Detecting Privilege Escalation via Windows Administrative Group Changes

By Adam Mohmoud

The goal of this lab is to detect unauthorized privilege escalation by identifying accounts added to privileged Windows groups, specifically local administrative groups, using Windows Security Event Logs and Splunk SPL.

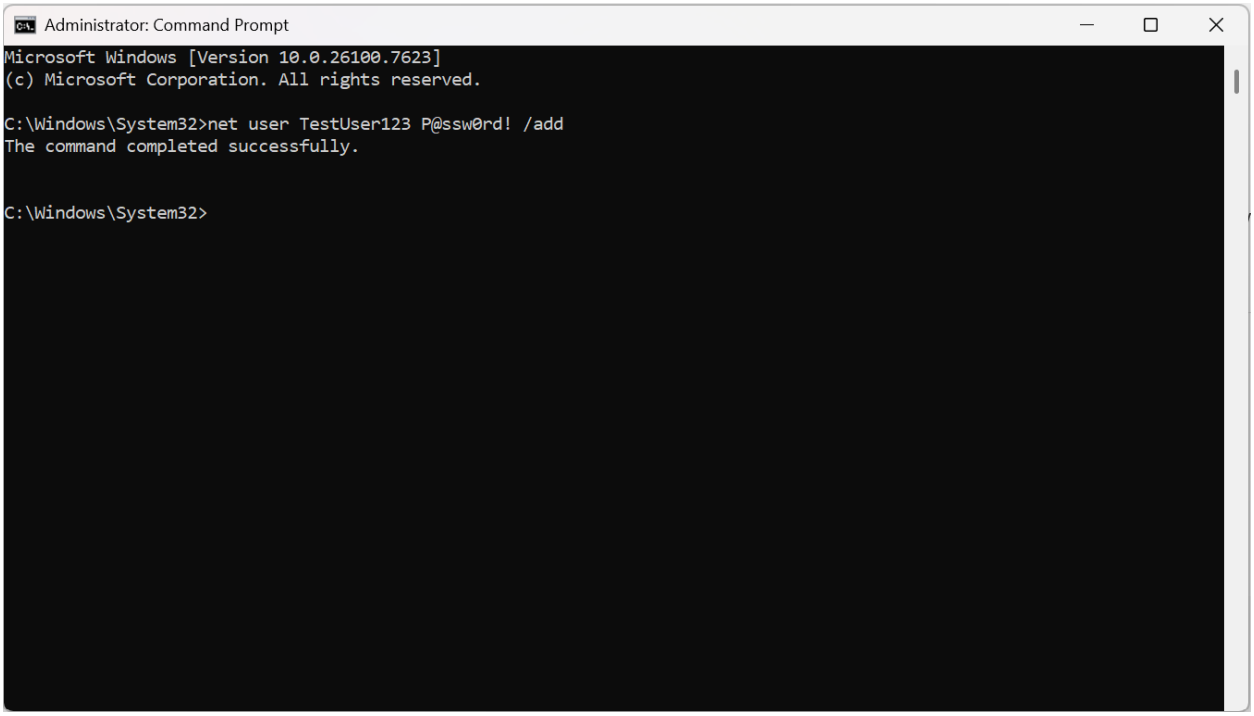
Tools & Environment:

- Windows 11 (Home Edition)
- Command Prompt (Administrator)
- Data ingestion via CSV upload
- Splunk Enterprise

MITRE ATT&CK Mapping

- T1078 – Valid Accounts
- T1068 – Privilege Escalation

Step 1: Created a Test User (Command Prompt)




```
net user TestUser123 P@ssw0rd! /add
```

This creates a local user account to simulate privilege escalation.

Field	Value
Event ID	4732
Description	A member was added to a security-enabled local group
Subject	Account that ran the command
Member Name	TestUser123
Group	Administrators

Step 2: Add the User to the Local Administrators Group

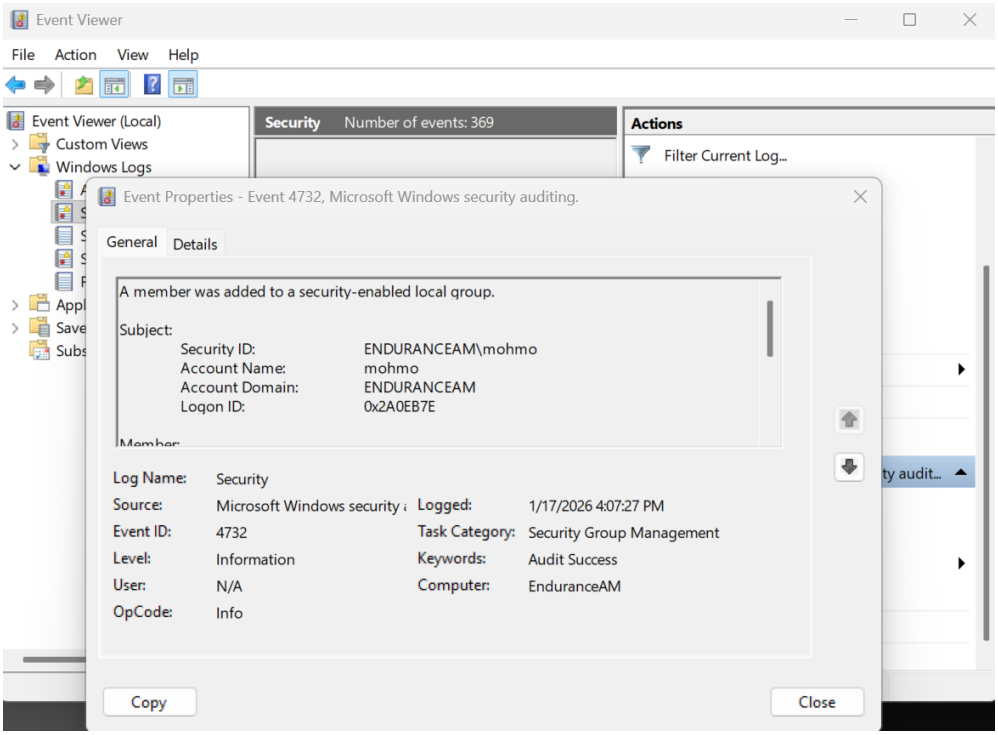
User added to Administrators that will generate **event 4732**:

```
net localgroup administrators Testuser123 /add
```

This action simulates privilege escalation and triggers a Windows Security event.

Step 3: Verify Event 4732 in Event Viewer

Windows logs → Security → Filter current log '4732'



Step 4: Export Event to CSV and Upload to Splunk

The log was still filtered to 4732 and saved as ‘privilege_escalation_4732.csv’; uploaded to Splunk to complete ingestion.

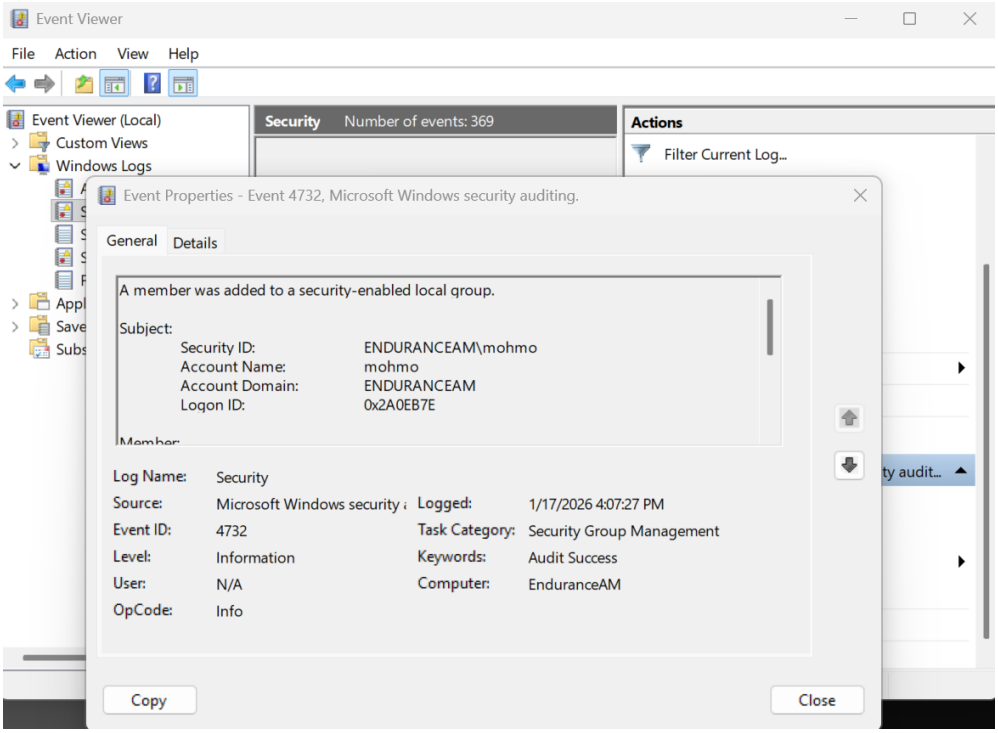
Step 5: Confirm Data Ingestion in Splunk and Build Privilege Escalation Detection Search

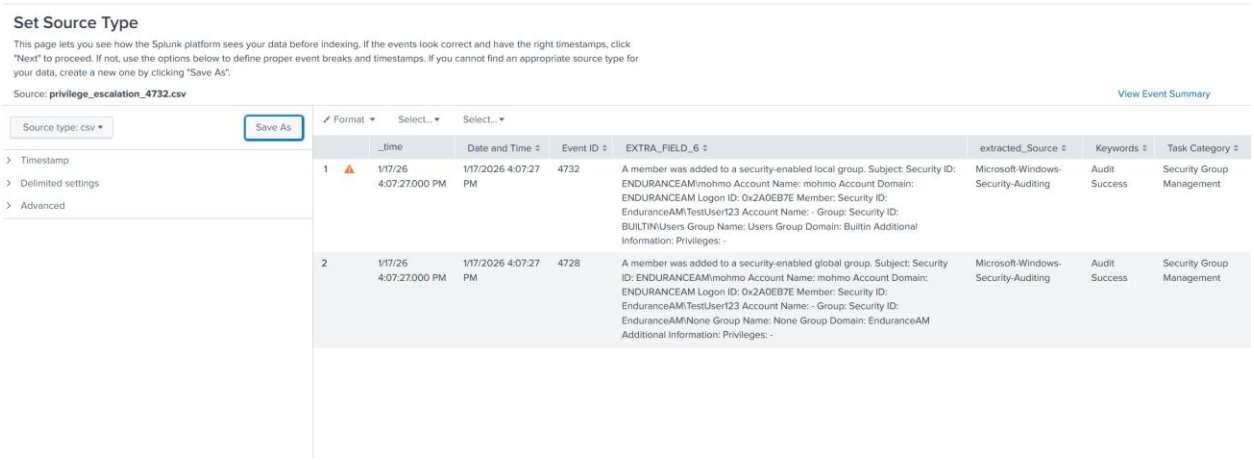
SPL - *index=windows EventCode IN (4728,4732)*

```
| stats count by Subject_Account_Name Target_Account_Name host
| sort – count
```

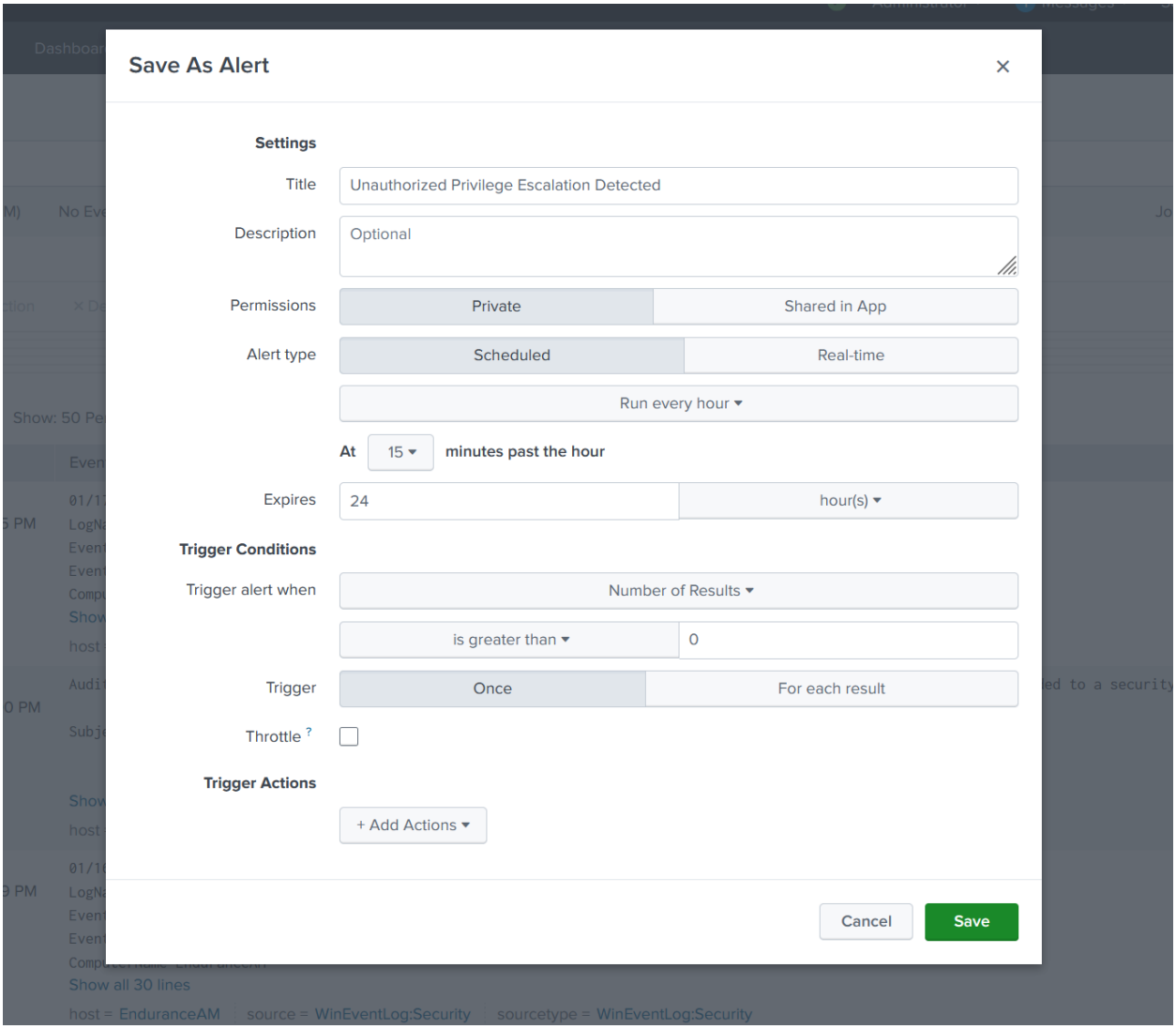
The Detection Logic:

- Identifies who performed the group change
- Identifies who received elevated privileges
- Displays affected hosts
- Highlights repeated or suspicious activity


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Security Number of events: 369
Actions
Filter Current Log...
Event Properties - Event 4732, Microsoft Windows security auditing.
General Details
A member was added to a security-enabled local group.
Subject:
Security ID: ENDURANCEAM\mohmo
Account Name: mohmo
Account Domain: ENDURANCEAM
Logon ID: 0x2A0EB7E
Log Name: Security
Source: Microsoft Windows security
Logged: 1/17/2026 4:07:27 PM
Event ID: 4732
Task Category: Security Group Management
Level: Information
Keywords: Audit Success
User: N/A
Computer: EnduranceAM
OpCode: Info
Copy
Close


Set Source Type
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".
Source: privilege_escalation_4732.csv
View Event Summary
Source type: csv
Save As
Timestamp
Delimited settings
Advanced
Format
Select...
Select...
_time
Date and Time
Event ID
EXTRA_FIELD_6
extracted_Source
Keywords
Task Category
1
1/17/26 4:07:27.000 PM
1/17/2026 4:07:27 PM
4732
A member was added to a security-enabled local group. Subject: Security ID: ENDURANCEAM\mohmo Account Name: mohmo Account Domain: ENDURANCEAM Logon ID: 0x2A0EB7E Member: Security ID: EnduranceAM\TestUser123 Account Name: - Group: Security ID: BUILTIN\Users Group Name: Users Group Domain: Builtin Additional Information: Privileges: -
Microsoft-Windows-Security-Auditing
Audit Success
Security Group Management
2
1/17/26 4:07:27.000 PM
1/17/2026 4:07:27 PM
4728
A member was added to a security-enabled global group. Subject: Security ID: ENDURANCEAM\mohmo Account Name: mohmo Account Domain: ENDURANCEAM Logon ID: 0x2A0EB7E Member: Security ID: EnduranceAM\TestUser123 Account Name: - Group: Security ID: EnduranceAM\None Group Name: None Group Domain: EnduranceAM Additional Information: Privileges: -
Microsoft-Windows-Security-Auditing
Audit Success
Security Group Management

Step 6: Create A Splunk Alert



Unauthorized Privilege Escalation Detected

Enabled: ..... Yes. Disable
App: ..... search
Permissions: ..... Private. Owned by shadowsun. Edit
Modified: ..... Jan 17, 2026 7:05:22 PM
Alert Type: ..... Scheduled. Hourly, at 15 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 0. Edit
Actions: ..... 1 Action Edit
Add to Triggered Alerts