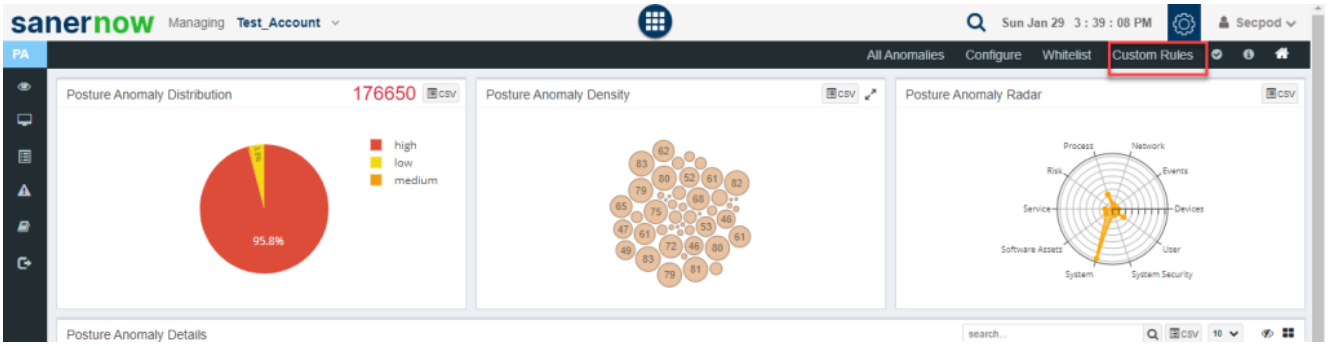
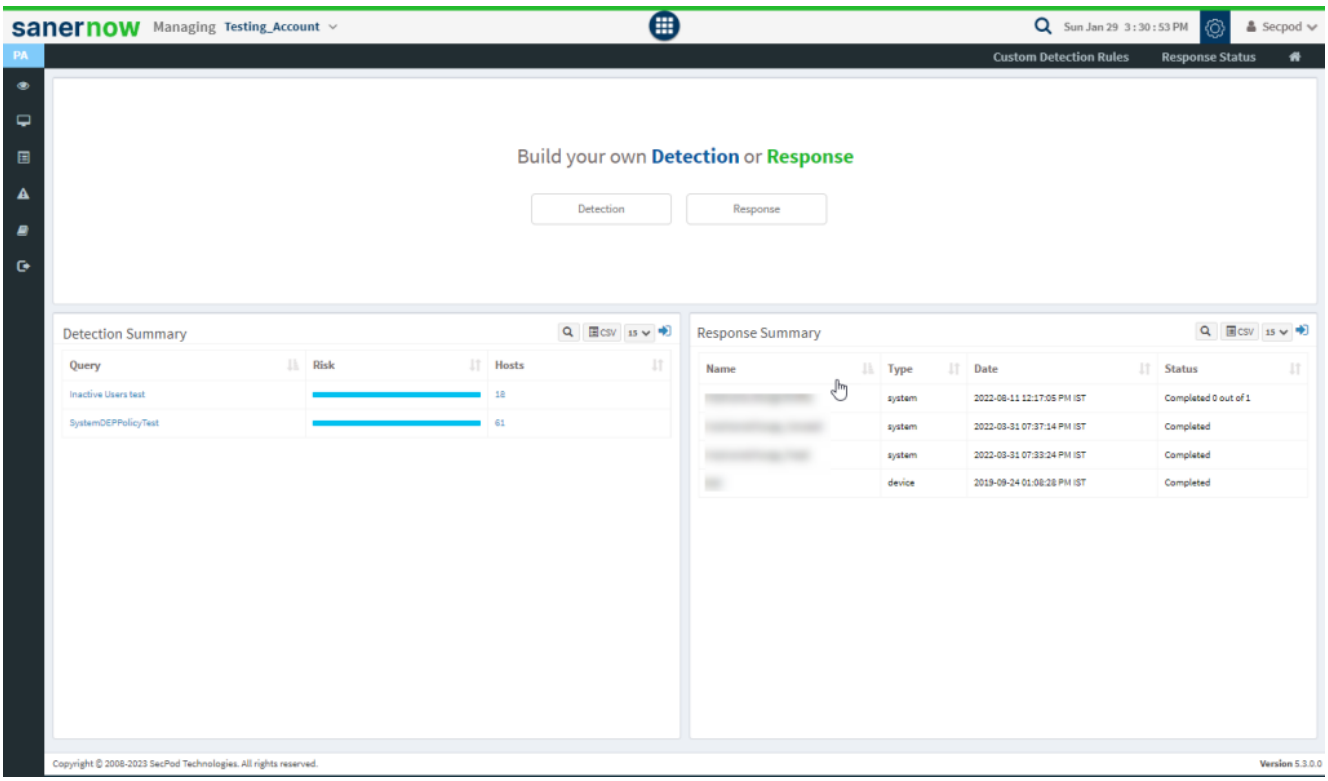
How to build your own detection and response in PA tool?

1. Click on **Custom Rules** on the PA Dashboard to build your custom detection and response.



2. This will take you to the page where you can build your own Detection and Response.



3. You can use default queries provided by SanerNow or create your own queries.

- **Default Queries** – The SanerNow solution provides default queries that can fetch information such as anti-virus information, hosts that have disabled the firewall, hosts that

have disabled Bit locker protection, and more.
- **Custom Queries** – Users can create custom queries.

4. To create a custom query, click the **Detection or Response** button. A query contains two options:

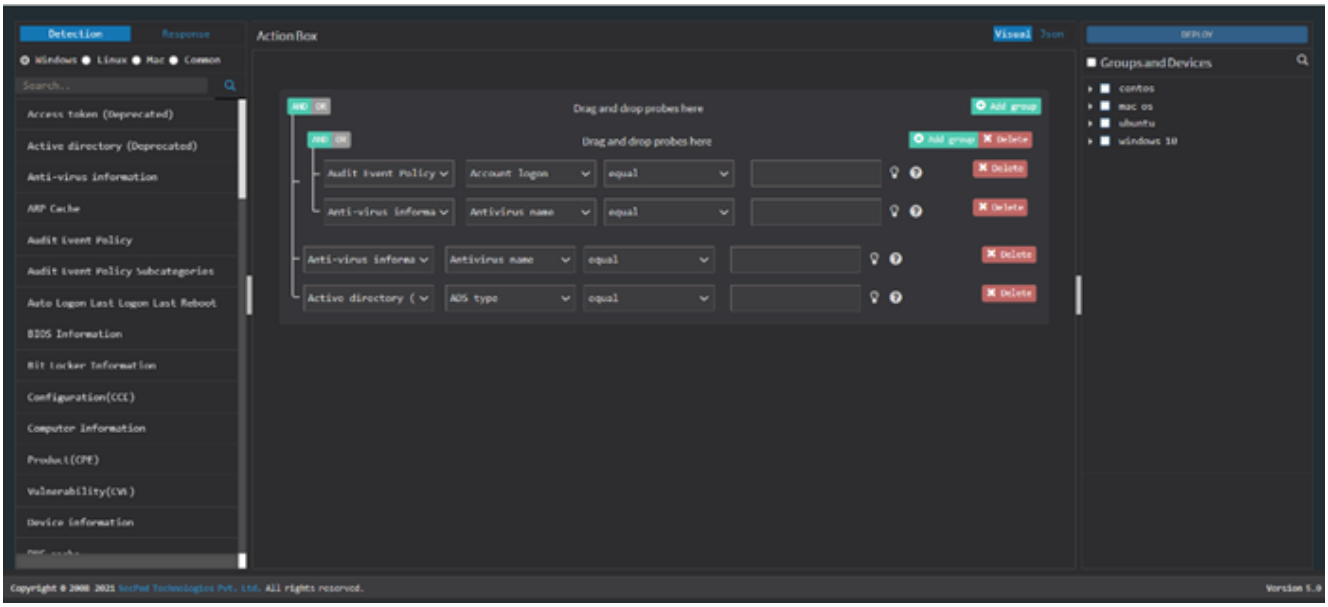
- **Add Rule** – to select supported probes. Multiple rules can be selected with AND or OR operations.
- **Add Group** – to join rules based on conditions. Multiple rules can be joined into one group.

5. The **Run** option displays the query results fetched from the database. The **Edit and Delete** buttons allow you to edit or delete the queries.

6. To create a custom query for threat detection:

- Click Detection in the Build your own Detection and Response pane. The query building page is displayed with a drag and drop library of probes.
- Filter the probes according to the operating system for which you want to write a query.

7. For example, to check for Locky using multiple rules, drag and drop Registry Key Effective Rights probes into the Action Box pane, as shown below. Drag and drop Hive and Key as the parameters. Add a file and the file path.

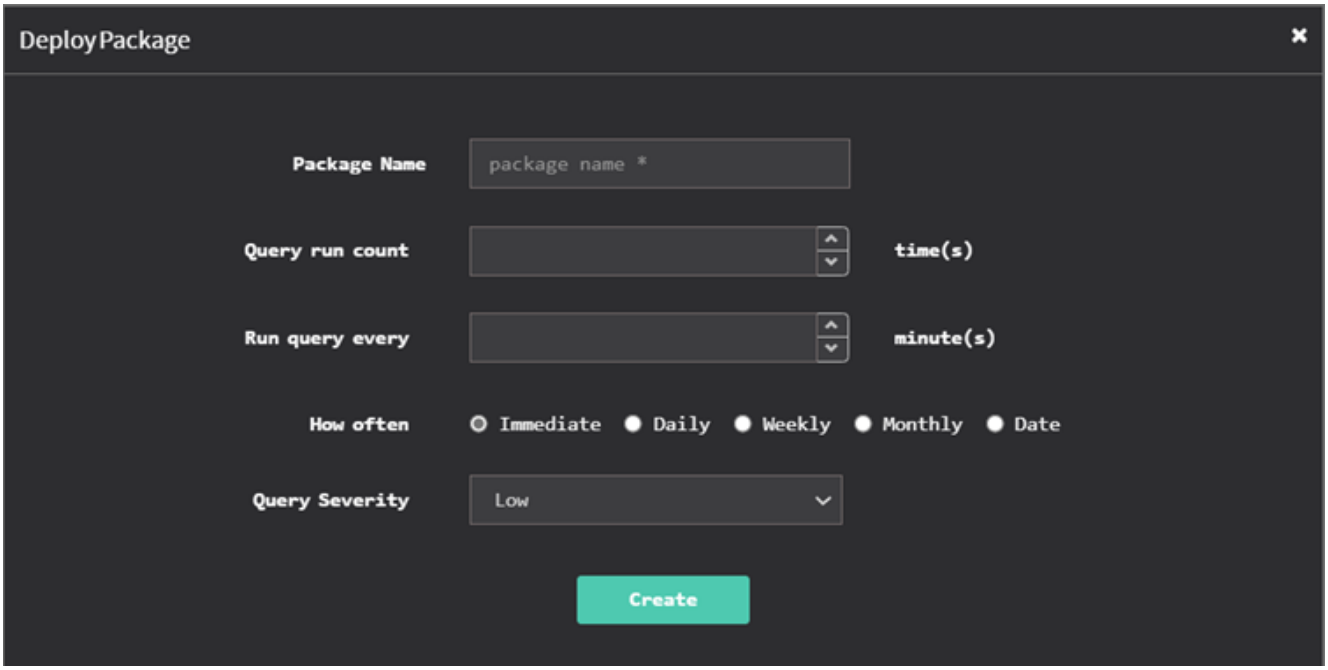


8. Select the devices and groups you want to query. Click the Deploy option at the top right corner. Select the devices and groups you want to query. Click the Deploy button at the top right corner.

9. Now, '**DeployPackage**' window appears. Here, you can specify the package name, the number of times you want the query to run, and the intervals at which the query should be executed.

10. Specify when the query should be run – immediately, daily, weekly, monthly, or on a specific date. Specify the time and the corresponding days of the week, month, or date. And then assign the query a severity – low, medium, high, or critical.

11. And then click on the **Create** button.



12. Once the query is created or updated, the results are displayed in real-time. After the task is created, SanerNow searches the system reports' local database. Click on Submit to retrieve the report. Clicking Submit sends the queries to the Saner Agent to fetch the current data.

Now you know how to build custom detection and response in PA tool.