INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 11, Issue 1 - V11I1-1390)
Available online at: https://www.ijariit.com

Threat Scoring Model Basis Hybrid Attack Emulation

Mukul Kulshrestha
mukul.gaharana@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Satish Salunkhe
satishssalunkhe@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Dr. Vaishali Khairnar
vaishalikhairnar@ternaengg.ac.in
Terna Engineering College, Navi Mumbai, Maharashtra

ABSTRACT

In today's world, as the globe moves towards Metaverse, all commercial and business transactions are digitalized, and digital transformation is the new need of the hour owing to Covid and other environmental and health problems. On the one hand, digitalization is transforming the world; on the other with an expanding attack surface and a variety of attacker modus operandi, it is critical and long overdue to develop a threat classification model that can provide clear insight into adversaries through their appropriate classification and threat scoring. Research aims to emulate "Threat Scoring based on the Hybrid Attack Model" which consist of Red Teaming, Attack vectors and Threat Hunting models. Model will be simulated to understand the threat landscape for potential trigger points in network and operation by initiating a wide range of attacks at various levels with respect to security posture. Hypothesis of results based on attack vectors will be mapped with Threat Intel received from various open Threat Scoring model based on analysis of adversities. The threat modelling process will be based on the MITRE & ATTACK Framework, with discovered threats further classified according to MITRE Tactics, Techniques and Procedures.

Keywords— *Threat Scoring, Red Teaming, OSINT, Attack Vector, Threat Hunting*

INTRODUCTION

In today's scenario where world is moving towards Metaverse, all commercial and business transactions are digitalised, and digital transformation is the new need of time due to Covid and other such environmental and health concerns.

Where digitalisation is opening the barrier of geolocation, time zones and amalgamation of different systems but as these nodes get connected, the possibility of luring malicious actors grow. These interconnected systems and networks are keeping tremendous information which is of substantial value for attackers or the person who wants to use it with any malicious intention.

It leads to many corporations and businesses getting targeted. In recent years, the market for security tools to help secure systems and detect attacks has risen, but many of these tools are not interactive, instead relying on pre-programmed logic, such as monitoring a specific signature with wrong classification of threat values which always result either as false positive or non-detectable attack which are laying in the environment for years without even organisation knows about

Sometimes situation is so graveyard that underlying threat are detected at time but absence of right Threat Modelling will let them pursue those threats as benign making organisation to sit on the edge of exfiltration or denial of service

Hybrid attack model refers to the composition of various attack vectors, red teaming exercises or different threat hunting Models which can be used attacking a simulated environment Those adversaries can be linked with Open-Source Intelligence or Threat Feeds to have visibility on its malicious nature.

This Project is research to further add Threat Scoring on the adversities received after Red Teaming or using different attack vectors which will be linked to TTPs of MITRE framework as well It will help systems to get a holistic approach on adversaries and to identify which are actionable intel or events basis on Threat Risk Score.

In existing system research is limited to threat Hunting through Hybrid Attack simulations. Researcher has identified the below research gaps through various literature review of the paper published by different researcher.

Earlier research carries Limited Scope and focused on threat hunting with lack of Scoring mechanism .Fredericka Araju with IBM research [1] tries to go with evidential threat hunting but it was only a framework and other researcher like [2] was not able to integrate OSINT and attack model. Researchers tries to be focused on only offensive side of security and with limited scope all possible hybrid attack model was not explored [3]. Dulaunoy, Alexandre & Wagener[2021] were able to successfully define scoring mechanism for MISP platform but they missed threat hunting part [4][5]. Xiang [6] tries a threat modelling approach with MITRE Framework but his work was concentrated on developing a Meta language and workable methodology was lacking to integrate with Attack model till Threat scoring system.

With the GAP identified, it is evident that the vast majority of studies and systems are either operating in silos or addressing a single point problem rather than offering a holistic and full picture of the situation. Research is entitled to fill this gap by developing a Threat Scoring Model, which will provide a complete 360-degree image, starting with assault simulation and going through hunting and scoring, as well as converting that knowledge into actionable intel. Key action point of research are:-

a. To develop an attack simulation Model

b. To Develop Threat Scoring Model mapped with MITRE Framework

In order to address Problem Statement , Objectives can be further classified in 2 phases where Phase 1 will be addressing the need of attack simulation environment for real time testing and developing an workable model and Phase2 where Identification of Threat will be conducted and based on Threat Scoring Model threat will further converted into actionable intelligence along with mapping of MITRE Framework . Objectives can be classified as follows:-

Create a simulated environment

Initiate attack through various ways (Hybrid Model of attacking)

Identification and hunting of attacks on hybrid model with MITRE Mapping

Critical and Non Critical Asset Impact calculation

Severity Impact calculation

Threat Scoring And Grading

PROPOSED METHODOLOGY

From creation of attack simulated environment till capturing Threat and aligning them to actionable Score along with mapping to Mitre. Approach here is to create a stage wise methodology which can cater all of our objective needs. Following are the defined precise way to define methodology and stage wise approach.

In principle, Logical flow can be defined where logs are getting inserted from data sources like Win or Linux servers through logger or directly into Hybrid Emulator. Hybrid Emulator is the component which is capturing attack happening and after categorising Threat it is again fed into Threat scoring system where Threat Score are getting aligned to the attack. Output of Threat Scoring model is the final Threat Score along with actionable intel which is mapped with MITRE Framework

TABLE I. ***METHODOLOGY USED [7][8]***

Phased approach	Objectives	System Requirements	Tools used
Phase 1	Creation of simulated environment for Hybrid attack Simulation	Hybrid Emulator Windows Machine Ubuntu Machine	WEF Firewall
	Attack initiation through hybrid approach	Kali Linux Power shell Logger	Metasploit and other Kali Tools Downloadable Test virus Github scripts for Red Teaming Autorun scripts
	Identification and hunting of attacks on hybrid model with MITRE Mapping	Qradar or Splunk or ELK or any SIEM Server and Logger	Suricata Velociraptor Zeek Firewall
Phase 2	Asset Impact & Severity Impact Calculations	Manual or Scripts	Python Script
	Threat Scoring and Grading	Manual or Scripts	Python script

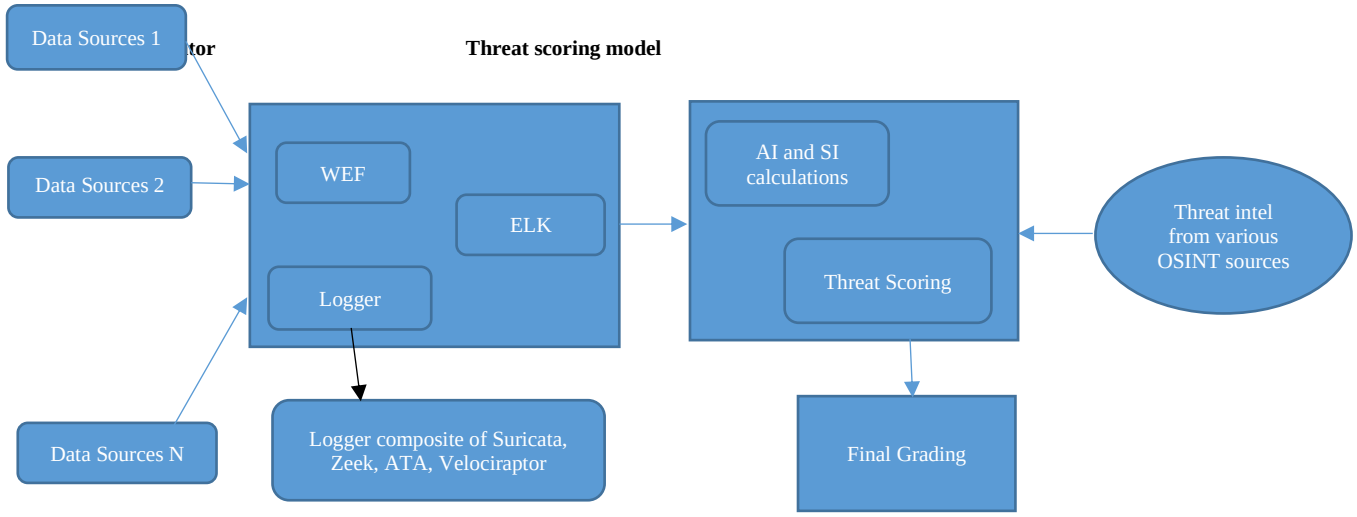

FIG. 1. LOGICAL FLOW DIAGRAM

SIMULATED ENVIRONMENT

Following LAB scenario is suggested to test the minimal form of above logical flow,

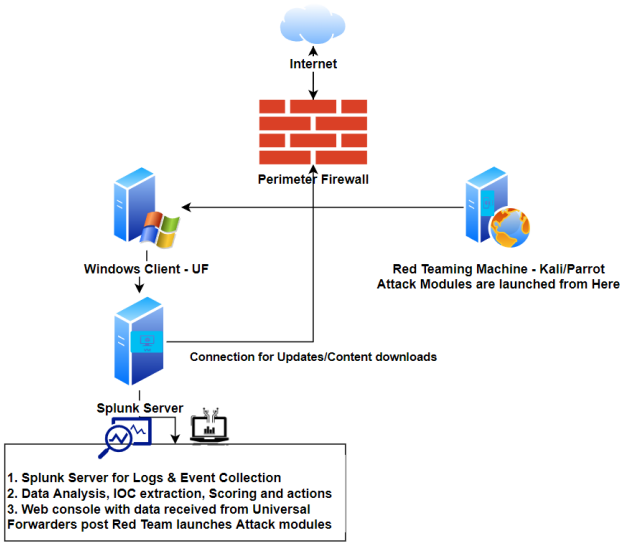

FIG. 2. SIMULATED ATTACK ENVIRONMENT

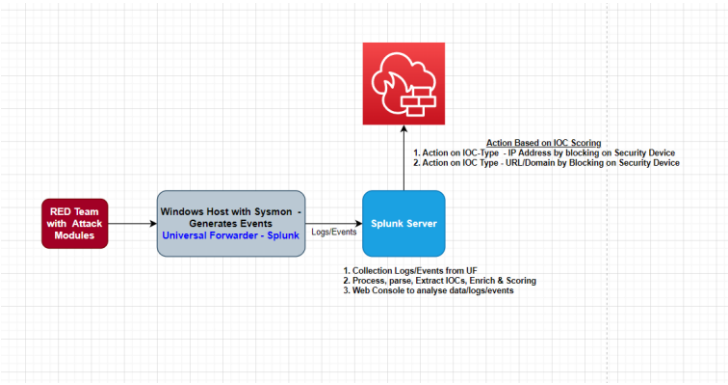

FIG. 3. SYSTEM ARCHITECTURE OF SYSTEM EMULATOR

RESULTS

The Attack & Detection [Red Teaming & Blue Teaming] is emulated on virtual environment. An emulated lab of a Splunk Server & Universal Forwarder nodes for data collection, parsing, analysis, enrichment, IOC Scoring & action. Sysmon for windows for extended Event details will be shipped to Splunk Server through Universal Forwarder in client VM installed. Universal forwarders

ship log/event data to Splunk server. Attacks are initiated/launched from a separate VM instance called Red Teaming image. Threat Intel IOC scraping from Internet – OSINT. Enrichment Sources currently used: MITRE ATT&CK TTPs collected via UF, AlienVault OTX, ThreatFox etc. and many more could be added for reducing false positives and actionize/prioritize the actions basis scoring parameters on relevant security devices in any network.

For simulation environment to emulate Attack and Threat Scoring Parameters we have opted 7 Critical Assets and One Non Critical Asset , overall Asset attacked were eight.

Result Table for phase 1 Activity :

Sample Offense Data (Qradar API)						
OFFENSE TYPE	OFFENSE ID	OFFENSE SOURCE	SEVERITY	CREDIBILITY	OFFENSE RISK SCORE WEIGHTAGE	EVENT COUNT
Username	572897	root	6	2	4	382
Source IP	572996	192.168.37	10	2	8	4
Username	573080	MK	4	2	3	21
Username	573081	Hack	4	2	3	9
Username	573140	Test/Hack	4	2	3	9
Username	573157	HBTFI-1	4	2	3	5
Source IP	573369	10.10.0.5	10	2	8	8
Source IP	573863	10.10.0.6	0	3	0	7
Source IP	576832	10.10.0.7	10	5	8	2

Result table for Phase 2 :

Offense MITRE Mapping			
OFFENSE ID	DESCRIPTION	Avg Sev	MITRE Mapping used
572897	UCI 102 - Linux - Possible Bruteforce	4	T110
572996	ICritical System Notify	7	T110
573080	Login Failure for Firewall Devices	3	T110
573081	Login Failure for Firewall Devices	3	T110
573140	Login Failure for Firewall Devices	3	T110
573157	Login Failure for Firewall Devices	3	T110
573369	Infinity_Critical System Notify	7	T110
573863	Firewall Permit	1	T110
576832	Login Failure for Firewall Devices	8	T110

THREAT SCORE MODEL

Further, Threat scoring model can be developed and defined basis on Avg Severity extracted. We need to take out Median of Avg of Severity , Credebility and Offense risk score .

Formulae for Threat Scoring will be as follow

Threat Score = 80% of Severity Impact (SI) + 20% of Asset Impact (AI)

Where ,

SI = Median (Avg Severity Value for each incident)

Where ,

Avg Severity = Avg (Sev+Credibility+ Risk Score Weithage) per Offense

AND
AI = 80% of Critical Divison (CD)+ 20% of Non critical Divison (NCD)
Where,
CD = Total Critical Asset / Sum of all Asset

NCD = Total Non Critical Asset /Sum of all Asset

Applying the above formulae we can calculate Threat Score for the result observed in Phase 1 and Phase 2 activity

SI = 3
AI = 0.725

Threat Score *= (80%*SI)+(20%*AI)*
*= (80%*3) + (20%*0.725)*
= 2.545

GRADING –

if Score > 0 and Score <= 2.0		A
if Score > 2.1 and Score <= 4.0		B
if Score > 4.1		C

For Threat Score 2.545 , Grade is B

Grade define the Risk metrics for the Threat Score i.e Grade A is less risk ,B is moderate and C shows High Risk

CONCLUSIONS

With this research we are not only performing Threat Classification by identifying attack vectors and actors engaged with correct MITRE mapping but also adding Threat Scoring so that an actionable Intel can be generated. Future can be a single tool by expanding the research simulation to the large scale by creating one tool for all above requirements which are analyzing, hunting, classification and Scoring and generating actionable intel covering Threat Scoring and Grading

REFERENCES

[1] Evidential Cyber Threat Hunting arXiv:2104.10319v1 [cs.CR] 21 Apr 2021, Frederico aujo Dhilung Kirat Xiaokui Shu Teryl Taylor Jiyong Jang IBM Research, Yorktown Heights, NY, USA

[2] Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence, October 2020, Peng Gao,Fei Shao,Xiaoyuan Liu

[3] B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar and S. U. Islam, "Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation," in IEEE Access, vol. 9, pp. 126023-126033, 2021, doi: 10.1109/ACCESS.2021.3104260.

[4] Automated Threat Hunting Using ELK Stack - A Case Study,October 2019,Indian Journal of Computer Science and ngineering 10(5):118127,DOI: 10.21817/indjcse/2019/v10i5/191005008, MOZA AL SHIBANI,ANUPRIYA E

[5] AN INDICATOR SCORING METHOD FOR MISP PLATFORMS,June 2018,Conference: TNC 18,At: Trondheim.Norway

[6] Xiong, W., Legrand, E., Åberg, O. M, Robert Lagerström Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. Softw Syst Model (2021). https://doi.org/10.1007/s10270-021-00898-7

[7] https://github.com/clong/DetectionLab

[8] https://attack.mitre.org/