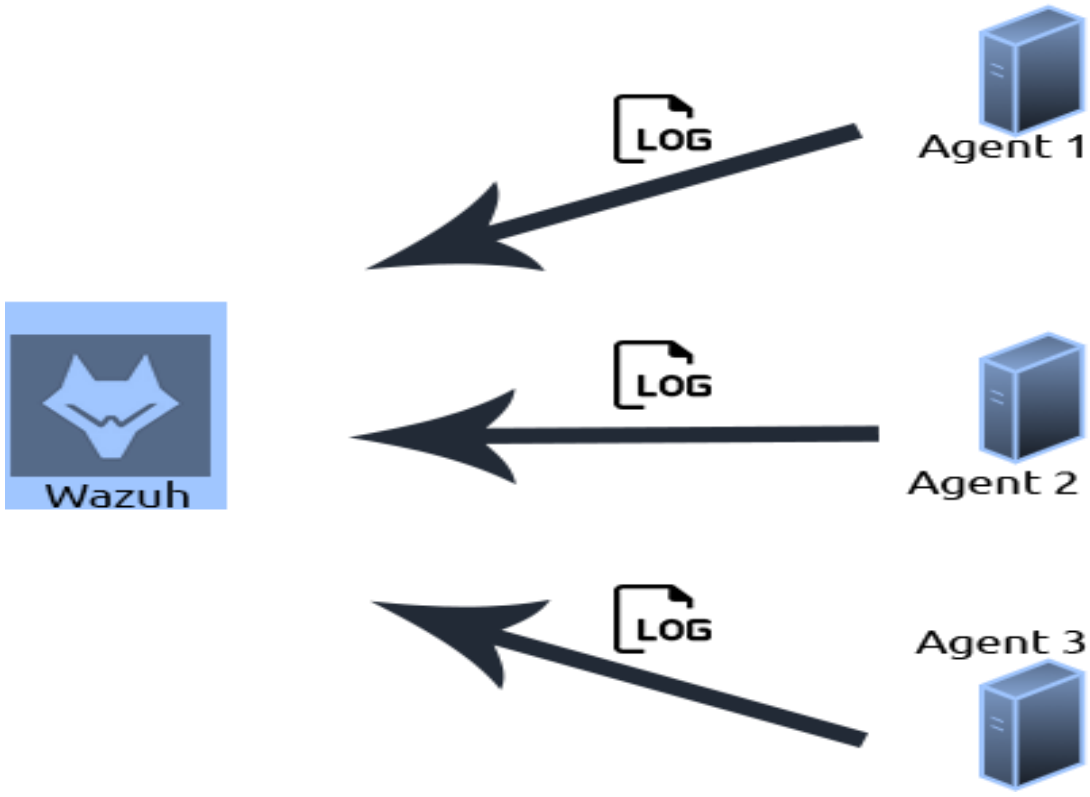
Introduction

This report provides a comprehensive overview of Wazuh, an advanced Endpoint Detection and Response (EDR) solution tailored to meet the evolving cybersecurity needs of modern organizations. It delves into the core functionalities, deployment procedures, and practical applications of Wazuh, shedding light on its effectiveness in safeguarding digital assets against potential threats.

https://tryhackme.com/p/Damiano254

- **Wazuh EDR Software Solution Overview**
  - **Task 1: Introduction**
  - Created in 2015, Wazuh is an open-source, freely available, and extensive EDR solution. It can be used in all scales of environments. Wazuh operates on a management and agent module. Simply, a device is dedicated to running Wazuh named a manager, where Wazuh operates on a management and agent model where the manager is responsible for managing agents installed on the devices you'd like to monitor. Let's look at this model in the diagram below:

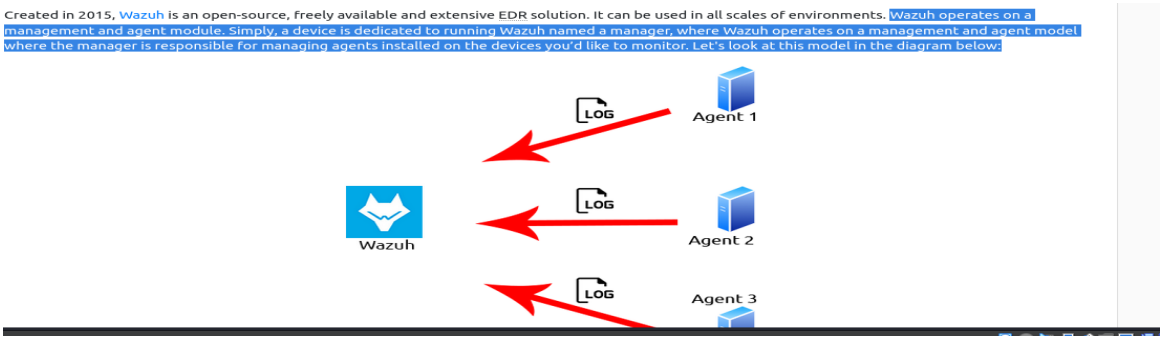


Answer the questions below:

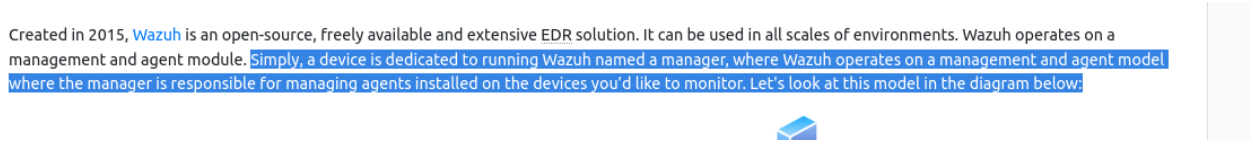
- When was Wazuh released?
  - **2015**

Created in 2015, Wazuh is an open-source, freely available and extensive EDR solution. It can be used in all scales of environments. Wazuh operates on a management and agent module. Simply, a device is dedicated to running Wazuh named a manager, where Wazuh operates on a management and agent model where the manager is responsible for managing agents installed on the devices you'd like to monitor. Let's look at this model in the diagram below:

- What is the term that Wazuh calls a device that is being monitored for suspicious activity and potential security threats?
    - **Agent**



- Lastly, what is the term for a device that is responsible for managing these devices?
    - **Manager**



- **Task 2: Required: Deploy Wazuh Server**
- Connected to the TryHackMe network and deployed the Wazuh management server attached to this task and waited a minimum of five minutes before visiting the Wazuh server on HTTP://MACHINE_IP.
- Once it has started, log in using the following credentials:

1. Username: Wazuh
2. Password: eYa0M1-hG0e7rjGi-lRB2qGYVoonsG1K

- **Task 3: Wazuh Agents**
    - Devices that record the events and processes of a system are called agents.
    - Agents monitor the processes and events that take place on the device.

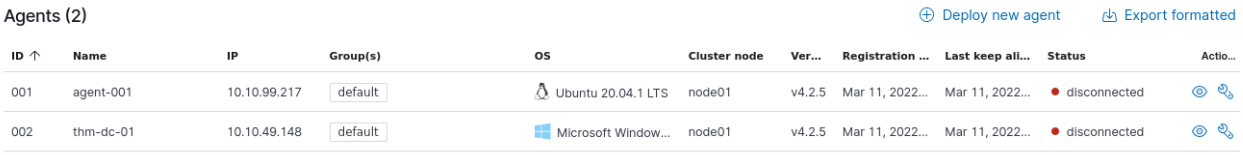
Answer the questions below:

- Ensure that you are logged in to the Wazuh management server on HTTPS://MACHINE_IP

Navigate to the "Agents" tab by pressing Wazuh -> Agents

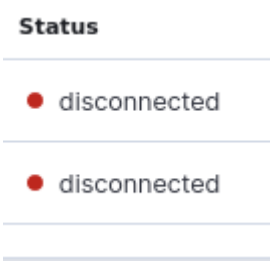
- How many agents does this Wazuh management server manage?

  2

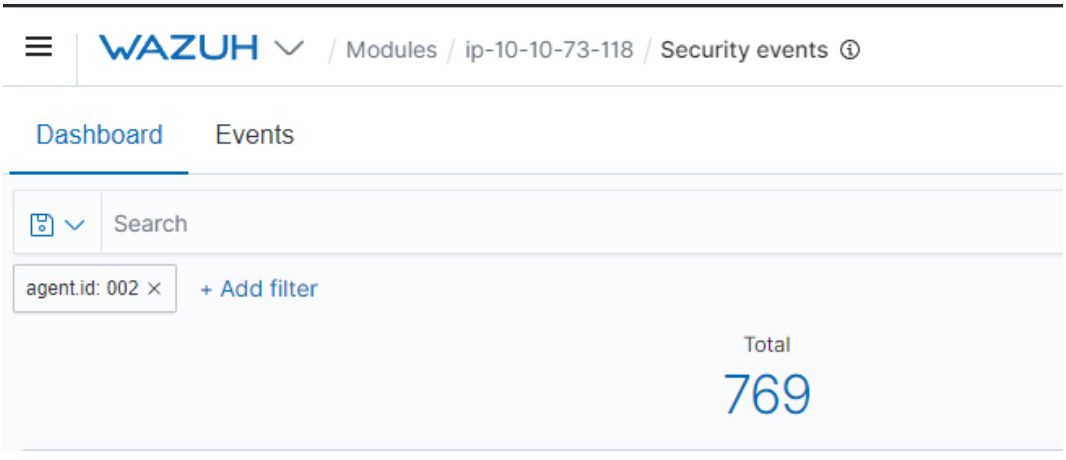


- What is the status of the agents managed by this Wazuh management server?

  Disconnected



- **Task 4: Wazuh Vulnerability Assessment & Security Events**
  - Wazuh’s Vulnerability Assessment module scans an agent's operating system for vulnerabilities.
  - Security event monitor records both successful and unsuccessful authentication attempts.



Ensure that you are logged in to the Wazuh management server on HTTPS://MACHINE_IP

No answer needed

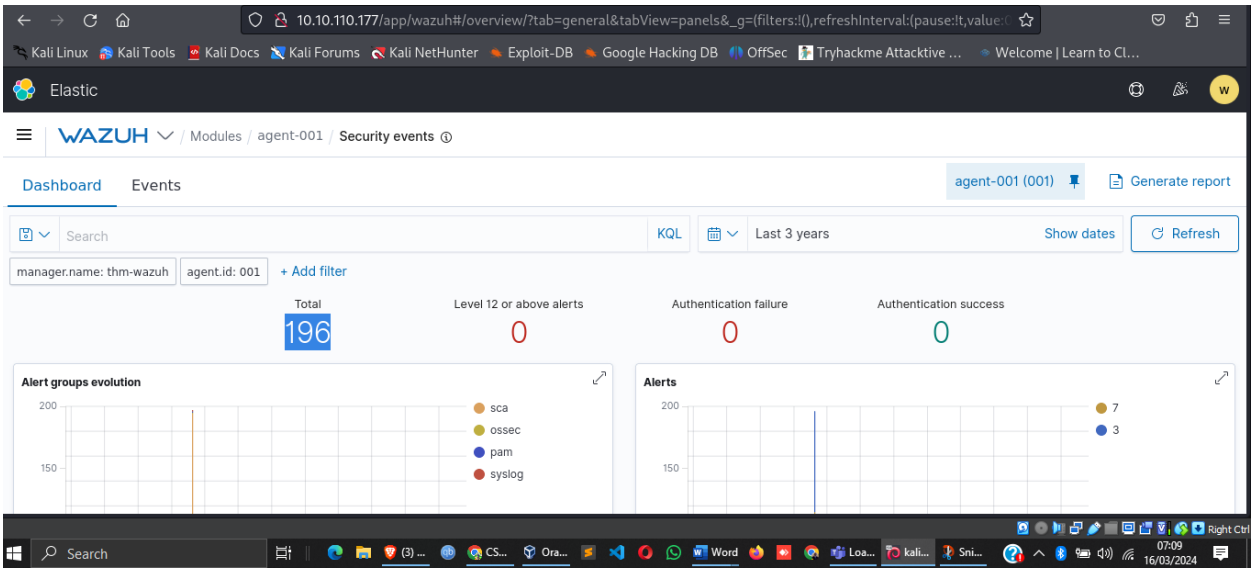
- Navigate to the Agents tab by pressing Wazuh -> Agents like so
  No answer needed
- Select the agent named "AGENT-001"

  No answer needed

- How many "Security Event" alerts have been generated by the agent "AGENT-001"?

  Note: You will need to make sure that your time range includes the 11th of March 2022

  196



- **Task 5: Integrating Wazuh with ELK Stack**
- The Elastic Stack is a powerful collection of open-source tools for search, log analysis, and visualization. Wazuh can be integrated with the Elastic Stack to provide an even more comprehensive security monitoring solution.

  To integrate Wazuh with the ELK Stack, follow these steps:

  - Install the Elastic Stack (Elasticsearch, Logstash, Kibana) on your server.
  - Configure Logstash to receive logs from Wazuh and forward them to Elasticsearch.
  - Install the Wazuh app for Kibana to visualize Wazuh alerts and data in Kibana.

- **Task 6: Monitoring Logons with Wazuh**

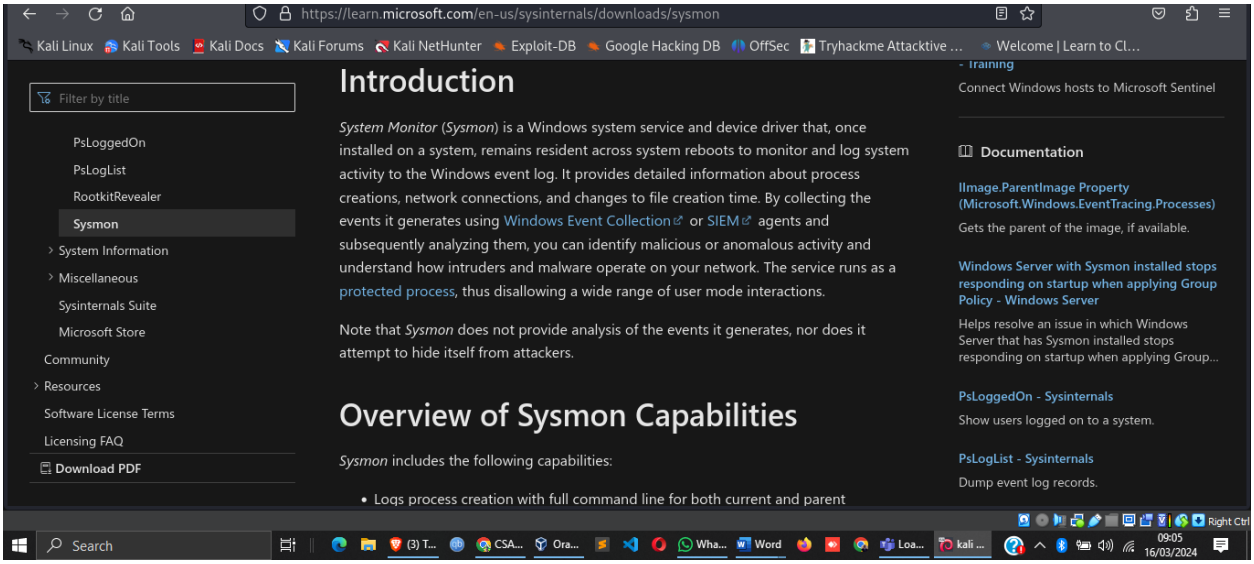
  - Wazuh's security event monitor records both successful and unsuccessful authentication attempts.

  - For reference, alerts are stored in a specific file on the Wazuh management server: /var/ossec/logs/alerts/alerts.log.

- **Task 7: Collecting Windows Logs with Wazuh**

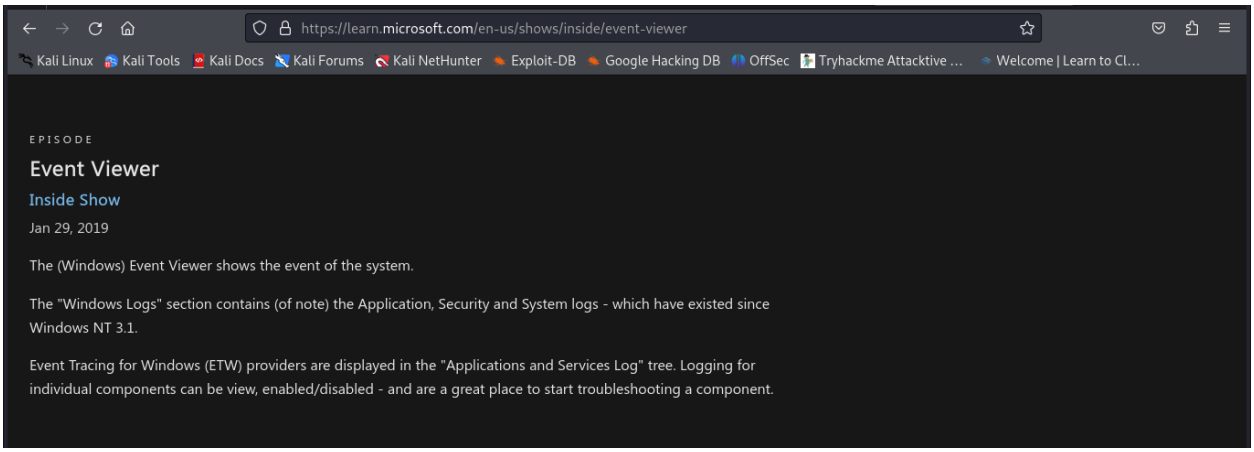
- Wazuh can aggregate events recorded by Sysmon on Windows systems for processing.
- To configure Sysmon, provide a configuration file (in XML format) to the Sysmon application. Then, configure the Wazuh agent on the Windows server to send Sysmon events to the Wazuh management server. Finally, add Sysmon as a rule on the Wazuh management server to visualize these events.
- **Answer the questions below**
- What is the name of the tool that we can use to monitor system events?

  Sysmon



- What standard application on Windows do these system events get recorded to?

  Event Viewer

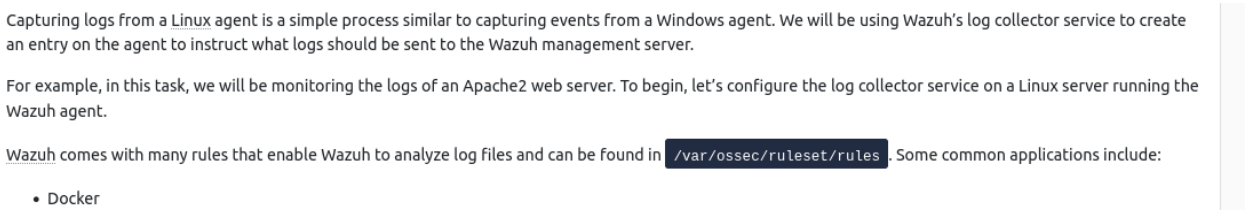


- **Task 8: Collecting Linux Logs with Wazuh**
  - Capturing logs from a Linux agent is similar to capturing events from a Windows agent**.**

  Answer the questions below

  - What is the full file path to the rules located on a Wazuh management server?

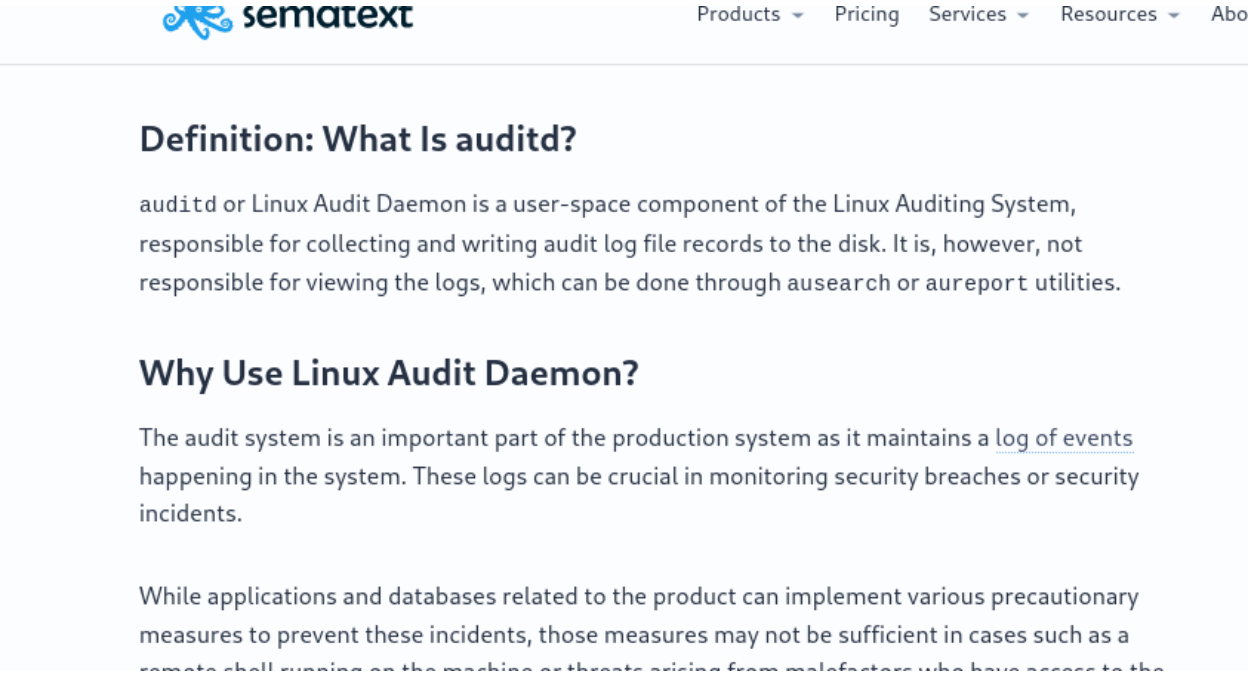
/var/ossec/ruleset/rules



- **Task 9: Auditing Commands on Linux with Wazuh**
    - Wazuh utilizes the auditd package to monitor system events on Debian/Ubuntu and CentOS operating systems.

      Answer the questions below

        - What application do we use on Linux to monitor events such as command execution?
          Auditd



        - What is the full path & filename for where the aforementioned application stores rules?
          /etc/audit/rules.d/audit.rules

- **Task 10: Wazuh API**

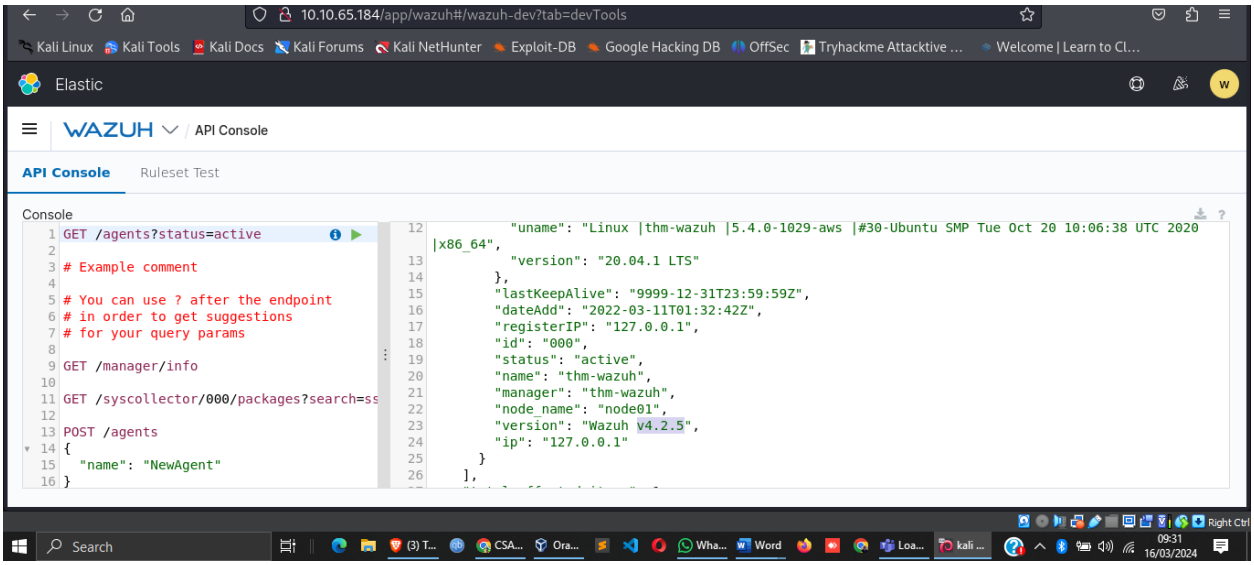
  The Wazuh management server features a rich and extensive API that allows interaction with the Wazuh management server using command-line tools like curl. To use the API, authentication is required, after which a token is provided for further interaction.

  Answer the questions below

- What is the name of the standard Linux tool that we can use to make requests to the Wazuh management server?
  Curl

  In this task, we will be using a Linux machine with the `curl` tool installed to interact with the Wazuh management server API. First, we will need to authenticat ourselves by providing a valid set of credentials to the authentication endpoint.

- What HTTP method would we use to retrieve information for a Wazuh management server API?
  GET
- What HTTP method would we use to perform an action on a Wazuh management server API?
  PUT
- Navigate to Wazuh's API console.
  No answer needed
- Use the API console to find the Wazuh server's version.
- Note: You will need to add the "v" prefix to the number for this answer. For example v1.2.3
  v4.2.5



- **Task 11: Generating Reports with Wazuh**

  Wazuh's reporting module allows users to generate reports summarizing events that have occurred on an agent. Reports can be generated from different views, such as security events, and downloaded as PDF files.

  - Use Wazuh's "Report" feature to generate a report of an agent.
    no answer needed
  - Navigate to the Wazuh "Report" dashboard
    No answer needed
  - Analyse the report. What is the name of the agent that has generated the most alerts?
    agent-001

- **Task 12: Loading Sample Data**
    - The Wazuh management server comes with sample data that can be loaded to demonstrate its capabilities further.
    - The Wazuh management server comes with sample data that can be loaded to demonstrate its capabilities further. Sample data can be imported from the Wazuh settings, which includes data for various modules such as security events.
    - After importing the sample data, users can explore the newly imported data in the Wazuh dashboard to understand how Wazuh processes and visualizes security events.

Conclusion

In conclusion, Wazuh stands as a robust and versatile EDR solution, offering extensive features for monitoring, analyzing, and responding to security events across diverse environments. With its user-friendly interface, flexible deployment options, and powerful API, Wazuh empowers organizations to enhance their security posture and safeguard against emerging threats effectively.