

# Windows log

## 1. Introduction

In this report, we aim to demonstrate how to collect and monitor Windows system logs using Sysmon and WinCollect, and forward them to IBM QRadar SIEM for centralized log analysis and threat detection.

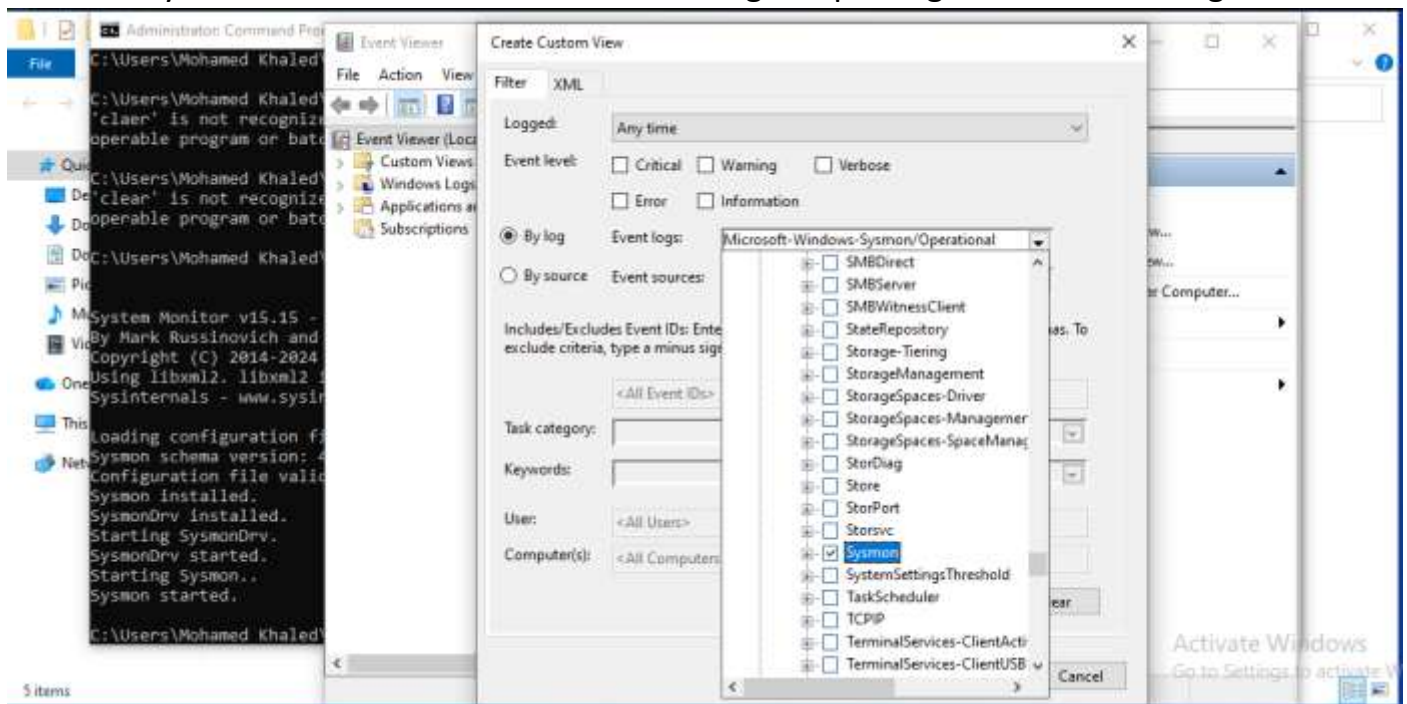
## 2. Tools Used

Sysmon (System Monitor): A Windows system service and device driver that logs detailed system activities into the Windows Event Log.

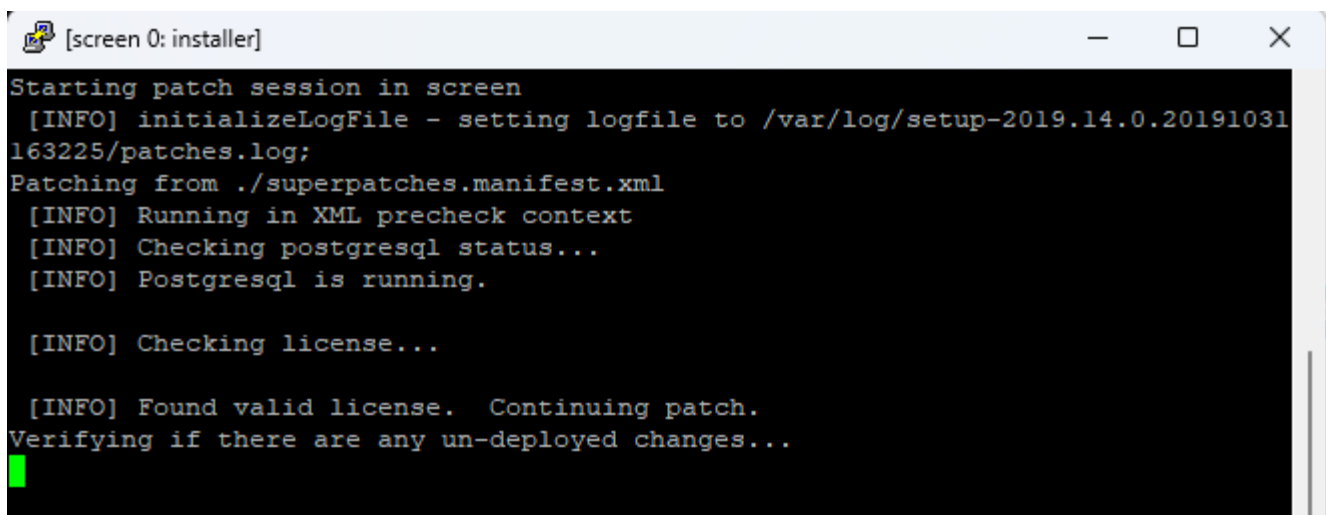
WinCollect: An IBM agent used to collect Windows logs and forward them to QRadar.

## 3. Implementation Steps

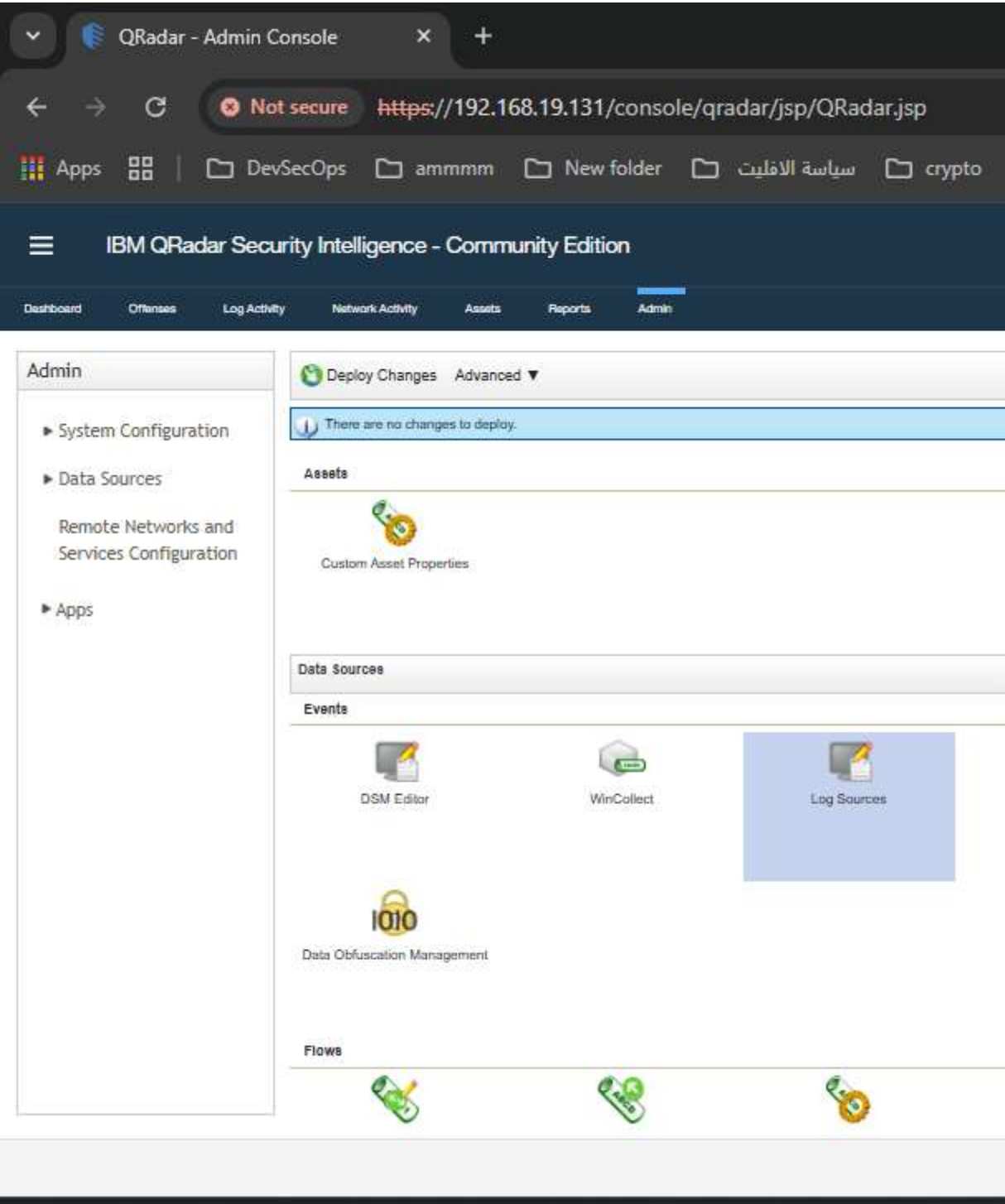
Installed Sysmon on the Windows machine to begin capturing detailed event logs.



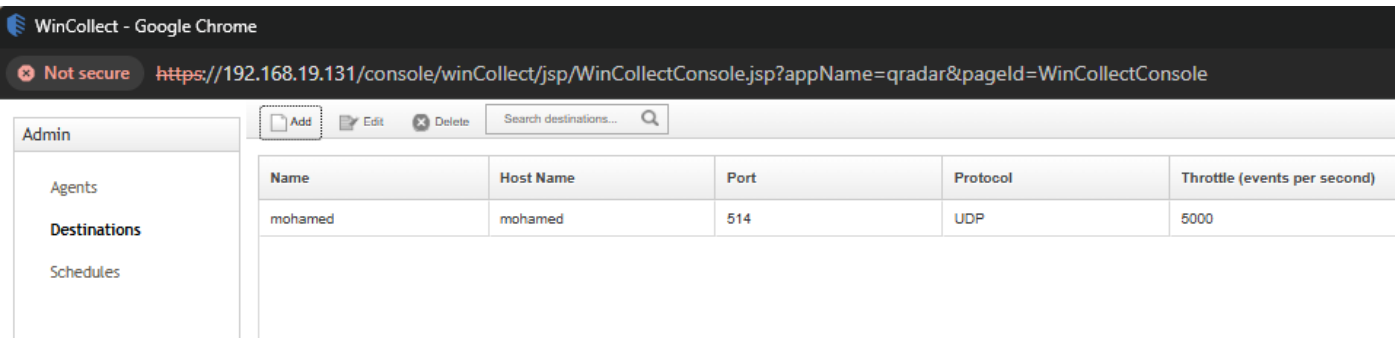
Installed WinCollect on the QRadar virtual machine by uploading the SFS installation package and completing the setup process.



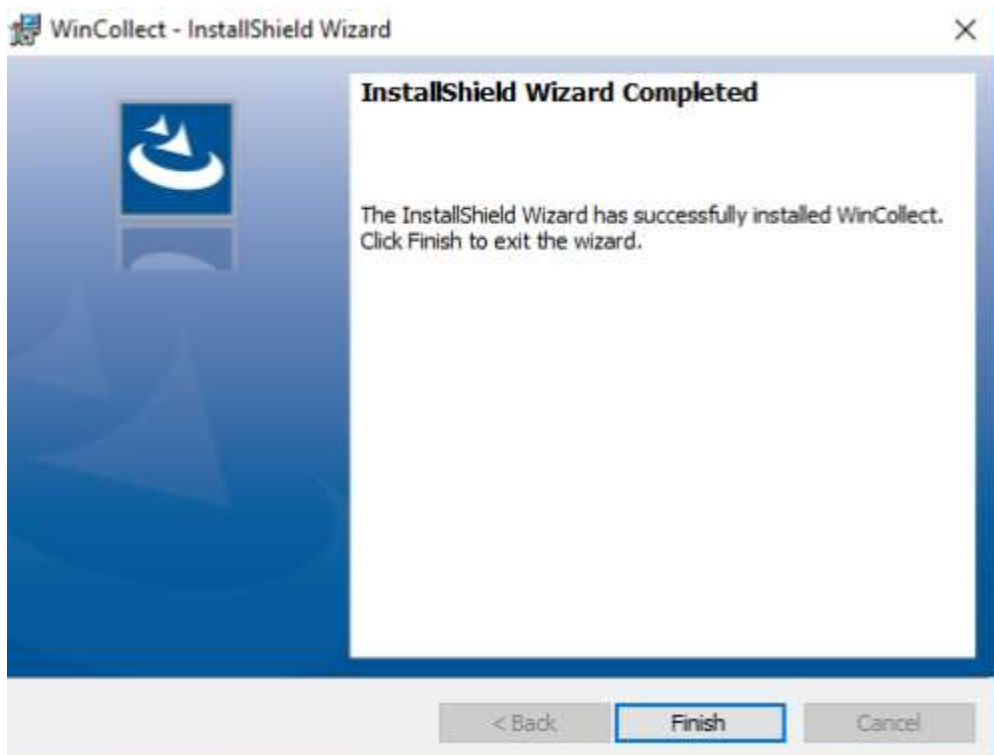
In QRadar, created a Destination to define where the collected logs will be sent.



Opened the WinCollect tab that appeared after installation and configured it to link with the created destination.



On the Windows machine (the log source), configured the WinCollect agent to connect to QRadar and send logs to the defined destination.



Verified that Windows event logs are successfully arriving in QRadar through the Log Activity tab.

The screenshot shows the IBM QRadar Security Intelligence - Community Edition interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity' (selected), 'Network Activity', 'Assets', 'Reports', and 'Admin'. Below the navigation bar is a search and filter section with options like 'Search...', 'Quick Searches', 'Add Filter', 'Save Criteria', 'Save Results', 'Cancel', 'False Positive', 'Rules', and 'Actions'. A 'Quick Filter' dropdown is also present. The main content area displays a table of log events. The table has columns for 'Event Name', 'Log Source', 'Event Count', 'Time', and 'Low Level Category'. The events listed include 'Information Message', 'Success Audit: A logon was successful using explicit...', 'Success Audit: An account was logged off', 'Success Audit: Successful logon with administrative ...', 'Success Audit: An account was successfully logged on', and several 'Information Message' entries. The log sources are 'System Notification-2 :: localdomainin' and 'Windows 10 pro'. The event counts are all '1'. The times are in ISO 8601 format. The low level categories are 'Information', 'User Login Success', 'Host Logout', 'Admin Login Successful', and 'User Login Success'.

Event Name	Log Source	Event Count	Time	Low Level Category
Information Message	System Notification-2 :: localdomainin	1	2023-10-10T10:10:10.000Z	Information
Information Message	System Notification-2 :: localdomainin	1	2023-10-10T10:10:10.000Z	Information
Success Audit: A logon was successful using explicit...	Windows 10 pro	1	2023-10-10T10:10:10.000Z	User Login Success
Success Audit: An account was logged off	Windows 10 pro	1	2023-10-10T10:10:10.000Z	Host Logout
Success Audit: Successful logon with administrative ...	Windows 10 pro	1	2023-10-10T10:10:10.000Z	Admin Login Successful
Success Audit: An account was successfully logged on	Windows 10 pro	1	2023-10-10T10:10:10.000Z	User Login Success
Information Message	System Notification-2 :: localdomainin	1	2023-10-10T10:10:10.000Z	Information
Information Message	System Notification-2 :: localdomainin	1	2023-10-10T10:10:10.000Z	Information
Information Message	System Notification-2 :: localdomainin	1	2023-10-10T10:10:10.000Z	Information
Information Message	System Notification-2 :: localdomainin	1	2023-10-10T10:10:10.000Z	Information

## 4. Results

Logs from the Windows system were successfully forwarded to QRadar.

Sysmon provided detailed logs about process creation, network connections, and registry changes.

WinCollect ensured reliable communication between the Windows host and QRadar.