INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER, UK

Unified Threat Regulation Framework for Sri Lankan Enterprise Organizations to mitigate threats.

A dissertation by

Mr Thebeyanthan Krishnamohan

Supervised by

Dr. Nimalaprakasan Skandhakumar

Submitted in partial fulfilment of the requirements for the Master of Science degree in Cyber Security & Forensics, Department of Computing, University of Westminster.

July 2022

Abstract

Every organization is challenged with newly emerging threats as the threat landscape is becoming larger and uncontrollable. Zero-day threats are considered more sophisticated as they can evade the traditional threat detection systems as they are more sophisticated, and their behavioural patterns keep on changing. So, to protect the organizations from this larger threat landscape, there is a need for an advanced threat detection framework adapted by the enterprise organizations to detect all sorts of threats which can be external as well as internal to an organization. There is a need to build a proper team with well-trained cybersecurity professionals to handle the technologies that would be implemented inside an organization. And there is a need for well-planned policies and procedures to be implemented in enterprise organizations to mitigate any threats. More concentration should be given to the Insider threats as the damage caused by the insider threats can be devastating compared to the external threats as the insider threats are mostly initiated by legitimate users who have all sorts of privileges in the internal systems of the organization. The organization should be ready at any time to respond to any kind of threat targeted towards them with all necessary cybersecurity controls for detection and response. The framework would explain the advanced cybersecurity solutions, human resources, and policies that need to be adapted by an enterprise organization, to protect themselves from both insider and external threats. Traditional cybersecurity solutions fail to detect and respond to the evolving insider and external threats as the traditional cybersecurity solutions are mostly signature-based, which detect the threats based on known signatures or patterns. And since there are many forms of external and internal threats, a single cybersecurity solution cannot stop these evading attacks. As a solution, there is a need for a multi-layered threat detection framework with multiple technologies and processes to be placed in the organization to detect and respond to any threats that are targeted at them.

This study of research put forward a framework for Sri Lankan enterprise organizations to protect themselves from both insider and external threats. The proposed framework can be customized according to the need and necessities of each organization as this framework considers multiple solutions and processes for multiple threats. An organization can independently opt to choose any process and the solutions proposed in this framework to protect themselves from both external and internal threats.

Keywords: Insider Threat, External Threat, Countermeasures, Process, Policies, Threat Detection, People, Technologies, Framework