

Professional Skills Reflection

Introduction

My experience completing my Bachelor of Science Degree in Cybersecurity has provided me with a variety of technical and professional skills to begin my career working to protect information systems and networks. I have completed numerous projects during the delivery of my course work on the following topics: network security, cybersecurity, research, systems administration, machine learning, and technical communications/writing; these projects have allowed me to gain experience in problem-solving on complex issues and as well as communicating technical information accurately.

These three (3) skills, Cybersecurity Analysis; Problem Solving; Written Communication, show my essential skills as they pertain to cybersecurity, assisting to identify cybersecurity threats, create solutions to those threats, and to provide written communication on my findings (using technical and non-technical means) to others. The artifacts I have included within my portfolio are examples of me utilizing my learned skills through; research papers, project work, and hands-on assignments.

Skill 1: Cybersecurity Analysis

The cyber security analysis involves vulnerability identification, threat assessment, and the application of security procedures that will ensure security. Security experts are expected to find out about the risk before any attack takes advantage of the risk. It is therefore a valuable tool for security experts.

There are several artifacts contained within my portfolio that illustrate this individual capability. One such artifact is my Windows server security research paper, in which I researched potential vulnerabilities in Active Directory and explored ways to defend against various types of attacks (including Pass-the-Hash, Kerberoasting, and Golden Ticket). Another artifact is my machine learning intrusion detection project where I applied multiple machine learning models to classify network traffic and identify instances of malicious network traffic. My phishing white paper was also included in my portfolio, and I examined some of the recent trends in phishing and provided recommendations for security awareness initiatives.

All three of these projects have required me to evaluate current cybersecurity threats, assess different types of security controls, and articulate the reasons why some mitigation strategies are more successful than others. In the future, I will leverage this skill to help me assess the risk to the organization I am working for, investigate incidents related to security, and recommend practical solutions to strengthen the overall security posture of the organization.

Skill 2: Problem Solving

As one of the most critical skills in the field, problem-solving is a critical component to effective security operations. Each incident presents a different set of obstacles, and it is thus necessary to routinely assess information available in order to identify the cause of the problem and develop appropriate responses in an efficient manner.

My portfolio contains a number of artefacts that demonstrate my ability to troubleshoot and develop solutions to problems. One project in particular which best illustrates my ability to troubleshoot is a machine-learning-based intrusion detection model based off a large dataset; this dataset allowed me to clean the datasets, create multiple machine-learning based models and then compare their effectiveness. Another example of my ability to troubleshoot and resolve issues is represented in my assignments from my networking and Linux laboratories; in these assignments, I was able to implement a variety of solutions to a number of different types of issues, and learn how each of the tools used in the laboratory worked.

After spending many hours doing technology troubleshooting and consulting, I have developed enough skills to address the most common technical issues that come up through the use of different software. I will use my experience on the job to respond to technical incidents, troubleshoot technical issues, and provide and apply viable solutions for creating less system down-time as well as lessening the chances that a business will create Cyber Security Breaches.

Skill 3: Written Communication

For cybersecurity professionals to be able to communicate their findings using written communication, they have to make sure that the written communication is directed at an audience who will understand the findings. The audiences which cybersecurity professionals communicate to include the management, customers and other professionals, most of whom may not necessarily have the technical skills to understand the technical findings of the professionals. The effectiveness of written communication can be judged by making sure that there are clear action plans provided from the communicated information.

Various samples related to my written communications skill development are available within my portfolio. The SCADA systems research paper displays how I analyzed the need to protect critical infrastructure through the use of the CIA Triad; and that Thesis contains references to other sources. In my Phishing white paper, I examined various types of Cyber Security threats in a way that satisfied non-technical and technical audiences. My portfolio includes many assignment submission posts as well as various research projects summarizing technical subjects with references to appropriate academic literature.

Writing these assignments has allowed me to develop my ability to organize information in a logical manner, convey complex ideas in a clear manner, and support my conclusions using evidence. Communication skills are going to be a key part of my career as a cybersecurity professional, as cybersecurity professionals often need to write reports, document incidents, create policies, and communicate security recommendations to the people who manage their organizations.

Describing My Skills to an Employer or Supervisor

Cybersecurity Analyses

I have demonstrated strong skills in performing cybersecurity analyses as part of research projects and technical courses that focused on finding vulnerabilities and assessing risks to security. An example of this is my Windows Server security paper, where I researched the different types of attacks against Active Directory and provided recommendations for defensive strategies. These experiences have improved my ability to analyze security issues and develop practical solutions to those problems.

Problem-Solving

Throughout my coursework in cybersecurity, I learned how to take a systematic approach to solving technical problems by reviewing the parts that make up the problem, testing or creating solutions and measuring the results from each solution. For Example, I worked on a machine-learning intrusion detection project. To accomplish the objectives of the project, I needed to clean very large data sets, train multiple models, troubleshoot problems, and evaluate how well the various models performed. This experience helped me learn how to develop solutions for complex technical problems in an environment that constantly evolved.

Written Communication

I have developed strong written communication skills through completing multiple research reports and technical papers in cybersecurity. As part of my white paper on phishing and my SCADA research project, I needed to write in a clear manner so the reader could understand the technical information I provided, and I needed to provide credible evidence to support each of my conclusions. These experiences prepared me to communicate effectively to both technical personnel and to those in charge of an organization.

Strongest Skill Reflection

I consider the area I'm best at out of my three highlighted skills as the area of Cybersecurity Analysis. During my degree program, I was continually excited to research various security threats, how security attacks are executed and how organizations defend against security related attacks. After completing quite a few Cybersecurity related courses, I grew increasingly confident in my ability to evaluate security related risks and to advise on improving the security of an organization.

The assignment that aided the most in growing my Cybersecurity Analysis skill was my Machine Learning Intrusion Detection Systems project. For this assignment, I was tasked with interfacing my Cybersecurity knowledge with Data Analysis; I evaluated multiple machine learning algorithms and I interpreted the results to see which ones produced the most effective intrusion detection results. This particular assignment challenged me to think critically about many different types of Cybersecurity incidents while applying knowledge from several different domains within Cybersecurity.

Upon entering my professional career in Cybersecurity, I hope to grow my Cybersecurity Analysis skill by working within a Security Operations Center (SOC), Threat Analysis or Cybersecurity Engineering. In my employment, I would like to help organizations identify and mitigate security vulnerabilities and to assist organizations in improving their overall security.

Applying My Skills Going Forward

Upon graduation, I intend to develop my technical and practical knowledge/skills, through certifications and real-world, practical experience within the field, while also keeping up-to-date on the constantly-evolving cyber threats affecting the world today. As the cyber-security industry is growing and changing quickly, continued post-graduate education will be imperative in my cyber-security career. Additionally, I plan to expand upon my knowledge of cloud security, digital forensics, and security automation, thereby continuing my professional growth as a cyber-security expert, and being able to contribute positively to my prospective employers.