Baylor University

Final Report

To: Dr. Savanah N. Landerholm, Professor
From: Bryant Huang, Student
Subject: Final PDP Report
Date: February 20, 2025

The purpose of this memo is to present my findings and analysis from my interview with Harmond Drenth regarding written communication in my future professions. The goal of the project is to prepare me for technical writing in my chosen field through interviewing someone in the current field and examining related writing samples.

Introduction

Summary

The goal of the project is to gain experience from querying different sources for a wholesale view of technical communication within the field of cybersecurity. I learned that in cybersecurity, there are two main types of technical communication, beyond just the usual forms of corporate communication. First, there are vulnerability reports, which inform the reader of possible issues with current production environments or code. Then there are incident reports, which report on security events after the fact. These documents, along with other communication forms, vary widely in information and audience, so an important aspect of this is to understand who I'm writing to and how to best communicate the main point of each document. With this information, I will be able to communicate more effectively with my supervisors and peers within a professional environment in the future.

Methods

My main source of information was from Harmond Drenth. Harmond is a Cybersecurity Analyst Rotationer, which means that he was an analyst that worked several different positions over a certain amount of time. Unfortunately, although the original plan was to obtain real writing samples from Harmond, as he did not receive permission from his superiors to give me access to the documents. However, he was able to provide me with a detailed outline of what he writes whenever he details his results. I also sought out supplemental information from reputable cybersecurity resources online after the interview, looking to do more research on the different types of documents that Harmond was able to inform me about during our interview, looking for examples of those documents that contained publicly available information instead of confidential information.

Findings

Interview Results

SOC Analyst Flow

Harmond described his career at Dell in the interview. He outlined different technical reports he has written for each role, and how he has learned and grown through the process of writing each piece of communication. While at Dell, Harmond had a 6 month stint in the Security Operations Center as an analyst. He spent most of his time analyzing logs and writing incident reports, depending on what breaches in security he found that day. Because these reports were important legally, he often would take an entire day just to make sure something that he was writing was detailed and clear. The reports that he wrote varied widely in audience, as they could go to someone on the Senior Leadership Team, such as a Chief Information Security Officer (CISO), or just a coworker that was curious about the alert that was triggered. Because of his experience communicating with members of his cybersecurity team at Baylor and professors, Harmond found that code switching between Executive Leadership and coworkers was a task that came easily to him.

PCS Analyst Flow

Harmond compared this to his experiences on the Product Cybersecurity Team, where he currently is assigned. At this position, he rarely writes to anyone beyond Software Developers or Software Architects. This allows him more freedom to be more technical, as usually the people that he was writing to could understand the textual context that he uses. However, software developers are often very busy and want just the basic information so that they could patch or fix the weakness in their code. Harmond often found that he needed to spend extra time cutting down information into quick descriptions so that he could make the developers' lives easier.

Online Research Results

Incident Report Research

Incident reports are usually filed once a breach materializes or an alert is triggered. Most good incident reports are not very technical, in fact, most of them make very large abstractions as to the technical aspects of a breach. More often than not, they are going to be escalated to Executive Management to inform them of concerns that need to be addressed. However, it does need to be as clear as possible as to what the evidence is and what the recommended actions are. The incident report is meant to help make decisions as to what security measures to enact, and also to be used as evidence in case of a lawsuit. The incident report was surprisingly compact, and did not include a lot of technical details. This was another interesting point where the audience mattered, in which most people's objectives when reading an incident report will differ.

For example, when Senior Leadership reads incident reports, they are looking for impacts on the business model, not how to fix it. When the Security Operation Center reads the report, they are looking for technical options on how to fix the breach and how to prevent the incident from happening again.

Vulnerability Report Research

Vulnerability reports were an interesting breed of writing. Most vulnerability reports utilize a summary, overview, details on how to execute the vulnerability, findings, and recommended mitigations. (Poston) The main goal of the document is to guide the developer to bug fixes and timely patches. It's important to leave contact information in the vulnerability report, so that the engineers can involve the writer in the process of verifying and testing the changes, as the writer knows the vulnerability more intimately. A crucial part of every vulnerability report are severity level indicators. For example, the Hacken penetration test for Kalmar Smart Contracts utilizes a rating system of "Critical, High, Medium, Low, and Informational." (Matiukhin) These indicators give an easy way for developers and any other readers to qualify how urgent something needs to be fixed. It's a lot harder for a non-security professional to understand what a "Shellcode Buffer Overflow Attack" is, but much easier for people to understand "Easy to access, Critical" vulnerabilities. There are various scoring systems to give ratings, and usually they are expanded on in detail within the report. This textual context is also utilized in incident reports, but are usually not expanded on, as the goal isn't to find out specifically what the immediate patch is, but as to how to prevent it from happening again.

Email Etiquette Research

One of the main forms of formal communication between peers that Harmond described was through email. I found it interesting that it was essentially a way for communication to be documented for future use. There were only a few situations that Harmond mentioned that justified email usage over regular web chat services for communication. Among the situations that he detailed, filing complaints stood out the most to me. When filing complaints about a situation, a team member, or a client, there is much more pressure to follow formal writing practices and being as detailed as possible in describing the situation, sparing no room for miscommunication. This is a stark contrast to other forms of short or long form communication between peers and authorities, usually within tech companies there is a strong emphasis on being as quick and to-the-point as possible.

Conclusion

Discussion

From my interview and my research, I found that there were two major genres within cybersecurity, vulnerability reports and incident reports. Each one goes to varying audiences and each one utilizes different textual patterns, along with different messages. I didn't actually think that there would be such a huge difference in terms of documentation written between the varying levels of cybersecurity. I knew that there were a lot of roles, but there was a much bigger gap in terms of audience than I thought originally. From executives to peers to clients, each report requires a different approach, and the most important portion of this would be to identify what everyone's priorities are. However, something that I noticed was that the terminology was consistent throughout each report. The length of explanation as to what each term was, and the textual context behind each term might've been different, but many of the same concepts are repeated within each document, just some more abstracted than others.

Recommendations

The most impactful thing that I learned was that even in a field like cybersecurity, the types of written communication will differ slightly depending on your role and tasks. This is mainly because every role will report differently, and to different superiors or peers. I found this personally surprising, as I always assumed that writing in my field was somewhat uniform. After interviewing Harmond, I realized that it was paramount for me to learn to code-switch between my peers and my superiors, making sure I know who my audience is and how they are meant to react to my message. Especially after reading through the examples online, I gained a newfound appreciation of technical writing in cybersecurity. Who knew that it would have such a prevalent role in the inner workings of tech companies? This is definitely something that I'll have to be more careful about when I enter the workforce in the summer.

References

Drenth, Harmond. Personal Interview. 28 January 2025.

Poston, Howard. “HOW TO WRITE A Vulnerability Report” Infosec Institute, 1 Feb. 2022, www.infosecinstitute.com/resources/vulnerabilities/how-to-write-a-vulnerability-report/. Accessed 12 Jan. 2025.

Matiukhin, Andrew. SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT, 3 April, 2021. Accessed 12 Jan. 2025.

Appendices

List of Interview Questions:

- What would you say is the most interesting thing you’ve found at Dell? How did you communicate it to your peers or superiors?
- What would you say is the main form of informal peer to peer communication at Dell? What are the reasons that Dell would choose that service?
- What would you say are the main forms of formal peer to peer communication that you use at Dell? What are the reasons you would choose to use that service?
- What is the most common piece of paperwork you’d work on in your rotational periods? What did they usually consist of?
- Why did you choose Dell? What about their culture drew you to them?
- Who do you report to at Dell? What is your relationship like with him/her?
    - What is your most common form of communication with this person?
- What were some things that you found surprising about technical writing within cybersecurity?
- What were some thing that you struggled with or naturally did well at?