



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

2 Introduction..... 12

2.1 Background Context..... 12

2.2 Literature Review..... 14

 2.2.1 Risk Identification..... 15

 2.2.2 Notification for End User 17

2.3 Research Gap 18

2.4 Research Problem 21

3 Problem Statement 23

4 Research Objectives 26

4.1 Main Objective 26

4.2 Specific Objective..... 27

 4.2.1 Threat Intelligence base network traffic analysis 27

4.3 Risk Level Classification..... 28

4.4 Classification of Applications 29

 4.4.1 Critical applications..... 29

 4.4.2 Important applications..... 29

 4.4.3 Strategic applications..... 30

 4.4.4 Onsite support applications 30

 4.4.5 Support applications 30

4.5 Application Vulnerability Density..... 31

4.6 Countermeasure Efficiency 31

5 Research Questions 32

6 Literature Survey 34

7 Methodology 38

7.1 Traffic risk score calculator 41

7.2 Vulnerability risk score indicator 42

7.3 Risk Score calculator and indicator 44

7.4	Protocol level risk analysis	46
7.5	Application CVEs	51
8	Feasibility Study	53
8.1	Requirement Analysis	53
8.2	System Analysis	54
8.3	System Design	55
8.4	Identify User Cases	55
8.5	Communication Diagram	55
9	Testing and Implementation	56
9.1	System overview	56
9.2	Implementation	56
9.3	Implementation Techniques	57
9.4	Client Requirement	57
9.5	Hardware Requirement	57
9.6	Software Requirement	58
9.7	Testing Techniques	58
9.8	Test Cases	59
10	Result and Discussion	62
10.1	Research Findings	62
10.2	Results	63
10.3	User Characteristic	65
11	Work Plan and Time Schedule	71
12	Facilities Required	72
13	Feasibility	73
13.1	Time feasibility	73
13.2	Cost feasibility	73
13.3	Scope feasibility	73
13.4	Technical feasibility	74
14	Budget	75

15	Future Work.....	76
16	References.....	77
	Appendices	Error! Bookmark not defined.

List of Tables

Table 1 – Base Risk Score Rangers	42
Table 2 – Vulnerability risk score.....	44
Table 3 – Protocol stack.....	48
Table 4 – TCP/UDP Port on defined protocols.....	49
Table 5- Protocol risk indicator	50
Table 6 -Test Case 01.....	59
Table 7- Test Case 02.....	60
Table 8 – Test Case 03	60
Table 9 -Test Case 04.....	61
Table 10 – Test Case 05	61
Table 11 – Initial testing output	63
Table 12- Testing round two outputs	64
Table 13 – Risk Categorization.....	65
Table 14-Work from Home.....	65
Table 15-Work from Office	66
Table 16- Connected Through VPN	66
Table 17-Work From Home.....	67
Table 18-Work at Office	67
Table 19-Connection via VPN.....	67
Table 20-Direct Connect with internet.....	68
Table 21-Work from Home.....	68
Table 22-Work from Office	69
Table 23-Connect via VPN.....	69
Table 24-Direct Connected with Internet.....	69
Table 25-Risk Score Table.....	70
Table 26 - Work Plan and Time Schedules.....	71
Table 27-Time Feasibility.....	Error! Bookmark not defined.

List of Equations

1. Vulnerability Number of Vulnerabilities (Vu)

$$\text{Density (Vd)} = \frac{\text{i.}}{\text{Size of Software}}$$

2. Risk = Impact * Probability

List of Figures

Figure 1 17
Figure 2 38

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	Message Digest version 5
WMIC	Windows Management Instrumentation
SQL	Structured Query Language
RAM	Random Access Memory
CPU	Central Processing Unit