iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60266

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Improving Threat Detection with Elastic Stack based Security Information and Event Management

Suraj Regi[1], Dr. Gurpreet Kaur[2]
[1]*Amity Institute of Information and Technology, Amity University, Noida*
[2]*Assistant Professor, Amity Institute of Information and Technology, Amity University, Noida*

Abstract: ***In this digital era, where most businesses are transitioning from traditional to digital data storage methods, attackers are continuously developing new techniques and tools to target these systems. Security Information and Event Management (SIEM) systems have emerged as essential tools, providing a centralized platform for efficiently gathering and analyzing data to detect security breaches. This paper aims to explore an enhanced threat detection approach within the SIEM framework suitable for small to medium-sized organizations. Recognizing the cost constraints associated with traditional SIEM solutions, we have opted for an Elastic Stack-based SIEM solution. The Elastic Stack comprises open-source tools such as Elasticsearch, Logstash, and Kibana, offering scalability and cost efficiency. Additionally, we have integrated various other tools, such as VirusTotal, which provides real-time threat intelligence for detecting malicious files. Arkime, a network traffic analysis tool, has also been integrated with the SIEM system to enhance threat detection and incident response capabilities. Furthermore, the implementation includes the deployment of a honeypot to safeguard the network by diverting attackers from accessing it. This project is dedicated to consolidating these tools into an integrated SIEM solution aimed at improving threat detection and incident response capabilities.***

Keywords: SIEM, Elastic Stack, Security Information and Event Management, Threat Detection

I. INTRODUCTION

In today's interconnected digital era, cybersecurity has emerged as a critical concern for individuals, business, and governments worldwide. With all these sophisticated cyber threats ranging from malware and ransomware to phishing attacks and data breaches, organizations of all sizes are being affected by these threats and is a huge challenge for the organizations.

One of the main reasons behind this paper is to prevent data breaches in organizations. Data Breaches can cause a severe negative impact on the reputation of the organization. Identity theft is part of data breach where the attacker uses personal information of the victim without their knowledge. This is mainly used for fraud and unlawful purpose. In 2020 the number of identity theft victims have increased spontaneously by 23%. About 2 billion in losses occurred because of data breach [9]. Therefore, large amount of data breaches can result in severe consequences in society. With all these challenges in digital era, Security Information and Event Management (SIEM) systems have emerged as revolutionary tool for organizations seeking to fortify their defenses and proactively detect and respond to security incidents. SIEM framework provides a centralized platform to gather and analyze vast volume of security logs from various sources, enabling organizations to gain actionable insights into potential threats.

Security Information and Event Management (SIEM) is a combination of Security Information Management (SIM) and Security Event Management (SEM). It involves collecting and analyzing security data from various sources across the network, including logs, events etc. to detect and respond to potential security incidents in real time. It performs real-time monitoring, allowing security team to respond to the threat immediately. By centralizing the collection and analysis, it enables the organization to gain visibility into their IT environment, and improve threat detection.

Elastic Stack is a power full opensource suite used for log management and data analysis. At its core there are mainly 3 tools: Logstash, Elasticsearch and Kibana. Logstash is a server-side data process pipeline and transfers data into a storage from various sources. The main role of Logstash is to collect data from multiple sources and share the data into Elasticsearch. Elasticsearch is an opensource REST API and transfers data via JSON. It acts as a search engine, used for searching data stored in database. It can be used for querying and retrieving information and analyze the data quickly. Kibana is an opensource data visualization engine. It allows user to create customizable dashboard, charts, and graphs to effectively analyze and monitor data.

©IJRASET: All Rights are Reserved

VirusTotal is an opensource online service which can analyze files and URLs for potential malware and security threats. It is done with the help of multiple antivirus engine and various detection methods. With its vast database of known threats, it is a useful tool for enhancing threat detection. Arkime is an opensource tool used for collecting and analyzing network packets. It is integrated with Elastic stack specifically with Elasticsearch, which it is used as a database to gather network logs. T-Pot is honeypot designed to mimic diverse IT-environment therefore attracting and deflecting malicious actors from looking for vulnerabilities of organizations network. It can emulate real world network environment with which it can gain information on various emerging threats.

The authors Kumar and Haritha have used elk stack framework for their SIEM [1]. They have used the Elastic stack and they have set alerts to get notified for all the abnormal and unusual events. It also manages various logs from various sources into useful datapoints with Elastic Stack [6]. Logs are collected and forwarded with the help of File Beats. And we have also used Beats tool throughout the proposed solution. It deals with handling data collection through automation [7]. With the help of Elastic, we can evaluate the data in real time. It also covers a case study on technical solution for supporting long-term evaluation with Elastic Stack. Praneeth and Sreedevi have integrated Winlogbeat and Sysmon to their Elastic Stack [2]. These Winlogbeat and Sysmon can be used to gather event logs. And these event logs can be analyzed to detect various malicious activity with the help of virus total. Fabre and the other authors discuses about data management and data visualization within Elastic Stack [8]. They discuss about how data from various sources are gathered, analyzed, and visualized in real time. The paper also covers the integration of ELK and SKG GRAPHYP [8]. Open-source honey pots like T-pot to gather valuable information about type of attacks, activities, and attackers. This honeypot is integrated with the SIEM to improve the threat detection across network. And they analyze the performance using LogRhythm [4]. This authors Subramanian and Kiruthiga, does a comparative study of various SIEM in the market including Elastic stack based SIEM [3]. It also checks for the effectiveness of the ELK SIEM under various malicious attacks. The result shows how efficient and cost-efficient is Elastic based SIEM are for small and medium sized business. They went with Elastic stack for detecting and verifying various malicious events present in Linux [5]. For this reason, they have used syslog-ng for gathering network logs. They have also used moloch to collect and analyze various network packets within the network traffic [5].

This paper focuses on the development of an exhaustive SIEM which focuses on detection and analysis of both network and system-based logs using Elastic Stack based SIEM. For the development of SIEM we have used Elastic cloud through which we can allocate required resources for the SIEM. Various detection rules were set for detecting and alerting for various anomalies, unauthorized access etc. in real time. For improving threat detection, we have integrated tools like VirusTotal and Arkime. We have also added honeypot with the SIEM to detect and deflect the attackers.

II. METHODOLOGY

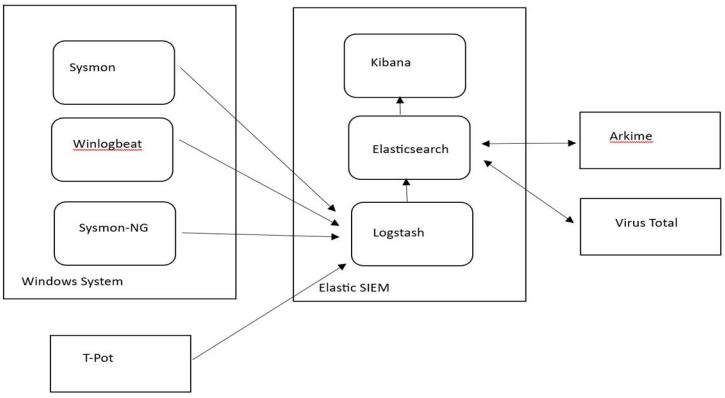


Fig. 1. Workflow of proposed solution

We begin by configuring Elastic cloud to establish a centralized platform for the security operations. With the help of elastic cloud you can access the Elastic SIEM remotely [10]. By configuring elastic cloud we were able to access elastic stack. Thus we were able to integrate Logstash, Elasticsearch and Kibana for the SIEM.

For this configuration we have used windows system. Windows system is used to gather data and logs for the SIEM. For connecting the SIEM with the system we have used elastic agent. For sharing the log data in this case we are using Sysmon and Winlogbeat. These tools enable us to capture detailed system-level event which are then send to Logstash and Elasticsearch for analysis [11].

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

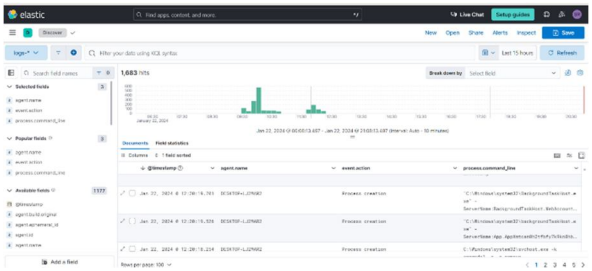


Fig. 2. Elastic dashboard

We have added various detection rules and alerts for detecting various anomalies and responding to it in real time. These rules function by leveraging the logs collected by Sysmon and Winlogbeat. By using these rules SIEM can detect suspicious behavior, unauthorized access, and various other security anomalies [2]. These anomalies can be detected in real time using elastic stack.

Fig. 3. Security alert with Elastic SIEM

We integrated VirusTotal to the elastic SIEM to improve the threat detection. Now it will automatically look through file hashes and this way it will look for malicious files within the system and therefore we can identify various malicious files and improve the security.

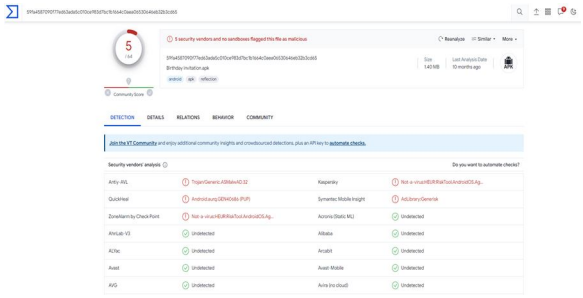


Fig. 4. VirusTotal Dashboard

We used T-Pot honeypot system for luring various malicious agent from the secure network. By looking through the honey pot traffic we can get various information regarding the type of attacks, the events that triggered and the attackers [4].

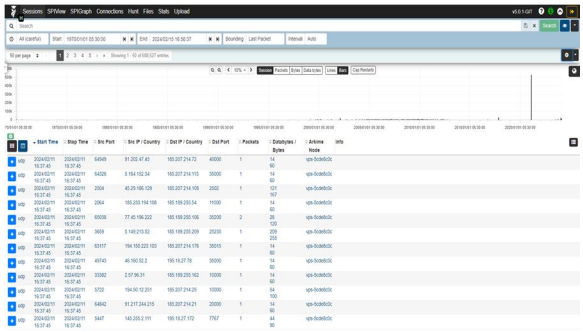


Fig. 5. Arkime Dashboard

We also integrated Arkime with Elastic Stack to process network logs. This tool is configured with Elasticsearch from which it gathers all the network packets which is being stored in Elasticsearch [5]. The collected data is then analyzed in isolated environment to see behavior of the traffic. It will look for malicious or suspicious activities within the network.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

III. RESULT

With Elastic Cloud configured, we have a centralized platform for security operations. This allows for easier management and monitoring of data in real time. It allows remote access to the Elastic SIEM, allowing security analyst to monitor and respond to various security incidents remotely. Elastic Stack suite consist of Logstash, Elasticsearch, and Kibana. These tools enable data collection, storage, analysis, and visualization. Elastic Agent facilitates the connection between the SIEM and the windows system, allowing for sharing of log data through Sysmon and Winlogbeat. Various detection rule and alerts have been configured to detect unauthorized events within the system in real time. Integrating VirusTotal enhances overall threat detection capabilities. With automated scanning, overall security is improved. In addition to VirusTotal integration Arkime also improved security from networking side. By adding Honeypot system, we can lure malicious actors and gather information about attack types, event triggers and attackers.

Overall, the proposed solution has improved threat detection, security monitoring and response capabilities to security events. By integrating Elastic SIEM with other tools and integrations, we can strengthen the organization's security efficiency.

IV. CONCLUSION AND FUTURE SCOPE

The main contributing factor of this paper is that it combines and integrates various technologies to improve threat detection capabilities of the Elastic Stack based SIEM. The solution is focused on small to medium sized enterprise and therefore it mainly focuses on opensource technologies. It focuses on both system and network traffic to look for malicious attacks.

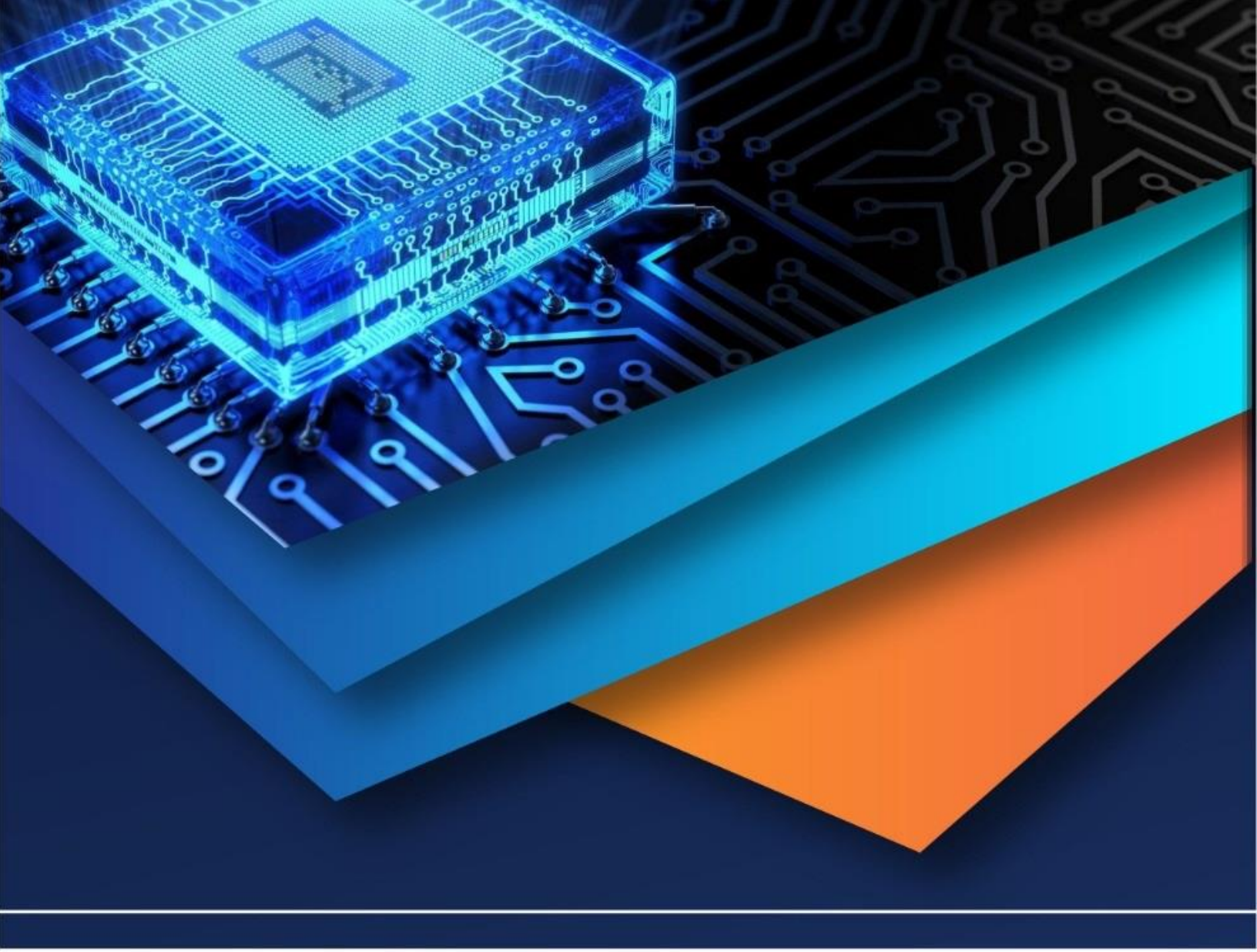
We have configured elastic stack with the elastic cloud. For this purpose, we have installed elastic agents in the system. For log collection we have added syslog and Winlogbeat. For Detection of various anomalies, we have also added various detection rules. For improving threat detection, we have integrated the SIEM with VirusTotal. For detecting various network anomalies, we have also integrated Arkime. We have also used T-Pot an opensource honey pot for gathering information regarding various event that triggers attack.

From the logs we collected through honey pot and SIEM, we have gathered signature of samples. Based on these signatures we can create threat intelligence database which can be used to detect various malicious anomalies. We can improve the SIEM by adding autonomous incident response and AI engine capabilities.

REFERENCES

[1] Kumar, Haritha. "Intrusion Detection System using ELK Stack." in International Journal for Research in Applied Science and Engineering Technology, vol. 7, issue 6, June. 2019
[2] Praneeth, J.N., Sreedevi, M. "Detecting and analyzing the malicious windows events using winlogbeat and ELK stack." in International Journal of Recent Technology and Engineering, Volume-7, Issue-6S, March 2019.
[3] Subramanian, Kiruthiga, Meng, Weizhi.. "Threats Hunting Using Elastic Stack: An Evaluation." 1-6. 10.1109/SOLI54607.2021.9672347, December 2021.
[4] Maduranga, G. L. D. "Network Security Enhancement through Effective Log Analysis using Elk for Small and Medium-Sized Business Environments." In Journal of Network Security and Data Mining volume- 4,issue 1, (2021).
[5] Babu, J.B., Prasad, S. and Prasad, G.S, "Detecting and Analyzing the Malicious Linux Events using Filebeat and ELK Stack." in International Journal of Engineering and Advanced Technology (IJEAT), Volume-8 Issue-4, April 2019.
[6] Vethanayagam, "Threat identification from access logs using elastic stack" in North Dakota State University of Agriculture and Applied Science, November 2020
[7] Rohde, Christopher; Koch, Michael; Stojko, Laura ,"Using an Elastic Stack as a Base for Logging and Evaluation of Public Displays". in Mensch und Computer 2023 - Workshopband. Volume- 3,issue -6. September 2023
[8] Azeroual O, Fabre R, Störl U, Qi R. "Elastic Stack and GRAPHYP Knowledge Graph of Web Usage: A Win–Win Workflow for Semantic Interoperability in Decision Making." In Future Internet 2023; volume- 15 issue- 6, May 2023
[9] Đức Phong, Lê & Isah, Haruna & Dadkhah, Sajjad & Yadoll ahi, Mohammad Mehdi & Zhang, Xichen & Ghorbani, Ali. "Data Breach: Analysis, Countermeasures, and Challenges." In International Journal of Information and Computer Security. Volume- 1. Issue- 1. May 2022.
[10] Elastic team, "Elastic Security Solution", https :// www.elastic.co/guide / en / siem /guide/current/install-siem.html. (accessed Feb 10,2024)
[11] Elastic team, "Winlogbeat quick start: installation and configuration" from https://www.elastic.co /guide /en/beats/winlogbeat/current/winlogbeat-installation-configuration.html (accessed Feb 10,2024)

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)