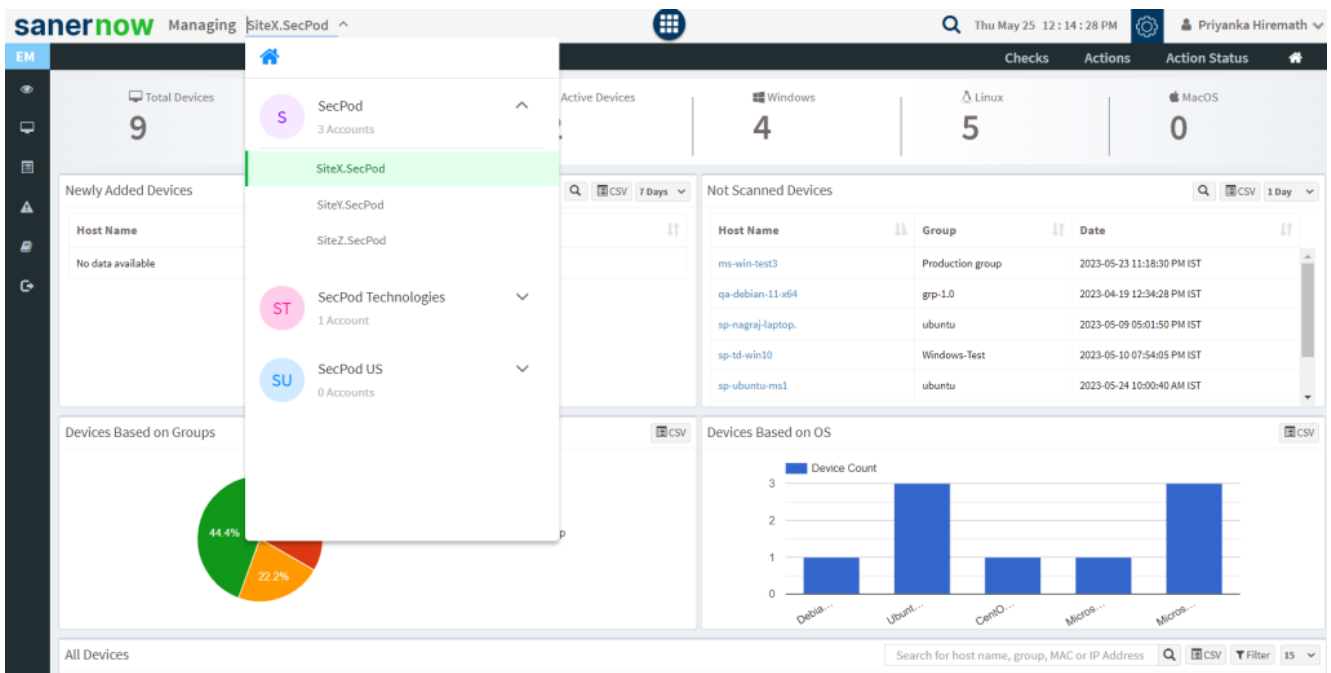
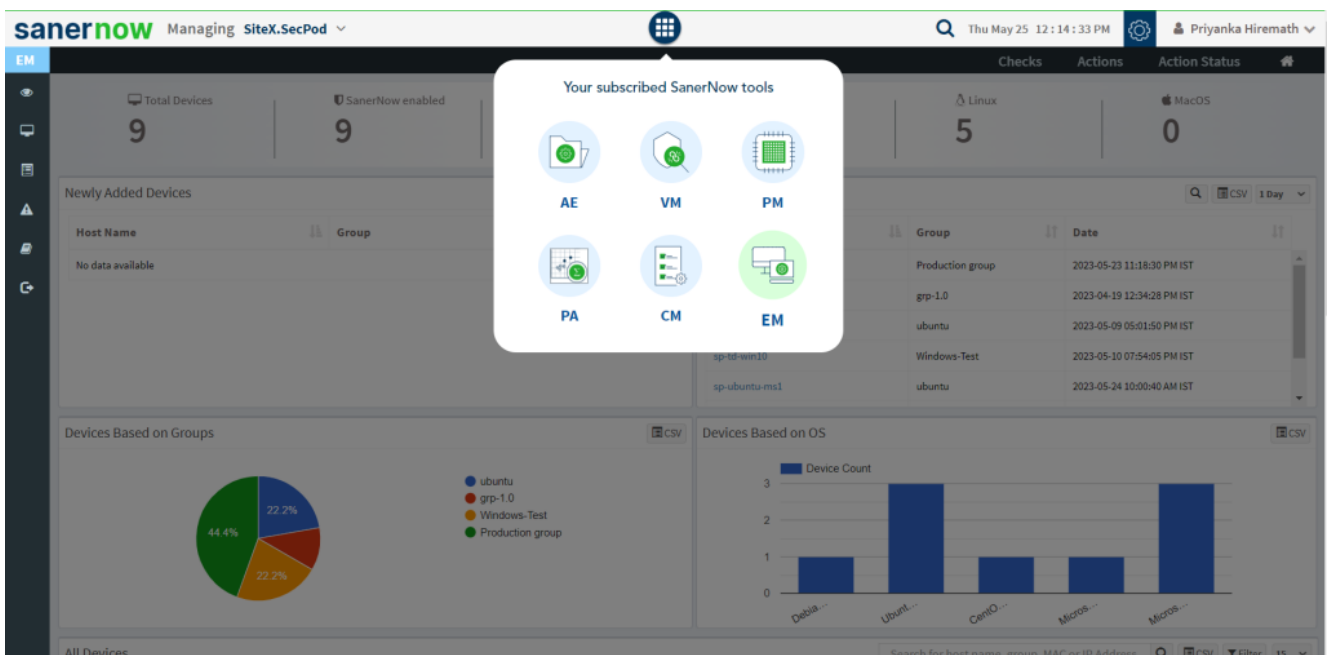


How to collect all security events from Windows Events Log?

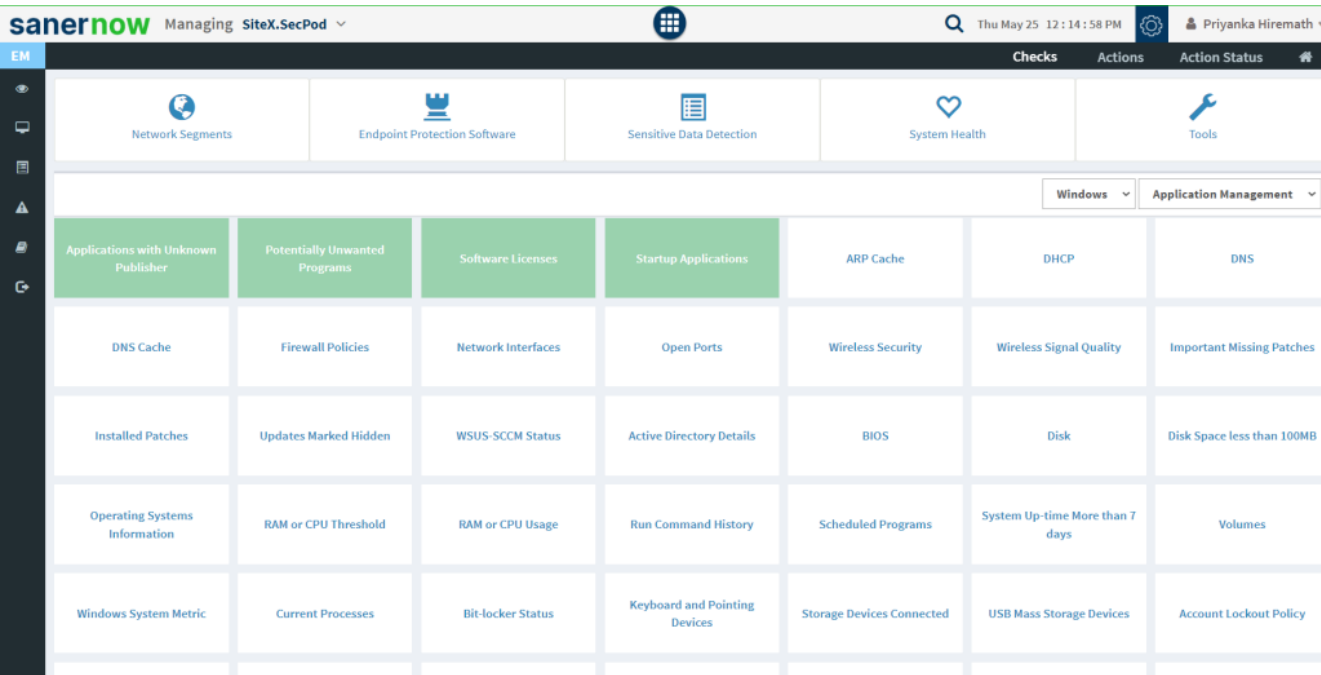
1. Login to SanerNow and choose the **Organization** and corresponding **Account** to collect all security events from Windows Events Log.



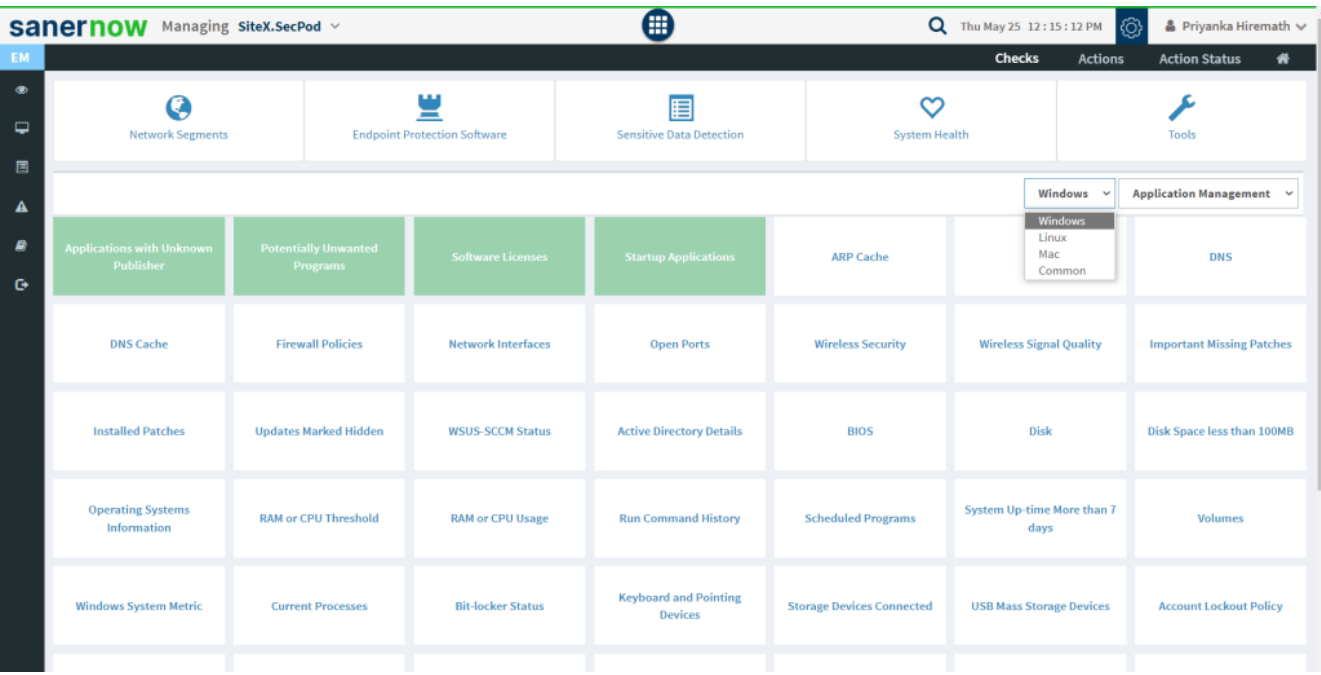
2. Select the **Endpoint Management** module

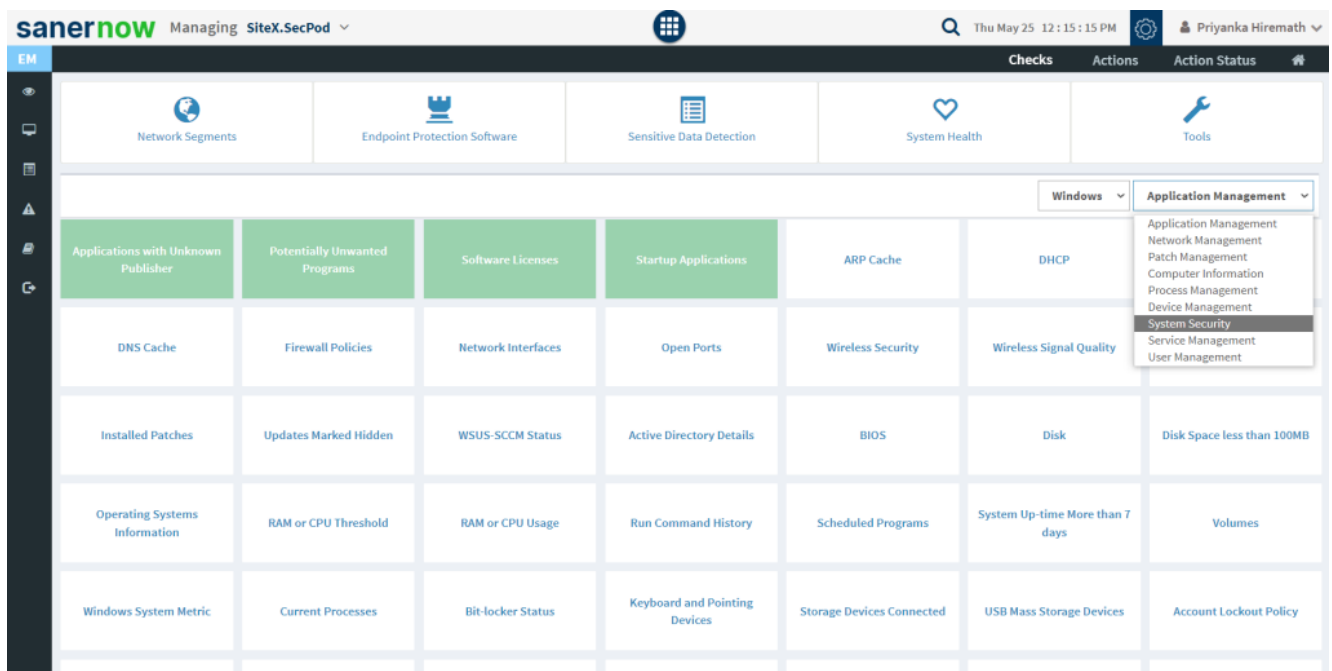


3. Click on **Checks** on the right top corner

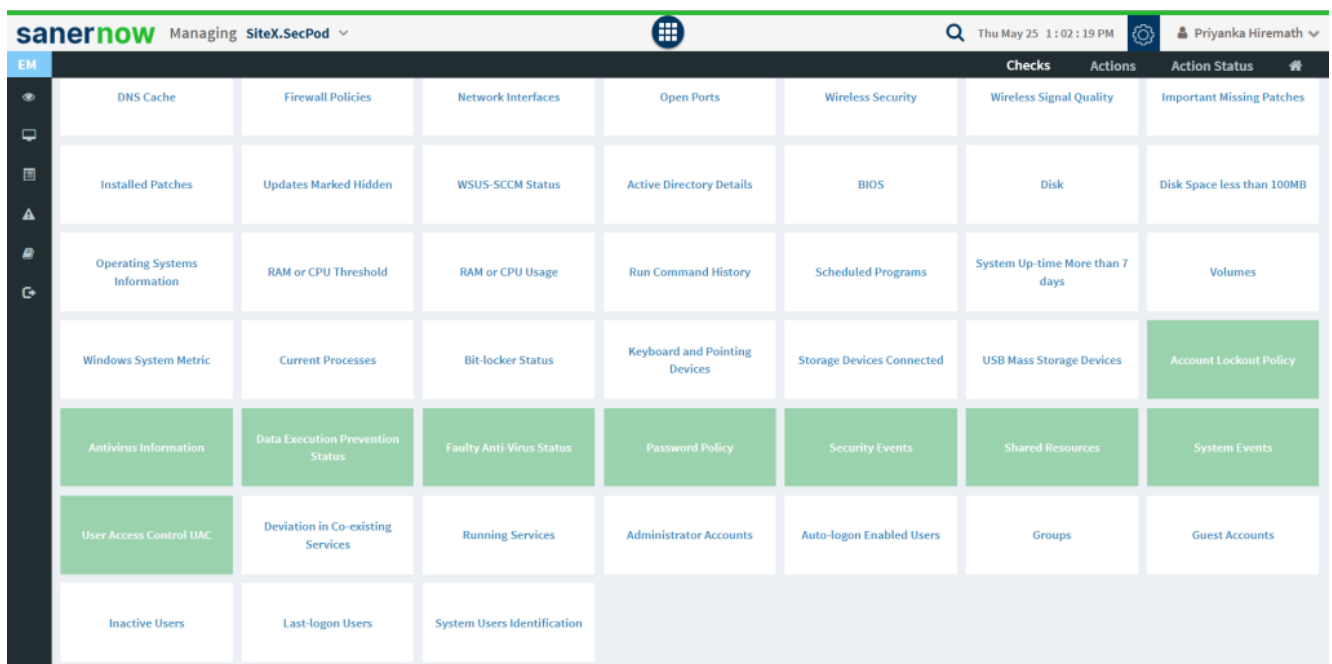


4. From the drop-down menu, select **Windows** and **System Security**





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.

Query Trigger Settings

Query run count: 5 time(s)

Run query every: minute(s)

Schedule options

How often: ☒ Immediate ☐ Daily ☐ Weekly ☐ Monthly ☐ Date

Query Trigger Time Frame: HH MM AM - HH MM AM

Update Close

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

Query Trigger Settings

Query run count: 5 time(s)

Run query every: 7 minute(s)

Schedule options

How often: ☒ Immediate ☐ Daily ☐ Weekly ☐ Monthly ☐ Date

Query Trigger Time Frame: HH MM AM - HH MM AM

Update Close

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

Query Trigger Settings

Query run count: 5 time(s)

Run query every: 7 minute(s)

Schedule options

How often: ☐ Immediate ☐ Daily ☒ Weekly ☐ Monthly ☐ Date

☒ Run Every: Selected Weeks weeks on Selected Days days

Query Trigger Time Frame: HH MM AM - HH MM AM

Update Close

- Click on **Update**.

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

Select Groups/Devices

Type here to search...

☐ grp-1.0

☐ Production group

☐ ubuntu

☒ Windows-Test

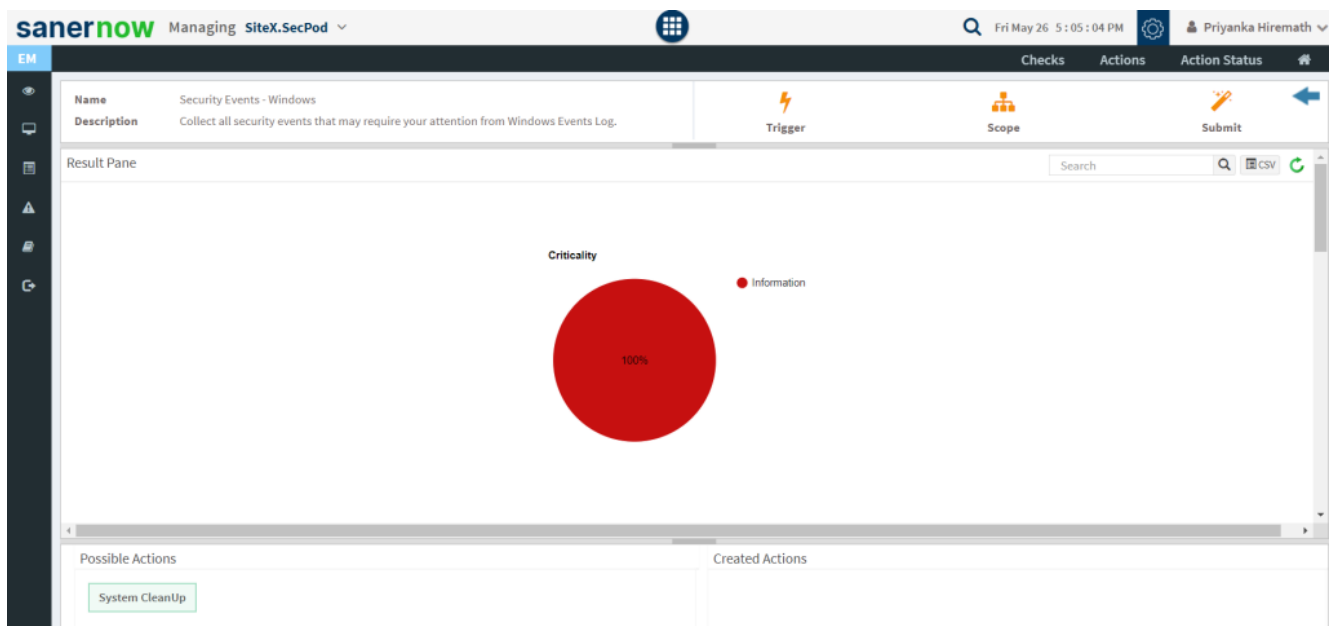
☒ sp-td-win10

☒ sp-win-2019-server

Update Close

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.





The screenshot shows the SanerNow web interface displaying a list of system cleanup actions. The table has columns for 'EventID', 'Level', 'Category', 'MessageID', 'SourceID', 'TaskID', 'SeverityID', 'SourceID', 'TaskID', and 'SeverityID'. The table contains 10 rows of data, all with a 'Level' of 'Information' and a 'Category' of 'System Cleanup'. The 'MessageID' column contains the text 'System Cleanup'. The 'SourceID' column contains the text 'System Cleanup'. The 'TaskID' column contains the text 'System Cleanup'. The 'SeverityID' column contains the text 'System Cleanup'. Below the table, there are two sections: 'Possible Actions' with a 'System CleanUp' button, and 'Created Actions' which is currently empty.

EventID	Level	Category	MessageID	SourceID	TaskID	SeverityID	SourceID	TaskID	SeverityID
1001	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup
1002	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup
1003	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup
1004	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup
1005	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup
1006	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup
1007	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup
1008	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup
1009	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup
1010	Information	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup	System Cleanup

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.

saner**now** Managing SiteX.SecPod   Fri May 26 4:45:27 PM  Priyanka Hiremath 

EM Checks Actions Action Status 

Create Response 

Operating System Family*

Windows

Sub task*

System CleanUp

Registry CleanUp

System CleanUp

Action*

Clean cache

Sub Category*

DNS Cache

Response Name*

name *

Response Description*

Action for Security Events - Windows

How often

☒ Immediate ☐ Daily ☐ Weekly ☐ Monthly ☐ Date

☐ grp-1.0

☐ Production group

☐ ubuntu

☐ Windows-Test

Create Response

Clear Fields

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