INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration With

UNIVERSITY OF WESTMINSTER

Framework to Identify Potential Insider Threats in SME Organizations

Dissertation by

Mr. Masevge Merin Deshan Fernando
UoW Student ID: w1911198
IIT Student ID: 20211571

Supervised by

Mr. Sithira Hewaarachchi

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

July 2023

Abstract

This research report addresses the critical issue of insider threat detection in small and medium-sized enterprises (SMEs) by introducing a comprehensive framework specifically designed for this context. The problem at hand is the increasing frequency and sophistication of insider attacks, which can lead to significant financial and reputational losses for SMEs. The absence of dedicated insider threat detection systems tailored to SMEs exacerbates their vulnerability to such attacks.

To tackle this challenge, the researchers developed a systematic framework for detecting insider threats within SMEs. The framework consists of four crucial stages: log collection, normalization, correlation, and detection. By analyzing log data generated from various sources within the organization, the framework identifies anomalous user behavior and potential indicators of malicious intent. Additionally, a risk scoring mechanism is implemented to prioritize incident response, enabling SMEs to allocate resources efficiently and respond promptly to the most critical threats.

The evaluation conducted by a team of cybersecurity expert evaluators demonstrated promising results. The framework proved effective in identifying insider threats and streamlining the incident response process. Notably, its simplicity and ease of implementation were particularly advantageous for SMEs, allowing them to bolster their cybersecurity defenses without significant investments in complex technologies. The framework's resource-friendliness addresses the unique challenges faced by SMEs, making it a valuable and practical solution to empower these businesses in safeguarding their sensitive data and mitigating insider threats effectively.

Keywords – Insider Threats, User Profiling, Risk Score, Log Collection, Normalization, Correlation, Indicator of Behavior, Malicious Users, Threats, Vulnerability.