Task 4: Security Onion Console

Objectives

- Understand the role of Security Onion in a Security Operations Center (SOC) and how it could be used by SOC analysts to enhance network security.
- Explore the Security Onion Console, which includes the Dashboard, Alerts, and Cases interfaces
- Understand the general components of Security Onion, including the tools it provides for intrusion detection, log analysis, and network monitoring.

Security Operations Center (SOC)

A Security Operations Center (SOC) is a centralized team or facility within an organization that is responsible for monitoring and responding to cybersecurity incidents. The primary objective of a SOC is to ensure the security of an organization's information systems and data. SOC analysts use specialized tools and techniques to detect, investigate, and respond to security incidents in real-time.

Security Onion

Security Onion, developed by Security Onion Solutions, LLC, is a free and open-source platform used for monitoring network, host, and enterprise, as well as managing logs (collecting and analyzing them). With its variety of package collections, Security Onion delivers a scalable solution that is ideal for incident response and forensics in high-demand environments. Security Onion is designed to help SOC analysts detect and respond to security incidents more effectively by providing a centralized platform for security monitoring.

Analyst Machine

A full-time SOC analyst may use a dedicated Analyst Machine to carry out his work. This allows the analyst to investigate potentially malicious artifacts such as PCAPs without affecting the Security Onion deployment/workstation. In a real-world scenario, multiple analysts need to access the same Security Onion Console simultaneously. In this case, each analyst uses a dedicated machine, ensuring that they all have access to the console and can work without impacting each other's tasks. Having a dedicated analyst machine also helps improve security, isolation, performance, customization, and maintenance, which are critical factors for enhanced cybersecurity.

Security Onion Console

After completing the installation and configuration of Security Onion, we have executed the "so-allow" command and set the "Analyst Role" to the Analyst IP address. Now you should be able to use the web browser to access the Security Onion Console. This serves as the central hub of the Security Onion platform, and mastering it will enable you to maximize your network management abilities. Within this document, you will learn how to leverage various tools, including:

- **Alerts Interface:** to see what security Onion has detected so far
- **Dashboard Interface:** for general overview of all logs collected
- **Cases Interface:** If any alert of interest you could escalate it to Cases to collect more evidence and analyze observables.

Task 4.1: Introduction

Once you login to Security Onion Console, you'll notice the user menu in the upper right corner. This allows you to manage your user settings and access documentation and other resources.
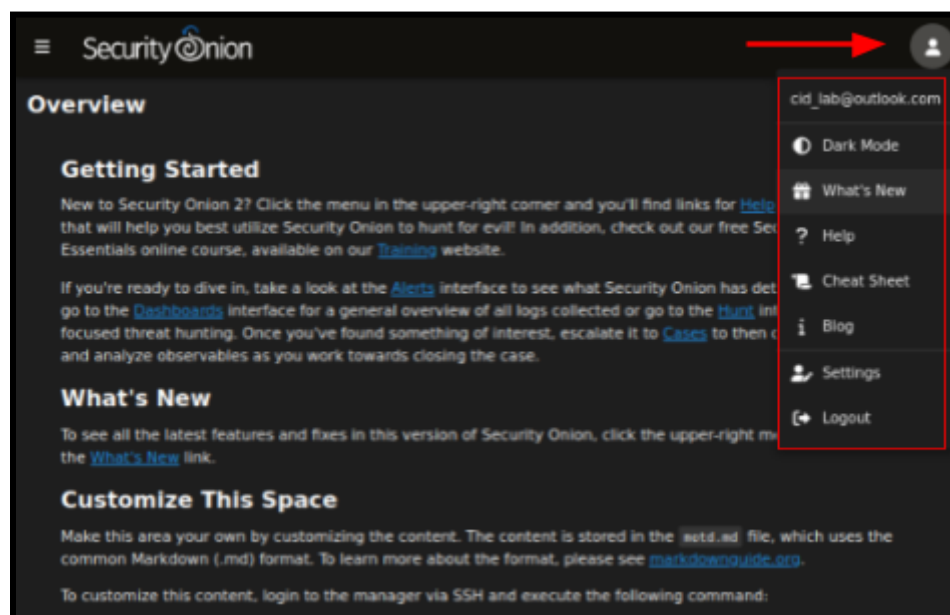
You'll notice a number of menu items on the left-hand side. The upper section includes the tools, which are built into Security Onion itself: Alerts, Hunt, PCAP, and Grid. Found in the lower section are other **third-party tools** which are integrated into Security Onion: Kibana, Grafana, CyberChef, Playbook, FleetDM, TheHive, and Navigator. Those tools are external and will spawn separate browser tabs. We will not be using all of these tools during this lab, but they each could come in handy when monitoring the network.
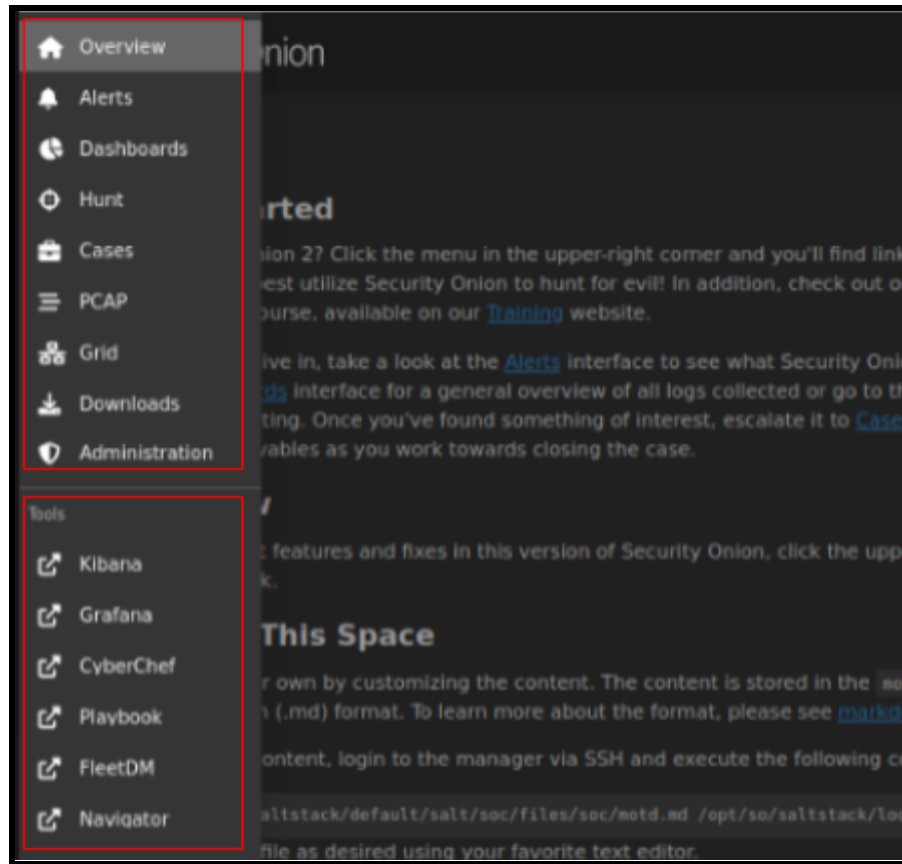
Task 4.1.1: Choose one of those <u>external tools</u> supported by Security Onion, conduct a quick internet search to learn more about it, and explain how this tool could be helpful for a Cybersecurity Analyst.

Task 4.2: Dashboard Interface

This interface provides a way for Analysts to quickly generate visualization of data. We will explore the basis of the Dashboard Interface including some built in visualization that come with the Security Onion platform

Components of the Dashboard Interface

There are many components within the Dashboard interface, please refer to the picture below.

1- Options
2- Time Selector
3- Basic Metrics
4- Query Field
5- Group Metrics
6- Events Table
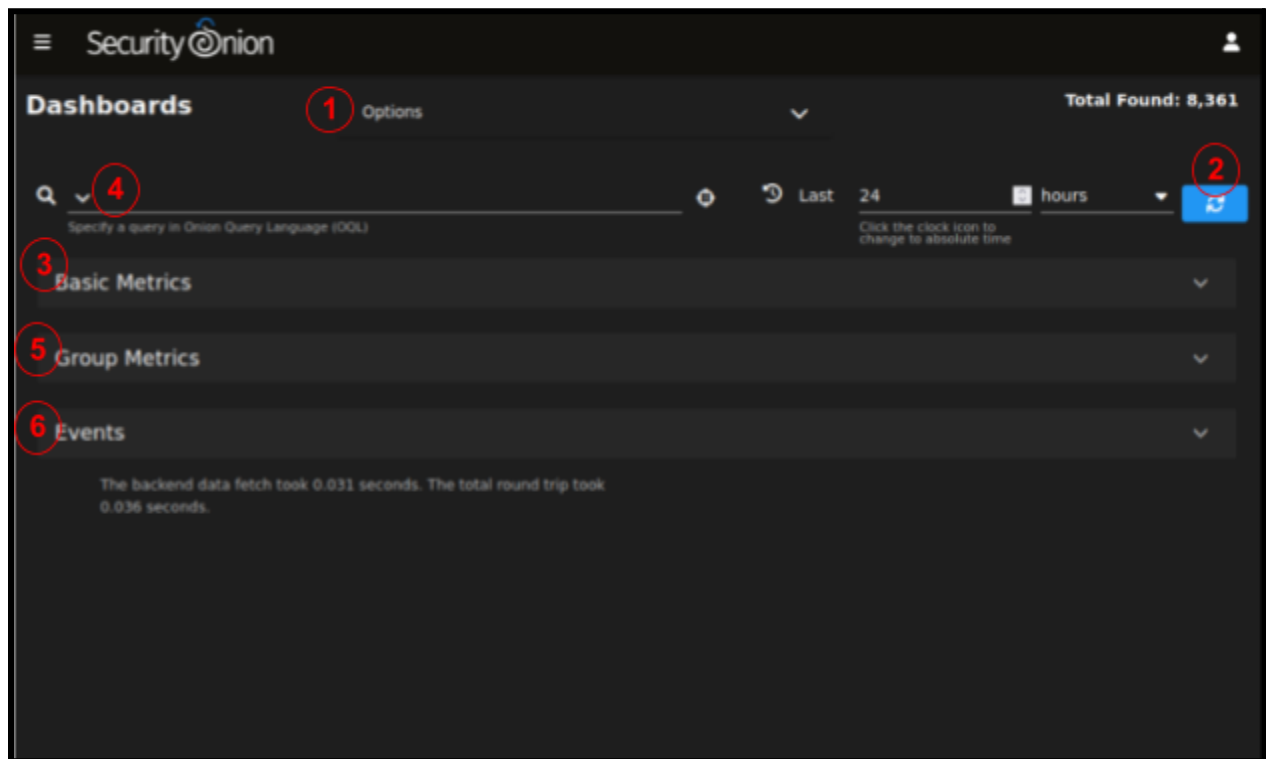
1- Options

At the top of the page, there is an Options drop-down menu that allows you to set options such as Auto Apply, Exclude case data, Automatic Refresh Interval, and Time Zone.
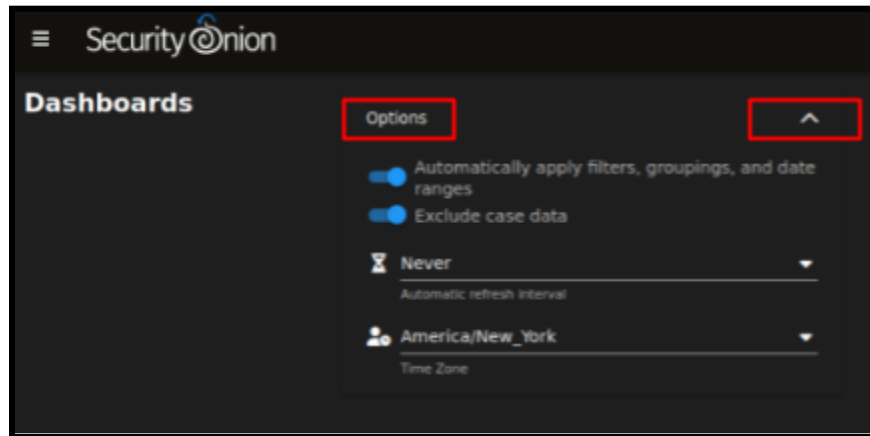
Task 4.2.1: What is the benefit of the Automatic Refresh Interval setting ?

2- Time Selector

In the upper right there is a time selector that allows you to designate what timeframe you would like to pull data from
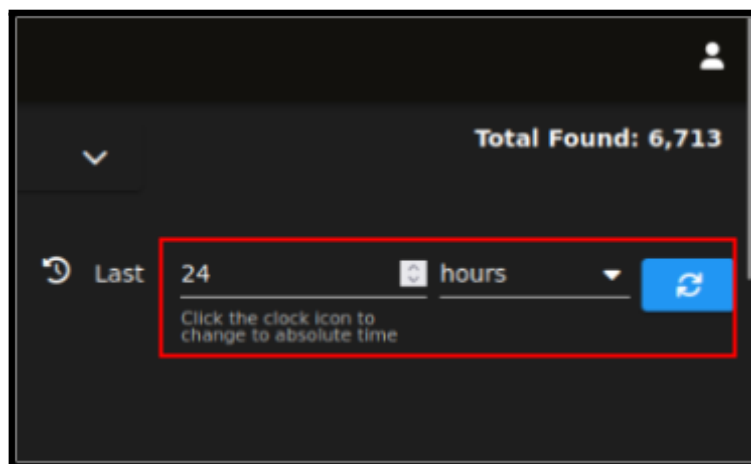
3- Basic Metrics

The first section of output contains a **Most Occurrences** visualization, a **timeline visualization**, and a **Fewest Occurrences** visualization.
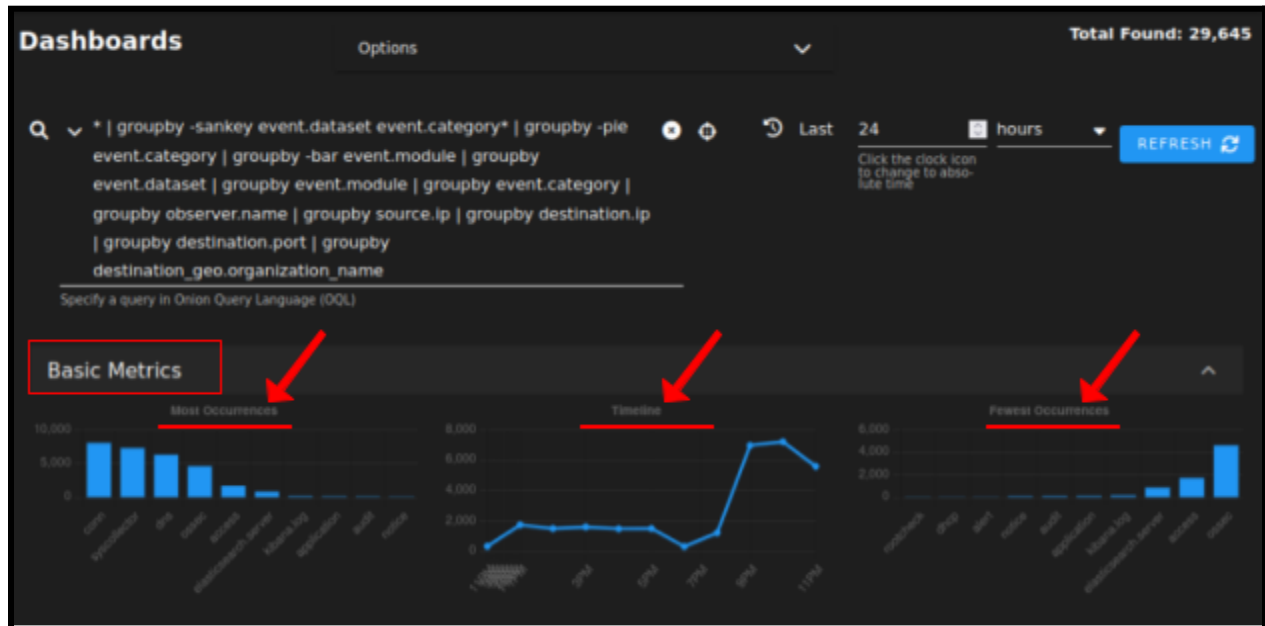
4- Query Field

In the upper left corner you can see there is a query box (field) that allows you to specify a query in a query language. The easiest way to get started is to click the query drop down box and select one of the **predefined dashboards**. These predefined dashboards cover most of the major data types that you would expect to see in a Security Onion deployment: NIDS alerts from Suricata, HIDS alerts from Wazuh, protocol metadata logs from Zeek or Suricata, endpoint logs, and firewall logs.

Task 4.2.2: Examine the predefined dashboard for DNS network traffic. What is the query used to help the Analyst examine the DNS data? Examine the predefined dashboard for HTTP network traffic, including the query used for that specific dashboard. Specify the unique components that were found in each specific query.

Beside the **predefined dashboards** there is a one specific **default dashboard**. Each time you pivot to the Dashboard Interface, you will be given the default query, which is the following:
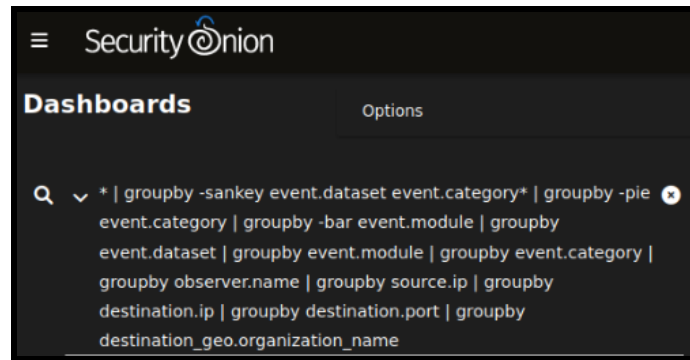
"* | groupby -sankey event.dataset event.category* | groupby -pie event.category | groupby -bar event.module | groupby event.dataset | groupby event.module | groupby event.category | groupby observer.name | groupby source.ip | groupby destination.ip | groupby destination.port | groupby destination_geo.organization_name".

This query start with a star "*" which means retrieve all the data'. Then you can see that the data is first grouped by a sanky diagram using event.dataset and even.category. Then the data is grouped into a pie based on the event categories and so on.
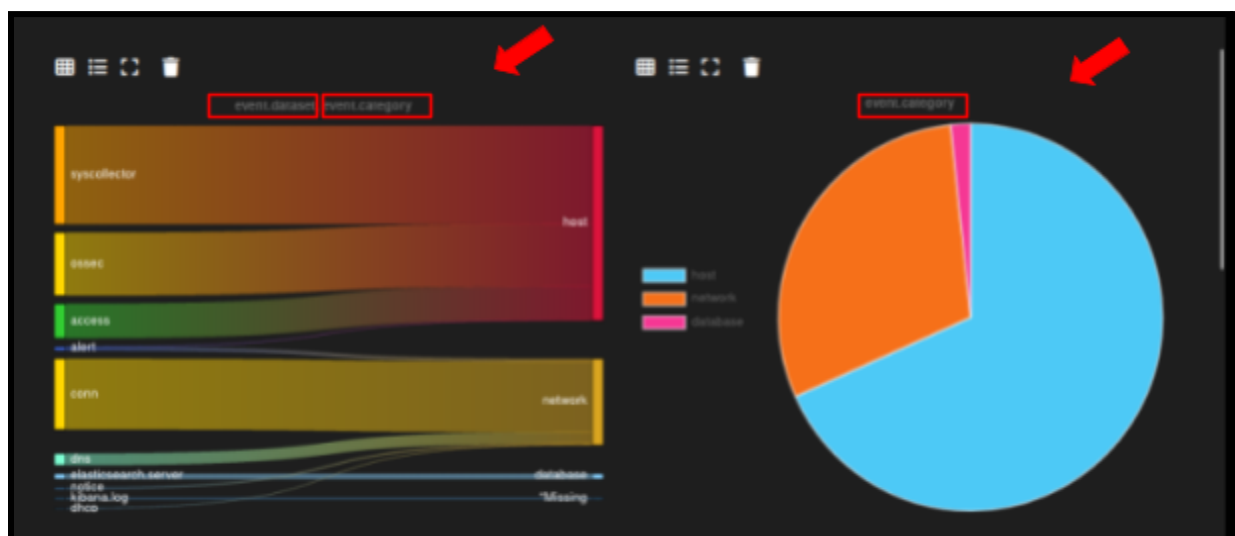
Task 4.2.3: What is the name of the query language that the Analyst could use to customize the dashboard interface of Security Onion?

5- Group Metrics

It consists of one or more data tables or visualizations that allow you to stack (aggregate) arbitrary fields. The result of your query will be displayed in this section

Task 4.2.4: Explain the Sankey graph in general. What does the thickness of the lines mean? Based on this diagram make an observation about two different event datasets and events categories.
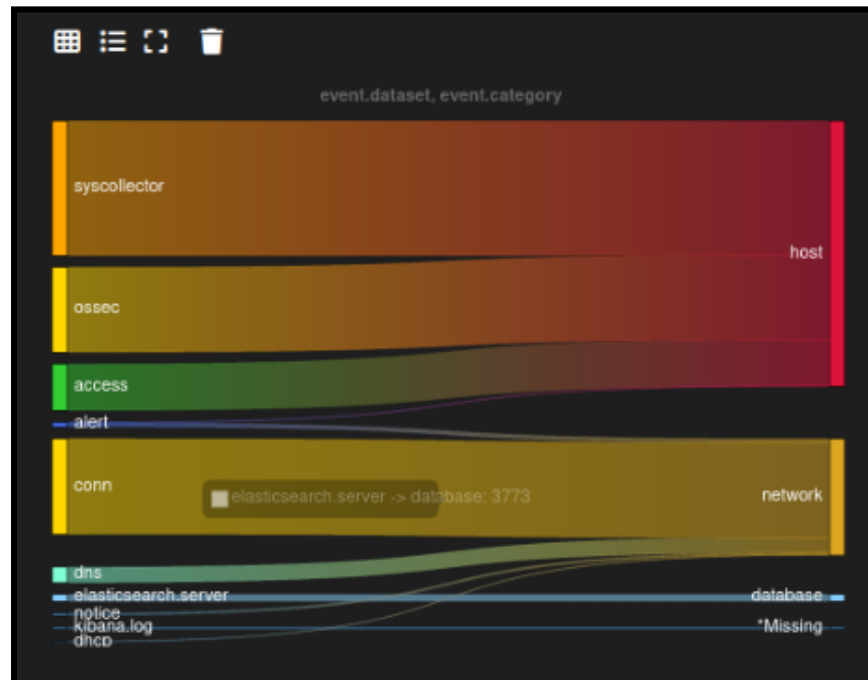
Task 4.2.5: Explore each one of the four options on top of the Sankey Diagram. Show each option and explain the differences between each specific option.
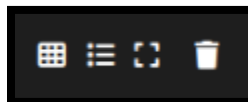
Task 4.2.6: While you are using the **default dashboard**, refer to the pie chart that you have, click on "host", what do you notice? How could this feature be helpful for the SOC Analyst?
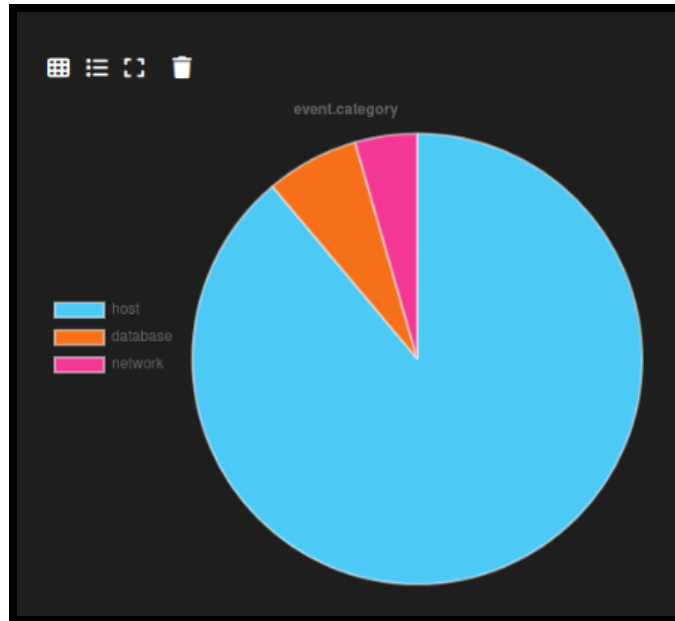
Task 4.2.7: Modify the **default dashboard** query to display the same dashboard components but for data from a specific IP address. Show the query the basics Metrics and the Group Metrics along with the Events Table

Task 4.2.8: Modify the previous query to perform all the following simultaneously
- Represent the data in a pie chart based on the distention ip
- Represent the data in a bar chart based on the distention port
- Group the data based on the destination ip (Table)
- Group the data based on the destination port (Table)

Please show the query, both graphs and both tables.

Task 4.2.9: Conduct internet search to explain what does the "event.module" stands for?

Task 4.2.11: Conduct a search to figure out what "OSSEC" stands for? explain what it is used for and how that is related to the alerts that you are seeing?

Task 4.2.12: Explain the relationship between OSSEC, Wazuh and Security Onion.

Task 4.2.13: Based on your understanding of the meaning of the event module, make an observation based of the following bar diagram
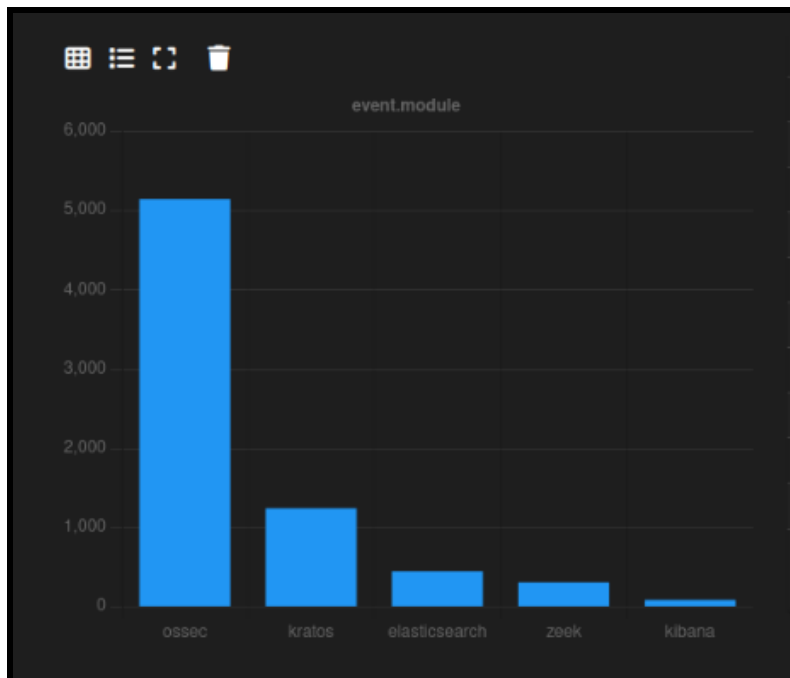
6- Events

The third and final section of the page is a data table that contains all search results and allows you to **drill** into individual search results as necessary. Clicking the table headers allows you to **sort ascending or descending**.

Starting from the left side of each row, there is an arrow which will expand the result to show all of its fields. When you click the arrow to expand a row in the Events table, it will show all of the individual fields from that event. Look for the event with the message "update role [analyst]". Click on the arrow on the left side and examine the specific details of that event.

Task 4.2.14: After you examine the details of the previous event, maneuver the mouse pointer to the value of the "Message" field. As an analyst you want to further examine this specific field across all different network traffics. Right click on it and select "New Group by". Explain your observation.

Task 4.2.15: Change the previous table to a pie chart. What is the most frequent Message across all network traffic. Now eliminate that specific Message type and examine the frequency of the rest of the messages.

Task 4.3 Alerts Interface
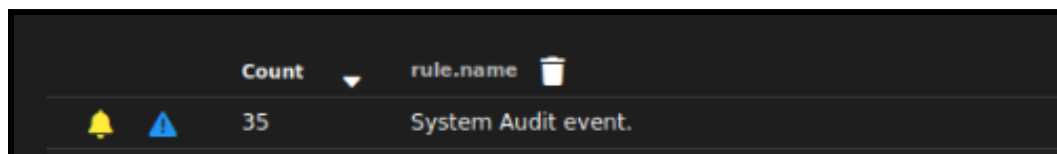
Alerts Interface presents an overview of the alerts generated by Security Onion. This interface enables you to easily examine details, switch to the Hunt or PCAP interface, and raise alerts to Cases. As this is a new installation and there is minimal network activity, all those alerts are related to the Security Onion VM itself. Furthermore, these alerts have been categorized as low-risk alerts.

Notice all events that were detected by Security Onion and triggered the same alert are grouped together. For example, there has been 35 events that triggered the same alert, which is based on the rule name "System Audit event"

Notice the Query specified at the top of the Alerts Interface "Group By Name, Module". The Alerts interface by default organizes each specific alert type by its name and the module engine.
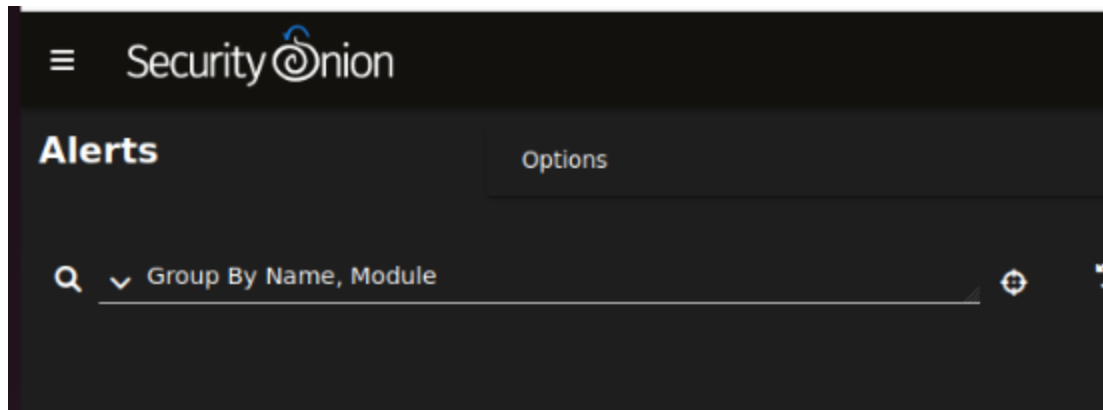
Task 4.3.1: What is the difference between having the query "Ungroup" and the query "group by name, module"

Task 4.3.2: How many total alerts has Security Onion generated for the last 3 days?

The Alerts Interface has similar components as the Dashboard Interface. Check the Options section.
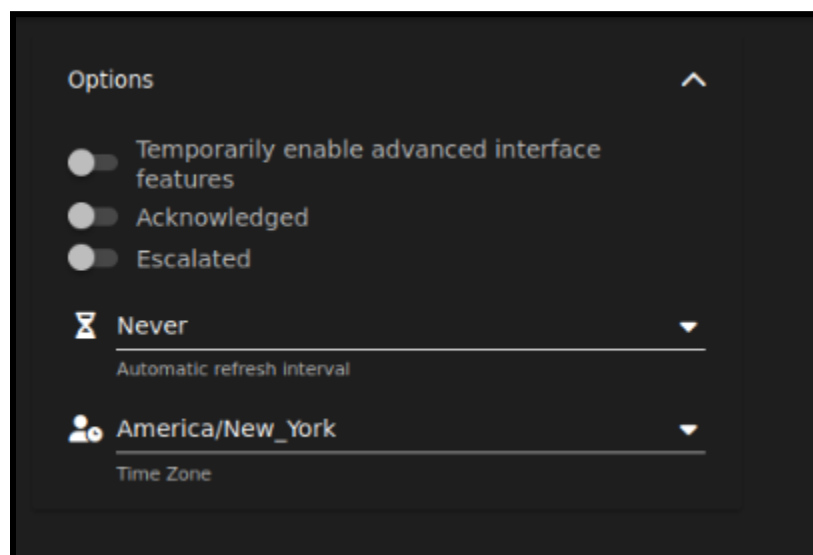
Task 4.3.3: Examine the Options section for Alerts Interface. Explain the function of Acknowledged toggle and Escalated toggle and how would the SOC Analyst utilize both

Task 4.3.4: Click on "options" and select "Temporarily enable advanced interface features". Convert the entire table of grouped alerts into a pie chart or bar chart and make a general observation about all alerts generated based on your network traffic

Based on the severity level, all of these events are likely routine events. To view more information about the **PAM: Login Session Opened** (which has a count of 6 alerts), hover over its row and click on it. Once the menu appears click on **[Drilldown]**.

Task 4.3.5: Based on the previous step, explain the change in the query and the data represented now?

Task 4.3.6: Specify the filter that was used to display only the alerts related to "PAM:login session opened"

This table displays the specific alerts identified as [PAM:Login Session Opened]. You can expand each individual event by clicking on the arrowhead.

To view all the metadata that Wazuh has collected and reported regarding this event, you need to scroll down the page.

Task 4.3.7: Examine the message filed, and determine when was this particular event generated? Also, explain what "PAM" means?
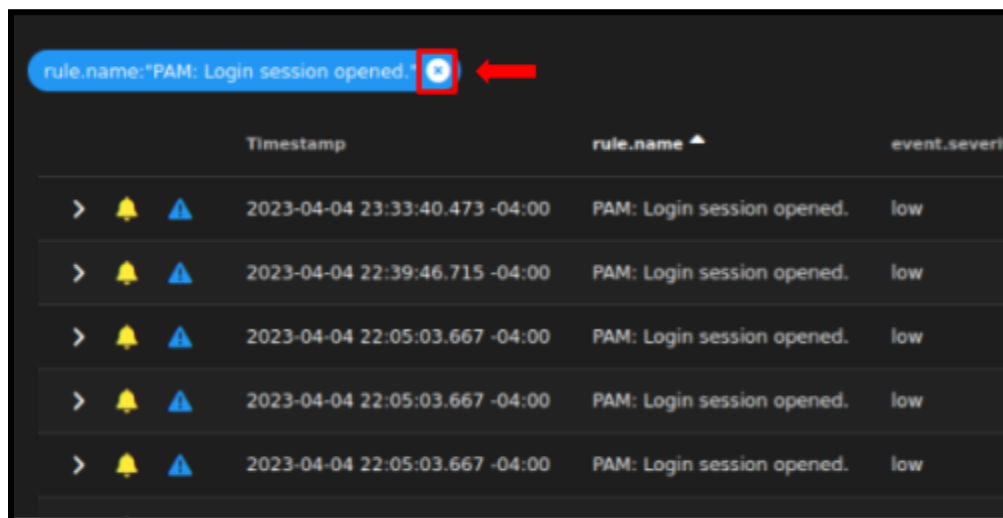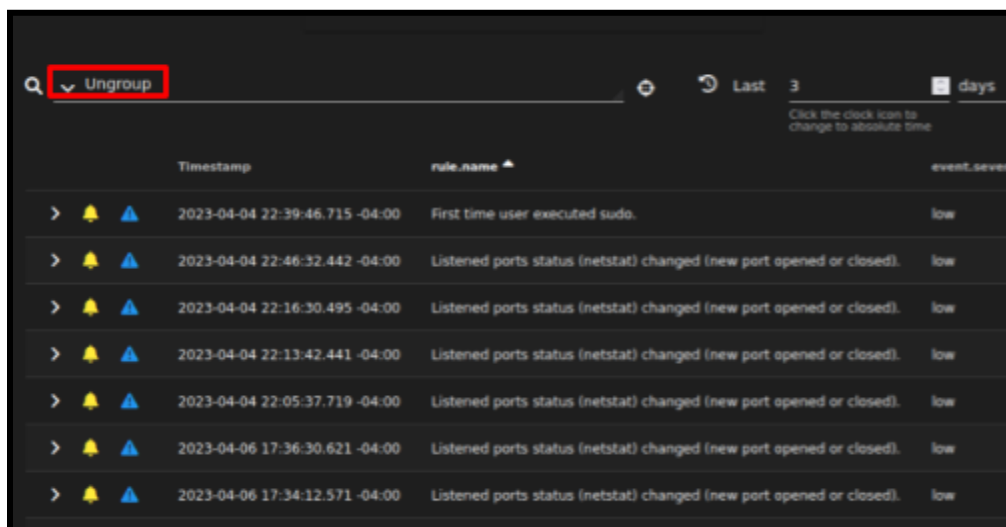
Scroll back up to the top of the table. Notice the bubble that says rule.name:"rule.name:"PAM: Login session opened."". This indicates that all the alerts you see are filtered by this rule name. Click the x to remove this filter.

When you see the Alerts table reload, it looks different. You see all of the individual rules, and the word Ungroup in the text field above.

If you click the down arrow next to the query field, you will see several **predefined queries**, including the **default one** that was selected when you first pivot to the Alerts page, "Group by Name, Module" Select this query.
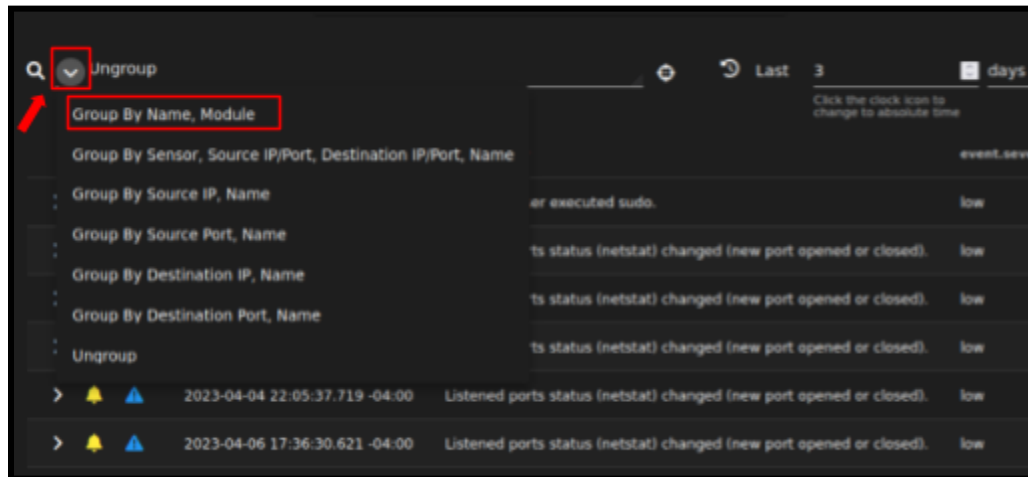
You are back where you started, with several uninteresting alerts. In the next document, we are going to establish our own alerts and generate malicious traffic for Security Onion to detect.