MSc Project - Reflective Essay

Project Title:	Evaluation of Splunk Enterprise for Monitoring and Investigating Cyber-Attacks
Student Name:	**Mahir Asif Khan Nargis**
Student Number:	**210777196**
Supervisor Name:	Dr Edmund Robinson
Programme of Study:	MSc. Computer Science

1. Introduction

In recent times, the focus on cybersecurity has increased. Companies have started to possess substantial digital assets and are more globally connected. Data collection and analysis are critical for organisations to expand, but this also brings the responsibility of protecting sensitive data. Audits are in place, and enormous fees are present for organisations that fail in their duty. To ensure cheaper insurance premiums, organisations must prove they have a cyber security team and a security operations centre to monitor and detect threats through suitable fail safes and measures. To my knowledge, a SIEM solution is vital for this purpose. The future lies in developing SIEMs until they are self-sufficient and need no human input to monitor, detect and protect systems.

2. Personal Development

I undertook this project to gain knowledge and experience using the Splunk SIEM software. To fulfil the goal of working as a security engineer whose responsibilities lie in constructing and implementing security measures that monitor and mitigate vulnerabilities. SIEMs are a key part of Security Operation Centers. Working on this project has given me a taste of what it would look like to work in such an environment and learn more about threat intelligence gathering.

While I was sure about my chosen field for my dissertation, I struggled to focus on a single targeted topic. My background research led me through the broad field of cybersecurity. There were many exciting fields I could work on, such as vulnerability detection, monitoring systems, responding to incidents, digital forensics and penetration testing. Ultimately, I decided to focus on SIEMs as I felt it would summarise all I learned in one place. It was challenging to determine what was relevant for the project, but I think I did an excellent job on the literature review and levelled up my research skills.

I improved my perseverance and time management skills starting a month after my summer exams. I built a habit of doing a little bit of work every day, setting realistic time goals on software to learn, topics to research and words to write for my report. By the time I decided on a topic, I had small nuggets of knowledge about many other areas, which helped me immensely to complete the practical part of my dissertation. This was also the first time in a long time that I completed an assignment two days before the deadline. It gave me plenty of time to proofread my work, reference things correctly and ensure the work standard was satisfactory.

2. Strengths/Weaknesses

2.1 Strengths

- The project used Splunk Enterprise to conduct two case studies of intrusion detection and investigation.
- Diamond Model of Intrusion System standards were applied while conducting the investigations.
- Identified the strengths of Splunk Enterprise and operational points where it is lacking.
- Proposed further areas of improvement and development for SIEM solutions currently in the market.

2.2 Weaknesses

- The investigations were very time-consuming, and a lot of background research was required to understand the necessary steps to progress further.
- I may not have used Splunk Enterprise to the fullest capacity as I am not familiar with the more advanced use cases of SPL (Search Processing Language).
- While my research used publicly available documentation of Splunk Enterprise SPL, there is not much information on the inner workings of the proprietary search processing language.
- A lot of Splunk's features rely on third-party software to complement it.
- Splunk Enterprise is expensive and not affordable for smaller companies or students like me.

3. Analysis of theory and practical work

Learning about Splunk through undertaking two case studies and answering pre-determined structured questions helped me gain initial knowledge of SIEM solutions and their essential components. The focus of my literature review was to write about the history of SIEMs and understand how they have developed over time.

Intrusion detection and threat hunting are best learnt through practice. There is abundant evidence suggesting focusing on practical aspects rather than theory, and this applies to most cybersecurity fields. The transfer of knowledge is usually done through stories or past scenarios/case studies. An example of learning through practice is the boom in creating honeypots (fake systems) to gather information on how attackers operate. Currently, there is a great need for information gathering and analysis of attack vectors for preparation to defend from similar cyber threats [1].

Before beginning my practical investigations, I had to learn more about Splunk and its proprietary search language, SPL. While not very challenging to do simple searches, getting into evaluation queries and calculations was challenging. I had to also learn about how professionals carry out investigations and learn more about the kill chain process. To think like my adversaries in order to carry out a proper step-by-step investigation and know where to look.

While investigating web activity, I had to refresh my memory on the fundamentals I learned in my Security and Authentication module. There was a lot on HTTP traffic; POST/GET methods in particular. I finished some courses on Windows Sysmon and Windows Event Manager, revised material on encryption and learnt to use a bit64 decoder to decipher raw email content.

The USB ransomware investigation was much harder to carry out, with many dead ends and trial and error. Thankfully, the scenario provided many hints, which I followed to carry out reconnaissance on the mode of delivery, identify the damage and find the source of malware. I also gained experience determining the type of malware and the required steps to quarantine it. Since we were dealing with a MAC OS machine, I had to learn how to use OSquery and apply it to SPL to search the directories for any malware event.

I have also covered topics such as Intrusion detection system (Suricata), Windows Events, Windows Sysmon events, Active Directory and privilege escalation.

4. Future Work

The alert feature of Splunk Enterprise is not available in the free version. This didn't allow me to carry out some case studies that involved setting up monitoring alerts. Alerts can detect suspicious activity like brute force attacks, connections from geographically blocked areas, failed privilege escalation, dormant service accounts being activated, unusual amounts of data downloaded, etc.

I would enjoy applying what I have learnt about SIEMs and building my own simple SIEM. My initial idea would collect logs from an Intrusion Detection System like Suricata and Windows Event System while using a storage system like Elastic Search.

A better method of testing Splunk's SIEM capabilities would be penetration testing. Through the use of attack vectors, we can test whether Splunk's alert systems and configurations are successful in providing an effective defence from cyber threats or they are bypassed, leaving the user vulnerable.

5. AWARENESS OF LEGAL AND SOCIAL ETHICS

Threat hunting and the act of investigating are perfectly legal. The actions tend to identify security flaws and resolve vulnerabilities in a system. This is, of course, considering that the person carrying out the investigation has the owner's permission. Once an organisation gives access to the system, you are still bound by rules such as not exposing confidential information, altering or destroying company data or creating backdoor access into the system for later use.

In our case, we used our own virtual machine and thus required no permission from anyone. The dataset we used collected evidence from artificial honeypot devices, and the scenarios/events were manufactured to be used for learning purposes. No harm was caused to anyone during the practical, and no sensitive data was involved. The dataset is available for public use. The version of Splunk Enterprise was free and publicly available. No internal proprietary information was divulged.

REFERENCES

1. Kaspersky "What is a Honeypot?" 2022.
   URL: https://www.kaspersky.co.uk/resource-center/threats/what-is-a-honeypot
2. McKinsey & Company "Perspectives on transforming cybersecurity" 2019
   URL:https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx
3. Splunk> "Penetration Testing: Practical introduction and tutorials" 2022
   URL: https://www.splunk.com/en_us/blog/learn/penetration-testing.html