Threat Intelligent Base Risk Observation Framework

S. A. D. K Lakshitha
(Reg. No.: MS20900786)
M.Sc. in IT
Specialized in Cyber Security

Supervisor : Dr Lakmal Rupashigha

Oct-2021

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

Abstract

Information systems of every organization are highly depending on information security framework. Day by day threat landscape is getting stronger and security technologies are developing accordingly. Always growing threat landscapes are adding organization an additional risk while organizations computer system risk factor is changing according to the end user traffic, running applications and operating system vulnerabilities. But enterprises always try to keep the risk factor in an acceptable level.

For risk assessment and security practices, efficient analysis of distributed Cyber Threat Intelligence (CTI) information is very important. Threat profiling is gaining popularity to enforce a proactive line of resistance. However, assessing a systems resiliency in the face of appropriate threats and identified in CTI shared data remains problematic, and it hold lack of semantics and background detail in textual representations of threat awareness.

This threat intelligence base risk observation framework (TIROF) is a software tool that observe and indicate risk level of the computer system using threat intelligence feed and National Vulnerability database. Further it will assess application risk factor separately using available Common Vulnerabilities and Exposure (CVE). Tool will be developed with rules and inferences, the system offers an automated method to examine about the cyber threats impacting the computer system by classifying threat significance, assessing threat probability, and identifying the affected and exposed properties.

Keywords – CTI-Cyber threat Intelligence Framework, TIROF – Threat Intelligence Risk Observation Framework, WOL – Web Ontology Language, CVE- Common Vulnerabilities and Exposure, vulnerabilities - possibility of being attacked or harmed

Acknowledgement

I would like to appreciate all the support received during the implementation of this project specially Dr. Lakmal rupashighe and all other academic staff for the provide guidance and advice.

Also, I'd want to express my gratitude to the survey participants who generously gave their time during the testing process. I'd like to express my gratitude to my loved ones for their unwavering support throughout the process, both in terms of keeping me calm and assisting me in putting the puzzle pieces together.

Table of Contents

List of Tables

List of Equations

1. Vulnerability Number of Vulnerabilities (Vu)
   i. $\text{Density (Vd)} = \frac{\text{Vu}}{\text{Size of Software}}$

2. Risk = Impact * Probability

List of Figures

List of Abbreviation

Abbreviation	Definition
CTI	Cyber Threat Intelligent
RM	Risk Management
RA	Risk Assessment
NRT	Near Real Time
WOL	Web Ontology Language
CVE	Common Vulnerabilities and Exposures
NVD	National Vulnerability Database
IOC	Indication of Compromise
VPN	Virtual Private Network
SWRL	Symantec web rule language
CVSS	The Common Vulnerability Scoring System
CFO	Chief Financial Officer
EDR	Endpoint Detection and Response
OSINT	Open-source intelligence
MISP	Organization Name
DRA	Dynamic Risk Assessment
DRM	Dynamic Risk Management
OS	Operating System
CRM	Customer Relationship Management
KLOC	Kilobyte of code
CE	Countermeasure Efficiency
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
C2	Command and Control
ML	Machine Learning
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol Secure
HTTPS	Hypertext Transfer Protocol
SNMP	Simple Network Management Protocol
DNS	Domain Name System
MD5	Massage Digest version 5
WMIC	Windows Management Instrumentation
SQL	Structured Query Language
RAM	Random Access Memory
CPU	Central Processing Unit