MITRE ATTACK FRAMEWORK ADOPTION AS A SIEM RULE BASE USING MACHINE LEARNING APPROACH

P.W.R.S Weeraman

(Reg. No: MS19801582)

M.Sc. in IT

Specialized in Cyber Security

Supervisor: Dr.Lakmal Rupasinghe

December 2021

Department of Computing

Faculty of Computing

Sri Lanka Institute of Information Technology

Table of Contents

List of Figures

List of Tables

Declaration

I, Rasika Senarath Weeraman, declare that this submission contents are my own works, and it does not contain any direct material which previously published or written by another author or material, which to substantial extent, has been accepted for the award of any other academic qualification of an academic or other institute of higher studies excluding where acknowledgements are made in the texts.

Certified by

Signature: ………………………………

Date: ………………………………

Name of Supervisor: Dr. Lakmal Rupasinghe

Signature: …………………………………….

Date: …………………………………….

Acknowledgement

First and foremost, heartily profound gratitude and appreciation to supervisor Dr Lakmal Ranasinghe for his valuable supervision. His guidance, supervision and knowledge sharing gave more enthusiastic support in successfully finish this Research. Thanks for his dedication, experience, knowledge, simplicity, work ethic, and exemplary ability to balance work and life. It has been an honor to work with him. I will always be thankful to him for the valuable time he contributed to supervising research progress.

I want to thank Mr.Haran Mamankara, Lead-Cyber Defense Engineer, Dialog Axiata (Pvt) Ltd, for his knowledge sharing about the threat hunting methods and ATTACK framework implementation large scale Security operation center. Furthermore, I want to be thankful for working place team members who supported completing this task on time by reducing workload d and cooperation during the absence.

Further, I am grateful to others who have supported and encouraged me to complete my progress in a short period. Finally, thanks to my wife, parent and family members who have supported, tolerated, and encouraged to continue my studies through their kindness and cooperation during a hard time.

Abstract

Digital transformation is the standard business strategy approach in most Organizations. Every person is looking for digital solutions to aid their routine works. Every Organization looking possibility move to physical office concept for virtual office concept. Even homemakers and bargain hunters also expect to move online shopping with doorstep delivery solutions with this COVID-19 pandemic. Every business needs to adopt IT functions for their business process to ensure business stability or increase their revenue. Most large-scale enterprises have a dedicated IT strategy approach to align with their business strategy. They follow best IT security practices such as SIEM, security operation centers (SOC), annual IT compliance review, IT audit and best security devices in the market. However, most of the business do IT system adoption without a preplanned process. They do not follow any best it practices in term of IT security.

Further, they do not have a proper IT strategy that aligns with business objectives. Most small and medium scale business with minimum IT infrastructures and IT operations. The absence of a proper IT security approach in the business may introduce new IT risk to their information and business.

This Research makes experimental approach to adopt cyber threat intelligence to SIEM detection base using adversary tactic, technique, procedure (TTP) and machine learning (ML) instead of signature-based detection methods. TTP change is relatively more challenging than IP address or file hash change. This research concern uses TTP-based Security information and event management systems (SIEM) solution using open-source software and MITRE ATT&CK community framework. Further, this Research aims to reduce operating expenses and capital expenses using a community-based framework and opensource software.

Keywords

COVID-19, MITRE ATT&CK, Framework, open-source, cybersecurity, network security, security, management, computer security, SIEM, Log analysis, SOC, incident management, cyber forensics, Machine Learning, Big data, SMB, SONAR, SNORT, Threat intelligent, CTI, ML, SOC