An Open-Source Solution for Corporates to Implement Scenario based Intrusion Detection for Incident Response

D.S Kithulgoda
Reg. No. MS20907198

M.Sc. in IT
Specialized in Cyber Security

Supervisor : Mr. Amila Nuwan Senarathne

December 2021

Dissertation submitted in partial fulfillment of requirements for the Degree of Master of Science in Information Technology - Specialized in Cyber Security

Faculty of Graduate Studies and Research
Sri Lanka Institute of Information Technology

Table of Contents

List of Figures

List of Tables

Declaration

I hereby declare that this work is my original research and formally acknowledge that this MSc. Thesis contains no material that has been previously submitted to another university or higher education institution for the purpose of earning a degree or diploma and, to the best of my knowledge and belief, contains no previously published or written material by another person, except where the author's name is acknowledged in the document. Additionally, I grant Sri Lanka Institute of Information Technology the non-exclusive right to reproduce and redistribute my dissertation, in whole or in part, in print and other media for the purpose of future works, with the understanding that this right will be revoked. I reserve the right to use this material in its entirety or in part in any manner I deem appropriate (such as any book or ongoing article).

……. …….

D.S Kithulgoda (MS20907198) Date

The above candidate has carried out the research for the MSc. under my supervision.

……. …….

Mr. Amila Nuwan Senarathne Date

Acknowledgement

Without the assistance from several individuals, the core of this research would not have been possible. I would like to express my humble appreciation to everyone who has aided me in any way with this project. My thesis supervisor, Mr. Amila Nuwan Senarathne, has provided me with exceptional guidance, encouragement, and support throughout the work and I really appreciate his assistance. I am grateful to my parents and all friends for their unflinching love and support received during my master's degree journey, as well as for everyone else who assisted me in many situations during the dissertation writing. I owe my university a debt of gratitude for providing timely and valuable course modules in the field of cybersecurity and also for guiding me in a multitude of ways to continue developing my theoretical and practical knowledge in this field while also advancing my professional career in a smooth yet revealing parallel timeline.

Abstract

Detecting potential security compromises to aid in formulating a proactive response strategy is still a relatively new field in the local network security arena. Even managed security service providers who support these corporates on different digital security tiers face difficulties when using practical implementations that have the capability to detect and escalate to relevant parties for mitigation. This research discusses how a third-tier detection strategy can be developed with open-source toolkits like the Snort intrusion detection system as the second line of defense to support network teams. The necessity of auxiliary packages to work along with Snort must be stressed upon because the demands are higher in corporate environment settings. Some examples include Zeek and Security Onion. The placement of an IDS to perform as expected requires careful planning after a thorough examination of the relevant network diagrams. For this, the recommendation is to use dedicated hardware composed of all tools mentioned on an ad-hoc basis with a switch-span setup. It is also commonly known as port mirroring, so that an exact copy of the traffic that flows can be fed for investigation. To suit the Sri Lankan context, a stripped-down version of the MITRE ATT&CK + SHIELD Active Defense Matrix will be used to choose the applied malicious datasets and for designing the security playbooks.