Digital Forensic Analyst

Jeremy Osborne

Old Dominion University

Cybersecurity & Social Science – CYSE201S

Professor Diwakar Yalpi

Due November 29, 2023

Introduction

It is an unfortunate reality that unlawful actions are performed on a daily bases. This applies to not just the physical world but the digital world as well. When a crime is committed in the physical world and the perpetrator isn't obvious it often falls to a detective to piece together physical clues and evidence to figure out what happened. But what happens when a crime is committed in the digital world where there isn't likely to be any physical clues or evidence? Enter the digital forensic analyst (henceforth referred to as DFA). And while the methods and medium may be different, these two roles share a striking amount of similarities. The role of a DFA may not seem very attractive at first glance, but if you take a deeper look, it quickly becomes clear just how important this position truly is to cybersecurity.

What is a digital Forensic analyst?

Despite the name, someone in the role of digital forensic analyst does more than just analyze. While analysis definitely falls in the scope of a DFA, the Cybersecurity & Infrastructure Security Agency (CISA, 2023) list a few other core responsibilities such as sorting through recovered data for relevant information and reporting technical summaries of whatever is found. The CISA (2023) categorizes the position of DFA as an investigative position. As such, an individual will spend a good amount of time going through a variety of data to determine what method(s) will work best to identify and track down the perpetrator(s) of a network intrusion. An individual may also be asked to use their experience and knowledge from past incidents to improve the defensive capabilities of a company's own network.

What does it take to become a successful DFA?

In order for an individual to succeed as a DFA, the CISA (2023) recommends that the individual possess a collection of skills and knowledge. This can range from having "[k]nowledge of investigative implications of hardware, Operating Systems, and network technologies" (CISA, 2023) to the ability to analyze and reverse engineer various malware programs. The EC-Council (2022) explains how the increase in data breaches and cyberattacks, plus the increase in price per incident, has brought about a growing need for DFAs. With the increasing number of available jobs and skills required to perform in the position, potential candidates have their pick of companies to work for. With the number of available opportunities and the skills required to qualify for the positions, the proverbial devil on the shoulder could start whispering in some people's ear.

As a DFA, individuals may find themselves with potentially valuable information in their possession. The skills possessed by someone in the position of DFA, put them in a prime position to understand not just security vulnerabilities but also the kinds of programs needed to take full advantage of those vulnerabilities. If a person doesn't have a strong moral foundation, the thought of easy money could cause them to start committing white-collar cybercrimes. Even though these crimes are certainly illegal, it is not unheard of individuals falling victim to the idea of making easy money selling information or programs on the dark web. For this reason, it is ever important for companies to have proper policies and checks in place to discourage anyone hoping to make a quick profit.

Why are DFAs important?

Just as detectives make it clear that a physical crime won't go unpunished, it is up to a DFA to make sure cybercriminals are caught and persecuted. A DFA takes it one step further however and attempts to fix the vulnerability that a cybercriminal used to perform their attack. As the world becomes more and more digital in nature, the threat of cyberattacks is most certainly going to rise exponentially. In order to protect ourselves individually and as a collective, jobs such as DFA will become critical in the attempt to counteract cybercriminals. A DFA is an invaluable asset for any company that is interested in not only catching potential perpetrators after a cyberattack, but also learning from an attack and better securing their assets against future attacks. While they may not be the poster figure for a company, DFAs stand as critical roles in the protection of not just a company but also as defenders of the information that has been trusted to a company by their customers.

Why would someone want to become a DFA?

With so many jobs available and a lack of qualified people applying for them, the job market is a wide open field ripe with potential. While most employers require some prerequisites, such as varying degrees of greater education or proof of skill via certifications, if an individual can prove themselves worthy of the position, they will find themselves with a career that is rewarding in several ways. Coursera (2023) tells that DFAs are often offered well-paying careers that offer an ever evolving and challenging environment. While working to make the internet safer for the average person is in itself a great reward, that alone is sadly not enough to pay for life's essentials. Fortunately, Coursera (2023) reported that as of September 2023, the average salary for a DFA was nearly $80,000. With the ability to earn a good salary

along with making the internet a safer place, it is not hard to see why someone would want to become a DFA.

Conclusion

Like the job of detective, people may often overlook the job of DFA on account of how simple the job may seem. In reality, being a DFA is a demanding career that not only makes extensive use of the skills and knowledge an individual possesses, it could at times test an individual's moral fortitude. However, if said individual can make a good name for themselves in such a diverse and ever growing industry, the opportunities for career advancement could be near infinite. When one considers all the aspects of the job, it's not hard to see why someone would obtain the degree and certifications required to become a DFA. And with the ever expanding digital world, the job of DFA is bound to only become more and more secure.

References

Computer Forensic investigator: 2023 career guide. Coursera. (n.d.). https://www.coursera.org/articles/computer-forensic-investigator

Cyber Defense Forensics Analyst: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/careers/work-rolescyber-defense-forensics-analyst#:~:text=This%20role%20analyzes%20digital%20evidence,Computer%20Forensic%20Analyst

What is a digital forensic analyst?. Cybersecurity Exchange. (2023, November 2). https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensic-analyst/