FERRIS STATE UNIVERSITY
College of Business

Internship Reflection

Name: William Kittredge
Report Date: 8/10/2025
Major: Information Security & Intelligence
Internship Location: National Heritage Academies
Internship Semester: Summer 2025
Internship Start Date: 5/12/2025
Internship End Date: 8/8/2025
Final Internship Worked Hours: 491

Introduction & Internship Details

- Employer Name: National Heritage Academies
- Supervisor Name and Title: Kristen Ryskamp (Internship Coordinator/Employee Experience Specialist)
- Position Title: IT Security Intern NEX

National Heritage Academies (NHA) is a charter school management company that operates 100+ schools across 9 states in the country. During this internship, I worked for the security team in the Information Technology (IT) department at NHA's main headquarters: the "Service Center" office in Grand Rapids, MI. The NHA Service Center provides support to all charter schools managed by the company – it is essentially what enables operations for schools, teachers, students, and the organization as a whole on a day-to-day basis. Within the IT department, security analysts work closely with the enterprise applications team to ensure that we are effectively managing risks and protecting the confidentiality, integrity, and availability of our information systems.

FERRIS STATE UNIVERSITY
College of Business

Internship Reflection

Internship Description/Project/Activities

Normal daily activities mainly involved investigating security alerts using the ANY.RUN malware sandbox and/or Rapid7 InsightIDR and Microsoft Defender XDR cloud SIEMs, evaluating phishing email reports in the KnowBe4 PhishER SOAR, handling tickets using the TeamDynamix ticketing system, and attending daily meetings to report our work. During downtime, I had the opportunity to deploy an up-to-date enterprise Security Onion grid, and I created new automation workflows using Rapid7 InsightConnect to help our team respond to incidents faster once we've confirmed that something malicious has occurred. Otherwise, there were various training and networking events scheduled all throughout the internship. These included (for example) a professionalism workshop, a presentation workshop, a resume workshop, a leadership questionnaire panel, and outings to the 2025 CloudCon cybersecurity convention. At the end of the internship, I prepared a slideshow describing the basic responsibilities of a security analyst and reviewing what I worked on over the summer to present to all the other interns.

I'm fortunate enough to say that most of those activities were not things that I had to learn how to do for the first time. However, this doesn't necessarily mean that they were all easy for me to complete or well within my comfort zone. Most of the *actual work* (i.e., specific steps taken towards a goal) that I completed wasn't too overwhelming, but I did sometimes find it hard to remain organized and effectively communicate what I did during the busy days that involved many different kinds of work.

FERRIS STATE UNIVERSITY
College of Business

Internship Reflection

Course/Knowledge & Integration

Nearly every single task that I worked on during my internship at NHA could be mapped to something that I can remember doing, learning about, or at least being exposed to in class. Because of this, I think that the ISI course material prepared me well. Experience using ANY.RUN and various types of SIEMs in Network Forensics & Analysis prepared me for looking at alerts and emails every day, and the practice we had using Security Onion paid off when I was able to combine it with my VM-wrangling skills from Secure Digital Technologies (plus various other classes and competitions) to replace an outdated and broken enterprise deployment. Knowledge about various types of networking concepts and troubleshooting tools/techniques from classes like Network Security helped me correctly identify root causes when our Security Onion sensor node was unable to connect to the manager node, and when traffic was not being ingested correctly into the grid. Programming knowledge thanks to classes like Database Security, AI Concepts & Problem Solving, and Security Informatics (plus many Python scripts that hold my laptop together) became useful for creating error-resistant and user-friendly automation workflows that are fast, reliable, and (most importantly) documented.

I can't identify an area related to any specific cybersecurity task that I did during my internship where I felt like I was unprepared. I could always use more knowledge – but I think the classes are structured in a way that we (the students) should always have enough to go on if we hold up our end of the deal by taking them seriously. However, I do feel like I could have used more preparation with things like organization skills. I've previously written that I can't recall ever taking a course focused on how to organize information in a scalable, practical, and sustainable way in any school that I've ever attended, which seems strange when one considers

that we're usually being asked to learn new information every day. I think that this problem is somewhat exacerbated when someone chooses to have a career in information security because the chances are that you will be expected to have a high capacity for handling information.

Technical and Non-Technical Skills Integration/Acquired

The main technical skill that I have improved is my log searching abilities. During the first few weeks of the internship, there were upwards of 9 billion logs flowing through our Rapid7 SIEM every week. In addition, at least 10,000 Windows endpoints (teacher laptops) were generating very detailed information in the Microsoft Defender XDR SIEM. It became very important for me to search through logs with intent, write queries that could show me exactly the data I wanted, and to know where (e.g., which security tool or which log set) to even search through in the first place.

Non-technical skills such as communication, professionalism, time management, presentations, and teamwork were also reinforced because of the nature of the work environment and its expectations. If I wasn't improving due to exposure, there were also training sessions dedicated to giving specific, actionable advice for most of those skills.

Internship Experience

My internship experience was beneficial to me because it exposed me to *real* work in the information security industry. Education and training are undoubtedly essential, but not the same as what you gain by grappling with real logs, endpoints, and risks in the work environment. Furthermore, it was a tremendous learning and networking opportunity. Thanks to the internship, I was able to learn from some experienced people and get my foot in the door at a few places

after making new connections at a conference. It was also beneficial to see exactly what it looks like (i.e., what is required) to keep security under control at an organization like NHA.

The one thing that I wish I would have known or had more experience with is that as long as you're approaching the problem correctly, it's okay not always having the answer. In the beginning, I came in trying not to doubt what I could do and wondering what the environment would be like. The feedback I received at the end was that I needed to work on displaying more confidence in my conclusions because the team was surprised by how quickly I learned to meaningfully use the tools to work on investigations and add value regardless of whether I was able to carry them to completion or not.

Feedback

I think that future interns could benefit from (1): coursework that teaches different methods for organizing personal information (e.g., notes and research related to security investigations/work) that scale to medium-large amounts. (2): learning how to "work through others" more effectively when you're delegating work and/or relying on somebody to complete a task for you, especially when that task isn't going according to plan. (3): training about how to leverage AI tools intelligently – learning what it looks like to use (for example) ChatGPT as a tool and avoiding using it as a crutch (I don't trust AI so much, but we were encouraged to use it).

Based on my academic and experiential learning, I felt prepared for (1): the daily analyst workflow. I understood what a SIEM was, what they do, and what (generally) they look like. After reading through the Rapid7 documentation and watching a few videos, it was relatively easy for me to complete investigations using the same problem-solving methods that we learned

in classes. (2): I was able to rely on general computing and cybersecurity concepts and terminology learned from classes and apply them to various tasks such as deploying new VMs (plus one physical server), troubleshooting connectivity, creating automation, and tuning detection rules. During vendor meetings, I was able to keep pace with the discussion and understand technical terms and jargon without needing to reference anything. (3): Because of project management training, I could handle project management-related tasks as they were assigned. I was asked to create project outlines for each of the major projects that I worked on, and I was expected to hold weekly project progress update meetings.

Advice and Recommendations

Remember that the goal of an internship should be to learn as much as you possibly can. Although it might sound obvious, “making the most out of every day” is important because the internship will be over before you know it. Do what you can to build connections with people who genuinely want to help you learn and progress.