Windows log

1. Introduction

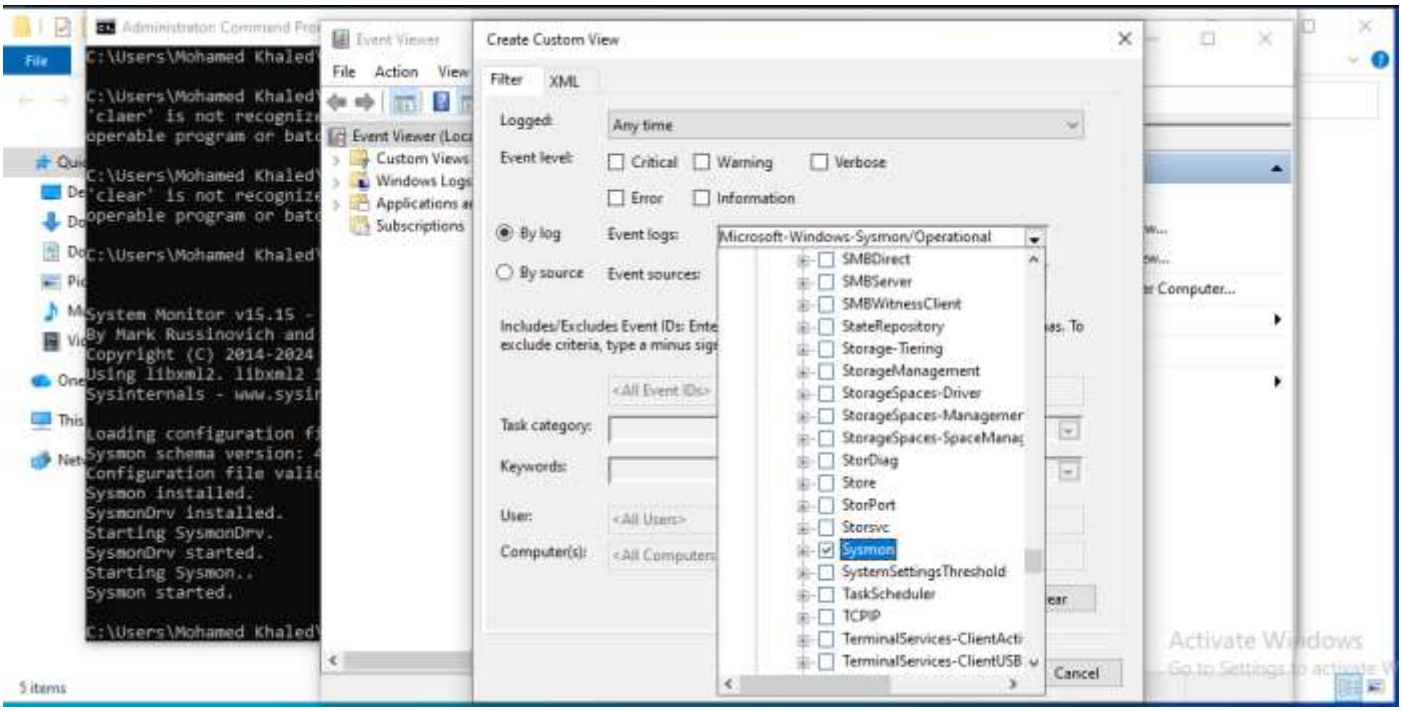
In this report, we aim to demonstrate how to collect and monitor Windows system logs using Sysmon and WinCollect, and forward them to IBM QRadar SIEM for centralized log analysis and threat detection.

2. Tools Used

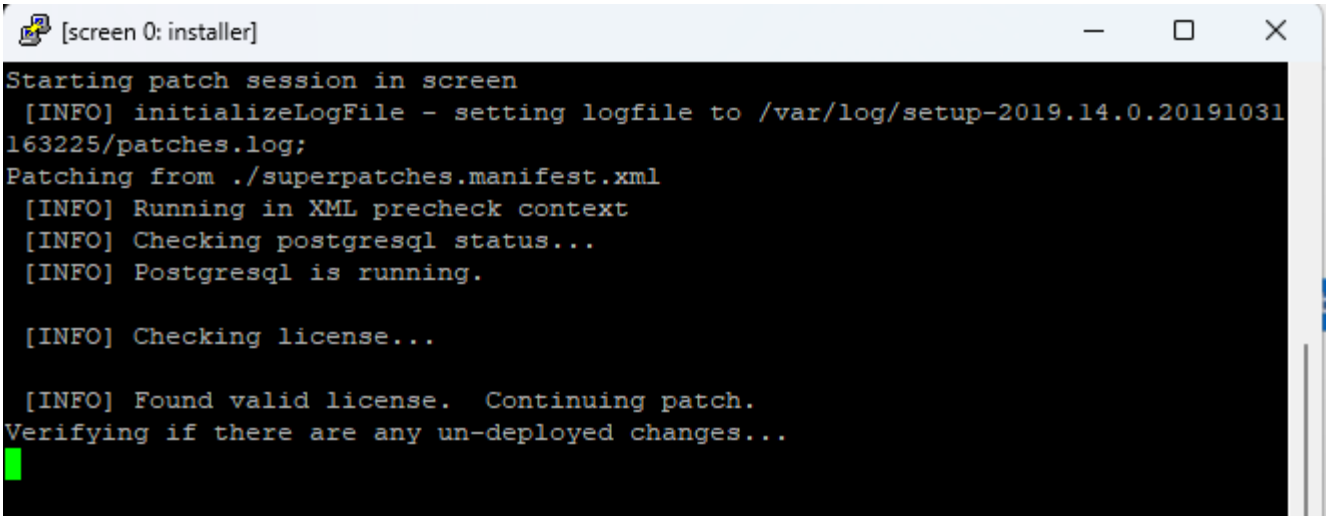
Sysmon (System Monitor): A Windows system service and device driver that logs detailed system activities into the Windows Event Log.
WinCollect: An IBM agent used to collect Windows logs and forward them to QRadar.

3. Implementation Steps

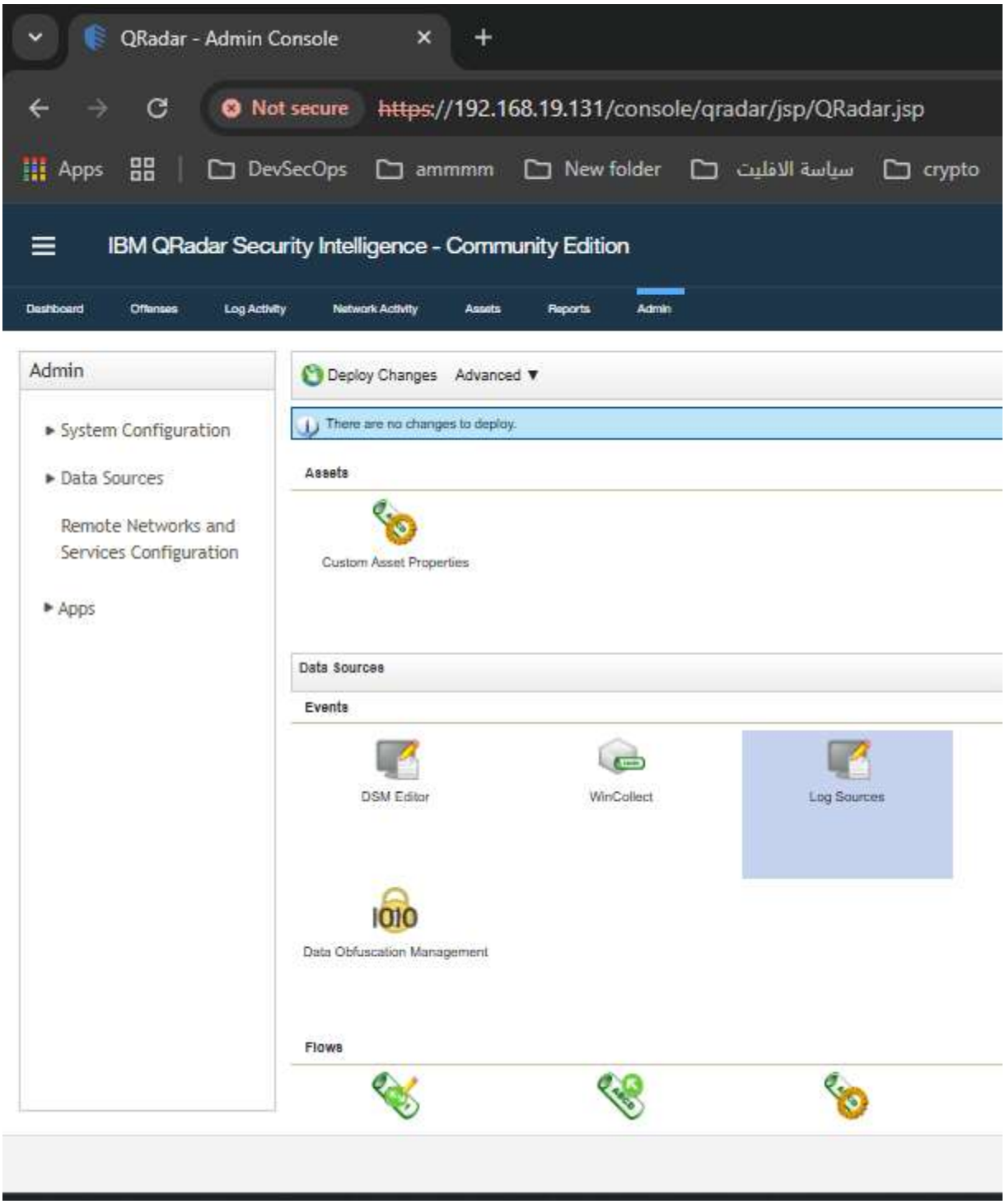
Installed Sysmon on the Windows machine to begin capturing detailed event logs.



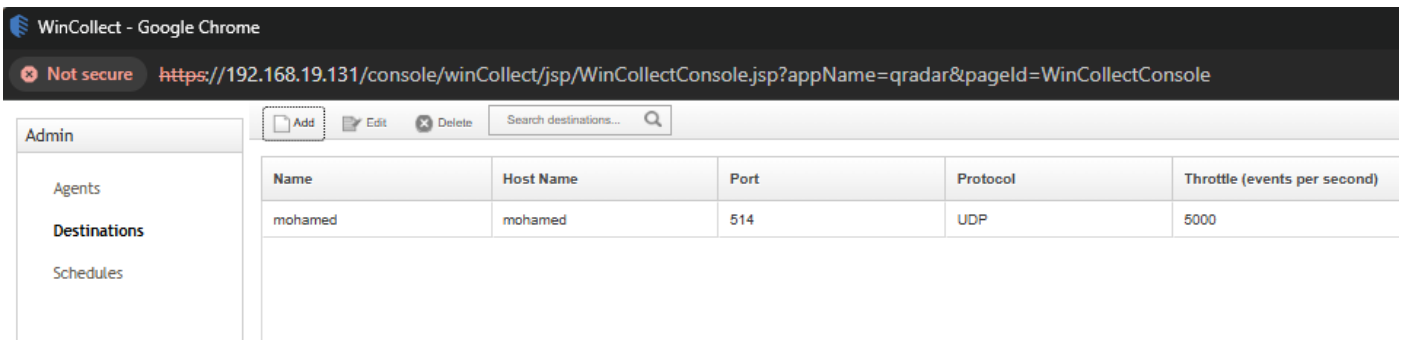
Installed WinCollect on the QRadar virtual machine by uploading the. SFS installation package and completing the setup process.



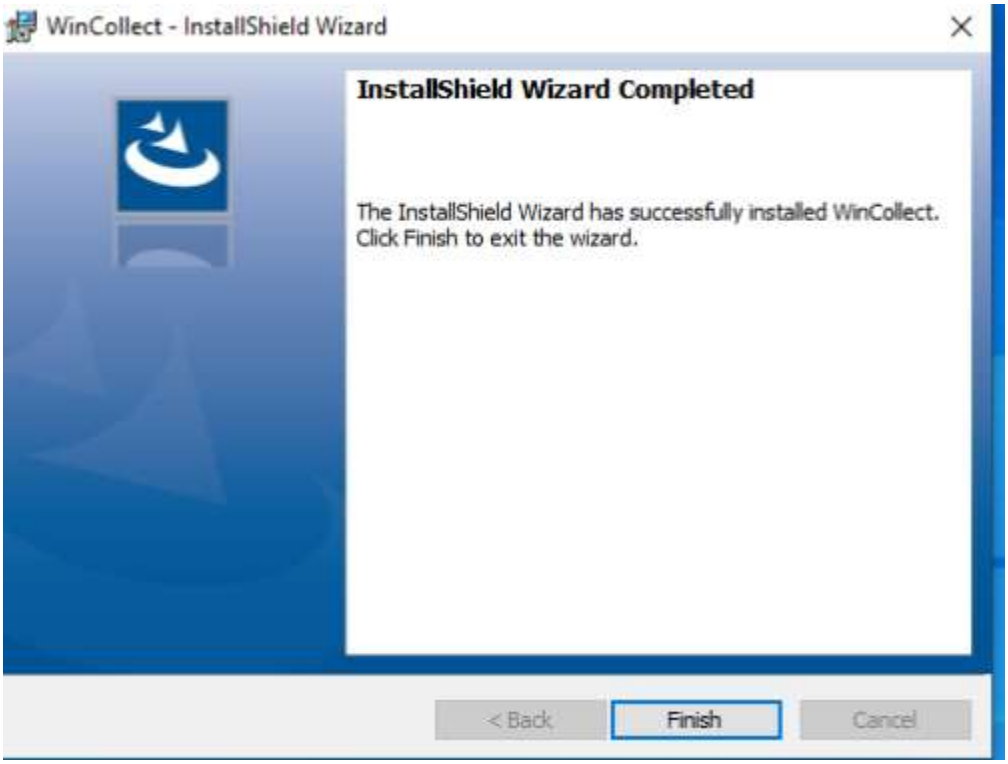
In QRadar, created a Destination to define where the collected logs will be sent.



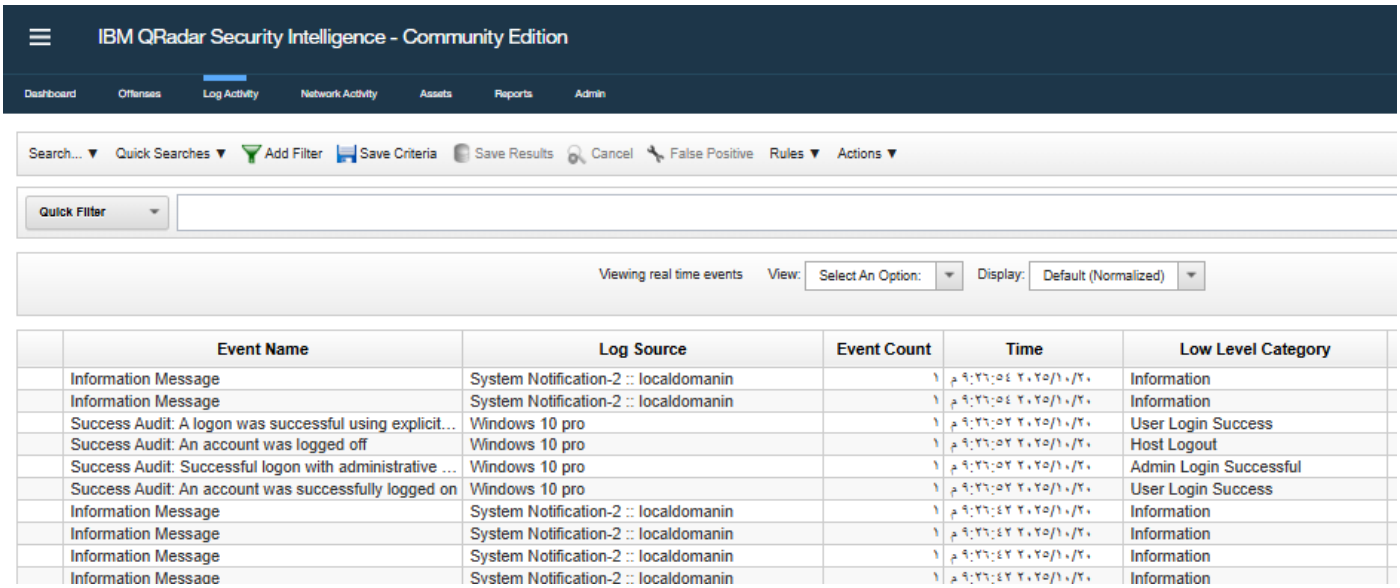
Opened the WinCollect tab that appeared after installation and configured it to link with the created destination.



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.



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.