Dashboard

The SEM dashboard displays activity summary of the network and device information to the users. This user-friendly dashboard allows users to easily identify any suspicious patterns using several graphs and tables. All events are categorized by the event type so the users can prioritize and easily troubleshoot or investigate problems when occur. This is a customizable dashboard., which allows users to customize log results in different ways according to their preference. Users can view logs as charts, list etc. The Dashboard uses several color codes to make the user experience smoother and make the events more identifiable.

Live Events

The SEM live events show the activity taking place in the network in real time, this is useful feature allows users to identify a malicious activity while it is taking place, for an example an unusual amount of traffic is received for a web server it shows a probability of a DDOS attack, by identifying this the organization have ability to prevent such situation before it happens. The live filtering option allows users to focus on a certain type of traffic or focus on a certain device.

Historic Events

The SEM historical feature allows users to view logs in a certain date and time. Apart from this user can use several other search filters to look for a specific event, users even can save these custom searches and reuse them. After finding the results they are looking for users have the ability to export the results to CSV format if they need. This is very useful feature in case if the organization is investigating an incident and want to view, compare older logs.

Rules

The SEM comes with many standard rules which users can configure accordingly, these rules belong to categories such authentication, compliance and much more. Users also can write custom rules according to their preference. Once a rule has been created the SEM can be configured to address the issue in automatically in real time.

Nodes

Using HTML 5 based node management feature, users can add agent nodes, configure and monitor them. There are two types of nodes such as agents and non-agent devices. The agent is application installed on the device which collects and normalize log data before sending it to the SEM device. The non-agent directly send the logs to the SEM device without normalizing the data.

Configure

SEM has four Configure options **Email templates**, **User defined groups**, **Users** and **Directory service groups**.

* SEM has many default **emails templates** and pre-configured **user defined group**. The admin can create new an **email template**, **user defined groups** according to their need.
* The **users** option contains the information about the current users, When creating a user, the SEM request the role of the new user so the privilege can be set accordingly.
* The **directory service group** shows the existing groups and if the user needs, they can create a new group.