

A Mid-Term Progress Report of Training

at

SAFEAEON INC., MOHALI

SUBMITTED IN PARTIAL FULFILMENT REQUIREMENT FOR THE AWARD OF

DEGREE OF

Bachelor of Technology

(Computer Science & Engineering)



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

Contents

Chapter 1: Introduction	3
1.1 Overview	3
1.2 Existing System	6
1.3 Objectives	6
Chapter 2. System Requirements	7
2.1 Software and Hardware Requirements	7
Chapter 3. Software Requirement Analysis	8
3.1 Problem Definition	8
3.2 Software Requirement Analysis	8
Chapter 4. Software Design	12
4.1 Software Design	12
Chapter 5. Core Module	22
5.1 Core modules in QRadar SIEM	22
Chapter 6. Performance of the Training work undertaken	24
6.1 Performance of the Training work undertaken	24
Chapter 7. Output Screens	25
7.1 Output screen of IBM QRadar	25
References	30

Chapter 1: Introduction

1.1 Overview

Security Operations Center (SOC) Analyst is the first line of defense in an organization, and if a SOC analyst fails to identify an adversary, no one else in the organization can find it out. Similar to cybersecurity analysts, SOC analysts are the first responders to cyber threats. They report threats to the second line of defense and then implement security strategies to protect the organization. There can be a single cybersecurity analyst in an organization, whereas SOC analysts form part of a large security team.

The specific responsibilities of SOC analyst are –

- Monitor security access and report suspicious activity to a higher level or team members.
- Conduct security assessments regularly to identify vulnerabilities and performing risk analysis.
- Analyze the breach to reach the root cause.
- Generate reports for IT administrators, business managers, and security leaders.
- These reports serve as an input to evaluate the efficacy of the security policies.
- Advise and implement necessary changes required to counter the attack or improvise security standards.
- Keep the security systems up to date and contributing to security strategies.
- Document incidents to contribute to incident response and disaster recovery plans.
- Perform internal and external security audits.
- In the case of third-party vendors, verify their security strength and collaborate with them.

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.

- **Working of SIEM:**

SIEM 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. From antivirus events to firewall logs, SIEM software identifies this data and sorts it into categories, such as malware activity, failed and successful logins and other potentially malicious activity.

When the software identifies activity that could signify a threat to the organization, alerts are generated to indicate a potential security issue. These alerts can be set as either low or high priority using a set of pre-defined rules. For example, if a user account generates 20 failed login attempts in 20 minutes, this could be flagged as suspicious activity, but set at a lower priority as it is most likely to be a user that has forgotten their login details. However, if an account experiences 120 failed login attempts in 5 minutes this is more likely to be a brute-force attack in progress and flagged as a high severity incident.

- **Benefits of using SIEM:**

- **Enhanced threat detection and response capabilities:** SIEM enables organizations to detect and respond to cyber threats more effectively by aggregating and correlating security events from various sources, providing real-time alerts and enabling proactive incident response.
- **Comprehensive visibility into security events:** SIEM collects and analyzes security logs and events from across the organization's network infrastructure, applications, and systems, providing a holistic view of the security posture and identifying potential vulnerabilities or malicious activities.

- Improved incident response and faster time to resolution: SIEM streamlines incident response processes by automating the collection, analysis, and prioritization of security events, enabling organizations to quickly identify and remediate security incidents, minimizing the impact of breaches.
- Advanced analytics and threat intelligence: SIEM systems incorporate advanced analytics and threat intelligence capabilities, enabling organizations to detect complex threats, identify patterns of malicious behavior, and leverage threat intelligence feeds to stay updated on emerging threats and vulnerabilities.
- Centralized log management and analysis: SIEM centralizes the collection, storage, and analysis of logs from diverse sources, simplifying log management and facilitating efficient log analysis, troubleshooting, and forensic investigations.

- **Companies that provide SIEM products**

Various companies that provide SIEM tools are:

- IBM Qradar
- Fortinet
- AlienVault Unified Security Management
- SolarWinds
- Splunk



1.2 Existing System

Security Information and event management (SIEM) provides an insight into a corporate IT environment by its functions like log management and security information management. Choice of SIEM is done by taking some basic features into consideration like threat detection, compliance reporting, historical log analysis, user friendly dashboards and sophisticated analytical capabilities. Instead of looking open-source platforms, companies mostly larger organizations rather prefer expensive SIEM products because existing solutions either lack core SIEM capabilities, such as event correlation and reporting or require combining with other tools.

In short, SIEM tools functions by collecting and aggregating log data. A SIEM solution analyzes all the security alerts from all manner of applications and hardware across a network and from antivirus tools to servers to firewalls and more. These tools alone aren't enough to protect a business. So only SIEM tool can give you a bigger picture in understanding of your cyber-security threat landscape.

1.3 Objectives

- **Understanding Cybersecurity Fundamentals and Familiarization with Security Tools and Technologies:** Gain a comprehensive understanding of the fundamental principles, concepts, and practices related to cybersecurity. This includes knowledge of common threats, attack vectors, vulnerabilities, and defense mechanisms and become proficient in using various security tools and technologies commonly used in a SOC environment.
- **Log Analysis and Monitoring:** Develop skills in analyzing logs and monitoring systems for security events. Understand how to identify and investigate security incidents based on log data, network traffic, and system behavior. Gain proficiency in log analysis tools and techniques.

- **Vulnerability Management:** Understand the importance of vulnerability management and its role in maintaining a secure environment. Learn how to assess and prioritize vulnerabilities, perform vulnerability scanning, and coordinate remediation efforts with system.
- **Continuous Learning and Professional Development:** Recognize the importance of continuous learning in the field of cybersecurity. Stay updated with the latest industry trends, emerging threats, and new technologies. Engage in professional development activities, such as attending conferences, participating in training programs, and obtaining relevant certifications.

Chapter 2. System Requirements

2.1 Software and Hardware Requirements

The hardware specifications (CPU, RAM, storage, network interfaces) vary depending on the appliance model and series. Higher-end appliances typically offer more processing power, storage capacity, and network throughput to handle larger data volumes and support scalability. Generally, the following are the hardware specifications in QRadar SIEM:

- A sufficient amount of RAM (e.g., 16 GB or more)
- High-speed storage (e.g., SSD)

The specific requirements of the SIEM tool QRadar are

Technical Requirement

QRadar SIEM requires Red Hat Enterprise Linux (RHEL) Server.

Software requirements

1. Java SDK: IBM Runtime Environment Java Technology edition 7.0.8
2. Security management: Tivoli Directory Integrator 7.1.7

Browser Requirements:

1. Google Chrome 43 and future fix packs
2. Microsoft Internet Explorer 10 and future fix packs
3. Mozilla Firefox ESR 38 and future fix packs.

Chapter 3. Software Requirement Analysis

3.1 Problem Definition

SafeAeon Inc. In India, delivers security services to other organizations who can't afford in-house SOC. As In the few past years after the security related issues were faced by the organizations than SOC came into practice. But SOC was considered as a heavyweight infrastructure which is only within the reach of very large or security-minded organizations. But today, with the arrival of new collaboration tools and security technology, virtual SOC's has been setup by many organizations which do not require a dedicated facility, and can use part-time staff from security, operations and development groups.

Today, many organizations are growing their business by setting up managed SOC's or a hybrid SOC's which combine in-house staff with proper tools and expertise from Managed Security Service Providers (MSSPs) and our organization SafeAeon is one amongst such Mssp's that provide security services to many Fortune 500 Companies by giving a real-time analysis of offenses, monitoring and risk management.

3.2 Software Requirement Analysis

IBM QRadar requires some specifications which can be categorized into following:

Data Requirement

Ensuring protection of sensitive data which is important for both brand reputation and compliance with requirements, IBM QRadar keeps sensitive data and critical data out of the hands of cyber criminals in the first step, but it also requires knowing what data is being used within organization, who is accessing it, and how it moves across the organization.

In actual, IBM QRadar works better if amount of data related to source IP's and destination IP's is large because it got trained itself on occurrence of each connection whether it is related to any firewall denies, multiple login failure or any type of malware attacks like DDOS, Remote Code Execution (RCE). In this admin can set rules according to particular offense type and can filter out any data related to offense and get to know more description about Source IP's, Destination IP's, Users, Logs, Events Occurred so to apply actions to normalize the raw data into useful information like which IP's are whitelisted and which offense is found is found to be genuine.

Functional Requirement

IBM QRadar SIEM offers a modular, appliance-based approach to SIEM that can scale to meet the event log and network flow monitoring and analysis needs of most organizations. Additional, integrated modules for risk and vulnerability management, forensics analysis of packet captures, and incident response (from the recently acquired Resilient Systems technology) are also available as options, though they are not included. The IBM QRadar SIEM also supports IBM X-Force Threat Intelligence and other third-party threat intelligence feeds via STIX and TAXI to improve threat detection. Organizations interested in evaluating enterprise SIEM products should gather additional information about IBM QRadar SIEM in order to help determine if it meets their requirements.

○ QRadar Console

The QRadar Console provides the QRadar user interface, and real-time event and flow views, reports, offenses, asset information, and administrative functions.

In distributed QRadar deployments, use the QRadar Console to manage hosts that include other components.

○ QRadar Event Collector

The Event Collector collects events from local and remote log sources and normalizes raw log source events to format them for use by QRadar. The Event Collector bundles or coalesces identical events to conserve system usage and sends the data to the Event Processor.

- Use the QRadar Event Collector 1501 in remote locations with slow WAN links. The Event Collector appliances do not store events locally. Instead, the appliances collect and parse events before they send events to an Event Processor appliance for storage.
- The Event Collector can use bandwidth limiters and schedules to send events to the Event Processor to overcome WAN limitations such as intermittent connectivity.
- The Event Collector is assigned to an EPS license that matches the Event Processor that it is connected to.

- **QRadar Event Processor**

The Event Processor processes events that are collected from one or more Event Collector components. The Event Processor processes events by using the Custom Rules Engine (CRE). If events are matched to the CRE custom rules that are predefined on the Console, the Event Processor executes the action that is defined for the rule response.

Each Event Processor has local storage, and event data is stored on the processor, or it can be stored on a Data Node.

The processing rate for events is determined by your events per second (EPS) license. If you exceed the EPS rate, events are buffered and remain in the Event Collector source queues until the rate drops. However, if you continue to exceed the EPS license rate, and the queue fills up, your system drops events, and QRadar issues a warning about exceeding your licensed EPS rate.

When you add an Event Processor to an All-in-One appliance, the event processing function is moved from the All-in-One to the Event Processor.

- **QRadar QFlow Collector**

The Flow Collector collects flows by connecting to a SPAN port, or a network TAP. The IBM QRadarQFlow Collector also supports the collection of external flow-based data sources, such as NetFlow from routers.

QRadarQFlow Collectors are not designed to be full packet capture systems. For full packet capture, review the QRadar Incident Forensics option. The QRadarQFlow Collector 1310 appliance specifically, can forward packets to a QRadar Packet Capture appliance, which allows for flow collection and packet collection from a single packet source.

You can install a QRadarQFlow Collector on your own hardware or use one of the QRadarQFlow Collector appliances.

Restriction The QRadar Log Manager does not support flow collection or Flow Collectors, which is supported only in QRadar SIEM deployments.

- **QRadar Flow Processor**

The Flow Processor processes flows from one or more QRadarQFlow Collector appliances. The Flow Processor appliance can also collect external network flows such as NetFlow, J-Flow, and S-Flow directly from routers in your network. You can use the Flow Processor appliance to scale your QRadar deployment to manage higher flows per minute (FPM) rates.

Flow Processors include an on-board Flow Processor, and internal storage for flow data. When you add a Flow Processor to an All-in-One appliance, the processing function is moved from the All-in-One appliance to the Flow Processor.

- **QRadar Data Node**

Data Nodes enable new and existing QRadar deployments to add storage and processing capacity on demand as required. Data Nodes help to increase the search speed in your deployment by providing more hardware resources to run search queries on.

- **QRadar App Host**

An App Host is a managed host that is dedicated to running apps. App Hosts provide extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console. Apps such as User Behavior Analytics with Machine Learning Analytics require more resources than are currently available on the Console.

Performance Requirement

FLEXIBILITY, SCALABILITY, AND SPEED OF DEPLOYMENT

With IBM QRadar on Cloud, customers can collect log source data and network flows with high EPS maximums. Customers reported the **flexibility** of the cloud allowed them to provision only what they needed and scale their deployment if their needs changed. Customers can scale their log collection without installing additional infrastructure or devoting additional resources to managing the solution. Customers were also impressed with how quickly the solution could be set up and start collecting logs.

The **speed of deployment** allowed customers to quickly transition to value-adding tasks. The internal due diligence of which log sources are important to collect versus which are noise helps to speed the process of gathering useful information once IBM QRadar on Cloud is deployed. Customers said:

- “The back-and-forth internal decision took about a month. Once we decided on IBM, it took about a day to get it stood up and collect the first logs.”
- “The ease of deployment was definitely one of the biggest benefits for us.”
- “We had one or two people working on deployment—not even full time—to do the technical setup of the gateway and connect to the cloud.”

Chapter 4. Software Design

4.1 Software Design

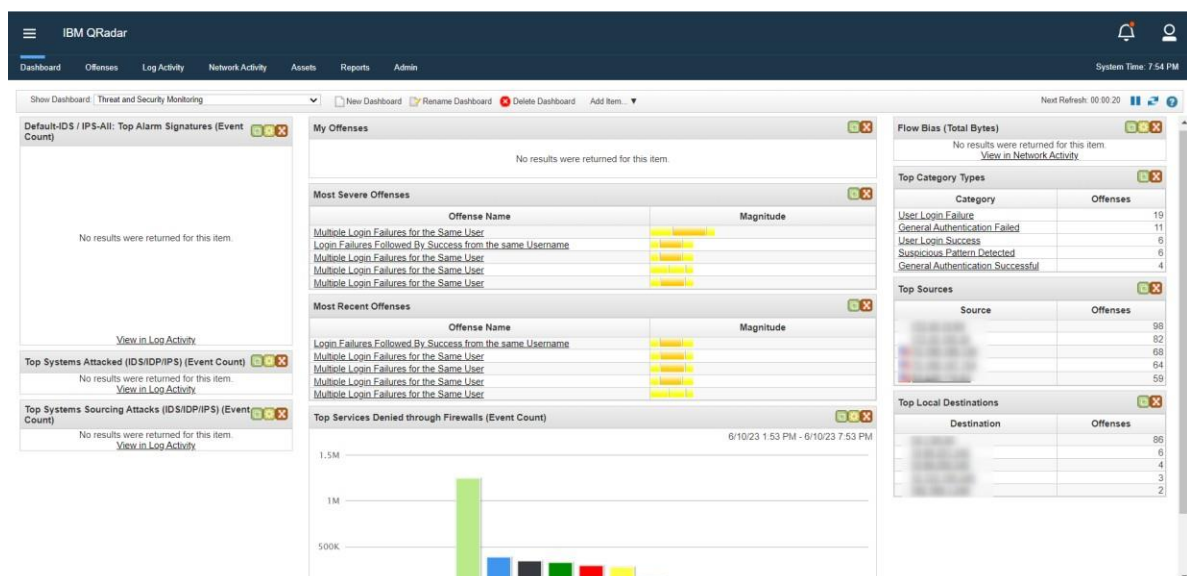
QRadar is a security information and event management or SIEM product that is designed for enterprises. The tool collects data from the organization and the network devices. It also connects to the operating systems, host assets, applications, vulnerabilities, user activities, and behaviors.

Login Page of IBM QRadar



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 network security, activity, or data that QRadar collects.



- **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.

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	Domain	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Source
4757		Multiple Login Failures for the Same User	Username		High			Multiple (2)	
18105		Login Failures Followed By Success from the same Username	Username		High			Multiple (9)	
17959		Multiple Login Failures for the Same User	Username		High			Multiple (1)	
18136		Multiple Login Failures for the Same User	Username		High			Multiple (2)	
18143		Multiple Login Failures for the Same User	Username		High			Multiple (3)	
9107		Multiple Login Failures for the Same User	Username		High			Multiple (8)	
17365		Login Failures Followed By Success from the same Username	Username		High			Multiple (7)	
17970		User Added to Privileged Group	Username		High			Multiple (2)	
5322		Multiple Login Failures for the Same User	Username		High			Multiple (2)	
17013		Login Failures Followed By Success from the same Username	Username		High			Multiple (4)	
17053		Multiple Login Failures for the Same User	Username		High			Multiple (4)	
17154		Multiple Login Failures for the Same User	Username		High			Multiple (7)	
17433		Login Failures Followed By Success from the same Username	Username		High			Multiple (5)	
17699		Login Failures Followed By Success from the same Username	Username		High			Multiple (5)	
17804		Login Failures Followed By Success from the same Username	Username		High			Multiple (3)	
17901		C365 - Multiple Login Failures for Single Username	Username		High			Multiple (2)	
18026		Login Failures Followed By Success from the same Username	Username		High			Multiple (4)	
17047		Multiple Login Failures for the Same User	Username		High			Multiple (1)	
17203		Multiple Login Failures for the Same User	Username		High			Multiple (9)	
17318		Login Failures Followed By Success from the same Username	Username		High			Multiple (8)	
17543		Login Failures Followed By Success from the same Username	Username		High			Multiple (6)	
17624		Login Failures Followed By Success from the same Username	Username		High			Multiple (1)	
17628		Login Failures Followed By Success from the same Username	Username		High			Multiple (6)	
12020		Multiple Login Failures for the Same User	Username		High			Multiple (2)	
16987		Multiple Login Failures for the Same User	Username		High			Multiple (2)	

Offenses Tab

Offense 4757 (Summary)

Offense 4757

Magnitude

Domain

Description

Source IP(s)

Destination IP(s)

Network(s)

Multiple Login Failures for the Same User

Multiple (4)

Other

Status

Relevance

Severity

Credibility

2

5

2

Offense Type

Event/Flow count

Start

Duration

Assigned to

Username

329 521 events and 8 flows in 2 categories

Jan 14, 2022, 8:51:59 AM

511d 23h 7m 25s

Offense Source Summary

Username

MAC Address

Last Known Host

Last Known MAC

Last Observed

Offenses

A_#

Unknown NIC

Unknown

Unknown

Unknown

1

Host Name

Last Known Machine

Last Known IP

Last Known Group

Events/Flows

Unknown

Unknown

Unknown

Unknown

373,970

Last 5 Notes

Notes

Username

Creation Date

Last 5 Search Results

Magnitude

Started On

Ended On

Duration

Events/Flows

Offense summary page

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.

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.

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.

- **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.

[illegible]

Log Activity Tab

- **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 table displays real-time 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 data is filtered by 'Default-Short' search criteria. The status at the bottom 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
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	90 (C)	164 (C)	1	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					tcp_ip	Web Sec...	17,675	7,377	36	30	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					tcp_ip	Web Sec...	1,345	3,805	9	8	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	136 (C)	217 (C)	1	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	90 (C)	164 (C)	1	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					tcp_ip	Other	141 (C)	140 (C)	2	2	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	136 (C)	217 (C)	1	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					tcp_ip	Misc Syslog	148	78	2	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	90 (C)	164 (C)	1	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					tcp_ip	Web Sec...	946	381	6	4	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					tcp_ip	Web Sec...	1,665	2,376	10	7	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	88 (C)	544 (C)	1	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					tcp_ip	Data/Var...	3,069 (C)	3,369 (C)	17	10	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	136 (C)	217 (C)	1	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	136 (C)	217 (C)	1	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	90 (C)	164 (C)	1	1	N/A	100134	100134.en
<input type="checkbox"/>	Dec 12, 2...					udp_ip	Misc dom...	91 (C)	165 (C)	1	1	N/A	100134	100134.en

Network activity tab

- **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.

Id	Domain	IP Address	Asset Name	Operating System	Aggregated CVSS	Vulnerabilities	Services	Last User	User Last Seen
1779					0.0	0	0		2023-06-11 02:10:38.41
1801					0.0	0	0		2023-06-01 15:16:35.734
1805					0.0	0	0		2023-06-09 13:29:47.17
1842					0.0	0	0		2023-06-08 12:31:25.646
1858					0.0	0	0		2023-06-09 12:53:24.39
1863					0.0	0	0		2023-06-02 23:41:12.12
1864					0.0	0	0		2023-06-10 07:01:46.308
1865					0.0	0	0		2023-06-08 05:19:38.056
1878					0.0	0	0		2023-06-11 03:40:19.402
1879					0.0	0	0		2023-06-10 05:34:25.925
1949					0.0	0	0		2023-06-08 13:47:04.353
1966					0.0	0	0		2023-06-11 03:52:31.269
1979					0.0	0	0		
2014					0.0	0	0		2023-05-12 07:07:29.226
2020					0.0	0	0		2023-06-11 03:56:46.918
2026					0.0	0	0		
2044					0.0	0	0		2023-06-02 20:08:36.174
2052					0.0	0	0		
2079					0.0	0	0		
2105					0.0	0	0		
2144					0.0	0	0		2023-06-11 03:23:57.266
2151					0.0	0	0		2023-06-08 06:58:53.501
2159					0.0	0	0		
2188					0.0	0	0		2023-06-10 15:18:20.994
2191					0.0	0	0		2023-06-09 13:27:22.352
2209					0.0	0	0		
2226					0.0	0	0		
2235					0.0	0	0		2023-06-10 15:54:34.922
2250					0.0	0	0		2023-06-11 04:17:57.216
2298					0.0	0	0		2023-06-11 04:11:09.121
2311					0.0	0	0		2023-06-10 21:54:26.316
2355					0.0	0	0		2023-06-10 07:00:52.563
2391					0.0	0	0		2023-05-13 01:14:54.982
2414					0.0	0	0		2023-06-09 12:04:42.518
2418					0.0	0	0		

Assets Tab

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.

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.

- **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.

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.

The screenshot shows the IBM QRadar Reports interface. The top navigation bar includes links for Dashboard, Overview, Log Activity, Network Activity, Assets, Reports (active), Risks, Vulnerabilities, Admin, Pulse, and Forwarding from Splunk. The system time is 11:49 AM.

On the left sidebar, there are sections for "Reports" and "Branding".

The main area displays a table of reports. At the top, there's a search bar labeled "Group Select a group..." and a link to "Manage Groups". Below the search bar, it says "View the IBM App Exchange for more...".

Report Name	Group	Schedule	Next Run Time	Creation Date	Owner	Author	Generated Reports	Formats
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	None	
						admin	Dec 10, 2018, 2:0	
						admin	Dec 10, 2018, 2:0	
						admin	Dec 10, 2018, 2:0	
						admin	Dec 9, 2018, 2:0	
						admin	Dec 12, 2018, 1:0	

At the bottom, it says "Displaying 1 to 26 of 26 items (Elapsed time: 0:00:02.962)".

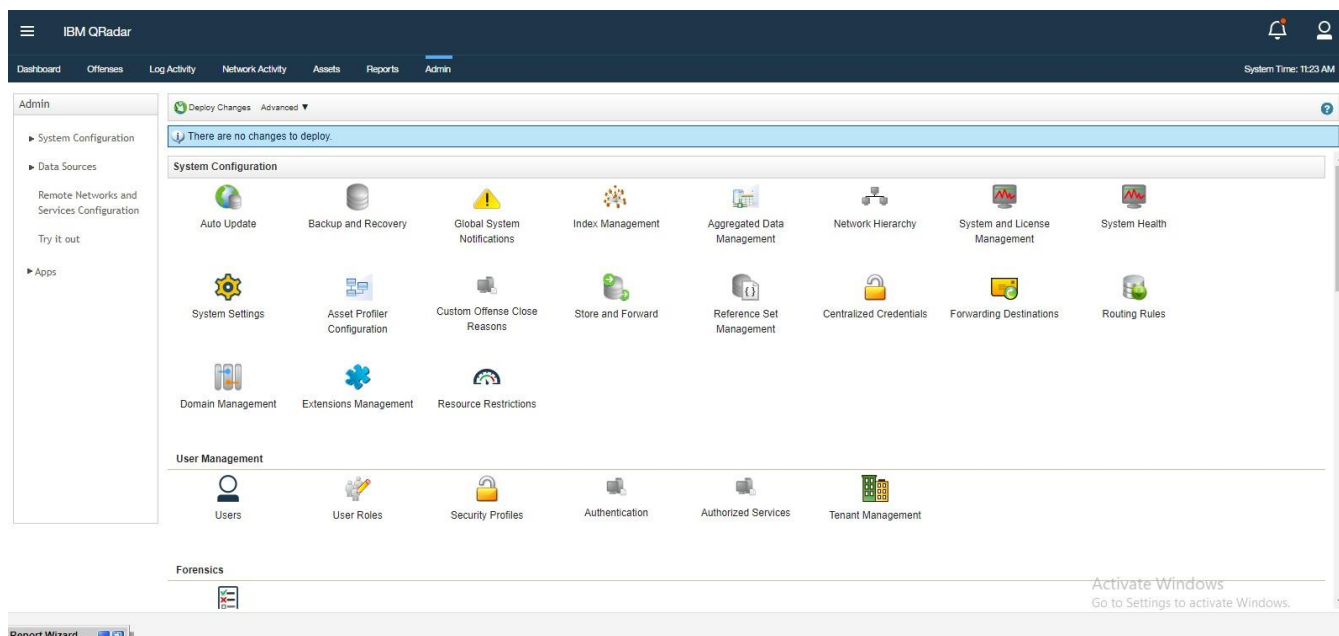
Reports Tab

- **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.



Admin Tab

Chapter 5. Core Module

5.1 Core modules in QRadar SIEM

1. **QRadar Console:** The QRadar Console is the main user interface for managing and configuring the QRadar system. It provides a centralized console for security analysts to monitor security events, investigate incidents, and manage the overall security posture.
2. **QRadar Event Processor:** The Event Processor module collects, normalizes, and processes security event data from various sources, such as logs, network flows, and system events. It performs real-time event correlation, applies rules and policies, and generates alerts for potential security incidents.
3. **QRadar Risk Manager:** The Risk Manager module provides a comprehensive view of an organization's network topology, including routers, switches, and firewalls. It helps security teams assess network vulnerabilities, manage access controls, and identify potential risks and misconfigurations.
4. **QRadar Vulnerability Manager:** The Vulnerability Manager module integrates with vulnerability assessment tools and performs continuous scanning of the network to identify vulnerabilities and potential security risks. It helps organizations prioritize remediation efforts based on the severity of vulnerabilities and provides actionable insights for improving the security posture.
5. **QRadar Flow Processor:** The Flow Processor module collects and analyzes network flow data, providing visibility into network traffic patterns, communication behavior, and network anomalies. It helps detect network-based attacks, monitor bandwidth usage, and identify suspicious or unauthorized network activities.
6. **QRadar QFlow Collector:** The QFlow Collector module captures and analyzes network flow data from routers, switches, and other network devices. It provides detailed insights into network traffic, enabling security teams to identify and investigate anomalous behavior, perform network forensics, and detect advanced threats.
7. **QRadar Data Nodes:** Data Nodes are distributed components of QRadar that store and manage the collected security event and log data. They provide scalability and high-performance data storage capabilities, ensuring that organizations can effectively handle and analyze large volumes of security data.
8. **QRadar Incident Forensics:** The Incident Forensics module allows security analysts to conduct in-depth investigations into security incidents. It captures and retains network

packet data for forensic analysis, helping analysts understand the full scope of an incident, identify attack vectors, and gather evidence for incident response and legal purposes.

9. QRadar Risk Intelligence: The Risk Intelligence module integrates external threat intelligence feeds into the QRadar system. It enriches security event data with up-to-date information on known threats, indicators of compromise, and malicious IP addresses, enhancing the accuracy of threat detection and enabling proactive threat hunting.
10. QRadar Apps: QRadar supports the development and integration of custom applications through its App Framework. QRadar Apps extend the functionality of QRadar by adding additional features, integrations, and customization options based on specific security requirements.

Chapter 6. Performance of the Training work undertaken

6.1 Performance of the Training work undertaken

- We have covered different networking concepts like cryptography, access control, Attacks and exploitation, etc.
- We have learnt about the introduction to various tools like SIEM tool QRadar, introduction to Endpoint Detection and Response, etc.
- Till now, we are working on monitoring QRadar SIEM tool and are generating the practice reports when the alert triggers.

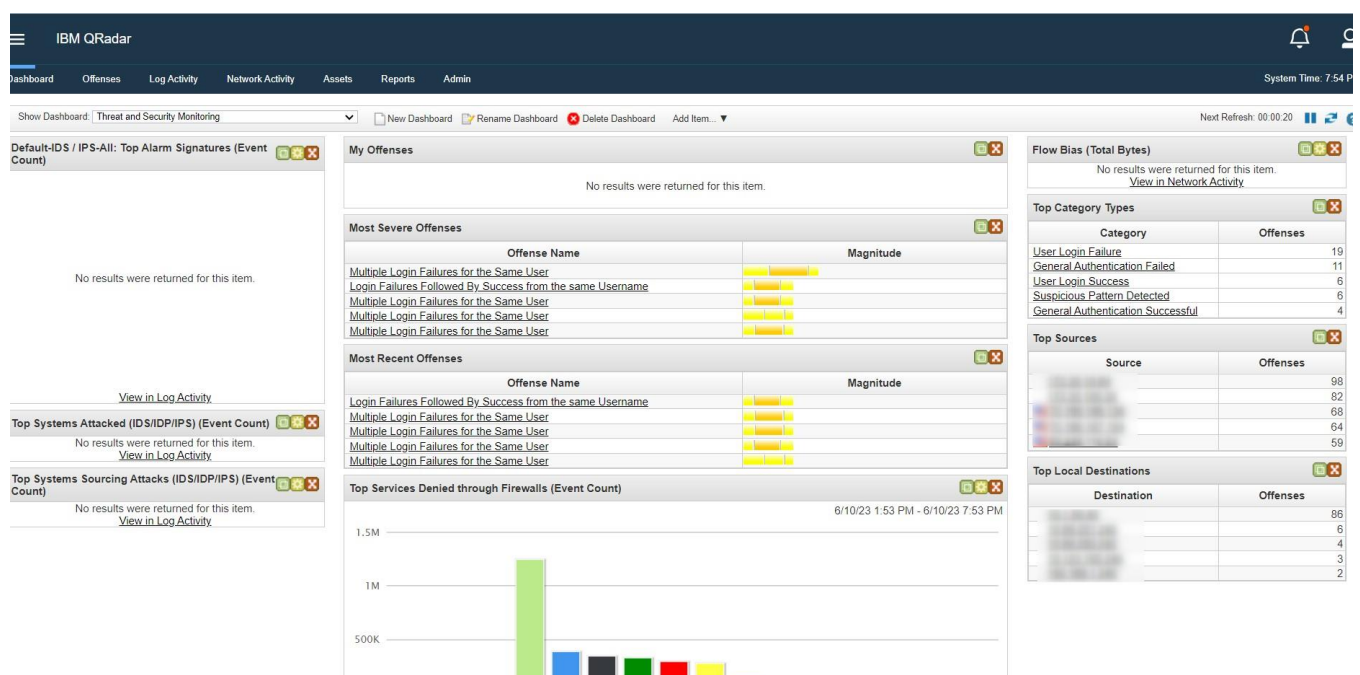
Chapter 7. Output Screens

7.1 Output screen of IBM QRadar

Working of QRadar- A SIEM Tool:

Dashboard Tab:

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



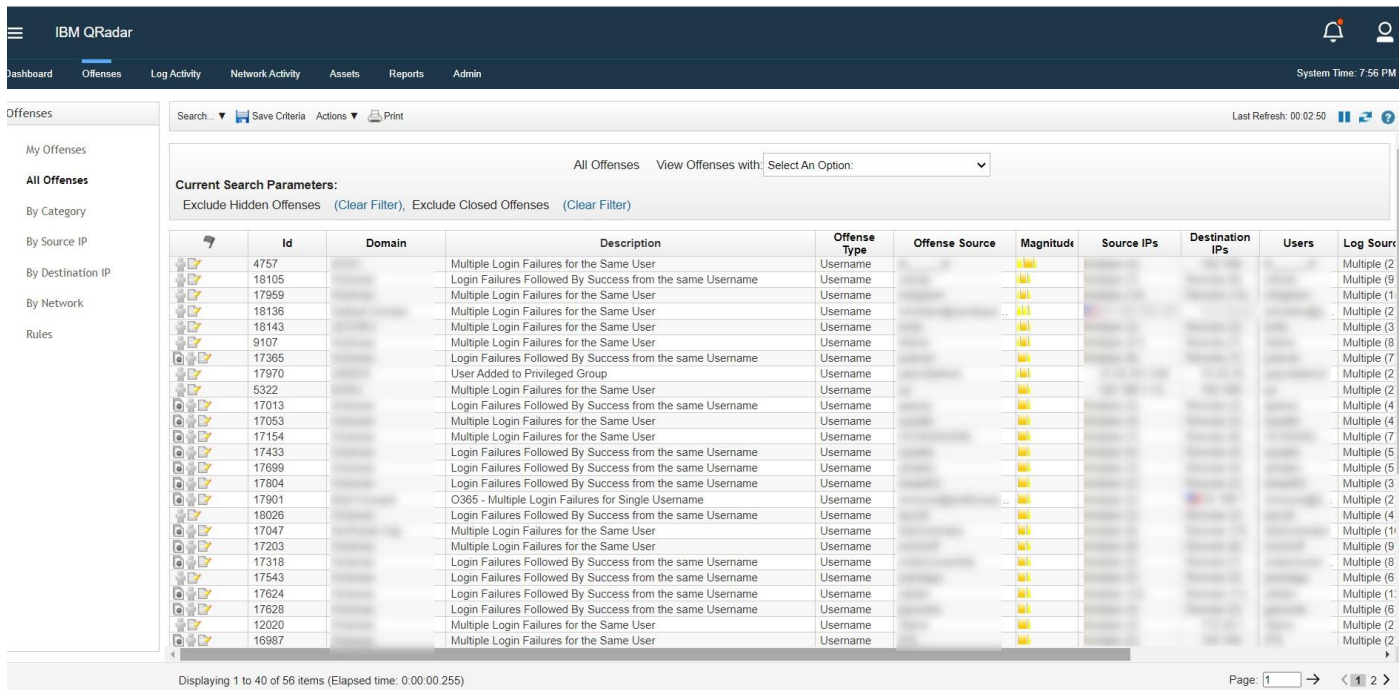
OFFENCES TAB:

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.

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 screenshot shows the IBM QRadar interface with the 'Offenses' tab selected. The left sidebar contains navigation options: 'My Offenses', 'All Offenses', 'By Category', 'By Source IP', 'By Destination IP', 'By Network', and 'Rules'. The main area displays a table of offenses. The table has columns: Id, Domain, Description, Offense Type, Offense Source, Magnitude, Source IPs, Destination IPs, Users, and Log Source. The table shows a list of offenses, many of which are 'Multiple Login Failures for the Same User' or 'Login Failures Followed By Success from the same Username'. The 'Magnitude' column shows values like 1, 2, 3, 4, 5, 6, 7, 8, 9. The 'Log Source' column shows values like 'Multiple (2)', 'Multiple (9)', 'Multiple (1)', 'Multiple (2)', 'Multiple (3)', 'Multiple (8)', 'Multiple (7)', 'Multiple (2)', 'Multiple (2)', 'Multiple (4)', 'Multiple (4)', 'Multiple (7)', 'Multiple (5)', 'Multiple (5)', 'Multiple (3)', 'Multiple (2)', 'Multiple (4)', 'Multiple (1)', 'Multiple (9)', 'Multiple (8)', 'Multiple (6)', 'Multiple (1)', 'Multiple (6)', 'Multiple (2)', 'Multiple (2)'. The bottom of the screen shows 'Displaying 1 to 40 of 56 items (Elapsed time: 0:00:00.255)' and 'Page: 1'.

Id	Domain	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Source
4757		Multiple Login Failures for the Same User	Username		1				Multiple (2)
18105		Login Failures Followed By Success from the same Username	Username		1				Multiple (9)
17959		Multiple Login Failures for the Same User	Username		1				Multiple (1)
18136		Multiple Login Failures for the Same User	Username		1				Multiple (2)
18143		Multiple Login Failures for the Same User	Username		1				Multiple (3)
9107		Multiple Login Failures for the Same User	Username		1				Multiple (8)
17365		Login Failures Followed By Success from the same Username	Username		1				Multiple (7)
17970		User Added to Privileged Group	Username		1				Multiple (2)
5322		Multiple Login Failures for the Same User	Username		1				Multiple (2)
17013		Login Failures Followed By Success from the same Username	Username		1				Multiple (4)
17053		Multiple Login Failures for the Same User	Username		1				Multiple (4)
17154		Multiple Login Failures for the Same User	Username		1				Multiple (7)
17433		Login Failures Followed By Success from the same Username	Username		1				Multiple (5)
17699		Login Failures Followed By Success from the same Username	Username		1				Multiple (5)
17804		Login Failures Followed By Success from the same Username	Username		1				Multiple (3)
17901		O365 - Multiple Login Failures for Single Username	Username		1				Multiple (2)
18026		Login Failures Followed By Success from the same Username	Username		1				Multiple (4)
17047		Multiple Login Failures for the Same User	Username		1				Multiple (1)
17203		Multiple Login Failures for the Same User	Username		1				Multiple (9)
17318		Login Failures Followed By Success from the same Username	Username		1				Multiple (8)
17543		Login Failures Followed By Success from the same Username	Username		1				Multiple (6)
17624		Login Failures Followed By Success from the same Username	Username		1				Multiple (1)
17628		Login Failures Followed By Success from the same Username	Username		1				Multiple (6)
12020		Multiple Login Failures for the Same User	Username		1				Multiple (2)
16987		Multiple Login Failures for the Same User	Username		1				Multiple (2)

Offenses tab showing alerts

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.

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.

Offense 4757 (Summary)

Offense 4757

Summary

Display

Events

Flows

Actions

Print

Magnitude		Status		Relevance	2	Severity	5	Credibility	2
Domain									
Description	Multiple Login Failures for the Same User			Offense Type	Username				
Source IP(s)	Multiple (4)			Event/Flow count	329 521 events and 0 flows in 2 categories				
Destination IP(s)				Start	Jan 14, 2022, 8:51:59 AM				
Network(s)	other			Duration	511d 23h 7m 25s				
				Assigned to					

Offense Source Summary

Username	A__#		
MAC Address	Unknown NIC	Host Name	Unknown
Last Known Host	Unknown	Last Known Machine	Unknown
Last Known MAC	Unknown	Last Known IP	Unknown
Last Observed	Unknown	Last Known Group	Unknown
Offenses	1	Events/Flows	373,970

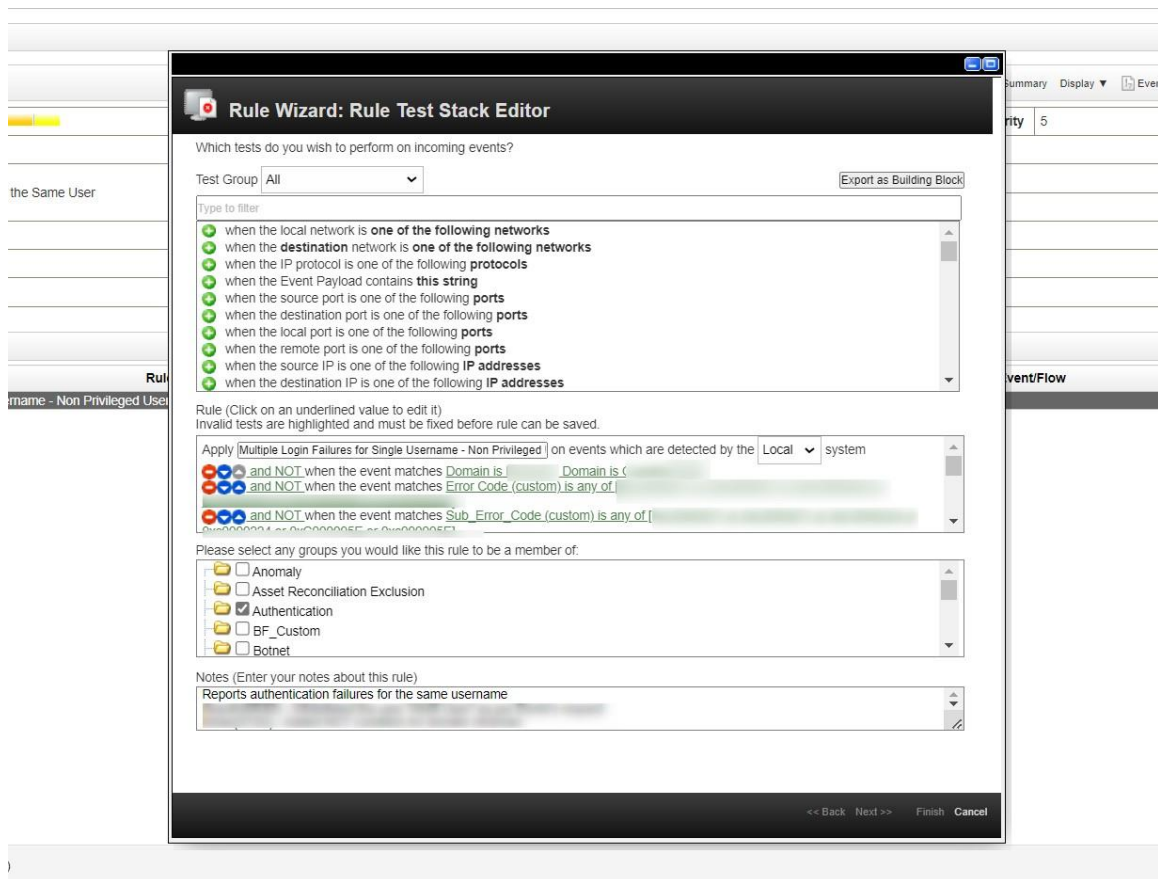
Last 5 Notes

Notes	Username	Creation Date

Last 5 Search Results

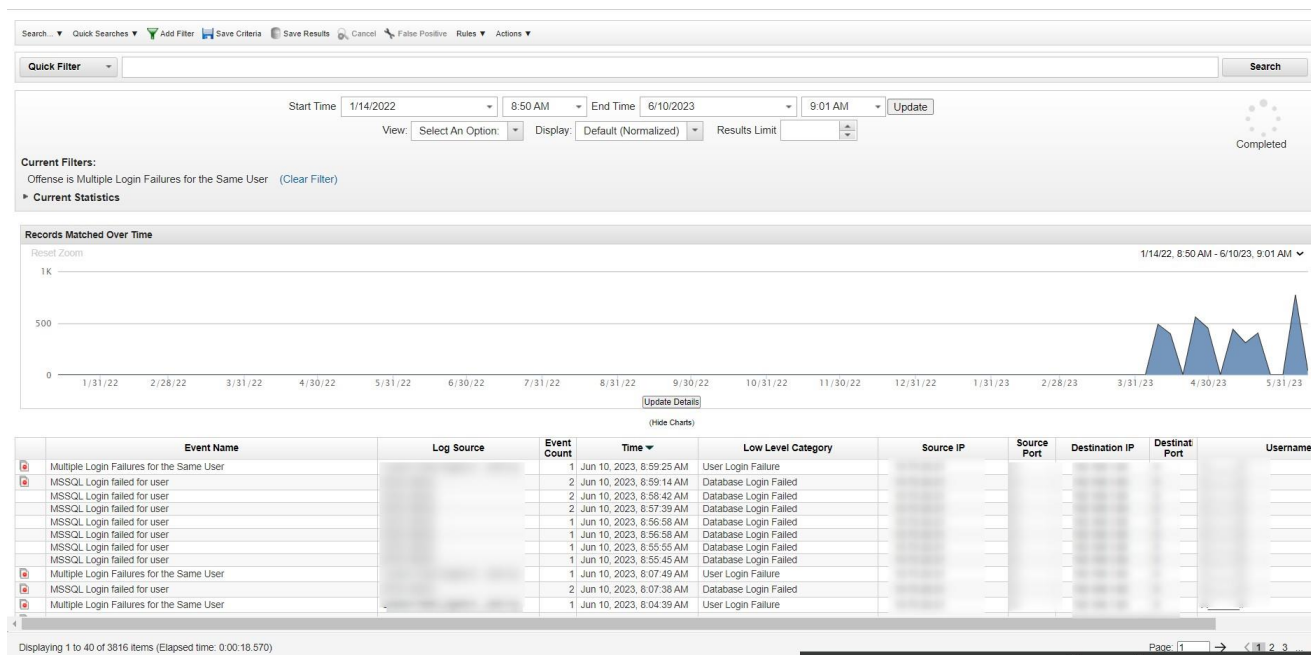
Magnitude	Started On	Ended On	Duration	Events/Flows

Elapsed time: 0 00:00.318



Rule Wizard in QRadar

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



Logs in QRadar

Return to Event List Offense False Positive Extract Property Previous Next Print Obfuscation

Event Information

Event Name	Multiple Login Failures for the Same User								
Low Level Category	User Login Failure								
Event Description	Detected multiple () authentication failures for the same user name in a minute period.								
Magnitude			(5)	Relevance	3	Severity	5	Credibility	7
Username									
Start Time	Jun 10, 2023, 8:59:25 AM			Storage Time	Jun 10, 2023, 8:59:25 AM		Log Source Time	Jun 10, 2023, 8:59:25 AM	
CRE Description (custom)	Detected multiple authentication failures for the same user name in a minute period.								
CRE Name (custom)	Multiple Login Failures for the Same User								
Domain									

Source and Destination Information

Source IP		Destination IP	
Source Asset Name		Destination Asset Name	
Source Port		Destination Port	
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port		Pre NAT Destination Port	
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port		Post NAT Destination Port	
Source IPv6		Destination IPv6	
Source MAC		Destination MAC	

Payload Information

utf hex base64

Wrap Text

Multiple Login Failures for the Same User Detected multiple () authentication failures for the same user name in a minute period.

Event Log Information

References

- [1] IBM QRadar SIEM 7.2 Foundations
- [2] IBM QRadar User Guide
- [3] <https://www.ibm.com/support/>
- [4] https://en.wikipedia.org/wiki/Security_information_and_event_management