



# A Self Organized Threat Intelligence Architecture for Intrusion Detection Systems

by  
*DGCP Piyasena (168255E)*

A thesis submitted to University of Moratuwa in partial fulfilment of the requirements for  
the  
Master of Computer Science, *Specialized in Security Engineering*

Department of Computer Science & Engineering  
University of Moratuwa, Sri Lanka

*February 2020*



# A Self Organized Threat Intelligence Architecture for Intrusion Detection Systems

by  
*DGCP Piyasena (168255E)*

A thesis submitted to University of Moratuwa in partial fulfilment of the requirements for  
the  
Master of Computer Science, *Specialized in Security Engineering*

Department of Computer Science & Engineering  
University of Moratuwa, Sri Lanka

*February 2020*

# Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text. Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

---

DGCP Piyasena:

---

Date

Approved by:

---

Lt Col Dr Chandana D. Gamage  
Department of Computer Science and Engineering  
University of Moratuwa

---

Date

# Copyright Statement

I hereby grant the University of Moratuwa the right to archive and to make available my thesis or dissertation in whole or part in the University Libraries in all forms of media, subject to the provisions of the current copyright act of Sri Lanka. I retrain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

---

DGCP Piyasena

---

Date

I have supervised and accepted this thesis/dissertation for the award of the degree.

---

Lt Col Dr Chandana D. Gamage  
Department of Computer Science and Engineering  
University of Moratuwa

---

Date

# Abstract

An Intrusion Detection System (IDS) is a software application that monitor a corporate network or a computer system and flag activities which it construes to be malicious operations. The rapid and expansive growth of Internet has heightened concerns on how to protect both stored and transmitted digital information in an effective manner.

The reactive IDS will primarily detect intrusions and send out alerts. Defending the system is a secondary task, and its success depends on how early detection can occur when an intrusion is ongoing so that warnings can be sent in time. IPS, which is mainly proactive, will primarily detect vulnerabilities and take preventive measures in addition to providing the second stage functionality for an IDS but with limited knowledge and countermeasure capabilities.

As a solution to this problem, research has been conducted on an area called Automated Defense. The design of Automated Defense systems needs to be radically different from the IDS/IPS schemes as properties such as on-line real-time availability of all participants, use of threat intelligence schemes, availability of high computation power, etc have to be considered. Taking into consideration the context in which Threat Intelligence Architecture operates, where transaction value is very low, IDS/IPS systems need to be designed with a careful trade-off between reliability and cost of implementation.

The research presented in this thesis aims to develop a solution to the problem of providing the functionality of an IDS with an IPS capability that is highly responsive, adaptive and able to leverage the most up-to-date knowledge on dealing with threats. The main objective of the research is to combine an IDS with Threat Intelligence in a manner that can detect file creations and copying anomalies and provide the mechanisms to alert and initiate actions to take defensive measures to decrease the potential for damage from attackers.

The main objective of the research is to combine with Threat Intelligence to provide a mechanism to alert and initiate actions to take defensive measures to decrease the potential for damage.

# Acknowledgements

First of all I would like to thank my supervisor Dr. Chandana Gamage whose encouragement, guidance, support, and criticism from start to the very end, allowed me to understand the objectives and challenges of a master degree thesis. I would also like to thank Dr. Shehan Perera (Project Coordinator) for extensive advice, helpful feedback, and constant support.

Furthermore, my special thanks go to Dr. Shantha Fernando who provided an excellent, supporting, innovative, and inspiring environment in which it was a pleasure to create this thesis. Last but not its a pleasure to thank all my CiTes colleagues those who helped to make my thesis in a motion. I would also like to express my sincere gratitude to Mr Tim Crothers from Vice President Security Solutions at Target Minneapolis, Minnesota for the technical expertise provided.

Finally, words alone cannot express the thanks I owe Mr. DG Piyasena my father, Mrs. Pathma Swarnalatha my mother for all the encouragement extended.

# Abbreviations

IDS - Intrusion Detection Systems  
IPS - Intrusion Prevention Systems  
TI - Threat Intelligence  
CTI - Cyber Threat Intelligence  
SOC - Security Operation Center  
SIEM - Security information and event management  
openIOC - Open Indicators of Compromise  
STIX - Structured Threat Information Expression  
CybOX - Cyber Observable  
CybOX - Cyber Observable  
TAXII - Trusted Automated Exchange of Indicator Information  
IODEF - The Incident Object Description and Exchange Format  
TIE - Threat Intelligence Exchange  
TISP - Threat Intelligence Sharing Platform  
HTTP - Hypertext Transfer Protocol  
TPM - Trusted Platform Module  
VM - Virtual Machine  
VME - Virtual Machine Environment  
VMM - Virtual Machine Monitor  
NIDS - Network Based Intruder Detection Systems  
HIDS - Host Based Intruder Detection Systems  
PIDS - Physical Intruder Detection Systems  
OSSIM - Open Source Security Information Management

# Table of Contents

<b>Declaration</b>	<b>v</b>
<b>Copyright Statement</b>	<b>vi</b>
<b>Abstract</b>	<b>vii</b>
<b>Acknowledgements</b>	<b>viii</b>
<b>Abbreviations</b>	<b>ix</b>
<b>List of Tables</b>	<b>xiii</b>
<b>List of Figures</b>	<b>xiv</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Background . . . . .	1
1.2 Research Problem . . . . .	3
1.3 Objective . . . . .	5
1.4 Methodology . . . . .	6
1.5 Summary . . . . .	7
<b>2 Literature Review on Intrusion Detection Systems</b>	<b>9</b>
2.1 Introduction . . . . .	9
2.2 History and Evolution . . . . .	10
2.3 Architecture of the IDS . . . . .	11
2.4 Detection Approaches . . . . .	16
2.4.1 Misuse Detection . . . . .	17
2.4.2 Pattern Matching . . . . .	18



2.4.3	Rule-based Techniques . . . . .	18
2.4.4	State-based Techniques . . . . .	18
2.4.5	Anomaly Detection . . . . .	19
2.4.6	Use of Honeypots in Intruder Detection Systems . . . . .	20
2.5	Intrusion Prevention Systems (IPS) . . . . .	22
2.5.1	Rate-based IPS . . . . .	22
2.5.2	Disadvantages of Rate-based IPS . . . . .	22
2.5.3	Content-based Products . . . . .	22
2.6	Threat Intelligence . . . . .	24
2.6.1	Current Threat Intelligence Definition . . . . .	24
2.6.2	Types of Threat Intelligence . . . . .	25
2.6.3	Threat Intelligence Platform Capabilities . . . . .	25
2.6.4	Cyber Threat Intelligence Challenges . . . . .	27
2.6.5	Attack Vector Reconnaissance . . . . .	27
2.6.6	Attack Indicator Reconnaissance . . . . .	27
2.6.7	Cyber Threat Intelligence Opportunities . . . . .	28
2.7	Threat Sharing Platform . . . . .	28
2.8	Enabling Automated Responses from Policy . . . . .	29
2.8.1	Security Policies . . . . .	29
2.8.2	Engineering and Enforcing Security Policies . . . . .	30
2.9	Threat Hunting . . . . .	31
2.9.1	Intel Sources . . . . .	31
2.9.2	Importance of Detection . . . . .	32
2.10	Summary . . . . .	33
<b>3</b>	<b>Methodology for Cyber TI Support to Incident Handling</b>	<b>34</b>
3.1	Introduction . . . . .	34
3.2	Requirement 1: Sharing Mechanism of the Cyber-Trust Platform	35
3.3	Requirement 2: Expressibility, Flexibility, & Scalability of TI . .	36
3.4	Requirement 3. Information Used to Facilitate Automation . . .	37
3.5	Requirement 4. Streamlining of Hunting and Incident Response Process . . . . .	38
3.6	Summary . . . . .	40
<b>4</b>	<b>Solution Framework for Detection and Analysis</b>	<b>41</b>
4.1	Introduction . . . . .	41

4.2	Tactics Used for Threat Intelligence . . . . .	41
4.3	Automation of the Threat Intelligence . . . . .	43
4.4	Building Maturity Model . . . . .	46
4.5	Summary . . . . .	49
<b>5</b>	<b>Simulation of TI Automation and Event Sharing</b>	<b>50</b>
5.1	Introduction . . . . .	50
5.2	Threat Intelligence . . . . .	50
5.3	Threat Hunting . . . . .	58
5.4	Summary . . . . .	63
<b>6</b>	<b>Analysis of Automated Threat Intelligence Architecture</b>	<b>65</b>
6.1	Introduction . . . . .	65
6.2	Key Findings . . . . .	66
6.2.1	Key Finding 1: On TI Sharing Platforms . . . . .	66
6.2.2	Key Finding 2: On Sharing of Indicators of Compromise . . . . .	67
6.2.3	Key Finding 3 : On TI Platform Availability . . . . .	67
6.2.4	Key Finding 4 : On TI Platform Availability . . . . .	67
6.2.5	Key Finding 5 : On Lack of Automation . . . . .	68
6.3	Discussion of Results . . . . .	69
6.4	Summary . . . . .	72
<b>7</b>	<b>Conclusions</b>	<b>73</b>
7.1	Introduction . . . . .	73
7.2	Observation from CTI . . . . .	74
7.3	SOAR vs Proposed Framework . . . . .	75
7.4	Data Feed Providers . . . . .	76
7.5	Future Work . . . . .	76
7.6	Summary . . . . .	78
	<b>References</b>	<b>79</b>

# List of Tables

3.1	Threat Intelligence use cases . . . . .	39
4.1	Confidence matrix for measurable decision making . . . . .	42
4.2	Confidence-based actions . . . . .	42
5.1	Security Tools Intel Integration . . . . .	55

# List of Figures

2.1	Structure of Intrusion Detection System . . . . .	9
2.2	Architecture of IDS . . . . .	12
2.3	Architecture of IDS with sensor . . . . .	13
2.4	Console fault tollerance implementation . . . . .	14
2.5	Hierarchy management of IDS . . . . .	15
2.6	Three level sensor management scheme . . . . .	16
2.7	Structure of Misuse Detection . . . . .	17
2.8	State transition diagrams . . . . .	19
2.9	Anomaly detection model . . . . .	19
3.1	David Bianco - Pyramid of Pain . . . . .	37
4.1	Initializing Intel Feeds on devices . . . . .	43
4.2	Anecdotal data by using augmented default feeds . . . . .	44
4.3	Central collection of Intelligence . . . . .	46
4.4	Centralized Storage and Collection . . . . .	47
4.5	Centralize intelligence collection with automated action . . . . .	48
5.1	CRITs observable details . . . . .	51
5.2	CRITs Analysis Services . . . . .	52
5.3	Relationships in CRITs . . . . .	53
5.4	QRadar intel-based rules . . . . .	53
5.5	Flow of the the monitoring . . . . .	56
5.6	QRadar Context Menu . . . . .	58
5.7	MANTIS first run . . . . .	59
5.8	MANTIS import data . . . . .	60
5.9	MANTIS User Interface . . . . .	61
5.10	MANTIS Observables . . . . .	62

5.11 MANTIS Hashes . . . . .	63
5.12 MANTIS alert generation . . . . .	64
5.13 MANTIS with virus total . . . . .	64