INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

PowerShell Base Incident Response Framework (IRF)

A Dissertation by

Mr. Kasun Priyadarshana

Supervised by

Mr. Sithira Hewaarachchi

Submitted in partial fulfilment of the requirements for the MSc in Cyber Security and Forensics at the University of Westminster.

July 2023

ABSTRACT

Analyzing security incidents is a critical phase within the incident response process, wherein the required measures to alleviate the incident are determined. This undertaking is both time-intensive and necessitates professional analysts equipped with specialized tools. Conventional approaches rely on many potentially costly and intricate mechanisms, often resulting in errors and overlooked evidence that impedes a comprehensive understanding and effective response to the incident.

To address this problem, the author proposes a PowerShell-based incident response framework that helps security analysts to identify early signs and indicators of security incidents more efficiently. This framework reduces the time and resources required for incident analysis and helps to enhance the process's overall efficiency by enabling automatic event correlations to the incident analysis.

During the evaluation, the solution underwent testing with the latest malware samples to assess its capability to capture IOCs accurately. Furthermore, the author of this project shared the framework with industry experts for their evaluation. The quantitative review revealed significant improvements, including a 17% increase in the accuracy of security incident analysis, a 28% improvement in the efficiency of security incident analysis, and a 28% enhancement in user-friendliness. Consequently, based on the overall summary, it is evident that the proposed framework successfully improves and enhances the security incident analysis process.

Keywords: Malware analysis, Indicator of compromises, MITRE ATT&CK techniques, Forensics investigations, Anomaly detection, TTPS, Incident Response Framework, Endpoint Detect and Response

Subject Descriptors: Security and privacy → Intrusion/anomaly detection and malware mitigation →Malware and its mitigation