**QRadar SIEM Use Cases Examples**

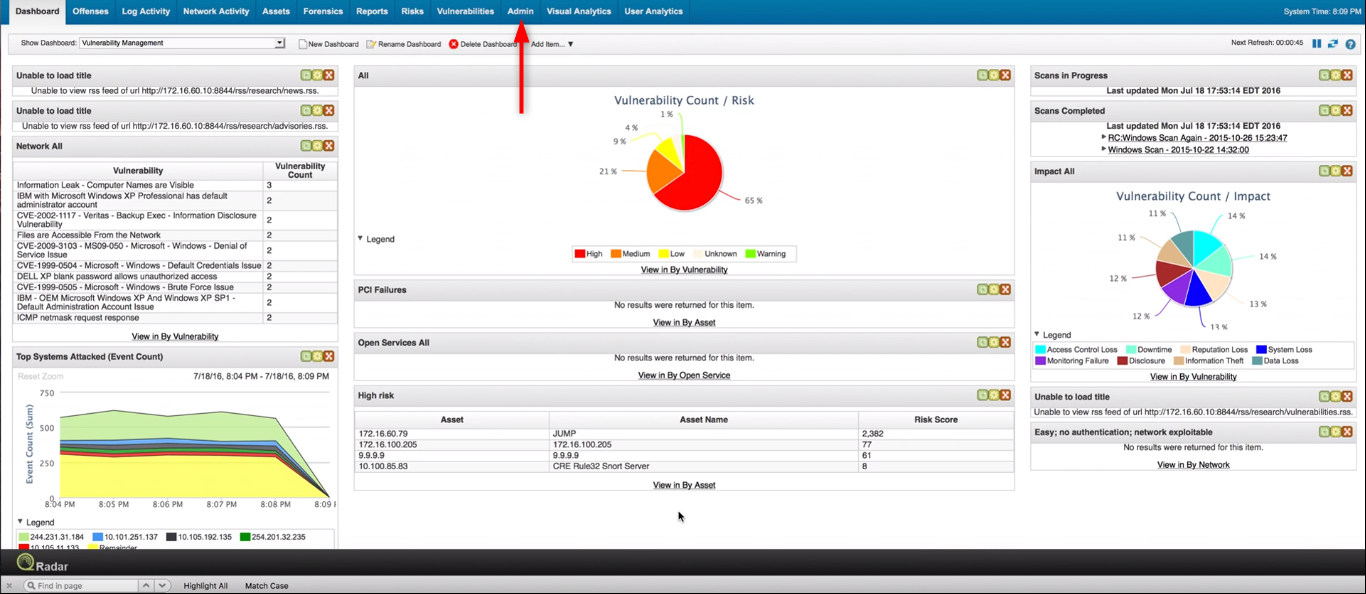
|  |  |
| --- | --- |
| **Use case** | **Name** |
| 1 | Detecting multiple login failures to compliance servers |
| 2 | Monitoring VPN access from countries a company business with |
| 3 | Detecting chatting to a malicious site using non-standard ports to avoid detection |
| 4 | Detecting Remote Scans |
| 5 | Detecting Internal Communication to a Command& Control Site |
| 6 | User Activity Monitoring - Employee Probation |
| 7 | Data Exfiltration Attempt through Online Storage |
| 8 | Performing DNS Analysis |
| 9 | Detecting Phishing Emails |
| 10 | Detecting DDoS attacks and Superflows |
| 11 | Detecting insertion of USB by an insider and visiting a Restricted Site |

**Use case #1: Detecting multiple login failures to compliance servers**

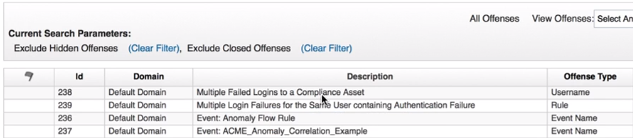
Multiple login attempts are done on the websites to gain access to the servers which lead to the compromise of the data of the database. In some cases, the attacker or a bot tries to attempt login to a particular website with numerous number of times until the attempts gets successful. Some websites may not allow huge number of attempts, but there will be a particular limit. In order to monitor those login attempts that occur from inside the network or from compliance servers, tools like QRadar can perform the monitoring task. Here QRadar is taken as an example.

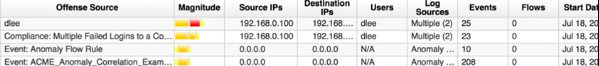
**Overview:**

Generally, the dash board of the QRadar consists of different sections. There are some predefined rules in the QRadar in the initial stage itself which are used to detect and monitor activities that are going on in the network. In order to perform the specified task like, detecting multiple login failures to compliance servers, new rule has to be defined. By clicking the Admin and by logging in new rules can be added and can also be modified.



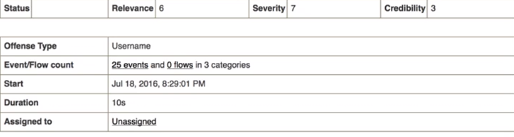
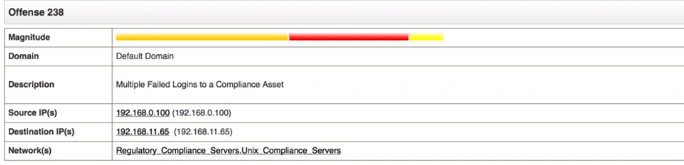
**Detecting the Login Failures:**

After creating and implementing the rules, the actual output is seen by going to the log activity section where all the logs are noted. By searching the required logs like login failure, the required information can be seen. The details like the ID , Domain name, description, offence type, offence source, magnitude of the attempt, source IPs, destination IPs, events that are created by this attempt and other kinds of information will be available.



**Detailed Information:**

By selecting a particular activity, in depth information will be available for that in particular. The magnitude section is available in which severity of the condition can be seen, the domain name, description of it, source IPs, destination IPs, Network, status of the activity, relevance, severity in number, credibility is also available.

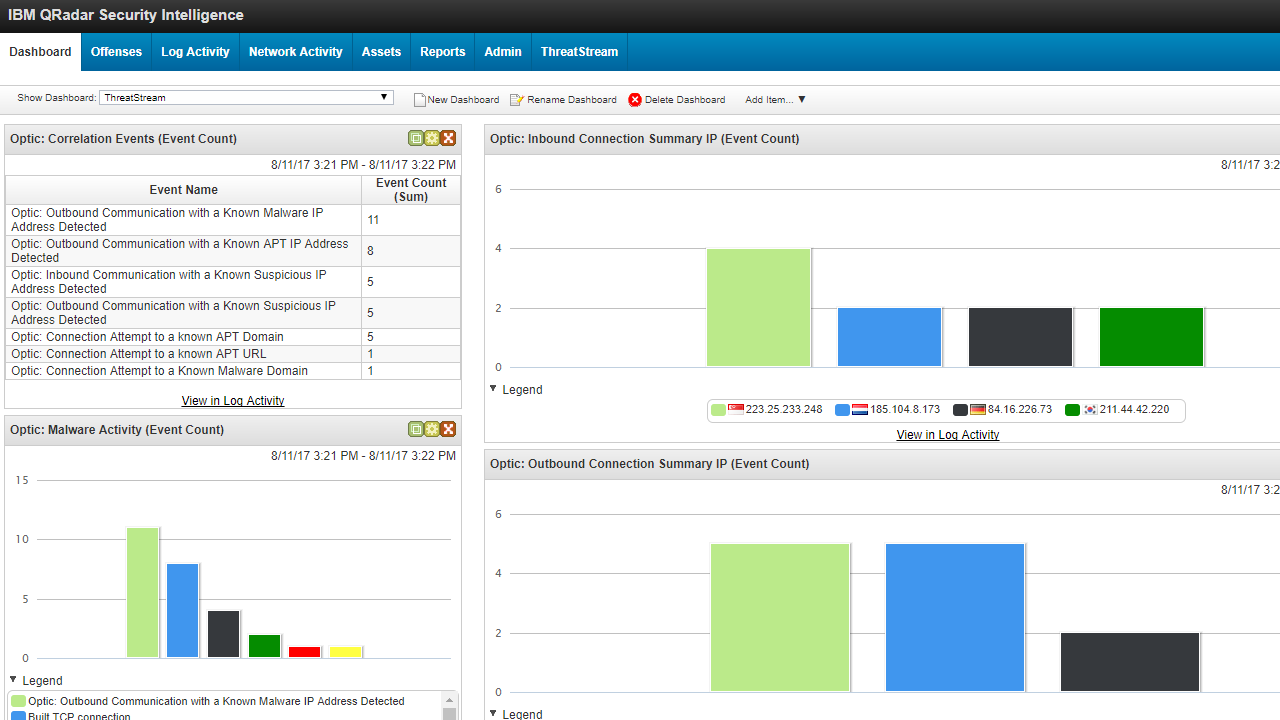


**Use case #2: Monitoring VPN access from countries a company business with**

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. Some companies will do business with different companies that are present in other countries. They have to communicate securely so they use VPN connections. 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. In order to do this task there are different tools but here we are taking QRadar as an example.

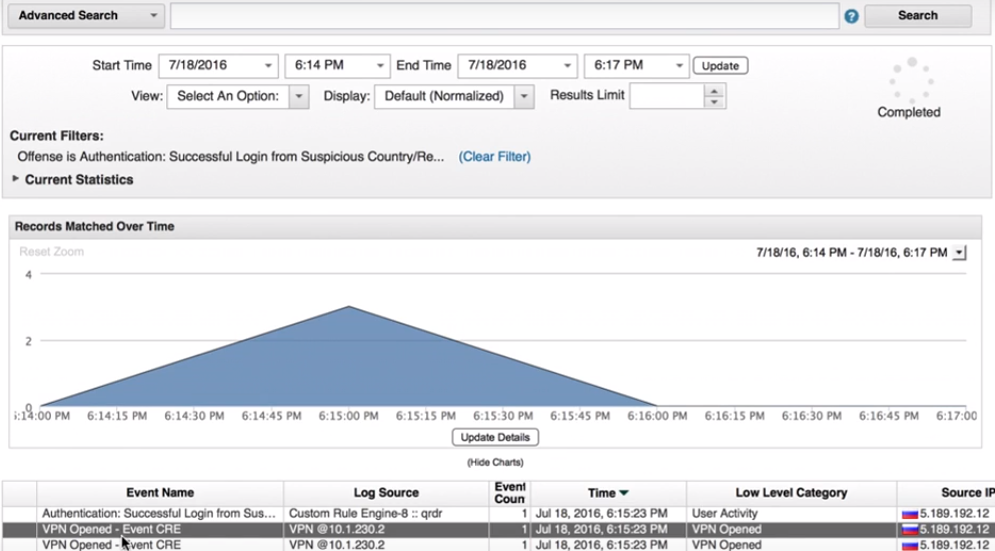
**Overview:**

QRadar initially has its own rules predefined. The new rules have to be added according to the needs of the user. In the dashboard details like correlation events, events count, malware activity, inbound and outbound connections summary IP and other can be seen. By clicking any of the section will give detailed information about them.



**Monitoring VPN access:**

Monitoring of the VPN activity that is going on and the connections that are being made to the network are noticed by defining the rules in the admin section. By monitoring the VPN connections, the details like event name, log source, event count, time of that event, low level category, source IP and other details like from which country the connection is made can also be noticed. The peak time at which the connections are made is also known.

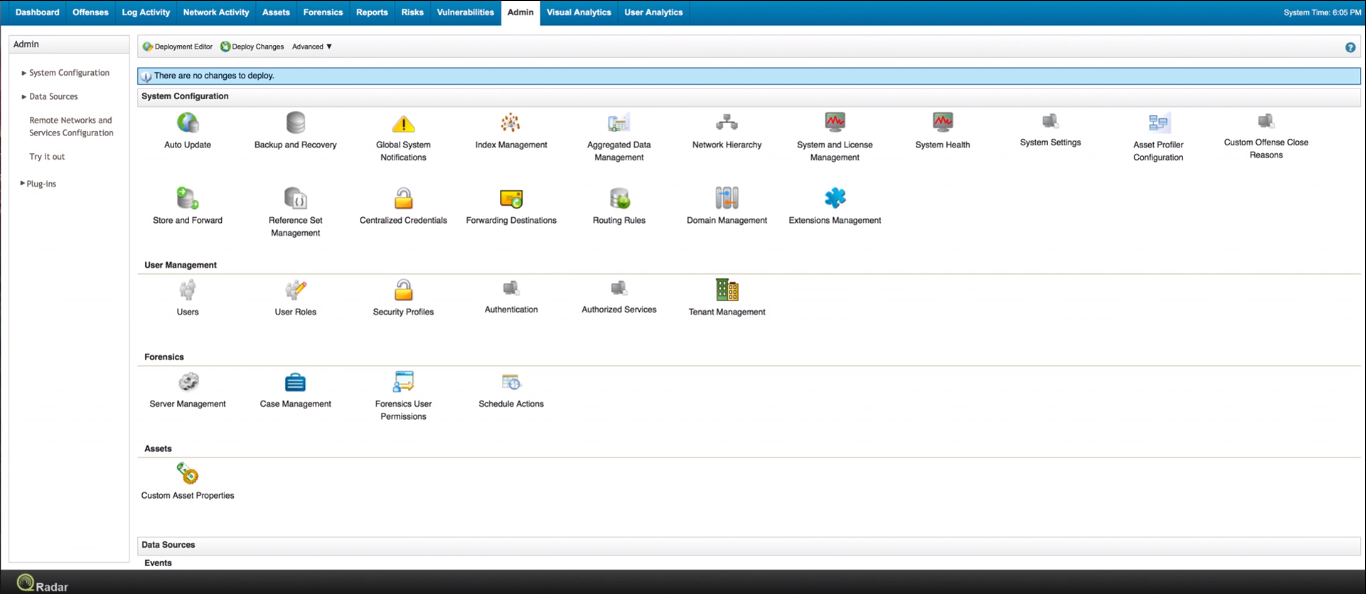


**Use case #3: Detecting chatting to a malicious site using non-standard ports to avoid detection**

There are different ports for a system from which can be used to transfer the files, mails and can also be used to make connections with other systems. Those ports can also be used to make connections between the websites and systems. Some insiders use non-standard ports to connect with the malicious sites and try to not get detected. To monitor these kinds of activities QRadar is taken as an example here.

**Overview:**

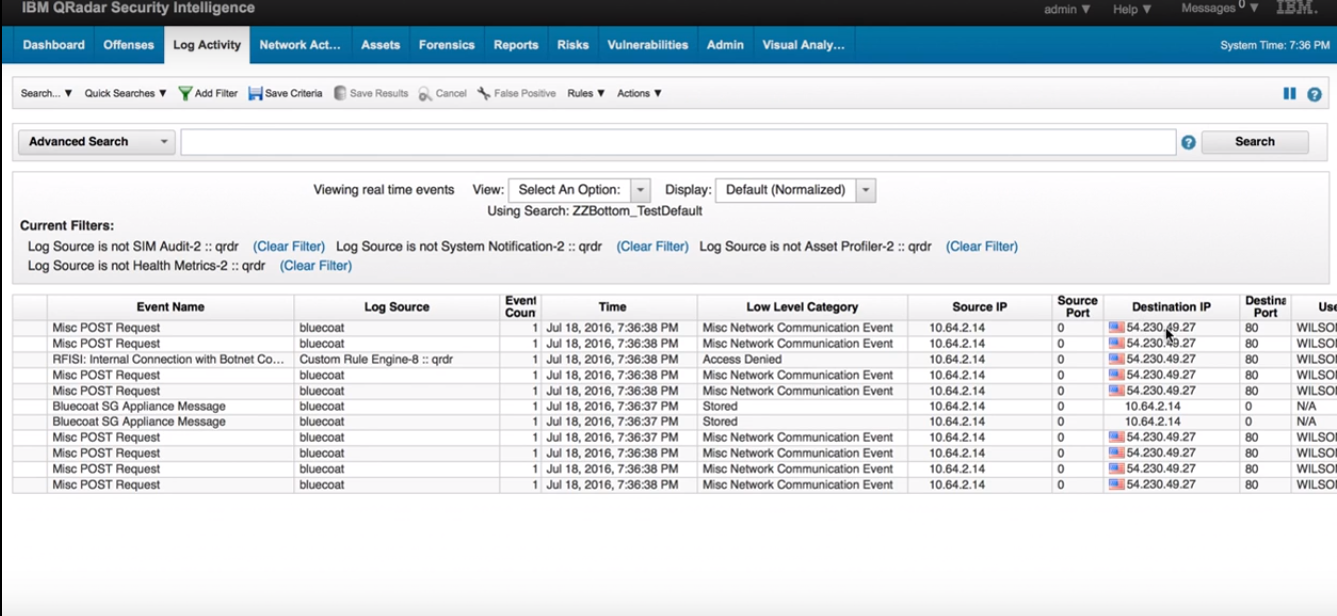
The main screen of the QRadar consists of different sections like Dashboard, offences, log activity, network activity, forensics, reports, risks, vulnerabilities, admin, visual analysis. To change the rules according to the needs, go to the admin section and by going to extension management and adding the required rules.

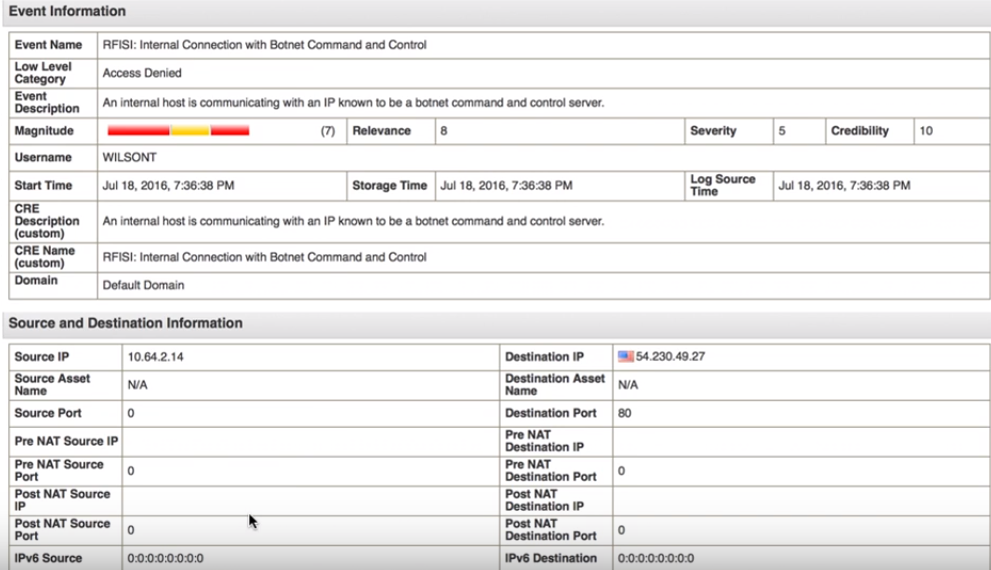


**Monitoring:**

There will be so many logs that are stored in the log activity. Manually searching the required event is not possible. Even if you find the required log the time taken will be in hours and even days in some cases. So using filters is the best option to do this. By applying filters required logs can be found easily. After finding the events, the details can be log sources, event count, time, low level category, Source IP, Source Port, Destination IP, Destination Port and other details can be found.

By clicking the events individually detailed information for them are known. Details like Event name, low level category, event description, magnitude, event name, start time, storage time, log source, domain and details of the source and destination can also be found.



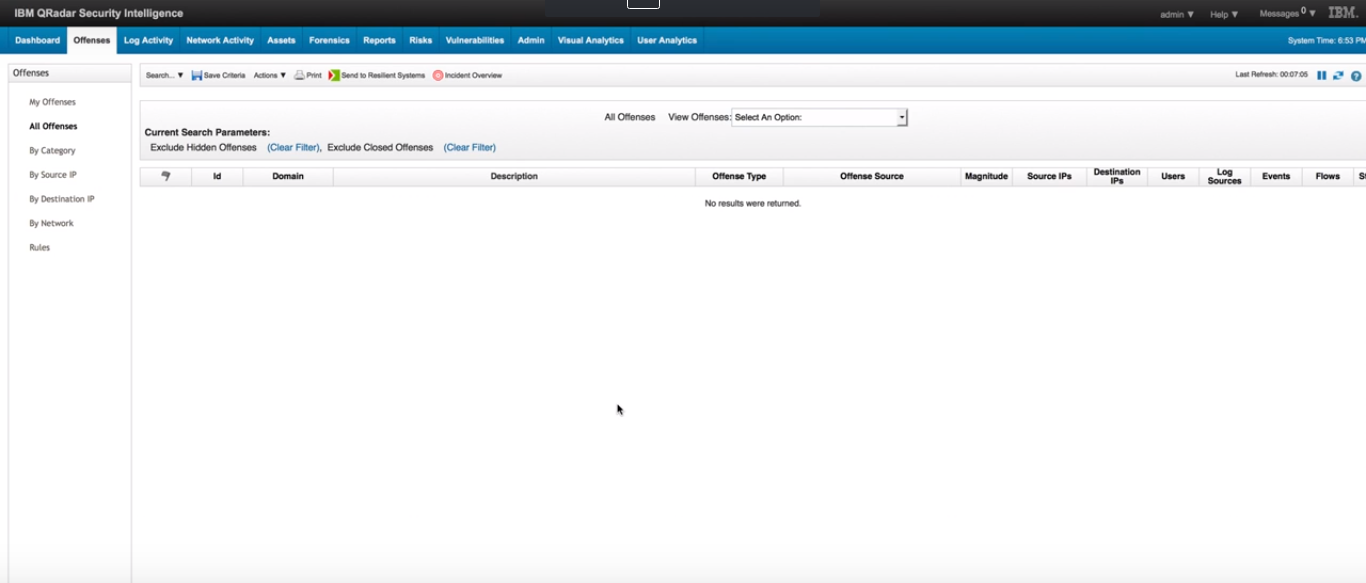


**Use case #4: Detecting Remote Scans**

Every network is vulnerable if their ports are open and there is a chance for the network to get compromised by the attackers. To perform the attacks, the remote scan is needed. To monitor these kinds of activities, the QRadar is an option to consider. Other than QRadar there are different tools available to do this job, but here we are taking this as an example.

**Overview:**

Defining a rule is the important task in order to perform an action. Without defining the rules, the machine cannot do anything. So initially the offences tab where the information has to be shown will be empty. By going to the admin section, then select the network hierarchy and go to the DMZ where the external server is present. That is the remote server which is scanned in order to perform the attack. Rules like multiple login failures to the same destination from the same source, remote access from the foreign country region, DMZ host port scan detected by foreign host is defined to obtain the required output.

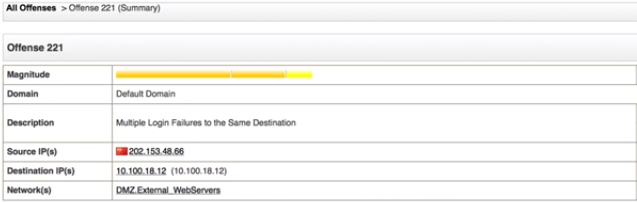


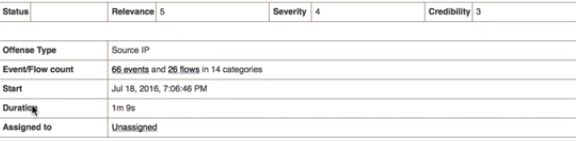




**Offences**:

Based on the rules that are defined the correlation is done on the log data and the output is shown in the offenses section. Here the ID of the activity, domain, description, offence type, offence source, magnitude, source and destination IP’s, users, log sources, events, flows and other details are also known. By selecting a particular activity magnitude of the attack, domain of it, description of the attack, network, status, relevance, severity of the attack is also shown.



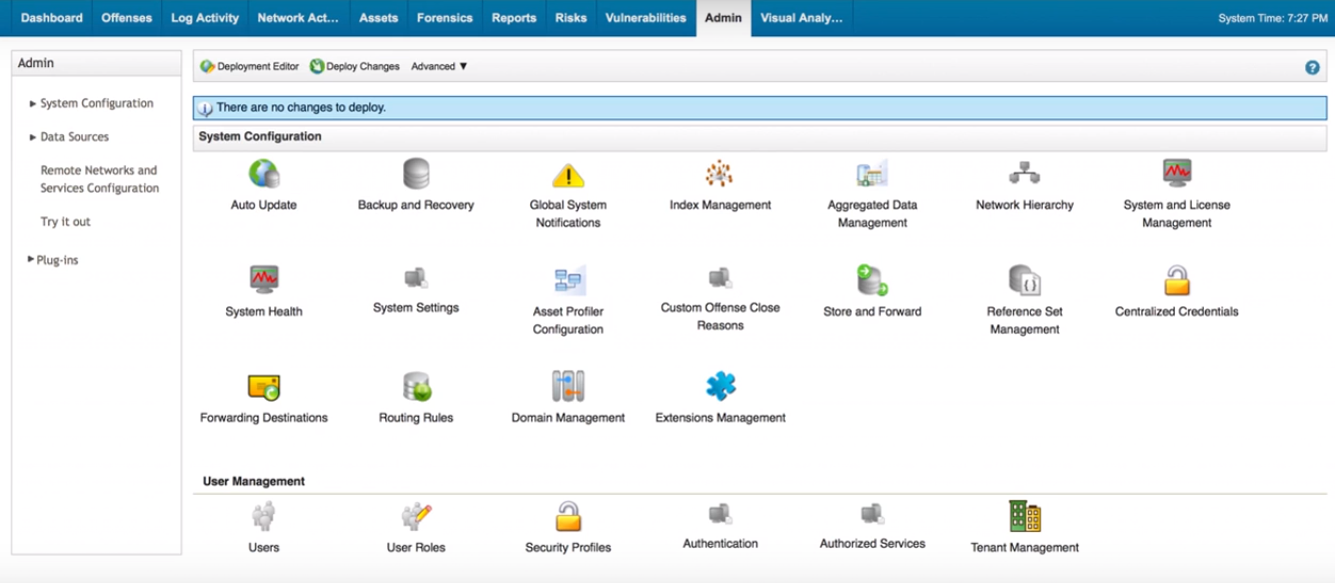


**Use case #5: Detecting Internal Communication to a Command& Control Site**

Generally, in a network there will be a proxy from which the connections to the internet is made. The logs that are created will store the information of the event that is happened. In this process the insiders may try to connect to the malicious site through the proxy which will not basically fire an alarm. The command and control sites or malicious sites could affect the system which is visiting it with ransomware or rootkits. So defining rules is important and it can be made such that these events can also be stored as logs.

**Overview**:

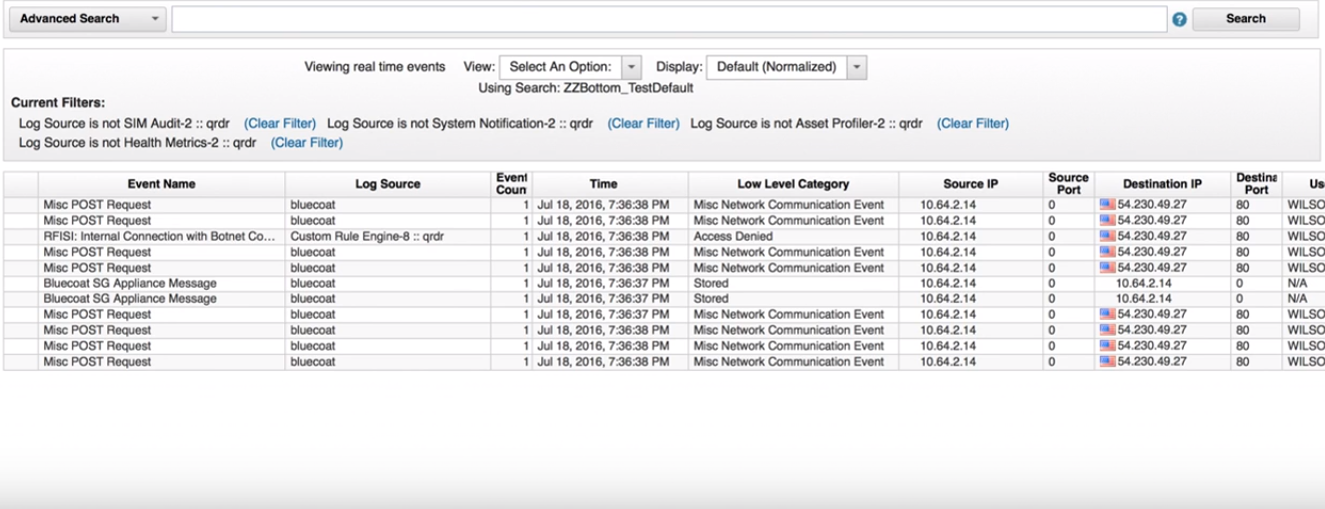
In the opening screen the dashboard, offences, log activity, network activity and many other sections will be seen. By going into the admin section, you have to click the extension management to add the rule. In the extension management there are different rules available you have to select the IBM Security App exchange where all the rules are available in a list. Then IBM Security RFISI Content is to be downloaded and added. In the same way IBM Threat Intelligence is to be downloaded and added. By downloading these two there will be no need to write a code.

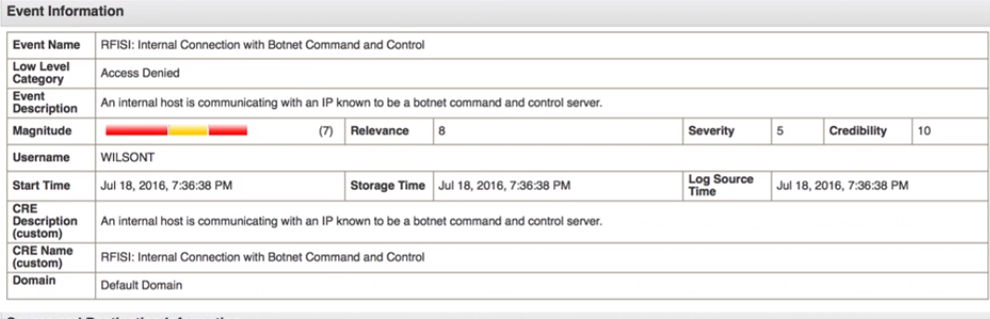




**Monitoring**:

In order to monitor the logs of the network check the log activity section. There all the events that are happening in the network is shown. By applying the filters of the rules that are defined the required output will be shown. For further analysis, click the suspicious activity. Here detailed information like event name, low level category, magnitude of the attack, relevance, credibility, severity, username, start time, storage time and many other details are known.





**Use case #6: User Activity Monitoring - Employee Probation**

Every company recruit new employees every year. All of them may not be good. Some of them may perform insider attacks or preform data exfiltration which will lead to the breach of the data. So monitoring the user activity is important. In order to do this QRadar is taken as an example. This use case helps to understand the actual situation if happens in an organization.

**Overview:**

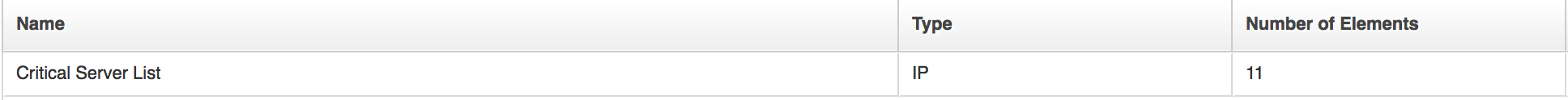
The initial details which are available while applying the rule is the name of the event, type, number of elements. There will be a table where value of the value of the events where the information like test user, demo user etc., will be seen, in the row of the origin information like new employee probation parts will be seen, another row called Time to Live is present the time to live period is the probation period of the employee. All this information is shown in the log activity section by applying “user activity: data exfiltration” rule.

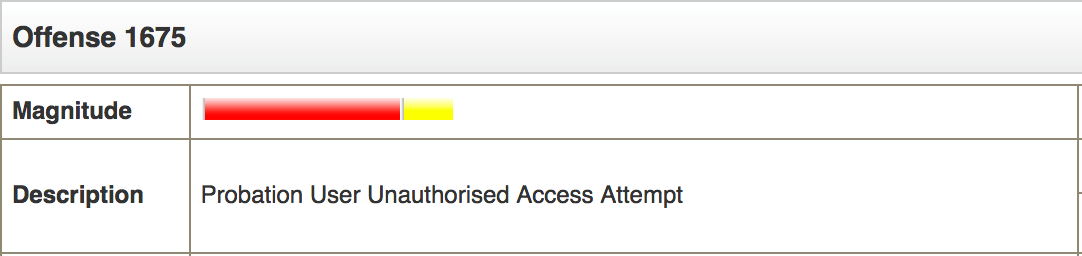




**Detailed View:**

Once the list with the details of the employee information is added as reference, the launch of the monitoring is done. After starting the monitoring, the if an employee tries to perform the exfiltration activity, an alarm is fired. In that the details like the source and destination IPs, name of the employee, start and end time of the connection, severity of the situation, magnitude of the attack, description and other details are found.





**Use case #7: Data Exfiltration Attempt through Online Storage**

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. The data exfiltration not only takes place on the storage devices but also on the cloud storages like google drive, dropbox etc., If the connection is made to the online storage those logs have to be logged. This can be done by many tools but here QRadar is taken as an example.

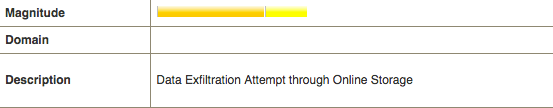
**Overview**:

The initial details which are available while applying the rule is the name of the event, type, number of elements. There will be a table where value of the events, number of elements, destination and other information will be seen. All this information is shown in the log activity section by applying “user activity: data exfiltration” rule.



**Detailed View:**

Based on the rules that are defined the correlation is done on the log data and the output is shown in the offenses section. Here the ID of the activity, domain, description, offence type, offence source, magnitude, source and destination IP’s, users, log sources, events, flows and other details are also known. In the picture shown below only few details are shown but by selecting a particular activity magnitude of the attack, domain of it, description of the attack, network, status, relevance, severity of the attack is also shown.



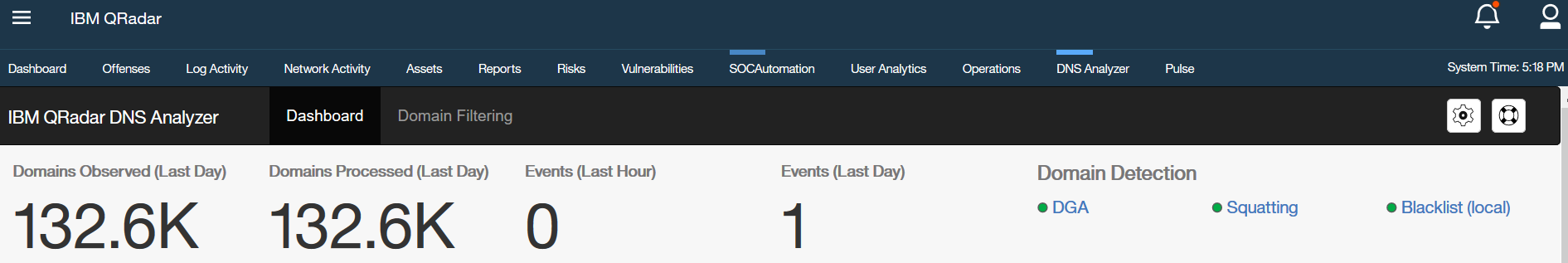
**Use case #8: Performing DNS Analysis**

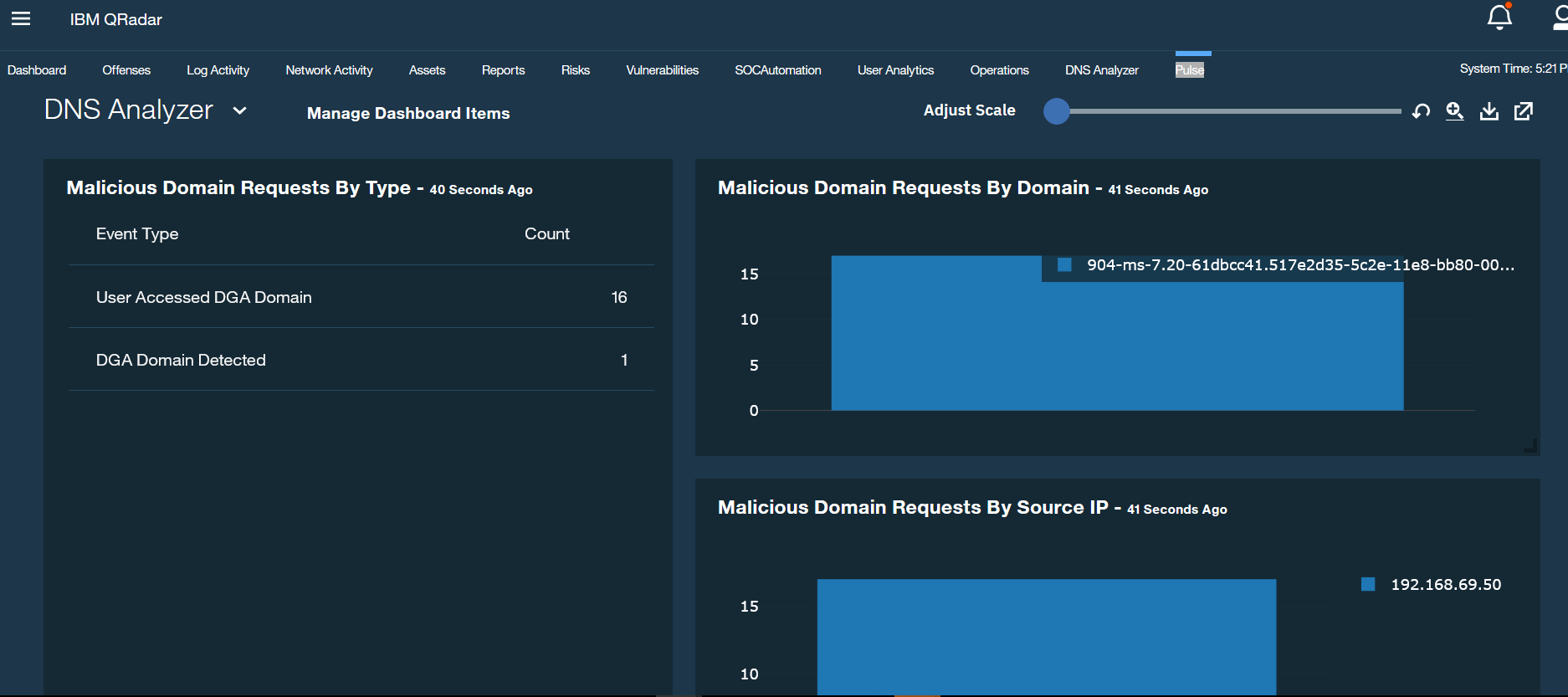
Data analytics id the analysis or collection of information of the DNS servers in a network. This is used to identify the threats and vulnerabilities of the network. Performing the DNS analysis is an important task. To do this there are different tools available. But here we are taking IBM QRadar DNS Analyzer as an example.

**Overview**:

The dashboard of the DNS Analyzer consists of overall number of domains observed, domains processed, events recorded in the last hour, last day and other details. There are separate sections for offences, log activity, network activity, reports, rules, vulnerabilities etc.,

In the DNS analyzer Managing the dashboard items is present. By using this the scale can be adjusted by which Malicious Domains by requests by domain, source IP’s graphs will be shown. This gives an overview of the network. The event type, user accessed domain, domain type can also be found out.



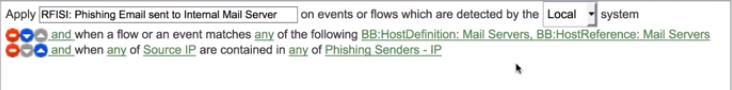


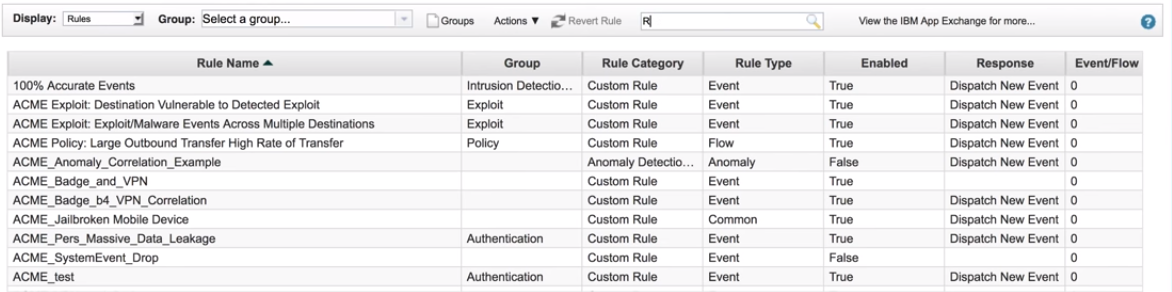
**Use case #9: Detecting Phishing Emails**

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 details like favorite sport, favorite place etc., are gathered. Then emails are sent based on the preferences of the victim like tickets to the game he likes or free tickets to his favorite sport etc., Those emails are linked with malicious links which install ransomware once they are installed. If that employee clicks that email, then the whole network of the organization can be compromised. So monitoring of emails is necessary. Here QRadar is take as an example to perform this task.

**Overview**:

Generally, the dash board of the QRadar consists of different sections. There are some predefined rules in the QRadar in the initial stage itself which are used to detect and monitor activities that are going on in the network. In order to perform the specified task like, detecting multiple login failures to compliance servers, new rule has to be defined. By clicking the Admin and by logging in new rules can be added and can also be modified. Here the rule of RFISI: Phishing Email sent to Internal Mail Server is to be defined so that it collects the events that are performed against this rule.



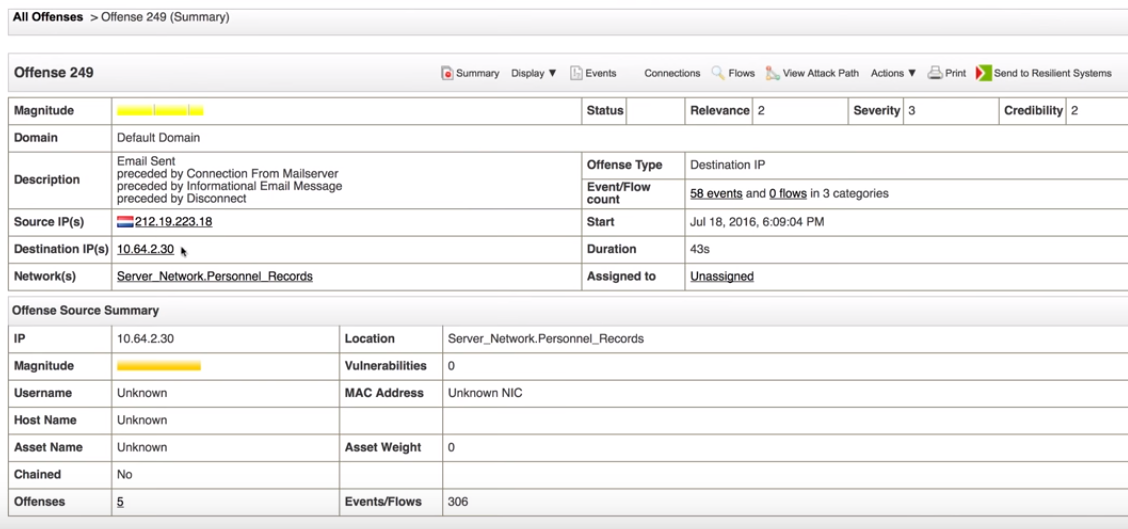


**Offences**:

As the required rules are defined, the required details are shown in the offences tab. As there are different rules predefined, huge number of logs are shown. To see the desired logs, filters are to be applied. After the application of the filters using search parameter, details like domain name, description of the event, source of the offence, type of the offence etc., are listed.

By selecting the specific event, in-depth information of it will be revealed. Information like the magnitude of the attack, count of time that this has occurred, start time of the attack, total duration, offence source summary, IP address, vulnerabilities, count of the events/flows and other details can be known.



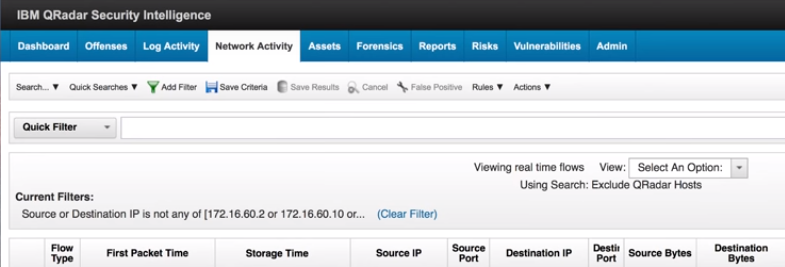


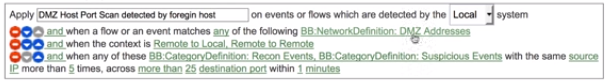
**Use case #10: Detecting DDoS attacks and Superflows**

There are different types of attacks that can be performed on the system. DDoS attacks are one of them. DDoS attacks are performed by taking control over hundreds of systems using Trojans and use them as zombies to attack a single system or a server. They will send data packets continuously to make the system or server malfunction. Superflows are same kind of issues where the systems from different locations are taken into control and made to perform this DDoS. So detecting these kinds of attacks is important. In order to do this task, QRadar is taken as an example here.

**Overview**:

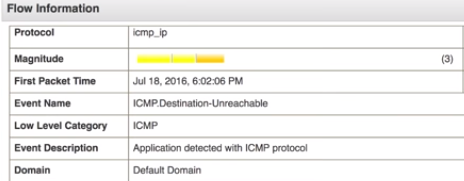
No rules are defined at the initial stages to perform these tasks. So even after applying the filters to search for the particular logs they will not appear. So defining the rules is the next step. The rule “DMZ port scan detected by foreign host” is to be defined to make the required logs noted. The events or flows are detected by the local system.

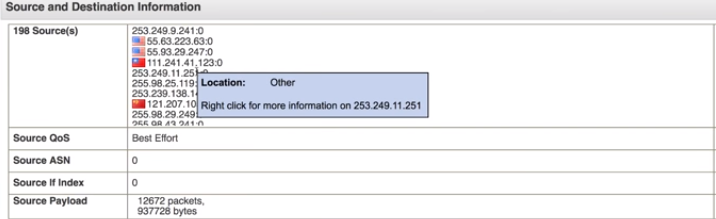




**Network Activity:**

The events or flows that are happening in the network can be seen in the network activity. If any particular offence is occurred against the rules, then those events are noted in the Offence section. There all the events that are happening in the network is shown. By applying the filters of the rules that are defined then, only particular output will be shown. For further analysis, click the activity which seems suspicious. The details for the superflows can also be seen here.



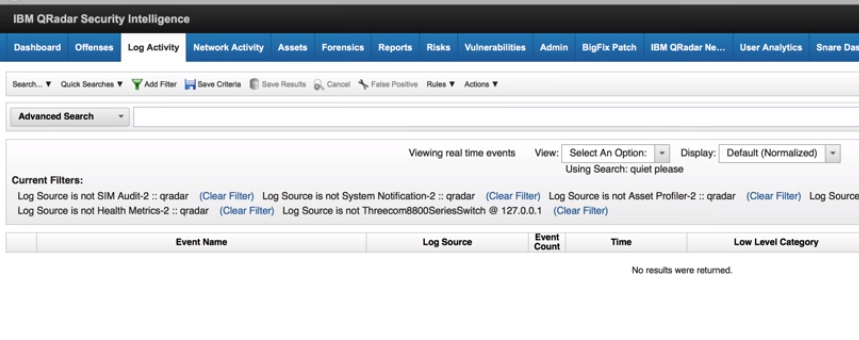


**Use case #11: Detecting insertion of USB by an insider and visiting a Restricted Site**

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. On the other hand, visiting social media sites, online shopping at the time of work is restricted. So, in order to detect the insertion of the USB in an organization and to monitor visiting of restricted sites, there are different tools available. Here QRadar is uses as an example to perform these tasks.

**Overview**:

The initial details which are available while applying the rule is the name of the event, type, number of elements. There will be a table where value of the events, number of elements, destination and other information will be seen. All this information is shown in the log activity section by applying “Insider Threat: USB and restricted Site” rule. Without defining the rules require information will not be seen.



**Offences**:

Based on the rules that are defined the correlation is done on the log data and the output is shown in the offenses section. Here the ID of the activity, domain, description, offence type, offence source, magnitude, source and destination IP’s, users, log sources, events, flows and other details are also known. By selecting a particular activity magnitude of the attack, domain of it, description of the attack, network, status, relevance, severity of the attack is also shown.

