**Splunk SIEM Use Cases Examples**

|  |  |
| --- | --- |
| **Use case** | **Name** |
| 1 | Detection of Virus outbreak |
| 2 | Zero-day Attacks |
| 3 | Privileged User Monitoring |

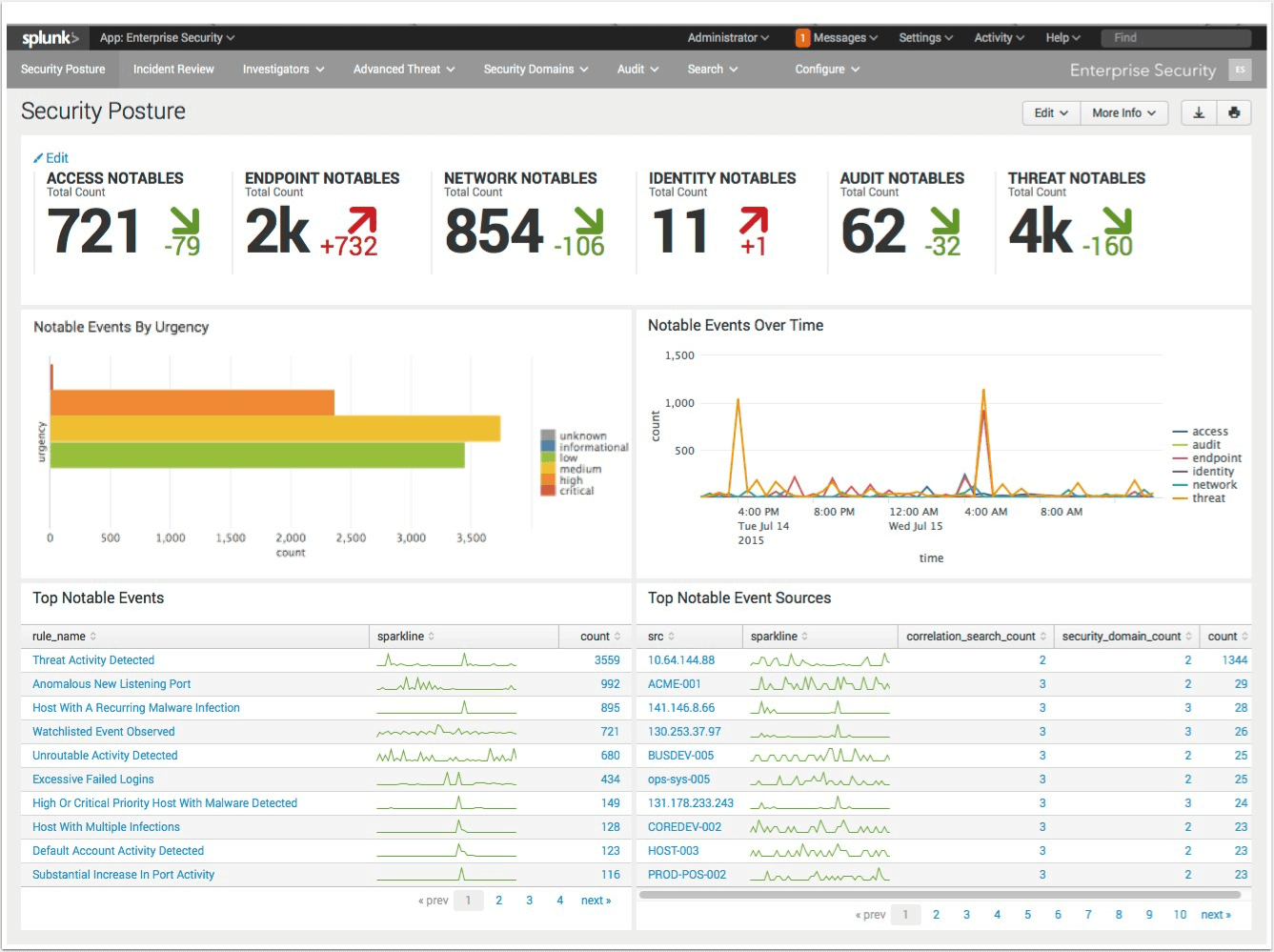
**Use case #1: Detection of Virus Outbreak**

SIEM can be used for different purposes. One of the uses of implementing an SIEM is for detecting the outbreak of virus. By implementing Splunk Enterprise Security the detection of malware is made easier with the help of dashboards, correlation techniques, and by the reports which are generated after the search. As traditional antivirus software only recognizes the specific kinds of malwares which caused the previous attacks, but SIEM can be modified by changing the enabled the rules and also by modifying the correlation techniques in order to find the patterns of the attack. By using SIEM only particular devices which needs attention can be taken under observation without leaving other devices.

In this use case Splunk Enterprise Security is taken as an example and by using this how viruses are detected and how the remedial activities are initiated after that are also discussed.

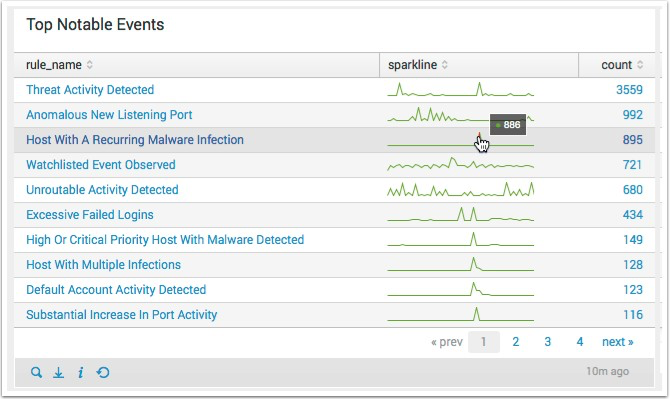
**Overview:**

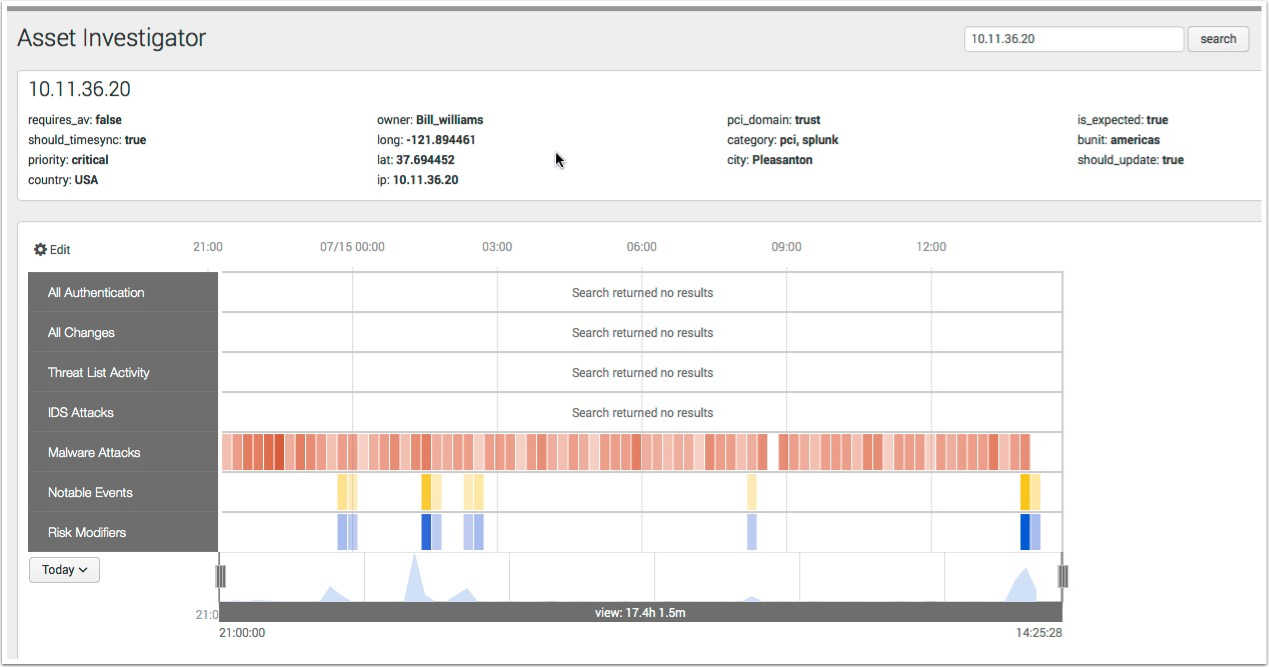
The dashboard of the Splunk Enterprise Security looks like this. In that the notable events and notable events over time are displayed. By clicking the top notable events on the dashboard, for example we want to know about the host with the recurring malware infection, by just clicking that the details of that issue will be displayed.



**Details of the infected host:**

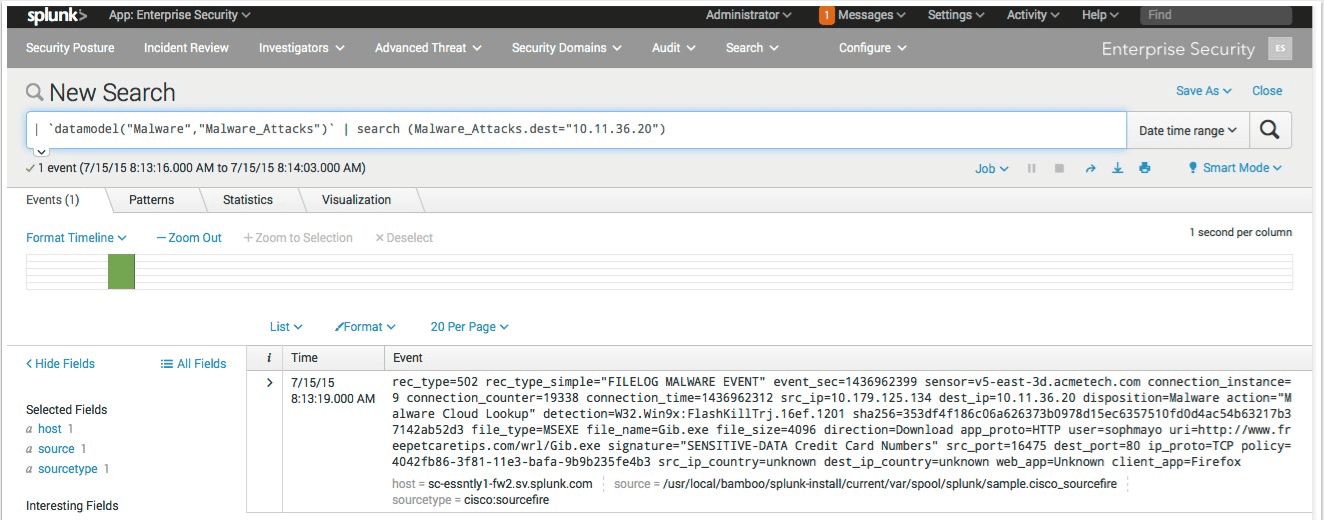
Details like source and destination IP addresses, at what time the event happened, the count of times it happened, the name of the rule which is given to it before the implementation and other kinds of details are known.

  
**Details about the malware attack:**

In the asset investigator section, the details about the malware attacks that happened on the network are known. Notable events are also detected along with the details of the owner, IP address of the host and severity if the issue are also known. 

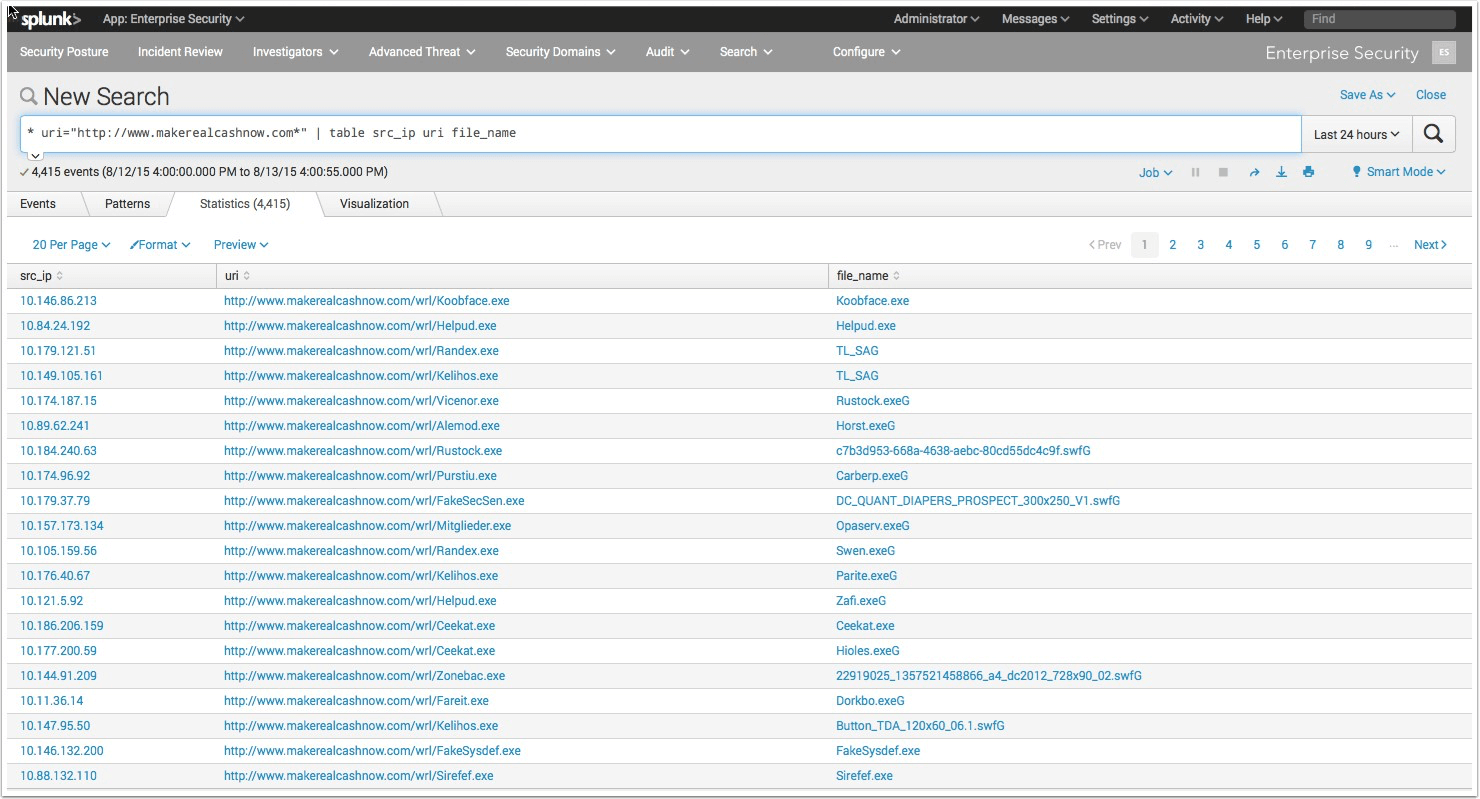
**Detecting the Spread:**

After detecting the initiation of the malware attack, the spread of the attack on the network is to be detected. The source IP which initiated the attack is to be recognized. Details like from where the malware is entered and the by accessing which website the network got effected, which employee made that mistake and details like if and any employee did the same kind if mistake by downloading the malicious file and caused the spread of the virus is known.



**Initiating Remedial Activity:**

By isolating the systems that are effected, the spread of the virus among the network can be controlled. By doing further research in the logs, the details like the domain name which is used at the time of download is known. By searching the devices which used the same domain will help to find other affected hosts. In the last stage all these hosts, domains, devices list is sent to the admin so that further investigation is done in the process of getting rid of the malware.



**Use case #2: Zero-day Attacks**

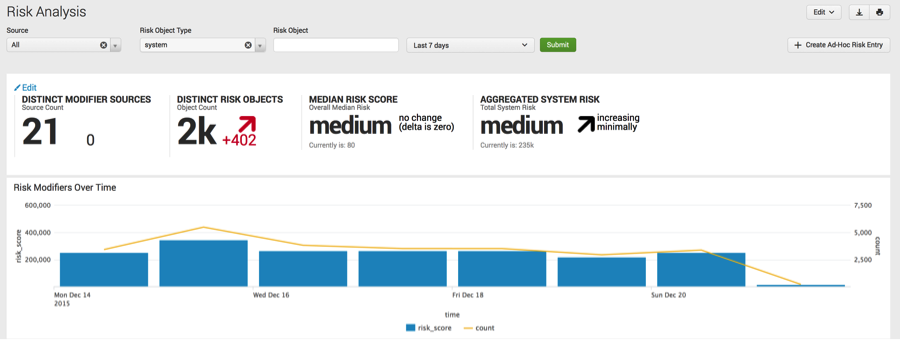
Every application or a software has its own vulnerabilities. If an application is exploited even before the vulnerabilities got eliminated, then those kinds of attacks are known as Zero-day attacks. These kinds of attacks are the worst because the developers of the application or software have not even detected the vulnerability by the time the attackers started performing exploitation. The only way to get away from this Zero-day attack once it is performed is to wait for the developers to give an update of the application or the software by removing its vulnerabilities and other kinds of bugs (if any).

In order to make these kinds of attacks from not happening is to prevent them from occurring. This can be done by keeping a good eye on the activities that are happening around the network. To do these kinds of tasks there are different kinds of tools. Here we are taking Splunk as an example.

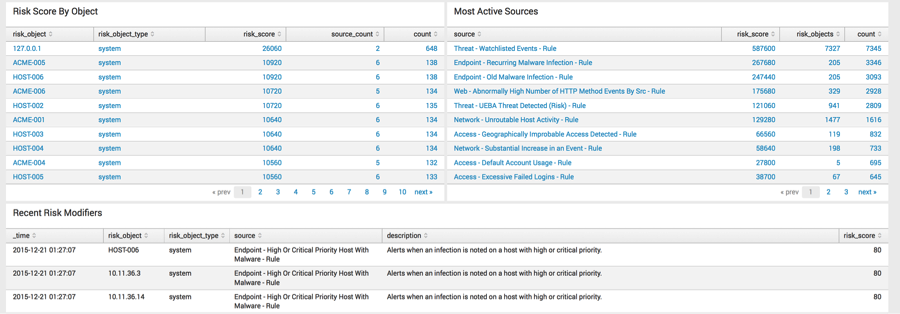
**Dashboard:**

Splunk Enterprise Security is the add on which is to be installed and added to the Splunk enterprise application. Then configure the sources of the data from which the data is to be retrieved. After configuring the sources go to the risk analysis dashboard to inspect the activities that are going on in the network.

**Review Risk Score by Object:**

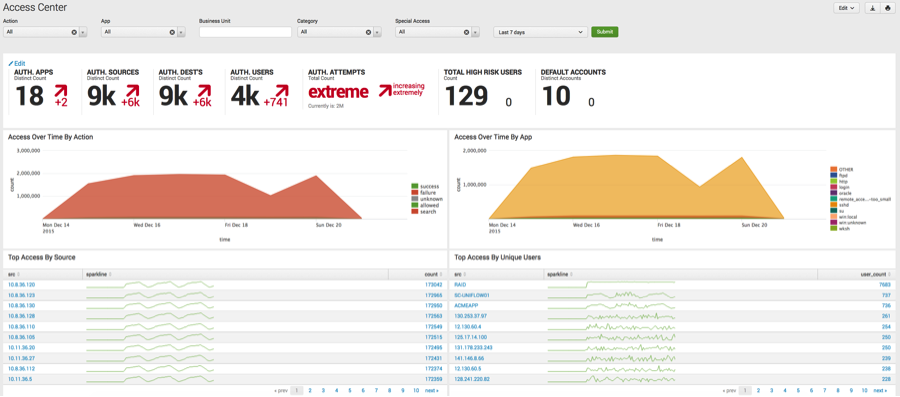


By reviewing the risk score, the risk modifies can be analyzed which gives an idea over the network and the sources which are active in those activities are also known. The time at which the alerts are initiated, the risk object, risk object type and the score of the risk is also known.



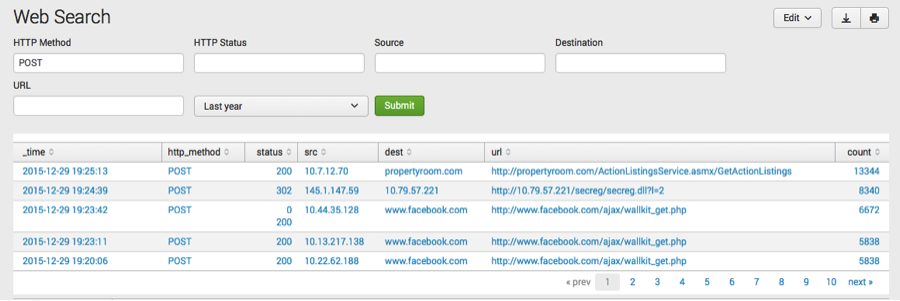
**Detection of Malicious Authentication Attempts:**

In the Access Center details like Authenticated Apps, Authenticated users along with details like authenticated attempts. Form this the user can know whether the network is compromised or how many systems got effected, number of attempts made other data.



**Web Search and Malware Search Dashboard:**

By using this dashboard data, the details like if the data exfiltration using the HTTP ports if taken place can be found. Web proxy logs are used as source in order to find these kinds of information. In the other hand, Malware search is used to find if any malware attacks are taken place by using the web proxy logs as source same as Web Search.

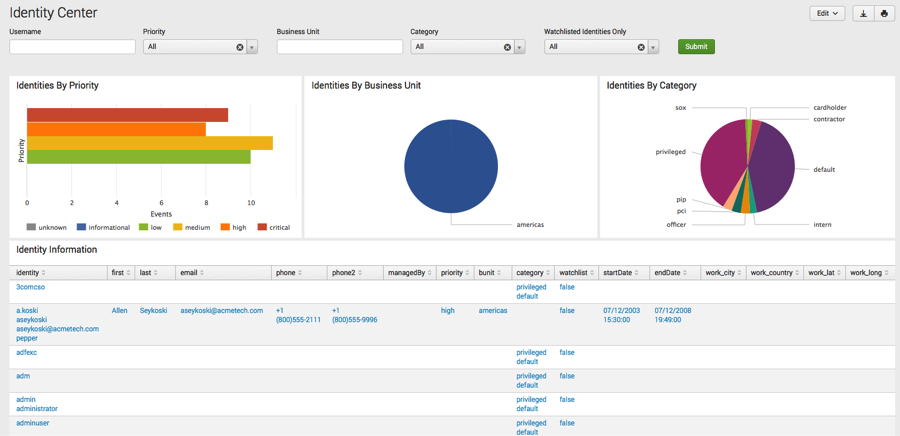


**Use Case #3: Privileged User Monitoring**

In recent days the attackers are performing phishing attacks and getting details of the authenticated credentials. Those credentials are used to perform escalated privilege attacks in order to gain access to the restricted data, confidential files and even to perform actions of managerial level. To ensure that these kinds of attacks will not happen there are some tools which can be implemented inside the network of an organization. Splunk Enterprise Security is an example for those kinds of tools.

**Overview**:

Install and configure the Enterprise Security in the Splunk Cloud, then you are ready to go. In the dashboard there will be information about the identities, and they are divide by priorities, business unit and by category. In the identity information there will be detailed information like to which category it belongs to, the identity of it, priority of it and many other things.



**Dashboard**:

In the Enterprise Security there is an in-built section which will allow to perform searches of privileged actions. In the privilege user monitoring dashboard, there will be two different sections like privileged accounts usage and privileged accounts in use, which shows different types of details like how many time the user made the login attempts, how much time he has spent while he was logged in etc.,

