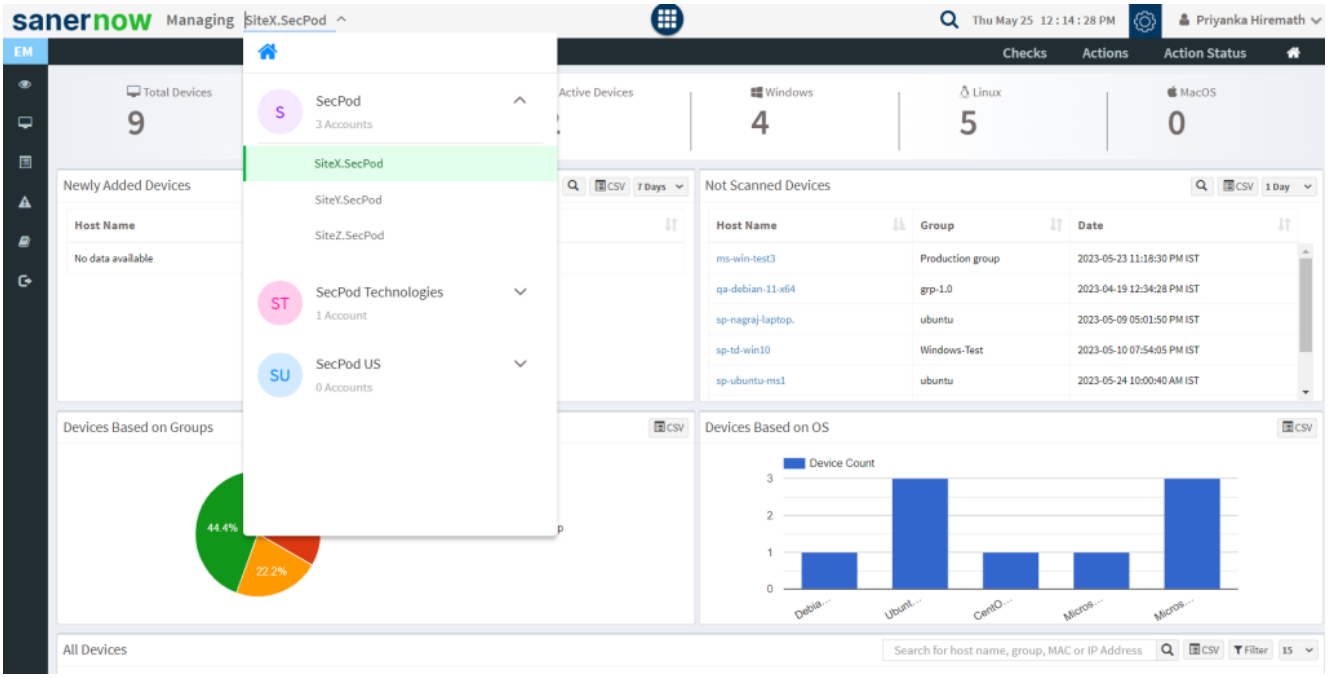
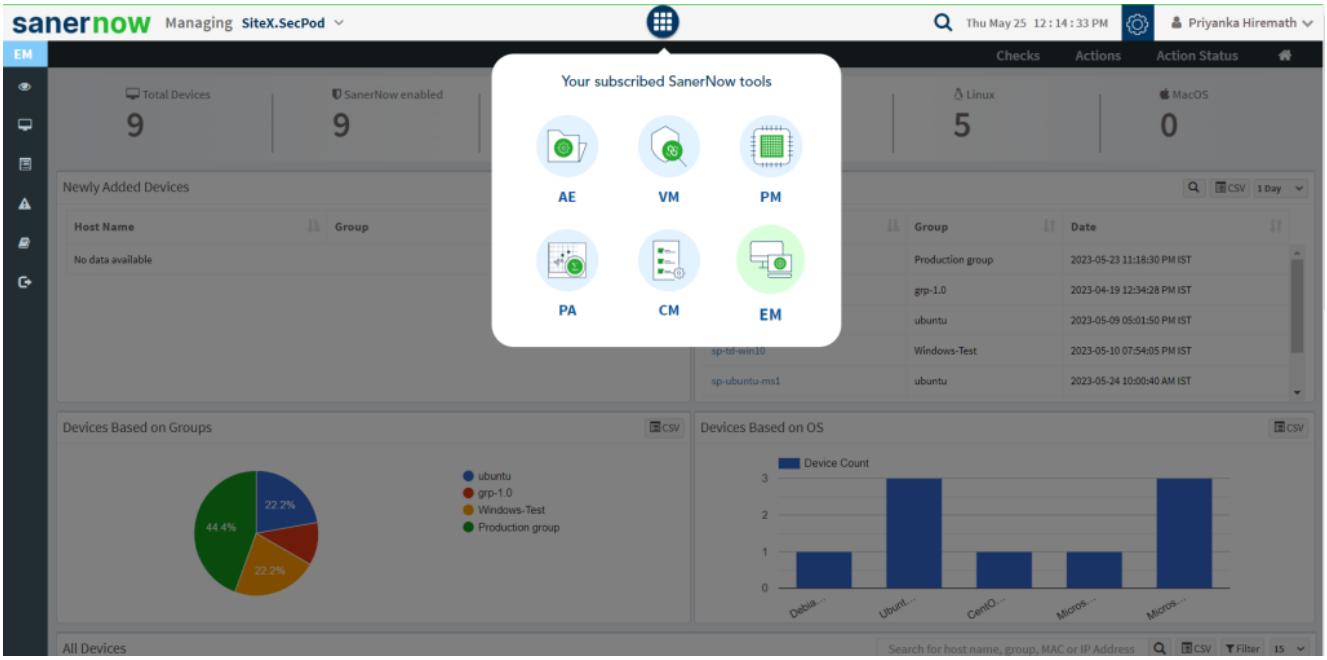
How to collect all security events from Windows Events Log?

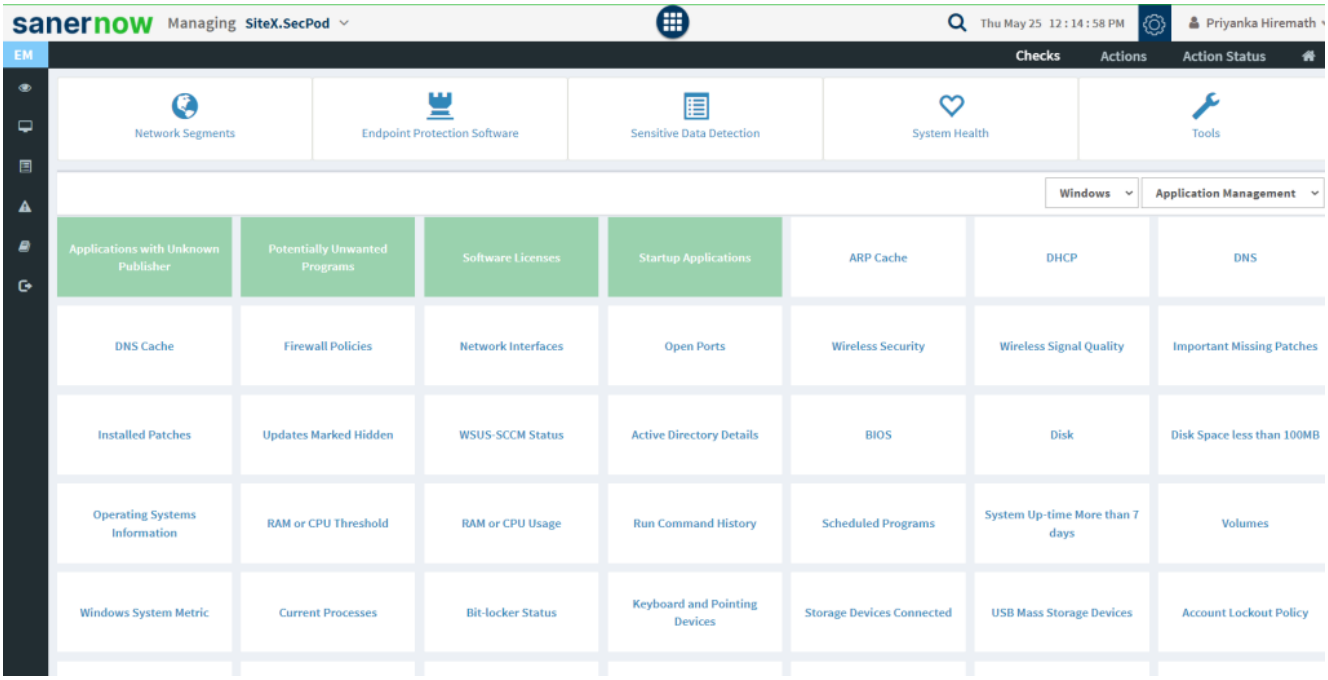
1. Login to SanerNow and choose the **Organization** and corresponding **Account** to collect all security events from Windows Events Log.



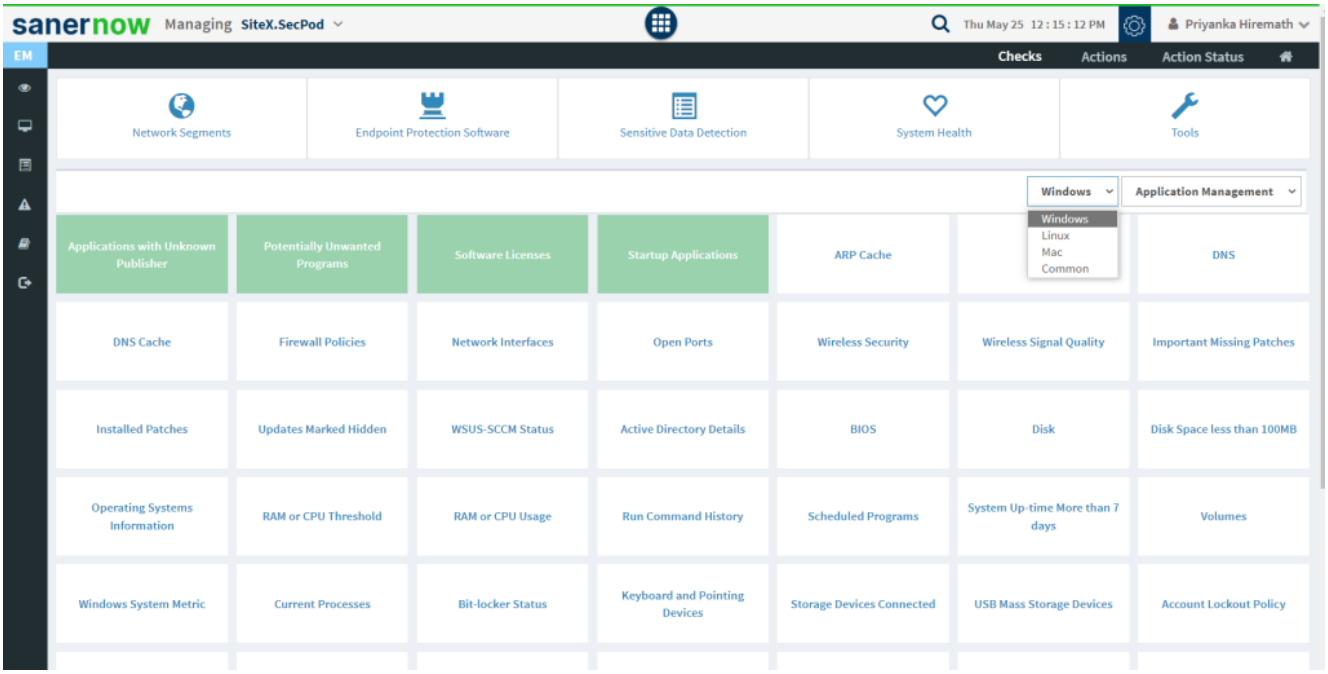
2. Select the **Endpoint Management** module

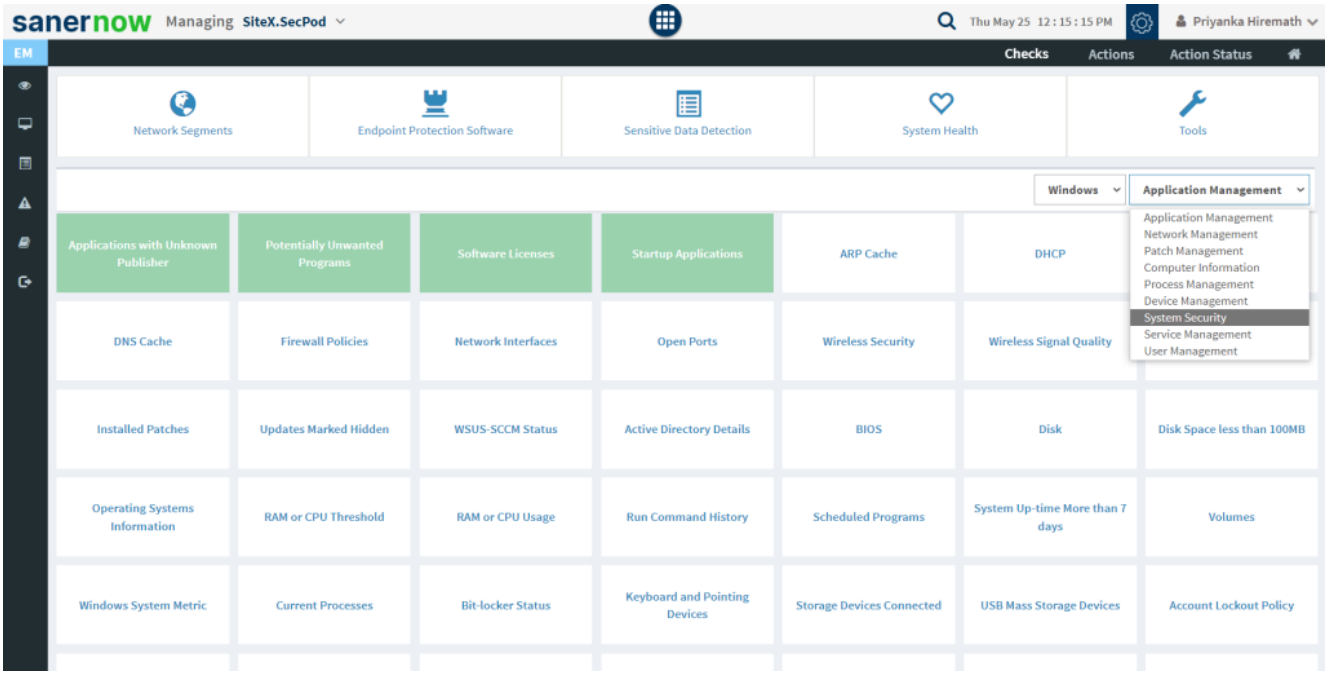


3. Click on **Checks** on the right top corner

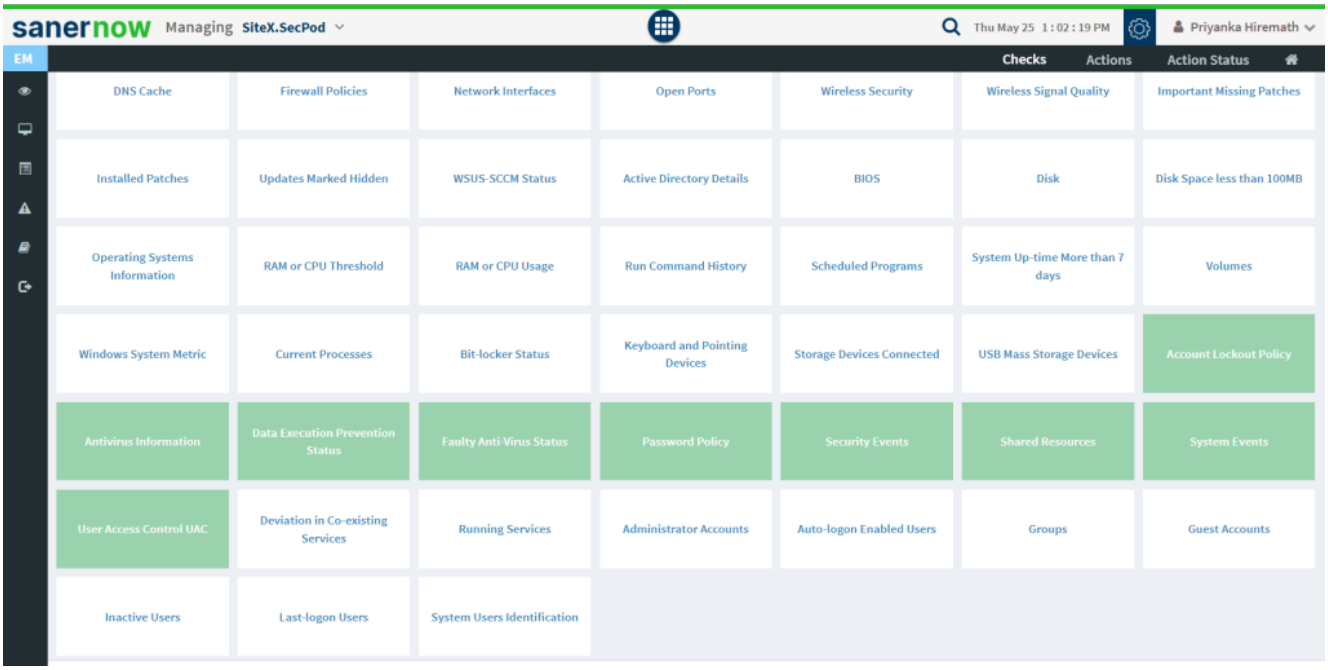


4. From the drop-down menu, select **Windows** and **System Security**



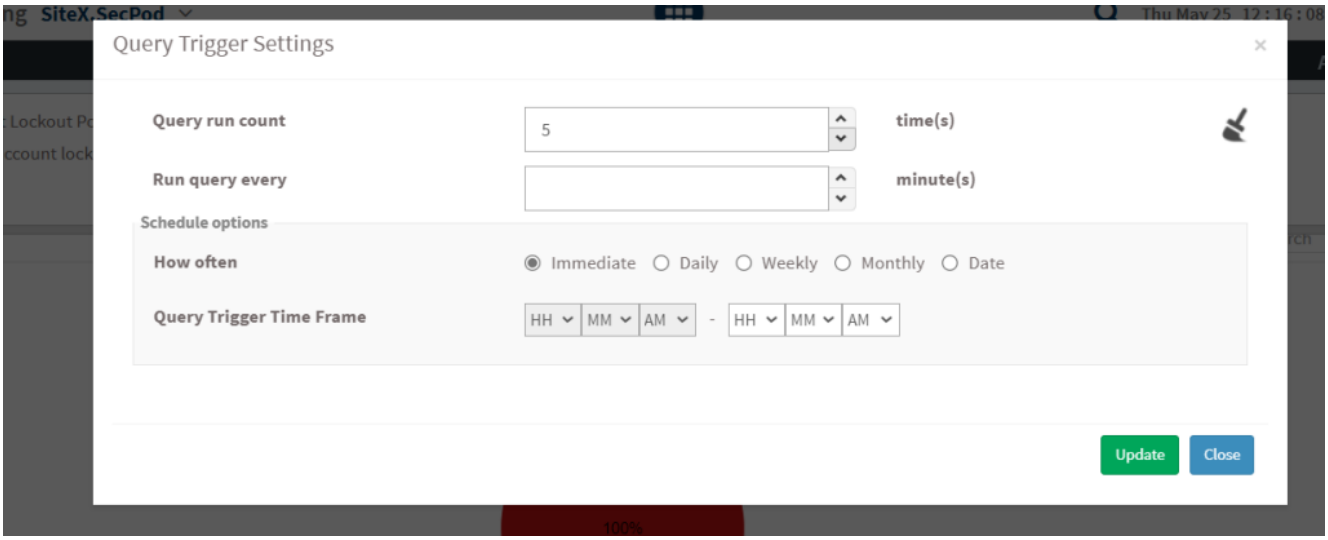


5. Followed by scrolling down, the checks are highlighted in green. Select **Security Events**.

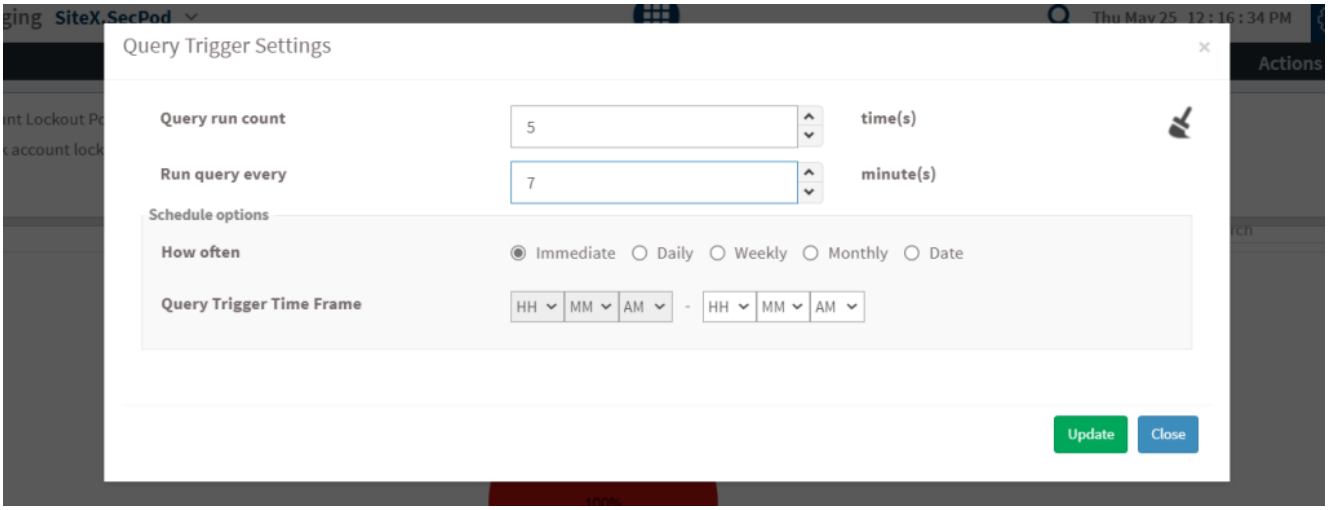


6. To schedule the query execution for the agent, click on **Trigger**. You need to fill up query trigger settings:

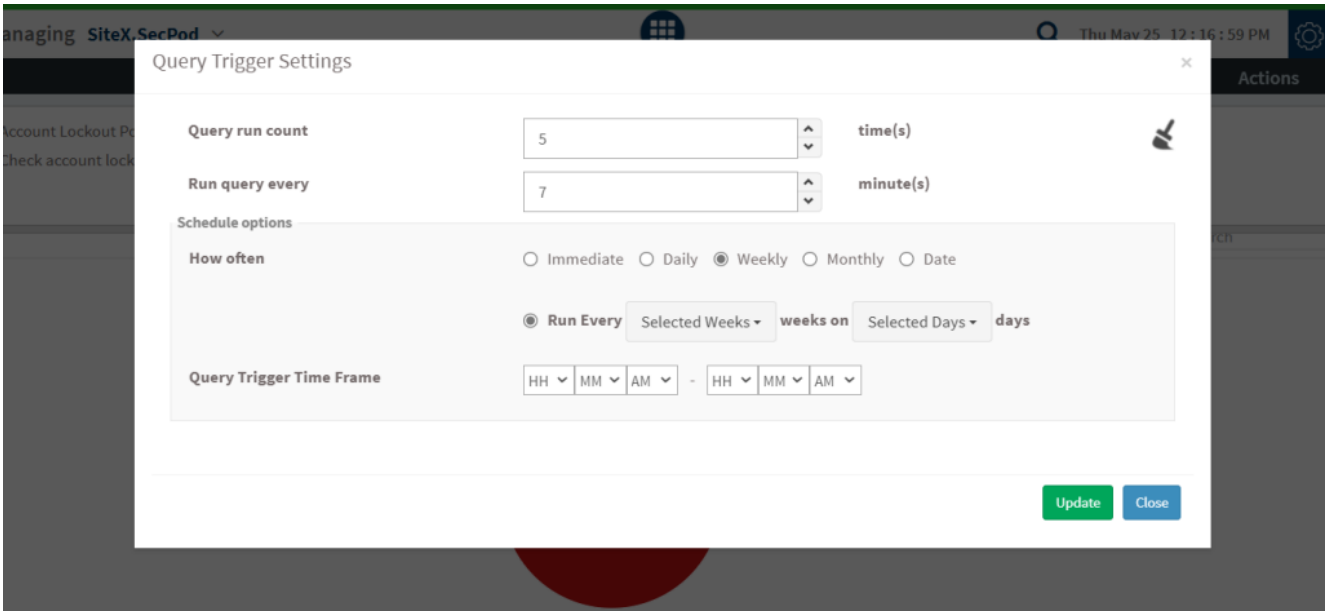
- Set the Query run count time in seconds.



- Set the time in minutes to run the query often.

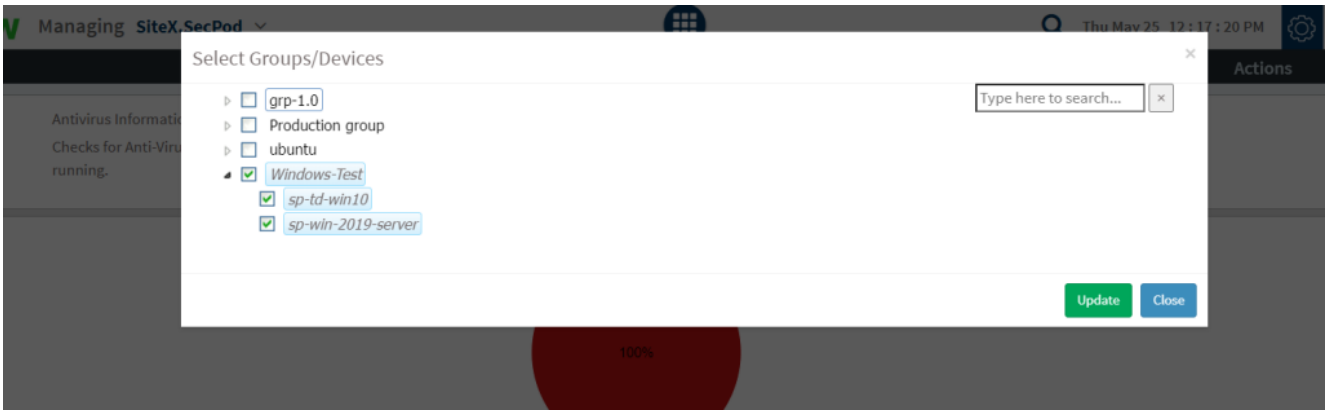


- In Schedule options pane, set the **Query Trigger Time Frame**.



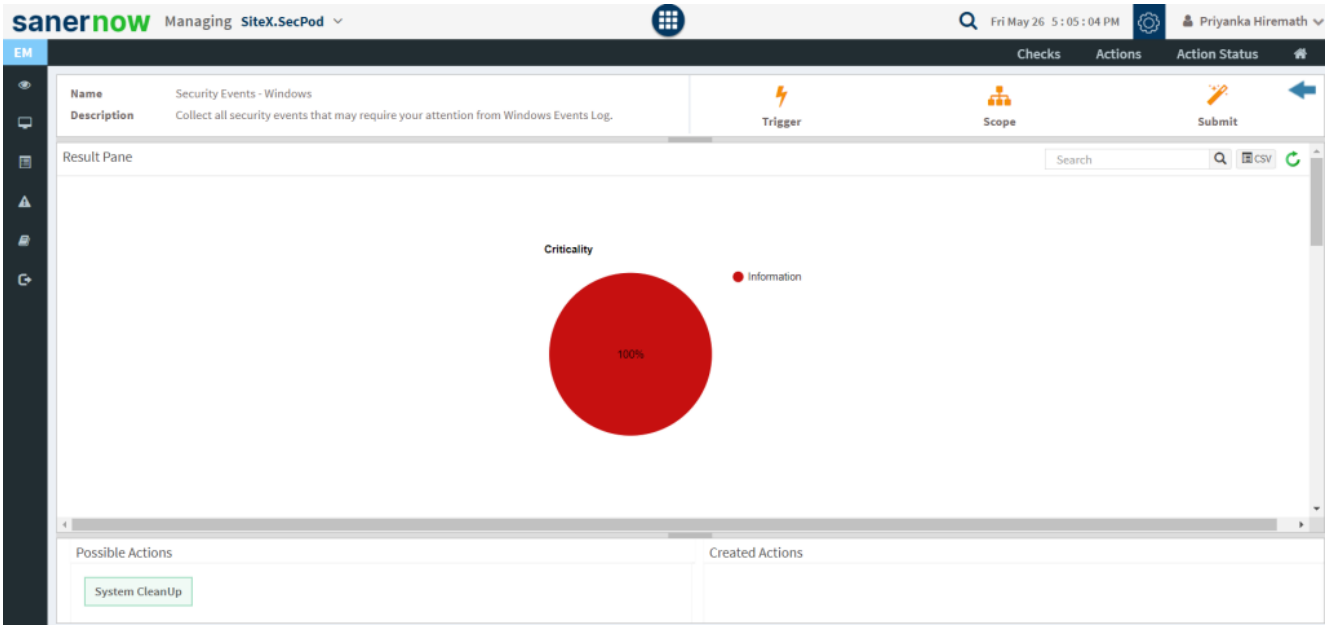
- Click on **Update**.

8. Click on the '**Scope**' to choose the scope of the query.

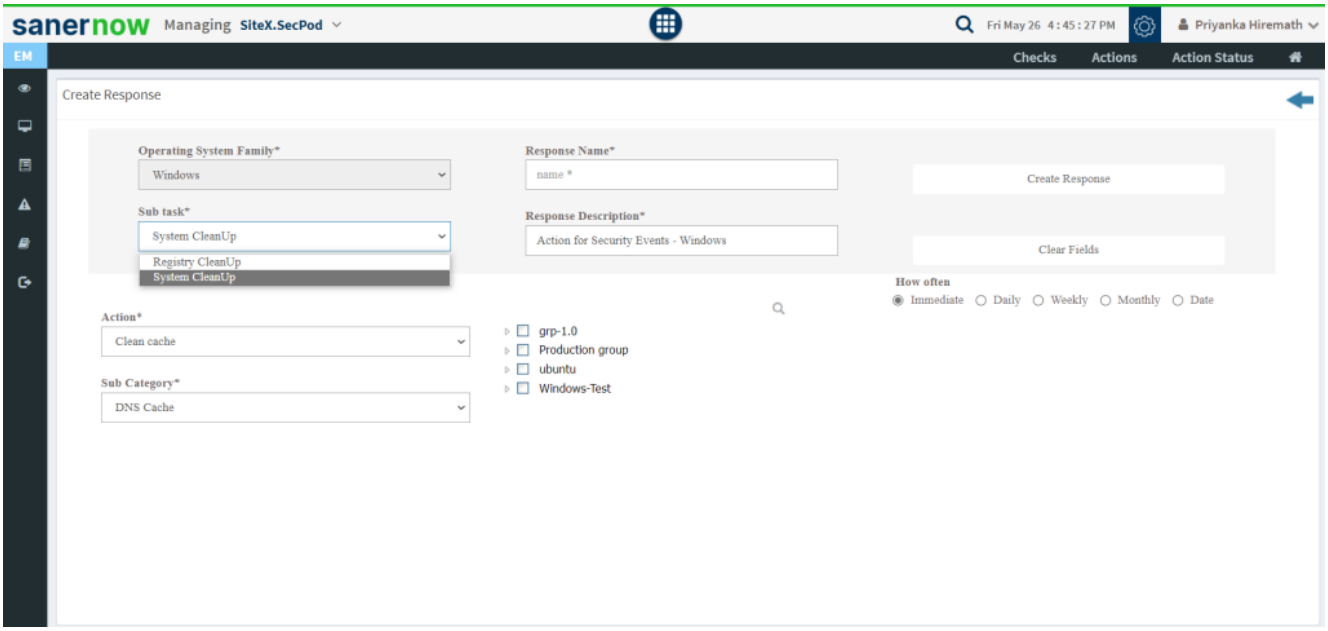


9. To send the query to agent, click on '**Submit**'.

10. In the **Result Pane**, you can collect all security events that may require your attention from Windows Events Log. You can fetch the results and download the CSV format of the result pane.



11. You can clean up your system. Click on the System CleanUp action, you will be redirected to **Create Response page**. In **Created Actions**, you will find all the responses created for the following check.



Now you know how to collect all security events from Windows Events Log.