# QRadar SIEM RDP Offense Detection Report

*Based on IBM Security Learning Academy Virtual Lab – Course Code: LSL0232X*
**Analyst:** Farah Mae Sumajit
**Role:** Cybersecurity Enthusiast | Entry-Level SOC Analyst
**Completion Date:** May 2025

## 1. Executive Summary

This report outlines the investigation of a suspicious Remote Desktop Protocol (RDP) connection within a simulated Security Operations Center (SOC) environment using IBM QRadar SIEM v7.4.0 FP4. The simulation included detecting offenses, analyzing rule logic, configuring dashboards, writing AQL queries, and generating custom reports. This scenario mirrors a real-world incident response workflow and demonstrates my readiness for SOC operations.

## 2. Investigation Objective

- Detect and investigate suspicious RDP access from a remote IP
- Use Pulse dashboards and AQL to visualize flow data
- Analyze offense rule logic using the Analyst App
- Create report templates based on saved searches
- Update network hierarchy to avoid false positives
- Close and justify the offense after analysis

## 3. Environment and Tools Used

Tool / PlatformVersion / DescriptionIBM QRadar SIEMVersion 7.4.0 FP4 (Simulated)Pulse Dashboard AppFor visual analytics and widget creationAriel Query LanguageFor flow and event log analysisAnalyst AppStreamlined offense triage UICentOS ClientGUI for analyst console access

## 4. Offense Summary

- **Offense ID:** 2
- **Name:** Remote Desktop Access from the Internet
- **Source IP:** 195.54.160.21
- **Destination IP:** 192.168.10.12
- **Protocol:** TCP/3389 (RDP)
- **Category:** Remote Access Violation
- **Trigger Rule: Remote: Remote Desktop Access from the Internet**

## 5. Analytical Actions Performed

### 🔎 Exercise-Based Actions

#Task1Logged into the QRadar Console and reviewed dashboards2Created a new custom dashboard "Watch" and added Flow Bias item3Used QFlow to monitor flow biases (Mostly In, Mostly Out, etc.)4Opened Pulse App, created “Flow Bias” widget with AQL query5Investigated the RDP offense using the Offense tab and Rule Wizard6Reviewed Rule Test Stack and actions triggered by offense7Analyzed same offense using the Analyst App (new UI)8Wrote and executed AQL to monitor RDP traffic9Saved the RDP flow query as a search and added it to the dashboard10Created a PDF report template titled “RDP to My Server”11Updated Network Hierarchy to mark source IP as internal12Closed the offense and documented it as a false positive13Explored additional QRadar tabs (Log Activity, Network Activity, Assets)

## 6. AQL Queries Used

```
-- Pulse Dashboard Widget (Flow Bias) SELECT starttime AS Time, flowbias AS
'Flow Bias',  long(SUM(sourcebytes+destinationbytes)) AS 'TotalBytes'  FROM
flows  GROUP BY Time/60000  ORDER BY Time LAST 1 HOURS;  -- Search for RDP
Traffic SELECT * FROM flows  WHERE destinationport = 3389  LAST 2 HOURS;
```

## 7. Findings & Justification

- Offense was triggered due to **remote RDP traffic** from IP **195.54.160.21**.
- Upon investigation, the source IP was identified as part of internal operations ( Jumpbox.Support).
- The offense was a **false positive** caused by a missing internal network entry in the hierarchy.
- Adding the IP/subnet to **Network Hierarchy** resolved the issue.

## 8. Report Generation

- A **report template** titled "RDP to My Server" was created using the saved search.
- The report included:
  - **Chart View**: Flow volume by time
  - **Table View**: Flow details grouped by source IP
- Format: PDF
- Group: Usage Monitoring
- Frequency: Manual (can be automated in production)

## 9. Conclusion

This simulation demonstrates the core responsibilities of a SOC analyst using QRadar SIEM: offense detection, triage, dashboard creation, network tuning, and reporting. These skills are essential in responding to real-world threats and aligning security operations with compliance standards.