

A REPORT OF SIX-MONTH TRAINING

at

SAFEAEON INC., MOHALI

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE  
AWARD

OF THE DEGREE OF

**BACHELOR OF TECHNOLOGY**

(Computer Science & Engineering)



January 2023 to June 2023

Submitted By:

Arshdeep Singh (2004693)

Submitted To:

Prof. Priyanka Arora

Prof. Kapil Sharma

Training Coordinators

CSE Department

Department of Computer Science & Engineering

**Guru Nanak Dev Engineering College** Ludhiana,

141006

---

## SafeAeon Inc.

6701, Koll Center Parkway, Suite 250,  
Pleasanton, California 94566, USA.



### TO WHOM IT MAY CONCERN

This is to certify that Mr. Arshdeep Singh, S/O Mr. Harpreet Singh student of the Department of Computer Science and Engineering, Guru Nanak Dev Engineering College, Ludhiana, having Reg no- 2004693, has started an internship as a SOC Analyst from January 09, 2023, to till date under the guidance of the Senior team.

During his internship, he was exposed to different processes and was diligent, hardworking, and inquisitive.

We wish him a bright future.

Sincerely,

Date: June 01, 2023

A handwritten signature in blue ink, appearing to read 'Gurwinder Singh'.

Gurwinder Singh

Director of Talent Acquisition, SafeAeon Inc.

## **CANDIDATE’S DECLEARATION**

I **“ARSHDEEP SINGH”** hereby declare that I have undertaken six month training at **“SafeAeon Inc., Mohali”** during a period from January,2023 to June,2023 in partial fulfilment of requirement for the award of degree of B.Tech (Computer Science & Engineering) at GURU NANAK DEV ENGINEERING COLLEGE, LUDHIANA. The work which is being presented in the training report submitted to Department of Computer Science & Engineering at GURU NANAK DEV ENGINEERING COLLEGE, LUDHIANA is an authentic record of training work.

Signature of Student

The six-month industrial training Viva-Voce Examination of \_\_\_\_\_ has been held on \_\_\_\_\_ and accepted.

## ABSTRACT

As a result of signing a non-disclosure agreement with the corporation, We are unable to reveal the project's technical details.

However, We gained knowledge about current industry technology. We learned about the SIEM (Security Information and Event Management) and EDR (End point detection response) and had hand of experience.

**Security Information and Event Management (SIEM)** is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure.

SIEM collects security data from network devices, servers, domain controllers, and more. SIEM stores, normalizes, aggregates, and applies analytics to that data to discover trends, detect threats, and enable organizations to investigate any alerts.

There are different tools for SIEM, the one on which we have worked upon is **IBM QRADAR**.

**EDR** software works by collecting log and event data that is generated by host systems, security devices and applications throughout an organization's infrastructure and collating it on a centralized platform. Using EDR, the threat hunters work proactively to hunt, investigate, and advise on threat activity in your environment. When they find a threat, they work alongside your team to triage, investigate and remediate the incident, before it has the chance to become a full-blown breach.

There are different tools for EDR, the one on which we have worked upon is **SentinelOne**.

## ACKNOWLEDGEMENT

We are highly grateful to **Dr. Sehijpal Singh**, Principal of Guru Nanak Dev Engineering College, Ludhiana and from **Dr. Parminder Singh**, Head of Department CSE for providing this opportunity to carry out the six-month industrial training.

We would like to express our gratitude to other faculty members, for providing academic inputs, guidance & encouragement throughout the training period.

The internship opportunity we had with **SafeAeon Inc.** was a great chance for learning and professional development. Therefore, we consider ourselves as very lucky individuals as we were provided with an opportunity to be a part of it.

We express our deepest gratitude and special thanks to the MD of SafeAeon Inc. **Mr. Gurwinder Singh** who despite being extraordinarily busy with his duties, took time out to hear guide and keep us on the correct path and allowing us to carry out our project at their esteemed organization and extending during the training.

We express our deepest thanks to all Team Leads for taking part in useful decision & giving necessary advice and guidance and arranged all facilities to make project easier.

We are grateful to all the Senior Analyst of each shift their careful and precious guidance which were extremely valuable for our study both theoretically and practically. We perceive as this opportunity as a big milestone in our career development.

## **ABOUT THE COMPANY**

SafeAeon is a Managed Cyber security provider with its inhouse SOC. It is US Silicon Valleybased company and provide US, UK, Canada and a Global based SOC as-a-Service offering.

SafeAeon's 24×7 Security Teams work around the clock to monitor, detect, and respond to cyberattacks before they have the chance to impact your business. SafeAeon is your ArmoredSecurity Shield. Their highly trained, certified, and expert team providing exceptional services at an affordable price like never seen before. Enlist SafeAeon's security experts to help you achieve true digital resilience. Get the time advantage back so you can focus on your core competency. SafeAeon offers management and monitoring services for a wide array of security products from different vendors. It has in-house expertise of most of industry leading security vendor products available in the market.

### **SERVICES THEY OFFER:**

- Security incident and crisis
- Forensic Analysis
- Data Loss and Prevention (DLP)
- Database Audit and Monitoring (DAM)
- End point Detection and Prevention
- Next-Gen Firewalls

## List of Figures

Fig 2.1 General Overview of SIEM	5
Fig 2.2 Login page of IBM QRADAR	6
Fig 2.3 Dashboard tab in QRadar Console	8
Fig 2.4 Offense Tab	10
Fig 2.5 Offense summary page	13
Fig 2.6 Log Activity Tab	14
Fig 2.7 Network activity tab	15
Fig 2.8 Assets Tab	17
Fig 2.9 Reports Tab	18
Fig 2.10 Admin Tab	19
Fig 4.1 General Overview of SentinelOne	24
Fig 4.2 General Overview of EDR	24
Fig 4.3 Why we need EDR	25
Fig 4.4 Dashboard	27
Fig 4.5 Endpoints Tab	29
Fig 4.6 Selecting an offense to investigate	29

## Table of Contents

<b>Certificate</b>	<i>i</i>
<b>Candidate's Declaration</b>	<i>ii</i>
<b>Abstract</b>	<i>iii</i>
<b>Acknowledgement</b>	<i>iv</i>
<b>About The Company</b>	<i>v</i>
<b>List Of Figures</b>	<i>vi</i>
<b>Chapter 1: SIEM</b>	<b>1-4</b>
1. Security Information and Event Management	1
1.1 How Does a SIEM Works?	2
1.2 Why is SIEM Important?	2
1.3 Benefits of SIEM	3
1.4 Limitation of SIEM	3
1.5 SIEM Tools And Software	4
<b>Chapter 2: IBM Qradar</b>	<b>5-21</b>
2. IBM Qradar	5
2.1 Features of Qradar	5
2.2 Restful API	6
2.3 User Interface	6
2.4 Dashboard Tab	7
2.5 Custom Dashboard	7-8
2.5.1 Procedure	8
2.6. Offenses Tab	9
2.6.1 Offenses Prioritization	9-10
2.6.2 Offenses Chaining	10
2.6.3 Offense Indexing	11
2.6.4 Offense Retention	11
2.6.5 Offense Investigation	12-13
2.7 Log Activity Tab	14
2.7.1 Log Activity Tab Toolbar	14
2.8 Network Activity Tab	15
2.9 Assets Tab	16
2.9.1 Asset Data	16
2.9.2 Asset Profile	16-17
2.10 Reports Tab	18
2.10.1 Report Layout	18
2.11 Admin Tab	19
2.12 How Qradar SIEM Collects Security Data	20



2.12.1 Event Collection and Processing	20
2.13 Rules	21
2.13.1 What are Rules?	21
2.13.2 What are building blocks?	21
2.13.3 How Do rules Works?	21
<b>Chapter 3: EDR</b>	<b>22-23</b>
3.1 EDR	22
3.2 How Does EDR Work?	22-23
3.3 Benefits of Using EDR	23
<b>Chapter 4: SentinelOne</b>	<b>24-29</b>
4.1 SentinelOne	24
4.2 Key Features	25
4.3 EDR capabilities	26
4.4 EDR Dashboard	26-27
4.5 How EDR collects security data	28-29
<b>CONCULSION</b>	<b>30</b>
<b>FUTURE SCOPE</b>	<b>31</b>
<b>REFRENCES</b>	<b>32</b>

## **CHAPTER 1: SIEM**

### **1. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)**

Security information and event management (SIEM) is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system. The acronym SIEM is pronounced "sim" with a silent e.

The underlying principles of every SIEM system is to aggregate relevant data from multiple sources, identify deviations from the norm and take appropriate action. For example, when a potential issue is detected, a SIEM system might log additional information, generate an alert, and instruct other security controls to stop an activity's progress.

At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event log entries. Advanced SIEM systems have evolved to include user and entity behaviour analytics (UEBA) and security orchestration, automation and response (SOAR).

Payment Card Industry Data Security Standard (PCI DSS) compliance originally drove SIEM adoption in large enterprises, but concerns over advanced persistent threats (APTs) have led smaller organizations to look at the benefits SIEM managed security service providers (MSSPs) can offer. Being able to look at all security-related data from a single point of view makes it easier for organizations of all sizes to spot patterns that are out of the ordinary.

SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers and network equipment, as well as specialized security equipment, such as firewalls, antivirus or intrusion prevention systems (IPSeS). The collectors' forward events to a centralized management console, where security analysts sift through the noise, connecting the dots and prioritizing security incidents.

In some systems, pre-processing may happen at edge collectors, with only certain events being passed through to a centralized management node. In this way, the volume of information being communicated and stored can be reduced. Although advancements in

machine learning are helping systems to flag anomalies more accurately, analysts must still provide feedback, continuously educating the system about the environment.

## **1.1 HOW DOES A SIEM WORKS?**

SIEM tools work by gathering event and log data created by host systems, applications and security devices, such as antivirus filters and firewalls, throughout a company's infrastructure and bringing that data together on a centralized platform.

The SIEM tools identify and sort the data into such categories as successful and failed logins, malware activity and other likely malicious activity. The SIEM software then generates security alerts when it identifies potential security issues. Using a set of predefined rules, organizations can set these alerts as low or high priority.

For instance, a user account that generates 25 failed login attempts in 25 minutes could be flagged as suspicious but still be set at a lower priority because the login attempts were probably made by the user who had probably forgotten his login information. However, a user account that generates 130 failed login attempts in five minutes would be flagged as a high-priority event because it's most likely a brute-force attack in progress.

## **1.2 WHY IS SIEM IMPORTANT?**

SIEM is important because it makes it easier for enterprises to manage security by filtering massive amounts of security data and prioritizing the security alerts the software generates. SIEM software enables organizations to detect incidents that may otherwise go undetected. The software analyses the log entries to identify signs of malicious activity. In addition, since the system gathers events from different sources across the network, it can recreate the timeline of an attack, enabling a company to determine the nature of the attack and its impact on the business.

A SIEM system can also help an organization meet compliance requirements by automatically generating reports that include all the logged security events among these sources. Without SIEM software, the company would have to gather log data and compile the reports manually.

A SIEM system also enhances incident management by enabling the company's security team to uncover the route an attack takes across the network, identify the sources that were compromised and provide the automated tools to prevent the attacks in progress.

### **1.3 BENEFITS OF SIEM**

Some of the benefits of SIEM include the following:

- shortens the time it takes to identify threats significantly, minimizing the damage from those threats;
- offers a holistic view of an organization's information security environment, making it easier to gather and analyze security information to keep systems safe -- all of an organization's data goes into a centralized repository where it is stored and easily accessible;
- can be used by companies for a variety of use cases that revolve around data or logs, including security programs, audit and compliance reporting, help desk and network troubleshooting;
- supports large amounts of data so organizations can continue to scale out and increase their data;
- provides threat detection and security alerts; and
- can perform detailed forensic analysis in the event of major security breaches.

### **1.4 LIMITATIONS OF SIEM**

Despite its benefits, there are still some limitations of SIEM, including the following:

- Usually, it takes a long time to implement because it requires support to ensure successful integration with an organization's security controls and the many hosts in its infrastructure. It typically takes 90 days or longer to install SIEM before it starts to work.
- It's expensive. The initial investment in SIEM can be in the hundreds of thousands of dollars. And the associated costs can also add up, including the costs of personnel to manage and monitor a SIEM implementation, annual support, and software or agents to collect data.
- Analyzing, configuring and integrating reports require the talent of experts. That's why some SIEM systems are managed directly within a security operations center (SOC)

## 1.5 SIEM TOOLS AND SOFTWARE

Some of the tools in the SIEM space include the following:

- **Splunk** Splunk is a full on-premises SIEM system. Splunk supports security monitoring and offers advanced threat detection capabilities
- **IBM QRadar**. QRadar can be deployed as a hardware appliance, a virtual appliance or a software appliance, depending on a company's needs and capacity. QRadar on Cloud is a cloud service delivered from IBM Cloud based on the QRadar SIEM product.
- **LogRhythm**. LogRhythm, a good SIEM system for smaller organizations, unifies SIEM, log management, network and endpoint monitoring and forensics, and security analytics.
- **Exabeam**. Exabeam's SIEM product offers several capabilities, including UEBA, a data lake, advanced analytics and a threat hunter.
- **RSA**. RSA NetWitness Platform is a threat detection and response tool that includes data acquisition, forwarding, storage and analysis. RSA also offers SOAR

## CHAPTER 2: IBM QRADAR

### 2. IBM QRADAR

QRadar is a security information and event management or SIEM product that is designed for enterprises. The tool collects data from the organization and the network devices. It also connects to the operating systems, host assets, applications, vulnerabilities, user activities, and behaviors.

IBM QRadar is used to perform analysis of the log data and the network flows in real time so that malicious activities can be identified and stopped as soon as possible. Thus, the main aim of the IBM QRadar is to prevent or minimize the damage to its host organization.

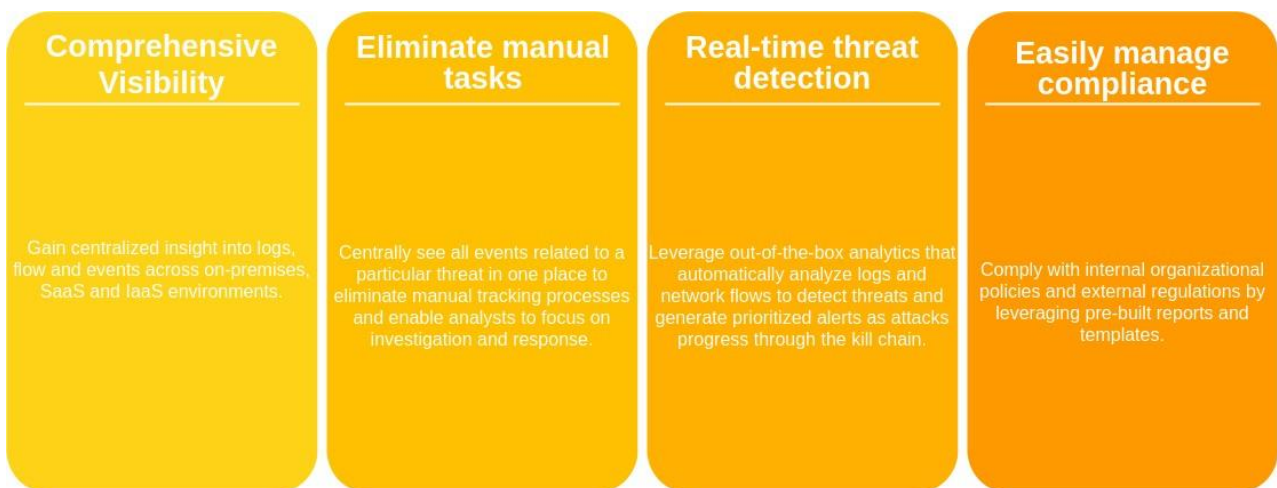


Figure 2.1 General Overview of SIEM

#### 2.1 Features of QRadar

There are many different tools under IBM Q-Radar that aid in the data processing. The important ones are:

- **IBM Q-Radar Vulnerability Manager:** This tool is used to scan the process and network vulnerability data. This data is then utilized to recognize the security risks in the network.
- **IBM Q-Radar Risk Manager:** This tool is used to collect the network infrastructure configuration and issue a draft of the network topology. The data can be practiced to control risk by the simulation of network situations by executing rules and modifying the configurations in the network.

## 2.2 RESTFUL API

The representational state transfer (REST) application programming interface (API) is useful when you want to integrate IBM QRadar with other solutions. You can perform actions on the QRadar Console by sending HTTPS requests to specific endpoints (URLs) on the QRadar Console.

Each endpoint contains the URL of the resource that you want to access and the action that you want to complete on that resource. The action is indicated by the HTTP method of the request: GET, POST, PUT, or DELETE.



Figure 2.2 Login page of IBM QRADAR

## 2.3 USER INTERFACE TABS

Functionality is divided into tabs. The Dashboard tab is displayed when we log in. We can easily navigate the tabs to locate the data or functionality you require.

- **Dashboard:** The initial summary view.
- **Offenses:** Displays offenses; list of prioritized incidents.
- **Log Activity:** Query and display events.
- **Network Activity:** Query and display flows.
- **Assets:** Query and display information about systems in your network.
- **Reports:** Create templates and generate reports.
- **Admin:** Administrative system management.



## 2.4 DASHBOARD TAB

The Dashboard tab is a workspace environment that provides summary and detailed information on events occurring in your network.

The Dashboard tab supports multiple dashboards where you can display your views of networksecurity, activity, or data that QRadar collects.

The Dashboard tab provides five default dashboards that are focused on security, network activity, application activity, system monitoring, and compliance. Each dashboard displays a default set of dashboard items. The dashboard items act as starting point to navigate to more detailed data.

We can also create a custom dashboard to focus on your security or network operations responsibilities.

The following table defines the default dashboards:

- Application Overview
- Compliance Overview
- Network Overview
- System Monitoring
- Threat and Security Monitoring

## 2.5 Custom Dashboard

We can customize your dashboards. The content that is displayed on the Dashboard tab is user-specific. Changes that are made within a QRadar session affect only your system. To customize our Dashboard tab, we can perform the following tasks:

- Create custom dashboards that are relevant to your responsibilities. 255 dashboards per user is the maximum; however, performance issues might occur if you create more than 10 dashboards.
- Add and remove dashboard items from default or custom dashboards.
- Move and position items to meet your requirements. When you position items, each item automatically resizes in proportion to the dashboard.
- Add custom dashboard items that are based on any data. For example, you can add a dashboard item that provides a time series graph or a bar chart that represents top 10 network activity.

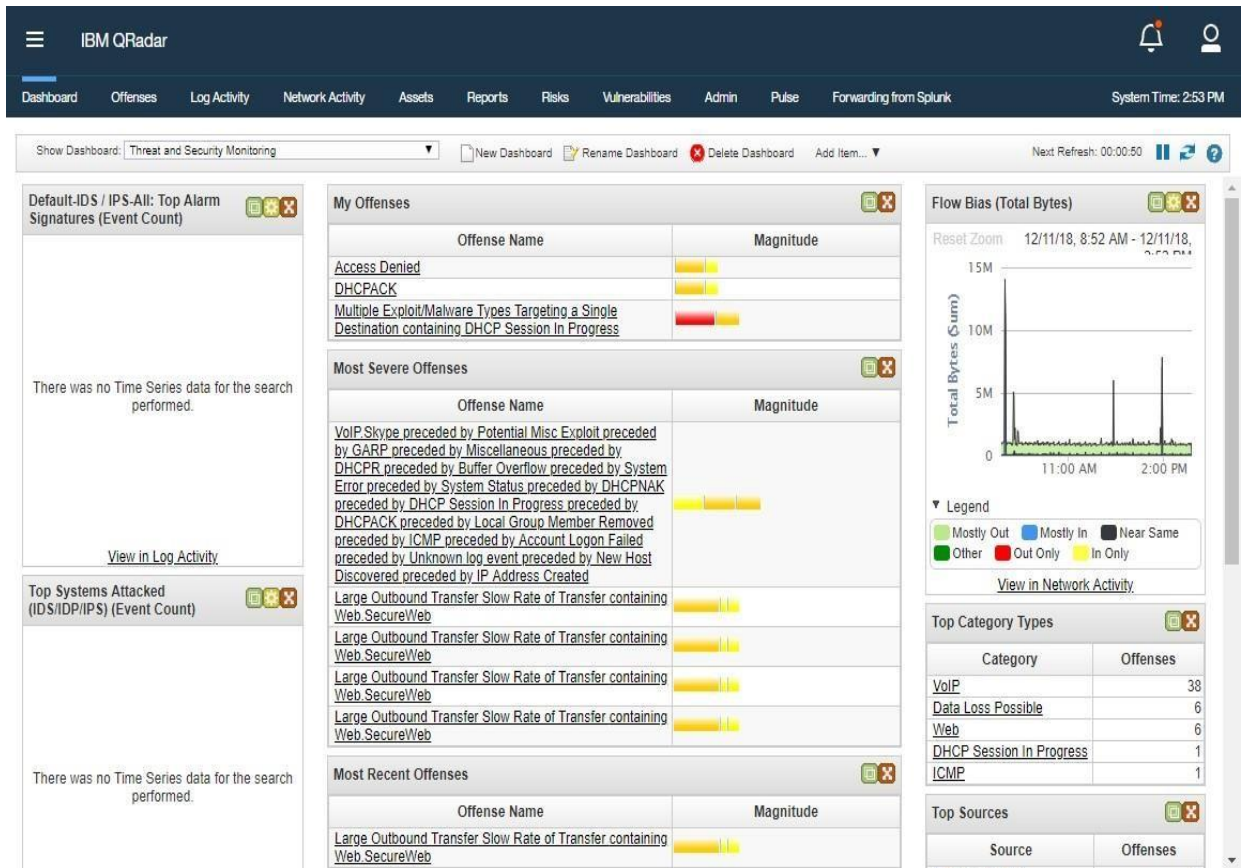


Figure 2.3 Dashboard tab in QRadar Console

## 2.5.1 Procedure

1. Click the Dashboard tab.
2. Click the New Dashboard icon.
3. In the Name field, type a unique name for the dashboard. The maximum length is 65 characters.
4. In the Description field, type a description of the dashboard. The maximum length is 1024 characters. This description is displayed in the tooltip for the dashboard name in the Show Dashboard list box.
5. Click OK.

## 2.6 OFFENCES TAB

IBM QRadar reduces billions of events and flows into a manageable number of actionable offenses that are prioritized by their impact on your business operations. Use the Offenses tab to access all of the data that you need to understand even the most complex threats.

By providing immediate context for the offense, QRadar helps you to quickly identify which offenses are the most important, and to begin an investigation to find the source of the suspected security attack or policy breach.

### 2.6.1 Offence Prioritization

The magnitude rating of an offense is a measure of the importance of the offense in your environment. IBM QRadar uses the magnitude rating to prioritize offenses and help you to determine which offenses to investigate first. The magnitude rating of an offense is calculated based on relevance, severity, and credibility.

- **Relevance** determines the impact of the offense on your network. For example, if a port is open, the relevance is high.
- **Credibility** indicates the integrity of the offense as determined by the credibility rating that is configured in the log source. Credibility increases as multiple sources report the same event.
- **Severity** indicates the level of threat that a source poses in relation to how prepared the destination is for the attack.

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs
2	VoIP/Skype preceded by Potential Misc Exploit preceded by GARP...	Rule	AAA Offense Indexin...		Multiple (3)	Multiple (64)
135	Large Outbound Transfer Slow Rate of Transfer containing Web...	Source IP	172.16.88.245		172.16.88.245	Remote (2)
131	Large Outbound Transfer Slow Rate of Transfer containing Web...	Source IP	172.16.89.221		172.16.89.221	Remote (2)
132	Large Outbound Transfer Slow Rate of Transfer containing Web...	Source IP	172.16.89.134		172.16.89.134	Remote (3)
133	Large Outbound Transfer Slow Rate of Transfer containing Web...	Source IP	172.16.89.185		172.16.89.185	Remote (2)
134	Large Outbound Transfer Slow Rate of Transfer containing Web...	Source IP	172.16.89.151		172.16.89.151	Remote (2)
21	Multiple Exploit/Malware Types Targeting a Single Destination co...	Source Port	0		Multiple (39)	Multiple (31)
73	IP	Event Name	IP			
87	MEM	Event Name	MEM			
93	GARP	Event Name	GARP			
174	Large Outbound Transfer Slow Rate of Transfer containing Web...	Source IP	172.16.88.33		172.16.88.33	
11	Multiple Exploit/Malware Types Targeting a Single Destination co...	Source IP	192.168.0.1		192.168.0.1	
1	IP Address Created	Destination IP	127.0.0.1		Multiple (4)	127.0.0.1
74	SOCKET	Event Name	SOCKET		192.168.0.1	
82	DHCPD	Event Name	DHCPD			
100	MSTP_ERROR	Event Name	MSTP_ERROR			
110	VTY	Event Name	VTY		Multiple (2)	
117	Multiple Exploit/Malware Types Targeting a Single Destination	Event Name	Multiple Exploit/Mal...		192.168.0.1	
7	Multiple Exploit/Malware Types Targeting a Single Destination co...	Destination IP			Multiple (39)	
9	Successful Network Logon	Source Port	25		192.168.0.1	
10	Successful Network Logon	Username	admin1000M		192.168.0.1	

Figure 2.4 Offense Tab

## 2.6.2 Offense chaining

IBM QRadar chains offenses together to reduce the number of offenses that you need to review, which reduces the time to investigate and remediate the threat. Offense chaining helps you find the root cause of a problem by connecting multiple symptoms together and showing them in a single offense.

By understanding how an offense changed over time, you can see things that might be overlooked during your analysis. Some events that would not be worth investigating on their own might suddenly be of interest when they are correlated with other events to show a pattern. Offense chaining is based on the offense index field that is specified on the rule.

For example, if your rule is configured to use the source IP address as the offense index field, there is only one offense that has that source IP address for while the offense is active.

### 2.6.3 Offense indexing

Offense indexing provides the capability to group events or flows from different rules indexed on the same property together in a single offense. IBM QRadar uses the offense index parameter to determine which offenses to chain together.

For example, an offense that has only one source IP address and multiple destination IP addresses indicates that the threat has a single attacker and multiple victims. If you index this type of offense by the source IP address, all events and flows that originate from the same IP address are added to the same offense. You can configure rules to index an offense based on any piece of information.

QRadar includes a set of predefined, normalized fields that you can use to index your offenses. If the field that you want to index on is not included in the normalized fields, create a custom event or a custom flow property to extract the data from the payload and use it as the offense indexing field in your rule. The custom property that you index on can be based on a regular expression, a calculation, or an AQL-based expression.

### 2.6.4 Offense retention

The state of an offense determines how long IBM QRadar keeps the offense in the system. The offense retention period determines how long inactive and closed offenses are kept before they are removed from the QRadar console.

- **Active offenses:** When a rule triggers an offense, the offense is active. In this state, QRadar is waiting to evaluate new events or flows against the offense rule test. When new events are evaluated, the offense clock is reset to keep the offense active for another 30 minutes.
- **Dormant offenses:** An offense becomes dormant if new events or flows are not added to the offense within 30 minutes, or if QRadar did not process any events within 4 hours. An offense remains in a dormant state for 5 days. If an event is added while an offense is dormant, the five-day counter is reset.
- **Inactive offenses:** An offense becomes inactive after 5 days in a dormant state. In the inactive state, new events that trigger the offense rule test do not contribute to the inactive offense. They are added to a new offense. Inactive offenses are removed after the offense retention period elapses.

## 2.6.5 Offense Investigation

The **Offense Summary** window helps you begin your offense investigation by providing context to help you understand what happened and determine how to isolate and resolve the problem.

### Investigating an offense triggered by events

QRadar SIEM correlates events and flows into an offense, if it assumes suspicious activity.

- QRadar SIEMs prime benefit for security analysts is that it detects suspicious activities and ties them together into offenses.
- An offense represents a suspected attack or policy breach. Some common offenses include these examples:
  - Multiple login failures
  - Worm infection
  - P2P traffic
  - Scanner reconnaissance.

Some of the most common offenses that a typical security analyst investigates include:

- Clear Text Application Usage
- Remote Desktop Access from the Internet
- Connection to a remote proxy or anonymization service
- SSH or Telnet detected on Non-Standard Port
- Large Outbound Transfer
- Communication to a known Bot Command and Control
- Local IRC Server detected

## The sections of the Offense Summary window include:

- Offense Parameters
- Offense Source Summary
- Last 5 Notes
- Top 5 Source IPs
- Top 5 Destination IPs
- Top 5 Log Sources
- Top 5 Users

**Offense 31**

Summary | Display | Events | Connections | Flows | View Attack Path | Actions | Print

Magnitude		Status	Relevance	5	Severity	0	Credibility	3
Domain	Default Domain							
Description	Large Outbound Transfer Slow Rate of Transfer preceded by Large Outbound Transfer High Rate of Transfer containing unknown		Offense Type	Source IP				
Source IP(s)			Event/Flow count	58 events and 2				
Destination IP(s)			Start	Apr 13, 2016, 4:1				
Network(s)	other		Duration	4d 18h 18m				
			Assigned to	Unassigned				

**Offense Source Summary**

IP		Location	
Magnitude		Vulnerabilities	0
Username	Unknown	ress	Unknown NIC
Host Name	Unknown		
Asset Name			0
Offenses	1	Events/Flows	3,528

**Top 5 Source IPs**

Source IP	Magnitude	ser	own	Offenses	Destinati...	Last Event/Flow	Events/F
				0		1h 18m 15s	3,528

**Top 5 Destination IPs**

Destination IP	Magnitu...	Location	Vulnerability	Chained	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events/...
		Net...	No	No	Unknow	Unknc	0	6	7	3d 21h...	464

**Last 10 Events**

Event Name	Magnitude	Log Source	Category	Destinatio	Time
Authentication Fail...			SSH Login Failed		16, 2016, 4:55
Authentication Fail...			SSH Login Failed		Mar 16, 2016, 4:52
Authentication Fail...			SSH Login Failed		Mar 16, 2016, 4:56
Authentication Fail...			SSH Login Failed		Mar 16, 2016, 4:56
Authentication Fail...		LinuxServer @ qaf...	SSH Login Failed		Mar 16, 2016, 4:59
Authentication Fail...		LinuxServer @ qaf...	SSH Login Failed		Mar 16, 2016, 4:59
Root Login Failed		LinuxServer @ qaf...	Admin Login Failure		Mar 16, 2016, 4:58

**Top 5 Annotations**

Annotation

**Callout Questions:**

- What was the attack?
- Was it successful?
- Who was responsible?
- Where can I find them?
- How many targets are involved?
- Are the targets vulnerable?
- Where is the evidence?
- How valuable are the targets to the business?
- Why does QRadar consider the event threatening?

Figure 2.5 Offense summary page

## 2.7 LOG ACTIVITY TAB

Investigate event logs that are sent to QRadar in real-time, perform powerful searches, and view log activity by using configurable time-series charts. Use the Log Activity tab to perform in-depth investigations on event data.

An event is a record from a log source, such as a firewall or router device, that describes an action on a network or host. The Log Activity tab specifies which events are associated with offenses. You must have permission to view the Log Activity tab.

### 2.7.1 Log activity tab toolbar

We can access several options from the Log Activity toolbar Using the toolbar, we can accessthe following options:

- Search
- Quick Searches
- Add filter
- Save results
- Cancel
- False Positive
- Rules

IBM QRadar
System Time: 11:47 AM

---

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

**Quick Filter**  Search

Viewing real time events    View: Select An Option:    Display: Default (Normalized)

	Event Name	Log Source	Even Count	Time	Low Level Category	Source IP	Source Port	Destin
	User Login	SIM Audit-2 :: idd134	1	Dec 12, 2018, 11:47...	SIM User Authentication	172.16.89.134	0	172.16.
	User Login	SIM Audit-2 :: idd134	1	Dec 12, 2018, 11:47...	SIM User Authentication	172.16.89.134	0	172.16.
	Information Message	System Notification-2 :: idd134	1	Dec 12, 2018, 11:47...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.
	Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46...	Information	172.16.89.134	0	127.0.0.

Receiving an average of less than one result per second.

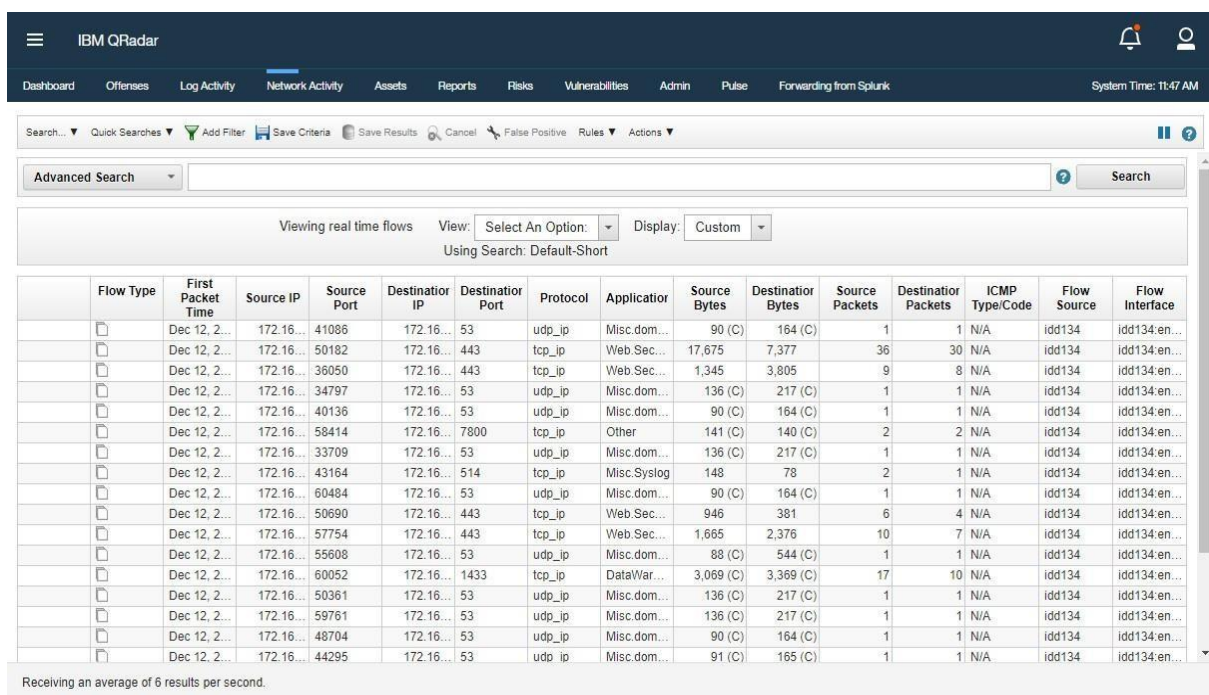
Figure 2.6 Log Activity Tab



## 2.8 NETWORK ACTIVITY TAB

Use the Network Activity tab to investigate flows that are sent in real-time, perform powerful searches, and view network activity by using configurable time-series charts. A flow is a communication session between two hosts.

Viewing flow information helps you determine how the traffic is communicated, what is communicated (if the content capture option is enabled), and who is communicating. Flow data also includes details such as protocols, ASN values, IFIndex values, and priorities



The screenshot shows the IBM QRadar interface with the 'Network Activity' tab selected. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', 'Admin', 'Pulse', and 'Forwarding from Splunk'. The system time is 11:47 AM. Below the navigation bar is a search bar with 'Advanced Search' and a 'Search' button. The main content area displays 'Viewing real time flows' with a 'View' dropdown set to 'Select An Option' and a 'Display' dropdown set to 'Custom'. The table below shows a list of network flows with columns for Flow Type, First Packet Time, Source IP, Source Port, Destination IP, Destination Port, Protocol, Application, Source Bytes, Destination Bytes, Source Packets, Destination Packets, ICMP Type/Code, Flow Source, and Flow Interface. The table contains 15 rows of data, showing various protocols like udp\_ip, tcp\_ip, and Misc.dom... with corresponding byte and packet counts. At the bottom, a status bar indicates 'Receiving an average of 6 results per second.'

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source	Flow Interface
	Dec 12, 2...	172.16...	41086	172.16...	53	udp_ip	Misc.dom...	90 (C)	164 (C)	1	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	50182	172.16...	443	tcp_ip	Web Sec...	17,675	7,377	36	30	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	36050	172.16...	443	tcp_ip	Web Sec...	1,345	3,805	9	8	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	34797	172.16...	53	udp_ip	Misc.dom...	136 (C)	217 (C)	1	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	40136	172.16...	53	udp_ip	Misc.dom...	90 (C)	164 (C)	1	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	58414	172.16...	7800	tcp_ip	Other	141 (C)	140 (C)	2	2	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	33709	172.16...	53	udp_ip	Misc.dom...	136 (C)	217 (C)	1	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	43164	172.16...	514	tcp_ip	Misc.Syslog	148	78	2	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	60484	172.16...	53	udp_ip	Misc.dom...	90 (C)	164 (C)	1	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	50690	172.16...	443	tcp_ip	Web Sec...	946	381	6	4	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	57754	172.16...	443	tcp_ip	Web Sec...	1,665	2,376	10	7	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	55608	172.16...	53	udp_ip	Misc.dom...	88 (C)	544 (C)	1	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	60052	172.16...	1433	tcp_ip	DataWar...	3,069 (C)	3,369 (C)	17	10	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	50361	172.16...	53	udp_ip	Misc.dom...	136 (C)	217 (C)	1	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	59761	172.16...	53	udp_ip	Misc.dom...	136 (C)	217 (C)	1	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	48704	172.16...	53	udp_ip	Misc.dom...	90 (C)	164 (C)	1	1	N/A	idd134	idd134:en...
	Dec 12, 2...	172.16...	44295	172.16...	53	udp_ip	Misc.dom...	91 (C)	165 (C)	1	1	N/A	idd134	idd134:en...

Figure 2.7 Network activity tab

## 2.9 ASSETS TAB

QRadar automatically discovers assets, servers, and hosts that are operating on your network. Automatic discovery is based on passive flow data and vulnerability data, allowing QRadar to build an asset profile.

Asset profiles provide information about each known asset in your network, including identity information, if available, and what services are running on each asset. This profile data is used for correlation purposes to help reduce false positives.

For example, an attack tries to use a specific service that is running on a specific asset. In this situation, QRadar can determine whether the asset is vulnerable to this attack by correlating the attack to the asset profile. Using the Assets tab, you can view the learned assets or search for specific assets to view their profiles.

**2.9.1 Asset data:** An asset is any network endpoint that sends or receives data across your network infrastructure. For example, notebooks, servers, virtual machines, and handheld devices are all assets. Every asset in the asset database is assigned a unique identifier so that it can be distinguished from other asset records. Detecting devices is also useful in building a data set of historical information about the asset. Tracking asset information as it changes helps you monitor asset usage across your network.

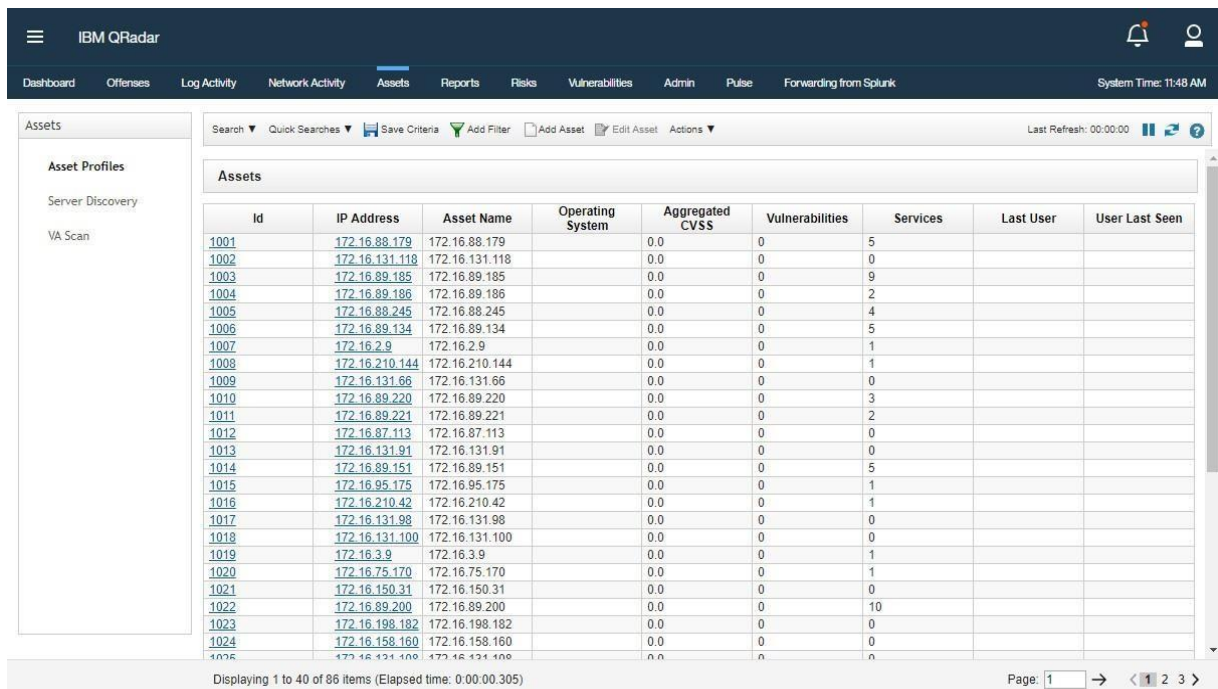
**2.9.2 Asset profiles:** An asset profile is a collection of all information that IBM QRadar SIEM collected over time about a specific asset. The profile includes information about the services that are running on the asset and any identity information that is known. QRadar SIEM automatically creates asset profiles from identity events and bidirectional flow data or, if they are configured, vulnerability assessment scans. The data is correlated through a process that is called asset reconciliation and the profile is updated as new information comes into QRadar.

The asset name is derived from the information in the asset update in the following order of precedence:

- Given name

- NETBios host name
- DNS host name
- IP address

Collecting asset data Asset profiles are built dynamically from identity information that is passively absorbed from event or flow data, or from data that QRadar actively looks for during a vulnerability scan. You can also import asset data or edit the asset profile manually.



Id	IP Address	Asset Name	Operating System	Aggregated CVSS	Vulnerabilities	Services	Last User	User Last Seen
1001	172.16.88.179	172.16.88.179		0.0	0	5		
1002	172.16.131.118	172.16.131.118		0.0	0	0		
1003	172.16.89.185	172.16.89.185		0.0	0	9		
1004	172.16.89.186	172.16.89.186		0.0	0	2		
1005	172.16.88.245	172.16.88.245		0.0	0	4		
1006	172.16.89.134	172.16.89.134		0.0	0	5		
1007	172.16.2.9	172.16.2.9		0.0	0	1		
1008	172.16.210.144	172.16.210.144		0.0	0	1		
1009	172.16.131.66	172.16.131.66		0.0	0	0		
1010	172.16.89.220	172.16.89.220		0.0	0	3		
1011	172.16.89.221	172.16.89.221		0.0	0	2		
1012	172.16.87.113	172.16.87.113		0.0	0	0		
1013	172.16.131.91	172.16.131.91		0.0	0	0		
1014	172.16.89.151	172.16.89.151		0.0	0	5		
1015	172.16.95.175	172.16.95.175		0.0	0	1		
1016	172.16.210.42	172.16.210.42		0.0	0	1		
1017	172.16.131.98	172.16.131.98		0.0	0	0		
1018	172.16.131.100	172.16.131.100		0.0	0	0		
1019	172.16.3.9	172.16.3.9		0.0	0	1		
1020	172.16.75.170	172.16.75.170		0.0	0	1		
1021	172.16.150.31	172.16.150.31		0.0	0	0		
1022	172.16.89.200	172.16.89.200		0.0	0	10		
1023	172.16.198.182	172.16.198.182		0.0	0	0		
1024	172.16.158.160	172.16.158.160		0.0	0	0		
1025	172.16.131.100	172.16.131.100		0.0	0	0		

Figure 2.8 Assets Tab

## 2.10 REPORTS TAB

Use the Reports tab to create, distribute, and manage reports for any data within QRadar. Create customized reports for operational and executive use. Combine information (such as security or network) into a single report.

We can also use preinstalled report templates that are included with QRadar. We can also brand your reports with customized logos. This customization is beneficial for distributing reports to different audiences.

### 2.10.1 Report Layout

A report can consist of several data elements and can represent network and security data in various styles, such as tables, line charts, pie charts, and bar charts.

When you select the layout of a report, consider the type of report you want to create. For example, do not choose a small chart container for graph content that displays many objects. Each graph includes a legend and a list of networks from which the content is derived; choose a large enough container to hold the data.

Report Name	Group	Schedule	Next Run Time	Creation Date	Owner	Author	Generated Reports	Formats
Weekly Success...	Security	Manual	Manual	Apr 13, 2017, 9:...	admin	admin	None	
Asset Compliance	CIS Benchmark...	Manual	Manual	Aug 12, 2014, 6:...	admin	admin	None	
Scan Overview	Scan Reports	Manual	Manual	May 30, 2014, ...	admin	admin	None	
New Vulnerabili...	Scan Reports	Manual	Manual	May 30, 2014, ...	admin	admin	None	
Missing Patches	Scan Reports	Manual	Manual	May 30, 2014, ...	admin	admin	None	
Scan Results (...)	Scan Reports	Manual	Manual	May 30, 2014, ...	admin	admin	None	
Scan Summary...	Scan Reports	Manual	Manual	May 6, 2014, 11:...	admin	admin	None	
Accessible files...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Default logon v...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Annual Vulnera...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Monthly Vulner...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Vulnerability Ex...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Obsolete Envir...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
Vulnerability Ov...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
Network Vulner...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
Last 7 Days Vul...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
Weekly PCI Co...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
PCI Complianc...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 5:...	admin	admin	None	
Weekly Firewall...	Network Manag...	Weekly	4 days 14 hour...	Oct 18, 2010, 7:...	admin	admin	Dec 10, 2018, 2:0	
Top IDS/IPS Al...	Security	Weekly	4 days 14 hour...	Sep 23, 2010, 4:...	admin	admin	Dec 10, 2018, 2:0	
Top IDS/IPS Al...	Security	Weekly	4 days 14 hour...	Sep 23, 2010, 4:...	admin	admin	Dec 10, 2018, 2:0	
Top Application...	Network Manag...	Weekly	3 days 14 hour...	Sep 23, 2010, 4:...	admin	admin	Dec 9, 2018, 2:01	
Daily User Auth...	Authentication, ...	Daily	13 hours 10 mi...	Sep 23, 2010, 4:...	admin	admin	Dec 12, 2018, 1:0	

Figure 2.9 Reports Tab

## 2.11 ADMIN TAB

As an IBM® QRadar® administrator, we have a variety of tools available to help us configure and manage your QRadar deployment.

For example, using the tools on the **Admin** tab, you can perform the following tasks:

- Deploy and manage QRadar hosts and licenses.
- Configure user accounts and authentication.
- Build a network hierarchy.
- Configure domains and set up a multi-tenant environment.
- Define and manage log and flow data sources.
- Manage QRadar data retention.
- Manage assets and reference data.
- Schedule regular backups of QRadar configuration and data.
- Monitor the system health of managed hosts.

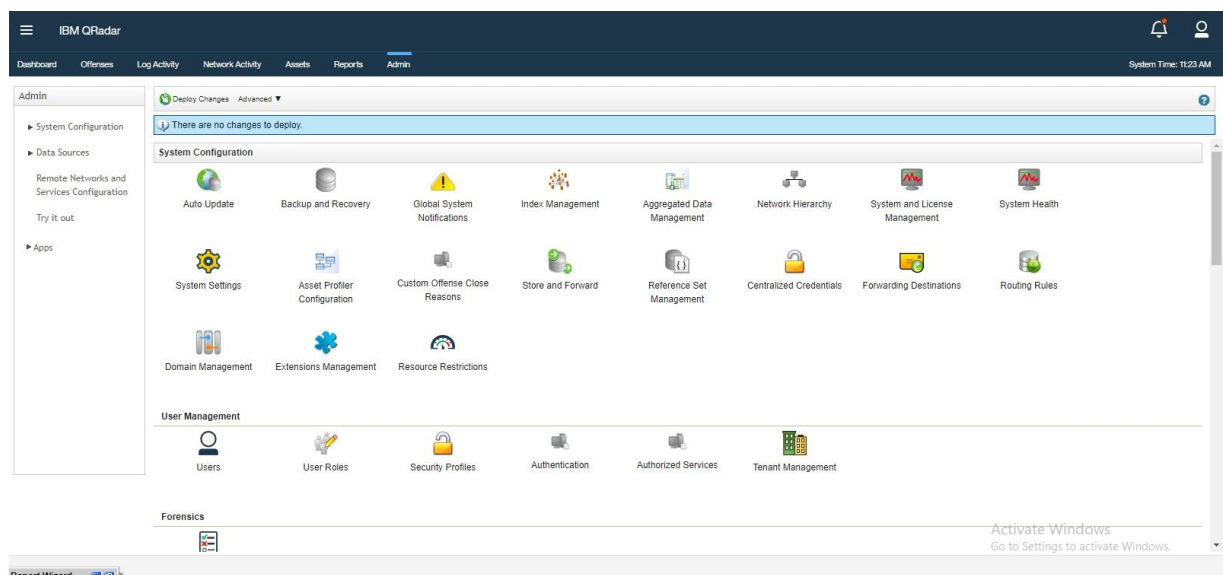


Figure 2.10 Admin Tab

## 2.12 HOW QRADAR SIEM COLLECTS SECURITY DATA

QRadar SIEM collects and processes the event data and vulnerability assessment data gathered by the systems in your network.

- An event is a record from a device that describes an action on a network or host.
- QRadar SIEM normalizes the varied information found in raw events:
  - Normalizing means to map information to common field names, for example:
  - SRC\_IP, Source, IP, and others are normalized to Source IP.
  - user\_name, username, login, and others are normalized to User.
  - Normalized Events are mapped to high-level and low-level categories to facilitate further processing.
- After raw events are normalized, it is easy to search, report, and cross-correlate these normalized events.

### 2.12.1 Event collection and processing

- **Log Sources** typically send syslog messages, but they can use other protocols also.
- **Event Collectors** receive raw events as log messages from a wide variety of external log sources.
- **Device Support Modules (DSMs)** in the event collectors parse and normalize raw events. Raw log messages remain intact.
- **Event Processors** receive the normalized events and raw events to analyze and store them.
- **Magistrate** correlates data from event processors and creates offenses.

## **2.13 RULES**

Rules, sometimes called correlation rules are applied to events, flows, or offenses to search for or detect anomalies. If all the conditions of a test are met, the rule generates response.

### **2.13.1 What are rules?**

Custom rules test events, flow, and offenses to detect unusual activity in your network. You create new rules by using AND and OR combinations of existing rule tests. Anomaly detection rules test the results of saved flow or events searches to detect when unusual traffic patterns occur in your network. Anomaly detection rules require a saved search that is grouped around a common parameter.

### **2.13.2 What are building blocks?**

A building block is a collection of tests that don't result in a response or an action.

A building block groups commonly used tests to build complex logic so that it can be reused in rules. A building block often tests for IP addresses, privileged user names, or collections of event names. For example, a building block can include the IP addresses of all DNS servers. Rules can then use this building block.

### **2.13.3 How do rules work?**

QRadar Event Collectors gather events from local and remote sources, normalize these events, and classify them into low-level and high-level categories. For flows, QRadar QFlow Collectors read packets from the wire or receive flows from other devices and then convert the network data to flow records.

Each Event Processor processes events or flow data from the QRadar Event Collectors. Flow Processors examine and correlate the information to indicate behavioral changes or policy violations. The custom rules engine (CRE) processes events and compares them against defined rules to search for anomalies. When a rule condition is met, the Event Processor generates an action that is defined in the rule response. The CRE tracks the systems that are involved in incidents, contributes events to offenses, and generates notifications.

## **CHAPTER 3: EDR**

### **3 EDR:**

Endpoint security is a cornerstone of IT security. To help you navigate this growing marketplace, our team has researched and analyzed this list of top endpoint detection and response (EDR) vendors, which carries out analysis of event and log data in real-time to provide event correlation, threat monitoring and incident response - with Security Information Management which retrieves and analyzes log data and generates a report. For the organization that wants complete visibility and control over what is happening on their network in real-time, EDR solutions are critical.

#### **3.1 How Does EDR Work?**

EDR software works by collecting log and event data that is generated by host systems, security devices and applications throughout an organization's infrastructure and collating it on a centralized platform. Using EDR, the threat hunters work proactively to hunt, investigate and advise on threat activity in your environment. When they find a threat, they work alongside your team to triage, investigate and remediate the incident, before it has the chance to become a full-blown breach.

It uses advanced algorithms to analyze the behaviors of individual users on your system, allowing to connect their activities. In the same way that you often notice when something feels off or different about someone you're close to, the technology can "sense" behavior that is out of the ordinary for a given user on your system. The data is immediately filtered, enriched, and monitored for signs of malicious behavior. These signs trigger an alarm and the investigation begins—determining if a hit is true or a false positive. If malicious activity is detected, the algorithms track the path of the attack and build it back to the point of entry. The technology then consolidates all data points into narrow categories called MalOps to make it easier for analysts to review. In the event of a true hit, the customer is notified and given actionable response steps and recommendations for further investigation and



advanced forensics. If it is a false positive, the alarm is closed, investigation notes are added.

### **3.2 Benefits of Using EDR**

EDR provide a powerful method of threat detection, real-time reporting and long-term analytics of security logs and events. This tool can be incredibly useful for safeguarding organizations of all sizes.

Benefits of EDR include:

- Increased efficiency
- Preventing potential security threats
- Reducing the impact of security breaches
- Reducing costs
- Better reporting, log analysis and retention
- IT compliance

In a nutshell, it allows IT teams to see the bigger picture by collecting security event data from multiple sources in one place. A single alert from an antivirus filter may not be a cause of panic on its own, but if traffic anomaly alerts are received from the firewall at the same time, this could signify that a severe breach is in progress. It collects all of these alerts in a centralized console, allowing fast and thorough analysis

## CHAPTER 4: SentinelOne

**SentinelOne** provides broad protection against a diverse modes of attack



Figure 4.1 General Overview of SentinelOne

### 4.1 Sentinelone:

Detecting threats in real-time supports immediate response that mitigates discovered threats before they harm IT ecosystems. SentinelOne uses a patented Behavioral AI feature to recognize malicious actions and patterns. Threat detection is applied to detect file-less, zero- day, and nation-grade attacks. The integration of AI ensures threats are discovered in in a timelymanner which reduces the effects of ransomware and phishing attacks.

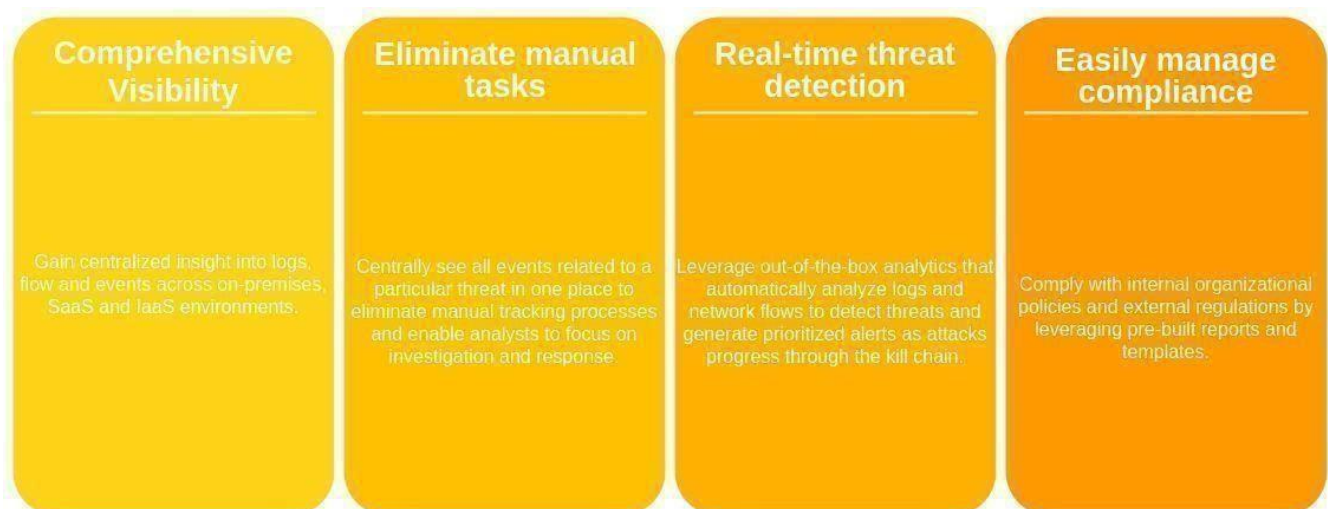


Figure 4.2 General Overview of EDR

## 4.2 Key Features:

- Ingest vast amounts of data from on-prem and cloud sources
- Applies built-in analytics to accurately detect threats Correlate related activities to prioritize incidents
- Automatically parses and normalizes logs
- Integrates out-of-the-box with 450 solutions
- Flexible architecture can be deployed on-prem or on cloud Highly scalable, self-tuning and self-managing database.



Figure 4.3 Why we need EDR

### **4.3 EDR capabilities:**

- Collection, normalization, correlation and secure storage of raw events, network flows, vulnerabilities, assets, and threat intelligence data.
- Layer 7 payload capture up to a configurable number of bytes from unencrypted traffic.
- Comprehensive search capabilities.
- Monitor host and network behavior changes that could indicate an attack or policy breach such as these examples:
  - Off hours or excessive usage of an application or network activity patterns inconsistent with historical profiles.
  - Prioritization of suspected attacks and policy breaches.
- Notification by email, SNMP, and others.
- Many generic reporting templates included.
- Scalable architecture to support large deployments.
- Single user interface.

### **4.4 EDR Dashboard:**

EDR shows the Dashboard tab when you log in.

- You can create multiple dashboards.
- Each dashboard can contain items that provide summary and detailed information.
- Six default dashboards are available.
- You can create custom dashboards to focus on your security or operations responsibilities

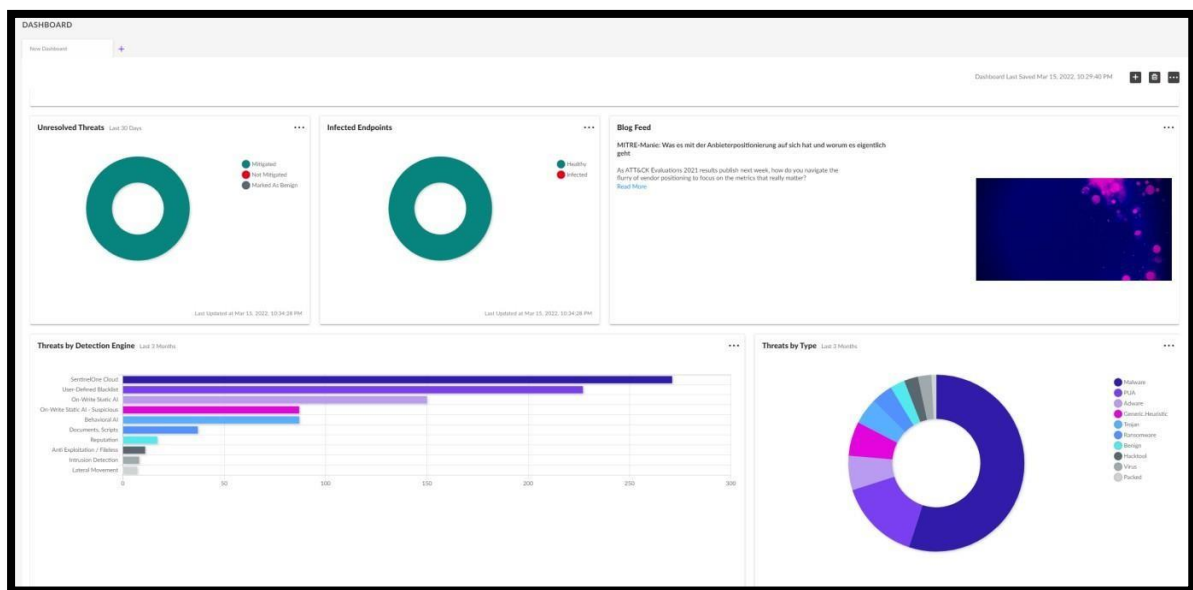


Figure 4.4 Dashboard

Use tabs to navigate the primary functions:

- **Dashboard:** The initial summary view.
- **Visibility:** Displays offenses; list of prioritized incidents.
- **Sentinels:** Query and display events.
- **Incidents:** Query and display flows.
- **Reports:** Create templates and generate reports.
- **Admin:** Administrative system management

## **4.5 How EDR collects security data**

SentinelOne integrates Static AI on endpoints to prevent attacks in real-time. The integration of AI ensures threats are quickly culled and dealt with before they can affect network systems. The SentinelOne prevention model can be more efficient than legacy antivirus solutions as it produces low false positives while focusing on preventing real threats.

SentinelOne makes use of ActiveEDR to respond to issues within a network. ActiveEDR integrates behavioral AI and is capable of surgically reversing and removing malicious activities. Organizations can automate the response process to ensure it occurs in real-time. The AI-assisted response ensures devices connected to enterprise networks can individually respond to threats in real-time.

Organizations should make it a goal to have a proactive process to discovering threats rather than a reactive one. Proactive threat hunting ensures attacks are sought out before they reach an enterprise network or infrastructure. SentinelOne delivers quick query times, and advanced actions when threat hunting. The advanced actions include pre-indexed forensic context to understand the motive behind attacks, full-native remote shell, and more.

Comprehensive security measures are those that provide edge-to-edge protection for assets within an enterprise's IT architecture.

SentinelOne is an example of a comprehensive enterprise security platform that provides threat detection, hunting, and response features that enable organizations to discover vulnerabilities and protect IT operations.

SentinelOne integrates static artificial intelligence (AI) to provide real-time endpoint protection and reduce false positives that derail investigations or make threat detection a capital-intensive process.

Endpoint	Endpoint Type	Account	Site	Last Logged In User	Group	Domain	Console Visible IP	Agent Version	Last Active	Registered On	Health State
[Icon]	N/A	Procuro	Procuro AS	N/A	Default Group	WORKGROUP	86.62.171.134	21.7.5.1080	Last 4 minutes	Mar 24, 2022 22:27:10	Healthy
[Icon]	N/A	Procuro	Procuro AS	N/A	Default Group	WORKGROUP	82.196.200.90	21.7.5.1080	Last 4 minutes	Mar 25, 2022 09:59:36	Healthy
[Icon]	N/A	Procuro	Procuro AS	N/A	Default Group	WORKGROUP	86.62.171.134	21.7.5.1080	Last 4 minutes	Mar 25, 2022 09:59:45	Healthy
[Icon]	N/A	Procuro	Procuro AS	Powershell	Default Group	WORKGROUP	86.62.171.134	21.7.5.1080	Last 4 minutes	Mar 25, 2022 09:59:47	Healthy
[Icon]	N/A	Procuro	Procuro AS	N/A	Default Group	WORKGROUP	80.213.87.51	21.7.5.1080	Last 4 minutes	Mar 25, 2022 09:59:50	Healthy
[Icon]	N/A	Procuro	Procuro AS	Procuro_admin	Default Group	WORKGROUP	86.62.171.134	21.7.5.1080	7 hours ago	Mar 25, 2022 09:59:52	Healthy
[Icon]	N/A	Procuro	Procuro AS	Defaultuser1	Default Group	WORKGROUP	46.9.191.228	21.7.5.1080	10 hours ago	Mar 25, 2022 09:59:54	Healthy
[Icon]	N/A	Procuro	Procuro AS	Defaultuser1	Default Group	WORKGROUP	85.165.147.168	21.7.5.1080	19 hours ago	Mar 25, 2022 09:59:59	Healthy
[Icon]	N/A	Procuro	Procuro AS	Ty330	Default Group	WORKGROUP	217.171.201.11	21.7.5.1080	Last 4 minutes	Mar 25, 2022 10:00:06	Healthy
[Icon]	N/A	Procuro	Procuro AS	Procuro_admin	Default Group	WORKGROUP	82.196.200.90	21.7.5.1080	Last 4 minutes	Mar 25, 2022 10:00:08	Healthy
[Icon]	N/A	Procuro	Procuro AS	CI_admin	Default Group	WORKGROUP	79.160.141.176	21.6.5.1072	1 month ago	Mar 25, 2022 10:00:09	Healthy
[Icon]	N/A	Procuro	Procuro AS	Setup	Default Group	WORKGROUP	86.62.171.134	21.7.5.1080	15 hours ago	Mar 25, 2022 10:00:18	Healthy
[Icon]	N/A	Procuro	Procuro AS	N/A	Default Group	WORKGROUP	51.174.187.158	21.7.5.1080	Last 4 minutes	Mar 25, 2022 10:00:26	Healthy
[Icon]	N/A	Procuro	Procuro AS	One	Default Group	PROCANO	87.2480.107	21.6.5.1072	2 months ago	Mar 25, 2022 10:00:27	Healthy
[Icon]	N/A	Procuro	Procuro AS	N/A	Default Group	WORKGROUP	84.208.48.222	21.7.5.1080	2 hours ago	Mar 25, 2022 11:36:57	Healthy
[Icon]	N/A	Procuro	Procuro AS	N/A	Default Group	WORKGROUP	85.195.36.229	21.7.5.1080	10 hours ago	Mar 25, 2022 13:35:10	Healthy
[Icon]	N/A	Procuro	Procuro AS	SHC	Default Group	PROCANO	84.2154.100	21.6.5.1072	2 months ago	Mar 25, 2022 14:25:14	Healthy
[Icon]	N/A	Procuro	Procuro AS	N/A	Server	BW-CEN	109.235.118.33	21.7.5.1080	Last 4 minutes	Mar 25, 2022 19:57:43	Healthy
[Icon]	N/A	Procuro	Procuro AS	N/A	Server	OSL5-PP	109.235.118.33	21.7.5.1080	Last 4 minutes	Mar 25, 2022 19:57:43	Healthy
[Icon]	N/A	Procuro	Procuro AS	N/A	Server	WORKGROUP	109.235.114.24	21.7.5.1080	Last 4 minutes	Mar 25, 2022 19:57:45	Healthy

Figure 4.5 Endpoints Tab

All collected information is available for reports. Thousands of report templates are available. With the report wizard, you can create new templates and change existing templates.

**Threat Status:** MITIGATED | **AI Confidence Level:** MALICIOUS | **Analyst Verdict:** True Positive | **Incident Status:** Resolved

**Identified Time:** Mar 15, 2022 13:02:02 | **Reporting Time:** Mar 15, 2022 13:02:03

**Migration Actions taken:** KILLED 6/6 | QUARANTINED 1/1

**First seen:** Mar 15, 2022 13:02:03 | **Last seen:** Mar 15, 2022 13:02:03

**Only 1 time on the current endpoint:** 1 Account / 1 Site / 1 Group

**Find this host on Deep Visibility:** [Find Now](#)

**THREAT FILE NAME:** update2.hta

**Path:** \Device\HarddiskVolume2\Users\tsctest\Downloads\update2.hta

**Command Line Arguments:** "C:\Users\tsctest\Downloads\update2.hta" [1E460BD7-F1C3-482E-88...

**Process User:** tsctest

**Publisher Name:** N/A

**Signer Identity:** N/A

**Signature Verification:** NotSigned

**Originating Process:** chrome.exe

**SHA1:** dff7b2eb87072159250c8631311e9889eb93004b

**Initiated By:** Agent Policy

**Engine:** Documents, Scripts

**Detection type:** Dynamic

**Classification:** Malware

**File Size:** 6.98 KB

**Storyline:** 0A9CFBDE12EC2C81

**Threat id:** 1376954127127274282

**ENDPOINT**

**Real-time data about the endpoint:**

**At detection time:** 3/15/2022

**Scope:** Windows 10 Pro 19044

**OS Version:** 21H2.272

**Agent Version:** 21.6.2.272

**Policy:** Protect

**Logged in User:** tsctest

**UUID:** 800X04408994b42a786147c33173677

**Domain:** LICOR

**IP v4 Address:** 172.24.86.64

**IP v6 Address:** 2607:ds00:307:0:d44e:9e20:16d3:7a1a:2607:ds00:307:0:b...

**Console Visible IP Address:** 208.82.105.140

**Subscription Time:** Dec 14, 2021 06:37:29

**THREAT INDICATORS (3):**

- Post Exploitation:** Detected penetration framework
- Exploitation:** Shellcode execution from Powershell was detected (MITRE : Execution [T1059.001][T1106])
- Shellcode execution was detected (MITRE : Execution [T1106][T1059])

**NOTES:**

Figure 4.6 Selecting an offense to investigate

## CONCLUSIONS

In conclusion, SOC (Security Operations Center) analysts play a crucial role in maintaining the cybersecurity of organizations. As the cybersecurity landscape continues to evolve, the future scope of SOC analysts is filled with opportunities and challenges. Here are the key points to summarize their role and future prospects:

**Rapidly Evolving Threat Landscape:** SOC analysts will face increasingly sophisticated and persistent cyber threats. They need to stay updated with the latest threat intelligence, adopt advanced detection and response techniques, and leverage automation and orchestration tools to keep pace with evolving threats.

**Emphasis on Proactive Defense:** The future of SOC analysts lies in proactive defense strategies. They will focus on threat hunting, red teaming, and continuous monitoring to identify and mitigate potential threats before they cause damage.

**Cloud and IoT Security:** SOC analysts will need to develop expertise in securing cloud environments and addressing the unique challenges posed by IoT devices. They must understand the specific risks associated with these technologies and implement effective monitoring and response measures.



## **FUTURE SCOPE**

The future scope of SOC (Security Operations Center) analysts is expected to expand and evolve in response to the continuously evolving cybersecurity landscape. Here are some potential areas of growth and development for SOC analysts:

**Advanced Threat Detection and Response:** As cyber threats become more sophisticated, SOC analysts will need to enhance their skills in advanced threat detection and response techniques. This includes leveraging artificial intelligence (AI) and machine learning (ML) algorithms for anomaly detection, behavioral analysis, and proactive threat hunting.

**Automation and Orchestration:** SOC analysts will increasingly rely on automation and orchestration tools to streamline routine tasks, such as incident triage, alert validation, and containment. This allows them to focus on more complex and strategic activities, improving efficiency and response times.

## REFERENCES

- <https://www.ibm.com/support/>
- [https://en.wikipedia.org/wiki/Security\\_information\\_and\\_event\\_management](https://en.wikipedia.org/wiki/Security_information_and_event_management)
- [https://en.wikipedia.org/wiki/Endpoint\\_detection\\_and\\_response](https://en.wikipedia.org/wiki/Endpoint_detection_and_response)
- IBM QRadar SIEM 7.2 Foundations
- IBM QRadar User Guide