## **2) Lab5-2: Security Information and Event Management (SIEM) (35-points)**

Lab **Submission**

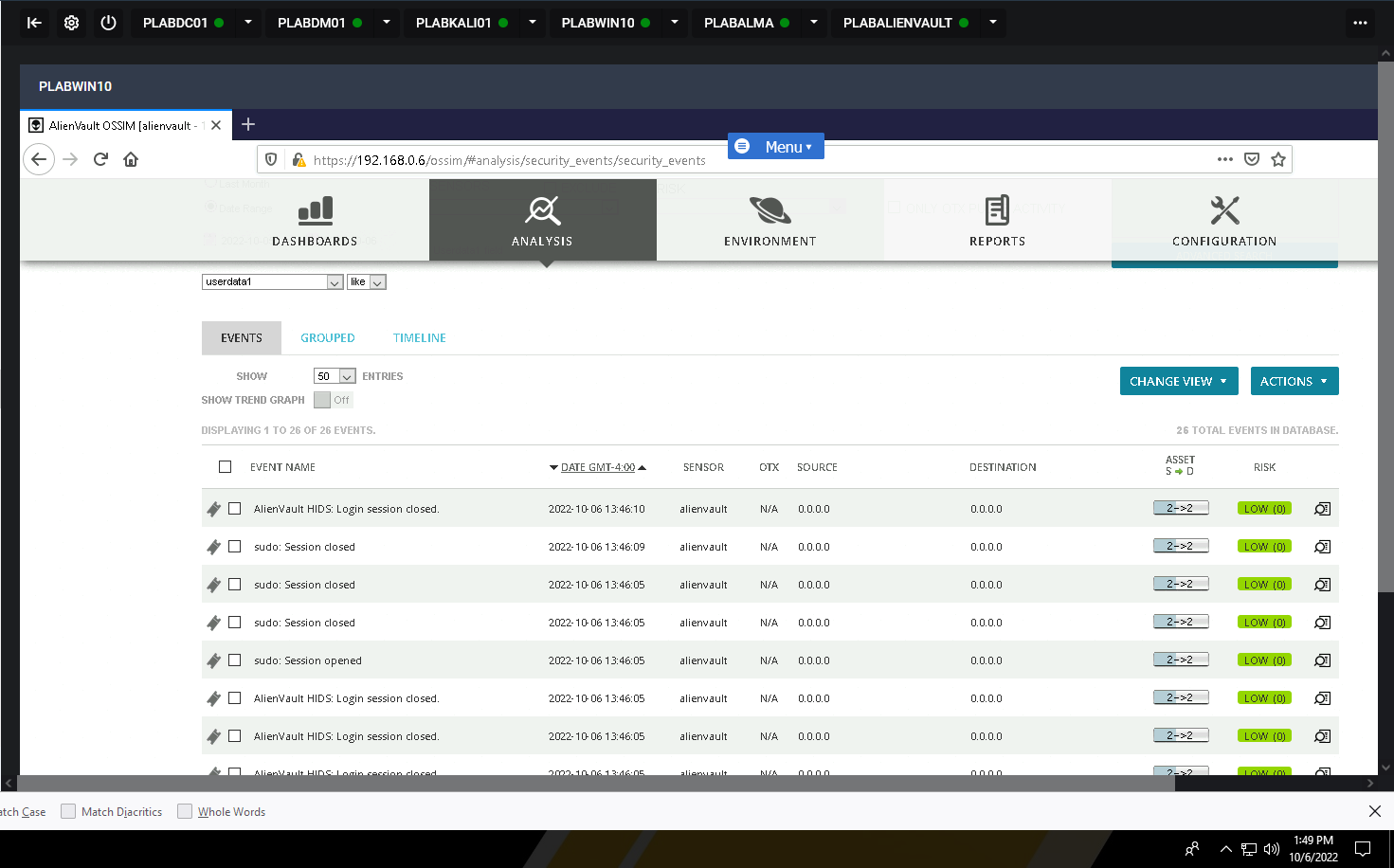
Please make sure to do all the exercises.

**Exercise 1 - Security Information and Event Management (SIEM)**

**Task 1 - Understanding the SIEM Dashboard**

#### **Perform the Step 1 - Step 8 Understanding the SIEM Dashboard and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**

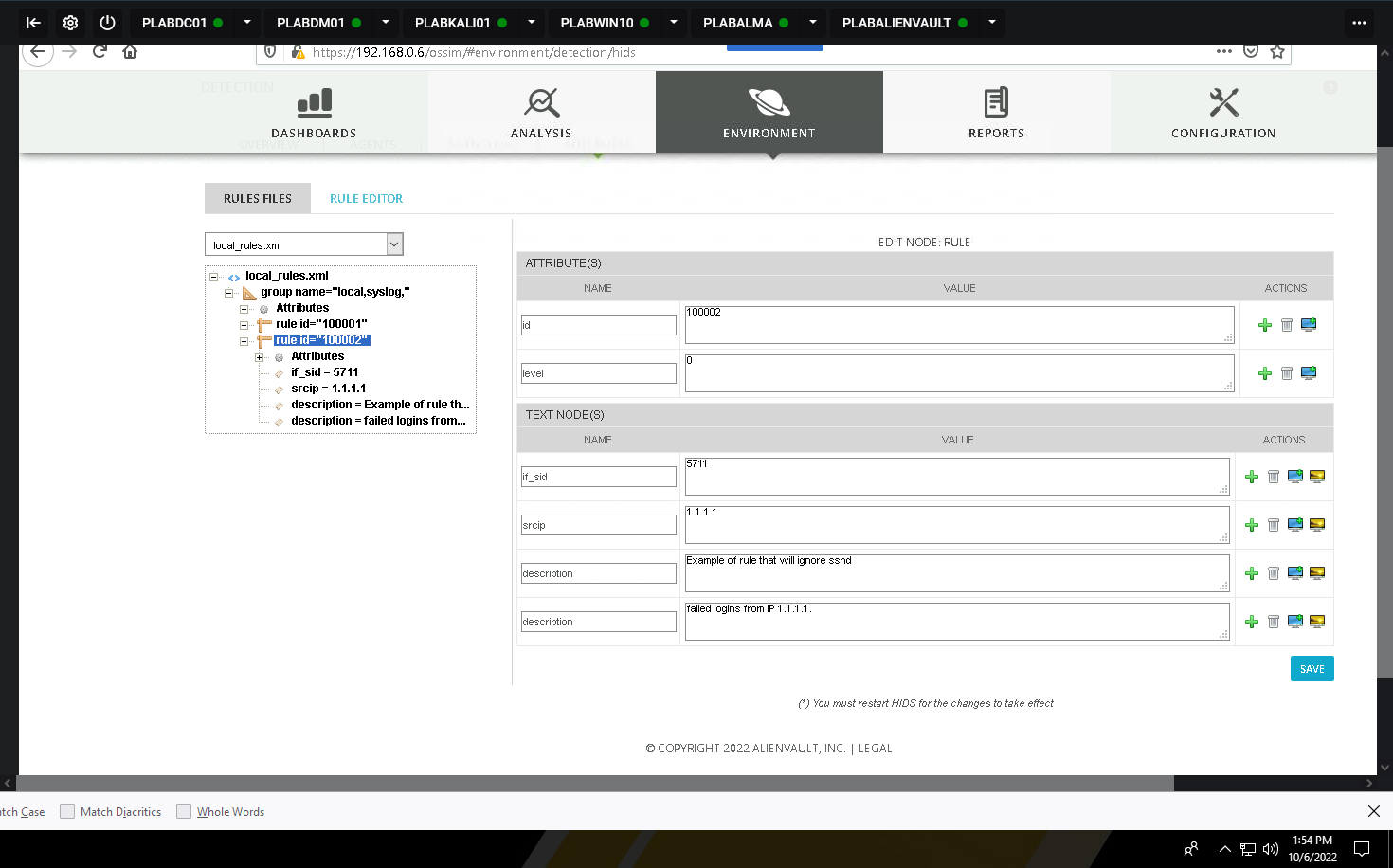
**Understanding SIEM dash**

****

**Task 2 - Write Rules using SIEM**

Perform the Step 1 - Step 11Write Rules using SIEM and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

**Written rules using SIEM**

****

· Save the report as a docx file (first name and last name: ex. Awad\_Mussa2.docx)

· Keep this file as you will upload it when you take the lab4’s quiz.