

**Naif Arab University for Security Sciences**

**College of Computer and**

**Information Security**

**Department of Information Security**



# **A Cyber Threat Intelligence Approach for Improving Cybersecurity Defense Strategy**

**Presented by**

Yusuf Mohamud Jama

**Supervisor**

Dr. Meryem Ammi

Submitted in partial fulfillment of the requirement for the master's degree of  
Information Security

**Riyadh**

1441 - 2020



جامعة نايف العربية للعلوم الأمنية  
كلية أمن الحاسب والمعلومات  
قسم أمن المعلومات

# استخبارات التهديدات السيبرانية لتحسين استراتيجية دفاع الأمن السيبراني

إعداد

يوسف محمود جامع

إشراف

د. مريم عمي

رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير  
في أمن المعلومات

الرياض

1441 هـ - 2020 م

## **Table of Contents**

Abstract	I
Arabic Abstract	II
Dedications	III
Acknowledgment	IV
Statement of Original Authorship	V
Table of Contents	VI
List of Tables	IX
List of Figures	X
List of Abbreviations	XII
List of Appendices	XIII
<b>Chapter 1 Introduction</b>	
1.1 Overview	1
1.2 Objectives	2
1.3 Problem Statement	2
1.4 Proposed Solution	3
1.5 Contributions	4
1.6 Thesis Organization	4
Summary	5
<b>Chapter 2 Background and Literature Review</b>	
2.1 Cyber Threat Intelligence Overview	6
2.2 Cyber Threat Intelligence Definition	7
2.3 Sub-domains of Cyber Threat Intelligence	9
2.3.1 Strategic Cyber Threat Intelligence	10
2.3.2 Operational Cyber Threat Intelligence	10
2.3.3 Tactical Cyber Threat Intelligence	10

2.3.4 Technical Cyber Threat Intelligence	11
2.4 Sources of Cyber Threat Intelligence	12
2.4.1 Internal Sources	13
2.4.2 External Sources	14
2.5 Operationalizing CTI using ATT&CK Framework	15
2.6 Cyber Threat Intelligence Information Sharing and Standards	17
2.6.1 Information Sharing	17
2.6.2 Standards	18
2.7 Related Work for Cyber Threat Intelligence	19
Summary	21
<b>Chapter 3 Proposed Methodology</b>	
3.1 Proposed Approach Components	22
3.1.1 Cyber Threat Intelligence Platform: MISP Project	22
3.1.2 Intrusion Detection Systems: Suricata IDS/IPS and WAZUH HIDS	26
A. Suricata IDS/IPS	26
B. WAZUH HIDS	27
3.1.3 Elastic Stack SIEM	28
3.2 Cyber Security Defense Strategy Proposed Approach Architecture	30
3.3 Implementation and Testing Environment of the Proposed Approach	32
3.3.1 Data Collection (Data Aggregation)	32
3.3.2 Data Preprocessing (Normalization and Enrichment)	36
3.3.2.1 Feedback and Addition	36
3.3.2.2 Collaborative Analysis	37
3.3.3 CTI Integration with SOC tools: Suricata Network IDS/IPS and Wazuh HIDS	40
3.3.4 Real Time Monitoring with Elastic Stack SIEM	43
Summary	47

## **Chapter 4. Results and Discussion**

4.1 Reviewing Threat Landscape to Identify our Adversaries	48
4.2 Threat Hunting using IoCs	49
4.2.1 Detecting MuddyWater Threat Actor	49
4.2.2 Detecting Emerging Cyberattacks	51
4.3 Threat Hunting using TTPs of MuddyWater Threat Actor	56
4.4 Results Discussions	60
Summary	64

## **Chapter 5. Conclusion and Future Work**

5.1 Conclusion	65
5.2 Future Work	67
References	70

## List of Tables

4.1	Summarize of the categories of Event ID 398	50
4.2	Techniques of MuddyWater Threat Actor	56
4.3	The Input Rules of the Detection	62
4.4	Summary of Result Discussion	64

## List of Figures

2.1	CTI Process Lifecycle [57]	9
2.2	Source of Threat Intelligence do you rely on? [12]	13
2.3	The Pyramid of Pain [46]	15
2.4	MITRE ATT&CK Navigator [48]	16
2.5	STIX Domain with Relationships Objects	19
3.1	MISP Project Overview	23
3.2	MISP Data Model	24
3.3	Overall Process of Collecting and Analyzing OSINT using MISP	25
3.4	Suricata IDS/IPS Architecture	27
3.5	Wazuh Feature [30]	27
3.6	Wazuh Architecture Single Host [30]	28
3.7	Elastic Stack Architecture	28
3.8	Traditional Cybersecurity Defense Approach	30
3.9	Proposed Approach Architecture	32
3.10	Hub-Spoke Model	33
3.11	MISP Login	34
3.12	Feeds	35
3.13	Events	35
3.14	Sighting	36
3.15	Cyber Kill Chain [38]	37
3.16	Iranian APT & TEMP Group [40]	38
3.17	Organizational Heat Map	39
3.18	MISP Export Suricata Rules	40
3.19	Updating Suricata Rules	41
3.20	Wazuh Agent	42
3.21	Registered Agents	46
3.22	Wazuh HIDS Logs	46

3.23	Suricata IDS/IPS Logs	47
4.1	OSINT-MuddyWater expands Operation	49
4.2	Suricata Alert	50
4.3	The Triggered Alert	51
4.4	CVE2020-0796 Mitigation Alert	52
4.5	Alert Covid-19 Cyber Threat	53
4.6	Detailed Information about the Alert	54
4.7	VirusTotal Detection of this Domain	54
4.8	Suricata Alerts Summary	55
4.9	Atomic Test T1033 (System Owner/User Discovery)	57
4.10	Alert T1033 (System Owner/User Discovery)	57
4.11	Detailed Incident T1033	58
4.12	Wazuh HIDS TTPs Alert Summary	59
4.13	Summary of all Alerts	61
4.14	Proposed Approach Detection Heat Map	63
5.1	Proposed Future Work ATIC	68