National College of Ireland

Configuration Manual

MSc Research Project
Msc in CyberSecurity

Bhanu Prakash Rayabandi
Student ID: 21189731

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	……Bhanu Prakash Rayabandi.
Student ID:	21189731
Programme:	Msc in Cyber Security …… **Year:** 2024
Module:	Msc Research Project
Lecturer:	Michael Pantridge
Submission Due Date:	14/12/2023
Project Title:	Integration of Elastic Search and Kibana Siem for Malware Detection
Word Count:	……1063…… **Page Count:** ……12…….…….

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	R Bhanu ……
Date:	12/12/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Bhanu Prakash Rayabandi
Student ID: 21189731

1 Introduction

1.1 1.1 Overview

Our integrated malware detection system addresses the limitations of traditional security methods by combining proactive measures with predictive threat mechanisms. Tailored for small to medium-sized businesses, the project utilizes Elastic Search and Kibana, integrating prebuilt detection rules and custom sigma rules for comprehensive malware detection and analysis. The system seamlessly coordinates through Fleet Server, with the Windows 10 VM serving as an endpoint. Leveraging the MITRE ATT&CK matrix, the project successfully analyzes malware attacks, generating custom sigma rules and alerts through Elastic Search and Kibana. This scalable solution not only fills gaps in outdated security but also empowers organizations to proactively tackle modern computer-based threats.

1.2 System Environment

Elastic Search and Kibana:

Hardware:
Base Memory:4608 MB
Processor: 4
Storage: 25 GB of free disk space
Network: Intel Pro/1000 MT Desktop(Nat Network, 'NatNetwork')

Software Dependencies:
Java Runtime Environment (JRE) 8 or higher

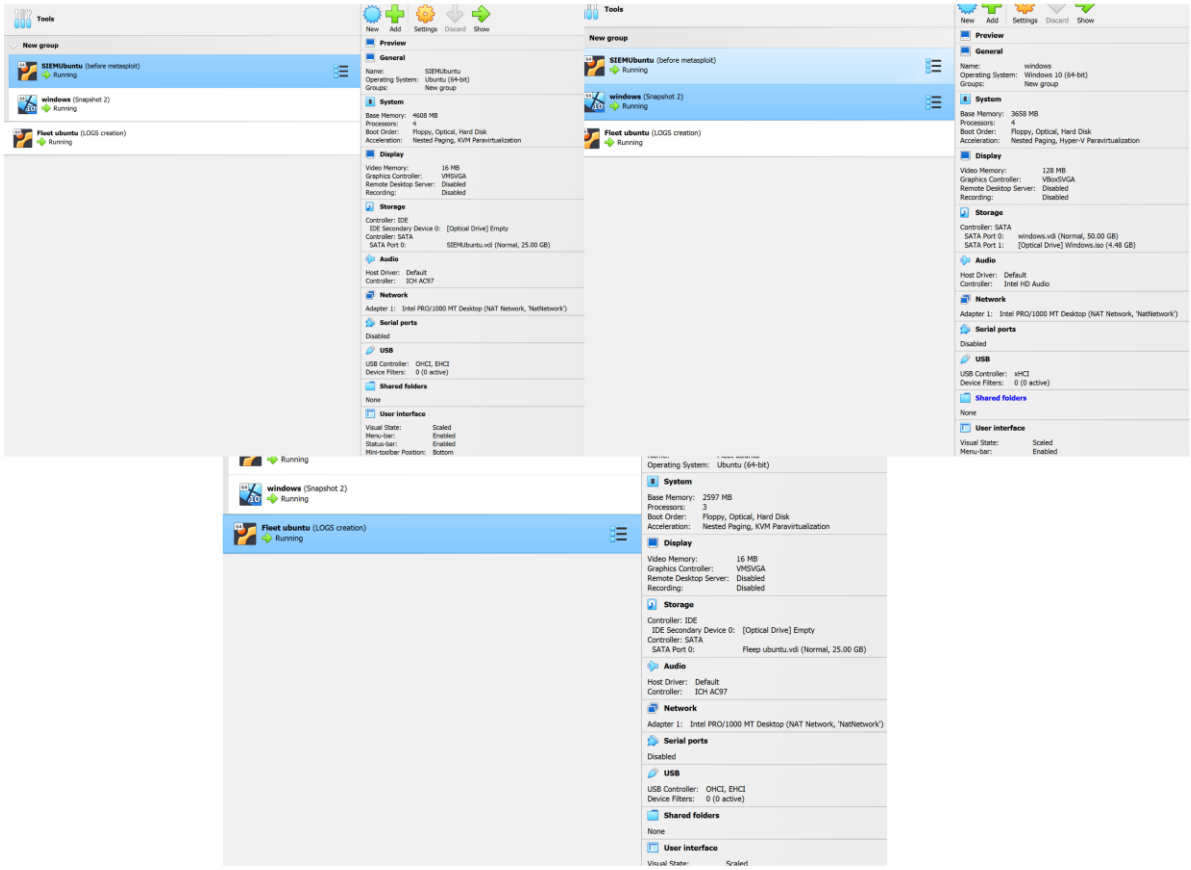
Fleet Server:

Hardware:
Base Memory:2597 MB
Processor: 3
Storage: 25 GB of free disk space
Network: Intel Pro/1000 MT Desktop(Nat Network, 'NatNetwork')
Software Dependencies:
Elastic Search and Kibana (compatible versions)
Elastic Agent installed on managed endpoints.

Windows 10 VM:

Hardware:
Base Memory:3658 MB
Processor: 4

Storage: 30 GB of free disk space
Network: Intel Pro/1000 MT Desktop (Nat Network, ‘NatNetwork’)
Software Dependencies:
Windows 10 operating system
Elastic Agent for Windows
All



Fiure1: hardware environment of ubuntu, ubuntu and windows10.

All the machines are connected in Nat network.

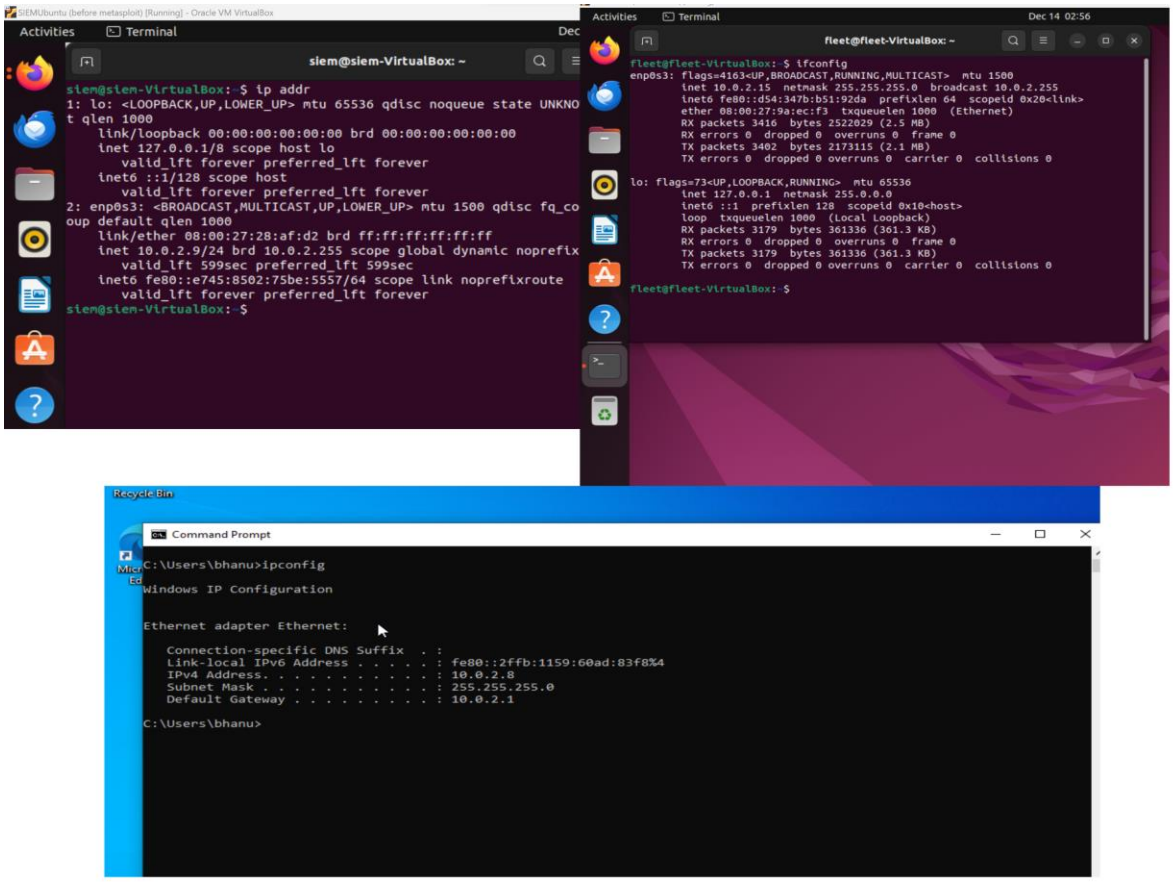


Figure : All machines are connected, with their respective IP addresses.

2 Installation

2.1 Elastic Search and Kibana

Download the OVA file, install virtualbox, Open the link
https://drive.google.com/file/d/1lXFobJOHrBvqJlVHivcLSFjNbLmoCG2k/view?usp=drive_link

Step 1 — Installing and Configuring Elasticsearch

Enter the following commands in Ubuntu 1 for installing elasticsearch, enter the elastic password provided by it.

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch |sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg
echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-8.x.list
sudo apt update
sudo apt install elasticsearch
sudo nano /etc/elasticsearch/elasticsearch.yml
sudo systemctl start elasticsearch
sudo systemctl enable elasticsearch
curl -X GET "localhost:9200"

Step 2 – Installating and configuring Kibana

After installing elasticsearch then enter this commands in ubuntu 1.
sudo apt install kibana
sudo systemctl enable kibana
sudo systemctl start kibana

The following figure is configuration file of Kibana adding encryption by generating encryption keys.

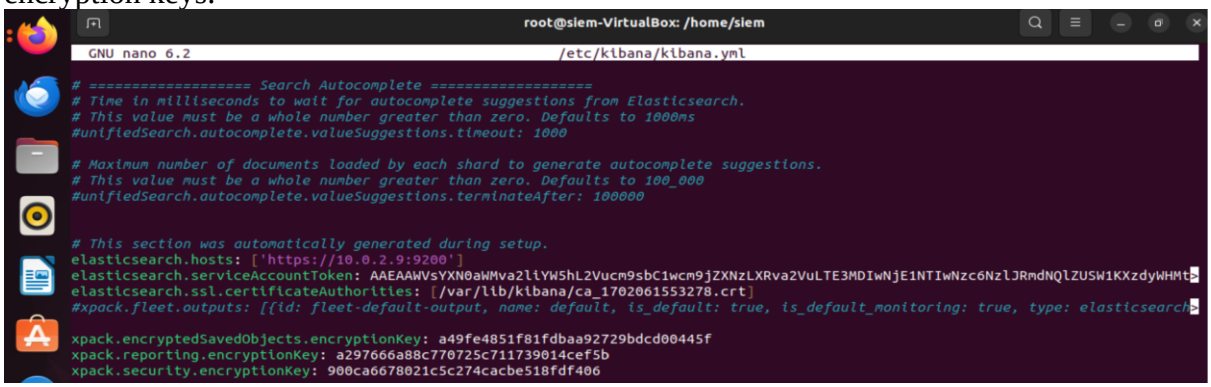
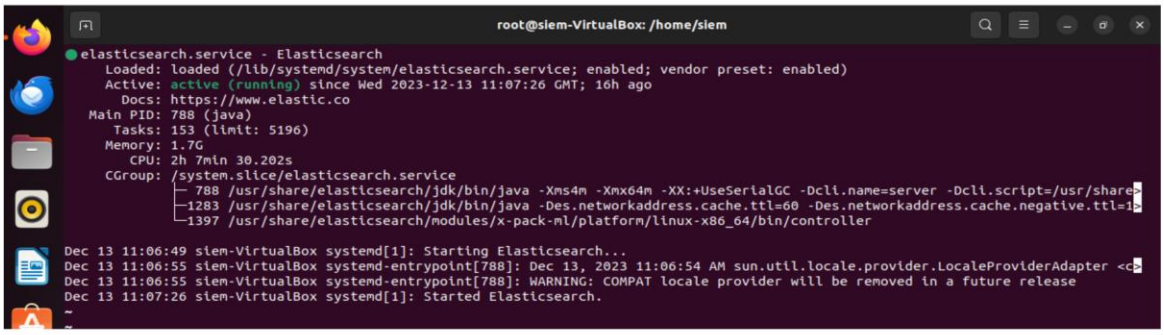


Figure 1: Kibana configuration file.
After installing above commands we can see elasticsearch and kibana are working.



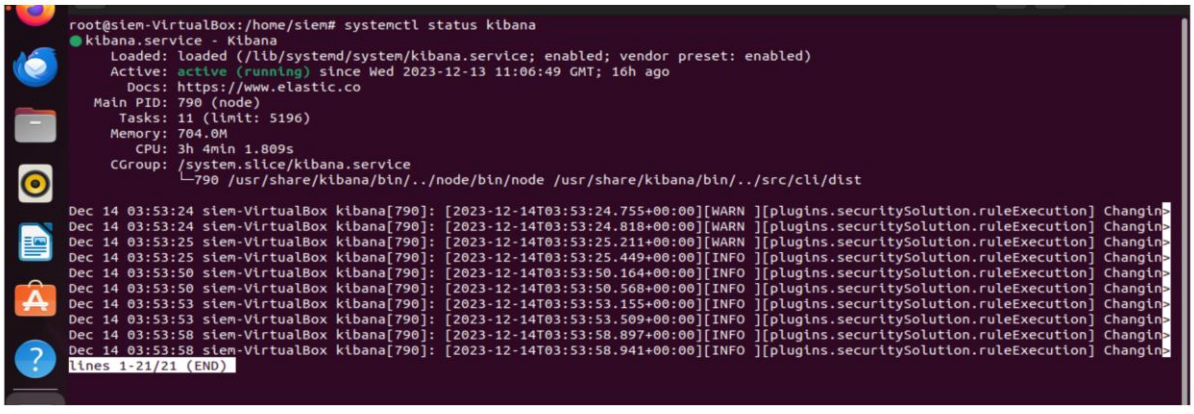


Figure 3 shows confirmation that elasticsearch and kibana are running.

2.2 Fleet Server and Fleet agent.

Download the ova file from the following link, open with virtual box, set the hardware settings are:
https://www.dropbox.com/scl/fi/2lxrvbd02zwz47lvm0lvc/Fleet-ubuntu.ova?rlkey=vprglxx36m98rdznoriml6z5n&dl=0
After entering command given by Elastic when fleet integration added and also fleet agent command in ubuntu 2
Download the ova file from the following link, open with virtual box set the hardware settings are:
https://www.dropbox.com/scl/fi/8gp7px87ilba59ix6crox/windows.ova?rlkey=e3gvlggrmi54yb9fl5f9v4pdq&dl=0
windows machine respectively. We can see both the fleet server and the windows are working in fleet management.

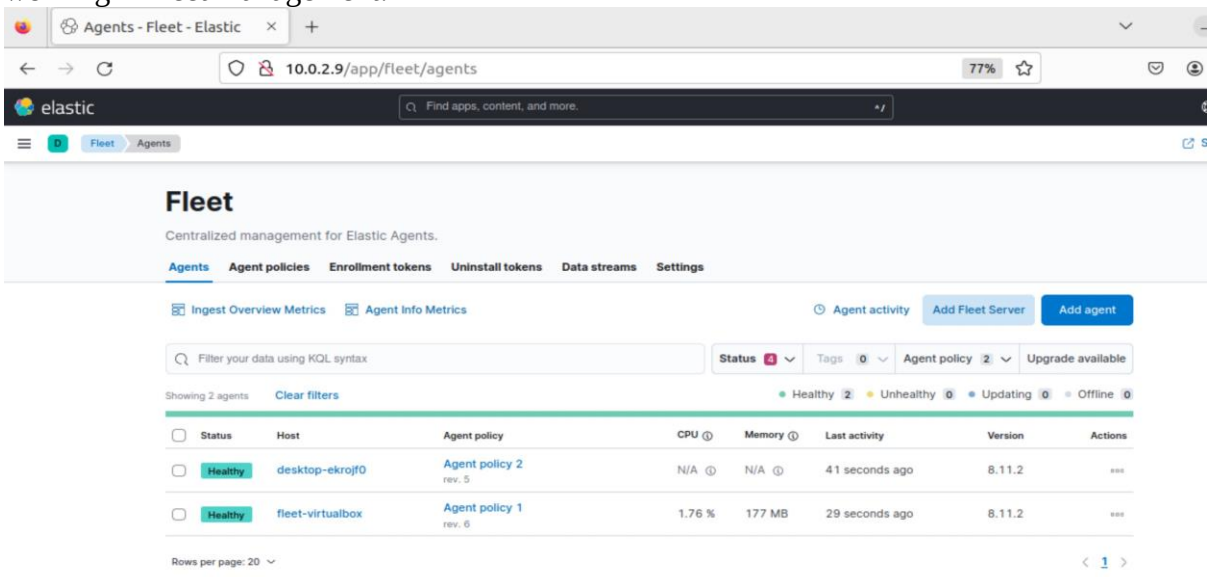


Figure: Fleet management.

3 Implementation

3.1 Integration of END POINT SECURITY, loaded prebuilt detection rules of elastic

After installation fleet, Install Integration called Endpoint Security to Elastic which enable organizations to defend against a wide range of cyber threats at the endpoint level. Elastic Endpoint Security combines features like malware prevention, threat hunting, and behavioural analytics to provide real-time threat detection and response. It's designed to strengthen overall security postures by offering a unified approach to safeguarding endpoints within an organization's IT infrastructure, loaded prebuilt detection rules of elastic Prebuilt rules in Elastic Security are predefined detection rules designed to identify common security threats or suspicious activities. To use them, you access the Kibana interface, navigate to the Security app, and load or import these rules. After loading, it's essential to review and customize them to suit your specific security needs. Activating the rules enables monitoring, and alerts are generated in response to potential security incidents, enhancing your ability to detect and respond to threats efficiently. I enabled all the windows 57 rules for windows in order to get alert.

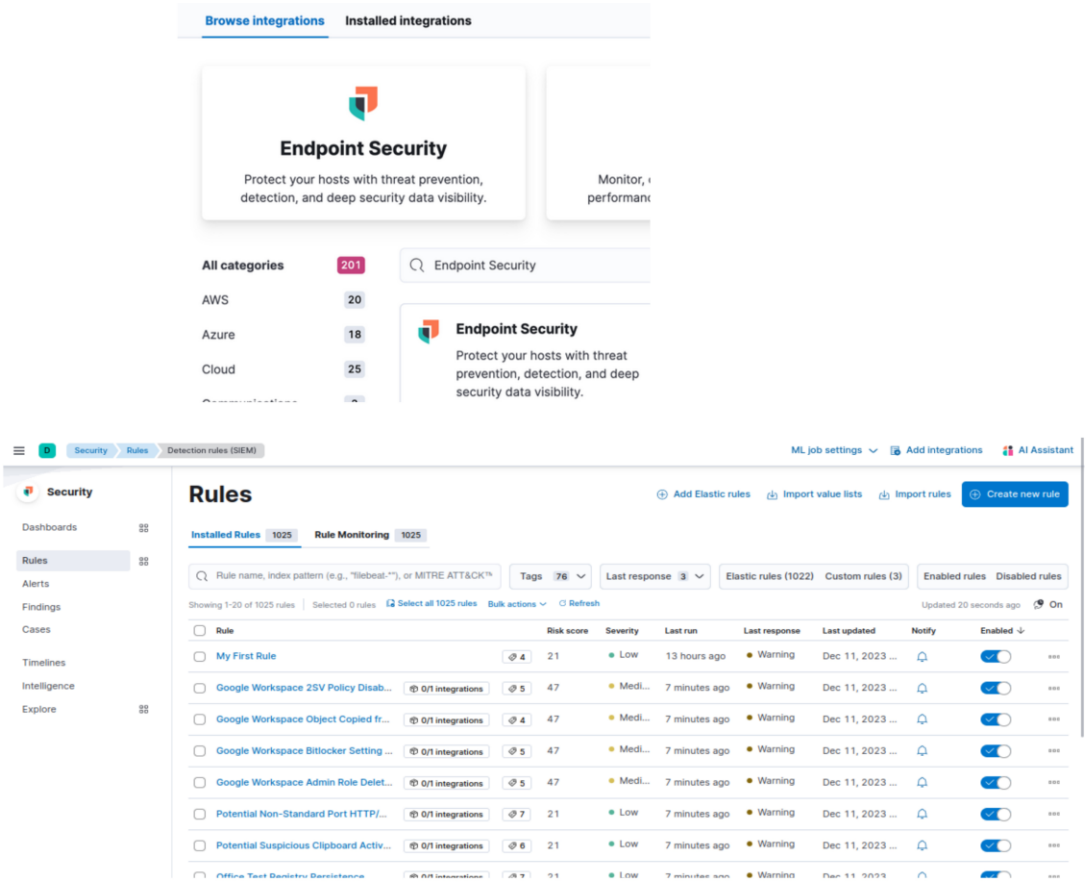


Figure: integration of endpoint secuirty and prebuilt detection rules.

3.2 Analyzing Malware Patterns

Executed different variants of malwares like emotet, trickbot, iced-id on windows vm.The whole setup until now will may or may not detect the malware, from the logs coming from windows, but to detect malwares with lesser falser positives, to add additional security I have crafted sigma rules for three different malwares like emotet, trickbot, IcedID by analysis different malwers and the extraction of Indicators of Compromise (IOCs).

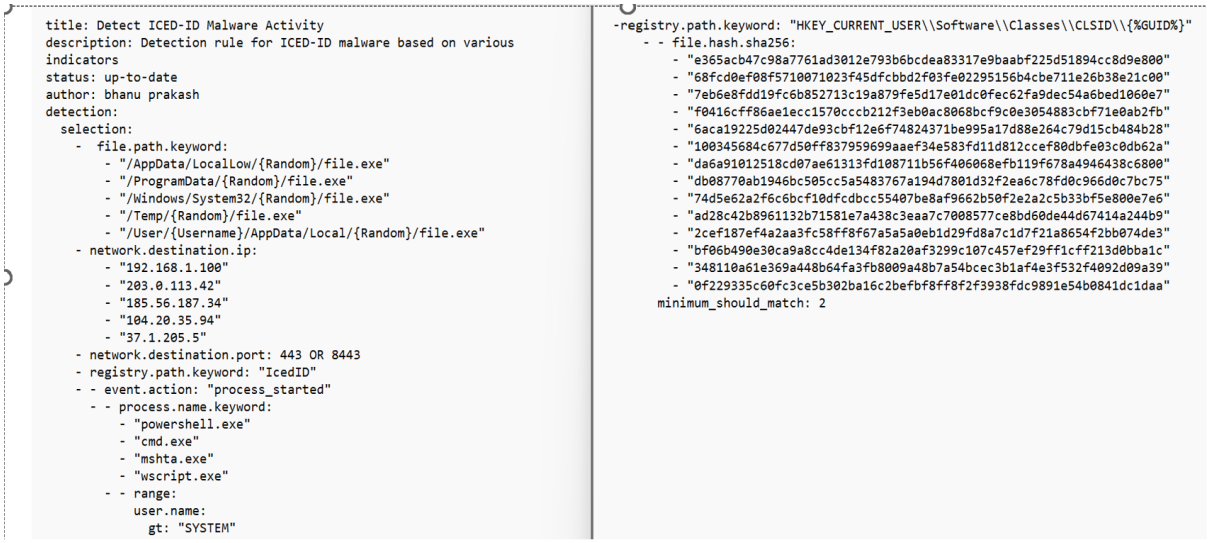
3.3 IOC HANDLING

Identified different ioc's like file path, destination.path, destination.port, event.action, process.name, file.hash.sha256, command line, powerhshell, The choice of various Indicators of Compromise (IOCs) such as file path, destination.path, destination.port, event.action, process.name, file.hash.sha256, command line, and PowerShell in crafting Sigma rules for malware is strategically aligned with the MITRE ATT&CK framework. MITRE ATT&CK provides a comprehensive matrix that categorizes adversary tactics and techniques, offering insights into the diverse ways malware can manifest and operate. By incorporating these

specific IOCs into Sigma rules, you create a rule set that covers a broad spectrum of potential malicious activities.

3.4 Crafting Sigma Rules

Sigma Rule for Iced-ID malware:



```
title: Detect ICED-ID Malware Activity
description: Detection rule for ICED-ID malware based on various
indicators
status: up-to-date
author: bhanu prakash
detection:
  selection:
    -  file.path.keyword:
        - "/AppData/LocalLow/{Random}/file.exe"
        - "/ProgramData/{Random}/file.exe"
        - "/Windows/System32/{Random}/file.exe"
        - "/Temp/{Random}/file.exe"
        - "/User/{Username}/AppData/Local/{Random}/file.exe"
    - network.destination.ip:
        - "192.168.1.100"
        - "203.0.113.42"
        - "185.56.187.34"
        - "104.20.35.94"
        - "37.1.205.5"
    - network.destination.port: 443 OR 8443
    - registry.path.keyword: "IcedID"
    - - event.action: "process_started"
      - - process.name.keyword:
          - "powershell.exe"
          - "cmd.exe"
          - "mshta.exe"
          - "wscript.exe"
        - - range:
            user.name:
              gt: "SYSTEM"
-registry.path.keyword: "HKEY_CURRENT_USER\\Software\\Classes\\CLSID\\{%GUID%}"
    - - file.hash.sha256:
        - "e365acb47c98a7761ad3012e793b6bcdea83317e9baabf225d51894cc8d9e800"
        - "68fcd0ef08f5710071023f45dfcbbd2f03fe02295156b4cbe711e26b38e21c00"
        - "7eb6e8fdd19fc6b852713c19a879fe5d17e01dc0fec62fa9dec54a6bed1060e7"
        - "f0416cff86ae1ecc1570cccb212f3eb0ac8068bcf9c0e3054883cbf71e0ab2fb"
        - "6aca19225d02447de93cbf12e6f74824371be995a17d88e264c79d15cb484b28"
        - "100345684c677d50ff837959699aaef34e583fd11d812ccef80dbfe03c0db62a"
        - "da6a91012518cd07ae61313fd108711b56f406068efb119f678a4946438c6800"
        - "db08770ab1946bc505cc5a5483767a194d7801d32f2ea6c78fd0c966d0c7bc75"
        - "74d5e62a2f6c6bcf10dfcdbcc55407be8af9662b50f2e2a2c5b33bf5e800e7e6"
        - "ad28c42b8961132b71581e7a438c3eaa7c7008577ce8bd60de44d67414a244b9"
        - "2cef187ef4a2aa3fc58ff8f67a5a5a0eb1d29fd8a7c1d7f21a8654f2bb074de3"
        - "bf06b490e30ca9a8cc4de134f82a20af3299c107c457ef29ff1cff213d0bba1c"
        - "348110a61e369a448b64fa3fb8009a48b7a54bcec3b1af4e3f532f4092d09a39"
        - "0f229335c60fc3ce5b302ba16c2befbf8ff8f2f3938fdc9891e54b0841dc1daa"
      minimum_should_match: 2
```

Sigma rule for TrickBot malware:

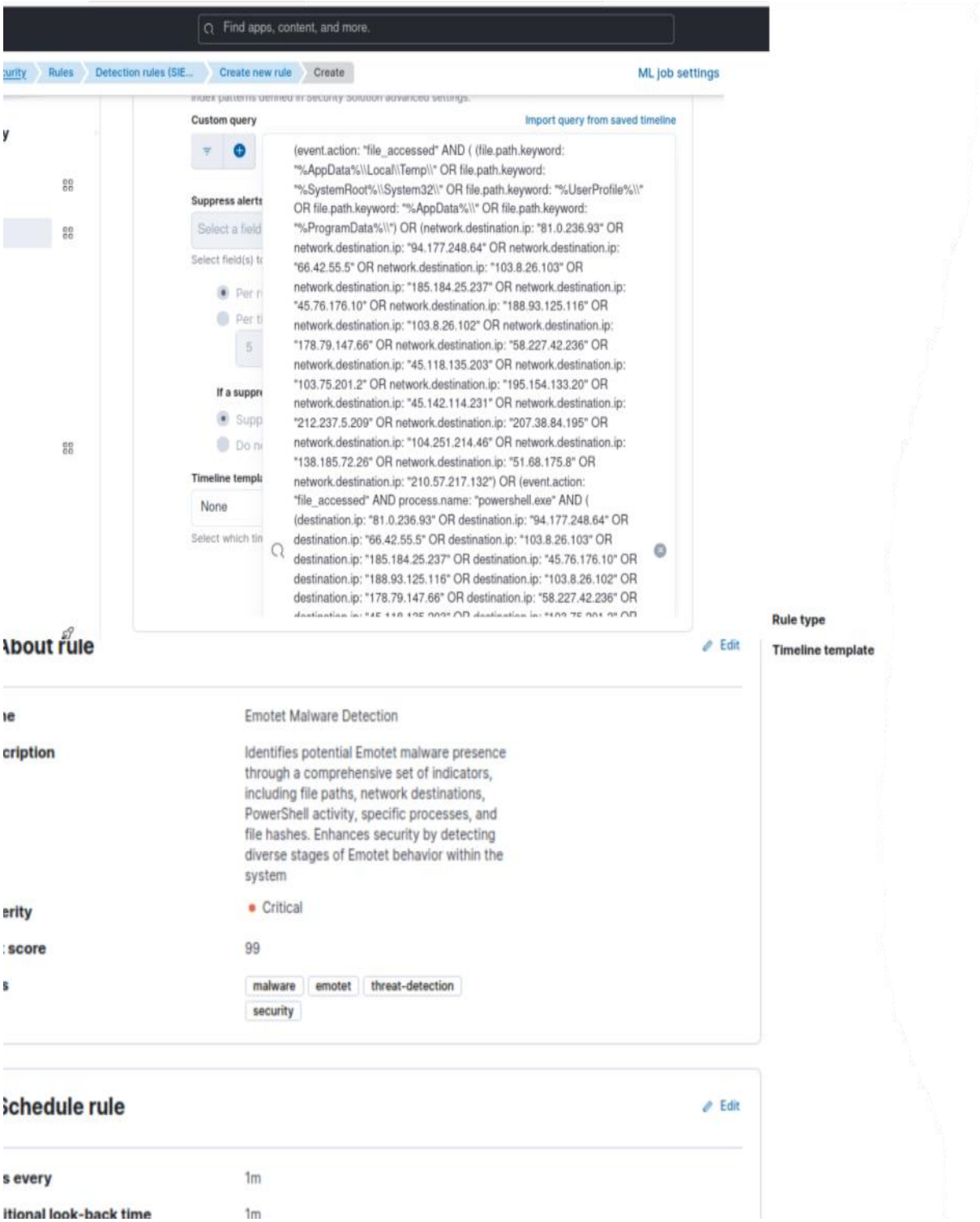
```
title: Detect TrickBot Malware Activity
description: Sigma rule for detecting TrickBot malware based on various
indicators
status: UPTO TO DATE.
author: bhanu Prakash
detection:
  selection:
    - logsource:
        category: file
        keyword: "path"
        values:
          - "%AppData%\\Local\\Temp\\"
          - "%SystemRoot%\\System32\\"
          - "%UserProfile%\\"
          - "%AppData%\\"
          - "%ProgramData%\\"
      condition: "contains"
    - logsource:
        category: network
        keyword: "destination.ip"
        values:
          - "103.207.85.8"
          - "85.101.222.222"
          - "202.134.152.129"
condition: "is"
    - logsource:
        category: registry
        keyword: "path"
        values:
          - "HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run"
          - "HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services"
          - "HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\User Shell Folders"
          -"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows"
      condition: "contains"
    - logsource:
        category: process
        keyword: "name"
        values:
          - "run32dll.exe"
          - "asdfasdf.exe"
          - "qwerty123.exe"
      condition: "is"
  condition: "2 of them"
```

Sigma rule for Emotet Malware:

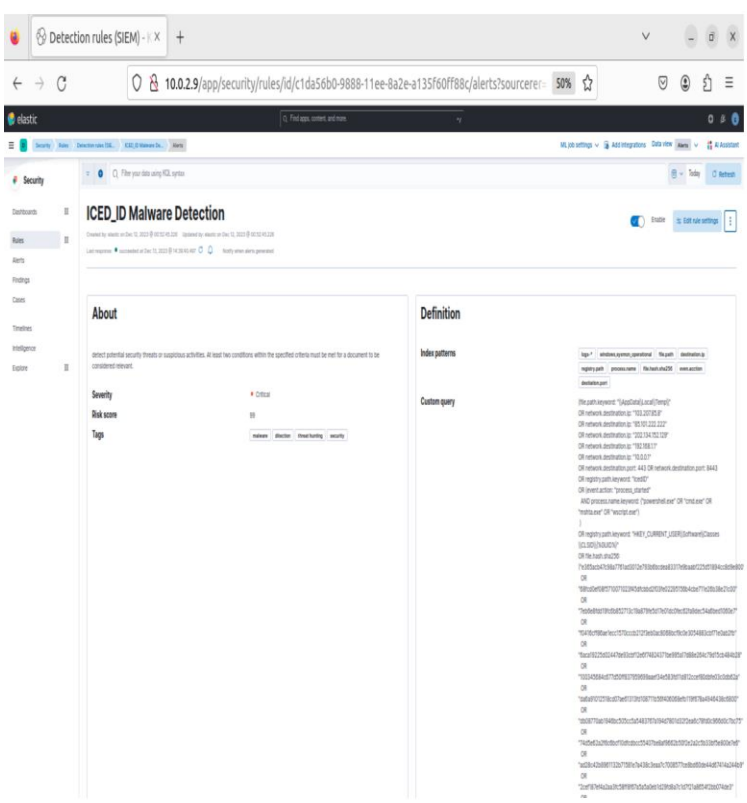
```
title: Detect Emotet Malware Activity
id: detect_emotet_activity
status: upto-to-date
description:
  Sigma rule for detecting Emotet malware based on diverse indicators.
author: Bhanu Prakash
logsource:
  category: process_creation
  product: windows
  service: null
detection:
  selection:
    - Image:
        - '*\AppData\Local\Temp\*'
        - '*\System32\*'
        - '*\*'
        - '*\AppData\*'
        - '*\ProgramData\*'
    - CommandLine|contains|all:
        - 'powershell.exe'
    - CommandLine|contains|all:
        - '-command'
        - 'iex'
        - 'downloadstring'
        - 'invoke-expression'
        - 'downloadstring'
        - 'invoke-restmethod'
    - (ParentImage|contains|all:
        - 'powershell.exe'
      AND DestinationIp|in:
        - '81.0.236.93'
        - '94.177.248.64'
        - '66.42.55.5'
        - '103.8.26.103'
        - '185.184.25.237'
        - '45.76.176.10'
        - '188.93.125.116'
        - '103.8.26.102'
        - '178.79.147.66'
        - '58.227.42.236'
        - '45.118.135.203'
        - '103.75.201.2'
        - '195.154.133.20'
        - '45.142.114.231'
        - '212.237.5.209'
        - '207.38.84.195'
        - '104.251.214.46'
        - '138.185.72.26'
        - '51.68.175.8'
        - '210.57.217.132'
    AND (ParentCommandLine|contains|all:
        - 'C:\sensitive_data\*'
        - 'D:\important_info\*'
        - '/home/user/secret/*'))
    - (ParentImage|in:
        - 'rbh4.dll'
        - 'XqxpdSzTEl.dll'
        - 'mLF68FXslK.dll'
        - 'SCygJvetwW.dll'
        - 'MHJMUoe2aN.dll'
        - '5n12AI5xgr.dll'
        - 'pOGMK5bfVw.dll'
        - 'up3R.dll'
        - '3P9.dll'
      OR Image|in:
        - 'rbh4.dll'
        - 'XqxpdSzTEl.dll'
        - 'mLF68FXslK.dll'
        - 'SCygJvetwW.dll'
        - 'MHJMUoe2aN.dll'
        - '5n12AI5xgr.dll'
        - 'pOGMK5bfVw.dll'
        - 'up3R.dll'
        - '3P9.dll')
    - (ParentImage|contains|all:
        - 'powershell.exe'
      AND File|hashes.sha256|in:
        - '05a3a84096bcdc2a5cf87d07ede96aff7fd5037679f9585fee9a227c0d9cbf51'
        - '99580385a4fef0ebba70134a3d0cb143ebe0946df148d84f9e43334ec506e301')
  condition: selection
  minimum_match: 2
```

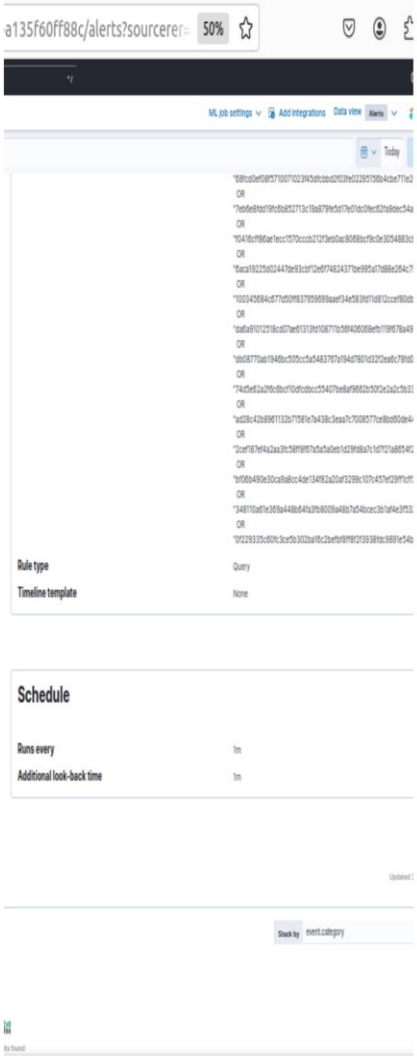
4 Integrating Sigma Rules in Elastic Stack

4.1 Integrating of Emotet malware into Elastic Stack

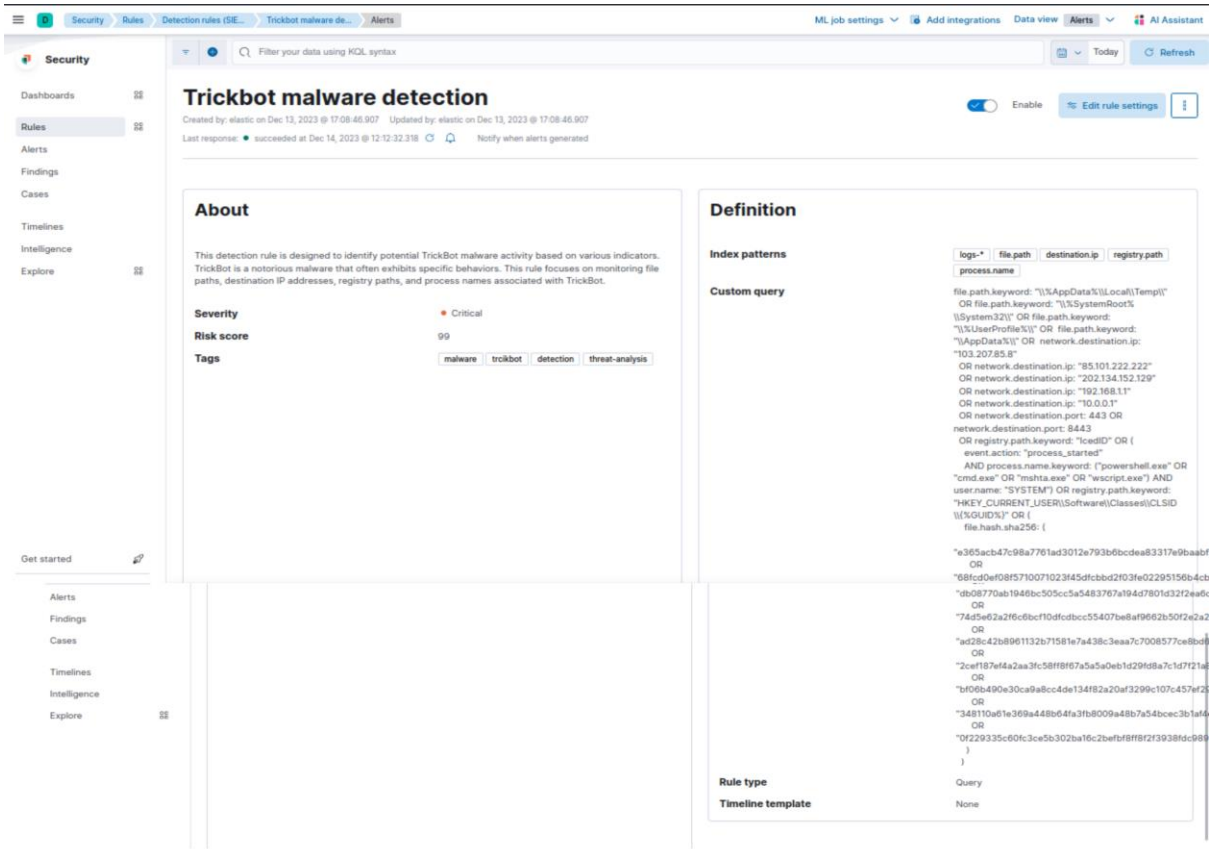


4.2 Integrating of Iced ID malware into Elastic Stack





4.3 Integrating of TRickbot malware into Elastic Stack



7. Conclusion

In conclusion, this research highlights the inadequacies of traditional security methods focused on either network or endpoint security, citing their outdated and simplistic nature. The paper introduces an innovative approach that combines proactive measures with predictive threat mechanisms to enhance detection and response speed. The proposed method, tailored for small and medium-sized businesses, integrates Elastic Search and Kibana, utilizing prebuilt detection rules from Elastic. Notably, endpoint security is integrated, and custom sigma rules are crafted for malware detection, addressing the vulnerabilities of existing security measures.

The study successfully analyzes malware attacks using techniques from the MITRE ATT&CK matrix, creating custom sigma rules and alerts in Elastic Search and Kibana. The integration of Windows Elastic Agent facilitates the collection of metrics and logs from

Windows machines, enabling the visualization of data in Kibana. The research extends to practical experimentation, executing malware in a Windows VM, and formulating sigma rules based on Indicators of Compromise (IOCs) for specific malware types such as Emotet, IcedID, and Trickbot. Furthermore, SIEM rules are integrated into Elastic Search, enhancing the overall security setup by creating rules that trigger alerts in response to identified threats. This comprehensive system, spanning both network and endpoint levels, represents a robust and effective approach to malware detection and analysis in contemporary computing environments.
Remember to include screenshots, code snippets, and examples where necessary to enhance clarity. Keep the language simple and provide clear instructions for each step.

References:

https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-22-04

https://www.elastic.co/guide/en/elasticsearch/reference/current/settings.html

https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

www.malware-traffic-analysis.net

https://youtu.be/wiQ8U5mFncw?si=gMrmKQol7v_ZhON5

https://www.youtube.com/watch?v=Ts-ofIVRMo4&t=2119s

Gorment, N.Z., Selamat, A., Cheng, L.K. and Krejcar, O. (2023). Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges and Future Directions. *IEEE Access*, pp.1–1. doi:https://doi.org/10.1109/access.2023.3256979.

Al-Shaer, R., Spring, J.M. and Christou, E. (2020). *Learning the Associations of MITRE ATT CK Adversarial Techniques*. [online] IEEE Xplore. doi:https://doi.org/10.1109/CNS48642.2020.9162207.

Muhammad, A.R., Sukarno, P. and Wardana, A.A. (2023). Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. *Procedia Computer Science*, [online] 217, pp.1406–1415. doi:https://doi.org/10.1016/j.procs.2022.12.339.

Hristov, M., Nenova, M., Iliev, G. and Avresky, D. (2021). *Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT*. [online] IEEE Xplore. doi:https://doi.org/10.1109/NCA53618.2021.9685977.