SECURITY MONITORING TOOL SYSTEM USING THREAT INTELLIGENCE vs THREAT HUNTING

WAN IKBAL ISMAT BIN WAN KAMAL

OPEN UNIVERSITY MALAYSIA

2021

SECURITY MONITORING TOOL SYSTEM USING THREAT INTELLIGENCE vs THREAT HUNTING

WAN IKBAL ISMAT BIN WAN KAMAL

A Final Year Project submitted in fulfilment of the requirements

for the degree of

Bachelor of Information Technology in Network Computing with Honours (BITN)

Open University Malaysia

2021

SECURITY MONITORING TOOL SYSTEM USING THREAT INTELLIGENCE vs THREAT HUNTING

ABSTRACT

This project is about developing a Security Monitoring Tool System using Graylog SIEM (Security Information Event Management) with a combination of Threat Intelligence and an expected outcome for Threat Hunting results. This is built in accordance to specific ruleset been made for threat hunting purposes with an automation of logs from Windows endpoint host and Network activity. A datasets of Threat Intelligence enrichment will be integrated to the provided platform which is Graylog. Main objective is to ensure Security Analyst or Network Analyst to have a look at any suspicious behavior of attacks by hackers and act to it in a timely manner. Most organizations normally ingesting network and endpoint logs to the SIEM tools and integrating with some commercial tools to detect or trigger anomalies and directly send them notifications via email or 3rd party channel like Slack channel. Bear in mind that, the commercial tools is highly expensive and not really cost effective, however with this development definitely will help them to deploy the same approach with very limited budget or could be at zero cost for small medium enterprise but for big enterprise it will only cost \$1500 at fixed price which considered as cheaper than the other tools. There are many developments out there whereby they are using wellknown open-source IDS like Suricata and open source SIEM like elastic stack comprises of Elasticsearch, Kibana and Logstash. However, in this development, Graylog been used with the usage of Elasticsearch and MongoDB as a database server and to store, search and analyze huge volumes of data ingested. Generally, the Graylog is introduced as a powerful logging tool with a simple user-friendly interface visualized with Grafana as well as offering minimal effort to configure with very low maintenance. Due to that, creating a ruleset for Threat Hunting and Threat Intelligence enrichment, it will be much easier to configure and straight forward to compare with other competitors in the market.

Keywords: Graylog, Threat Intelligence, Threat Hunting, Centralized Log Solution, Security Monitoring Tool

ACKNOWLEDGEMENT

I would like to take this opportunity to express my gratitude and appreciation to my supervisor, Puan Zarinah Mohammed Mohaideen for her guidance, patience of guiding me whilst identified as covid-19 patient and invaluable advice throughout this project.

I also would like to express my appreciation to my family and friends for their endless support whenever I face problems. Without the mentioned parties, it is impossible for me to complete this project report successfully.

THANK YOU.

WAN IKBAL ISMAT BIN WAN KAMAL 30 AUGUST, 2021

TABLE OF CONTENTS

TITLE PAGE			
DECLARATIO	DN		ii
ABSTRACT			iii
ACKNOWLEI	DGEM	ENTS	iv
TABLE OF CO	ONTE	NTS	V
LIST OF TAB	LES		vi
LIST OF FIGU	JRES		vii-vii
LIST OF ABB	REVIA	ATIONS	ix
CHAPTER 1	INT	RODUCTION	
	1.1	Background to the Study	1
	1.2	Problem Statement	2
	1.3	Objectives of the Study	2
	1.4	Scope and Limitation	3
	1.5	Implementation Plan	5
CHAPTER 2	LIT	ERATURE REVIEW	
	2.1	Security Monitoring Tool Review	6
	2.2	Threat Intelligence Review	12
	2.3	Threat Hunting Review	15
	2.4	Intrusion Detection in General	17
	2.5	Conclusion of Review	18
СНАРТЕР 3	SVS	TEM ANALVSIS AND DESIGN	
CHAI IEK J	31	Fassibility Studies	10
	3.1	System Dequirement	19
	2.2	System Development Method	22
	3.5 3.4	System Development Method System Design Attack Based	20 26
CHAPTER 4	SYST	EM IMPLEMENTATION AND TESTING	. –
	4.1	System Guides / Manual	27
	4.2	Installation Manual	28
	4.3	Testing Plan, Test Output	45
CHAPTER 5	SUM	MARY AND CONCLUSION	
	5.1	Summary of main findings	59
	5.2	Discussion and Implications	56
	5.3	Limitations of the Study	60
	5.4	Future Development	60
REFERENCES	S		61

LIST OF TABLES

TABLE NO	TITLE	PAGE
1.0	User & Administrator Scope for System Development	3

LIST OF FIGURES

FIGURE	TITLE	PAGE
NO		
1	Implementation Pre-Planning	5
2	Development & Execution Plan	5
3	Pilot-Testing Plan	5
4	Splunk Log Monitoring Tool	7
5	Price Differences between Splunk Enterprise and Graylog Small Business	8
6	SIEM Elastic Log Monitoring Tool	8
7	Price Differences between Elastic Standard and Graylog Small Business	9
8	SIEMonster Log Monitoring Tool	10
9	Price Differences between SIEMonster and Graylog Small Business	11
10	EPS Analysis and Log Volume Result	12
11	Common Types of IOC (Indicator of Compromise) in Cyber Threat Intelligence	13
12	Comparison of Threat Intelligence feature between Four Competitors	14
13	An example of Threat Hunting Hypothesis	15
14	Comparison of Threat Hunting Feature between Four Competitors	16
15	System Requirements List to Develop the Platform	22
16	An overview of Network Architecture Diagram for the Platform	23
17	Basic Overview Traffic Communication between Devices	24
18	System Design Attack Based	26
19	Graylog Virtual Machine Instance	28
20	Graylog Instance Running with Ubuntu 20.04 LT	28

21	Zeek Virtual Machine Instance	29
22	Zeek Instance Running with Ubuntu 18.04.5 LTS	29
23	From Windows NXLog	46
24	From Zeek IDS Filebeat	47
25	Event Streams Configuration for Windows and Zeek	48
26	Event Test Rules for Windows Logs	49
27	Event Test Rules for Zeek IDS	49
28	Aggregated Events Dummy-PC from Windows NXLog	50
29	Aggregated Events Zeek IDS from Filebeat	50
30	Threat Intelligence Features	51
31	Threat Intelligence Content Packs	51
32	Message Processors Configuration for Threat Intelligence	52
33	Threat Intelligence Rule Feature	53
34	True Positive Event	54
35	False Positive Event	54
36	Threat Hunting Rule Feature	55
37	True Positive Event	55
38	Slack App Directory Configuration	56
39	Graylog Alert & Events Feature	56
40	Threat Intelligence Alert	57
41	Threat Hunting Alert	58

LIST OF ABBREVIATIONS

ABBREVIATIONS	DESCRIPTIONS
SIEM	Security Information Event Management
SOC	Security Operation Centre
IR	Incident Response
EPS	Events Per Seconds
СТІ	Cyber Threat Intelligence
ΙΟϹ	Indicator of Compromise
ΙΟΑ	Indicator of Attacks
C2	Command & Control
GB	Gigabyte
MB	Megabyte
IDS	Intrusion Detection System
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
CRM	Customer Relationship Management
LTS	Long Term Support
OPENSSH	OpenBSD Secure Shell
TOR	The Onion Router
UDP	User Datagram Protocol

CHAPTER 1

INTRODUCTION

1.1 Background to the study

Cybercriminals are getting sophisticated nowadays in terms of developing new techniques, tools and tactics in cyber hacking world. With several of tactics that is commonly known as Phishing attacks or also known as one of the techniques called Social Engineering to deliver malicious script embedded in the link and executing malware or virus or retrieving user's credentials like usernames and passwords, end users are prone to this attack every day. Further to this, one way to spot if users are impacted with these kinds of attacks, the introduction of Graylog Log Monitoring Tool and data enrichment of Threat Intelligence and Threat Hunting is useful so then the security analyst or network analyst can be fully aware of what is actually happening within their network perimeters.

Generally, the Threat Intelligence is known as threat information that is known historically. Threat intelligence data are known as artifacts generally retrieving an IP address, domains, registry key, mutex, hashes of executable files and several others. If found, all of this relevant information is called as an IOC's known as (Indicator of Compromise). As for Threat Hunting, it is an IOA's (Indicator of Attacks) that is not known historically and meant to know possible suspicious attacks residing in the host machine.

In this study of developing Graylog operated with Ubuntu operating system, there are two approaches that will be developed. The first one is Threat Intelligence enrichment powered by third parties that will be enabled and the logs of host endpoint network activities will be logged and to be received by the Graylog via Zeek Intrusion Detection System. A span network also known as port mirroring is connected from Cisco ASA firewall to Zeek Intrusion Detection System operated with Ubuntu operating system. Secondly, for Threat Hunting, a log shipper of NXLog will be installed and configured on Windows 7 machine and push the log to the Graylog directly. Once all of these enabled, the threat hunting and threat intelligence rules are created to ensure an analyst to be notified and the analyst can act or respond to this threat accordingly.

1.2 Problem Statement

The problem statement as follows:

- The evasive techniques like fileless malware attack to bypass Cyber Security tools or operating system security levels is increasing every day by hackers and therefore Threat Hunting is introduced to reduce the risk.
- A database signature from Anti-Virus or any other security tools is just a database of the sign of attacks which is known from the past and cannot detect a behaviour-based attacks on the present day by hackers. In order to overcome and reduce this risk, a Threat Intelligence is one of the ways to act as an added value tool.

1.3 Objectives of the study

Objectives of this project are:

- To configure and deploy Graylog logging tool and Zeek Intrusion Detection System for Threat Intelligence and Threat Hunting method.
- To create and enable Threat Intelligence enrichment and Threat Hunting rules, and to receive alerts from it.
- To enable the mechanism to push logs from Zeek Intrusion Detection System and Windows operating system to Graylog.
- To configure network threat types of Zeek Intrusion Detection System and NXlog from Windows operating system.
- To monitor traffic flow and windows logs, and detect suspicious activities.

Generally, an intrusion may happen externally and internally and this could resulting to data breaches of sensitive information, modifying of vital system or disrupting vital services that may impact financially to organization.

The most highly dangerous intrusion is actually within internal networking system. This commonly called as insider threats. The insider threats comprise of employees, partners, vendors, friends or customers. External intrusion is an intrusion coming outside of the in-house networking system whereby most of the attacks are coming from the internet. In fact, for this deployment, it gives value to companies of using Graylog logging tools alongside NXLog shipper and Zeek Intrusion Detection System as an added value tool.

1.4 Scope and Limitation

Graylog logging tool and Zeek Intrusion Detection System comprise of lot of scopes. In this study of configuring and deploying of these two for Threat Intelligence and Threat Hunting purposes, the scope is

- Network traffic of endpoint host activities.
- User's activities on Windows Operating System.

1.4.1 System Scope

At least two users involved in using the said system of Graylog Monitoring Tool:

- i) Administrator the administrator who have highest privilege over the system.
- ii) User normal user created by Administrator who has read, edit and write access to perform any configuration or fine tuning within the said system.

Graylog	Zeek IDS	Filebeat	NXLog	VMWare ESXi
OS: Ubuntu	OS: Ubuntu	OS: Ubuntu	OS: Windows 7	OS: VMKernel
Administrator – The	root – The root	root – The root		
administrator who	access running on	access running on		
administered the	Ubuntu which can	Ubuntu which can		
configuration with full	read,write,read+write	read,write,read+write		
privilege access	with full privilege	with full privilege		
	access configuring	access configuring		
	Zeek IDS	Filebeat		
	configuration for	configuration for		
	Graylog integration	Zeek IDS integration		
User – The member who	No other user created	No other user created	No other user	No other user created
can read and edit several	for this development	for this development	created for this	for this development
key functions with least			development	
privilege access				

1.4.2 User Scope

Table 1: User & Administrator Scope for System Development

1.4.3 Limitation

The major part of this development is definitely the Graylog logging tool and since we have created another user with least privilege access who can read, write and edit several key functions, it is sufficient for the user to look at necessary functions relevant to the requirements as a Security or Network Analyst.

However, the only issue is that since we are using free trial access for 30 days which given more log storage size, in the end of trial license ended, it will move back to default state which is a community edition. If this is the case, the log storage size will be decreased to smaller size and when the log reaches the limit, the old log data will be overwritten.

Additionally, for Threat Intelligence integration part, Graylog version 4.1 only provides two sources which is different than the previous version of Graylog 3.x which offers three of them. In order to create an additional custom Threat Intelligence data enrichment, it will be quite time consuming and therefore it will be not implemented during this development phase.

1.5 Implementation Plan

Gantt chart as shown below:

	40.0224.0	171000	1021	8FR 2021	MAY 2021 JUM 2028
			1 0009	5 12 19 362	1017-34517 14-51-58
Graylog&Zeek Project		98%			
* Pre-planning		13.091			
Identifying requirements for selected tools of Graylog & Zeek.	Warr Robel	100%	1	() () () () () () () () () ()	Wan Isbal
Identifying architecture model for Grayloy & Zeek	Wan likbal	10095	1	6	Warstkbal
Identifying deployment method for Graylog, Filebeat Zeek & NKLog,	Wan Ikbal	10096			Wars1Rbal:
Identifying on how to ingest logs from Allebeat Zeek & NXLog to Graylog	Warr Nobal	10.095	1	6 - 6	Wars Ikbal
Identifying on how to create Threat Hunting rules in Graylog.	Wan Ikbal	10.0%	1		Warn Ukbal
Identifying on how to create rule and aggregate and correlate logs with Threat Intelligence lookup data.	Wan Ikbal	10.0%	1	2 - 9	Wanshipel
Identifying on how to setup SPAN network from VMWare east to Zeek interface for traffic mirroring.	Wan Robal	100%			WarniRbal
Identifying on how to set alert notifications to Stack channel.	Wan Hosal	10.0%	1	1 - N	Warnikbal
Identifying how to setup & configure filebeat on Zeek and NOLog Windows Operating System.	Wan Ikbal	10.095			Wars Robal

Figure 1: Implementation Pre-Planning

	- Andrews	Digue	*R#1834	And Dates	08104	407 1824	(8H109)	m, dayy . Ald ad	Ň7
			8 8321	8 18 22 28 1	2 8 30	D 8.5 811	1 1421 281		-
Sta y/o g8.Zielet Prova ct		54%							
• Perphaning		100%							
* Development & Execution		99%			1.11	-	115		
Deployment of Libertia 20.04 LTS for Genylog Logging Tool.	War Rizal	100%					Was Size.		
Deployment of Uburitu 1804 5 175 for Zeek Intration Detection System.	Wen Rout	100%					Was Store		
Costiguing WWWere ESSI for Span Port Intertace.	Wat Edgel	100%					Was Not		
Installing Graviog version 41 in Ubenta 2004 LFS.	Wax Koal	100%					Wat Mail		
Installing Zauk Intrusion Dataptive System in Uberts 18 44.5 LTS.	West #doal	100%					Was Store		
Installing Flebust log shipper for Zeek IDS in Uberts 18,045 LTS.	Wax Schall	100%					Wat Note		
Installing KOLog log skipper for Windows OS.	Wax 800a1	10098					Web Ages		
Configure h6Grig shipper in Windows 05	Wey Koba (100%			1.1		Wax Adat		
Configure Risbesting shipper in Zeak DS.	Wate Bobal	10096					Was NO.		
Configure Zeak DS log types and enable the revolutes provided.	Was Moal	100%					WHENDER		
Ellable and start Filebeart & NX log log skipper	Wax lidsat	100%					W39.843m		
Create stream is Graying for Zeek IDS & Windows OS	Wein Adual	100%					Web \$255		
Check & search for lags of Zeek IDS & Wit down IDS via Stream.	Wat Rizel	100%					Was 80.8		
Create dashboard for Zeek IDS & Windows OS is Garying	War Rosal	100%				-	Wah Adlar		
Elsente: Thread Intelligence: Rolex pipeline of TCH exit restee.	Wen Roul	100%					Was Store		
Create Threat Hanning Rules	Wat Edgel		Wen 3cb	a: 1					
Eastle Treat Intelligence pluging in Graylog	Wat tidoal	100%				1	Wat Mail		
herhil content pucks in Graylog.	Was Idasi	100%					Was Stol		
Chiefe Stack Channel webbook for slerf.	Was Schol							Novitte)	
Crastla Evant notifilar in Bitstog.	Wax 800a1							Was risted.	
Craste start opecition for Zeak IDS & Windows OS Stream.	Wax Rosal							Wak Iktal	

Figure 2: Development & Execution Plan

¢ + Pilot testing	281	506	1 / - 1
Test and check the logr ingested from Windows OS and Zeek IDS.	Wan Hitsel	508	🕴 Wan Roal
Test and check stack channel and alert notifier.	Wen Notel		Wati Mibai
Test for Zeek IDS Filebeat and Windows MdLog after configured.	Wan Iktosi	50%	Wan Robal
Test for Threat Hunting rules & Threat Intelligence rules in Grapiog.	Wen Ribel	50%	🚦 Wayn Bebel
Check for Zeek ID5& N0Log enabled modules.	Warr Mosel	100%	Wan Sibat

Figure 3: Pilot-Testing Plan

CHAPTER 2

LITERATURE REVIEW

2.1 Security Monitoring Tool Review

In this chapter 2.1, we will be discussing and review about the platform about Security Monitoring Tool as known as SIEM (Security Information Event Management. Take note that, most enterprise are exposed to a growing number of security threats, the visibility knowing the inside out about network traffic and user activity is a mandatory. According to (Mitkovskiy, Ponomarev and Proletarskiy, 2019), to form a holistic view of any organization's IT security is necessary to process a large volumes of log information from multitude of systems with different kind of formats that normally difficult without an automated system. In order to solve this problem, a Security Information Event Management (SIEM) been designed to pinpoint to potential security breaches.

According to (David, Amanda, David Sutton, Andy, 2020), a SIEM is to be facilitated by using an automated tools is to analyze logs, system activity and network traffic with the objective for identification and investigation. Further to this, since there's so much of log data and system activity, it is impossible for one person to monitor it all in real time and therefore the only practical solution is an automation work.

Due to that, a SIEM or also known as Security Information Event Management is introduced with the purpose to have full visibility knowing what is happening in network environment. We live in an era with Information Technology comprise of computers, servers, mobile phones, routers, switches, firewalls, clouds and many others. Each one of this assets or technology has its own threats whereby hackers can take advantage to exploit it and achieving their objectives. Further to this, let's review on several platform that implementing the same concept as Graylog Monitoring Tool (Free License). For this review, it will enlighten us to understand the differences of features introduced from other platforms.

Robert Daniel Summer	Sull During Users and	Group Para	ing Dones Processes Trained	invest into See	an bestoore boor		Trinting				Co Damba
rocenses										1.0	Prest .
Lat Head	1000000 - 1000	** 	tan ini di manani ini dan secondari tan ini di manani ini dan secondari tan ini dan secondari	e Managara di Managara di Angereta Managara di Managara di Man Managara di Managara di Man	Annes Incomp				The second second	-	
							10				
maring Provide											
in the second	and i	Access April	Street, Square, Spin, 5				1 200	Vinal	manufactures been by	(pr. 5-10)	11
21 m 9 41 21	(and the state and party		The strength of the start of the	mount of annihi or	of the Westmanness of			The second	the second life second is a life of the second seco	200	0.015
	Anter and some local		And in case of the second seco	make and fail using the fill	CARLES AND DOUBLES			-	The late start in proceed at	1.00	August .
	(1007)0.0000.0000(1000)	-	President and the first sector of the	Sector 10 (1997)	(1000)-001010000000000000000000000000000	196 - 19 -		-	for the cost of concept of	1000	100
all the Promotion											
	141	Summi farer	Sect. Proved Street 1		24 ji					Special Distance and	and Advert
10 - C (1.0.0)	CREW AND THE PARTY		A Lot days by Lington, and	7	an and " a statement of the	-				(m) 640.	1124
(((((((((((((((((((((((((((((((((((((((dotter according to a		1. (1. (1. (1. (1. (1. (1. (1. (1. (1. (an order the partners.					****	1000
	1.000 - 222 - 000 1000		Service tone surface the	Distance from the	Contraction and the second secon		100	MARK PLAN DA	and the property of the proper	-	Read of
1212-00-14 (1-10,14)	California and Section	14 million	A Designer frame (add/9878) Antonio designation in the last United and	-1. mage of 1.0m (14	COMM Research Residence (Section	()(===)				aler.	
water to do not	Limits and read here.		A rest operation of the local sectors of		The Average Street Street and					-	-

Figure 4: Splunk Log Monitoring Tool

Splunk in general is very well-known log monitoring solutions that is established since year 2003. It has nearly 90% similarities in terms of features and functions if we compare with the Graylog Monitoring Tool where it can ingest logs, allowing to search and visualizing said logs. Splunk also working well in terms of scalability and flexibility giving to its users when it comes to resizing, reducing or increasing CPU resources, RAM size or Data Storage. From here, the abilities between Graylog and Splunk is pretty similar.

Generally, the obstacles of using Splunk is that the solution given is considered as the most expensive log monitoring tool in the world. The charges normally been charged as per GB of storage logged, per node (per server), or based on unlimited plan for the highest subscription. Splunk currently only offers cloud-based deployment solution for the paid subscription and the free license of Splunk Enterprise is on premise whilst Graylog Small Business provides on-premise. Shown below a table of pricing between Splunk Enterprise (Free License) and Graylog Small Business (Free License).

Platform	Price Per Year	Deployment Type	Log Volume
Splunk Enterprise	Free	On Premise	500 MB / Day Max
(Free License)			
Graylog Small Business	Free	On Premise	Up to 5GB / Day
(Free License)			

Figure 5: Price Differences between Splunk Enterprise and Graylog Small Business Retrieved at:

https://splunkpricing.com/, https://www.splunk.com/view/SP-CAAAAEQ & https://www.graylog.org/pricing

As we can see as shown at Figure 5 above, an identical in terms of pricing offering which given free and the same of deployment type. In fact, the offering of the log volume ingestion is slightly difference whereby Splunk Enterprise capped to only 500 MB and Graylog Small Business is giving more than that, but the solution given is similar to Graylog Small Business. Moreover, Graylog Small Business is given free of charge for the logs ingested with On-Premise deployment.

(and the second s				Chief and Chief and Long
Col Barriel			PIR. [] - Lost TE Rev. Rev.	The second second second second
a stated from				
add-Margersening.*	4,000 110	Deg 0, 2027 @ 2010/04/073 - Deg 0, 2027 @ 2010/04/027	8 AMU -	dit kauschast
C. State State Sector				100
HIGH BY TIDE I	100			
- Namah (1884		THE R. LEWIS CO., Name of Concession, or other	And in case of the local division of the loc	
AGAS		ا بي کا ان کا ان کا بي کا کا کا کا ان کا بي ب		100 Hill 100
(Joseph)	8.000	100 0.00 000 000 000 000 000 000	the second secon	
(mark)		Belleville and Minister		
	700.	build		
1. distances	I make strate to the local state	and another that a merid of the second of a second of a second of the second of the second of the second of the	and the second se	Printing and and a second second
Beel 100	I I make an environ	second reaction of the second reaction of the second reaction of the second sec	support support tortain tortaining interest / support	ar her tany shirt or the set in an
and the second se		partial asymptotic and rest for rest black on the terms in the bagineries, the of the terminate game when	tour inter or visco parts rationed this beginn	M. Could and a lowery house of
and the second		changes and servery and hypoth. In stand-party worky and the charactery and	continuous in stars going success, and , but	Land
		identaria rente sie henri (19der vien ana ac 80.00.00.00 diant ana b	could 10.79 class and bolices 1 revenues	er of the sector in the transfer there.
barra-	1. Ban A. MET A MILLION	In Brancost, and a second the Burliner's Brancost States, States, States, States, St.	contingentity of Front Intelligit," here our herberty	a manimum ferrer in hanne our the sectory
Print Print		menter bightererer partas bourts signatures and have based because were back	ning berti brite; tellening pepert men	al forfung paraget 180 att. 58 and
		sense terrer 10.00 (0.00 (0.00 (0.00))) and the same result of the balance of the	part, out of stars and consists and types	a st starstance course and the
and hand in this 1		class, and country, and target 10 classical models, and yound? To class and re-	anded however, to afree areas seen in age, but	Ind
Sec Taxa La Land		CONTINUE INFORMATION PROVIDED TO AN ADDRESS OF THE VERY METHOD AND A	Calling of the state sector provides a resolution	the first state of the state of
and the second second	1 No. 1, NO. 1 IN CO.	and memorys; by h. mit & in p. 21 and son density. I density system I proves, Ginese at	the second different manifest of be	and improved in \$7. Amounts
		menter function append beaution branch beaution beautions from become	million of Service Services Service Court S	strong schools, Log 142, 81 141
		This mean in the section of the sect	and had a large class design the same same of	Press tumpol
and street of the second second		itter ann meret entel anne e tiget pere matte ane bierte time pro in	any case income balance where provide and	the should be added to the second second second
	the second second second second	and sufficiently and a state of a state of the second state of the		
and statistics		Figure and a second brack interaction in the second in the second second second second second bracks in the second brack in the second brack in the second secon	the second to be a se	Company of the state of the state of the state
and the second second		tartes becards on the bit of the low to a time below to be added and a second second	and main times what your out the departs	Their context
NAME AND DESCRIPTION AND A		chine, peak size sheet hale, of plane, peak services, and because if all whates sizes	S. Intell Pro Chief, proid Long Sci. comb Aryan A. P.	Clare-pers.matro-passi #
where many harm have		slave and both south layers. W slave and subsystem blavas slave prosition	Very name income. Milance where prove has 170.	THE AD, FFT AGAINST SPICE AND ADDRESS OF THE

Figure 6: SIEM Elastic Log Monitoring Tool

Another competitor is based on ELK with the usage of (Elasticsearch, Logstash, Kibana) commonly known as SIEM Elastic Stack as shown at Figure 6 above, is established since year 2000.

Take note that, Graylog framework is also using Elasticsearch for its data processing as well but for MongoDB are for searching and storage purposes. Therefore, it has similarities to SIEM Elastic Stack.

Elastic is quite popular since the day it was introduced. It was first known as Elasticsearch and then changed its name to Elastic in 2015. During those years, it gives users to use Elasticsearch, Kibana and Logstash for free but the paid subscription based is quite limited. The reasons it was known as Elastic Stack because the solution is comprising of Elasticsearch, Kibana and Logstash whereby Elasticsearch is for open-source full-text search and analytics engine, Kibana is for data visualization and exploration tool and Logstash act as a server-side data processing pipeline that allows collecting data from variety of sources, transform and send to desired destination.

Nowadays, since most of users are using it for SIEM, it is known as SIEM Elastic and they are offering four types of subscriptions named as Standard, Gold, Platinum and Enterprise. As we know, the SIEM Elastic Standard (Free License) subscription is the lowest and we can compare it to Graylog Small Business (Free License) subscription accordingly as shown at Figure 7 below.

Platform		Price Per Year	Deployment Type	Log Volume
Elastic	Standard	Free / \$679	On Premise	60 GB Max
(Free/Non-Fr	ee License)			
Graylog Small Business		Free	On Premise	Up to 5GB / Day
(Free License	e			

Figure 7: Price Differences between Elastic Standard and Graylog Small Business Retrieved at:

https://cloud.elastic.co/pricing

https://www.graylog.org/pricing

If we compare the features offering between SIEM Elastic Standard and Graylog Small Business, the SIEM Elastic Standard offer more features than the Graylog Small Business, however, the only drawbacks by SIEM Elastic Standard are that even it can be used with Free under trial plan, the subscription only offer one node of server deployment and this will lead to missing events during log shipping. If the Standard plan with standard license, the user can scale and install multiple nodes of clustering servers while Graylog Small Business can be scale with additional clustering servers for free. Moreover, since that the objective using the Log Monitoring Tool is to let user to have looks and feels of UI/UX that facilitate them using the platform. In this case, Graylog Small Business is far easier to be used compare to SIEM Elastic Standard.



Figure 8: SIEMonster Log Monitoring Tool

The last competitor of the SIEM platform is named as SIEMonster. The SIEMonster is founded in the year of 2016 and if we compare with another competitors, the SIEMonster is quite new in the market.

The SIEMonster also using Elasticsearch for data analytics engine but it is known platform for integration flexibility whereby most of the components are integrated with multiple solutions for the purpose of Security Operation Centre, Incident Response, Threat Intelligence and several others. Additionally, the SIEMonster is yet to known worldwide because often enterprise is looking for more established SIEM solution. The pricing model for this SIEMonster is known not that cheap as well. It offers variety of solutions well integrated with another solution that makes it not that cheap nor expensive. It also gives user a free version named as Community Edition but it has limitations.

Platform	Price Per Year	Deployment Type	Log Volume
SIEMonster Community Edition	Free	On Premise	5K EPS* = 18GB / Day
(Free License)			
Graylog Small Business	Free	On Premise	Up to 5GB / Day
(Free License)			

Figure 9: Price Differences between SIEMonster and Graylog Small Business Retrieved at: https://siemonster.com/pricing/ & https://www.graylog.org/pricing

From the price comparison as shown above at Figure 9, clearly shown that the price is given free which is identical to Graylog Small Business (Free License), the only drawbacks is that SIEMonster (Free License) only given for on-premise deployment type with limitation of five thousand EPS (Events Per Seconds). This EPS is the event of logs that is sent from data sources that is ingested to the SIEM platform.

If the data sources are the busiest device like firewalls or routers, it is not enough to receives all of the logs due to the limitation given. If it hits more than five thousand events per seconds, the rest of the log of events will be discarded and will not be received. The rough estimation is pretty simple, the higher devices monitored, the higher of Events Per Seconds will be generated.

	Device	EPS	+ Count +		Device	EPS	+ Count +
1	Windows Servers - HIGH EPS (~50 eps)	50	20	17	Other Network Devices	5	40
2	Windows Servers - MED EPS (-3 eps)	3	30	18	Network Firewalls (Check Point - Internal)	10	3
3	Windows Servers - LOW EPS (~1 eps)	1	20	19	Network Finewallis (Check Point - DMZ)	50	6
4	Windows Workstations	1	300	20	Network Firewalls (Cisco - Internal)	10	6
5	Windows AD Servers	10	10	21	Network Firewalls (Clisco - DMZ)	30	6
6	Linux Servers	1	20	22	Network IPS/IDS	15	6
7	IBM AIX Unix Servers	2	5	23	Network VPN	2	2
8	HP-UX Unit: Servers	2	3	24	Network Antispam	10	5
9	Sun Solaris Unix Servers	2	3	25	Network Web Proxy	15	5
10	IBM Mainframe / Midrange	2	1	26	Other Security Devices	10	20
11	Network Routers	1	7	27	Web Servers (#S, Tomcat, Apache)	1	20
12	Network Switches	2	1	20	Database (MSSQL, Oracle, Sybase - # of		20
13	Network Switches (Netflow)	30	10	20	instances)		20
14	Network Wineless LAN	5	4	29	Email Servers (Exchange, Sandmail, etc)	2	8
15	Network Load balancers	5	6	30	AntiVirus Server (indicate number of AV	5	300
16	WAL Accelerator	14	3	-	clients)		
	1		12010	31	Other Applications (Email, DB, AV, etc)	5	20

Figure 10: EPS Analysis and Log Volume Result Retrieved at: http://www.aspiretss.com/tools

An example of calculation of Events Per Seconds (EPS) with numerous types of monitored devices with quantity as shown at Figure 10 above. Count means quantity of devices to be monitored and from the calculation shown above, the total of EPS is equivalent to five thousand Events Per Seconds or equivalent to 18 GB per day. In this case, if it exceeds more than that per day, the logs will be discarded. Graylog even it says up to 5GB per day, the events will still be stored and will not be discarded.

2.2 Threat Intelligence Review

In this chapter of 2.2, we will be discussing and reviewing features that related to Threat Intelligence for each of the platforms such as a Splunk Enterprise (Free License), Elastic Stack Standard (Free License), SIEMonster Community Edition (Free License) against Graylog Small Business (Free License). Also, we will be discussing what Threat Intelligence is all about.

Generally, Threat Intelligence in this context is called as Cyber Threat Intelligence where all information about the known or confirmed threats are collected from cyber world. Furthermore, this attacks information from the hackers are based on how they perform the attacks with the development phases comprise of tactics, techniques and tools in order to achieve their objective. According to (Kure and Islam, 2019), most of the attacks nowadays more sophisticated, multi-vectored and less predictable and critical infrastructure needs a new line of security defense to control these threats and reducing risks. A Cyber Threat Intelligence provides more evidence-based information about the threats particularly to prevent threats. An example attribution of Cyber Threat Intelligence that we can use in this study for better understanding as shown below at Figure 11:

IOC Type	Terms	General Type	
IP	ReceivedFromIP, Port/remoteIP	IP, Received, Destination Remote, Port	
Hash	Service Item, DLL, EXE Md5sum, FileItem	Service, dll, sha1 / md5	
	Md5sum		
Domain / URL	ReceivedFromDomain/URL,	Domain/URL, Received, Destination	
	Port/remoteDomain/URL	Remote, Port	
Registry	Service Item, DLL, EXE and any other malicious	WrittenFiles to Disk, Persistence	
	file extensions, File Item	Communication Destination Remote, Port	
File Type	Service Item, xls, docx and any other file	Drop to Disk, User Interaction or Execution	
	extensions, File Item	Required	

Figure 11: Common Types of IOC (Indicator of Compromise) in Cyber Threat Intelligence

According to (Liao, Xiaojing, Yuan, Kan, Wang, Xiaofeng, Li, Zhou, Xing, Luyi, Beyah and Raheem, 2016), with the use of these types of IOC's, it will enable organization to analyze the attack once it happens or counter during its execution. In fact, with such information of IOCs with overview of full context, it will help an organization to understand the security posture, detecting early signs of the threats and can continuously improving their security controls in place.

The table below describing the features offered in Threat Intelligence by Splunk Enterprise, Elastic Standard, SIEMonster Community Edition and Graylog Small Business;

Platform	Threat	Limitation
	Intelligence	
	Feature	
Splunk Enterprise	Ø	Free license allows only 500 MB data per day. No
(Free License)		Cloud deployment provided.
Elastic Standard	Ø	The greater events generated; the more node is
(Free License)		needed to provide High Availability to ensure zero
		downtime. Additional node requires paid license.
		Also, Elastic Threat Intelligence feature is complex
		to setup. No cloud deployment provided.
SIEMonster Community Edition	0	Free license allows only Events Per Seconds capped
(Free License)		to five thousand per day. No cloud deployment
		provided.
Graylog Small Business	Ø	Free license allows only logs data to be stored only
(Free License)		90 days. No cloud deployment provided.

Figure 12: Comparison of Threat Intelligence feature between Four Competitors

Retrieved from:

https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/TypesofSplunklicenses https://www.elastic.co/blog/establish-robust-threat-intelligence-with-elastic-security https://siemonster.com/products-overview/ https://www.graylog.org/pricing

To summarize this, we have to ensure that the features of using Log Monitoring Tool with the use of Threat Intelligence to be met. From the Figure 12 as shown above, we know that all provided Log Monitoring providers are offering Threat Intelligence feature. However, we need an unlimited log size with unlimited data sources to ensure no events is missing after log events is shipped. In this case, it is clearly shown that Graylog Small Business has more advantages.

2.3 Threat Hunting Review

In this chapter of 2.3, we will be discussing and reviewing features that related to Threat Hunting for each of the platforms such as a Splunk Enterprise (Free License), Elastic Stack Standard (Free License), SIEMonster Community Edition (Free License) against Graylog Small Business (Free License). Also, we will be discussing what threat hunting is all about.

According to (Lemos, 2018), they found out that, with the threat hunting approach, it is giving their organization a valuable exercise in order to improve their organization's security posture. In addition, instead of waiting for an incident to occur, the approach of using threat hunting proactively will definitely help in minimizing cyber risk in their organization's network perimeter.

Overall, threat hunting is not just passively waiting for an incident to occur, but it works with many ways. One of the ways is by leveraging an IOCs (Indicator of Compromise) and query or search the relevant artifacts within the tool provided. Another way is leveraging an IOA's (Indicator of Attacks) by researching a threat actor profiles in knowing their modus operandi by looking at their tactics, techniques and procedures.

An example of formulating a hypothesis before creating a threat hunting detection logic is shown below at Figure 13.

Hypothesis	Datasources	Common Network / Event	Common Application	
		Session	Protocol	
Threat actor using a	Zeek IDS, Firewall,	IP address, URL/Domain,	Domain (HTTP/DNS, SSL),	
C2 channel that uses	Netflow, NDR,	Port, Event ID	URL (HTTP), User Agent	
common protocol on a	Proxy, Windows		String (HTTP), Email	
common network port	Event		Address (SMTP)	

Figure 13: An example of Threat Hunting Hypothesis

From the hypothesis as shown above, we know the detection logic if we want to query a host machine running with Windows Operating System, for example it would be <ipaddress> or <domain> and <port80> or <port53> or <port 443> or port <25> or port<587>.

Herewith a feature in Threat Hunting by Splunk Enterprise, Elastic Standard, SIEMonster Community Edition and Graylog Small Business as shown below at Figure 14.

Platform	Threat Hunting Feature	Limitation
Splunk Enterprise		With only log ingested
(Free License)		maximum 500 MB per day.
		Threat Hunting will become
		useless due to missing events.
Elastic Standard	>	The greater events generated;
(Free License)		the more node is needed to
		provide High Availability to
		ensure zero downtime.
		Additional node requires paid
		license. Possible missing events
		might be occurred if the log
		ingested exceeds 60GB or no
		clustering servers in place.
SIEMonster Community	S	Log ingested only allows
Edition (Free License)		Events Per Seconds capped to
		five thousand per day. Threat
		Hunting will become useless
		due to missing events.
Graylog Small Business	>	Free license allows only logs
(Free License)		data to be stored only 90 days.

Figure 14: Comparison of Threat Hunting Feature between Four Competitors

As what is shown at Figure 14 shown above, under column limitation, each of the competitors has its own limitations. It seems like Graylog Small Business is giving more advantages to compare when the log can be received up to 5GB per day and log stored only 90 days. Even it only given 90 days, it is more than enough to handle any alert pertaining to threat hunting rules triggered and investigate the possible incident in a timely manner.

2.4 Intrusion Detection in General

Generally, an Intrusion Detection System (IDS) is a program or a software application embedded with a functionality to monitor a network for malicious or suspicious activities within internal network or external network. It is typically finding traffic that is deemed malicious depending on signature database that is stored in the program itself or anomaliesbased to detect unknown threat with the help of machine learning. Further to this, best practice to leverage its usage is to reported or collected to the SIEM (Security Information Event Management).

Typically, there are two types of IDS:

- Host Based Intrusion Detection System (HIDS)
 This is a system where it monitors key items or types residing within operating system. Most common operating systems are Microsoft Windows, Linux, Macintosh and Unix.
- Network Intrusion Detection System (NIDS)
 This is a system where it monitors and analyzed incoming network traffic within internal networks.

Additionally, between those two types of IDS, it has its own subset of IDS types. Typically known based on anomaly based and signature based.

- Anomalies: This anomaly based is intended to identify or detect to unknown threats within internal networks which could be related to worm, viruses, malware, botnet and other attacks.
- Signature: This signature-based detecting and identifying threats by looking for specific attack's types, patterns or bytes when the IDS monitoring is in place. However, this signature based is depending on the signature database that is saved and stored in the Zeek IDS for this system development project. It is therefore easy for signature-based IDS to detect known attacks but it would not be able to detect unknown threats with the Zeek IDS.

2.5 Conclusion of Review

This is to conclude the overall review from the perspective using the Graylog Monitoring Tool instead using other competitors in the market. The main objective is to defined and prioritized:

- a. Lowest cost solution
- b. Ability to have a Threat Intelligence function with ease without possible issues
- c. Ability to have a Threat Hunting function with ease without possible issues

From the reviewed results, it is clearly shown that Elastic Stack Standard (Free License) is the close competitor to Graylog Small Business (Free License) whereby they are offering more features other than Threat Intelligence and Threat Hunting. In fact, the Elastic Stack Standard is offering more log storage capped at 60GB maximum whilst the Graylog Small Business is offering up to 5GB per day.

As for SIEMonster Community Edition (Free License) and Splunk Enterprise (Free License) are only limited based on 5000 events per seconds generated and daily capped ingested log volume at 500 MB per day. This is too limited and low to compare with Elastic Stack Standard and Graylog Small Business. Due to this, this are the only drawbacks for these two platforms

Putting two competitors in place Elastic Stack Standard and Graylog Small Business, one of the biggest issues for Elastic Stack Standard are that, the complexity of integrating with Threat Intelligence is very complex to setup. It does not provide one click function for Threat Intelligence function. The only good feature from Elastic Stack Standard is the usage of Threat Hunting features, whilst the Graylog Small Business setup is pretty straightforward and simple under one single click for both features.

Overall, the Graylog Log Monitoring with the subscription of Small Business (Free License) has more advantages to compare with other competitors. Even the other competitors offering the same features for Threat Intelligence and Threat Hunting, the main limitations are the setup complexity, log retention, events per seconds generated and maximum log storage.

CHAPTER 3

SYSTEM ANALYSIS AND DESIGN

3.1 Feasibility Studies

There are about four feasibility study that were defined in this system development:

1. Technical

Technical wise, in this context, the Graylog Monitoring Tool platform are downloaded and installed from Graylog official website on Ubuntu Operating System. Once downloaded and installed, the platform can be accessed directly through web-based platform. Logging in as user is simple similar to any other web-based system that has username and password logging area.

As for Zeek IDS, this will be downloaded and installed on Ubuntu Operating System separately from Graylog Monitoring Tool. This Zeek IDS will act as a traffic receiver from Cisco ASA firewall. Typically, due to Zeek IDS instance will be running through virtual machine instance under VMWare, the Zeek IDS will need to enable promiscuous mode in order to receive traffic from Cisco firewall. It is indirectly act as a sniffing device.

The Cisco ASA Firewall itself, will need to enable the port mirroring which also known as switch port mirroring. In this stage, the Cisco ASA Firewall is physically connected to the VMWare ESXi and requires configuration virtually.

Lastly, the NXLog will be installed on the Windows Operating System in order to send logs to the Graylog Monitoring Tool platform.

2. Scope

This system is developed with the objective to use and leverage the method of Threat Intelligence and Threat Hunting with the suggested Log Monitoring Tool platform named as Graylog Log Monitoring Tool. Due to that, a pre-assessment is required in order to choose the best platform before go to on-production phase. However, in this development stage, the final stage only can be done until pilot-testing phase. Moreover, this development stage is developed in a smaller scale.

From here, this can be taken as a prototype for the said solution of Log Monitoring Tool with Threat Intelligence and Threat Hunting. Overall, from this development, it will only evolve the website development and other integrations between Graylog Log Monitoring, Zeek IDS and NXLog which are provided by respective entities. Further to this, we will need to perform installation, configuration and fine tuning by our own. Even though, the steps may look quite complex, but we do have a guideline provided by those three entities for reference purposes.

3. Economical

The development of Graylog Monitoring Tool for the purpose by leveraging Threat Intelligence and Threat Hunting are to gives insights and awareness to user or customer who might be looking for low cost-effective solutions focusing in SIEM. Whilst, in the end of the development stage, it can be considered as a pre-assessment stage before making final decision in selecting appropriate platform.

Prior developing the said platform, research had been conducted and by leveraging our own expertise in building up the said platform, the cost of development can be minimal. During this development stage, we use our own company VMWare ESXi hyper-virtualization as a hosted machine for Graylog Monitoring Tool and Zeek IDS, whilst the Windows Operating System acted as an endpoint windows machine to send the logs to the said platform.

Looking at the bigger picture, we can conclude that, to create and build this platform can be considered as zero cost. Only if, the user or customer do not have the VMWare ESXi hyper-virtualization to run a virtual machine, it still can be considered as low cost due to that the license of the said platform is given free.

4. Time

This project development is divided into three phases;

- Implementation Pre-Planning For research
- Development and Execution Plan For development and execution

• Pilot-Testing Plan – For testing of the said platform

Referring to the implementation pre-planning for research purposes, it took about at least 2 months to complete. This is to ensure that we have a solid understanding before developing the said platforms leveraging Threat Intelligence and Threat Hunting.

As for development and execution plan for the said platform, it took us about 3 months. During the development stages, we had encountered numerous types of non-functional services which includes system errors, application errors, downtime due to improper configuration and several other issues.

Moreover, it also requires us to complete the configuration phases that most of the consumed was coming from Graylog Monitoring Tool and Zeek IDS.

Ultimately, the final phase is the pilot-testing plan. From here, we have to ensure that the key functions are workable as intended and as designed. This includes the configuration, validation and testing for Threat Intelligence as well as Threat Hunting. All of these key function's coverage are coming from the Graylog Log Monitoring, Zeek IDS, NXLog and Slack Alert Channel for notification and it is therefore, requires close attention to these three entities.

3.2 System Requirement

Graylog	Zeek IDS	Filebeat	NXLog	VMWare ESXi
OS: Ubuntu 20.04 LTS	OS: Ubuntu	OS: Ubuntu	OS: Windows 7	OS: VMKernel
	18.04.5 LTS	18.04.5 LTS	Professional	
Store traffic and raw logs	Received traffics	Forward and	Forward and	
from host endpoint	from span port	centralizing log	centralizing log	
	from VMWare	data from Zeek	data from	
	ESXi	IDS to Graylog	Windows	

			machine to	
			Graylog	
Detect & improve system	Installed on	Installed on	Deployed on	
security	Ubuntu OS	Ubuntu OS	Windows 7	
	running with	running with	operating	
	Filebeat agent	Zeek IDS as	system with	
	and Zeek IDS	agent and	NXLog agent	Port mirroring sending
	provide real time	monitor log files	and monitor log	traffic to Zeek IDS
	traffic analysis	or location	files or location	instance
		specified	specified	
Regulatory compliance	Deep packet	Collect log	Collect	
	inspection for	events and	Windows log	
	each network	forwards them to	events and	
	logs	Graylog	forwards them	
Compliance with security	Network data	elasticsearch for	to Graylog	
policies	logging	indexing	elasticsearch for	
			indexing	

Figure 15: System Requirements List to Develop the Platform

Referring to the Figure 15 shown above, in this deployment method, about two instances are required for Zeek Intrusion Detection System and Graylog Logging Tool which is separately installed. The Graylog operated with Ubuntu 20.04 LTS and Zeek Intrusion Detection System altogether with Filebeat on the same machine operated with Ubuntu 18.04.5 LTS, and these two instances running in VMWare ESXi.

These virtual instances are deployed within internal networks. The Zeek Intrusion Detection System are installed with two network interfaces, one is for management with private IP address and another one is listening private IP address in order to receive span traffic from Cisco ASA firewall. Shown below Figure 16, a network diagram for basic understanding.



Figure 16: An overview of Network Architecture Diagram for the Platform

Based on Figure 16 above, this is basic overview to understand the objective of using the Zeek IDS and Graylog Logging Tool. The Zeek IDS are receiving data via mirror traffic from device known as Cisco ASA Firewall and it will route through router and switch.

Therefore, in this development phase, we relying on the system development of Zeek IDS and hardware dependent device known as VMWare ESXi, a hyper virtualization for virtual machines. The VMWare ESXi is capable allowing virtual machine to allow promiscuous mode to receive the mirror traffic from Cisco ASA Firewall. In computer networking, this mode is a mode for wired network interface controller that causes the controller to pass all traffic it receives to the destination network interface.

For this situation, the Zeek IDS is created under VMWare ESXi as a virtual machine and setup the promiscuous mode to receives the traffic from Cisco ASA Firewall. From the architecture shown above, the Cisco ASA Firewall is the heart of the internal network perimeter and the one to handles, receives and seeing every traffics internally and externally from all other devices within the internal networks.

To have a complete understanding how the devices play the roles based on the diagram shown above at Figure 16, have a look at the table shown below at Figure 17:

Device Name	Sent Traffic To	Received Traffic From
VM: Graylog Logging Tool	Not Sending Any	VM: Zeek IDS via Filebeat Log
		Shipper and Workstation PC
VMWare ESXi	Not Sending Any	
VM: Zeek IDS	VM: Graylog Logging Tool	Cisco ASA Firewall
Cisco ASA Firewall	VM: Zeek IDS via mirror traffic	Workstation PC, VM Database
		Server, VM File Server, VM CRM
		Server
Workstation PC	VM: Graylog Logging Tool	Not Sending Any

Figure 17: Basic Overview Traffic Communication between Devices

Referring to Figure 17 shown above, the device named VM:Graylog Logging Tool is not given privilege to send any traffics because it only acts as a SIEM and it is therefore only work as a standalone device to receive data logs that is sent from VM:Zeek IDS via Filebeat and Workstation PC.

The VMWare ESXi, is not sending any traffic but only receive port mirror of traffic that is coming from Cisco ASA Firewall and then VM: Zeek IDS will be sending the data logs to VM: Graylog Logging Tool.

As for Cisco ASA Firewall, its role is to send the traffic mirror to VM: Zeek IDS and receive traffic from other devices such as Workstation PC, VM Database Server, VM File Server and

VM CRM Server. This is because we know that Cisco ASA Firewall is the heart of the internal networks that can see every traffics inbound and outbound connections from other devices.

Lastly, the Workstation PC logs will be sent to VM: Graylog Logging Tool and not receiving traffic from other devices.

3.3 System Development Method

For this system development of Log Monitoring Tool with Threat Intelligence and Threat Hunting, we were using a complete Open-Source system like Ubuntu based on Debian, Elasticsearch, MongoDB, Zeek, Logstash through Filebeat.

Ubuntu is for operating system-based Debian. Elasticsearch is used to run with Graylog. MongoDB is to support Graylog for database. Zeek is for intrusion detection system and Filebeat with Logstash is to ship the Zeek IDS log events to Graylog.

All of these are installed separately and manually.

3.4 System Design Attack Based

Here is the system design architecture for this system development involving attacker. A close example whereby hacker could potentially perform an attack to Workstation-PC and the rest of the servers and compromise them with several ways.



Figure 18: System Design Attack Based

CHAPTER 4

SYSTEM IMPLEMENTATION AND TESTING

4.1 System Guides / Manual

After the implementation of pre-planning is clearly defined comprising of information collected from the research phase and expertise requirements especially in hands-on skills, in order to develop the said platform, we are ready to proceed for the next stage which is under development and execution phase.

The system development steps are structured with the following order:

- Ensure the Ubuntu operating system up and running. One for Graylog and another one for Zeek IDS.
- Download, install and configure Graylog.
- Download, install and configure Zeek IDS and Filebeat.
- Download and install NXLog agent in Workstation PC running with Windows 7
 Professional. Also, configure the types of system events required.
- Configure and fine-tuning data sources required from Zeek IDS and NXLog in Graylog.
- Enable and configure the feature for Threat Intelligence in Graylog.
- Create and test Threat Intelligence and Threat Hunting rules in Graylog.
- Create and test Slack Alert Channel for notifications.

4.2 Installation Manual

Firstly, we will make sure that the Ubuntu Operating System 20.04 LTS is installed for Graylog, refer Figure 20. Once installed in ESXi, we can see that the host is up and running, refer Figure 19.

finan Bover	Engline Engline		And
Gerrandus		- Rankar Colligiation	
- [] testing of		1200	1sDAa
Hed tarte			1.4
P (Detext)	1 (14) (40) (40) (1) 20 (40) (20) (20) (40) (40)	12 second	100.0
alle Aldanie Dalle	Induites and coming	- IN Smoth steple 1	And a second sec
100 times	194	- gerbar unti	14
inter (/ sal sea	1.0280904441	a start
		+ NE Divert	Antonia Tacher

Figure 19: Graylog Virtual Machine Instance

		📄 admin -	– graylog@gi	raylog: ~ — ssh graylog@192.168.10.111 — 143×24
Usage of /: Memory usage: Swap usage:	90.0% of 48.96G8 15% 0%	Users logged IPv4 address	in: for ens160:	1 192.168.10.111
=> / is using	98.8% of 48.96GB			
* Super-optimi footprint of	zed for small spac MicroK8s to make	es - read how v it the smalles	we shrank th t full K8s a	e memory round.
https://ubun	tu.com/blog/microk	8s-memory-optin	nisation	
60 updates can 1 of these upda To see these ad	be applied immedia tes is a standard ditional updates r	tely. security update un: apt list	e. -upgradable	
Last login: Thu origing Graylog No LSB modules Distributor ID: Description: Release: Codename: gruptog@graylog	Sep 9 84:17:41 2 -\$ 1sb_release -a are available. Ubuntu Ubuntu 20.04 LTS 20.04 focal -\$	921		

Figure 20: Graylog Instance Running with Ubuntu 20.04 LTS

Secondly, we will make sure that the Ubuntu Operating System 18.04.5 LTS is installed for Zeek IDS, refer Figure 22. Once installed in ESXi, we can see that the host is up and running, refer Figure 21.

all in	And The Local District States Concentration States	Links (HH-BE) 1 and alow (HH-response Fig.)	
	e		
- Sever Memory		Remain for	Torquinin
- Second Statistics - [] Tanaming		1 Annual for 1 B (N)	forthurmen d richtes
- Second Multiplier - Q. Secondary - Secondary	-	· Herman For • 12 Oni	forgantes forgantes
- Konst Martina - Martina - Martina - Martina - Patrone	-	- Armon for - 13 cm - 13 cm - 2 marca	Congueges
- Sever Murraner - Murraner - Marrane - Fallmane	4 - He ment and - 4 - He ment a	- Antenen So + 20 Mi - 20 Mi - 20 Minutes - 20 Minutes	50%partities 2 = 27/10 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 =
- Sever Murrane - (2 Severage - 10 Severage - 10 March 199	C - Hannen and Anning R - Hannen and Anning Hannen and Anning	- Annexe for - 20 (%) - 20 (%)	Annuar Maria Annuar Annuar
- Samer Martabar - (gradening - natrone - Patholen - Martabar - Discover	4 4 - HE MARCH 14 2 - March 14 March 14 Ma	- Marman So + 2014 - 20	Andream
- Sever Montpler - () Sevening - not rank - Patteries - Discours - Discou	4 He meritari A He meritari A He meritari A meritari Hemeritari A He	- Antenna So - Antenna - Bonna - Bonna - Bonna - Stateman -	Dottouries

Figure 21: Zeek Virtual Machine Instance

		🚞 admin — zeek	@zeek: ~ — ssh zeek@192.168.10.127 — 143×24
System load:	0.0	Processes:	166
Usage of /:	20.2% of 88.080B	Users logged in:	0
Memory usage:	5%	IP address for ens160:	192.168.18.127
Swap usage:	8%		
 Super-optimi footprint of 	zed for small space MicroK8s to make	es – read how we shrank it the smallest full K8s	the memory around.
https://ubun	tu.com/blog/microk	8s-memory-optimisation	
16 updates can	be applied immedia	tely.	
To see these ad	ditional updates r	un; apt listupgradabl	e :
*** System rest	art required ***		
Last login: Fri	Jul 16 16:45:56 20 b release -a	821 from 192.168.18.92	
No LSB modules	are available.		
Distributor ID:	Ubuntu		
Description:	Ubuntu 18.04.5 LT	5	
Release:	18.04		
Codename:	bionic		
zook@zonk:~S			

Figure 22: Zeek Instance Running with Ubuntu 18.04.5 LTS

4.2.1 Download, Install and Configure Graylog

When the Graylog been installed with the Ubuntu OS, we need to access the instance with ease. In order to do that, we needed to perform SSH to the instance from the host machine. In this situation, we were using Macintosh Macbook. Therefore, in Graylog instance, we have installed OpenSSH so then we can perform SSH to the instance from Macbook terminal.

In the instance, we performed the following command to install OpenSSH.

\$ sudo apt update\$ sudo apt install openssh-server

Press Y to continue with the installation

Then, we can perform SSH from the Macbook machine to the instance.

```
    admin — graylog@graylog: ~ — ssh graylog@192.168.10.111 — 143×24

admins-MacBook-Pro:~ admin$ ssh graylog@192.168.18.111
graylog@192.168.18.111's passeord:
```

After successfully logged into Graylog instance via SSH. We started downloading and installed Graylog version 4.1.1 within the instance.

For the Graylog instance, running with Ubuntu 20.04 LTS, we chose DEB / APT options to install.

```
$ sudo apt-get install apt-transport-https
$ wget https://packages.graylog2.org/repo/packages/graylog-4.1-
repository_latest.deb
$ sudo dpkg -i graylog-4.1-repository_latest.deb
$ sudo apt-get update
$ sudo apt-get install graylog-server -y
```

Then, before starting the Graylog, we had to make sure the prerequisites are installed. Graylog 4.1.1 are depending and supported on Java version 8 and above, Elasticsearch version 6.x or 7x and MongoDB version 4, 4.2 or 4.4 only.

Before proceeding with the said dependencies, we installed Java for Graylog with the following command:

\$ sudo apt-get install openjdk-11-jre-headless -y

We will also require to generate a secret to secure password for Graylog user.

\$ pwgen -N 1 -s 96

And we got the following output:

oefAXKFoU93q18b2H7tLr0gATaB2w0CDJ11iP3fASy08dqa7ENLv7zg4e8epuF4p0qQQVVRnoArMIvtpSLNHXdvFo4fH0dvq Next thing, is to generate a password for the admin in order to login into the Graylog web system. From here, we generated a secure password with the following command:

\$ echo -n Cr@cker42 | sha256sum

And we got the following output:

973e1b07645e98444bc9491e3a568f0327649ee57ec4a71a77fc0e0fad132d1e

Then, we edit the existing configuration file and put those two passwords.

Password_secret = cefAXKFoU93q18b2H7tLr0gATaB2w0CDJ1IiP3fASy08dca7EMLv7zg4e8epuF4p0q0QVVRmoArMIvtpSLMHXdvFo4fH0dvq Root_password_sha2 = 973e1b07645e98444bc9491e3a568f0327649ee57ec4a71a77fc0e0fad132d1e

Then, saved and exited the changes.

Also, in order for allowing us to access the web system, we had to bind the local server with the propose port number:

\$ http_bind_address = localhost:9000

Then, save and exit the changes. After that, we had to start the Graylog service and enabled it accordingly with the following command:

```
$ sudo systemctl daemon-reload
$ sudo systemctl start graylog-server.service
$ sudo systemctl enable graylog-server.service
```

After performing those commands, we had to verify and validate whether the Graylog is working as intended with the following command:

\$ sudo systemctl status graylog-server.service

And the output was like this:

```
graylog-graylog:~$ sudo systemctl status graylog-server.service

graylog-server.service - Graylog server

Loaded: loaded (/lib/systemd/system/graylog-server.service; enabled; vendor preset: enabled)

Active: active (running) since Thu 2021-09-09 04:05:36 UTC; 4h 18min ago

Docs: http://docs.graylog.org/

Main PID: 781 (graylog-server)

Tasks: 175 (limit: 7029)

Memory: 1.46

CGroup: /system.slice/graylog-server.service

- 781 /bin/sh /usr/share/graylog-server/bin/graylog-server

- 1087 /usr/bin/java -Xms1g -Xmx1g -XX:NewRatio=1 -server -XX:+ResizeTLAB -XX:-OmitStackTraceInFastThrow -Djdk.tls.
```

Sep 09 04:05:36 graylog systemd[1]: Started Graylog server.

Now for Elasticsearch, we started installing and configuring Elasticsearch. With this case, we installed Elasticsearch version 7.x.

NY 886 - S. - 16.

```
$ sudo wget -q0 - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-
key add -
$ echo "deb https://artifacts.elastic.co/packages/oss-6.x/apt stable main" |
sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list
$ sudo apt-get update -y$
$ sudo apt-get install elasticsearch-oss -y
```

After installing Elasticsearch, we edited the Elasticsearch config file and inserted the cluster name.

```
$ sudo nano /etc/elasticsearch/elasticsearch.yml
Insert the cluster name and following settings to:
cluster.name: graylog
action.auto_create_index: false
```

After save and close the config file, we started the Elasticsearch service and enabled it.

```
$ systemctl daemon-reload
$ systemctl start elasticsearch.service
$ systemctl enable elasticsearch.service
```

From here, we needed to ensure the service is up and running without any error.

\$ systemctl status elasticsearch.service

Then, to verify whether if we send request to Elasticsearch, we will be able to receive the response, if there is no response, the installation is consider failed.

```
$ curl -X GET http://localhost:9200
```

```
graylog@graylog:~$ curl -X GET http://localhost:9200
{
  "name" : "graylog",
  "cluster_name" : "graylog",
  "cluster_uuid" : "rkF2QnZBR8yJTEfIqIxujQ",
  "version" : {
    "number" : "7.13.3",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "5d21bea28db1e89ecc1f66311ebdec9dc3aa7d64",
    "build_date" : "2021-07-02T12:06:10.804015202Z",
    "build_snapshot" : false,
    "lucene version" : "8.8.2",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
graylog@graylog:~$
```

Next, we installed MongoDB, because Graylog requires MongoDB as a database and works well with it. The following command:

\$ sudo apt-get install mongodb-server -y

Once installed, we started the MongoDB and enabled it.

```
$ sudo systemctl start mongod.service
$ systemctl enable mongod service
```

```
$ systemctl enable mongod.service
```

From here, we needed to ensure the service is up and running without any error.

\$ sudo systemctl status mongod.service

And the output was like this:

```
graylog@graylog:~$ sudo systemctl status mongod.service

• mongod.service - MongoDB Database Server

Loaded: loaded (/lib/systemd/system/mongod.service; enabled; vendor preset: enabled)

Active: active (running) since Thu 2021-09-09 04:05:36 UTC; 4h 37min ago

Docs: https://docs.mongodb.org/manual

Main PID: 785 (mongod)

Memory: 190.4M

CGroup: /system.slice/mongod.service

L-785 /usr/bin/mongod --config /etc/mongod.conf
```

```
Sep 09 04:05:36 graylog systemd[1]: Started MongoDB Database Server.
graylog@graylog:~$
```

4.2.2 Download, Install and Configure Zeek IDS and Filebeat

Similar to items 4.2.1, we installed OpenSSH in this Zeek IDS instance with the following command.

\$ sudo apt update
\$ sudo apt install openssh-server
Press Y to continue with the installation

Then, we can perform SSH to the instance from Macbook terminal.

```
e e ek@192.168.10.127 - 143×24
admins-MacBook-Pro:- admin$ ssh zeek@192.168.10.127
zeek@192.168.10.127's password:
```

After successfully logged into Zeek instance via SSH. We started downloading, installing and configuring Zeek IDS within the instance.

For the Zeek instance running with Ubuntu 18.04.5 LTS, we performed the update and did some upgrade with the following command.

\$ sudo apt-get update && sudo apt-get dist-upgrade

Then, to install Zeek, we needed to download and install few dependencies before installing, with the following commands:

```
$ sudo apt-get install cmake make gcc g++ flex bison libpcap-dev libssl-dev
python3 python3-dev swig zlib1g-dev
```

In order to download Zeek, we needed to download it from Zeek official GitHub. Therefore, we installed git with the following command.

\$ sudo apt-get install git

Then we cloned the Zeek from Zeek GitHub with the following command:

\$ sudo git clone --recursive https://github.com/zeek/zeek

Then, we used cd command to the Zeek directory after downloaded from GitHub, then we built and installed the Zeek IDS with this command:

\$ sudo ./configure && make && sudo make install

After built and installation is complete, we had to configure the run-time environment for the path environment, so then when we executed the Zeek the platform or shell and it were able to run under that specific path. Therefore, we had to open the following configuration file with the command:

\$ sudo nano ~/.bashrc

Then, we have inserted the shell syntax, save and exit after changes.

Export PATH=/usr/local/zeek/bin:\$PATH

Then, we had to manage the node for Zeek. In our case, we are only depending to one server for Zeek, it is therefore, we needed the ZeekControl to be installed as standalone. ZeekControl is an interactive shell for operating or managing Zeek on the system.

Thus, we needed to configure something inside node configuration file for ZeekControl with the following command and things to change.

```
$ sudo nano /usr/local/zeek/etc/node.cfg
```

Then, we changed the interface to monitor the traffic. This is mirror traffic that we received from Cisco ASA Firewall.

```
[zeek]
type=standalone
host=localhost
interface=ens192  # change this according to your
listening interface in ifconfig
```

In this case, our interface was ens192. Then changed it and saved accordingly.

After saving the node config file. We needed to enable the interface ens192 in order to receive mirror traffic with the following command.

\$ sudo ip link set dev ens192 up

To verify whether the ens192 was up or not with the following interfaces, we needed to perform this command:

\$ ip link

Then the results shown as:

```
Interview:-$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default glen 1000
link/loopback 00:00:00:00:00:00:00:00:00
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mg state UP mode DEFAULT group default glen 1000
link/ether 00:0c:29:88:b9:17 brd ff:ff:ff:ff:ff:ff
3: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mg state UP mode DEFAULT group default glen 1000
link/ether 00:0c:29:88:b9:21 brd ff:ff:ff:ff:ff
```

So, from here we know that ens160 was the management interface or known as localhost interface and ens192 was the mirroring interface to receive mirror traffic from Cisco ASA Firewall.

From here, we had to start the ZeekControl and executed this command:



Then we executed this command by order:



After deploying, we needed to check the status of the Zeek by executing:

```
[[ZeekControl] > status
Name Type Host Status Pid Started
zeek standalone localhost running 16562 09 Sep 10:24:18
```

Then, the next step is to define what kind of logs that we should select once the mirror traffic ingested into Zeek. As we know, the mirror traffic that is sent by Cisco ASA Firewall might be coming from multiple devices within the network. It is therefore important for us to defined what kind of logs that is critical for monitoring.

As we know, the Zeek is already enabled and now we needed to see what kind of logs Zeek IDS received thus far.

By using cd command in ubuntu to the path:

```
$ cd /usr/local/zeek/logs/current
```

We see the logs as shown below:

zeek@zeek:/usr/local/zeek/logs/current\$ 1s

capture_loss.log dhcp.log files.log known_hosts.log notice.log ocsp.log software.log ssl.log stderr.log syslog.log x509.log conn.log dns.log http.log known_services.log ntp.log sip.log ssh.log stats.log stdout.log weird.log reck@zeek:/usr/local/zeek/logs/current\$

It is decided that we chose the capture_loss log, conn.log, dce_rpc.log, dhcp.log, dns.log, dpd.log, files.log, ftp log, http.log, intel.log, kerberos.log, mysql.log, ntlm.log, oscp.log, pe.log, rdp.log, smb_files.log, socks.log, ssh.log, ssl.log, syslog.log, tunnel.log and weird.log.

Even some of these logs were not in the current logs, it still can be ingested to Graylog Logging Tool when there is an activity pertaining to that network protocol occurs. However, this is depending on the Filebeat module that we needed to configure.

After this stage, we had to install a log shipper, in this case, we installed a Filebeat log shipper. Filebeat does have the Zeek module after the installation. We executed this command to download Filebeat, installed and enabled them.

```
$ sudo apt-get update && sudo apt-get install filebeat
$ sudo systemctl enable filebeat
$ sudo filebeat modules enable zeek
```

The next stage, it requires us to configure the Zeek module in Filebeat path. We executed and modified them accordingly. Then we saved and closed it.

\$ sudo nano /etc/filebeat/modules.d/zeek.yml

The modified configuration in the zeek.yml as shown below:

- module: zeek
enabled: true
var.paths: ["/usr/local/zeek/logs/current/capture_loss.log"]
connection:
enabled: true
dce_rpc:
enabled: true
var.paths: ["/usr/local/zeek/logs/current/dce rpc.log"]
dhcp:
enabled: true
var.paths: ["/usr/local/zeek/logs/current/dhcp.log"]
dns:
var naths: ["/usr/local/zeek/logs/current/dns log"]
dpd:
enabled: true
var.paths: ["/usr/local/zeek/logs/current/dpd.log"]
files:
enabled: true
ftn:
enabled: true
var.paths: ["/usr/local/zeek/logs/current/ftp.log"]
http:
enabled: true
var.paths: ["/usr/local/zeek/logs/current/http.log"]
enabled: true
var.paths: ["/usr/local/zeek/logs/current/intel.log"]
kerberos:
enabled: true
var.paths: ["/usr/local/zeek/logs/current/kerberos.log"]

mysql: enabled: true var.paths: ["/usr/local/zeek/logs/current/mysql.log"] ntlm: enabled: true var.paths: ["/usr/local/zeek/logs/current/ntlm.log"] ocsp: enabled: true var.paths: ["/usr/local/zeek/logs/current/ocsp.log"] pe: enabled: true var.paths: ["/usr/local/zeek/logs/current/pe.log"] rdp: enabled: true var.paths: ["/usr/local/zeek/logs/current/rdp.log"] smb files: enabled: true var.paths: ["/usr/local/zeek/logs/current/smb files.log"] socks: enabled: true var.paths: ["/usr/local/zeek/logs/current/socks.log"] ssh: enabled: true var.paths: ["/usr/local/zeek/logs/current/ssh.log"] ssl: enabled: true var.paths: ["/usr/local/zeek/logs/current/ssl.log"] syslog: enabled: true var.paths: ["/usr/local/zeek/logs/current/syslog.log"] tunnel: enabled: true var.paths: ["/usr/local/zeek/logs/current/tunnel.log"] weird: enabled: true var.paths: ["/usr/local/zeek/logs/current/weird.log"

Zeek has its own policy of translating log extension to another extension and also it does provide policy tuning in it. Thus, in order to secure all protocols to be monitored by Zeek, we had to add all types of alerts in Zeek config file and change the log types received to. json format. We executed and added this up by the following:

```
$ sudo nano /usr/local/zeek/share/zeek/site/local.zeek
```

```
@load alert-all-notices
@load policy/tuning/json-logs.zeek
```

Then saved and closed.

Lastly, we needed to configure the Filebeat.yml file to change from default path to the destination path logs for retrieval as well as the destination IP of Graylog. We executed and made changes of the following:

```
$ sudo nano /etc/filebeat/filebeat.yml
```

```
Paths: - /usr/local/zeek/logs/current/*.log
Output.logstash:
Hosts: ["192.168.10.111:5044"]
```

Then we restarted the Filebeat.

```
$ sudo systemctl restart filebeat
```

After all configurations been made, the final stage is to deploy new config through ZeekControl.

Executed.

\$ sudo /usr/local/zeek/bin/zeekctl

```
[ZeekControl] > deploy
checking configurations ...
installing ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
starting ...
starting zeek ...
[ZeekControl] >
```

4.2.3 Download, Install and Configure NXLog Agent for Workstation PC

For Windows computer named as Workstation PC, this is the one requires an agent installation. This agent based is called as NXLog. This NXLog is a log shipper and look similar to Filebeat. It does have a configuration file that needs to be modified and some fine tuning of log types. We needed this to be modified to ensure appropriate logs is ingested into Graylog Log Monitoring Tool.

The Workstation PC is running with Windows 7 Professional and its running as a virtual machine. We configured this Windows machine with remote desktop enabled. We need to remotely control this machine from our Macbook machine and installed the NXLog.

Once we downloaded the NXLog from <u>https://nxlog.co/system/files/products/files/348/nxlog-ce-2.11.2190.msi</u>, we installed and modified few things inside the NXLog config file. The following changes as shown below.

define ROOT C:\Program Files (x86)\nxlog define CERTDIR %ROOT%\cert define CONFDIR %ROOT%\conf define LOGDIR %ROOT%\data define LOGFILE %LOGDIR%\nxlog.log LogFile %LOGFILE%

Moduledir %ROOT%\modules CacheDir %ROOT%\data Pidfile %ROOT%\data\nxlog.pid SpoolDir %ROOT%\data

<Extension _syslog> Module xm_syslog </Extension>

<Extension _charconv> Module xm_charconv AutodetectCharsets iso8859-2, utf-8, utf-16, utf-32 </Extension>

<Extension _exec> Module _xm_exec </Extension>

```
<Extension fileop>
 Module
        xm fileop
 # Check the size of our log file hourly, rotate if larger than 5MB
 <Schedule>
  Every 1 hour
   Exec if (file exists('%LOGFILE%') and \
       (file size('%LOGFILE%') >= 5M)) \setminus
       file cycle('%LOGFILE%', 8);
 </Schedule>
 # Rotate our log file every week on Sunday at midnight
 <Schedule>
   When @weekly
   Exec if file exists('%LOGFILE%') file_cycle('%LOGFILE%', 8);
 </Schedule>
</Extension>
<Extension gelf>
 Module
        xm gelf
</Extension>
<Input in>
 Module
        im mseventlog
# For windows 2003 and earlier use the following:
# Module
        im mseventlog
</Input>
<Output graylog>
 Module om udp
 Host
       192.168.10.111
 Port
       3514
 #Exec
        to syslog snare();
 OutputType GELF
</Output>
<Route 1>
 Path in => graylog
</Route>
```

From the config file as shown above, the most important things are the inputs from xm_gelf, im_mseventlog and the Graylog output. The input conditions are the one that NXLog will collect from the Windows 7 machine and send the logs to the output of Graylog. From here we can see the most important module is im_mseventlog. This is the Microsoft event logs that we normally see in Windows event viewer. It consists of many information pertaining to the application, system and security.

For the output of Graylog here, the events will be sent to the Graylog Monitoring Tool destination host IP through UDP protocol.

4.3 Testing Plan and Test Output

The following are the steps of testing and the output in order to receive logs from Zeek IDS and Windows machine which also requires fine tuning once Graylog able to receive from those two sources.

- a. Open Web System at <u>https://192.168.10.111:9000</u> and log in as admin
- b. Open System / Inputs, then go to Inputs
- c. Select Beats for Zeek IDS and GELF UDP for Windows machine to launch new input
- d. Enter the following information for both sources as shown below.
 - i. Tick Global
 - ii. For Windows insert as Windows-input and Zeek as Zeek
 - iii. Bind address leave as 0.0.0.0
 - iv. Port for Windows is 3514 and Zeek is 5044
 - v. And click save

The two data sources we configured for the above is shown as below:

Global

Should this input start on all nodes

Title

Windows-input

Bind address

0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port

3514

Port to listen on.

Receive Buffer Size (optional)

262144

The size in bytes of the recvBufferSize for network connections to this input.

No. of worker threads (optional)

1

Number of worker threads processing network connections for this input.

Override source (optional)

The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.

Decompressed size limit (optional)

8388608

The maximum number of bytes after decompression.

Cancel Save

Figure 23: From Windows NXLog

🗹 Global

Should this input start on all nodes

Title

Zeek

Bind address

0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port

5044

Port to listen on.

Receive Buffer Size (optional)

1048576

The size in bytes of the recvBufferSize for network connections to this input.

No. of worker threads (optional)

1

Number of worker threads processing network connections for this input.

TLS cert file (optional)

Path to the TLS certificate file

TLS private key file (optional)

Path to the TLS private key file

Enable TLS

Accept TLS connections

Figure 24: From Zeek IDS Filebeat

Now, after the inputs configured, we needed to validate by looking at the data streams that will be sent to Graylog. Therefore, we created the stream for those two sources of Zeek IDS and Windows machine.

- a. Open <u>https://192.168.10.111:9000</u> and log in as admin.
- b. Then go to streams and Create Stream
- c. Insert title and description and leave Index set as default for Zeek IDS and Windows separately.
- d. Tick remove matches from "All messages" stream and click save

And we can see those two stream sources been created as shown below.



Figure 25: Event Streams Configuration for Windows and Zeek

Then, for each of these, we had to click Manage Rules and select an input to type Server Input and select an input for those input sources Windows and Zeek and click Load Message.

From here we can see it has been loaded as shown in the following page.

1. Load a me	ssage to test ru	les
Recent Message	Message ID	
Select the Input typ	e you want to load the r	message from,
Server Input	÷	
Select an Input from	n the list below and clici	"Load Message" to load the most recent message received by this input within the last hour.
Windows-input (org.graylog2.inputs.gelf.	udp.GELFUDPInput) 🛩 Load Meisinge
➡ f7c206d0- Timestamp 2021-09-11 06:24:	12c8-11ec-93be-4	000c292ceabd CategoryNumber 8
Stored in index graylog_0		EventID 7836
Routed into stres All messages	ims	EventReceivedTime 2821-09-11 14:24:51
		EventTimeWritten 2821-89-11 14:24:49
		EventType INF0
		FileName System

Figure 26: Event Test Rules for Windows Logs

1. Load a me	ssage to test rule	es
Recent Message	Message ID	
Select the Input typ	e you want to load the me	essage from.
Server input	· · · ·	
Select an input from	n the list below and click "	Load Message' to load the most recent message received by this input within the last hour
Zeek (org.graylo	g.plugins.beats.Beats2Inpl	ut) ~ Loud Message
₩ 843934e1 Timestamp 2021-09-11 06:57:	-12cd-11ec-93be-0	OOc292ceabd @metadata_beat filebeat
Stored in Index graylog_0		@metadata_pipeline filebeat-7.13.2-zeek-dns-pipeline
Routed Into strea Al messages	ams	@metadata_type _dec
		Ometadata_version 7.13.2
		@timestamp 2821-89-11T86:57:23.2122
		agent_ophemeral_id 7e7575f7-3f52-442e-985e-985a75f1e14b

Figure 27: Event Test Rules for Zeek IDS

Then, we can see all events shown in Graylog. From here had to Search and aggregate these two sources as shown below:



Figure 28: Aggregated Events Dummy-PC from Windows NXLog

fill Search	Soreant Aletta	Dashboards Entergebe	- System -	•					110.00	12° Ø
Tese:	A hears age	Undit Nor		dot sittens the sear	marks.et mit.ele. 5	kanthés in etter	ural'erpo		C	Smeerry
Tipi yas				AND INTEG IN THE	p_feaponal_tice	(444 TE -484)		-	Crust	2/Dan
= Aggregiting co	until by source	$M \rightarrow V$								
3958										
ration by the										
Al Wessages	-						-			36 (1
3621-09-11 (21 09:25:12:139 +80:06		50 H	1444.10.70 54283				A Later -			53231

Figure 29: Aggregated Events Zeek IDS from Filebeat

4.3.1 Enable and Configure Threat Intelligence Feature in Graylog

In this part, we enabled and configured the Threat Intelligence features in Graylog. For this part, we will only be relying on Zeek IDS data source and not from Windows NXLog because Windows NXLog source of events is suitable for Threat Hunting.

We go the Web System and go to System / Configurations and enabled the following and click save:



Figure 30: Threat Intelligence Features

Then, still under System / Configurations, we went to Content Packs and installed the following:



Figure 31: Threat Intelligence Content Packs

4.3.2 Create and Test Threat Intelligence and Threat Hunting Rules in Graylog

Now, the most important thing in this development is to ensure the rules for Threat Intelligence and Threat Hunting workable as intended.

First, we created the Threat Intelligence rules and test to see whether will it work as intended.

Still in the Web System, we go to System / Configurations settings and click on Update at Message Processors Configuration. From here, we moved the pipeline processor to the bottom and enabled all the processors listed.

Order Use drag and drop to change the execution order of the me	ssage processors.
≡ AWS Instance Name Lookup	
≡ GeolP Resolver	
≡ Message Filter Chain	
≡ Pipeline Processor	
Statuc	
Status	
Change the checkboxes to change the status of a message p	processor.
Processor	Enabled
AWS Instance Name Lookup	S
GeoIP Resolver	X
Message Filter Chain	
Pipeline Processor	
	Cancel Save

Figure 32: Message Processors Configuration for Threat Intelligence

This pipeline processor is the processor for retrieving, aggregating and processing the thirdparty Threat Intelligence feeds which in this case, we used the Tor Exit Node List – Threat Intel Plugin as shown at page 51. Then, we create a Threat Intelligence pipeline and insert a title, its description and saved it. After that, we edited the pipeline connection and clicked on edit connections and select the Zeek stream for streams and saved.

Still under the same pipeline named Threat Intel: Tor Exit Nodes, we configured the rules by clicking on Manage rules at the top and Create rule. Once here, we inserted the description and the rule for Tor Lookup and saved it.

Pipeline rule Tor Lookup
ules are a way of applying changes to messages in Graylog. A rule consists of a condition and a list of actions. Graylog evaluates atisfied.
Read more about Graylog pipeline rules in the documentation.
itie
ou can set the rule title in the rule source. See the quick reference for more information.
Description
71
(ule description (optional).
ised in pipelines
hreat Intel: Tor Exit Nodes .
ipelines that use this rule in one or more of their stages.
tule source
1 rule "Tor Lookup"
2 when 3 when [ie] (["dectination address"))
4 then
<pre>5 let intel = tor_lookup(to_string(Snessage.destination_address));</pre>
6 set_field("threat_indicated", intel.threat_indicated);
uie source, see quick reference for more information.
Seve & Close Apply Cantel
le saurce, see quick reference far more information. Save & Close Apply Cancel

Figure 33: Threat Intelligence Rule Feature

Next, we had to test the rule and see whether it works or not. Open the Workstation PC running Windows 7 machine and open the browser and go to Tor Exit Node list. This Tor Exit node list can be retrieved at <u>https://www.dan.me.uk/tornodes</u>.

Then, we see the outcome of the threat_indicated it returned to true, which means it has been identified as true positive events mapped to Tor Exit Node Threat Intelligence list. If it shown as false, that means, it is not a Tor Exit Node.

(Leveslary)	Source =	thread_indicated 17	destrution_aldress	Andrathic port	atoria_eblicto	- www.jwt_f
2021-09-12 06:52:33.141 +00:00	zeek	true	101.99.90.171	80	192,168:10.230	50336

Figure 34: True Positive Event

Unefülling:	and ch.	thus, Housed T	destanantes address	distrator port - 11
2021-09-12 06:56:13.206 +00:00	2948	fater	103.157.198.5	123

Figure 35: False Positive Event

Second, now we need to create a Threat Hunting rule for Windows machine that running with Windows 7 Professional.

For this Threat Hunting, we will need to create a Threat Hunting pipeline and insert a title and its description and saved it. After that, we need to edit the pipeline connection and click on edit connections and select the Windows stream for streams and saved.

Still under the same pipeline named Threat Hunting: Failed Login, we configured the rules by clicking on Manage rules at the top and Create rule. Once here, we need to insert the description and the rule for Threat Hunting Failed Login and saved it.

Pipeline rule Threat Hunting Failed Login Rules are a way of applying changes to messages in Graylog. A rule consists of a condition and a list of actions satisfied.	Graylog evaluates the co
Read more about Graylog pipeline rules in the documentation.	
Title	
You can set the rule title in the rule source. See the quick reference for more information.	
Description	
TH Failed LogIn	
Rule description (optional).	2
Used in pipelines	
Threat Hunting: Failed Login.	
Pipelines that use this rule in one or more of their stages.	
Rule source	
<pre>1 rule "Threat Hunting Failed Login" 2 // to ensure that all tubsequent stopes only process relevant events 3 when 4 (// native event 10 4478 5 hos_field("EventID") OR 6 hos_field("teressage") AND 7 contains("4478",to_string(\$ressage.EventID)) OR 8 contains("5-1-5-18",to_string(\$ressage.message)) 9) 10 then 11 set_field("threat_detected","true");</pre>	
Rule source, see quick reference for more information. Save & Close Auply Concel	

Figure 36: Threat Hunting Rule Feature

Now, in order to test the rule, we tried to attempt to the Windows 7 machine with the wrong password three times. Once exceeded than 3 times, the login will be locked. By right, the result in Graylog of threat_detected should be returned to true condition.

Al Messages			
Am Lorg		Broad Library and 17	
2021-09-13 12:58-35.000 +00:00 A uter scourt was locked out	there is a second se	THE.	
Notest: Recursts ID: 5-1-1			



4.3.3 Create and Test Slack Alert Channel for Notifications

In this part, we will be creating the alert and notifications for Threat Intelligence and Threat Hunting rules. The medium which was used is Slack channel.

In order to create this Slack, we will need to register ourselves at <u>https://slack.com</u> and we created it via Slack App Directory. After created, we need to copy the Webhook URL and put into Graylog Alert feature.

≜ graylog-alert ~
or create a new channel
https://hooks.slack.com/services/TM89ERE55/B0288578DRB/fwFZzcyg7WrBX

Figure 38: Slack App Directory Configuration

Alerts & Events Information and a statement of the second second second second				Section: Sectoring	(atom)
Products III III					
Bassipter	Rev.	faire	two befoliae	Terreturna	
Christian Busing Particle Lagran Is an instant (Reveal, Addition CPUC)	-	-		3107-04 11 14,01 CT	
7 thread least for the following the test of the classifier a	10.00	-		2017-08-13 520127	

Figure 39: Graylog Alert & Events Feature

And here were the output results of Threat Intelligence from Slack channel that we received.

Graylog APP 12:55 AM @channel Alert Threat Intel: Tor Exit Nodes triggered: Custom Message: --- [Event Definition] -----Title: Threat Intel: Tor Exit Nodes Type: aggregation-v1 ---- [Event] ------Timestamp: 2021-09-13T16:55:27.377Z Message: Threat Intel: Tor Exit Nodes : false - count(threat_indicated)=8415.0 Source: graylog Key: Priority: 2 Alert: true Timestamp Processing: 2021-09-13T16:55:27.377Z Timerange Start: 2021-09-13T15:55:27.377Z Timerange End: 2021-09-13T16:55:27.376Z Event Fields: ---- [Backlog] ------Last messages accounting for this alert: 2021-09-13T15:55:28.040Z zeek Victim IP:192.168.10.70 Tor Address:192.168.10.111 2021-09-13T15:55:28.041Z zeek

Figure 40: Threat Intelligence Alert

The following is the output result of Threat Hunting from Slack channel that we have received.

Today ~ Graylog APP 12:11 AM @channel Alert Threat Hunting: Failed Login triggered: Custom Message: --- [Event Definition] -----Title: Threat Hunting: Failed Login Type: aggregation-v1 ---- [Event] ------Timestamp: 2021-09-13T16:11:01.632Z Threat Hunting: Failed Login: true - count(threat_detected)=9.0 Message: Source: graylog 1 Priority: Alert: true Timestamp Processing: 2021-09-13T16:11:01.632Z Timerange Start: 2021-09-13T15:11:01.632Z Timerange End: 2021-09-13T16:11:01.631Z Event Fields: ---- [Backlog] ------Last messages accounting for this alert: 2021-09-13T15:22:39.000Z dummy-PC A user account was locked out. Subject: Security ID: S-1-5 2021-09-13T15:24:11.000Z dummy-PC A user account was locked out. Subject: Security ID: S-1-5

Figure 41: Threat Hunting Alert

CHAPTER 5

SUMMARY AND CONCLUSION

5.1 Summary of main findings

As we know, most of the cyber-attacks are sophisticated and it comes with many ways. It could be coming from phishing techniques, social engineering techniques, vulnerabilities and many others. As cyber-attacks evolving every single day, we as a cyber defender in an organization are required to equip ourselves with correct tools and technologies in place in order to combat cyber-attacks. Despite that, a very skilful staff is also required to ensure that any attacks found are analysed properly. Organization nowadays is having difficulties finding the right people in protecting their network perimeter from attacker. However, the tool is vital to facilitate the objective in defending cyber-attacks with ease. With this development system of Log Monitoring Tool equipped of Threat Intelligence and Threat Hunting, it could help a small medium enterprise or small organization with an idea to protect their organization from cyberattacks with minimal cost. It is therefore, we decided to develop this platform to overcome their issues at very low cost. As we know, with the covid-19 as a new-norm to communities around the world, most of small business enterprise are impacted of this virus economically.

5.2 Discussion and Implications

Before we decided to use Graylog Log Monitoring Tool as a platform for this system development, we had reviewed the other competitors in the market. After taking into consideration of finding the best platform with a very minimal cost as well as finding platform that could give less complexity in configuring or installing it, we decided to choose Graylog Log Monitoring Tool.

We also compared the modules provided between the other competitors with Graylog. In terms of UI and UX satisfaction, to us Graylog is better. We also think, the close competitor to Graylog with similar solution is Elastic SIEM. The only part they cannot win is the feature of Threat Intelligence as a whole.

5.3 Limitations of the system

Even we know most of the platforms are offering similar features to Graylog, we seen that, the Graylog offer less complexity in developing it to compare to other competitors. However, throughout the system development took place, we faced challenges. One of the challenges are the rulesets we created for Threat Intelligence and Threat Hunting. When we created the rules, we are required to test it out and validate it. In the beginning, we found nothing is triggered which by right it should be sent to Slack channel for notification. After hundred times of reading the platform documentations, configuration and testing, we managed to get it done.

Also, as we know this platform which given free does have its limitation if we compare with the paid version. One of it, is correlation of the events and creating complex events and alerts. For the free version that we used, is only given aggregation and not correlation.

Even this system may not perfect to compared to other competitors which are quite expensive and easier to use, it suits the objective in achieving it at very minimal cost to develop.

5.4 Future Development

For future development, we think the Graylog can still consume more events from multiple devices as long as the 5 Gigabyte maximum storage stay intact per day. If this is done, we can create more use cases for Threat Intelligence rules and Threat Hunting rules. As we know, in this development, we only created two rules in total that is for Threat Intelligence and Threat Hunting.

Moreover, with the existing devices and rulesets in place, we could also create more rulesets based on continuous use-case development. Generally, building a SIEM is not one or two destinations. It is a marathon and never-ending destination. It requires a lot of efforts in maintaining, developing and configuring it. The cyber attackers never sleep in offending or compromising business assets and therefore, we as a cyber defender would need to do the same to ensure we are defending against them with modern technology, right process and right people.

REFERENCES

Lemos, R. (2018). On the Hunt for Security: Tired of waiting for signs of an attack, companies large and small add threat hunting capabilities to their playbooks. Information Security, 20(6), 4–9. Retrieved online: http://eds.a.ebscohost.com.newdc.oum.edu.my/eds.

David Alexander, Amanda Finch, David Sutton, & Andy Taylor. (2020). *Information Security Management Principles*.

BCS, The Chartered Institute for IT. Retrieved online: http://eds.a.ebscohost.com.newdc.oum.edu.my/eds.

Liao, Xiaojing & Yuan, Kan & Wang, Xiaofeng & Li, Zhou & Xing, Luyi & Beyah, Raheem. (2016). *Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence*.

755-766. 10.1145/2976749.2978315.

Retrieved online: http://eds.a.ebscohost.com.newdc.oum.edu.my/eds.

Kure, H., & Islam, S. (2019). *Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure*.

JUCS - Journal of Universal Computer Science. Retrieved online: http://eds.a.ebscohost.com.newdc.oum.edu.my/eds.

Mitkovskiy, A., Ponomarev, A., & Proletarskiy, A. (2019). SIEM-Platform for Research and Educational Tasks on Processing of Security Information Events.

ELearning & Software for Education, 3, 48–56.

Retrieved online: http://eds.a.ebscohost.com.newdc.oum.edu.my/eds.