Rapid7 Insightdr

SUBMITTED BY – HARSH SHARMA

Index Page

1. Introduction to Rapid7 InsightDR…………………………………………2
   1. What is a SIEM?
   2. How SIEM collects data?
2. Interacting with Rapid7 InsightDR...…….………………………………2
   1. Home
   2. Log Search
   3. Dashboard and Reports
   4. User and Accounts
   5. Assets and Endpoints
   6. Automation
   7. Investigations
   8. Data Collection
   9. Detection Rules
3. How to scan our own endpoints……………………………………………7
   1. Installing the collector
   2. Connecting with the collector
   3. Installing agent
   4. Executing the agent
   5. Logging

**Introduction to Rapid7 InsightDR**

Rapid7 InsightDR is a Next-gen SIEM which analyses logs and endpoint activities using its user behaviour analytics and log methods.

**What is a SIEM?**

SIEM stands for Security Information and Event Management is a tool which is used to analyse the logs of an endpoint. So that the security professionals can do an audit and watch any unusual activity within the endpoint.

NOTE: We cannot perform the whole analysis cycle only with SIEM it should be integrated with some threat intelligence tools.

**How SIEM collects data?**

An agent and a collector are installed in the endpoint. Collector collects the real-time data about the CPU and memory of the endpoint whereas the agent records the activities while I am making this report the agent recorded its process details.

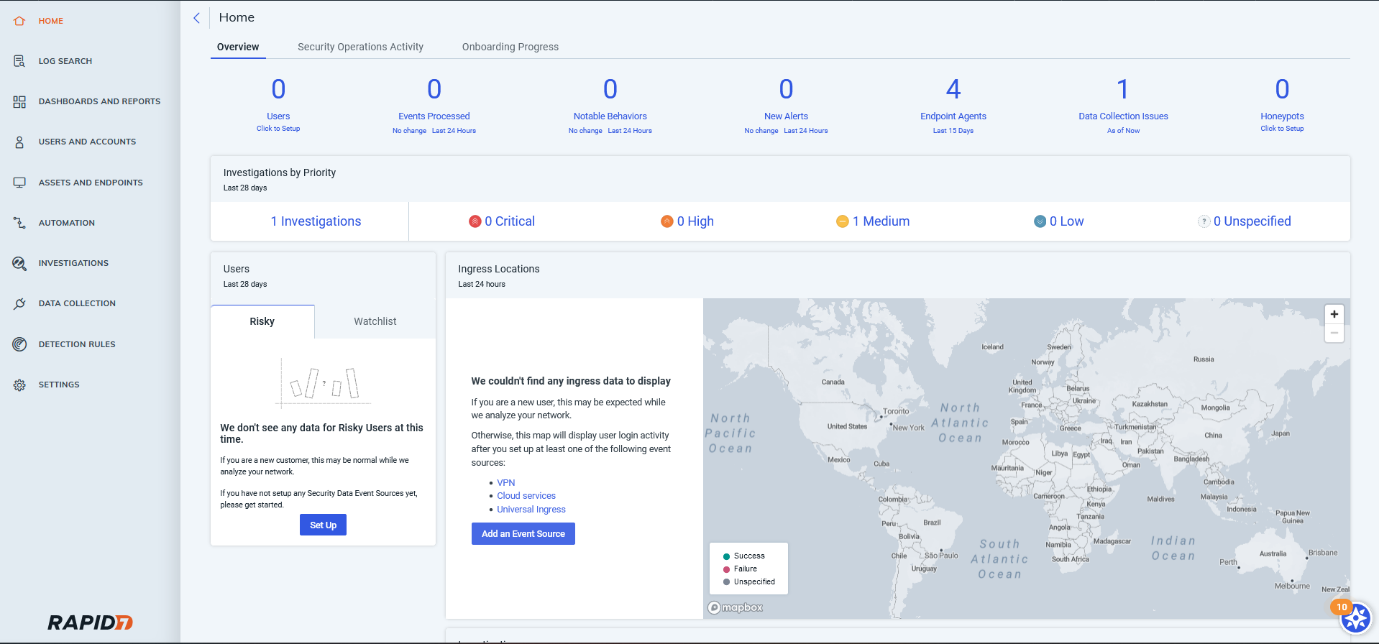
**Interacting with Rapid7 InsightDR**

At left side of the InsightDR there are 9 icons:

1. Home
2. Log Search
3. Dashboards and Reports
4. Users and Accounts
5. Assets and Endpoints
6. Automation
7. Investigations
8. Data Collection
9. Detection Rules

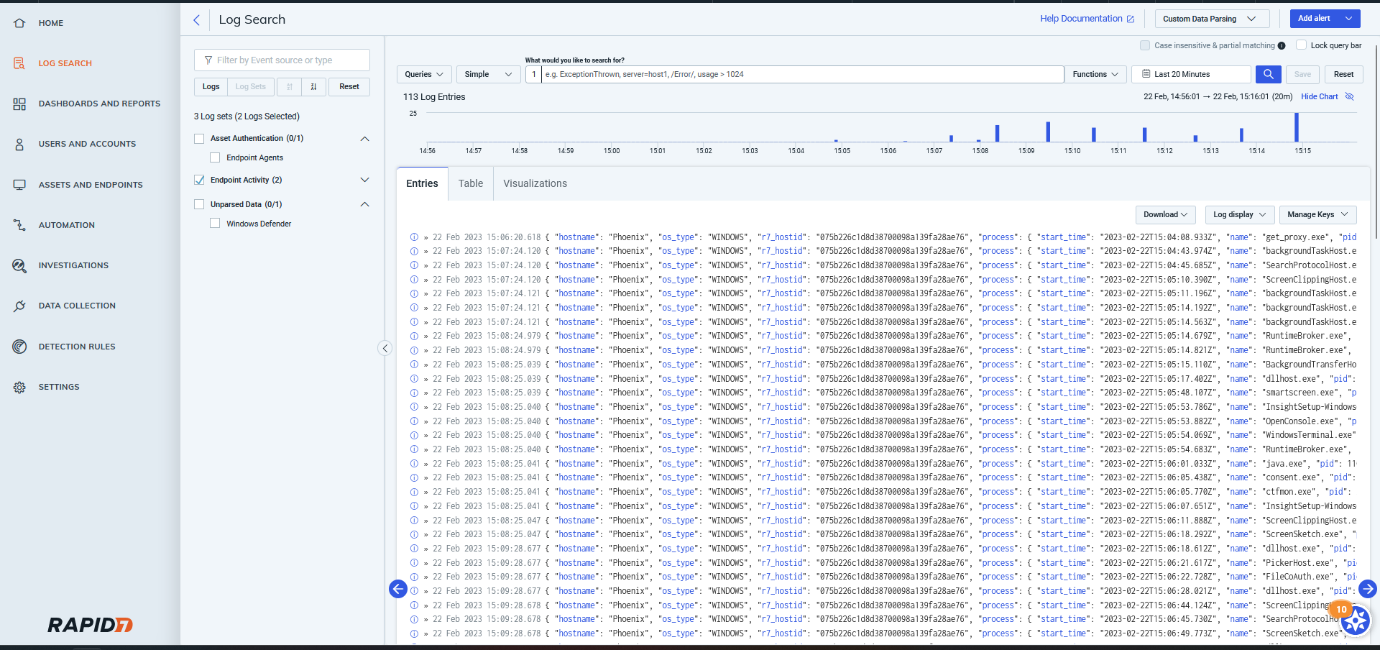
We will see the above in detail in this report.

**Home**

****

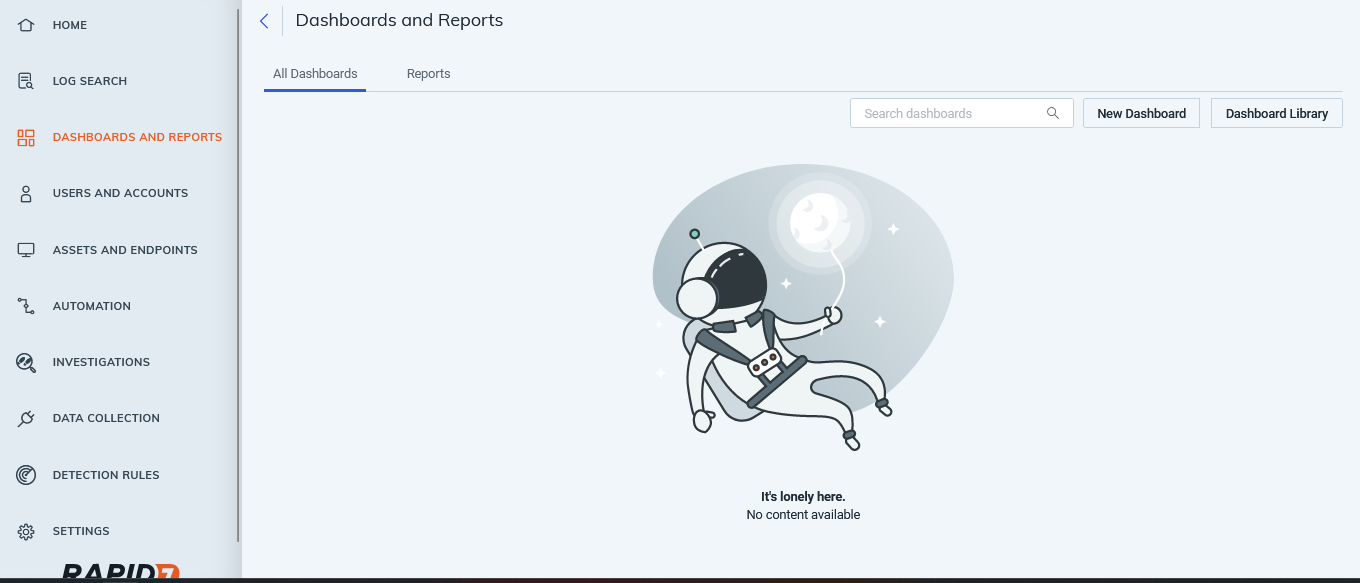
Home tab gives the brief of all the events, users, behaviours, alerts, endpoint agents, data collection issues and honeypots.

**Log Search**

****

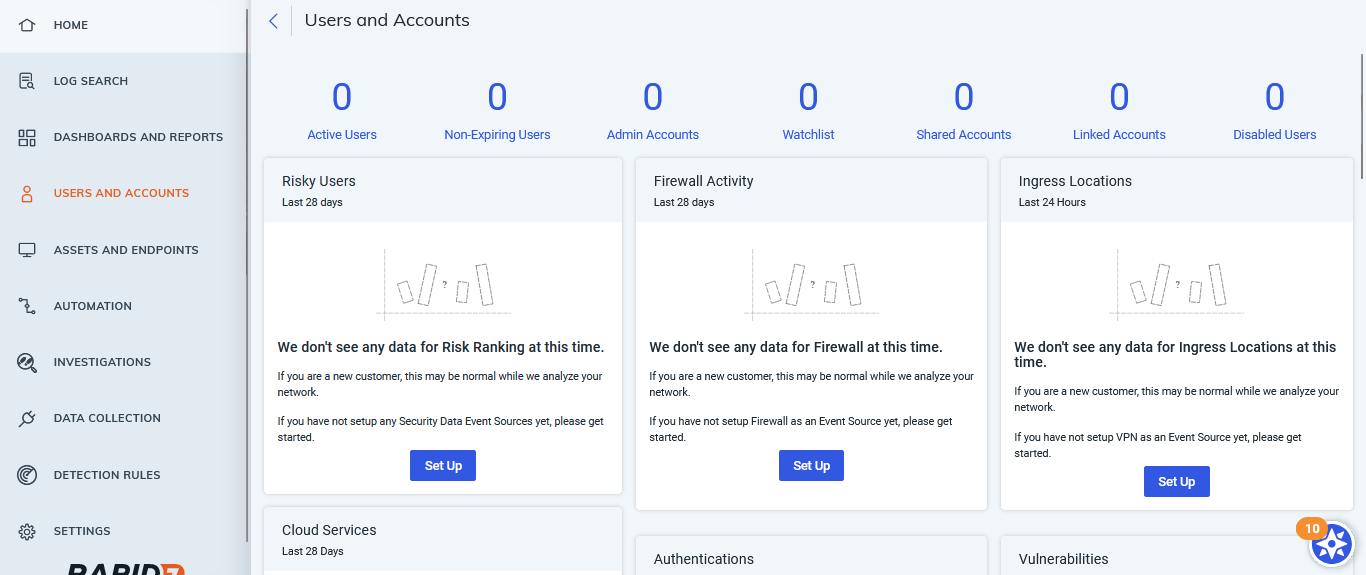
All the logs processed will display here when the agent starts recording the activity of the endpoint.

**Dashboard and Reports**



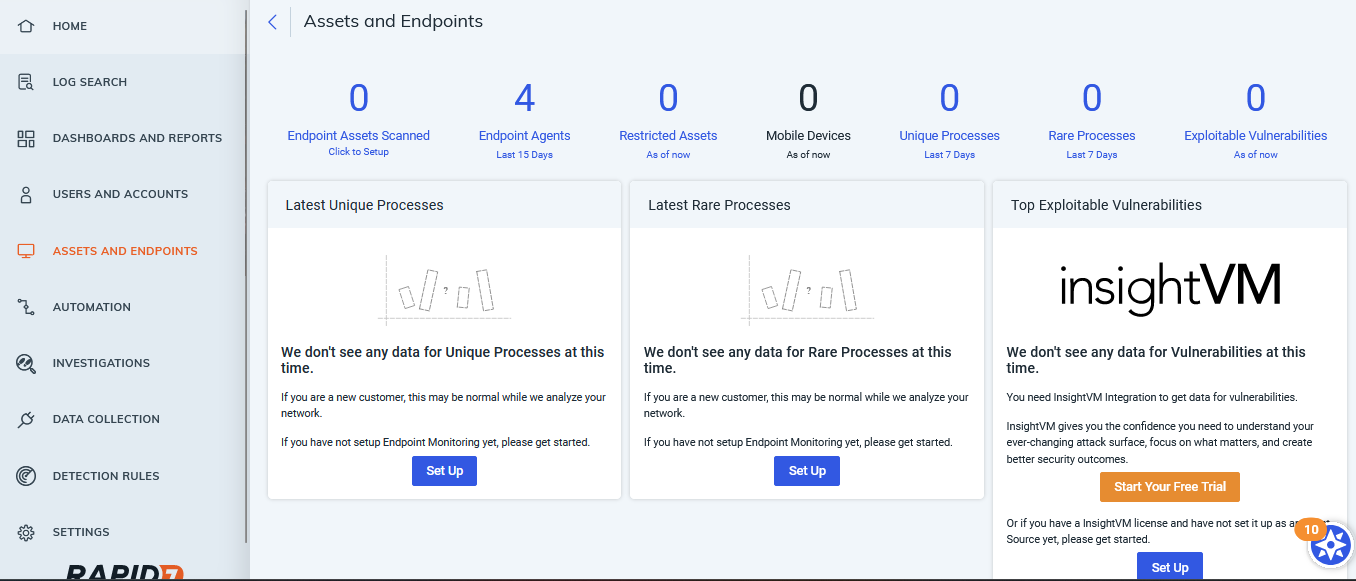
Here all the reports of the logs generated here.

**Users and Accounts**



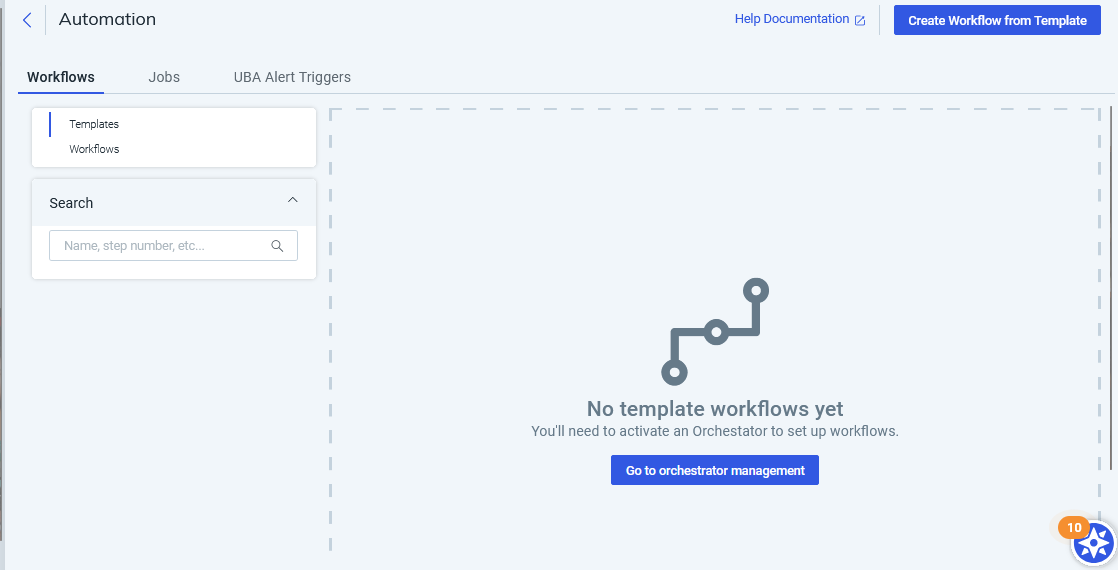
All the users can be created here, and the description shown here.

**Assets and Endpoints**



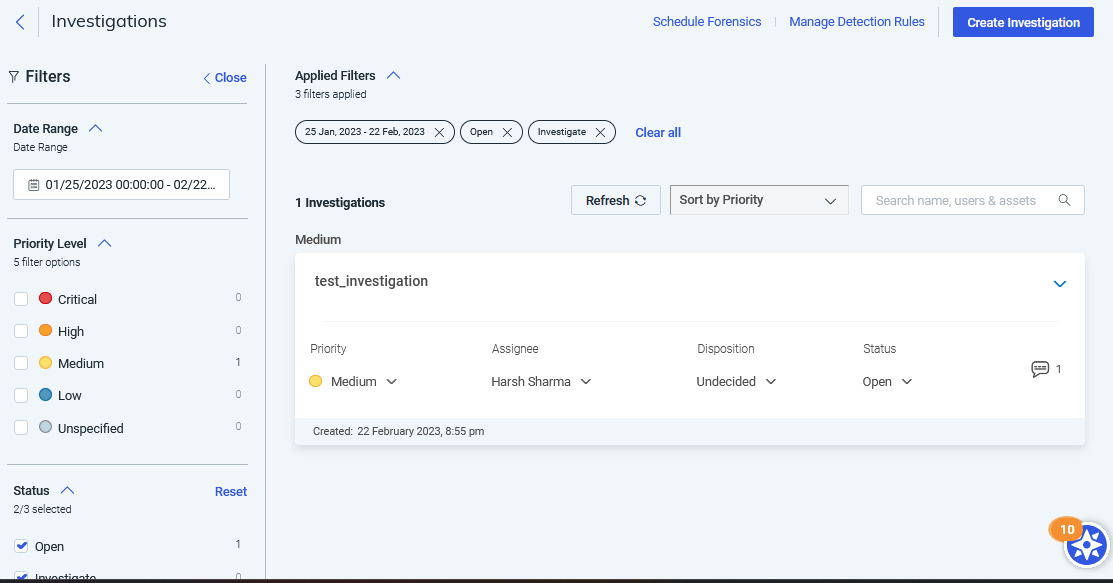
Information about the endpoints connected and different assets is shown here.

**Automation**



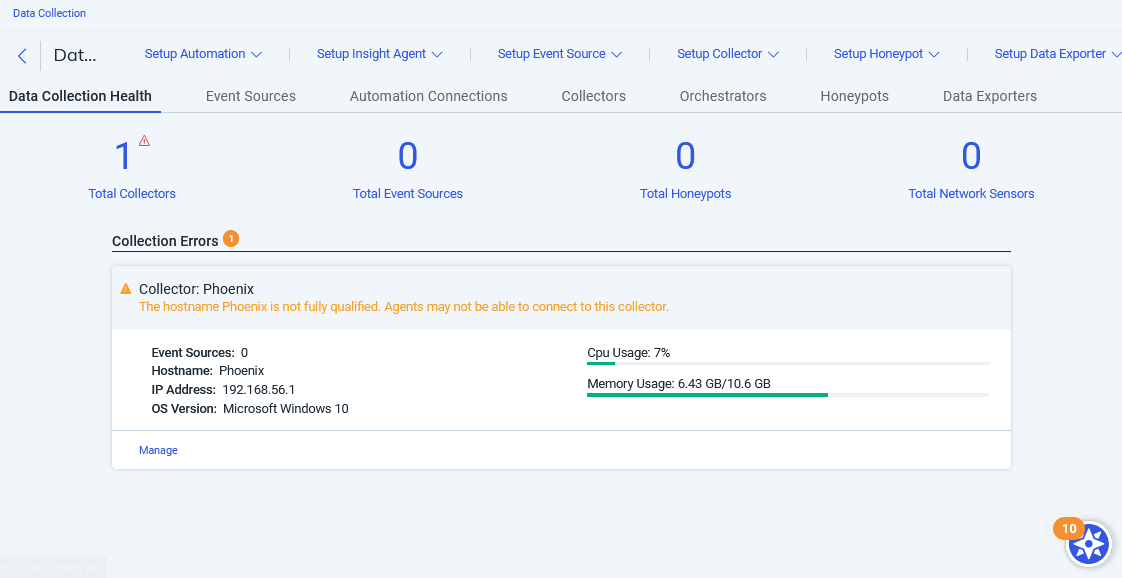
Making workflows and jobs to automate the task is done here.

**Investigations**



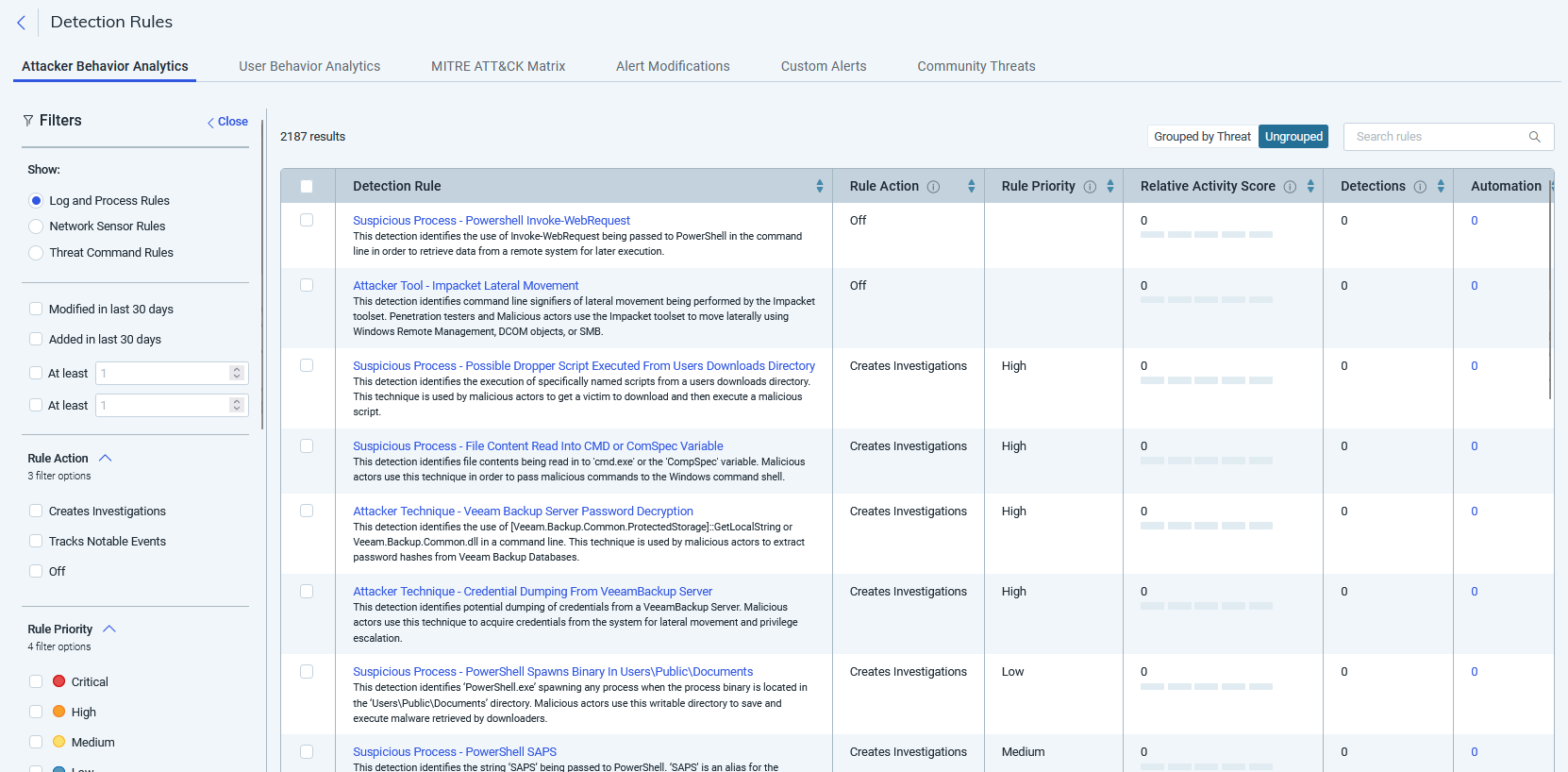
When an activity is marked suspicious, we can investigate them at this area. By marking them which kind of activity and severity it is.

**Data Collections**

****

Information about the collectors, event sources, honeypots and network sensors are shown here.

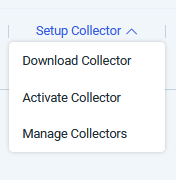
**Detection Rules**

****

Detection rules are set to detect an activity which is suspicious according to different patterns or frameworks here patterns can be made through User Behaviour Analytics and Mitre Attack Matrix which checks the patterns of an incident.

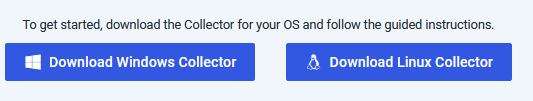
**Scanning our own Endpoints**

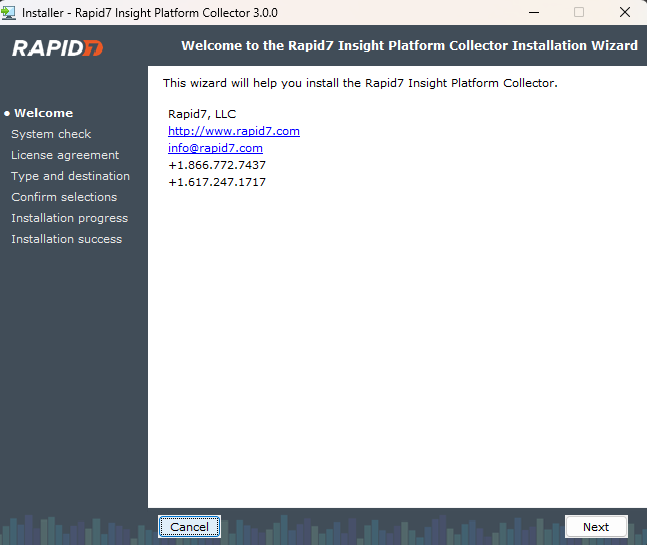
**Installing the Dependencies**

1. **Installing the collector**

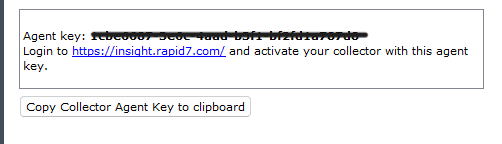
To install the collector, go to data collection tab and click on the setup collector option.

Select the download collector option.

Download the collector depending upon your operating system you want to perform the analysis.

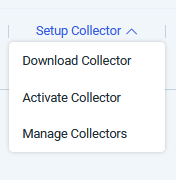
Launch the setup and follow through instructions.

Click on next.

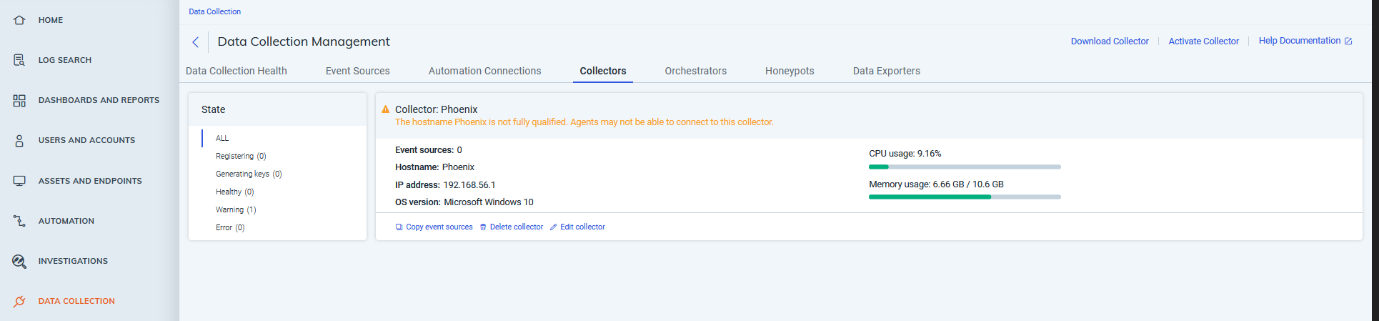


Make sure to copy the agent key. The key is needed for collector to connect itself with the system.

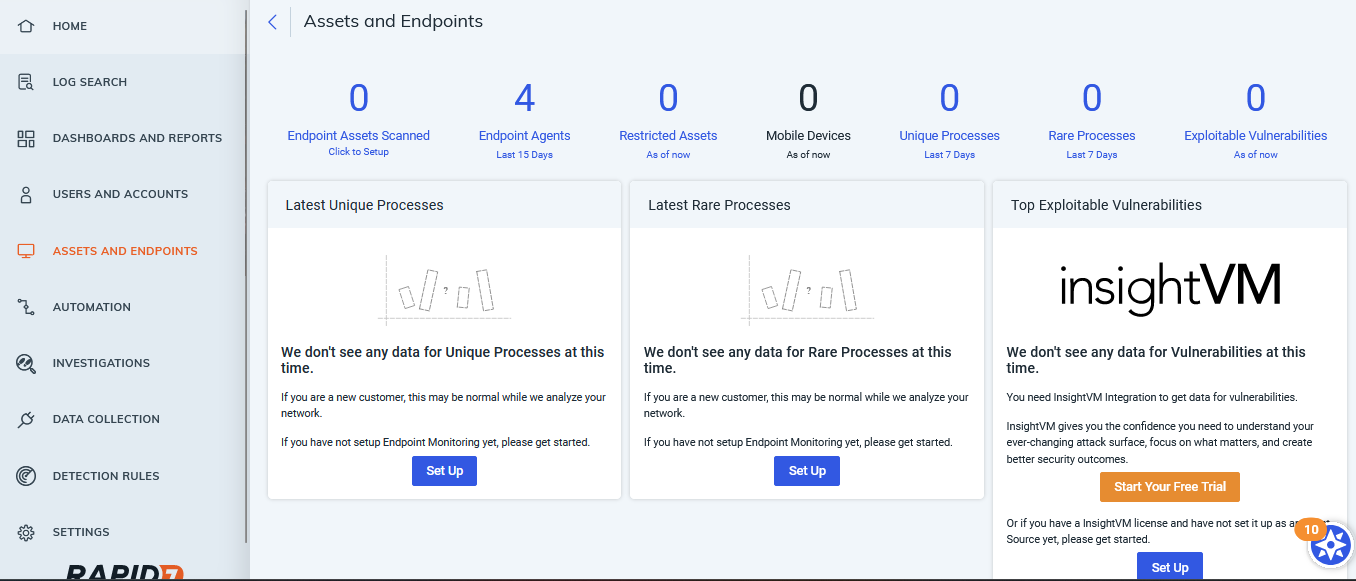
After installing the collector , go to Insight platform to connect the collector with the system.

 Select Activate Collector from the data collections tab in the platform.

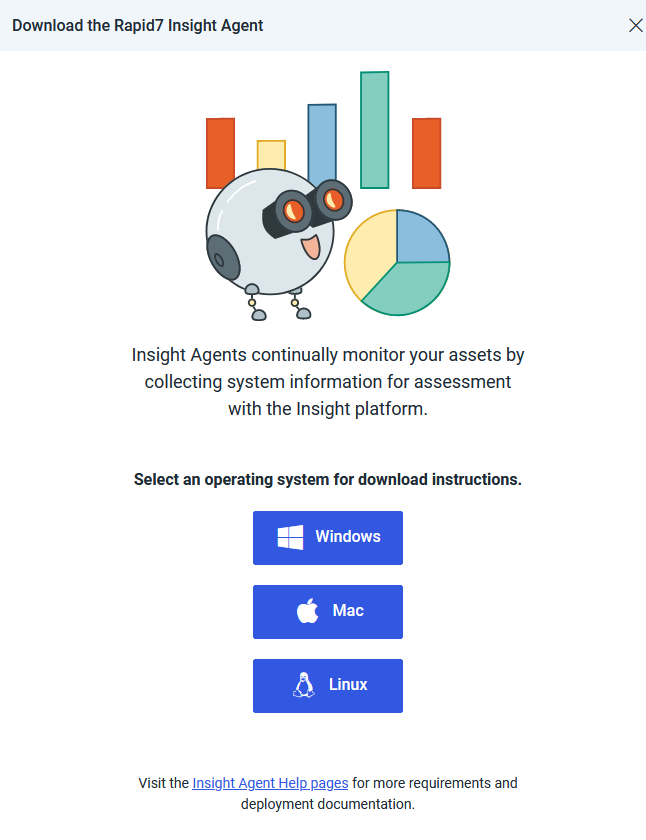
After giving the information and agent key copied, we can see the collector is providing the Realtime information of the system.



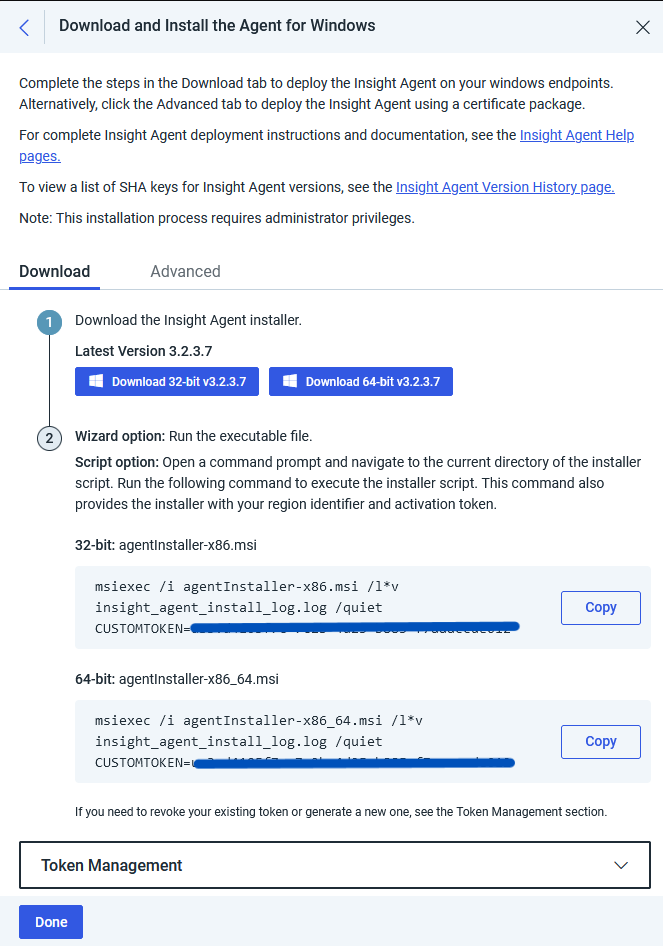
**Downloading the Insight agent**

****

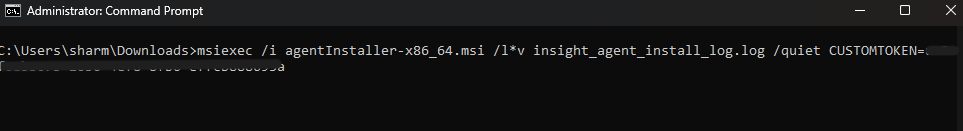
Navigate to Assets and endpoints then click on “set up” to download the agent.

Select your preferred operating system.

NOTE: The operating system must be same as before.

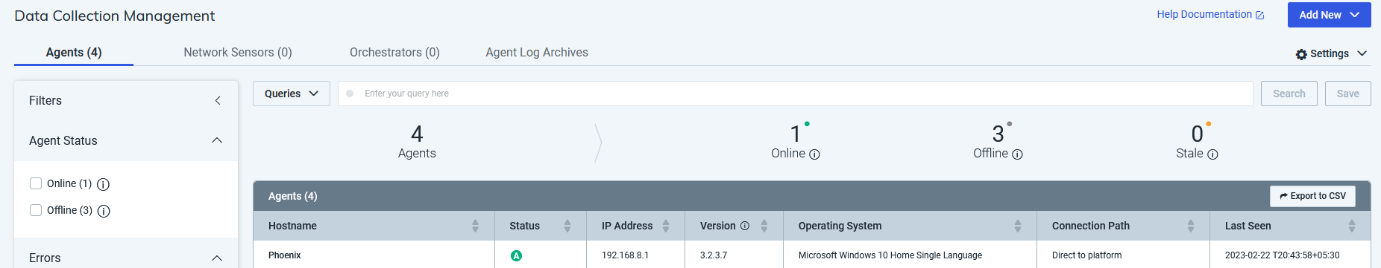


Download the setup and make sure to copy the command to install the agent with your token id.



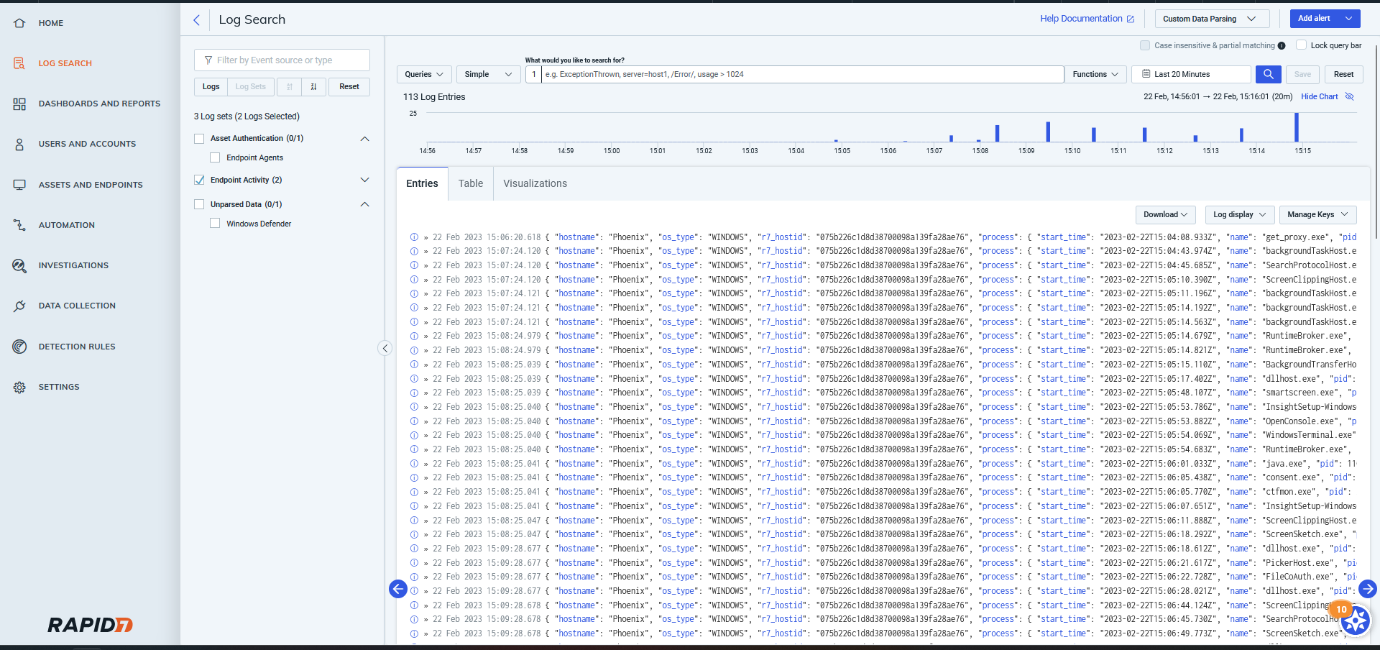
Run the command in command prompt (Run as administrator).

This will take some time to reflect to changes in the platform.



We can see our operating system in the list of endpoint and is marked online.

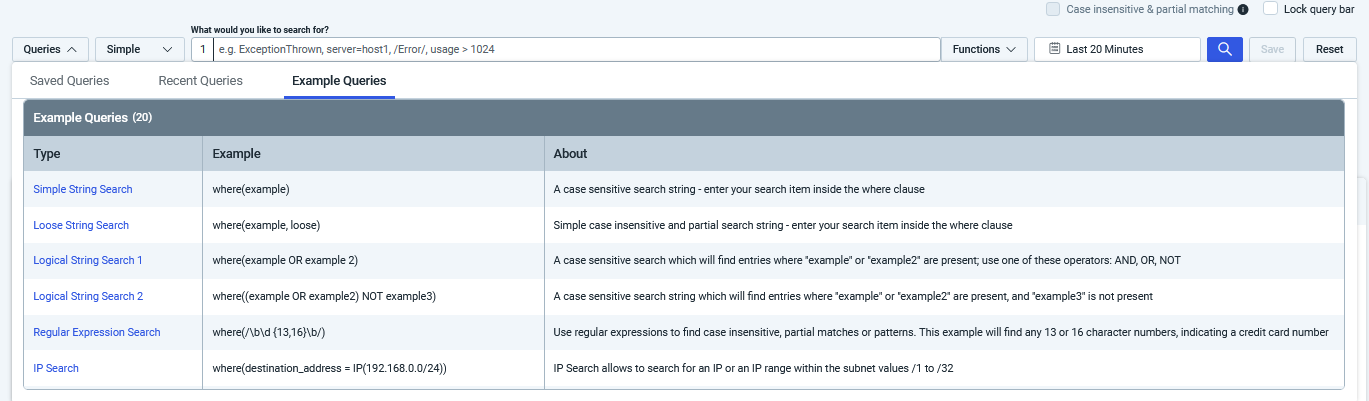
Deployment is completed now its time to analyse the logs.

**Analysing the logs**

By clicking on the “Log Search” tab we can see our logs.

Reading logs is one of the most hectic tasks , to make it more efficient use some filter within the logs.

By giving your queries about a specific process, it will be easy for us to analyse the log.



Example of queries is provided for reference.