to the Kindo products online and enhances the user experience of its customers. In some cases, content creation has also exposed limitations of the WhiteRabbitNeo model, such as which local hosting formats are best suited for it, which helps guide future customer interactions.

### **Cybersecurity Conferences**

The last of my major work duties is related to different cybersecurity conferences. One of my recurring assignments at work is to find different cybersecurity conferences I can attend and submit Call for Papers (CFP), which are applications to speak at the conference. This involves researching different conferences that I felt confident presenting at and creating different CFPs that are tailored to each conference's themes.

Thus far, I have applied to speak at Portland BSides, London BSides, Dresden BSides, and ShmooCon. BSides conferences are tailored for the local information security community. I was rejected from BSides Portland and did not hear back from Dresden BSides, but was accepted to speak at the London BSides conference, which will

be on December 14, 2024. My talk at London BSides is on the rookie track, which is for first-time speakers, 15 minutes long, and will give a general overview of WhiteRabbitNeo along with a few use cases (see Appendix, Figure 5). I recently submitted my CFP for ShmooCon, a cybersecurity conference in Washington D.C., which if accepted will detail how I used WhiteRabbitNeo as a digital red team cybersecurity mentor.

Outside of applying to speak at cybersecurity conferences, I also worked the sponsor booth for WhiteRabbitNeo at Chicago BSides at the beginning of November. This involved setting up our booth and demonstrating different use cases for WhiteRabbitNeo to attendees (see Appendix, Figure 6).

I have been greatly enjoying applying for and attending different cybersecurity conferences. Not only does this allow me to experience the information security community in various locations, but it also gives me experience talking to different people from a sales perspective, which will be beneficial no matter what role I end up in. I also enjoy traveling and attending these conferences allows me to explore different cities when not working.

Applying and attending cybersecurity conferences as a WhiteRabbitNeo representative is necessary for Kindo because it exposes local communities to WhiteRabbitNeo and Kindo products. The Kindo sales team primarily attends Chief Information Security Officer (CISO)-oriented conferences, so attending community-focused ones generates more overall awareness without overwhelming the sales team.

### **Usage of Cybersecurity Skills and Knowledge**

Before starting my internship, I was already knowledgeable in basic Linux/command line programming and possessed much “book knowledge” of different cybersecurity concepts, but lacked hands-on experience. Over the course of the semester, I gained real-world experience using the Command Line and learned more about its capabilities, particularly related to running AI models. On the job, I learned how security analysts and other information security professionals can use AI to augment their job duties, reducing tedium without replacing human workers. Due to this internship, I also gained tangible experience in explaining different cybersecurity and technical concepts to a general audience. While interning at Kindo, I used my knowledge of cybersecurity to find ways that AI can help automate processes to alleviate the burden of overworked security professionals.

### **Connections between the ODU Curriculum and the Internship**

Fall 2024 is my second semester at Old Dominion University (ODU) after spending two semesters at Georgia Tech and a semester abroad at the Technical University of Denmark. Due to my unique situation, my previous coursework at ODU did not prepare me for my internship at Kindo. However, I was taking 15 credit hours in addition to my internship this semester, and some of the concepts I learned in classes have helped me in my internship and vice versa. CYSE 270: Linux for Cybersecurity, helped me to review some of my fundamental Linux skills, which have come in handy as I experiment with different local host methods. This experimentation has also reinforced my Linux skills, which has helped me in my coursework. CYSE 300: Introduction to Cybersecurity, has also reinforced some of the cybersecurity basics I have used in my internship, giving me more exposure to concepts like firewall rules,

network traffic analysis, and different business security certification standards. I wrote the press release for Kindo's SOC 2 Type II certification before learning about it in CYSE 300, but seeing the behind-the-scenes of the process of achieving SOC 2 Type II helped to reinforce what I read in the textbook.

During my internship, I encountered many new concepts that I had not yet learned in school, especially concerning AI. Before working at Kindo, I had no idea of the process of locally hosting AI models, or that different AI models are better equipped for different things and that these metrics rapidly change.

### **Fulfillment of Learning Objectives**

As a reminder, at the end of August, I made the following learning objectives for this semester:

1. Develop educational content on using AI in cybersecurity tasks.
2. Gain confidence to give talks on AI in cybersecurity at cybersecurity conferences.
3. Research open-source AI tool-use projects focusing on cybersecurity.
4. Integrate WhiteRabbitNeo, a red-team open-source AI model, into these AI tool-use programs.

While some of these learning objectives were fulfilled during the past four months, due to the limited amount of time I could commit to work, some were not fulfilled.

The first goal, to create more AI in cybersecurity educational content, was mostly fulfilled. As I mentioned in the *Writing Content* subsection, I drafted a mini-series on locally hosting WhiteRabbitNeo, and have multiple new content ideas in the pipeline. Up to this point, however, my content has been focused more on the setup process than actually using AI in cybersecurity. I am hopeful that my future content creation will take me more into the cybersecurity space, rather than being fully AI-focused.

My second goal, gaining confidence to speak at conferences, cannot be fully assessed since I will give my first talk two weeks from now. At this point, however, I consider this goal fulfilled. Not only have I applied to multiple conferences, and been accepted at one so far, but I have also successfully worked at a conference as a sponsor, which intimidated me in the past. The true test of the work I have put into preparing for speaking at a conference will occur after the conclusion of this semester, but I hope it will be a success.

Unfortunately, the last two learning objectives involving integrating WhiteRabbitNeo into different AI tool-use programs have taken a back burner this semester. Due to personal circumstances outside my control, I was forced to cut back on my hours during November, which prevented me from doing more independent research and experimentation. I am hopeful that in the new year, I will be able to explore different tool-use programs and see if they will benefit the WhiteRabbitNeo community. While at Chicago BSides, I received many recommendations of programs to look into from attendees, and I look forward to researching them in the coming months.

### **Motivating & Exciting Aspects**

The most motivating aspects of my internship were attending Chicago BSides and being accepted to speak at London BSides. Working at Chicago BSides was my third work trip, and the first one over a weekend; where I would have free time to explore outside of working the conference. While in Chicago, I took the lead on collecting the packages and setting up the booth for WhiteRabbitNeo, which gave me confidence that I could successfully attend events by myself. During my free time outside of the conference, I was able to visit the Art Institute of Chicago and walk through Millennium

Park, which also helped motivate me to continue applying to conferences so that I could experience more places.

Being accepted to speak at London BSides has been the most exciting aspect of my internship over the past four months. It is discouraging to face rejections from conferences, so receiving an acceptance has motivated me to continue applying. It has also encouraged me to continue researching and experimenting with different applications so that I can find new things to talk about. I am also incredibly excited to go to London on a work trip, as I will have free time to explore the city while I am over there.

### **Discouraging Aspects**

As I alluded to in the previous section, one of the most discouraging aspects of this internship was receiving rejection emails from various conferences I had submitted CFPs to, or not hearing back at all. Another discouraging aspect tied to CFPs was missing several submission deadlines due to being caught up with schoolwork and other internship projects, lessening my chances of being accepted.

In addition to these challenges, I also faced discouragement from feeling like I had not accomplished enough during my internship, as it felt like it took weeks to finish any simple task. Upon reflection, however, I have realized that I have accomplished quite a lot in only 150 hours, especially since a decent amount of that was spent in Chicago.

### **Challenging Aspects**

The most challenging aspect of my internship experience came less than a week after I returned from Chicago when a close family member unexpectedly passed in early November. This passing took a toll on me, and it was challenging to focus on school or



internship work for a few weeks. My manager was incredibly supportive during this time and helped me to scale back my work commitments to avoid becoming overwhelmed. She, along with some of my coworkers, also sent me a very thoughtful succulent garden as a reminder that they are there if I ever need help. The best thing that I learned from this internship has nothing to do with my actual projects. The amount of support and compassion I received from my manager has taught me how I should support my future coworkers, especially those who report to me. While losing my grandmother is one of the most challenging things I have experienced, the support I received from my company will stay with me forever.

### **Recommendations for Future Interns**

My advice for any future Cybersecurity Interns at Kindo is to take advantage of any opportunities presented. Everyone at Kindo wants to see you succeed, but they cannot support you unless you let them know what you need. As a startup, Kindo has a very fast-paced environment, so be prepared to work hard and stay on top of your projects. You should also be prepared to be assigned lots of writing-related tasks. I feel that many cybersecurity students believe that internships and careers will be purely technical, but there is a lot of writing that goes into cybersecurity, especially as an intern. You should also be willing to experiment and think outside the box, as that will take you much further than blindly following directions. Kindo works on the cusp of innovation, so you should also be committed to learning on the job, as it is impossible to fully prepare for an internship that deals in AI.

### **Conclusion**

In conclusion, Kindo is a Venice Beach, CA startup focused on using generative AI to help automate tedious DevSecOps tasks, whether running playbooks, analyzing

logs, or securing source code. During my time at Kindo this semester, I worked with people spanning multiple time zones, which granted me flexibility with my work hours; but was occasionally challenging when I had to wait for someone to start their work day before I could ask questions. The primary Kindo product I interacted with was WhiteRabbitNeo, followed closely by the secure coding plugin.

During the past four months, my major work duties included creating tutorial videos on different functions of the Kindo product site and secure coding plugin, with a focus on WhiteRabbitNeo and cybersecurity, managing the WhiteRabbitNeo Discord server, writing content, and applying to speak at and attending cybersecurity conferences.

As stated in my *Challenging Aspects* section, the main takeaway from my internship experience was how to treat grieving coworkers, particularly subordinates, with compassion and grace. This internship experience will influence the remainder of my time at ODU by encouraging me to stay on top of recent developments in AI and cybersecurity, which is necessary to remain current in both fields. Building on that, this internship experience will influence my future professional path by helping me develop business writing and communication skills.

## References

*Kindo AI about.* (n.d.). LinkedIn. Retrieved December 1, 2024, from

<https://www.linkedin.com/company/kindo-ai/about/>

*Kindo features.* (n.d.). Retrieved December 1, 2024, from <https://kindo.ai/features>

Takahashi, D. (2024, July 15). Kindo raises \$20.6M to bring security to enterprise

AI. *VentureBeat*.

[https://venturebeat.com/ai/kindo-raises-20-6m-to-bring-security-to-enterpris  
e-ai/](https://venturebeat.com/ai/kindo-raises-20-6m-to-bring-security-to-enterprise-ai/)

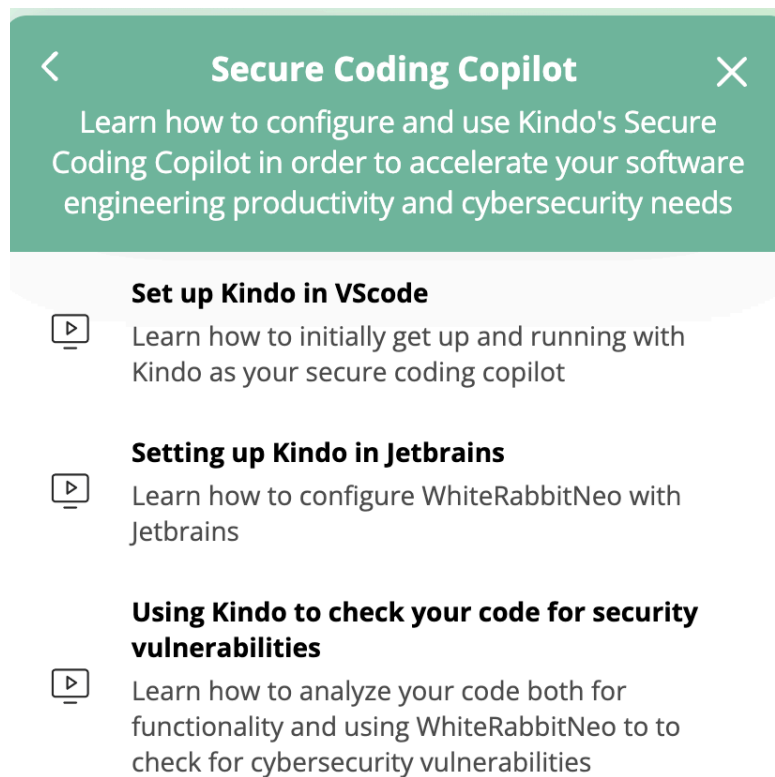
*What is DevSecOps?* (n.d.). Microsoft Security. Retrieved December 1, 2024, from

[https://www.microsoft.com/en-us/security/business/security-101/what-is-dev  
secops](https://www.microsoft.com/en-us/security/business/security-101/what-is-devsecops)

## Appendix

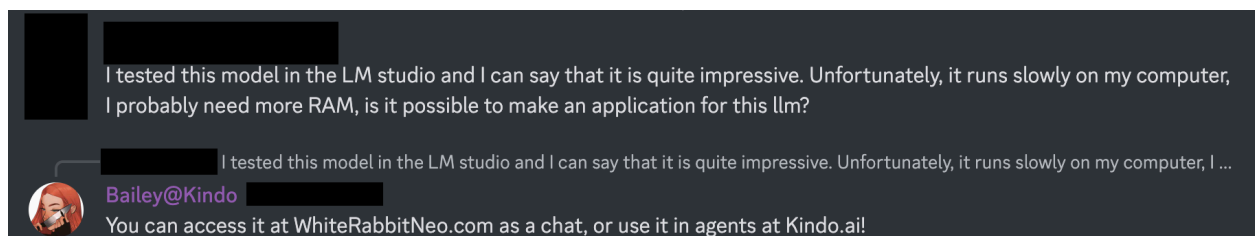
**Figure 1**

This screenshot shows the Secure Coding Copilot tutorial video playlist found on the sidebar of the Kindo product website.



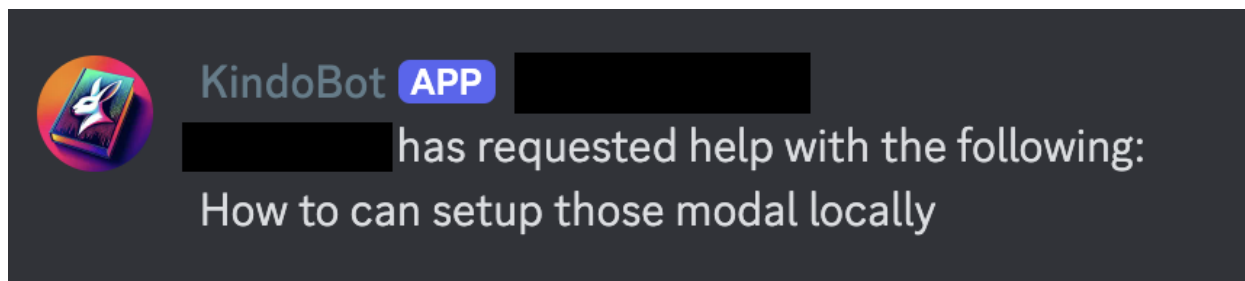
**Figure 2**

This screenshot, censored for privacy, shows an interaction between a member of the WhiteRabbitNeo Discord server and myself.



### Figure 3

This screenshot, censored for privacy, shows a request for help from a new member of the WhiteRabbitNeo Discord server, delivered via the Discord bot.



### Figure 4

This screenshot shows a step from my draft of a blog post detailing the steps to locally host WhiteRabbitNeo with Ollama. The screenshot displays the workaround I discovered to avoid problems with the Python 3.13.0 version.

#### 10. Set up a virtual environment

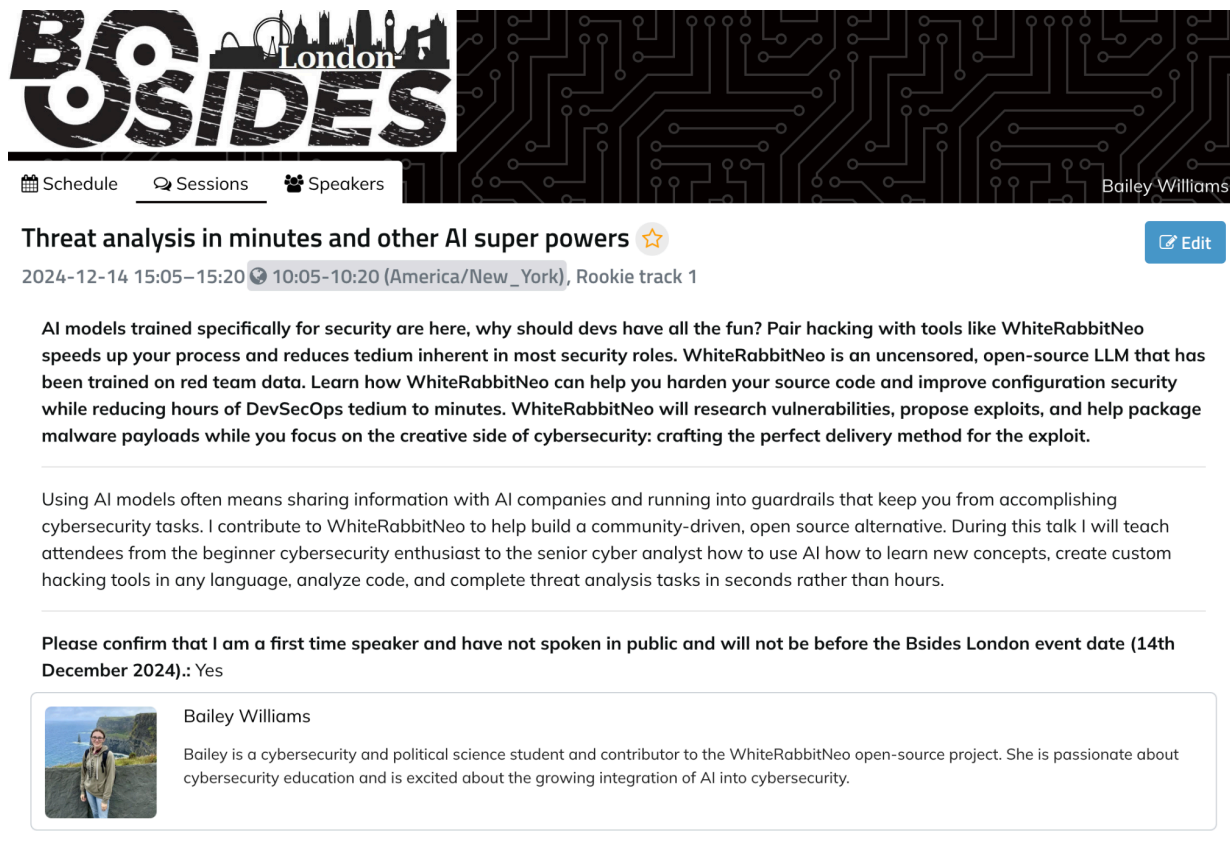
*The Python 3.13.0 update does not currently support some of the commands used below. To circumvent this, I downloaded Python version 3.12.7 from <https://www.python.org/downloads/>.*

*Once it is installed, run `python3 --version` in your terminal. If it says Python 3.13.0, run the command `alias python3='python3.12'`, then run `python3 --version` again. It should now read Python 3.12.7.*

```
python3 -m venv path/to/venv
```

**Figure 5**

This screenshot shows my talk information for London BSides 2024. It includes the title of my talk, *Threat analysis in minutes and other AI super powers*, along with the talk abstract, description, and my speaker biography.



The screenshot displays a web page for the BSides London 2024 event. The header features the BSides London logo on the left and a circuit board pattern on the right. Below the logo are navigation links for Schedule, Sessions, and Speakers. The main content area shows the talk title "Threat analysis in minutes and other AI super powers" with a star icon and an "Edit" button. The talk is scheduled for 2024-12-14 from 15:05 to 15:20, with a 10:05-10:20 slot for America/New\_York, and is part of the Rookie track 1. The abstract describes the talk's focus on using AI models for security, specifically mentioning WhiteRabbitNeo. The description elaborates on the challenges of sharing information with AI companies and the role of WhiteRabbitNeo in building a community-driven, open-source alternative. A confirmation prompt asks if the speaker is a first-time speaker and will not speak before the event date (14th December 2024). The speaker's name, Bailey Williams, is listed, along with a photo and a biography stating she is a cybersecurity and political science student and contributor to the WhiteRabbitNeo project.

**BSIDES London**

Schedule Sessions Speakers

**Threat analysis in minutes and other AI super powers** ☆

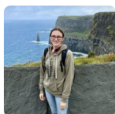
2024-12-14 15:05–15:20 10:05-10:20 (America/New\_York), Rookie track 1

✎ Edit

AI models trained specifically for security are here, why should devs have all the fun? Pair hacking with tools like WhiteRabbitNeo speeds up your process and reduces tedium inherent in most security roles. WhiteRabbitNeo is an uncensored, open-source LLM that has been trained on red team data. Learn how WhiteRabbitNeo can help you harden your source code and improve configuration security while reducing hours of DevSecOps tedium to minutes. WhiteRabbitNeo will research vulnerabilities, propose exploits, and help package malware payloads while you focus on the creative side of cybersecurity: crafting the perfect delivery method for the exploit.

Using AI models often means sharing information with AI companies and running into guardrails that keep you from accomplishing cybersecurity tasks. I contribute to WhiteRabbitNeo to help build a community-driven, open source alternative. During this talk I will teach attendees from the beginner cybersecurity enthusiast to the senior cyber analyst how to use AI how to learn new concepts, create custom hacking tools in any language, analyze code, and complete threat analysis tasks in seconds rather than hours.

Please confirm that I am a first time speaker and have not spoken in public and will not be before the BSides London event date (14th December 2024).: Yes

 Bailey Williams

Bailey is a cybersecurity and political science student and contributor to the WhiteRabbitNeo open-source project. She is passionate about cybersecurity education and is excited about the growing integration of AI into cybersecurity.

**Figure 6**

This screenshot shows the WhiteRabbitNeo booth at Chicago BSides after setup was completed before the conference began.

