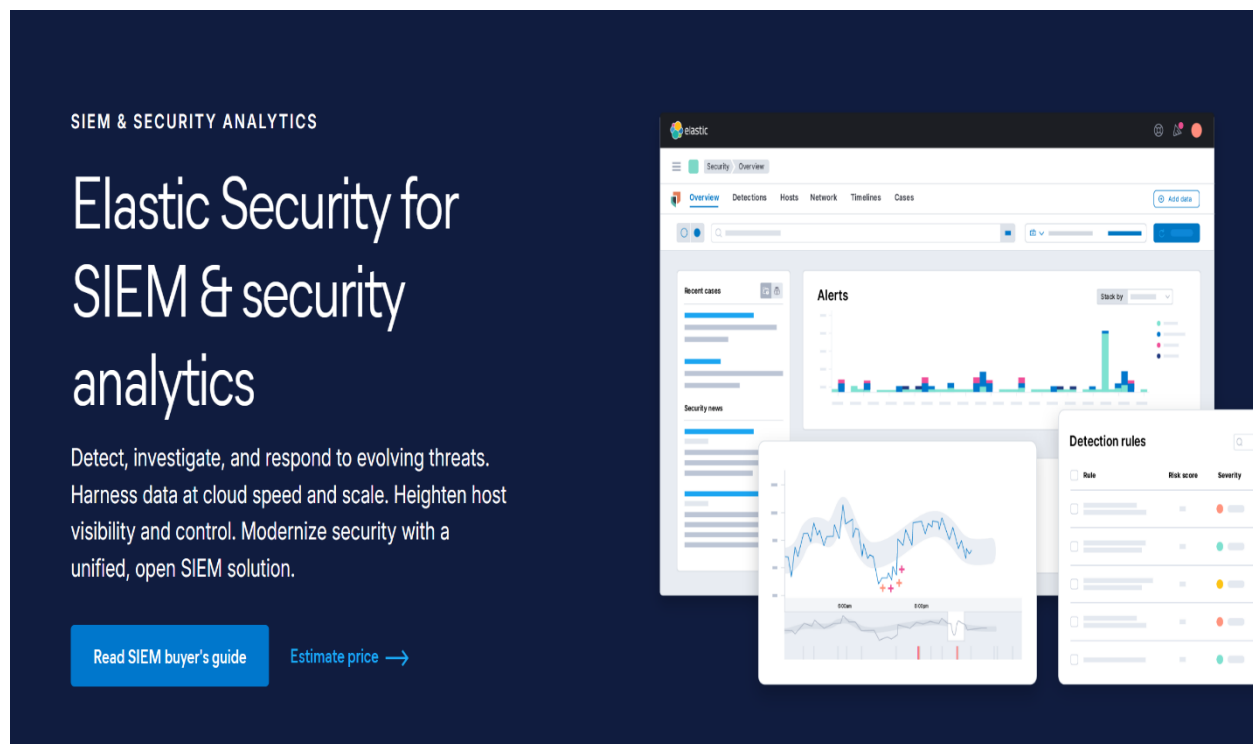


ELK

Practical Research Study: Simulating Attacks and Detection with ELK SIEM

Hands-on research experiment where you focus on compute-intensive machine learning processes and applications to monitor these processes with a SIEM. another great practical aspect in this task is also to fully behave in it, not just with reading and theatrical analysis of simulated solution.



SIEM & SECURITY ANALYTICS

Elastic Security for SIEM & security analytics

Detect, investigate, and respond to evolving threats. Harness data at cloud speed and scale. Heighten host visibility and control. Modernize security with a unified, open SIEM solution.

[Read SIEM buyer's guide](#) [Estimate price →](#)

The advertisement features a dark blue background with white text. On the right side, there is a screenshot of the Elastic Security interface. The interface includes a top navigation bar with 'Security' and 'Overview' tabs. Below this, there are several panels: 'Recent cases' on the left, 'Alerts' in the center with a bar chart, and 'Detection rules' on the right with a table. A smaller inset window shows a line graph with a blue line and red markers. The 'Detection rules' table has columns for 'Rule', 'Risk score', and 'Severity'.

Rule	Risk score	Severity
[Rule Name]	[Risk Score]	[Severity]
[Rule Name]	[Risk Score]	[Severity]
[Rule Name]	[Risk Score]	[Severity]
[Rule Name]	[Risk Score]	[Severity]
[Rule Name]	[Risk Score]	[Severity]

Table of Contents

1. Introduction-----	1
• Overview and Objectives-----	2
2. Infrastructure Setup and Research-----	3
2.1. ELK Server Setup-----	4
3. - Cloud Trial Signup and Deployment-----	5
Accessing the Dashboard -----	6
4. 2.2. Windows Server Configuration -----	7
Sysmon Installation and Configuration -----	8
5. - - ELK Agent Deployment - Auditing Logs Settings-----	9
6. Attack Execution -----	10
7. 3.1. Registry Edits -----	11
8. 3.2. Run Tool Execution -----	12
9. 3.3. Ping-----	13
10. Ping and Netcat Attacks-----	14
11. Attack Identification-----	15
12. 4.1. Monitoring Sysmon Logs -----	16
13. 4.2. Detection of Attacks-----	17
14. 4.3. Exploiting Vulnerabilities-----	18
15. Conclusion-----	20

Lab Scenario:

In the lab, we are going to find out how to detect and simulate `attack using ELK SIEM. First of all, we will design the framework and implement ELK stack in a cloud environment and then configure a windows machine to be the target. Thus, we'll go and install and configure Sysmon to be running effectively. Having the frame worked, we'll conduct faked attacks for instance registry editing and pinging to identify our system's reactions. By means of ELK utilization, we can respond to any fraud case immediately to keep a high level of security of our automated system.

Infrastructure Setup and Configuration

The setup system entails deploying the ELK server on a cloud platform, configuring a Windows as the attack goal, installing Sysmon, deploying ELK agents, each step is meticulously detailed to make sure replicability and accuracy.

ELK Server Deployment

Begin by signing up for the ELK SIEM cloud trial using your email. This allows you to access ELK's cloud-based services for security monitoring and threat detection. Later we can deploy our own server on site or purchase plans to fully access the capabilities of SIEM solution. This provides clear visualization of security posture.

Cloud Trial Signup and Deployment:

For having the trial of ELK Cloud, you are required to give required information for verification first. To get started, enter your email address that will be the main contact for your account where you will receive messages regarding your account.

Deployment completed on trial version:

The Trial version enables us to practice the siem capabilities and test them first on the pre-configured envorment do that we can practice out labs and after that we can purchase or deploy our own siem solution for now we are going with the trial version. Then, installing the ELK server on the platform of choice is a necessary step. Such implies to be configured by

the relevant settings and resources to be allocated in order to have that secure hosting.

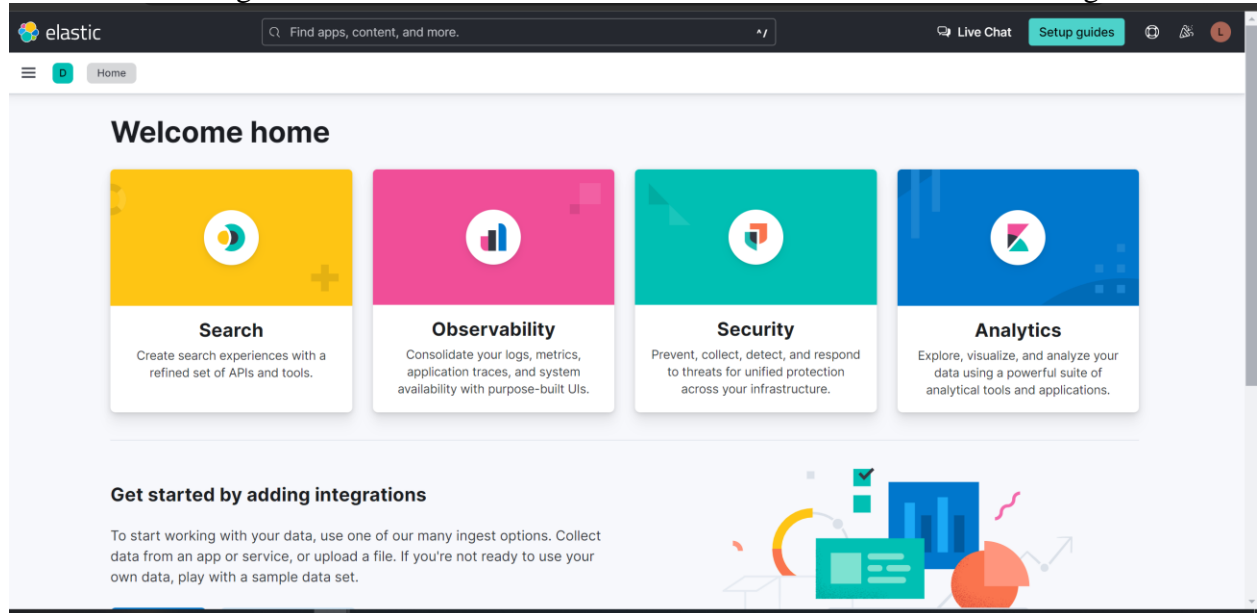


Figure-1 Signing up for ELK Server

Setting Operating system Windows:

The process of tuning VMS to be a target for simulated attacks includes setting required configurations on the server and ensuring its access within the virtualized environment. Much like the operation of a ELK on Windows, configuring the required settings as well as attaining the proper accessibility of the designated environment are parts of the setup of an ELK engine.

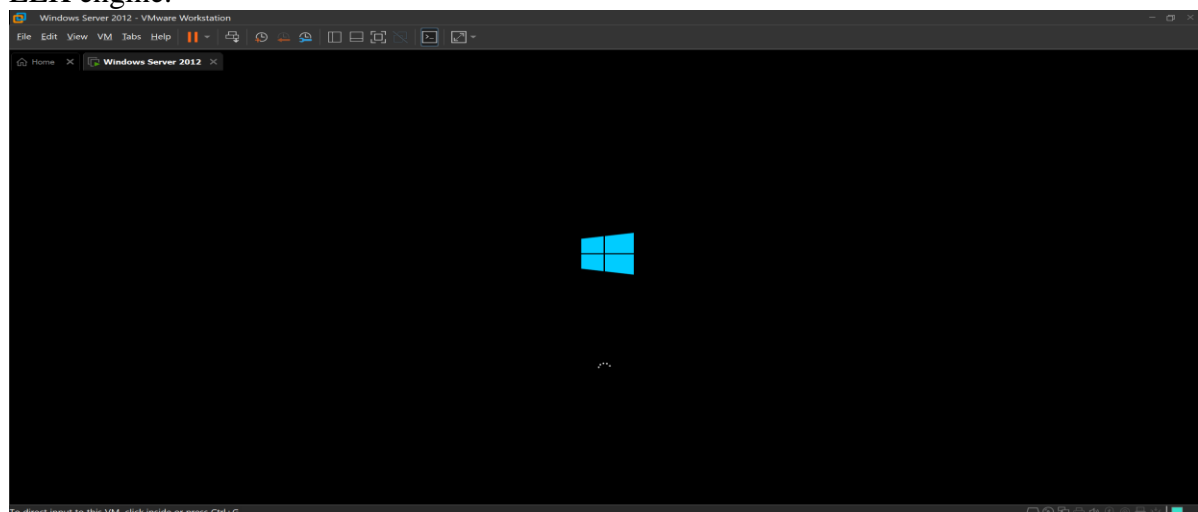
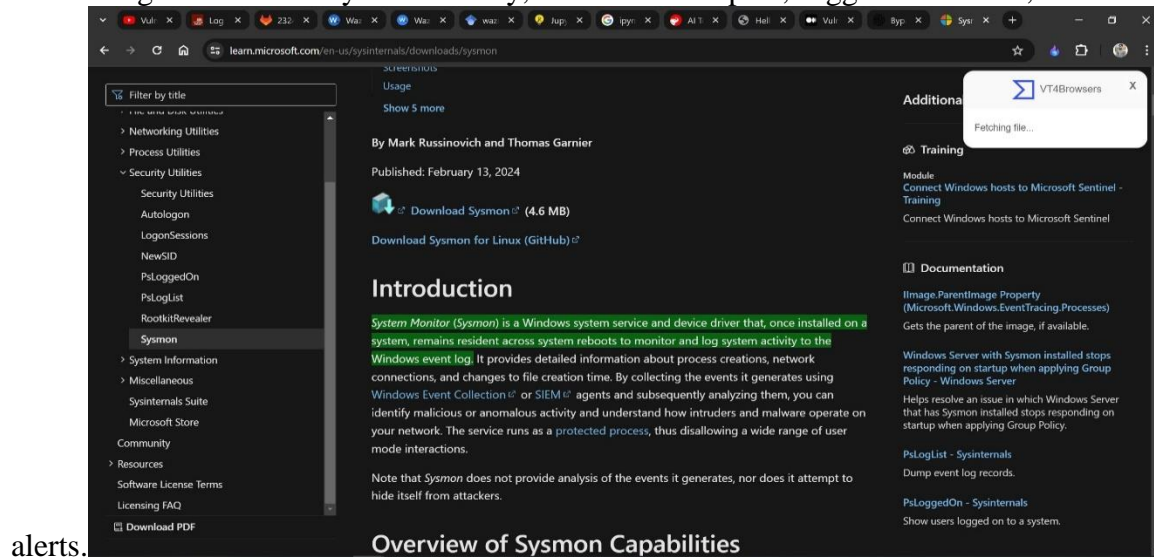


Figure-2 Power On Windows

Powering up Windows and running:

Having successfully put server on place, the Windows server booting is completed indicating readiness for cyber security trainings which aim to destroy the system.

Installing Sysmon in Windows for Logs collection: On the Windows Server, deploy Sysmon tool that captures process creation logs, network connection logs, and system-level event logs. This outstanding assistance extends the server's functioning capacity because it allows monitoring of the whole system activity, discovers hot spots, suggests antivirus, and malware



alerts.

Overview of Sysmon Capabilities

Figure-3 Downloading sysmon

Configuring Sysmon for logs collection:

While configuring Sysmon on the Windows Server, paying meticulous attention to settings is required so as to feature those security events that are in line with the specific data requirement of the research study. Such an activity requires as much optimization as possible in the way of event filtering, logging options and other settings to increase detection rate.

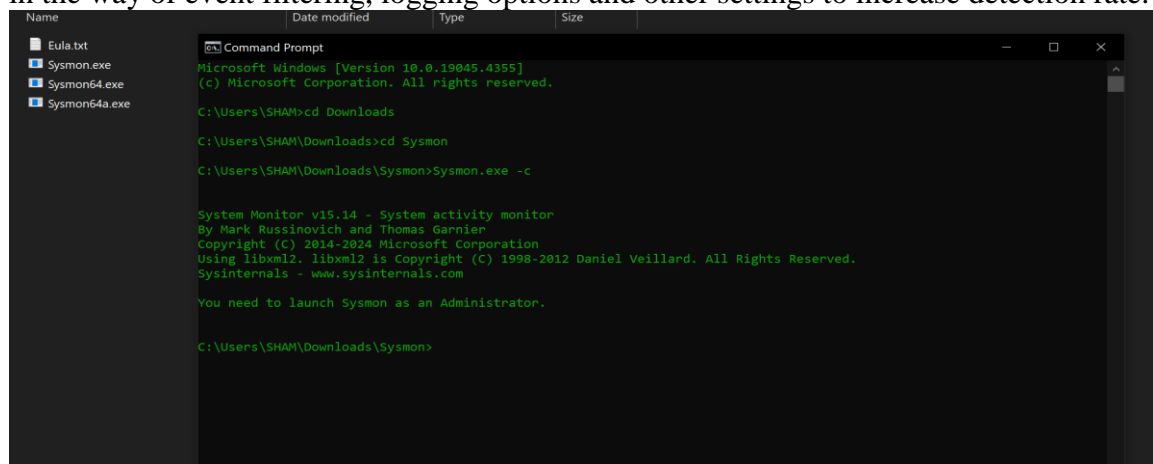


Figure-4 Installing and Configuring Sysmon

Starting service for Sysmon:

Sysmon configuration next, perform the necessary changes and then activate the Sysmon service on the Windows Server to get event data security capture on. This piece is the entry

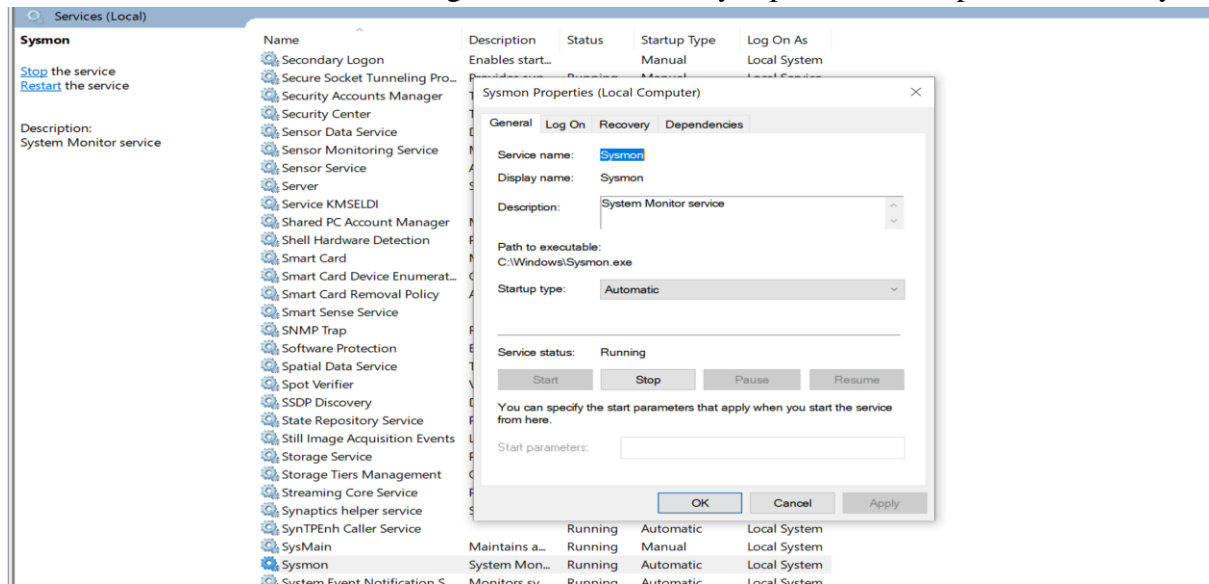


Figure-5 Starting Sysmon Service

Adding agent:

To enhance monitoring capabilities, add agents to the ELK environment. Agents are installed on individual systems and send security-related data to the ELK server for analysis and detection.

On Windows server:

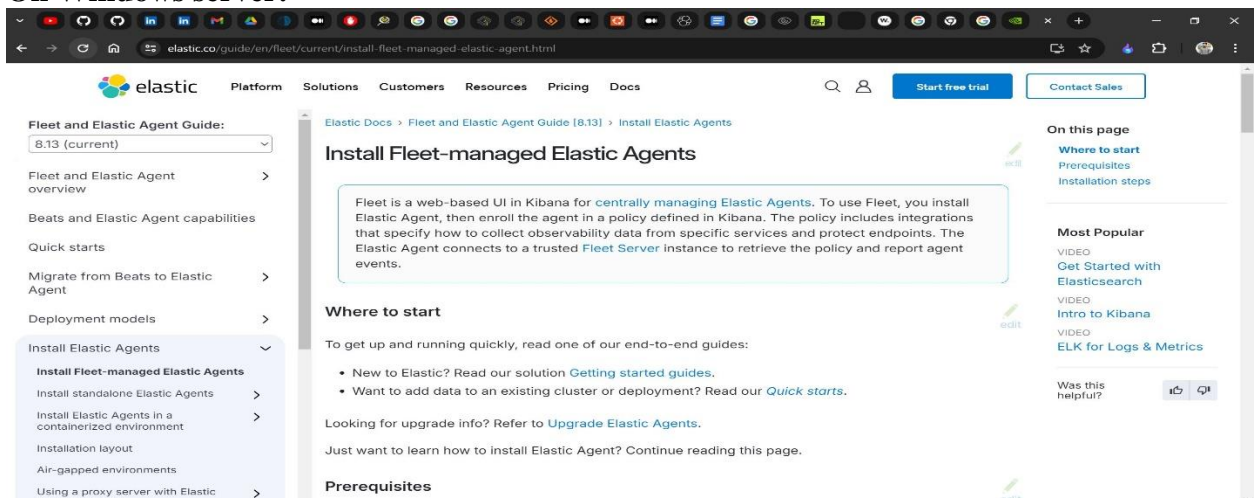


Figure-6 Agent Downloading and Installisation

PowerShell command to install agent on end point:

Executing commands that are provided on the agent deployment page to properly communicate with server. This process includes logs collection and sharing with the server. There logs are further security monitoring.

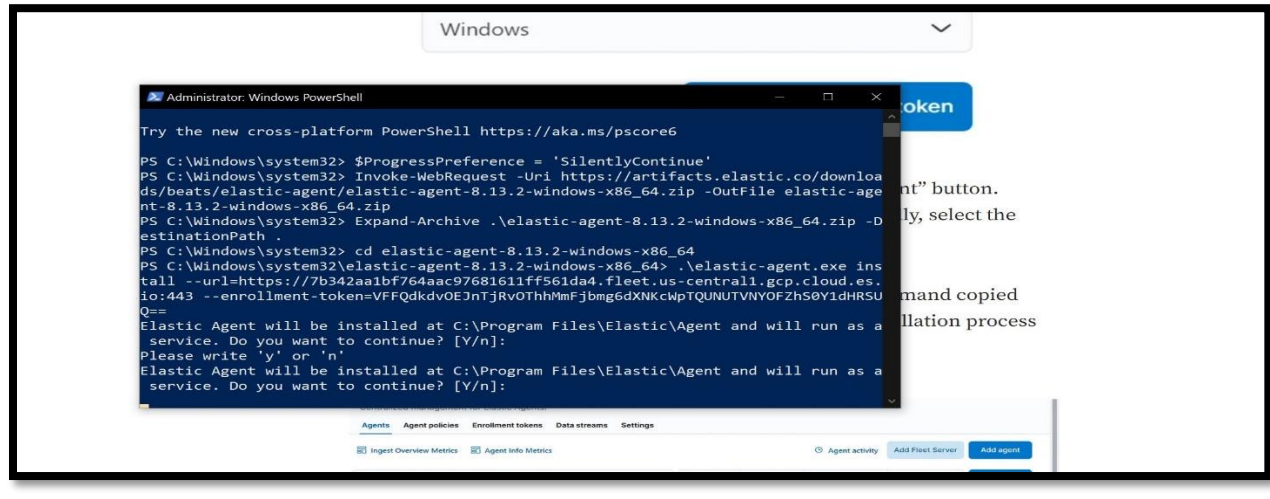
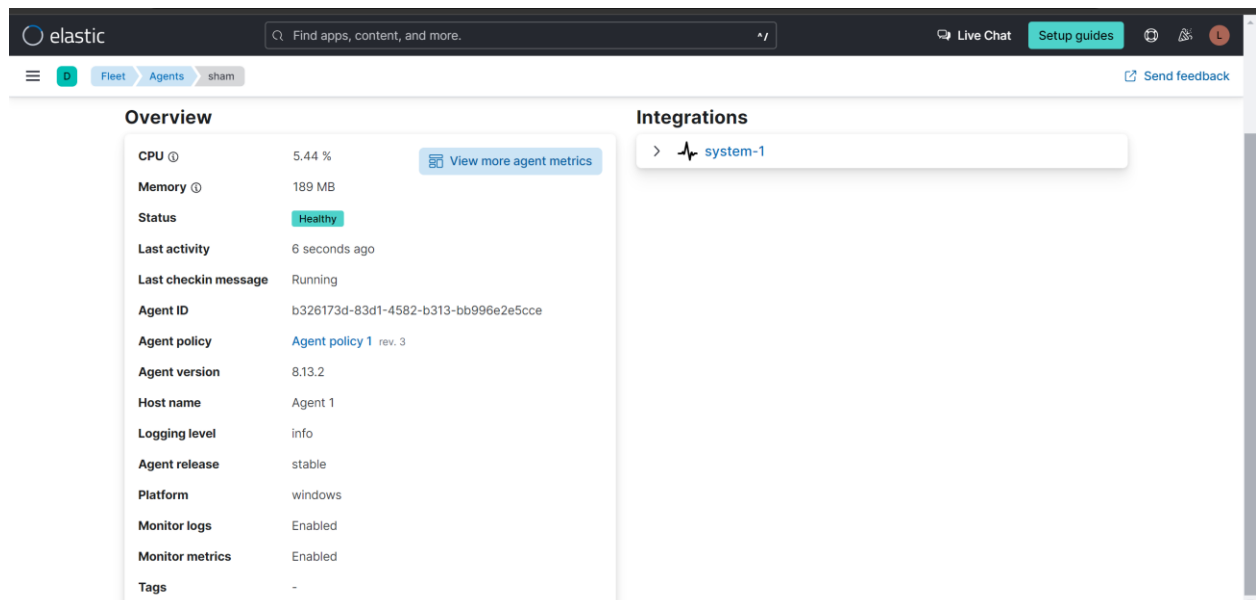


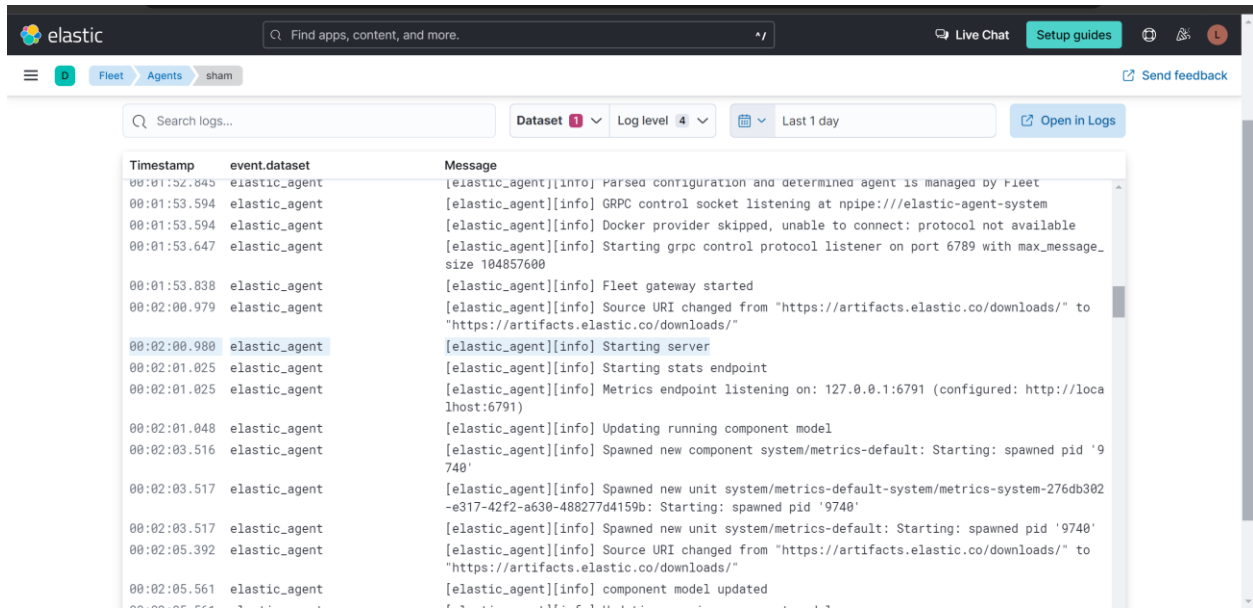
Figure-7 PowerShell command to Activate Agent

Successfully Deployed Agent:



After successfully executing the script to deploy agent we can Verify that the agent deployment process was successful and the Windows Server is now actively sending security event data to the ELK server. Making sure to check the deployment logs and services

Figure-9 Verifying Agent connectivity



Figur-10 showing logs status

Auditing logs settings:

Configure auditing settings on the Windows Server to ensure that relevant security events are logged and available for analysis by the ELK server. Auditing involves making changes to configuration file to collect logs that are related to security and errors directly tramisated to SIEM solution deployed in network or on cloud.

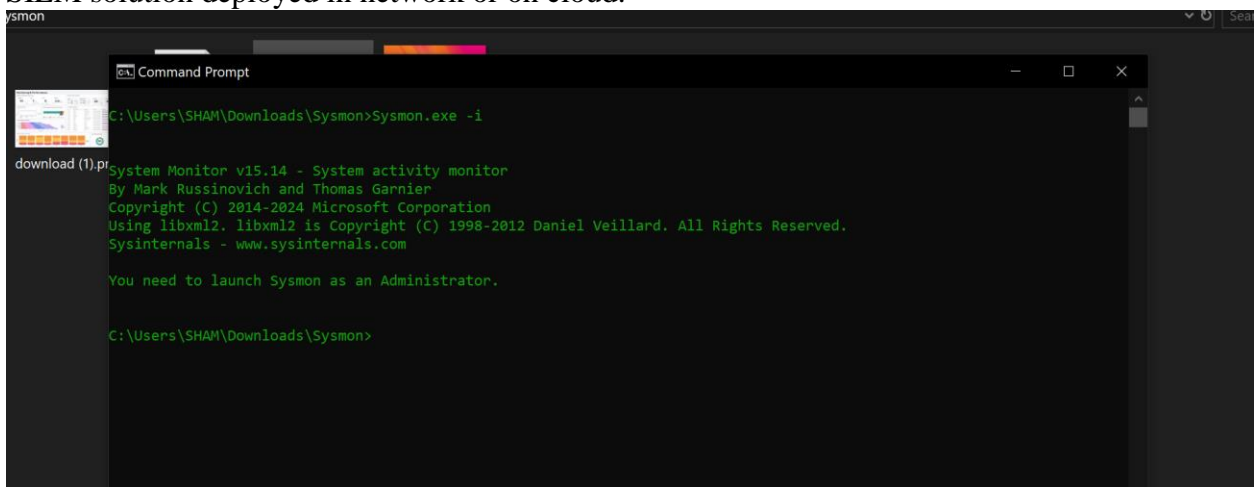


Figure-11 Configuring Sysmon

Attack execution (15 Marks)

Various assault techniques, together with registry edits, utilizing the Run device, and executing Ping, Nmap, and Netcat assaults at the Windows Server, are finished within the virtualized surroundings. These simulated assaults simulate actual-world threats, taking into consideration comprehensive assessment of detection and reaction competencies.

Registry edits:

Manipulate registry settings on the Windows Server to simulate unauthorized changes or modifications that could be indicative of malicious activity. The Windows registry stores crucial system configurations and settings, and unauthorized edits can have significant security implications.

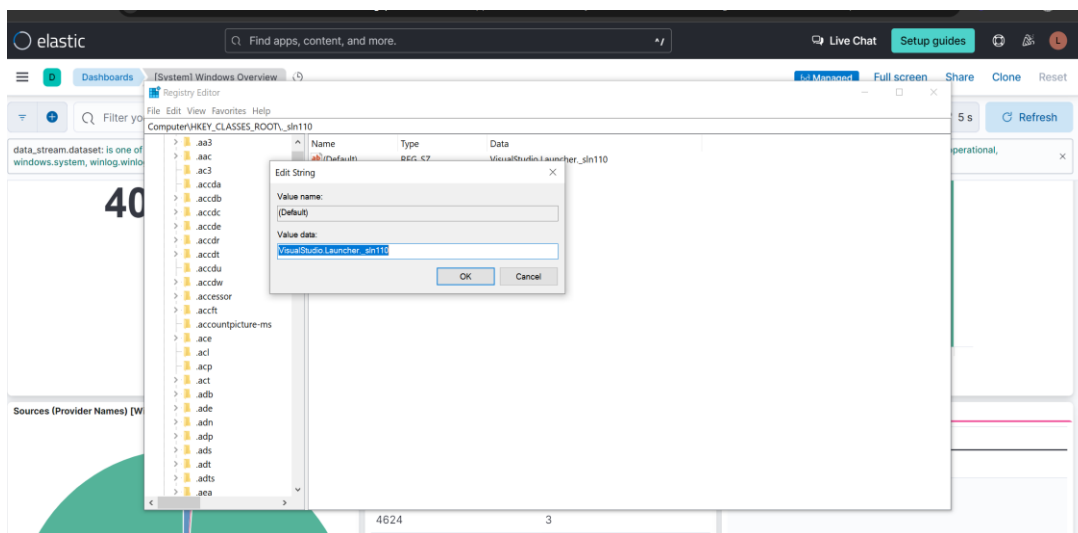


Figure-12 Editing Registry

Run:

Using Run tool to starting programs and executables that can be monitored on dashboard.

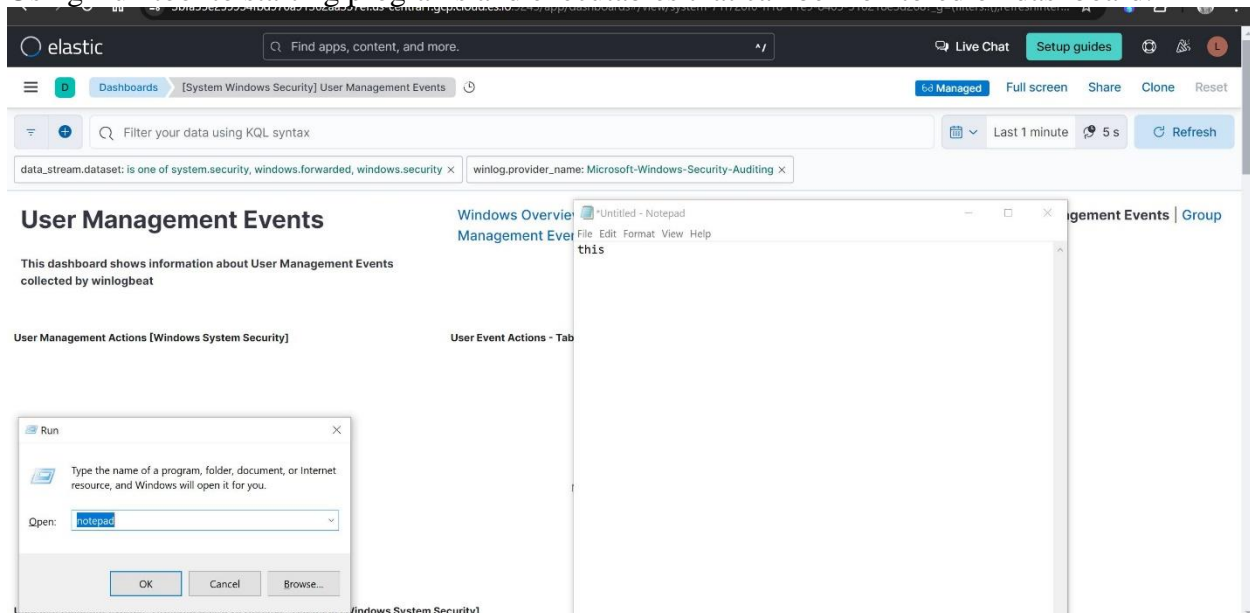


Figure-14 Opening programs

- **Ping**

Ping is the Networking tool that is used to check the connectivity to the end point over the network. We can use this tool to check the presence of device and it also generated alerts that can be monitored on dashboard.

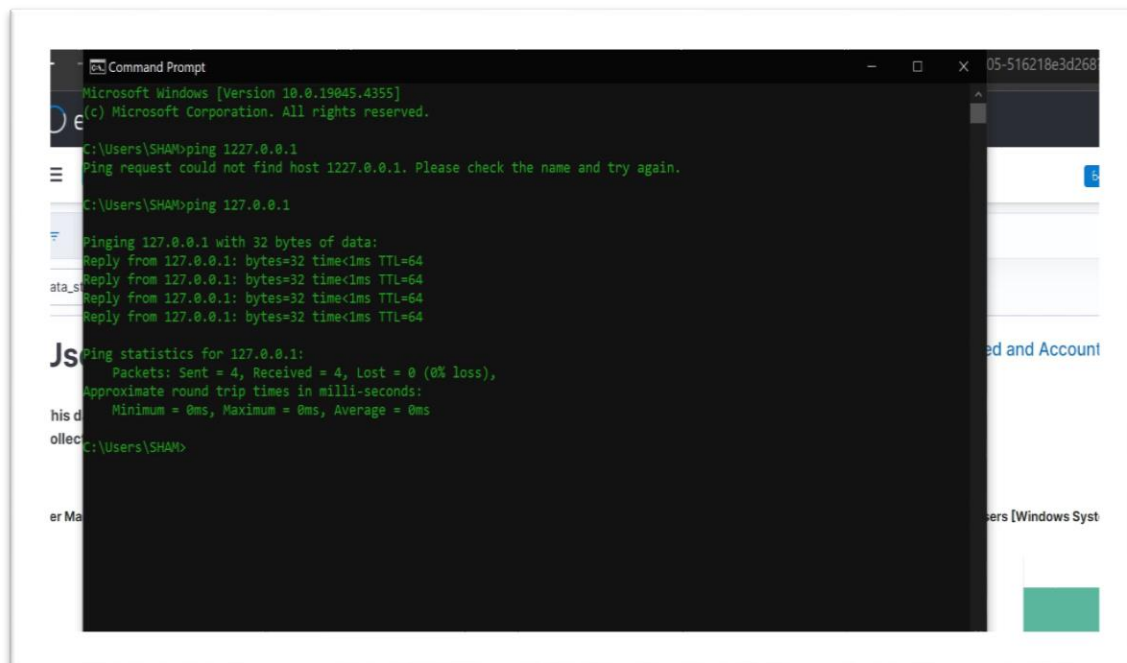


Figure-15 Ping Network

Attack Identification (15 Marks)

The part dedicated to the realization of the presence of the capacity attacks is professionalized in real-time. Through the investigation of Sysmon logs for unusual procedures and by using ELK's capabilities, the exam objectives are attaining and answering the attacks early, consequently preventing massive damages and strengthening the system's robustness.

Sysmon Suspicious process:

Run logs using ELK on Windows Server to look out for activities or susceptible processes which could be the initiation of security attacks. This means revealing of abnormal outcomes like creation of unnecessary processes, unauthorized access attempts as well as any operation that is not normal.

Detections:

Detection part involves detecting the logs that are generated by Sysmon. These detections can be visualized by the kibana dashboard for better understandings and smooth security monitoring. It is best practices to make visuals of logs as there are thousands of logs that can be very challenging for security analyst to monitor and higher chances of false positives.

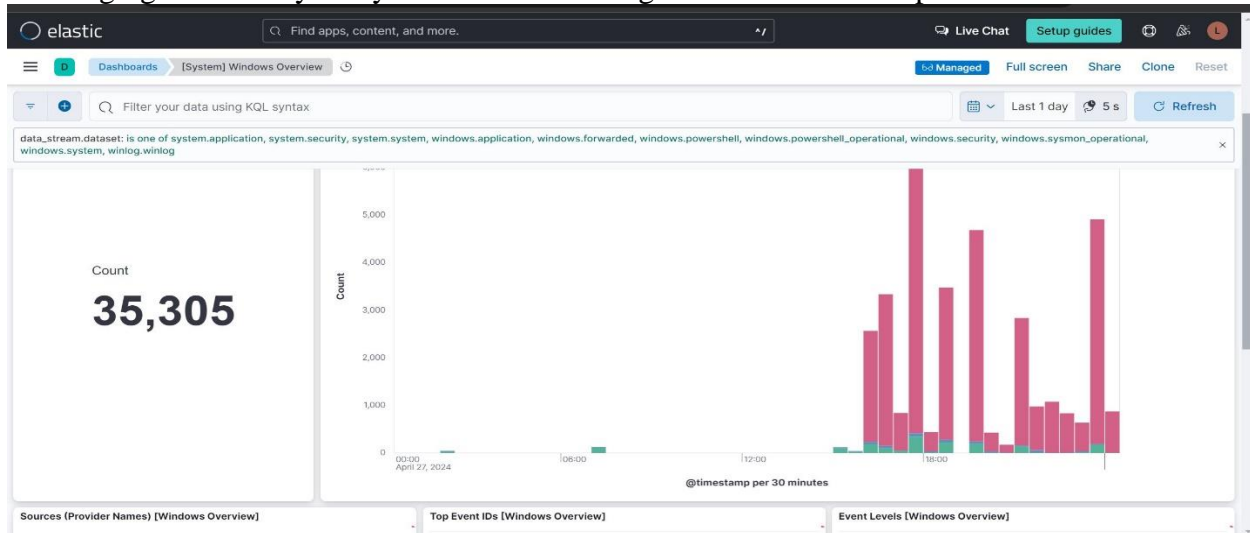


Figure-16 Sysmon Events

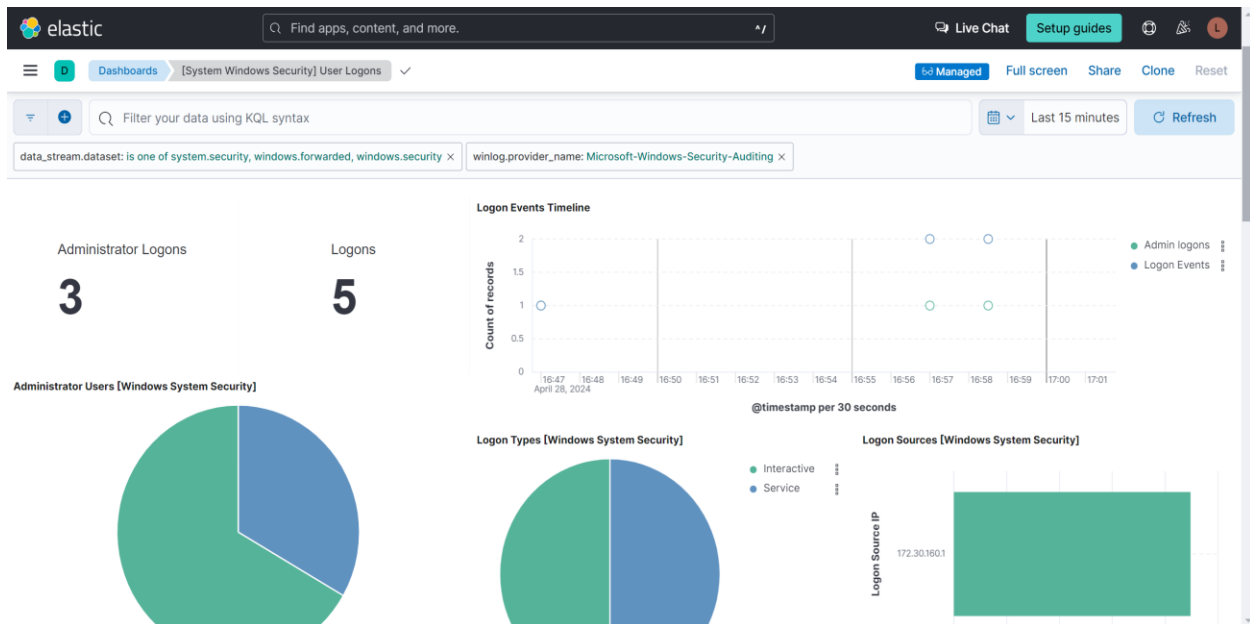


Figure-17 Dashboard Visuals

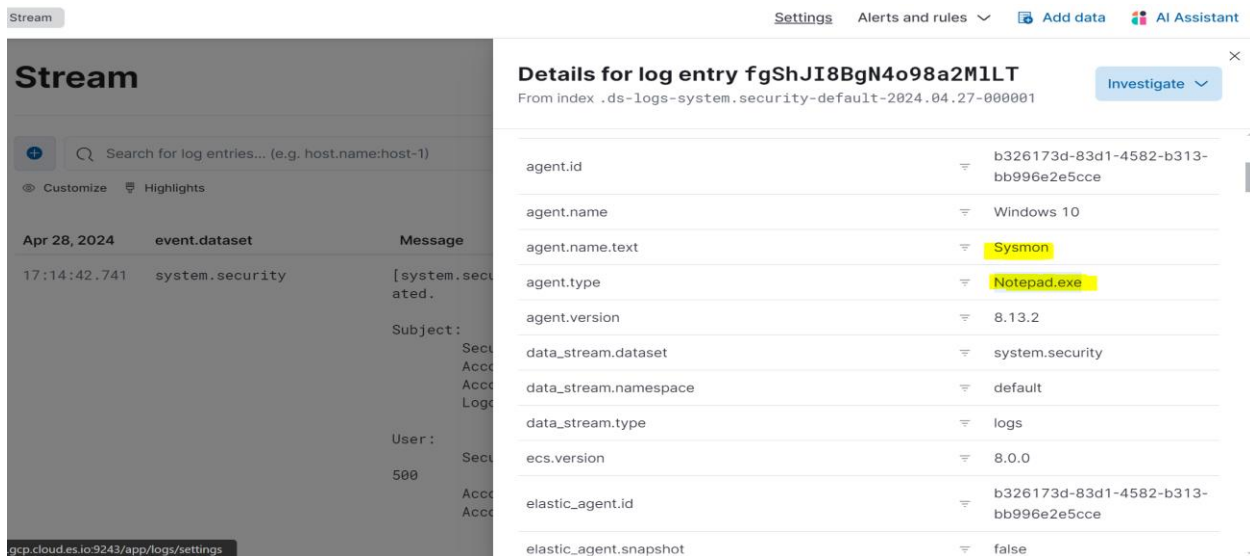


Figure: 18 Notepad started

Settings Alerts and rules ▾ Add data AI Assistant

Details for log entry fgShJI8BgN4o98a2M1LT

From index .ds-logs-system.security-default-2024.04.27-000001

Investigate ▾

agent.id	bb996e2e5cce
agent.name	Windows 10
agent.name.text	Sysmon
agent.type	Registry Modification
agent.version	8.13.2
data_stream.dataset	system.security
data_stream.namespace	default
data_stream.type	Unauthorized registry modification detected
ecs.version	8.0.0
affected_registry_key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Figure: 19 Registry Edit Log Detected

Alerts Mitigation

For registry edits, get right of entry to controls and audit rules had been implemented to display modifications and unexpectedly identify unauthorized changes. To deal with dangers associated with ping operations, network segmentation and firewall rules had been employed to restriction ICMP traffic completely to legal assets. Additionally, Sysmon became configured to screen ICMP activities and generate indicators for any unusual styles or immoderate pinging, enabling proactive response measures. Regarding the detection of uncommon software openings, software whitelisting techniques were deployed to allow best accepted software program to execute on the gadget. Any attempt to launch unauthorized packages induced on the spot indicators, facilitating speedy research and remediation

Conclusion:

In precis, our research task crew adeptly implemented a virtualized environment proposing key components: the ELK server, Windows Server equipped with Sysmon, and an Application for simulating log generation. Throughout our endeavor, we centered on growing logs from activities such as registry edits, ping operations, and application openings, without conducting any malicious assaults. we efficiently achieved real-time detection of those events and directly answered to any anomalies within our virtual surroundings

Referencing:

The references section provides a comprehensive list of all mentioned assets, allowing further exploration and verification of the study's claims and methodologies. These resources serve as valuable supplements for interested readers and researchers, aiding in a deeper understanding of the subject matter.

1. Hristov, M., Nenova, M., Iliev, G. and Avresky, D., 2021, November. Integration of ELK Enterprise SIEM for DDoS Attack Detection in IoT. In 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA) (pp. 1-5). IEEE.
2. Al-Duwairi, B., Al-Kahla, W., AlRefai, M.A., Abedalqader, Y., Rawash, A. and Fahmawi, R., 2020. SIEM-based detection and mitigation of IoT-botnet DDoS attacks. International Journal of Electrical and Computer Engineering, 10(2), p.2182.
3. Sheeraz, M., Paracha, M.A., Haque, M.U., Durad, M.H., Mohsin, S.M., Band, S.S. and Mosavi, A., 2023. Effective security monitoring using efficient SIEM architecture. Hum.-Centric Comput. Inf. Sci, 13, pp.1-18.
4. Vazao, A., Santos, L., Oliveira, A. and Rabadao, C., 2021, June. A gdpr compliant siem solution. In European Conference on Cyber Warfare and Security (pp. 440-XIV). Academic Conferences International Limited.