**Arc Sight SIEM Use Cases Examples**

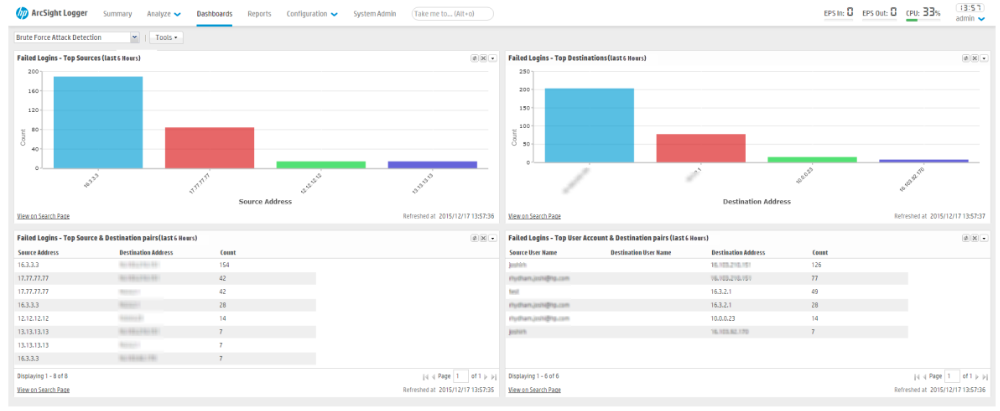
|  |  |
| --- | --- |
| **Use Case** | **Name** |
| 1 | Brute Force Attack Detection |
| 2 | Firewall Monitoring |
| 3 | Monitoring VPN Security |
| 4 | ArcSight vs WannaCry ransomware worm |
| 5 | Antivirus Monitoring |
| 6 | Reconnaissance Attack Monitoring |
| 7 | IDS- IPS Monitoring |
| 8 | Anomalous Traffic Detection |
| 9 | ArcSight for Cisco Solution Package |
| 10 | Email Malware Monitoring |

**Use case #1: Brute Force Attack Detection**

The attack which is performed number of times in order to gain access to the system by using different login credentials is known as brute force attack. In this kinds of attacks, a series of attempts are made on the server in order to login. There are different kinds of tools available to make a note of these attempts. ArcSight is one of them and it can be used to generate an alert when these kinds of attempts are made to login.

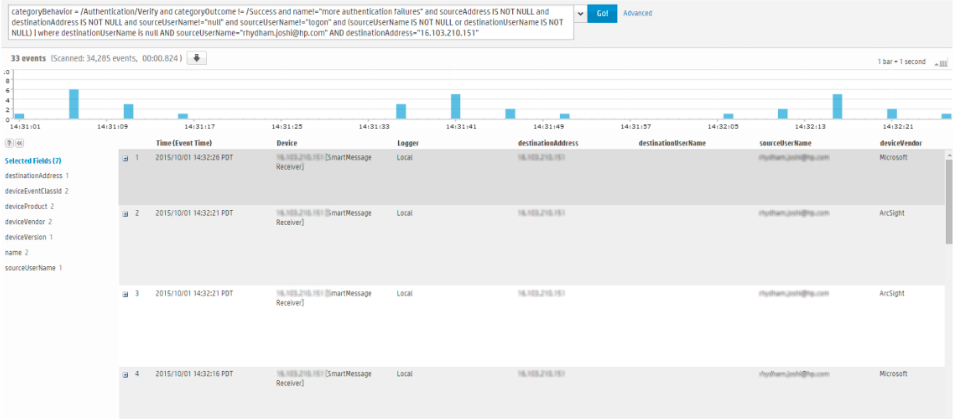
**Overview:**

The main parameters which will decide that the ongoing event as a brute force attack are to be configured in the ArcSight. The parameters are number of attempts that are made to login (some of them may be successful and some them may be unsuccessful both are considered as a brute force attack it the attempts are made several times), the source and destination of the attempts is also determined in the details, and the account form which these attempts are made can also be found.



**Dashboard**:

The primary page gives the details of the data about the source and destination. In order to get further information, click the event which you find suspicious, then additional information like event time, from which device it is originated, user names of the destination and the source, vendor of the device and other detailed information is given.

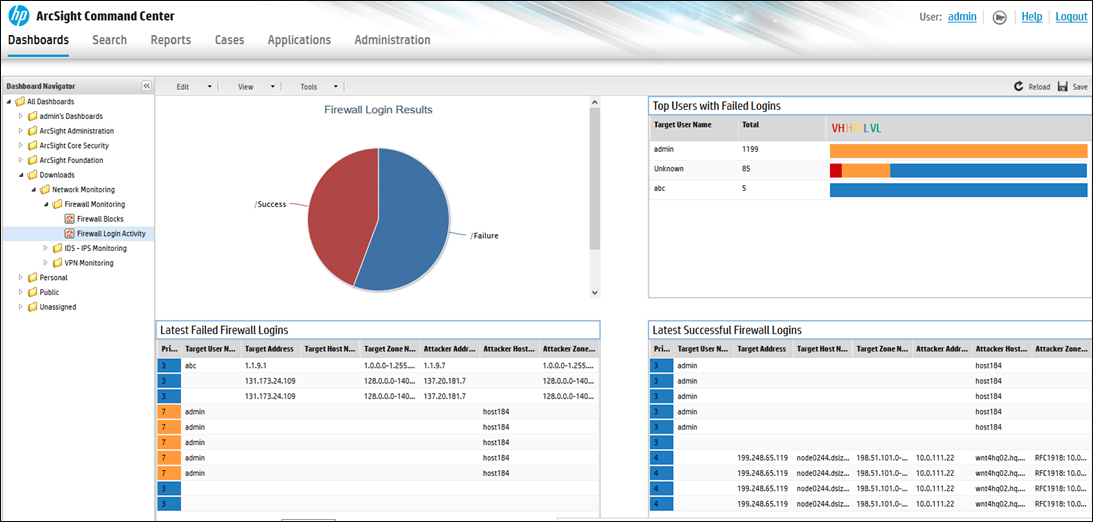


**Use case #2: Firewall Monitoring**

Firewall is the primary tool which is used to block the outside network traffic to effect the inside devices. This can only be achieved only if the rules are configured properly for the firewall. Monitoring the logs of the firewall is also important. There are different tools available out there, we are using ArcSight as an example.

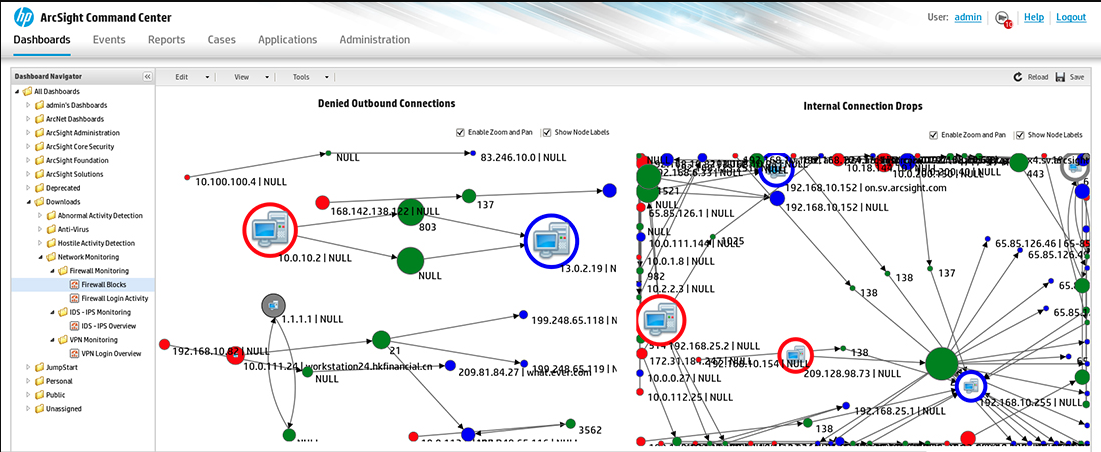
**Overview:**

In the firewall dashboard section of the ArcSight, the details like how many successful attempts of the firewall, how many failure attempts are done on the firewall, total number of attempts and other details like what activities does the firewall blocked are shown.



**Connection Drops:**

In the deeper view the ArcSight gives the detailed view about the internal connection drops, denied outbound connections, IP address of each device, mapping of the devices that are connected to the network, Firewall blocks that are done over the network are also can be viewed.

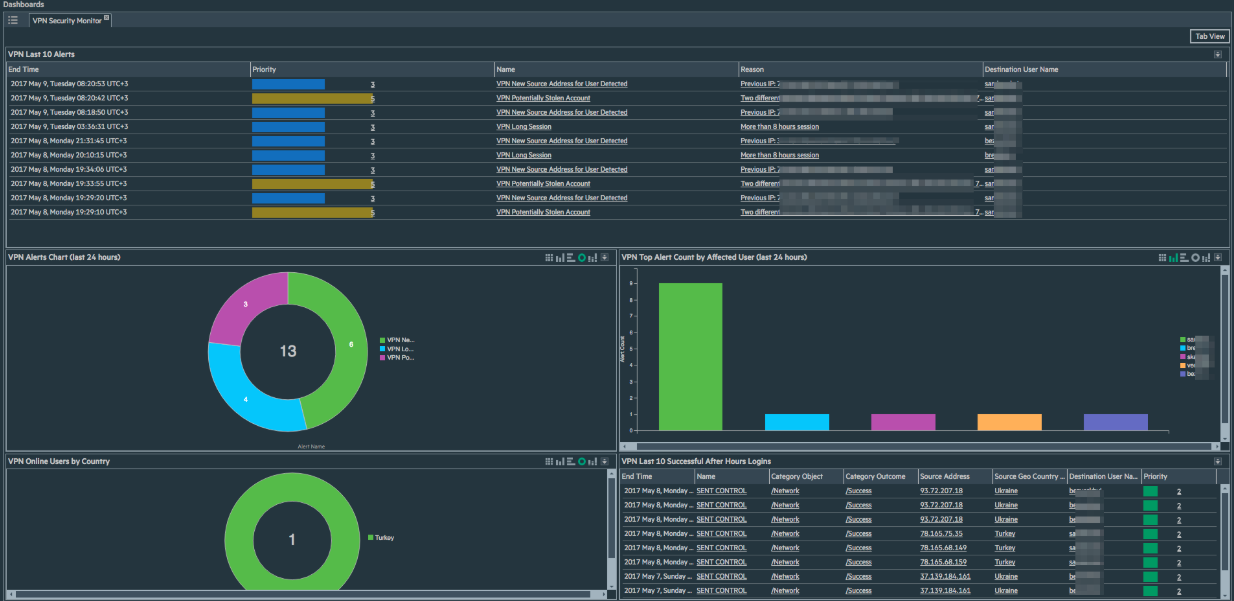


**Use case #3: Monitoring VPN Security**

Virtual Private Network provide a secure connection between the user and the network of the organization. This is mainly used by work from home employees. As these VPNs can be accessed from outside, there is a chance that the attackers may also gain access to the network of the organization. SO monitoring the VPN is important. To do this there are different kinds of tools available, here we are taking ArcSight ESM and Express 6.11 as an example.

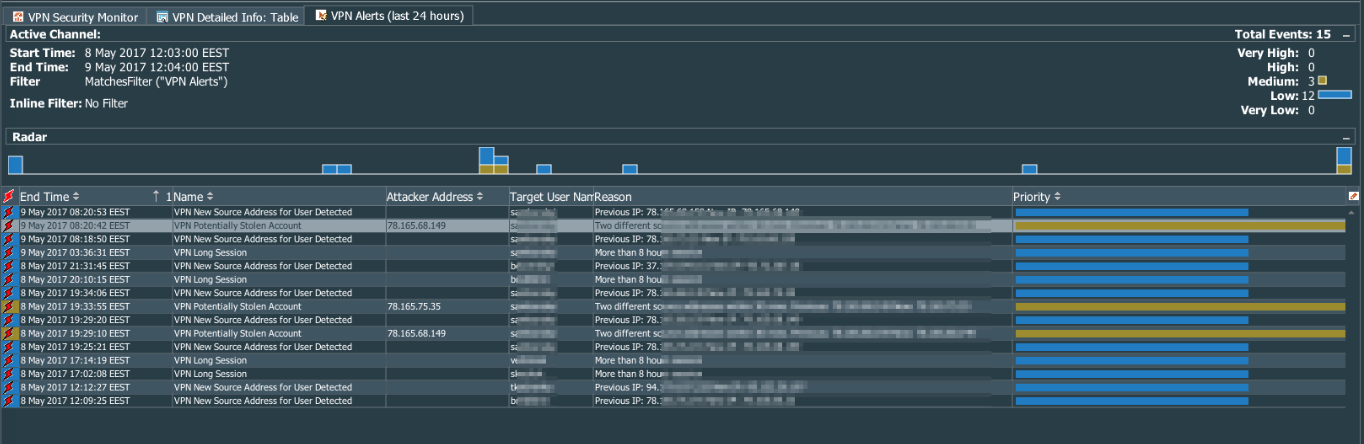
**Overview:**

By clicking VPN Security Monitor the details like the alerts which popped within the last 24 hours are shown and other details like name of the alerts, destination user name, end time of the alert, priority level if the alert, VPN top alerts count by affected user and many other details are known in the VPN Security Monitor.



**Test Events in Active Channels:**

In the test events section, the detailed information about the VPN will be shown. Details like start time of the connection, end time of it, the amount of data that is being transferred through the connection, attacker’s IP address, number of events that are produced with in a time period is also shown in the VPN Alerts window.

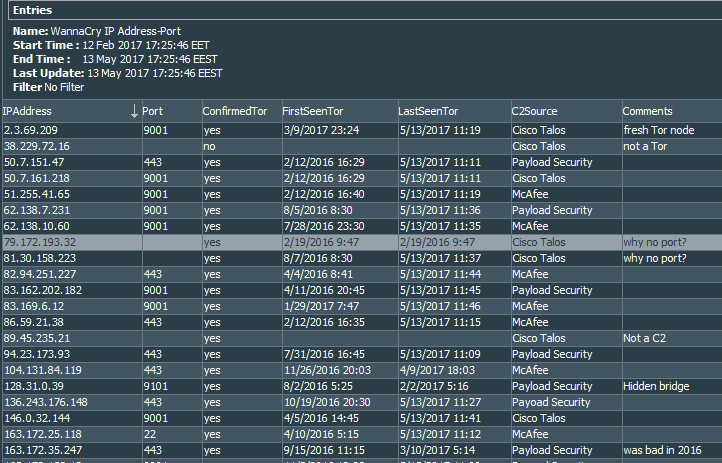


**Use case #4: ArcSight vs WannaCry ransomware worm**

WannaCry is an attack which used WannaCrypt ransomware to affect the systems which are running on older versions of Windows. This was happened on May 2017 and affected almost hundreds of countries worldwide. The ransomware even installed a backdoor on the systems that they have affected. In order to detect the wannacry ransomware, different kinds of software were made available and ArcSight’s WannaCry Ransomware Worm Detector is one of them. This helped the analysts team to detect the systems that got effected by this software using indicators of compromise (IOC)

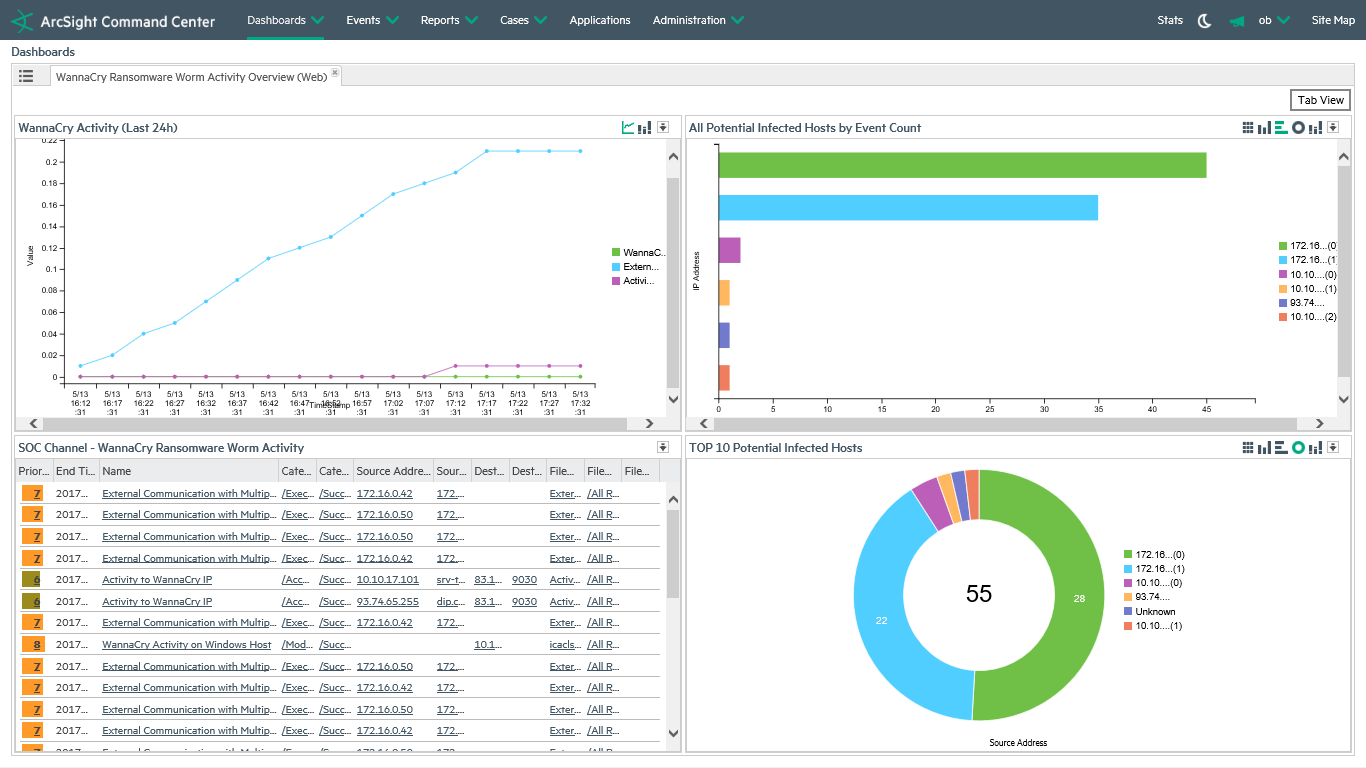
**Overview**:

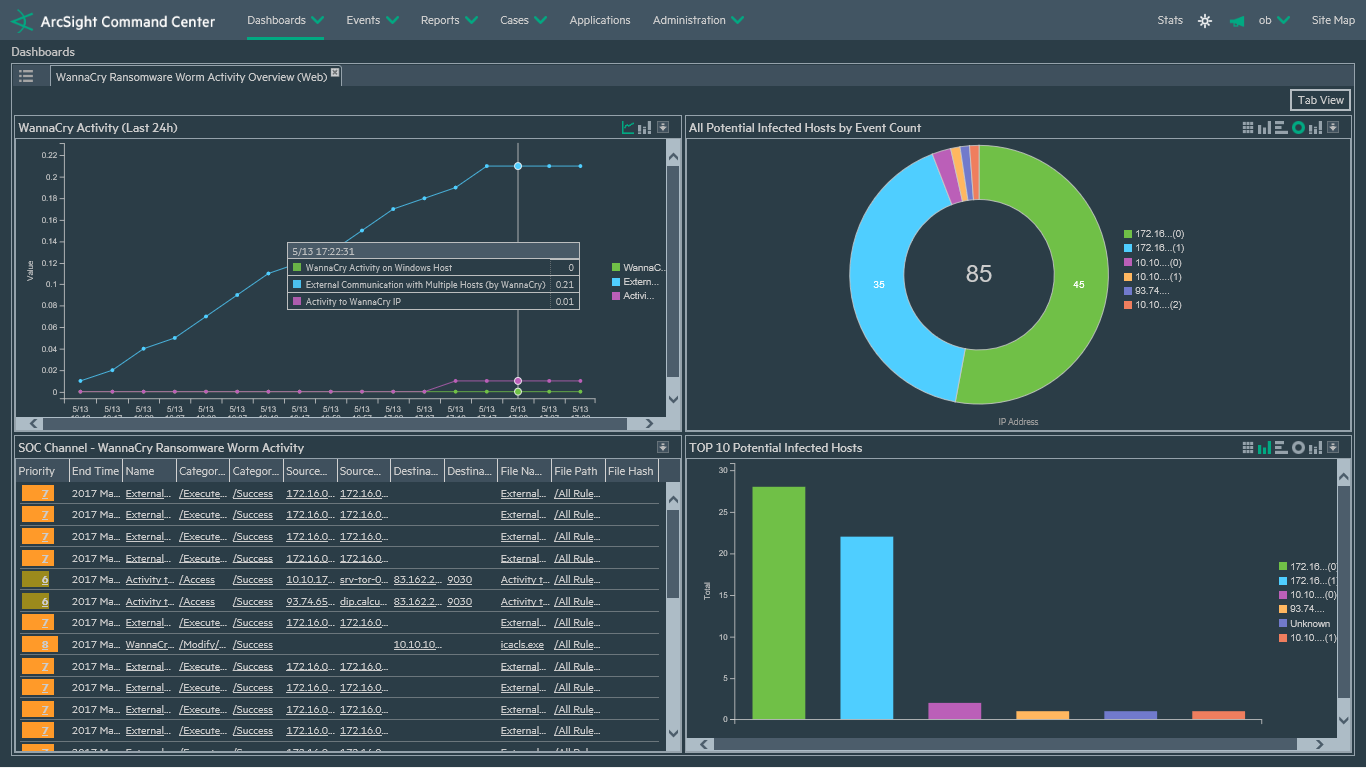
The WannaCry Ransomware Worm Detector is used to see the entries with the name of the port, start time and the end time of the action etc., In the list of the entries there will be categories of the port number from which the connection is made, the IP address of the connection. As this used Detect Tor technique, there are different categories in the table like First Seen Tor, Last seen Tor, Confirmed Tor and the comments for each connection (if any).



**Dashboard**:

In the dashboard of the ArcSight Command Center, there are different sections like Wannacry activity within last 24 hours which consists of a table with timestamp on the X-axis and Value on the Y-axis, all potential infected hosts by event count, SOC Channel-Wannacry Ransomware Worm Activity, Top 10 Potential infected Hosts etc.,



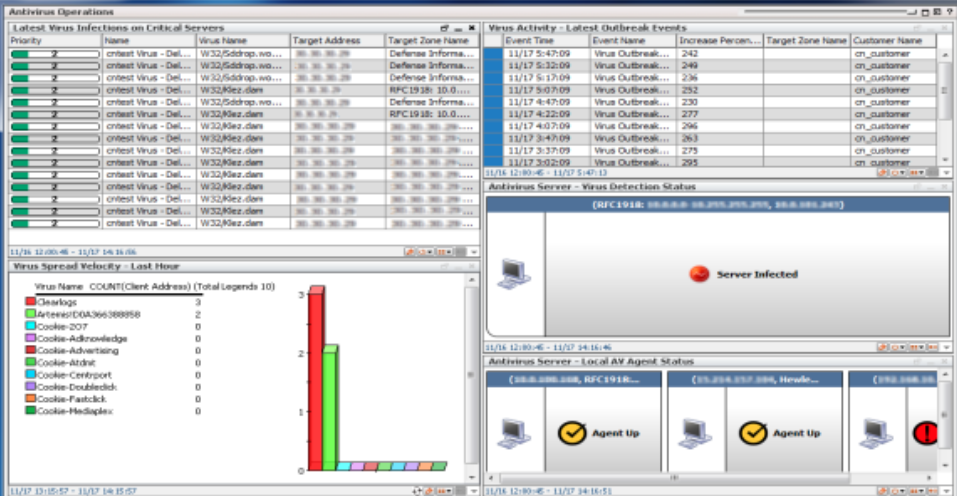


**Use case #5: Antivirus Monitoring**

Monitoring the activity of the virus in the organization is a process of scanning the devices which has a possibility of getting affected by virus and other kinds of malicious files. Virus is a program which is made to make the system to behave improperly. The virus is generally installed in devices like laptops, desktops etc., There are some kinds of virus which can replicate themselves and spread to other systems which are connected to them, these kinds of virus are known as worms. By installing the antivirus programs, the antivirus monitoring tool scans the devices to identify infected systems based on their abnormal behavior. There are different tools available to do this job, here we are using ArcSight Console.

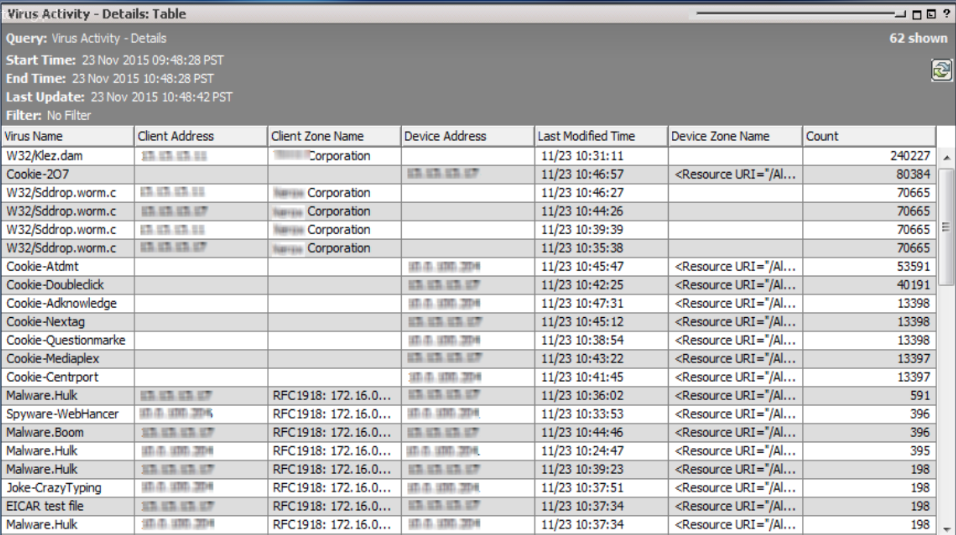
**Overview**:

The Antivirus Monitoring tool is used in the ArcSight by adding the zip file of Antivirus monitoring to the ArcSight Console. In the starting stage of implementing the tool you will see a dash board. The dashboard consists of the divisions with information like latest virus infections, the time at which they got affected, stage of the servers, virus activities, latest outbreak events, the velocity of the virus etc.,



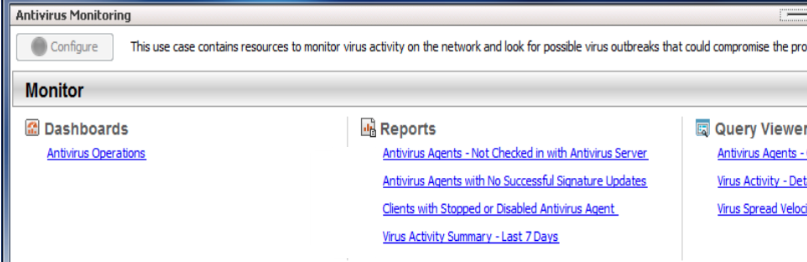
**Query Viewer:**

The query viewer gives detailed information of the virus activity in the form of a table. The table consists of the details like the type of query that is made, the start time of the activity, the end–time of it, last update that is done on the activity etc., If a virus gets detected then, the important information like virus name, client address, client zone name, the address of the device etc., The velocity at which the virus is spreading through the devices is known the number of count that it has made. If the count is higher then, the velocity is said to be higher.



**Reports**:

After completing the process of monitoring the activity of the virus, the reports of the progress are done. The time of making is report is based on the activities that are happened inside the network. If the activities that happened in the network are more then, the time taken to make a report is more. In the same way the time taken by the tool is less if the activities of the network are less. In default the reports are made in HTML format and the file which you want to save is to be converted into pdf of any other format so that they can be read in future.

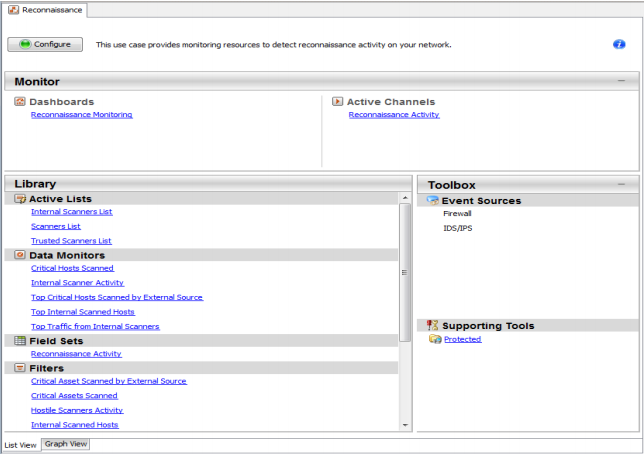


**Use case #6: Reconnaissance Attack Monitoring**

The objectives of a reconnaissance attack are to collect the target’s network information, system information, and the organizational information. By carrying out reconnaissance at various network levels, the attacker gains information such as network blocks, network services and applications, system architecture, intrusion detection systems, specific IP addresses, and access control mechanisms. With a reconnaissance attack, the attacker collects information such as employee names, phone numbers, contact addresses, designation, and work experience, etc., which leads to social engineering and other phases of the intrusion into the corporate network.

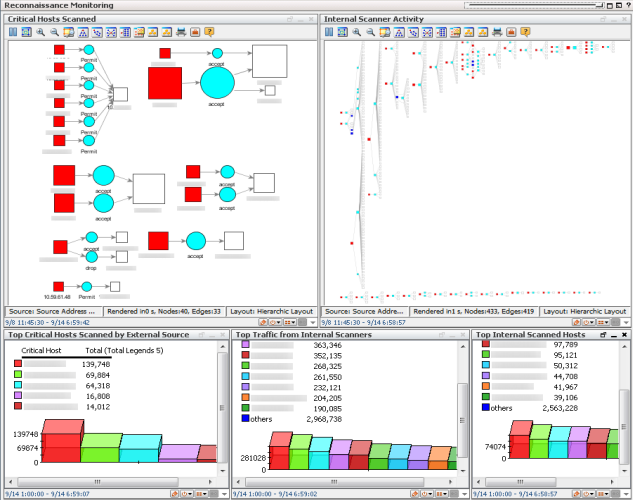
**Overview**:

The process of gathering the information to make an attack in future is known as reconnaissance. To monitor the activities that are happening in the network which resembles the reconnaissance can be monitored in the dashboard. From the dashboard the information like critical hosts scanned, internal scanner activity, reconnaissance activity and many more windows can be opened which gives a detailed information about the reconnaissance activity that is happening in the network.



**Reconnaissance Monitoring Dashboard:**

The reconnaissance dashboard is a separate window which specifically shows the information about the details of the critical hosts scanned, internal scanner activity, top critical hosts scanned by external sources, top traffic from internal scanner, top internal scanned hosts details are represented in the diagrammatic form and even some of them are represented in bar diagrams to make it more understandable.

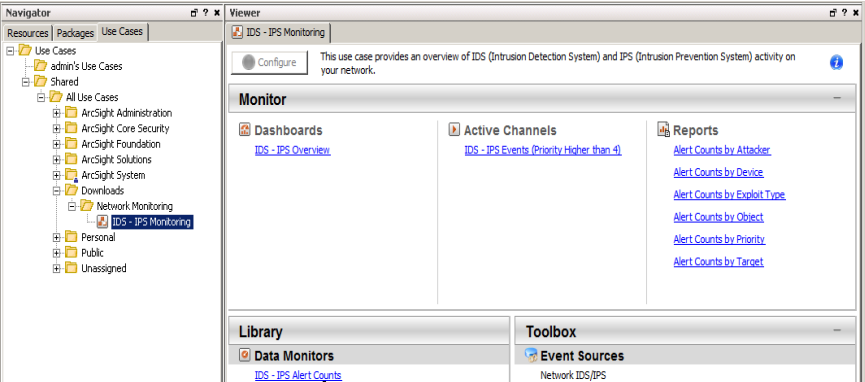


**Use case #7: IDS- IPS Monitoring**

Intrusion Detection Systems and Intrusion Prevention Systems are the devices which scan the data packets that are coming into the network and they try to find the suspicious data in it. They mainly work based on the signature mechanism in which they compare the data with the previously found malicious content and tries to relate them with the current content. If any suspicious or malicious content is found they blocks them as they violate the policy of the IDS and IPS. To monitor all these activities and the traffic that is going through IDS and IPS there are different kinds of tools that can be used. In this case we are using ArcSight tool as an example.

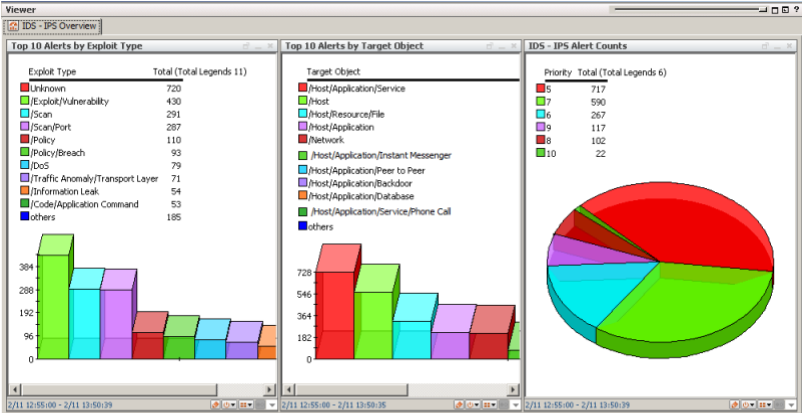
**Overview**:

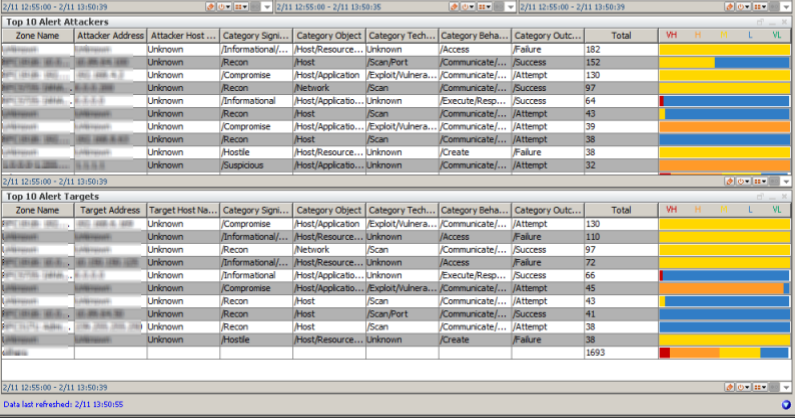
The first step of implementing it is to install it in the ArcSight Console and the launch it. The first that can be noticed is the navigator panel. Select the IDS-IPS monitoring in that where the dashboards, active channels and the report sections are shown.



**Dashboard**:

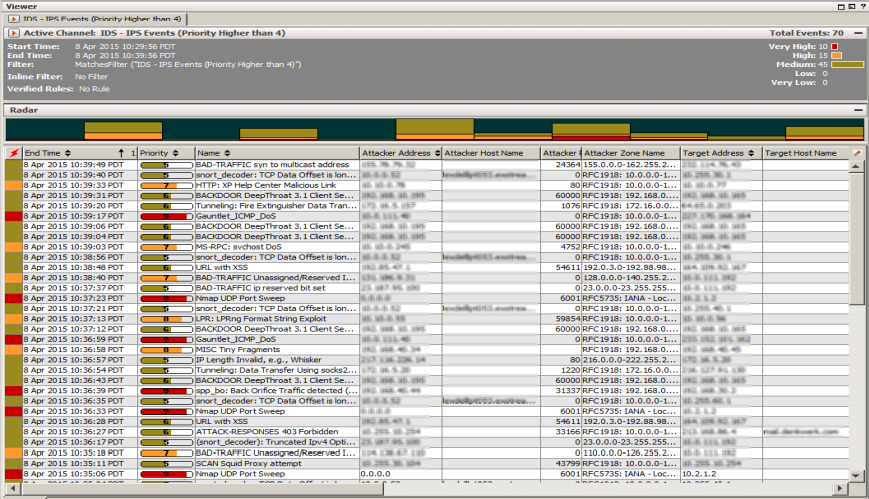
By clicking the dashboard in the opening screen, the activities that are happening in the network are shown and they are divided into separate divisions. There will be like Top 10 alerts by Exploit type, Top 10 alerts by Target Object, IDS-IPS Alert counts and other top 10 categories of attackers and targets. By going into the details of each of the category there will be details like type of the exploit, target object, priority total and other details like zone name, attacker address, target adders, other details regarding them can also be found.





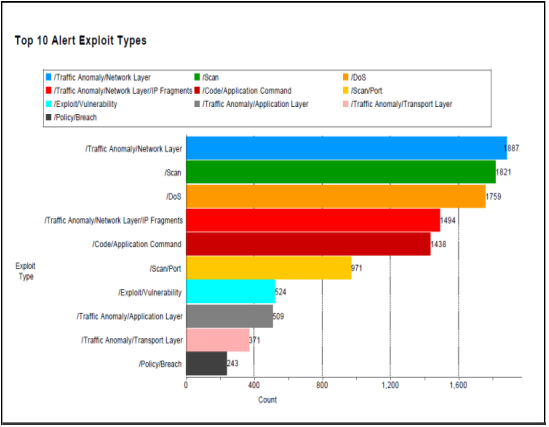
**Priority events in the Active Channel:**

Investigating the priority events in the active channel is done in the next stage as it was the second category the is showed on the dashboard of IDS-IPS monitoring. In the event priority only the events of priority level 4 and above are shown, along with some other details like start time and end time of the investigation, attackers address, attackers host name, target address etc.,



**Reports:**

The IDS and IPS monitoring lets the users to create the reports of the previously done monitoring and about the detected events, which can be submitted to the stakeholders of the company in the time of need. The data which is used for the report is generally will be the previous day data by default, we can change it to the day we need and create a report. There will be different kinds of reports of the alert counts, they are listed and divided by attacker, by device, by exploit type, by object, by priority, by target. A sample of the report is shown below as an example.

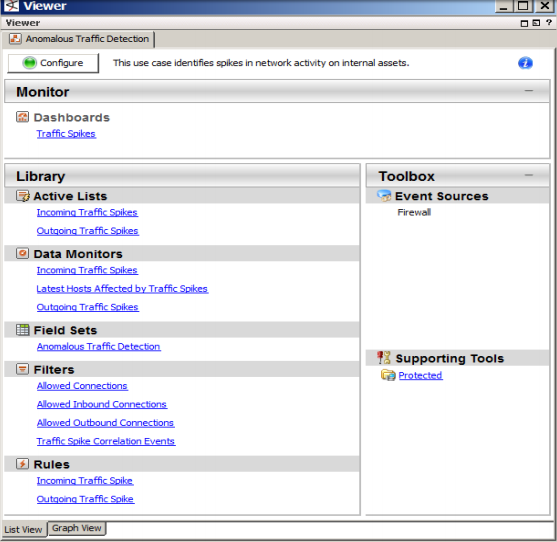


**Use case #8: Anomalous Traffic Detection**

In normal cases the spikes in the traffic will come from the scans and backups that are scheduled to be done on the network. All the spikes that happen on the network will not be good, some of them may actually refer an ongoing attack in the network. So monitoring the traffic is very important. To do this there are different tools available. Anomalous traffic detection use case of the ArcSight is one of them. So we are taking it as an example here.

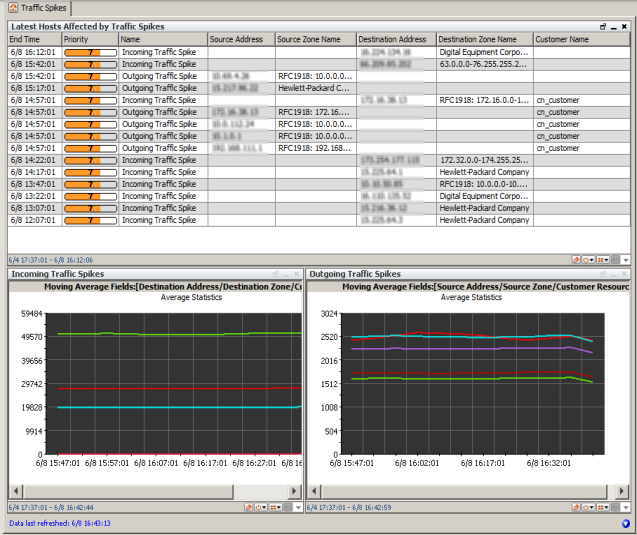
**Overview**:

By launching the anomalous traffic detection, the Viewer tab opens with the details like dashboard under the monitor section. There will be a separate section of the library tab where the active lists, data monitors, field sets, filters, rules, will be present.



**Dashboard:**

In the dashboard section, there will be a traffic spikes link. By clicking that the spikes that is happening in the network are shown. By the detailed view of it, we can get the information like latest hosts affected by the traffic spikes, which consists of information like end time, priority, name, source address, source zone name, destination address, destination zone name etc., In the other fields, further information of the incoming traffic spikes and outgoing traffic spikes are represented in the diagrammatic form which the actual spikes can be detected.

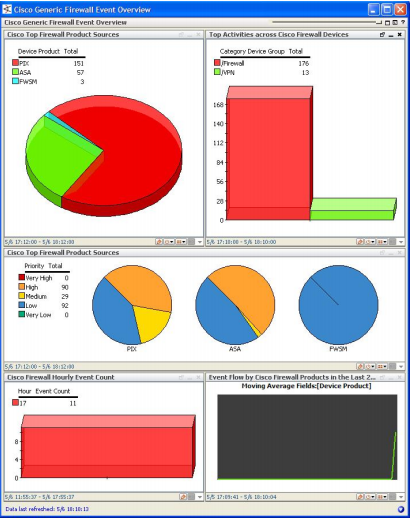


**Use case #9: ArcSight for Cisco Solution Package**

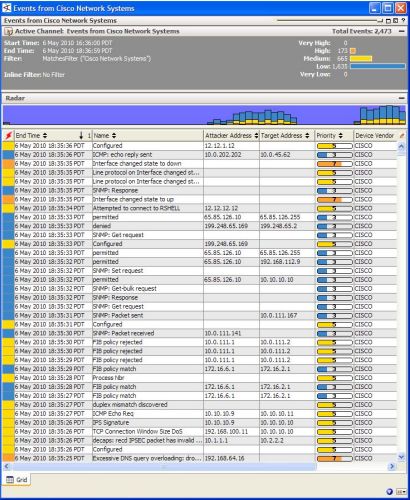
Cisco is a company which produces different kinds of networking hardware devices and telecommunication devices like routers, modems, IP phones, switches, security appliances, servers etc., The companies which use the Cisco devices can implement any kind of tools to monitor the activities that are going on in the network as these devices act as medium. ArcSight has a specific tool which is particularly used for these kind of situations where large enterprise uses huge infrastructure. SO ArcSight Enterprise View is taken as an example which is implemented for Cisco devices which are present in the network.

**Overview**:

The ArcSight Solution package provides a full coverage of monitoring over the cisco devices that are implemented in the network. It provides monitoring over the network traffic, devices that are functioning in the network, ports that active, changes in the configuration of any devices etc., can be noticed.



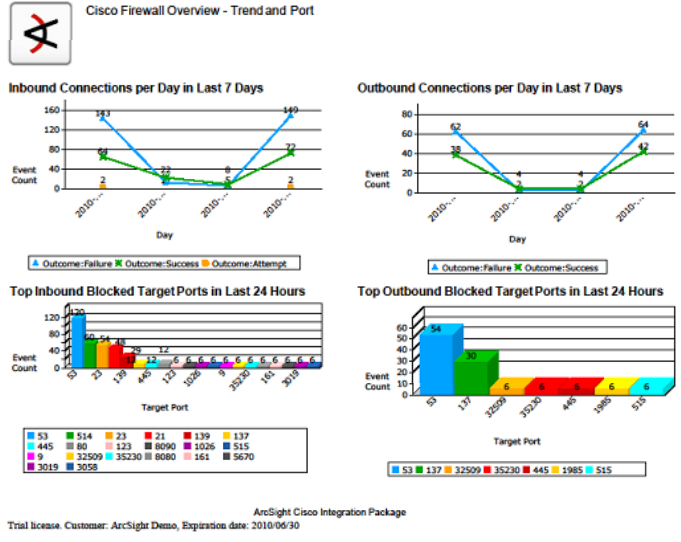
The above figure is an example of things that will show the details like top firewall product sources, Cisco Firewall events count, top activities across cisco firewall devices etc., can be known.



The above picture shows the events from cisco network systems with the priority levels and the name of the events. The attacker address, target address and if any other devices are added for monitoring then the device vendor section is also present to differentiate.

**Report**:

There are different kinds of reports that are already packed in the ArcSight Solution. As per the requirement the reports are to be prepared. Based on the need the data is recollected and represented in a simpler manner so that they can be understood easily. The reports may contain inbound and outbound connections per day in the last 7 days, top inbound and outbound blocked target ports in last 24 hours and other details are presented in pictorial form.



**Use case #10: Email Malware Monitoring**

Generally, Emails are used to sends the messages and it can also be used to send files and applications by attaching them to the messages. The user at the other end can download the files or applications to open them on his system. In these kinds of cases the attacker makes the user to download the malware affected files on the target system so that they can gain access to the files of it. The attacker can even install a backdoor so that he can come back whenever he needs without confronting the victim. So the activities of the mail have to be monitored. To perform this ArcSight has a tool named Email Malware Monitoring which can be installed and can be added to the ArcSight software.

**Overview:**

The main window that comes when the sensitive email recipients is selected, will contain start time and the end time of the activity, last update on that etc., There is a separate table where the list of the activities that are happening on the mail are updated continuously with the details like email, creation time, domain name, comments that are added to the email (if any) and the count of the events etc.,

