IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13608

Centralized IT Logging System

Amit Patne[1], Soham Sabale[2], Lokesh Mane[3], Anurag Sagare[4], Deep Palekar[5], Pranali Tilak[6], Tarannum Sayyad[7]

Students, Department of Computer Science, KBPCOE Satara, Satara, India[1,2,3,4,5,6]

Assistant Professor, Department of Computer Science, KBPCOE Satara, Satara, India[7]

Abstract: A centralized logging system for collection, aggregation, monitoring and analysis of log data from various data points leveraging open-source Elasticsearch (ELK) stack. ELK is comprised of three different tools Elasticsearch, Logstash, and Kibana. We are developing easily deployable automation script to remotely install required monitoring tools on endpoints. Tool offers Host Intrusion Detection System (HIDS) with threat hunting capabilities using Wazuh and Network Intrusion Detection System (NIDS) capabilities using Suricata, Zeek, and Snort. We are using machine learning models for threat detection. It comes with various deployment options (on-prem/cloud). Offering functionality to develop custom monitoring rules based on various signature heuristics. Because of the capabilities we are offering and the fact that storage is the only charge, it is a more cost-effective replacement for current systems.

Keywords: Elasticsearch stack (ELK stack), Network Intrusion Detection System (NIDS), Network Intrusion Detection System (NIDS), Firewall

I. INTRODUCTION

In recent years Data breaches, unauthorized access to sensitive information, and privacy concerns are serious problems. Log collection and retention policies are minimal or non-existent in various environments, this arises security concerns. Many organizations lack Threat Detection and Response (TDR) capabilities. It is difficult and time consuming to manage several logging systems that are dispersed across several locations, to overcome these problems there is a need of a Centralized logging system which will collects data from different locations and sent to a central location for monitoring. This paper aims to propose a centralized logging system using ELK stack with Security onion, Wazuh, Beats, Sysmon, Autoruns, with following purpose:

- Centralized logging system for collection, aggregation, monitoring and analysis of log data from various data points leveraging open-source Elasticsearch (ELK) stack.
- Easily deployable automation script to remotely install required monitoring tools on endpoints.
- Host Intrusion Detection System (HIDS) with threat hunting capabilities using Wazuh
- Network Intrusion Detection System (NIDS) capabilities using Suricata, Zeek, and Snort
- Machine learning based threat detection and real-time alerting.
- Easily deployable automated workflow with various deployment options available (on-prem/cloud).

II. LITERATURE REVIEW

1. Cyber Threat Intelligence for Malicious Event Detection using ELK Stack (M Harikanth, P Raja Rajeswari)

- The proposed system describes an environment that will check whether the operations are going good in an organization or not in real time.
- This solution detects most of the malicious operations that are going on their environment either local or remote. A threat intelligence interface, the proposed system will detect and prioritize the threats that are going on the network at a particular point of time.

2. ELK stack and commercial system performance in security log analysis. (Sung Jun Son, Youngmi Kwon.)

- Open-source platform, ELK stack, to build a big security log analysis system for small or medium sized enterprises.
- It cuts the concerns about the installation cost of commercial products in the beginning stage, and it makes startups free from the effort of building their own log analysis system with primitive Hadoop and MongoDB, etc.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

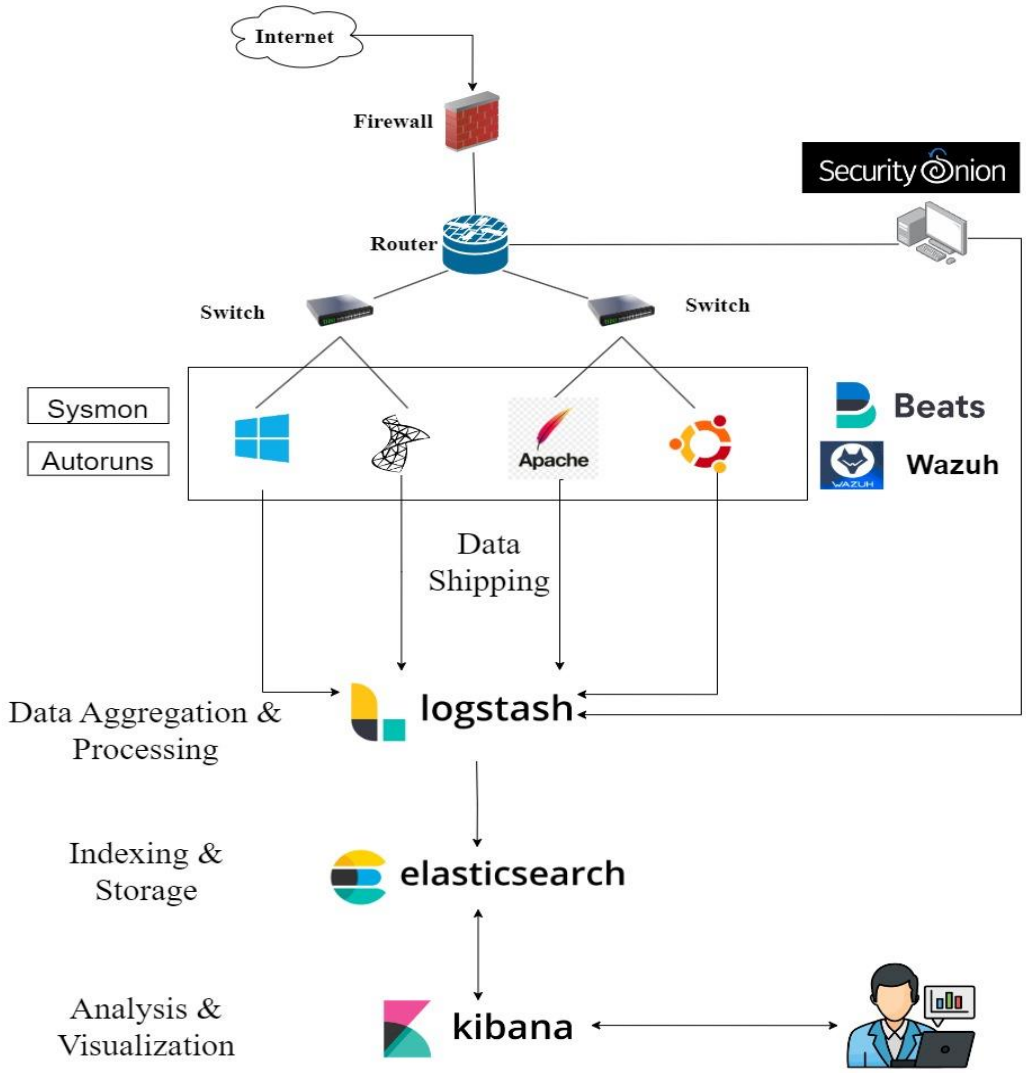
DOI: 10.17148/IJARCCE.2024.13608

- ELK stack shows similar or better performance in searching for particular security logs which match specific conditions. For 1,000 million log files, ELK stacks took 1 min and 14.4 sec, whereas 1 min and 22.2 sec with Splunk.
- In addition, ELK solution provides various kinds of visualization tools which are useful for security administrators. So, ELK stack can be a powerful beginning security log analysis tool with acceptable performance compared to high-cost commercial products.

3. Network Security Enhancement through Effective Log Analysis Using ELK. (Ibrahim Yahya Mohammed AL-Mahbashi, Dr. M. B. Potdar, Mr. Prashant Chauhan.)

- The commercial safeguard was not capable enough as it was supposed to be because of the critical gaps found.
- Starting from being able to bypass the portal access of our internal network which will allow the attacker to not just only use the network identity to initiate cybercrimes, but also it was not able to control the inbound and outbound connections.
- Such critical vulnerabilities existed on well-known safeguard will diffidently lead to no counted disasters which was not easily to be identified unless paper do continue analysis not just to only monitor the network but also to provide an always measurement for our safeguards to check their efficiency.

III. METHODOLOGY



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024
DOI: 10.17148/IJARCCE.2024.13608

1. To collect data from critical Windows and Linux endpoints tools like Beats, Sysmon, Wazuh, and Autoruns are installed using easily deployable automated scripts.
2. To capture network data, we will be forwarding networking logs from a router to the endpoint where tools Zeek, Suricata, Snort, and Beats are installed.
3. Collected data will be shipped by Beats to Logstash instance which will ingest data from multitude of sources, transforms it and then sends it to Elasticsearch.
4. Elasticsearch provides storing and indexing of logs centrally for lighting fast searching and analysis.
5. Kibana is a dashboard that will provide security analysts access to review and monitor log data indexed in Elasticsearch

IV. APPLICATIONS

- Defence Sectors: Centralized logging capabilities with network traffic monitoring in addition to safeguard military and defense data.
- Healthcare System: Analyze and Protected Health Information (PHI), medical equipment data, and Electronic Health Records (EHRs) from threats.
- Banking: Protect and analyze financial data, secure Payment Card Industry (PCI) data.

V. CONCLUSION

In conclusion, the implementation of a centralized IT system log analysis utilizing the ELK stack, Security Onion, and Wazuh presents a comprehensive solution for monitoring and managing security incidents within an organization. Through the integration of these tools, we have achieved enhanced visibility into system activities, real-time threat detection, and streamlined incident response capabilities. Together, the integration of the ELK stack, Security Onion, and Wazuh enables us to achieve a holistic approach to IT system log analysis and security monitoring. By centralizing log data, correlating events across multiple sources, and applying advanced analytics techniques, we can better protect our organization's assets, detect and respond to security threats in a timely manner, and continuously improve our overall security posture.

ACKNOWLEDGMENT

I would like to express my sincere appreciation to those who have contributed to the completion of this research paper on centralized log management. I am deeply grateful '**Prof. Tarannum Shaikh'** for her guidance, expertise, and unwavering support throughout the research process. She provided valuable insights and played a crucial role in shaping the direction of this study.

REFERENCES

[1]. https://www.elastic.co/elastic-stack
[2]. https://www.elastic.co/guide/index.html
[3]. https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html
[4]. https://github.com/wazuh/wazuh
[5]. https://www.elastic.co/guide/en/beats/winlogbeat/current/configuring-howto-winlogbeat.html
[6]. https://wazuh.com/
[7]. https://securityonionsolutions.com/
[8]. https://arkime.com/
[9]. https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

