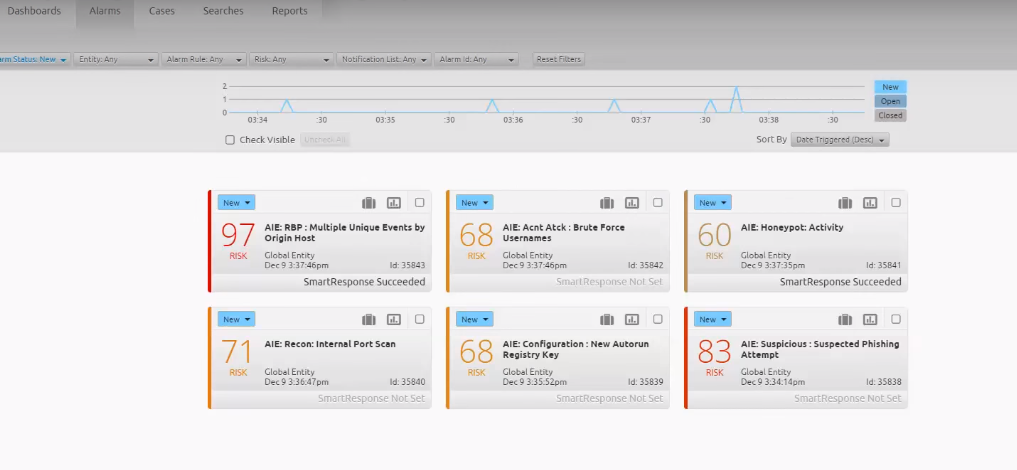
**LogRhythm Use Cases**

|  |  |
| --- | --- |
| **Use Case** | **Name** |
| 1 | Mitigating Threats |
| 2 | Detecting Ransomware |
| 3 | Phishing Emails |
| 4 | Detecting Data Exfiltration |
| 5 | Defending against Insider Threats |

**Use Case #1: Mitigating Threats**

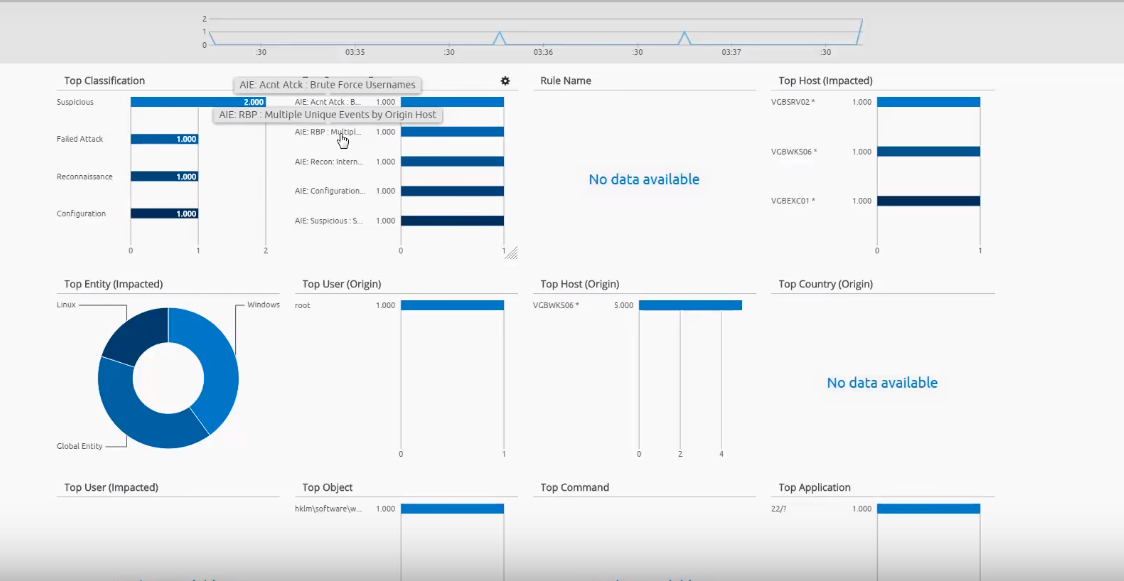
A network of an organization faces different kinds of threats every day. Some of the threats involve reconnaissance attacks, malware attacks, DDoS attacks etc., So monitoring of the activities that are happening on the network is important to protect from these kinds of attacks. To perform this task there are different kinds of tools available. But here we are taking LogRhythm as an example.

**Overview:**

When the LogRhythm application is opened, Dashboard will be seen first. On the dashboard many analyzed details about the network are showed. As there are predefined rules in the application, it performs analysis based on those rules and shows the results of it. We want to monitor the activities of threats. So rules are to be defined as per our requirement. If any activity that happens against the rules, then those kinds of events are noticed in the alarms section. 

**Analysis**:

An alarm rises when an activity against the rules occurs. That alarms come with the risk levels. If the risk level is high, then those kinds of alerts needed to be solves immediately. Other details like type of the attack, classification, name of the rule that made this happen, the host that has been impacted the most, top common event etc., can be known. The Smart Response function of the LogRhythm helps the organization by terminating the connection between the attacker and the network.

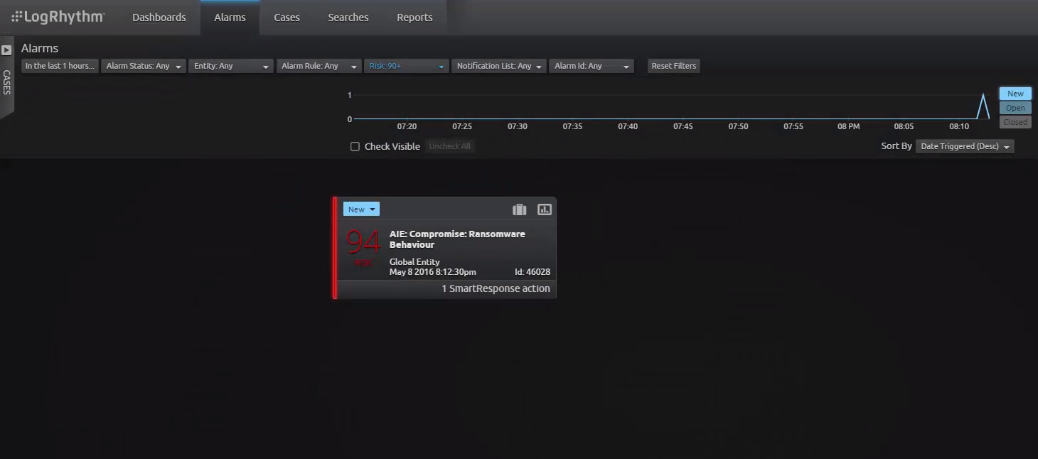


**Use Case #2: Detecting Ransomware**

To gain access to the system which is connected to the internet, there are many ways. One of the way is by doing some background work on an employee of an organization and sending emails based on their interests. Those emails are linked with malicious links which install ransomware once they are clicked. The systems of the network may get effected by the malware that is attached to the emails. So detection of these kinds of activities is important and it is done by LogRhythm here.

**Overview:**

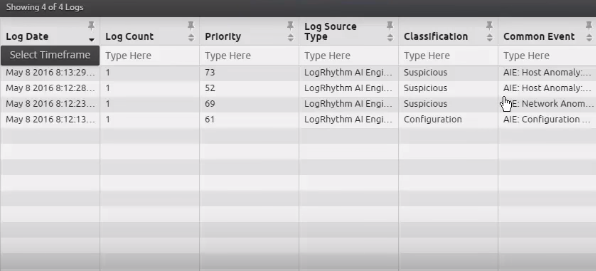
There will be different sections in the home screen of the application. They are the dashboard, alarms, cases, searches and reports. Dashboard is the place where the graphical representation of the activities that are happening on the network is showed. The alarms are the section in which the activities that happen against the defined rules are noted. If any activity seems to be interesting, then they can be added in the cases section. In the searches part, the searches can be done over the network as per the requirement. In the reports section, the activities that happened at the time of an attack is saved and used for further study.



**Analyzation**:

When the events happen against the rules, they fire alarms. In the alarms section, the events which raised the alarms are shown. Those events can be analyzed and priority is based on the risk level of the activity. Other details like classification of events, top common event, rule name, top host, top entity, top user, host and other details are known. There will be a list of events in which the information like log date, count, priority of the event, classification of it and other information of them is available.



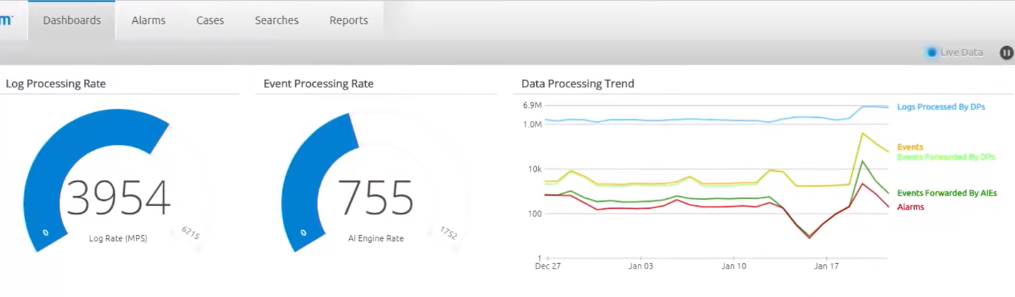


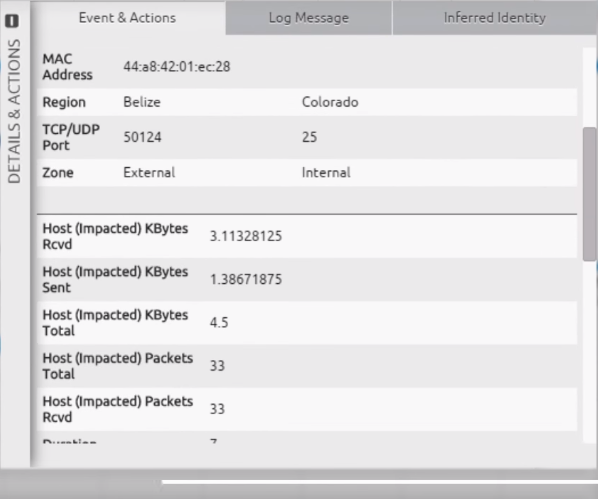
**Use Case #3: Phishing Emails**

There are many ways to gain access to one of the systems of an organization. One of the way is by making the victim click the email which is linked with a malicious file. This can be done by doing some background research on the interests of an employee of that organization and sending emails based on that. The systems of the network may get effected by the malware that is attached to the emails. These kinds of attacks are known as phishing email attacks. To monitor these kinds of attacks, LogRhythm is used here.

**Overview**:

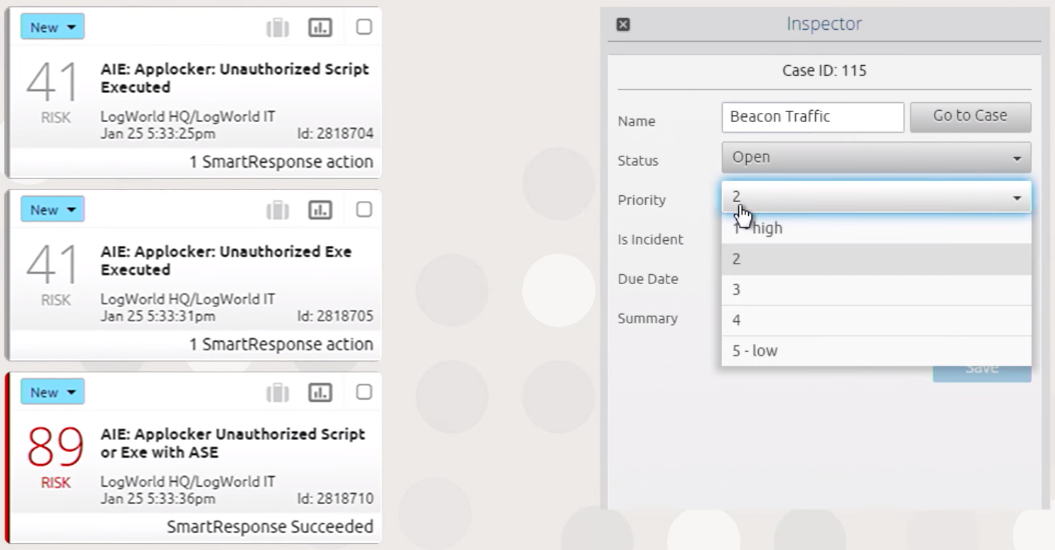
When the LogRhythm application is opened, Dashboard will be first section you will see. On the dashboard many analyzed details about the network are showed. As there are predefined rules in the application, it performs analysis based on those rules and shows the results of it. We want to monitor the activities of threats. So rules are to be defined as per our requirement. The results will be shown in the alarms section. Along with the dashboard and alarms there are other sections like cases, searches and reports.





**Explanation:**

The alarms are raised for the events which don’t follow the rules that are defined. If the risk level of that alert is high, then those kinds of alerts needed to be solved immediately. If the risk level is low, then those kind of alerts can be analyzed a bit later. If an alert seems suspicious then those kinds of alerts can be used as reference and a priority level can be set for them. In future if the same kinds of events occur, then those events will directly set to that priority level by default.

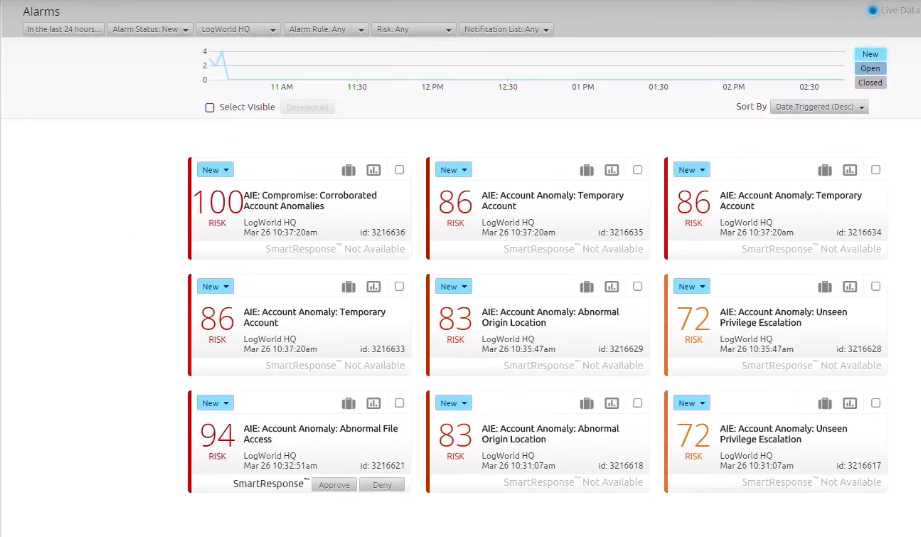


**Use Case #4: Detecting Data Exfiltration**

Data exfiltration is the process in which the attacker gains access to the system and performs the form inside or from outside the network to steal the data. This is generally done by the insiders using storage devices like USB. This can also be done by compromising the security of the network and taking access of the systems in the network and by maintaining the connection, data exfiltration can be done. So in order to prevent these kinds of things from happening monitoring of the activities that are happening in the network is to be done. To do this we are taking LogRhythm as an example here.

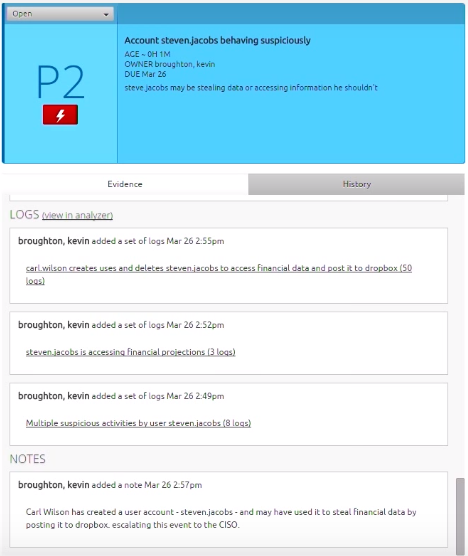
**Overview:**

There will be different sections in the home screen of the application. They are the dashboard, alarms, cases, searches and reports. Dashboard is the place where the graphical representation of the activities that are happening on the network is showed. If any activity seems to be interesting, then they can be added in the cases section. In the searches part, the searches can be done over the network as per the requirement. In the reports section, the activities that happened at the time of an attack is saved and used for further study. Here alarms section is shown where the recent events which fired the alarms are shown.



**Explanation**:

When the events happen against the rules, they fire alarms. The events which fired the alarms will be shown in the alarms section. Those events can be analyzed and priority is based on the risk level of the activity. Each alarm can be analyzed individually and if you find any of them suspicious, they can be used to create cases, which can be used as proofs and evidences in the court of law.

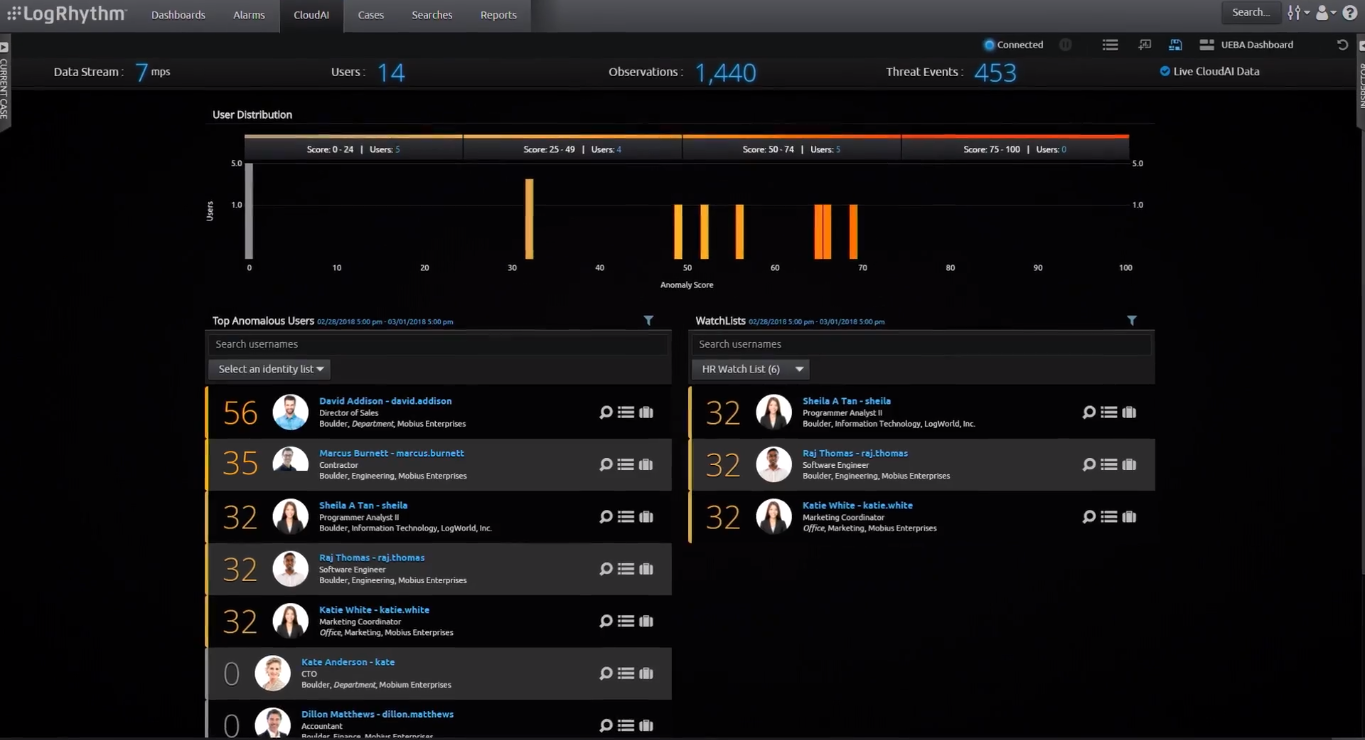


**Use Case #5: Defending against Insider Threats**

Threats for an organization comes from many different ways. Whether from an attacker from outside or from an insider. The threat from outside takes a larger amount of time as the attacker has to find the vulnerabilities and plan to perform the attack. But in the case of insider, he will already have the access to inside systems which makes the work a lot easier. The insider may use storage devices like USB for data exfiltration or he may even send the files using unregistered ports to an outsider. These kinds of activities have to be monitored to protect the data of the organization. There are many tools available to perform this task but here we are taking advantage of User and Entity Behavior Analytics(UEBA) of LogRhythm.

**Overview:**

When the LogRhythm application is opened, Dashboard will be first section you will see. On the dashboard many analyzed details about the network are showed. As there are predefined rules in the application, it performs analysis based on those rules and shows the results of it. The results will be shown in the alarms section. Along with the dashboard and alarms there are other sections like cases, searches and reports. Along with them there is an additional section called Cloud AI where the artificial intelligence is used to analyze the data and automatically characterize it based on the level of threat it may cause.



**Explanation:**

The alarms are raised for the events which don’t follow the rules that are defined. If the risk level is high, then those kinds of alerts needed to be solved immediately. If they can’t be solved by Tier 1 analyst, then they are escalated to Tier 2 analyst. If an alert seems suspicious then those kinds of alerts can be used as reference and a priority level can be set for them. The list can be updated as the level of priority increases. Along with the priority levels, the description for the alert can be added for easy reviewing. The Tier 2 analyst will analyze the escalated issue and if the situation is running out of hands, then he can terminate the connection from the network and can also abort the activities that are going on in the insider’s system.



