[First name] [Last name]
CS457: Computer and Network Security
SIEM Software Lab
Created by Andrew Tringali, Cary Keesler, Chuck Anderson, and Juno Meifert.

Lab slides and lab video are included with this assignment.

Procedure:

1. Follow the instructions in the video to install the Wazuh server and agent on a computer. Paste a screenshot of the “Endpoints Overview” page in Wazuh showing that the agent is connected.

2. In the “Discover” tab, follow the instructions in the video to use a filter to view the history of successful authentication attempt (“authentication_success”) events. Paste a screenshot of at least one of the events.

3. In the “Visualizations” tab, follow the instructions in the video to create a chart for successful authentication attempts. Paste a screenshot of the filter you used to create the visualization, as well as a screenshot of the visualization itself.

4. In the same way as Question 3, create a visualization for failed authentication attempts (“authentication_failed”), and save it. Paste a screenshot of the filter you used to create the visualization, as well as a screenshot of the visualization itself.

5. In the “Visualizations” tab, follow the instructions in the video to create a table of successful authentication attempts (“authentication_success”) per user. Paste a screenshot of the table.

6. In the same way as Question 5, create a table of failed authentication attempts (“authentication_failed”) per user. Paste a screenshot of the table.

7. In the “Dashboards” tab, follow the instructions in the video to create a dashboard. We can call this dashboard “Auth”. Add the visualizations you created in the earlier questions to this dashboard, and save it. Paste a screenshot of the finished dashboard below.

8. In the “Alerts” tab, follow the instructions in the video to create an alert that is fired if there are more than 5 successful login attempts in the span of a minute. Paste a screenshot of the alert below. Once you’ve created the alert, run “sudo su” a few times to set it off. Paste a screenshot of the alert’s history showing that it has been fired.

Reflection:

1. Explore the events listed in the “Discover” tab. What kind of events is Wazuh generating about the computer? Is there something it’s notifying you about that you haven’t thought about before? Do you see anything you think is a false positive?

2. Try exploring the Visualizations tool beyond the tasks described in the lab. Share one feature you find interesting and a possible use case for it.

3. How could Wazuh (or other SIEM software) be used to identify potential threats or other unusual system activity in a work environment? Could you see yourself using it in the future?