**SOC ANALYST TRANING REPORT**

ON

# EVENT VIEWER AUDIT REPORT

ANALYSED AND REPORTED

BY

**ALI CHINASA JULIET**

**INSTRUCTOR:** MR OLA OLAITAN

**DATE:** September 2024

## EXECUTIVE SUMMARY

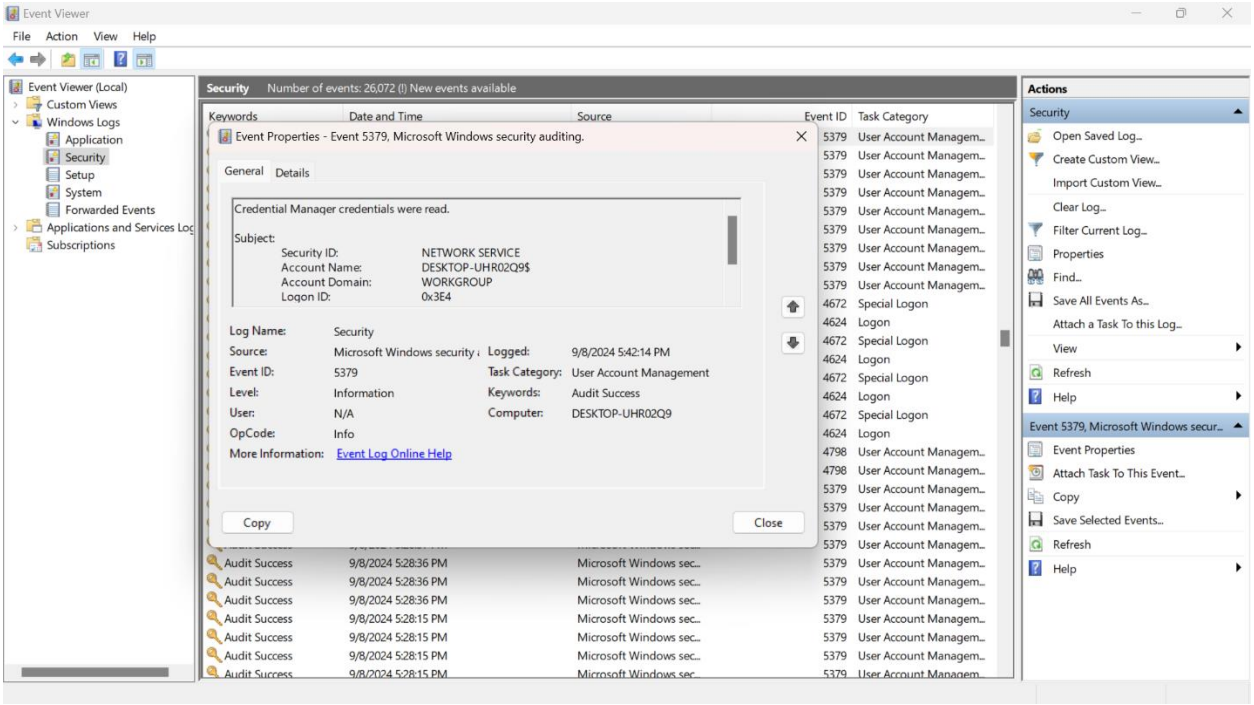
This report evaluates five different Event IDs from the Event Viewer to determine the host device's security status. Determining potential security risks or vulnerabilities is the goal. Analysis showed no dangers associated with unsuccessful login attempts or illegal access to private data. The fact that every audit was completed successfully shows that the host device is functioning within safe bounds. Nonetheless, suggestions are given to preserve this degree of security and guarantee ongoing defense against potential dangers.

## INTRODUCTION

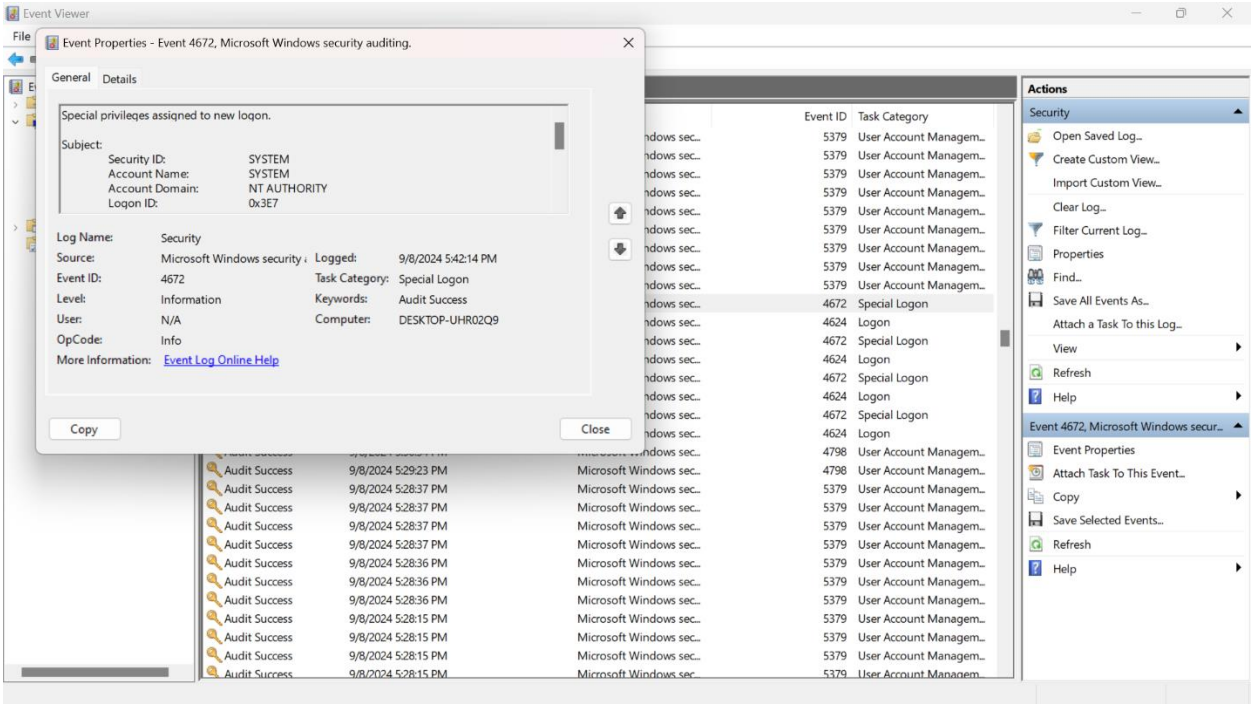
The Event Viewer is an essential tool for SOC analysts to monitor and audit system activity. By monitoring events linked to system faults, protected file access, logon attempts, and other associated activities, it assists in identifying security lapses, misconfigurations, or other vulnerabilities. In order to evaluate a host device's security posture and pinpoint any possible security issues, I examined five distinct event IDs in this report.

## ANALYSIS OF THE EVENT IDs

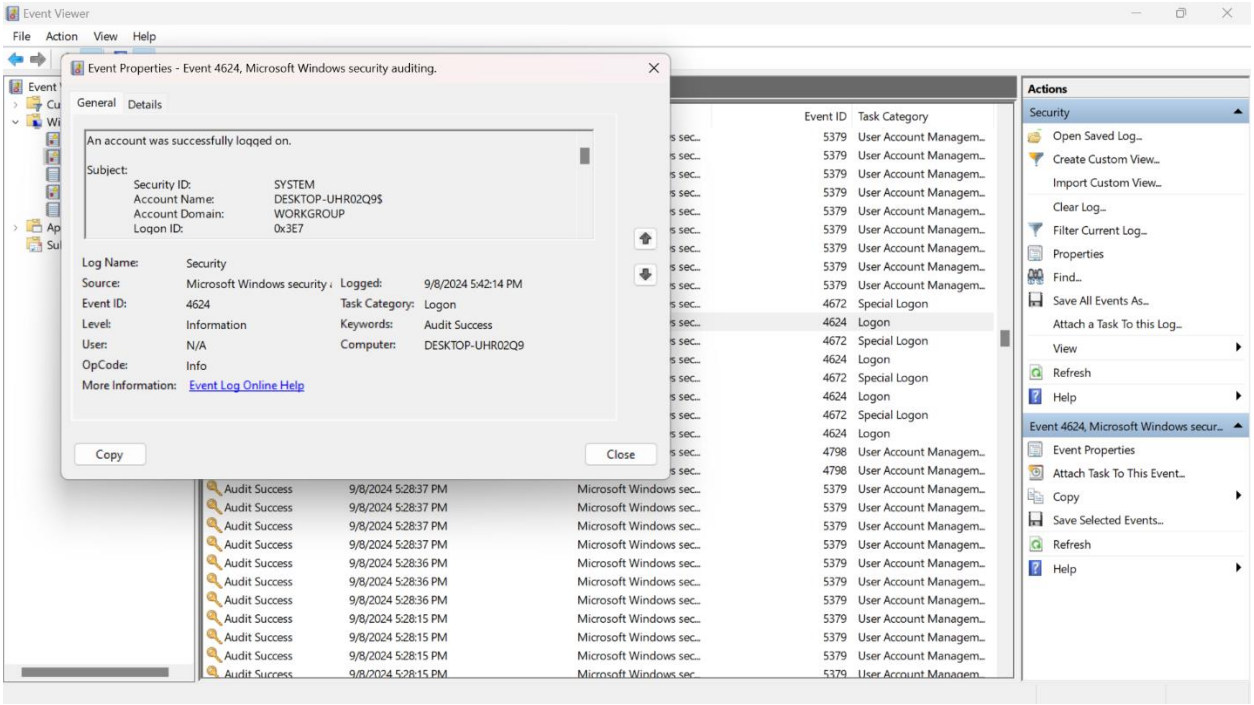
**1. Event ID: 5379**
Task Category: User Account Management
Security ID: NETWORK SERVICE
Account name: DESKTOP-UHR02Q9$
Date: 9/08/2024 5:42:14 PM
Keywords: Audit Success
Credential Manager credentials were successful



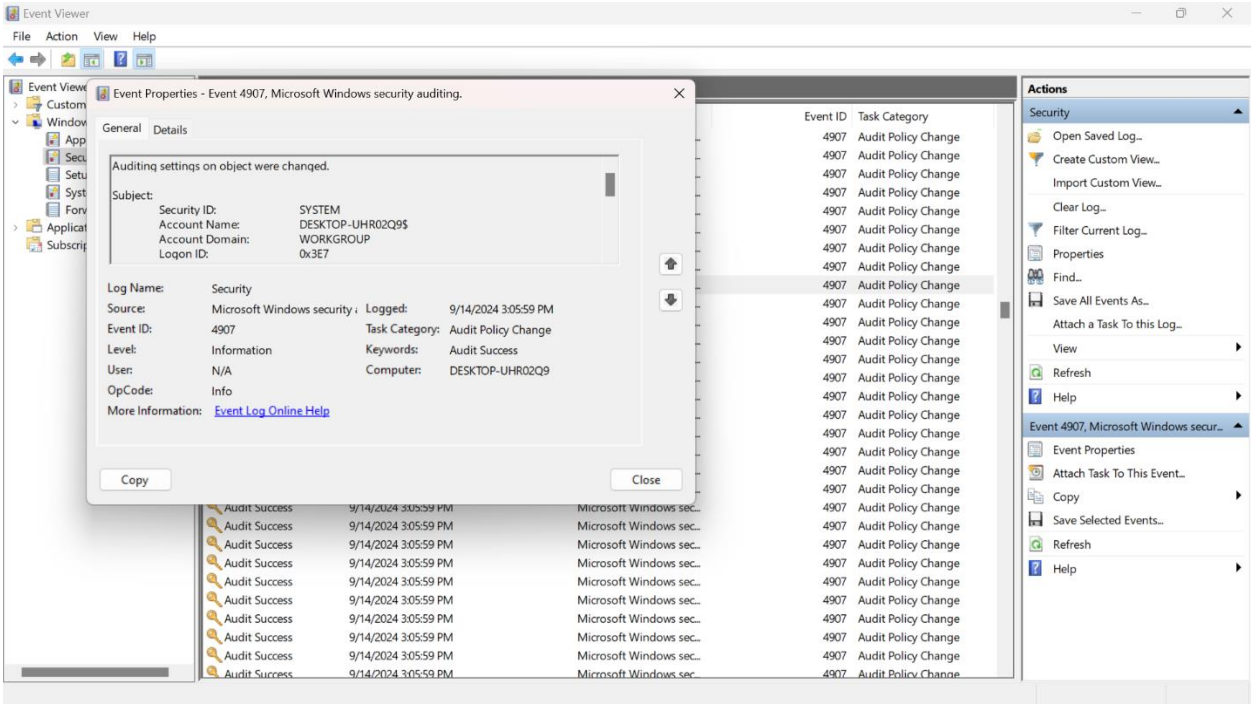

**2. Event ID: 4672**
Task Category: Special Logon
Security ID: SYSTEM
Account name: SYSTEM
Date: 9/08/2024 5:42:14 PM
Keywords: Audit Success
Credential Manager credentials were successful



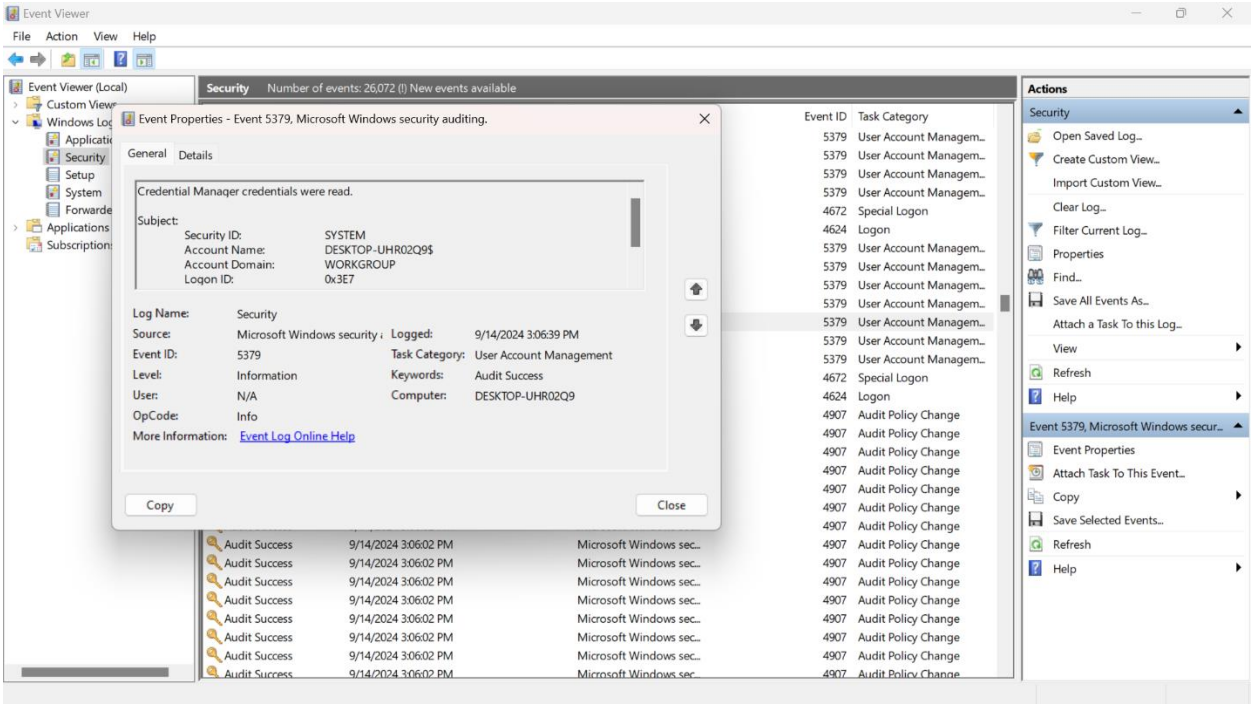

**3. Event ID: 4624**
Task Category: Logon
Security ID: SYSTEM
Account name: DESKTOP-UHR02Q9$
Date: 9/08/2024 5:42:14 PM
Keywords: Audit Success
Credential Manager credentials were successful




**4. Event ID: 4907**
Task Category: Audit Policy Change
Security ID: SYSTEM
Account name: DESKTOP-UHR02Q9$
Date: 9/14/2024 3:05:59 PM
Keywords: Audit Success
Credential Manager credentials were successful




**5. Event ID: 5379**
Task Category: User Account Management
Security ID: SYSTEM
Account name: DESKTOP-UHR02Q9$
Date: 9/08/2024 3:06:39 PM
Keywords: Audit Success
Credential Manager credentials were successful




## CONCLUSION

No serious security flaws or risks were found during the Event Viewer's event log analysis. Every audit, including file access, system activity, and logon attempts, was completed successfully and showed no evidence of unauthorized activity or suspicious behavior. This implies that the host device is working effectively and that the security strategies already in place are functional.

## RECOMMENDATION

Recommendation includes keeping up-to-date security rules, making sure security patches are updated on time, and carrying out routine event log monitoring to spot any irregularities fast. For future reference, audit logs should be regularly backed up. To reduce risks, user awareness training on security best practices should also continue.