

Report on EDR/SIEM Tool: ELK Stack

CSE406: Computer Security Sessional

Kazi Ababil Azam (1805077)

Fardin Anam Aungon (1805087)

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology (BUET)

September 13, 2023

Contents

1	Introduction	2
1.1	What is ELK Stack?	2
2	General Overview of ELK Stack	3
2.1	Components of ELK Stack	3
2.2	Working Principle of ELK Stack	4
2.3	Features of ELK Stack	4
2.4	SIEM components	4
2.5	SIEM with ELK Stack	5
3	Elastic Security Workflow	6
3.1	Elastic Security	6
3.2	Elastic Security Components and Workflow	6
4	Features to be Demonstrated	8
5	Demonstration	9
5.1	Elastic Cloud: Sign up	9
5.2	Adding the integration	10
5.3	Adding an agent	11
5.4	Dashboards	13
5.4.1	Network Packet Capture	13
5.4.2	Elastic Defend	15
5.4.3	Windows	15
6	Limitations	17
7	Conclusion	18

Chapter 1

Introduction

1.1 What is ELK Stack?

ELK Stack is a combination of three open source projects: Elasticsearch, Logstash, and Kibana. ELK Stack is most commonly used for log aggregation and log analysis. The ELK Stack is a great collection of tools to collect, analyze and visualize data. It is a very powerful stack that provides developers and system operators with great insights into their operational data.

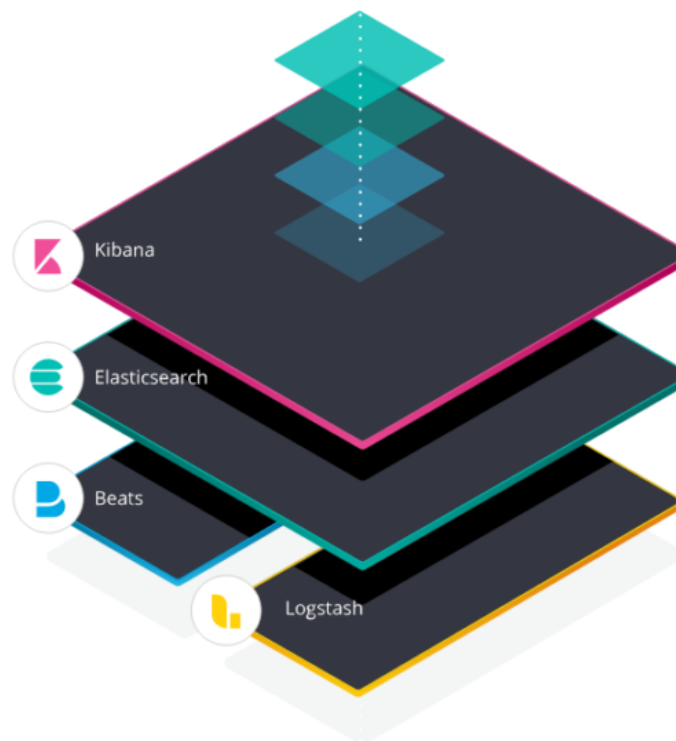


Figure 1.1: ELK Stack

Chapter 2

General Overview of ELK Stack

2.1 Components of ELK Stack

ELK Stack is mainly composed of three components:

- Elasticsearch, the search and analytics engine
- Logstash, the data processing pipeline
- Kibana, the data visualization tool

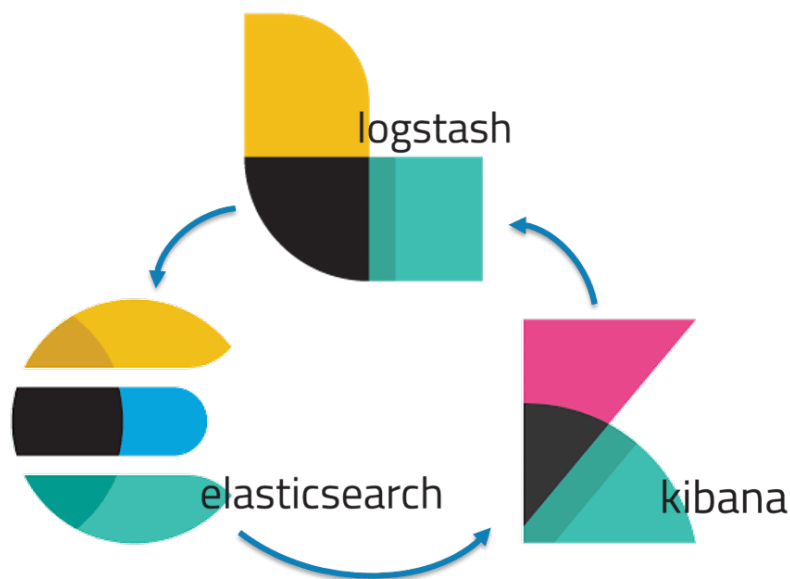


Figure 2.1: Components of ELK Stack

Elasticsearch

Elasticsearch is the centralized component of the Elastic Stack. It is a distributed, RESTful search and analytics engine capable of solving a growing number of use cases. It is based on a server that can process JSON requests, index documents containing JSON objects, and give back JSON responses. Using a structure based on documents instead of tables, it is able to provide a scalable search solution with a low latency, and comes with extensive REST APIs for storing and searching the data.

Logstash

Logstash is a open-source, server-side data processing pipeline which ingests data from multiple sources simultaneously. It has roughly 3 stages in its working principle.

- Input: listen for and accept log data
- Filter: filter, parse and enrich the log data
- Output: sends the log to another system

Kibana

Kibana is basically a data visualization and management tool. It lets users visualize the data handled by Elasticsearch and navigate the stack. All it needs is an index to search through the data. It is a web application that runs on top of Elasticsearch.

2.2 Working Principle of ELK Stack

The working principle of ELK Stack is shown below:



Figure 2.2: Working Principle of ELK Stack

2.3 Features of ELK Stack

- Open-source and Scalable
- Full-stack monitoring support
- Index based search
- Real-time data analysis
- Provides security solution through different integrations

2.4 SIEM components

SIEM means Security Information and Event Management. It delves into log records and real-time data to provide security intelligence for monitoring, event correlation, and incident response. SIEM is a combination of two technologies:

- Security Information Management (SIM): log records and event data
- Security Event Management (SEM): real-time monitoring and correlation of events

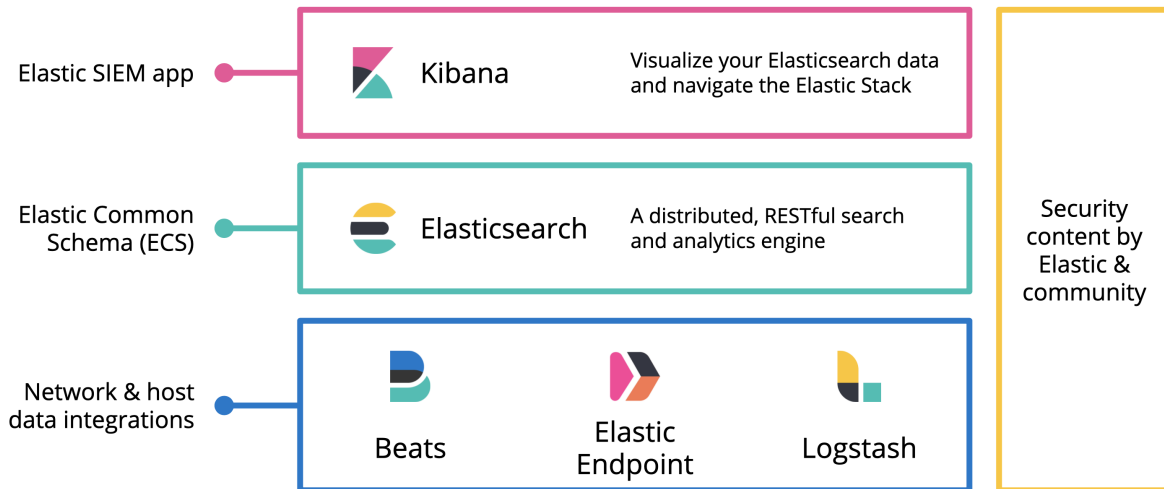


Figure 2.3: SIEM with ELK Stack

2.5 SIEM with ELK Stack

The way how SIEM works with ELK Stack is described as follows:

- **Elastic Endpoint Security** is an endpoint security platform and agent that provides prevention, detection, and response capabilities. It ships events and security alerts directly to Elasticsearch.
- **Beats** are open source data shippers that you install as agents on your systems. Beats send security events and other data to Elasticsearch.
- **Elasticsearch** excels at indexing streams of semi-structured data, such as logs or metrics, while **Kibana** is used to search, view, and interact with data stored in Elasticsearch indices. You can easily perform advanced data analysis and visualize your data in a variety of charts, tables, and maps.

SIEM enables analysis of host-related and network-related security events as part of alert investigations or interactive threat hunting.

The SIEM app provides an interactive workspace for security teams to **triage events** and **perform initial investigations**. Additionally, machine learning anomaly detection jobs and detection engine rules provide ways to **automatically detect suspicious activity** across a entire fleet of servers and workstations. It is now a part of the generalized Elastic Security solution. Elastic Security is highly customizable and can be adapted to various security use cases, making it a popular choice for organizations looking to enhance their security posture. It's used by security teams to monitor and respond to security incidents, investigate threats, and gain insights into their infrastructure's security.

Chapter 3

Elastic Security Workflow

3.1 Elastic Security

Elastic Security combines SIEM threat detection features with endpoint prevention and response capabilities in one solution. These analytical and protection capabilities, leveraged by the speed and extensibility of Elasticsearch, enable analysts to defend their organization from threats.

Elastic Security provides the following security benefits and capabilities:

- A detection engine to identify attacks and system misconfigurations
- A workspace for event triage and investigations
- Interactive visualizations to investigate process relationships
- Inbuilt case management with automated actions
- Detection of signatureless attacks with prebuilt machine learning anomaly jobs and detection rules

3.2 Elastic Security Components and Workflow

A comprehensive diagram of the Elastic Security components and workflow is shown below:

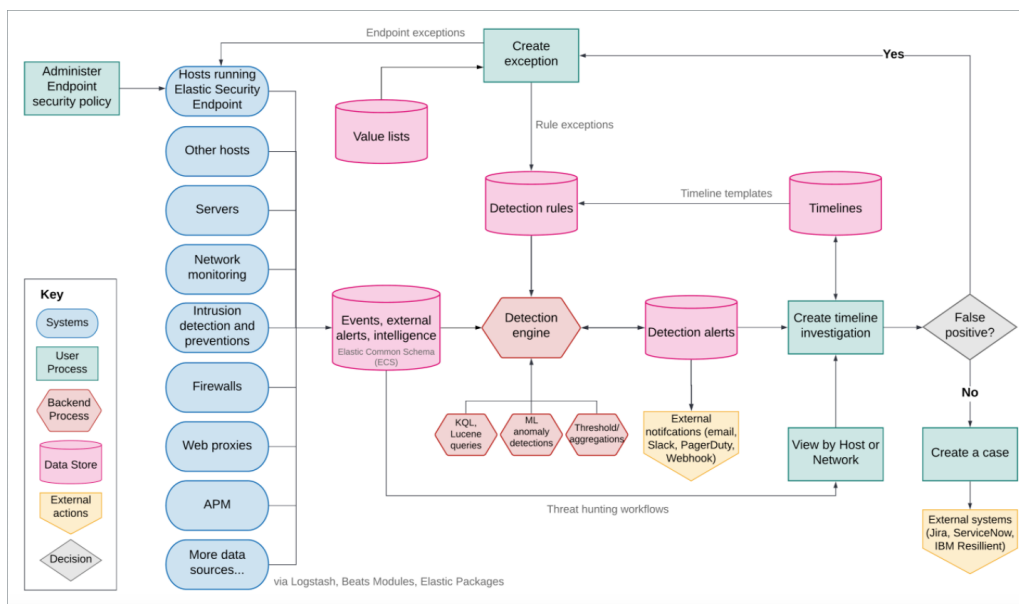


Figure 3.1: Elastic Security Components and Workflow

Here's an overview of the flow and its components:

- Data is shipped from your hosts to Elasticsearch in the following ways:
 - **Elastic Defend:** Elastic Agent integration that protects your hosts against malware and ships these data sets:
 - * Windows: Process, network, file, DNS, registry, DLL and driver loads, malware security detections
 - * Linux/macOS: Process, network, file
 - **Integrations:** Integrations are a streamlined way to send your data to the Elastic Stack. Integrations are available for popular services and platforms, like Nginx, AWS, and MongoDB, as well as many generic input types like log files.
 - **Beat modules:** Beats are lightweight data shippers. Beat modules provide a way of collecting and parsing specific data sets from common sources, such as cloud and OS events, logs, and metrics.
- The Elastic Security app in Kibana is used to manage the **Detection engine**, **Cases**, and **Timeline**, as well as administer hosts running Elastic Defend:
 - **Detection engine:** Automatically searches for suspicious host and network activity via the following:
 - * **Detection rules:** Periodically search the data (Elasticsearch indices) sent from your hosts for suspicious events. When a suspicious event is discovered, an alert is generated.
 - * **Exceptions:** Reduce noise and the number of false positives. Exceptions are associated with rules and prevent alerts when an exception's conditions are met. Value lists contain source event values that can be used as part of an exception's conditions.
 - * **Machine learning jobs:** Automatic anomaly detection of host and network events. Anomaly scores are provided per host and can be used with detection rules.
 - **Cases:** An internal system for opening, tracking, and sharing security issues directly in the Security app. Cases can be integrated with external ticketing systems.
 - **Timeline:** Workspace for investigating alerts and events. Timelines use queries and filters to drill down into events related to a specific incident. Timeline templates are attached to rules and use predefined queries when alerts are investigated. Timelines can be saved and shared with others, as well as attached to Cases.
 - **Administration:** View and manage hosts running Elastic Defend.

Chapter 4

Features to be Demonstrated

The SIEM features for different contexts are implemented through integrations installed in the cloud deployment (which we are accessing through the free trial) of Elastic Security. The features (integrations) that we have demonstrated are as follows:

- **Network Packet Capture**
- **Elastic Defend**
- **Windows**

Chapter 5

Demonstration

5.1 Elastic Cloud: Sign up

The first step is to create an Elastic Cloud deployment. We can create a free trial deployment by signing up for a free trial account.

- Go to <https://cloud.elastic.co/registration?elektra=guide-welcome-cta>.
- Sign up or log in.

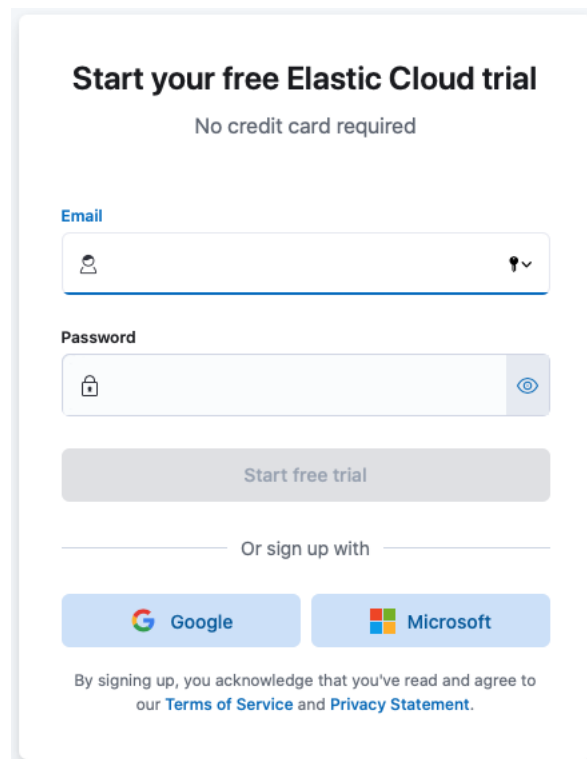
The image shows a web form for starting a free Elastic Cloud trial. At the top, it says "Start your free Elastic Cloud trial" in bold, followed by "No credit card required" in a smaller font. Below this are two input fields: "Email" with a user icon and a dropdown arrow, and "Password" with a lock icon and an eye icon for toggling visibility. A grey "Start free trial" button is positioned below the password field. Underneath the button is a horizontal line with the text "Or sign up with". Below this line are two buttons: "Google" with the Google logo and "Microsoft" with the Microsoft logo. At the bottom, a small line of text states: "By signing up, you acknowledge that you've read and agree to our [Terms of Service](#) and [Privacy Statement](#)."

Figure 5.1: Sign Up

- Create a deployment.
- Save your elastic superuser credentials.
- Once the deployment is ready, select continue.

The deployment includes a pre-configured instance of Fleet Server, which manages the Elastic Agents that can be used to monitor a host system.

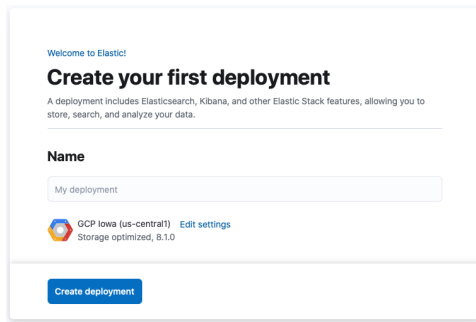


Figure 5.2: Create Deployment

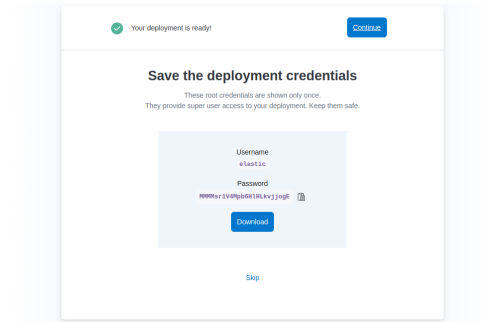


Figure 5.3: Save Superuser Credentials

Configure an integration for the selected agent policy.

1

Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name

Network Packet Capture

Description Optional

Network Packet Capture integration

[Advanced options](#)

☒ **Capture network traffic**

2

Where to add this integration?

[New hosts](#) [Existing hosts](#)

Create agent policy

Add this integration to a new set of hosts by creating a new agent policy. You can add agent in the next step.

New agent policy name

Network Packet Capture policy

☒ Collect system logs and metrics ⓘ

[Advanced options](#)

Figure 5.4: Add Integration

5.2 Adding the integration

- Log in to your cloud deployment, which will take you to Kibana Home.
- Click Add Integrations.
- Search and select the 'Network Packet Capture' integration.
- Click add and configure the integration with the following details:
 - Integration name: Give the integration a name.
 - Description: Enter a brief description of the integration.
 - New agent policy name: Since you'll be creating a new agent policy, enter a name to identify it. Ensure that you leave the Collect system logs and metrics option selected.

Click Save and continue to proceed.

- Click Add Elastic Agent to your hosts.

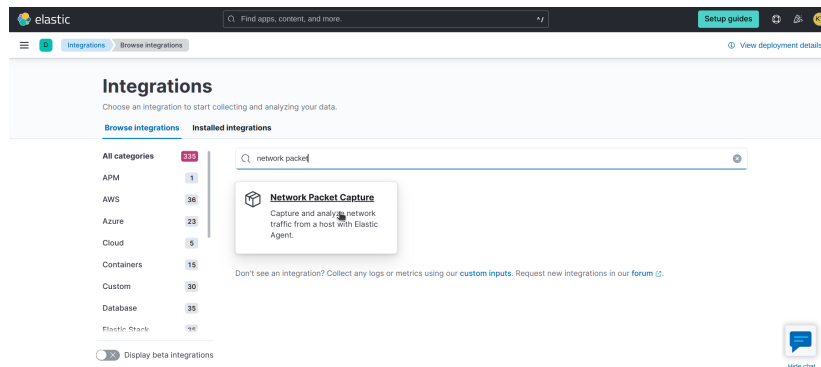


Figure 5.5: Search Integration

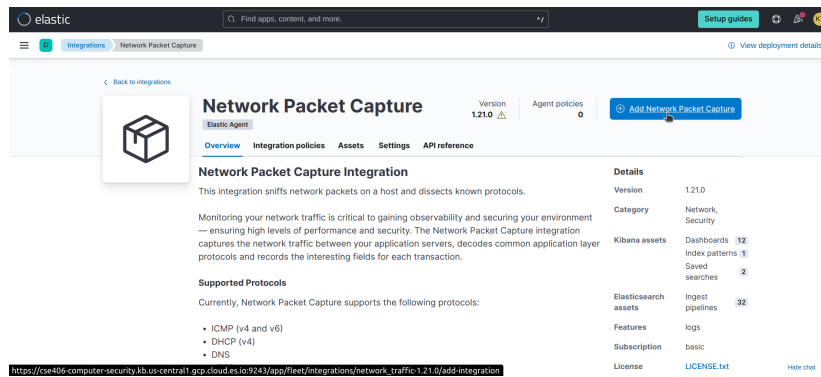


Figure 5.6: Add Network Packet Capture

5.3 Adding an agent

- Follow the Install Elastic Agent on you host step. Pick the appropriate operating system and download and install your agent.
- Once the agent is installed, the agent will automatically enroll with the Fleet Server. It is shown in the Agent enrollment confirmed step.
- Click on Add the integration at the bottom of the screen to proceed.
- The only step remaining is to confirm the incoming data. Click on confirm and it will show a preview of the data Kibana is receiving.
- Click on View Assets to show the Dashboards under Network Packet Capture integration.

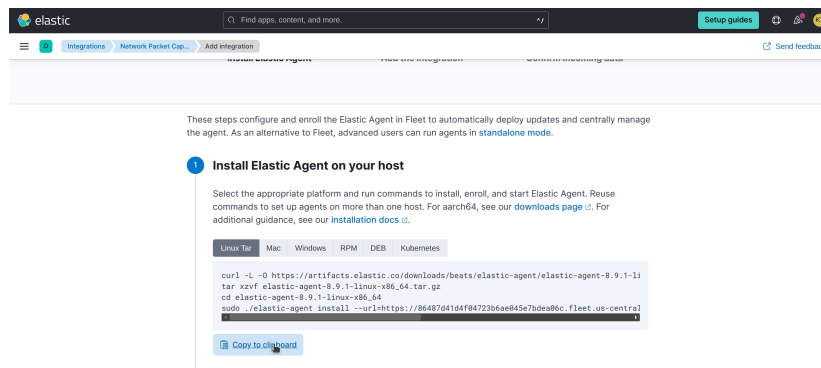


Figure 5.7: Install Agent

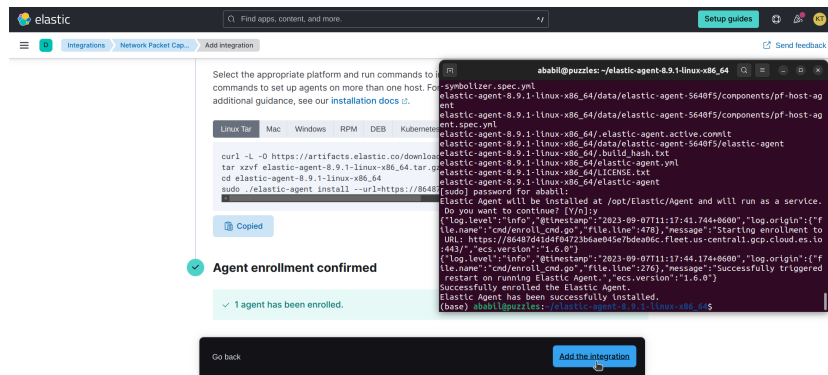


Figure 5.8: Agent Enrollment Confirmed

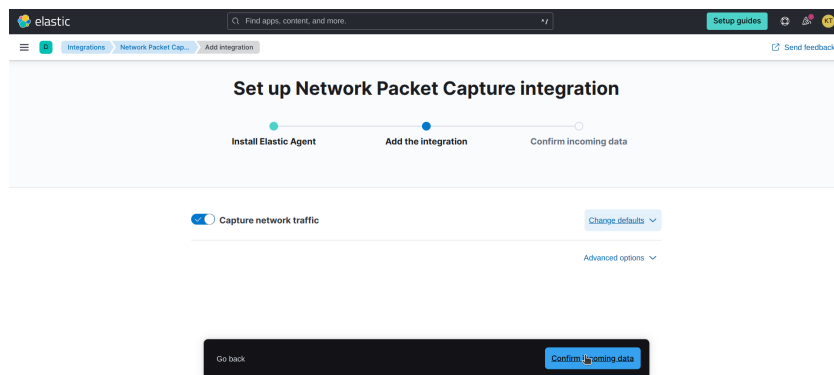


Figure 5.9: Confirm Data

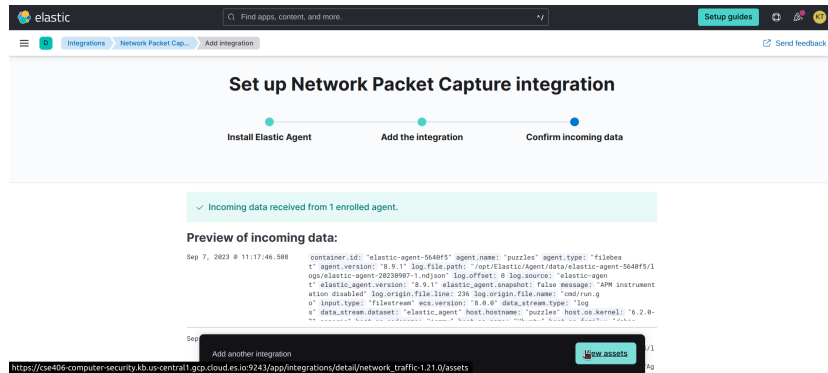


Figure 5.10: View Assets

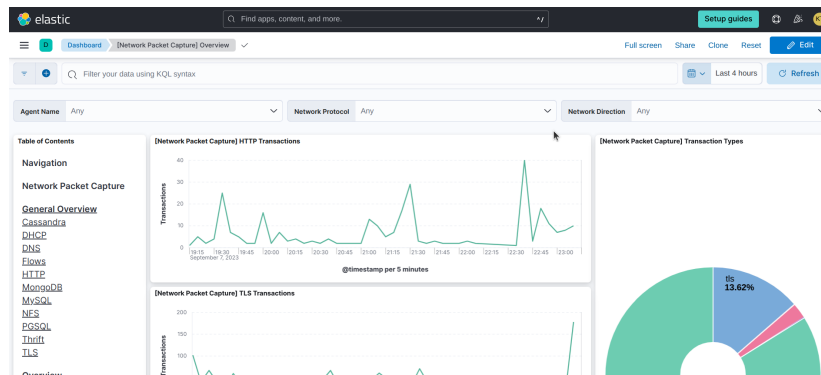


Figure 5.11: Network Overview

5.4 Dashboards

The dashboards are prepared using the data received from the agents installed in the host. They are prepared using Kibana.

5.4.1 Network Packet Capture

Network Packet Capture is a network monitoring tool that captures and analyzes network traffic. This integration sniffs network packets on a host and dissects known protocols.

Monitoring your network traffic is critical to gaining observability and securing your environment, ensuring high levels of performance and security. The Network Packet Capture integration captures the network traffic between your application servers, decodes common application layer protocols and records the interesting fields for each transaction.

The protocols for which the integration provides dashboards are:

- Overview
- DNS Overview
- DHCPv4
- Cassandra
- Network Flows
- HTTP
- MongoDB
- MySQL
- NFS
- PostgreSQL
- Thrift
- TLS Sessions

Here are some of the screenshots taken of the dashboards.

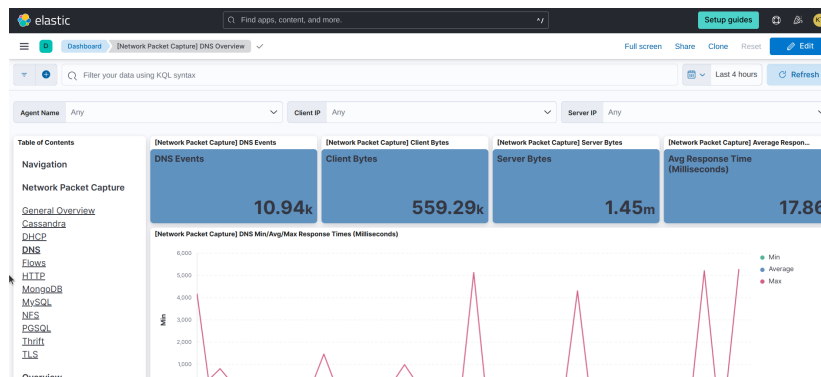


Figure 5.12: DNS Overview

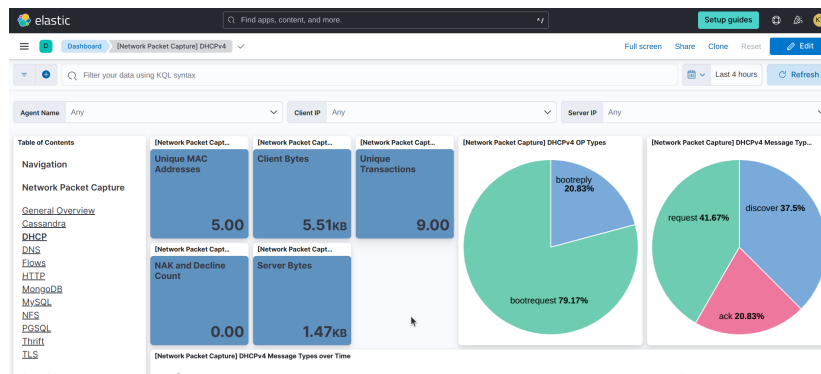


Figure 5.13: DHCPv4

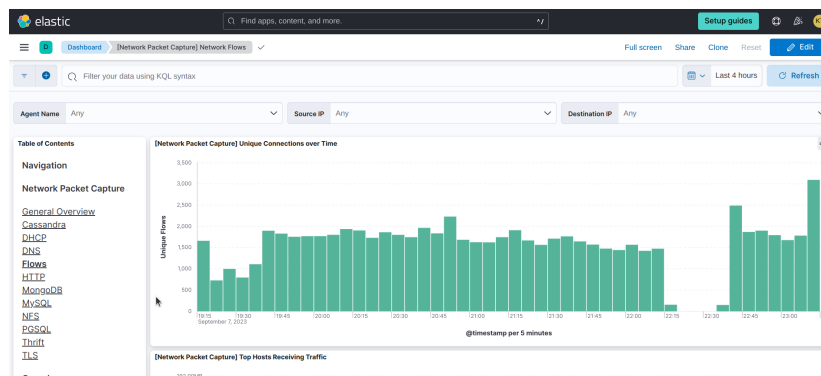


Figure 5.14: Network Flows

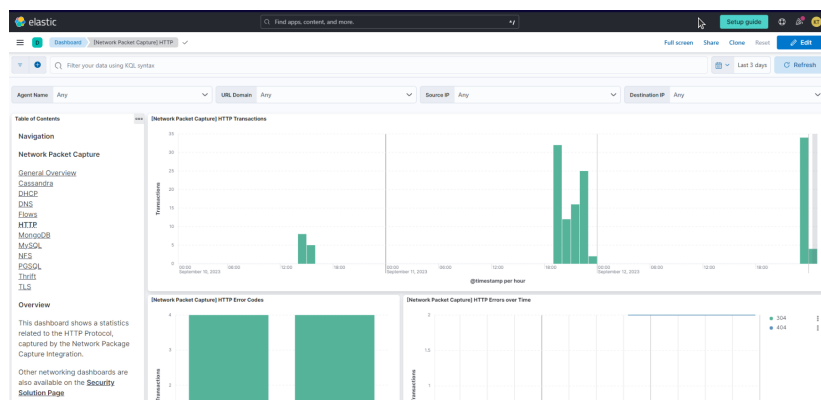


Figure 5.15: HTTP

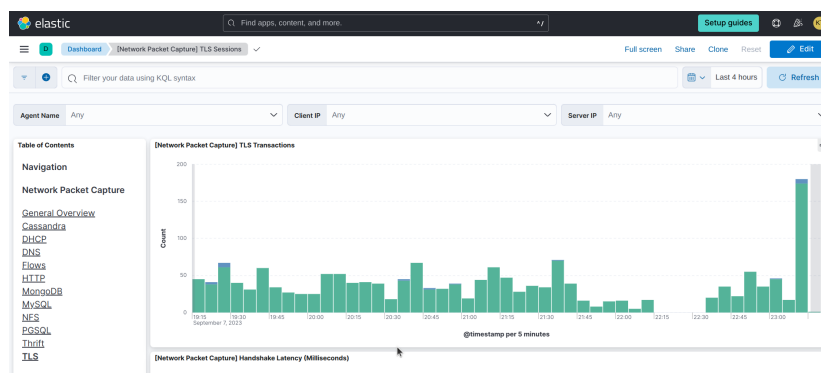


Figure 5.16: TLS Sessions

5.4.2 Elastic Defend

The Elastic Defend integration is used to monitor the host system. It has an alert section which shows the alerts generated by the system due to any malicious activity or vulnerability. Elastic Defend provides organizations with prevention, detection, and response capabilities with deep visibility for EPP, EDR, SIEM, and Security Analytics use cases across Windows, macOS, and Linux operating systems running on both traditional endpoints and public cloud environments. We can use it to:

- Prevent complex attacks
- Alert in high fidelity
- Detect threats in high fidelity
- Triage and respond rapidly
- Secure your cloud workloads
- View terminal sessions

The figures show the Alerts page where the activity alert in accordance with the set rules are shown. The event triggering the alert can be analyzed and marked as Acknowledged or Resolved.

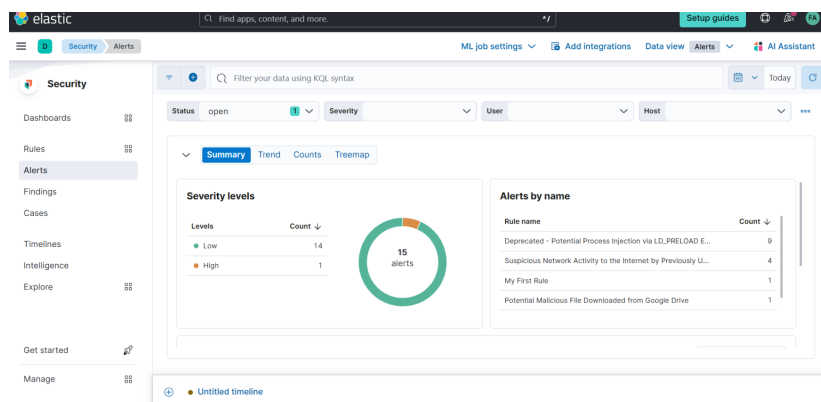


Figure 5.17: Alerts

5.4.3 Windows

The Windows integration is used to monitor a Windows operated host system. It collects metrics and logs from your machine. Then that data is visualized in Kibana, create alerts to notify you if something goes wrong, and reference data when troubleshooting an issue.

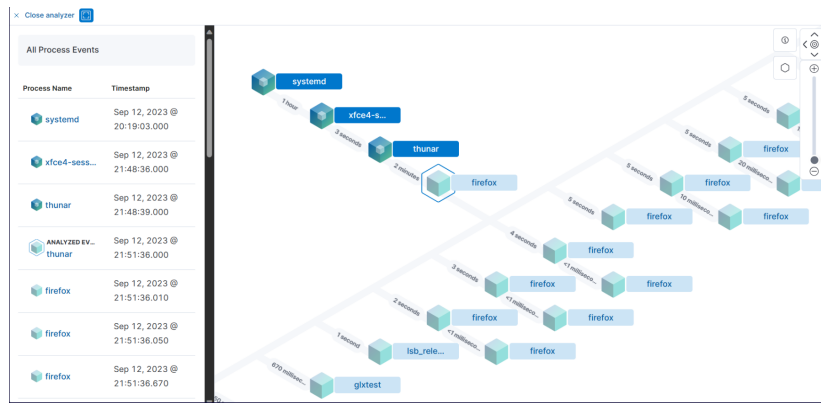


Figure 5.18: Analyze Event

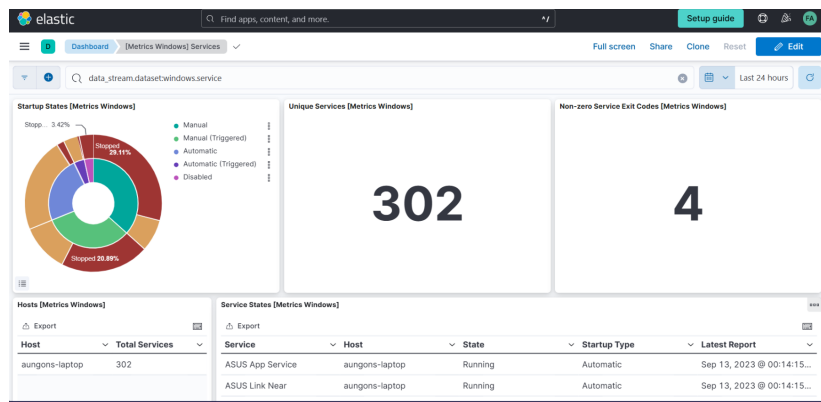


Figure 5.19: Windows Services

For example, if we wanted to know if a Windows service unexpectedly stops running, we could install the Windows integration to send service metrics to Elastic. Then, we could view real-time changes to service status in Kibana's Services dashboard.

Chapter 6

Limitations

We found a few limitations while trying to work with Elastic Security and ELK Stack.

- The documentations and guidelines for using the security tools are fairly backdated
- Not very beginner friendly
- Does not ship with built-in mechanism for alerting
- The app is designed for mostly enterprise purposes

Chapter 7

Conclusion

Elastic Security is a very powerful tool for security monitoring and analysis. Utilizing the integrations and the dashboards, we can monitor the host system and the network traffic. The dashboards provide a very detailed view of the system and the network. The alerts generated by the system can be analyzed and the event triggering the alert can be investigated. Overall, it provides a very comprehensive and expressive analysis as a EDR/SIEM tool.