Windows Event Log Analysis Lab. Building a timeline from Security.evtx

Overview

In this lab I analyzed Windows Security event logs to investigate after hours administrator activity and determine whether a new account was created, elevated, and then used. The goal was to produce an audit ready timeline where every conclusion is tied to a specific Windows event record.

SOC handoff summary

Classification: Suspicious account lifecycle activity
Severity: High
Confidence: High
Core finding: A new local user account was created, added to high privilege groups, then used to log on successfully
Primary evidence: Windows Security Event IDs 4720, 4732, 4624, plus privileged session context from 4672

Environment and data source

Primary tool: Windows Event Viewer
Primary log: Security.evtx

Investigation workflow

1. Open Security.evtx and validate the timeframe around the suspicious admin login.
2. Reduce noise by filtering on a small set of high value Event IDs.
3. Sort by time to build sequence.
4. Validate attribution using Subject fields and SIDs, then confirm the target account in the event details.
5. Record key timestamps and artifacts to produce a defensible timeline.

Key investigation findings

1. Privileged activity confirmed
   I started by filtering for Event ID 4672 to locate sessions where special privileges were assigned. This helped anchor the investigation to high risk access before looking for account lifecycle events.
2. Account creation tied to an admin context
   I pivoted to Event ID 4720 to confirm creation of a new local user account. I validated

attribution by reviewing the Subject fields and SIDs to ensure the initiating user context aligned with the administrator activity under investigation.

3. Privilege escalation through group membership changes
   After confirming the account creation, I filtered for Event ID 4732 to identify group membership changes for the new account. The log evidence showed the account being added to these local groups.
   Administrators
   ServiceAccount
   Users

This step matters because it shows impact. The account was not only created. It was granted elevated access and operational utility.

4. Account use confirmed with successful logon correlation
   To confirm the account was actually used, I filtered for Event ID 4624 and searched for the newly created username. This validated a successful logon occurring after the account creation and after the group membership changes.

Outcome and determination

The Security.evtx evidence supports a clear suspicious lifecycle pattern. Create, privilege, use. A new account was created, elevated into high privilege groups including Administrators, then used for a successful logon. This pattern is consistent with unauthorized access preparation and should be treated as an incident until proven otherwise.

Recommended response actions, production safe guidance

Immediate actions

Contain the affected host if possible, or restrict privileged access until scope is confirmed.

Preserve relevant logs and any supporting artifacts for the time window.

Scoping and follow up

Identify whether the new account was created elsewhere on additional hosts.

Review additional Security events around the same window, focusing on group changes and logon activity tied to the same Subject context.

Validate whether any follow on actions occurred after the first successful logon, using other available telemetry if present.

Detection improvements

Alert on Event ID 4720 followed closely by Event ID 4732 into Administrators, then Event ID 4624 for that same account.

Add a rule for after hours privileged activity that includes Event ID 4672 as supporting context.

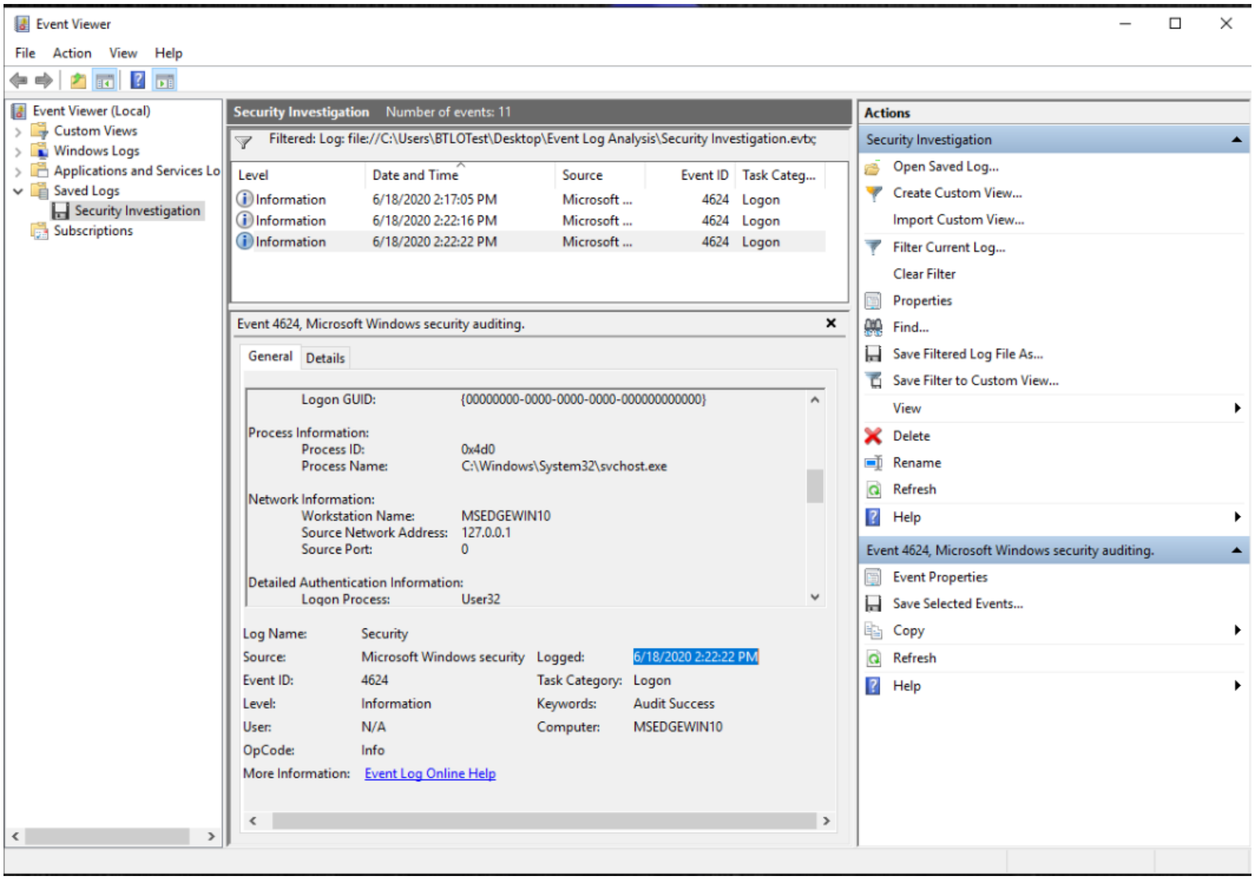
Skills demonstrated

Windows log triage and correlation in Event Viewer

Audit ready timeline building tied directly to Security event evidence

Attribution validation using Subject fields and SIDs

Detection oriented thinking by linking create, privilege, use into a repeatable alert pattern



Security Investigation Number of events: 11

Filtered: Log: file://C:\Users\BTLOTest\Desktop\Event Log Analysis\Security Investigation.evtx;

Level	Date and Time	Source	Event ID	Task Categ...
Information	6/18/2020 2:17:05 PM	Microsoft ...	4624	Logon
Information	6/18/2020 2:22:16 PM	Microsoft ...	4624	Logon
Information	6/18/2020 2:22:22 PM	Microsoft ...	4624	Logon

Event 4624, Microsoft Windows security auditing.

```
          Logon GUID:                {00000000-0000-0000-0000-000000000000}

Process Information:
          Process ID:                0x4d0
          Process Name:              C:\Windows\System32\svchost.exe

Network Information:
          Workstation Name:          MSEDGEWIN10
          Source Network Address:    127.0.0.1
          Source Port:               0

Detailed Authentication Information:
          Logon Process:             User32
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	6/18/2020 2:22:22 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	MSEDGEWIN10
OpCode:	Info		
More Information:	Event Log Online Help		