

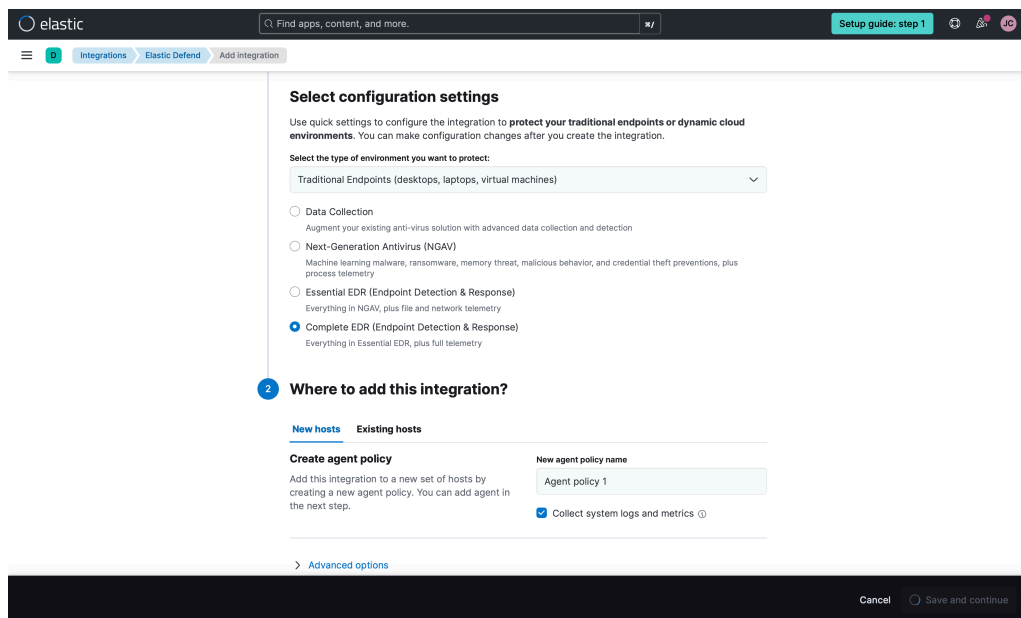
Elastic SIEM Setup & Configuration

Introduction

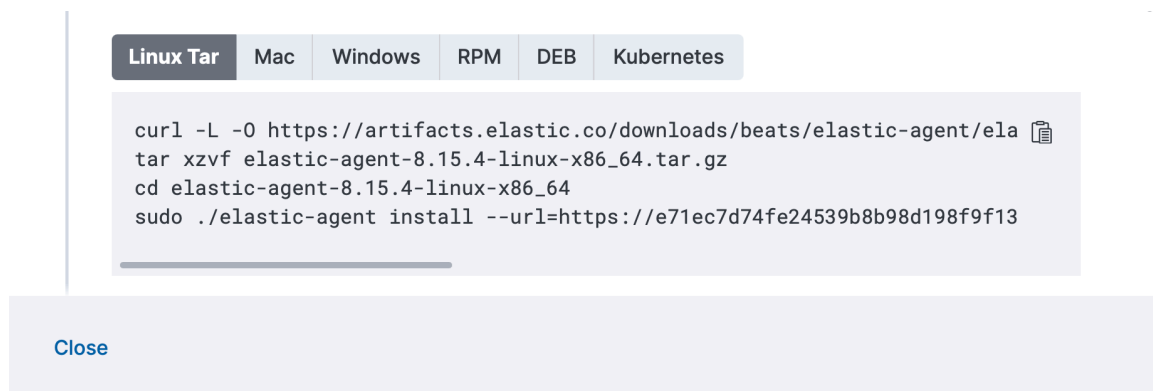
In this project, I have implemented and configured the Elastic Stack (Elasticsearch, Logstash and Kibana) to establish a centralized logging and security monitoring system. The primary objectives were to ensure seamless log collection, enhance log analysis capabilities, and enable proactive security incident response.

Steps Performed

1. Configuration and Installation



We began by installing the Elastic Stack components on a dedicated Kali Linux (VM) system using the commands in the screenshot below. Elasticsearch was configured as the centralized log storage and indexing engine, while Kibana provided the interface for log visualization and analysis.



Next, we configured the Elastic Agent on various endpoints to forward logs to Elasticsearch. The agent was set up to capture system logs, network activity, and security events.

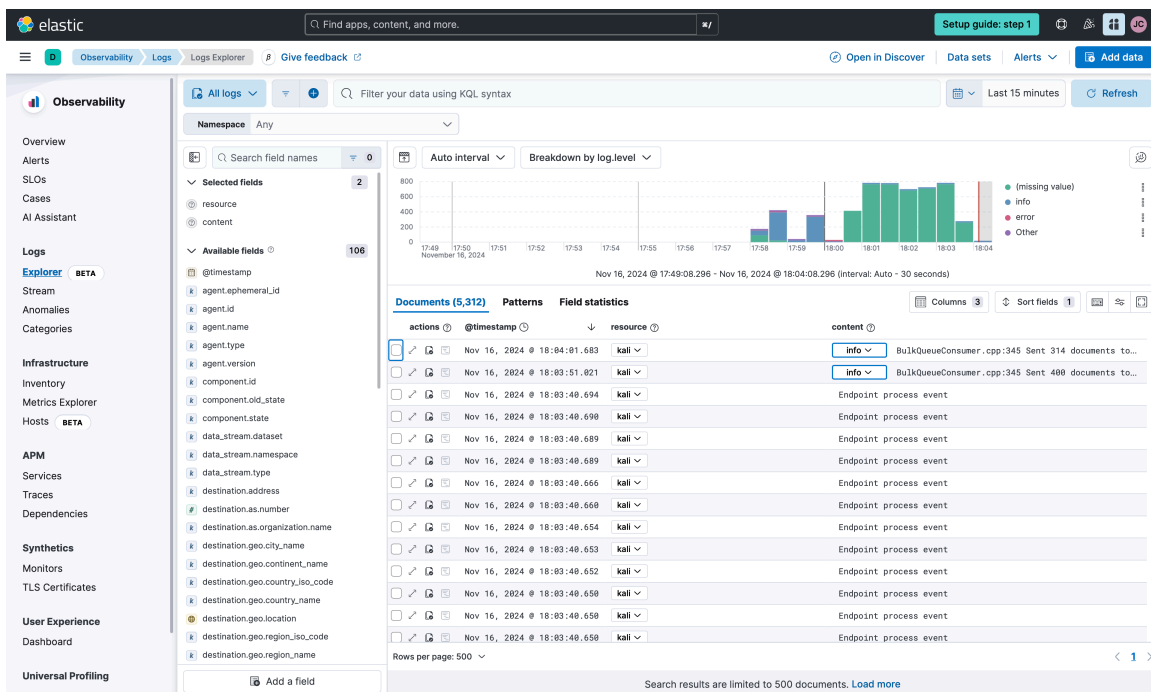
Challenges: During the setup, connectivity issues between the Elastic Agent and Elasticsearch were resolved by modifying firewall rules and ensuring proper authentication settings.

2. Simulating Activity to Generate Logs

To validate the Elastic Stack's configuration, I used the ***nmap -p- localhost*** command to simulate network activity. This full port scan of the localhost generated significant traffic and security events, mimicking real-world scenarios of system probing and reconnaissance.

```
kali@kali: ~  
└─$ nmap -p- localhost  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-16 18:06 EST  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.0092s latency).  
Other addresses for localhost (not scanned): ::1  
Not shown: 65533 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
6789/tcp  open  ibm-db2-admin  
6791/tcp  open  hnm  
  
Nmap done: 1 IP address (1 host up) scanned in 105.73 seconds  
  
kali@kali: ~  
└─$
```

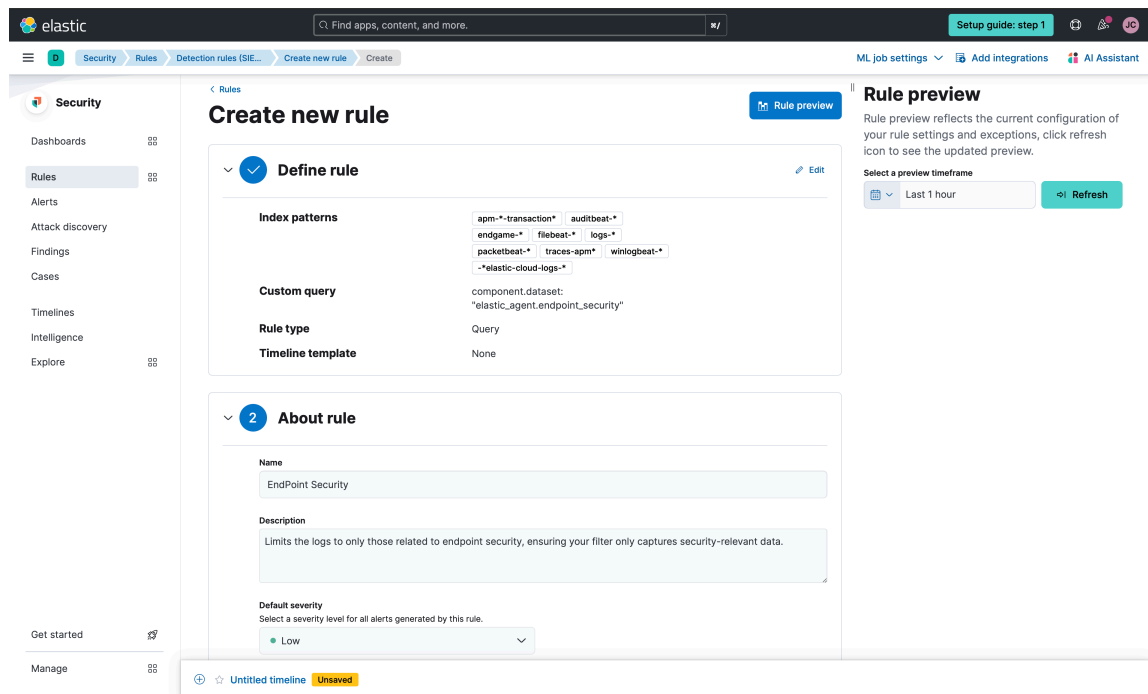
The activity was instrumental in verifying that the Elastic Agent successfully captured and forwarded log data to Elasticsearch. The logs were then visualized in Kibana, showcasing the seamless integration and functionality of the setup. By utilizing Kibana Query Language (KQL), I could efficiently filter logs to analyze specific events or activities. For instance, querying with ***process.args: "<process_name>"*** allowed me to pinpoint logs associated with a particular process, streamlining the investigation process and enhancing log analysis precision



This ability to filter and search logs using relevant KQL syntax ensures the system's utility in monitoring and responding to targeted activities, significantly improving the effectiveness of threat detection and response workflows.

2. Log Indexing and Custom Filters

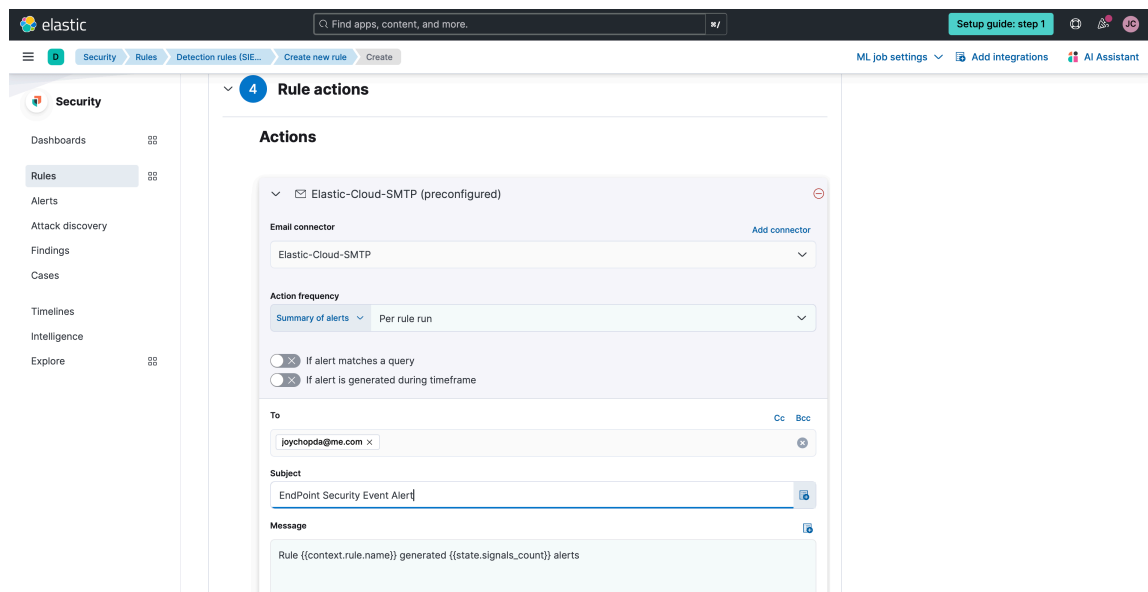
To improve log analysis, we developed and deployed custom log filters tailored to specific use cases. The filters enable precise categorization and tagging of logs, facilitating easier search and analysis. This page can be found by navigating the menu under Security > Rules.



Additionally, indices were optimized to handle high volumes of data efficiently. This included setting up log rotation to prevent storage overload.

3. Alerting Mechanism

Automated email alerts were configured for critical security events. For instance, alerts were triggered for unauthorized access attempts, unusual network traffic patterns, or high CPU usage. This ensured timely detection and response to potential incidents.



Conclusion

The Elastic SIEM successfully showcased our ability to establish a robust and scalable log collection and monitoring system. This implementation not only validated our skills in configuring the Elastic Stack but also provided us with valuable hands-on experience in troubleshooting and optimizing its functionality. Additionally, we achieved good visibility into the telemetry, enabling us to monitor and analyze network and system activities effectively. This visibility offered critical insights into event patterns, potential anomalies, and areas for improvement in security posture. Overall, the project significantly enhanced our expertise in advanced log analysis and SIEM operations, preparing for real-world cybersecurity challenges.