OPEN SOURCE SIEM OPTIONS

Version 1.0

ASH FRICKER
africker@deakin.edu.au

Author: Ash Fricker

Version History

Version	Description	Date	Author
1.0	Initial creation	04/12/2022	Ash Fricker

Contents

Overview

The purpose of this document is to reveal findings around the usability of open source SIEM software as an alternative to google chronicles. The document will address the options investigated, how to install and configure each option and finally a comparison of the options.

Dock Compose

During the testing of these solutions we will be attempting to install and configure them using Docker Compose. “Compose is a tool for defining and running multi-container Docker applications. With Compose, you use a YAML file to configure your application’s services. Then, with a single command, you create and start all the services from your configuration.” Using Docker Compose will allow us to spin up instances of the solutions with ease for testing purposes as well as allow us to keep our YAML configuration for future implementation.

Wazuh SIEM stack

Wazuh is a security information and event management (SIEM) tool that can help you monitor and protect your infrastructure. Wazuh provides security visibility by collecting, analysing, and alerting on data generated by your IT assets. It can be used to detect threats, vulnerabilities, and compliance issues, and to assist in the investigation and resolution of security incidents.

Wazuh is based on the popular open-source security tool, OSSEC, and includes additional features such as a web-based dashboard and integration with other security tools. It is available as a standalone package or as a Docker image and can be installed on premises or in the cloud. Wazuh can be used to monitor and protect a wide range of IT assets, including servers, network devices, cloud environments, and more.

Installation Guide

To install Wazuh using Docker, you will need to have Docker installed on your system. Once you have Docker installed, you can follow these steps to install Wazuh:

1. Pull the Wazuh Docker image from Docker Hub by using the following command: docker pull wazuh/wazuh
2. Run the Wazuh Docker image by using the following command:
3. docker run --name wazuh -d -p 1514:1514/udp -p 1515:1515 -p 1516:1516 -p 514:514/udp -p 55000:55000 -p 55001:55001 -p 55002:55002 wazuh/wazuh
4. Once the image is running, you can access the Wazuh web interface by going to http://localhost:1516 in your web browser.
5. Use the default username and password (admin and wazuh) to log in and start using Wazuh.

TheHive5

TheHive is an open-source security incident response platform that is used by organizations to manage, investigate, and respond to security incidents. It is designed to be scalable, flexible, and easy to use, and can be integrated with other security tools such as Wazuh, MISP, and Elasticsearch.

TheHive includes features such as a web-based interface, case management, collaboration tools, and integrations with external systems. It allows security teams to respond to incidents quickly and effectively, and to track and manage their investigations from start to finish. TheHive is built on top of the popular open-source ELK (Elasticsearch, Logstash, and Kibana) stack, and can be easily installed and configured on premises or in the cloud.

Installation Guide

To install TheHive using Docker, you will need to have Docker installed on your system. Once you have Docker installed, you can follow these steps to install TheHive:

1. Pull the TheHive Docker image from Docker Hub by using the following command: docker pull thehiveproject/thehive
2. Run the TheHive Docker image by using the following command: docker run -it -p 9000:9000 -v /your/data/directory:/data thehiveproject/thehive
3. Once the image is running, you can access the TheHive web interface by going to http://localhost:9000 in your web browser.
4. Use the default username and password (admin and admin) to log in and start using TheHive.

OpenCTI

OpenCTI (Open Cyber Threat Intelligence) is an open-source platform for managing cyber threat intelligence (CTI). It is designed to be scalable, flexible, and easy to use, and can be integrated with other security tools such as TheHive and MISP.

OpenCTI provides a range of features for managing CTI data, including a web-based interface, data model and schemas, import and export tools, and collaboration tools. It allows security teams to collect, analyse, and share CTI data, and to use that data to support their investigations and incident response efforts. OpenCTI is built on top of the popular open-source ELK (Elasticsearch, Logstash, and Kibana) stack, and can be easily installed and configured on premises or in the cloud.

Installation Guide

To install OpenCTI using Docker, you will need to have Docker installed on your system. Once you have Docker installed, you can follow these steps to install OpenCTI:

1. Pull the OpenCTI Docker image from Docker Hub by using the following command: docker pull opencti/opencti
2. Run the OpenCTI Docker image by using the following command: docker run -d -p 8080:8080 -v /your/data/directory:/data opencti/opencti
3. Once the image is running, you can access the OpenCTI web interface by going to http://localhost:8080 in your web browser.
4. Use the default username and password (admin and opencti) to log in and start using OpenCTI.

Comparison

TheHive, Wazuh, and OpenCTI are all open-source tools that are used for security incident response and management. However, each tool has its own specific focus and capabilities.

TheHive is a security incident response platform that is used to manage, investigate, and respond to security incidents. It provides features such as a web-based interface, case management, collaboration tools, and integrations with other security tools. TheHive is focused on helping security teams quickly and effectively respond to incidents and manage their investigations.

Wazuh is a security information and event management (SIEM) tool that is used to monitor and protect IT infrastructure. It collects, analyses, and alerts on data generated by IT assets, and can be used to detect threats, vulnerabilities, and compliance issues. Wazuh is focused on providing security visibility and helping organizations to prevent and respond to security incidents.

OpenCTI is a platform for managing cyber threat intelligence (CTI) data. It provides tools for collecting, analysing, and sharing CTI data, and can be integrated with other security tools. OpenCTI is focused on helping organizations to manage and use CTI data to support their security operations.

In summary, TheHive, Wazuh, and OpenCTI are all useful tools for security incident response and management, but they have different focuses and capabilities. TheHive is focused on incident response, Wazuh is focused on security monitoring and protection, and OpenCTI is focused on CTI management. It is possible to use these tools together in a coordinated manner to support a comprehensive security operations program.

Conclusion

After extensive research and testing into all three open-source alternative solutions to google chronicles, it is clear that Wazuh shares the most similarities with google chronicles and therefore is the recommendation for a SIEM solution.

References

https://docs.docker.com/compose/

https://www.youtube.com/watch?v=8DuptAc5GdE&ab_channel=TaylorWalton

https://www.youtube.com/watch?v=xiJOzZQ3YwM&ab_channel=TaylorWalton

https://github.com/OpenCTI-Platform/opencti/blob/master/README.md