

**Fundamentals for IT Professionals II**

Year 2 (2022/23), Semester 4

**SCHOOL OF INFOCOMM TECHNOLOGY**

Diploma in Cybersecurity & Digital Forensics

**Assignment 2**

**Industry Engagement**

**Duration:** Weeks 13 - 15

**Weightage:** 20%

**Individual/Team/Both:** Individual

**Deadline:** Report

Softcopy (submit to BrightSpace)

**27 Jan 2023, 8.30am (Friday)**

|  |  |
| --- | --- |
| **Student ID** | **S10222894G** |
| **Name** | **Dominic Lee** |
| **Module Group** | **P02** |
| **Grade** |  |

**Reflection 1: Zero Trust Network**

Diagram

Description automatically generated

The first webinar I attended was called the BlackBerry Security Summit 2022 which touched on the topic of “Unpacking of Zero Trust Network”. It was conducted by Shishir Singh, the executive vice president of BlackBerry.

**Nature of the online seminar:**

I attended the talk through my computer on the Bright Talk website, it was a live presentation by one speaker, Shishir Singh, and there was a question box where viewers could send questions to the speaker. This was an educational online seminar.

**Reasons for choosing the online seminar:**

“Zero Trust” is a cybersecurity principle that emphasizes the need to always verify a user’s identity and the security of their device before granting access to sensitive information. This is important because it helps to prevent unauthorized access as well as protect against threats like malware. Additionally, Zero Trust, limits the attack surface for most organization and is seen as a great practice for security.

With the increased usage of technology, the attack surface of many organizations is rapidly increasing, and security is becoming more and more important to organizations around the world. The zero-trust model in turn is thus becoming increasingly popular and I believe that it is important to have a deeper understanding of it as it becomes more widespread across various organizations.

**Details and Insights of the Webinar:**

I will first talk about the overview of what the webinar touched on before diving into the details. The webinar talked about the zero-trust framework, describing, and elaborating on it, unpacked how to deploy zero trust frameworks, and lastly talked about how zero trust is becoming more popular by companies.

The webinar started off by showing the increasing popularity of zero trust through the diagram below.

Timeline

Description automatically generated

The diagram above illustrates how many companies are starting to see the importance of security as well as the need to implement it via zero trust.

Following, the presenter talked about the zero-trust framework. From this section of the webinar, I learned that zero trust is a concept that assumes all devices, users and networks are potentially compromised and it lives by the principle of “never trust, always verify”. Also, zero trust differs from traditional security models which often rely on tools such as firewalls to protect against threats. Furthermore, security is becoming harder to ensure for multiple reasons. Firstly, attacks are becoming more sophisticated, payloads used are becoming more complex and harder to understand which would make it hard to defend against. Also, using more security products does not translate to having a more secure system.

Lastly, the presenter went on to unpack zero trust by mentioning that there are no clear security parameters as well as the key aspects of the Zero Trust model. The key aspects mentioned included Identity and access management (IAM), Device Trust and Network segmentation. Regarding IAM, users and devices must be authenticated and authorized before they can access sensitive information, this can be done through techniques like MFA. Device trust refers to the security of the device that is being used to access sensitive information. This can be done by checking for malware on the device or ensuring that it is updated. Finally, network segmentation refers to the fact that sensitive information should be segmented from the rest of the network and only accessible to authorized users which can be done through virtual private networks VPNs.

**Relevancy of the Webinar:**

Zero trust is highly relevant in cybersecurity because is addresses any of the challenges face by organizations when protecting their systems from cyber threats. Zero trust allows organizations to better deal with the problems arising from increase in remote work among employees, rapid increase in cloud and mobile computing and lastly advanced threats such as malware. All these issues mentioned can be better combatted with zero trust which makes it extremely useful as tool when trying to ensure cybersecurity. Through this webinar, I realizes just how complex it really is to ensure set up a zero-trust network that is functional which inspires me to learn more about how I can do so in the future.

**Impact of Webinar on future goal:**

While I do not fully know what I will be doing in the future, having a better understanding of a zero-trust security model will aid should I work in an organization that deals with sensitive information such as the healthcare or finance industry. Also, as there is a high chance I will be working in the IT or cybersecurity field understanding the concept of zero trust and its implementation can give me an edge over others when searching for a job.

The online seminar also reminded me of modules that I learnt previously and am currently learning which are SSD and SCS. Both modules apply or taught the concept of zero-trust or in other words the concept of least privilege. This has allowed me to have a better understanding of how zero-trust works in the real world as during this module, I learnt zero trust on a very theoretical plane. Regarding my future goals, zero trust will be extremely useful to me as more and more companies are starting to implement zero trust models into their organizations. This gives me an edge over others if I learn it well. Lastly, when in secondary school there was a project where because I trusted my teammates so much, I did not check their work and they delivered poor quality of work which costed our group the project, and after learning about zero trust I can relate these 2 events.

Overall, while the future is unknown, I know that a better understanding of zero trust is bound to help me one way or another.

**Reflection 2: Top Security Trends in 2023**

Diagram

Description automatically generated

**Nature of the Webinar:**

Likewise, this webinar was held online on the same website Bright Talk as the first webinar. It was also a live broadcast where 3 experts Martin Lee, Richard Archdeacon, and Wendy Nather shared their thoughts on the topic discussed: “Top Security Trends for 2023”. Furthermore, it was an interactive webinar as viewers had the option of asking questions to the live guests.

**Reasons for choosing the Webinar:**

Cybersecurity is a rapidly evolving field, and it is important to stay up to date on the latest trends and threats. This online seminar covers what experts in the field believe will be the trends for the coming year which allows us to better understand and prepare for what's to come into the cybersecurity field in 2023 and the coming years. This would aid in my career development as I learn on how to stay current and improve my skills which would help me should I pick a career in this field. Additionally, understanding cybersecurity helps me to better keep my personal information safe. As cyber-attacks are becoming more and more sophisticated, a webinar like this will allow me to learn how to protect myself from cyber-attacks. Lastly, for both webinars, I chose to attend them because webinars are cost-effective and convenient. I can attend both webinars from the comfort of my home and not have to pay any money to attend them. This allows me to learn without having to commit any money or time travelling.

**Details and insights of the Webinar:**

The first point that was discussed was the fact that by 2025, threat actors will have the ability to perform disruption to operational technology which could cause human casualties. This signifies the convergence between the cyber and physical world. Also, as there will be a continued rise of ransomware attacks, the speakers pointed out the importance of being resilient to cyberattacks. A method stated was that using employees reserved for responding and reacting to a cyber crisis, an organization’s resilience increases by 10 – 15%. This also meant that the ability for an organization to adapt on the spot is much more valuable. Another point mentioned was that governments around the world are going to continue to introduce more stringent regulations and compliance requirements to address the growing threat of cyber-attacks. Lastly, the speakers mentioned the likely increase in targeted attacks on IoT devices as they become increasingly common and to conclude the speakers mentioned how to conduct threat intelligence which is basically finding out what the threat actors are trying to do. The method goes as follow: Identify likely scenarios -> Prepare for the worst -> Find ways to reduce likelihood of such scenarios -> Find ways to reduce the impact should the worst case occurs.

**Relevancy of the Webinar:**

This webinar is relevant because through understanding the top security trends are individuals and organizations able to protect themselves from cyberattacks. Without keeping up to date in the cybersecurity field, it is easy to lose relevancy as the field is ever evolving. Prior information becomes quickly outdated and ineffective against the ever-evolving attacks of threat actors. Hence the best way of protecting and ensuring cybersecurity is to keep up with the trends as both individuals and organizations can take proactive steps to protect themselves and minimize the risk of any security incident. From this webinar, I would like to learn more about the various ways attackers use to attack IoT devices. This is important to me as I believe IoT is growing rapidly and often, security for IoT is neglected which leaves big security vulnerabilities. By learning more, I believe I will be learning something useful in the time to come.

**Impact of the Webinar on Future goal:**

This webinar helped me to understand what it is like keeping up to date with cybersecurity trends. I have always been told that cybersecurity is an everchanging field and that it is vital to be up to date with what is happening, but I never attended any events that updated me until this webinar. As I am still considering whether I will pursue a career in cybersecurity, this webinar gave me greater insight as to whether I am committed to keeping up to date which I can say for now that I am. Also, by attending this webinar I have a better understanding of the nature of careers in cybersecurity.

Additionally, by learning the top security trends I learnt on how to keep up to date with the industry similarly modules like WAPT which I am currently learning, it is important to keep up to date with the top vulnerabilities to see which ones are on a rise and decline i.e., Top 10 CVE vulnerabilities. Through this I see the practical side of what keeping up to date means in the cybersecurity industry. Furthermore, I can connect this to my past life experience as when I was younger, I enjoyed playing Football and I would keep practicing and researching on the topic of football which allowed me to improve much faster than my peers and understand the game at a deeper level.