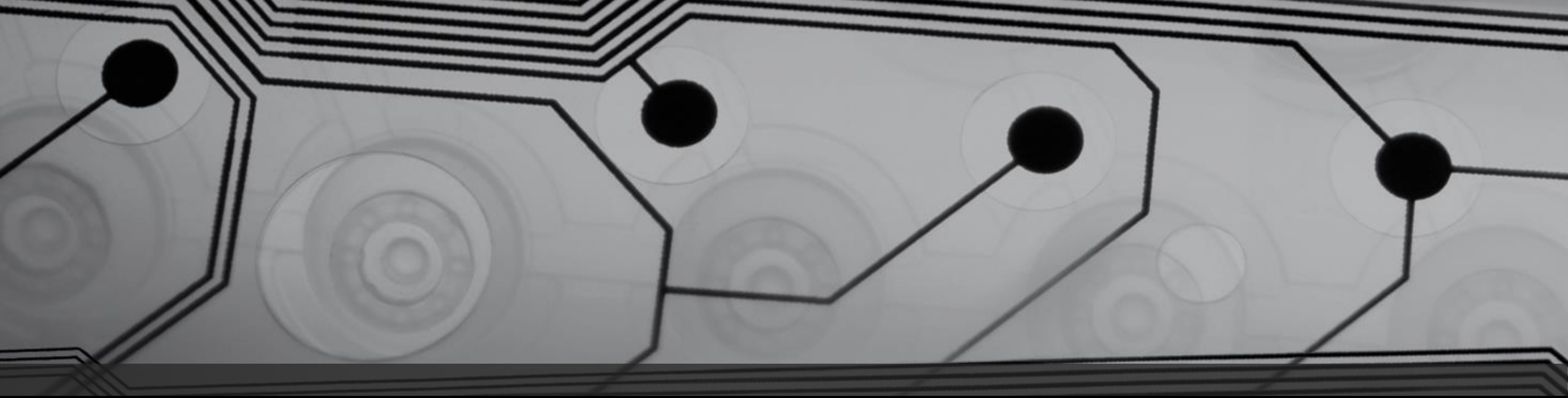


suspicious events for threat hunter

Ahmad abdelnasser Soliman

abdelnassersoliman0@gmail.com

Using Sysmon & Event Codes for Threat Hunting

✓ Sysmon

- ➢ which stands for “ **system monitor** " is a detection technology rather than a preventative one.

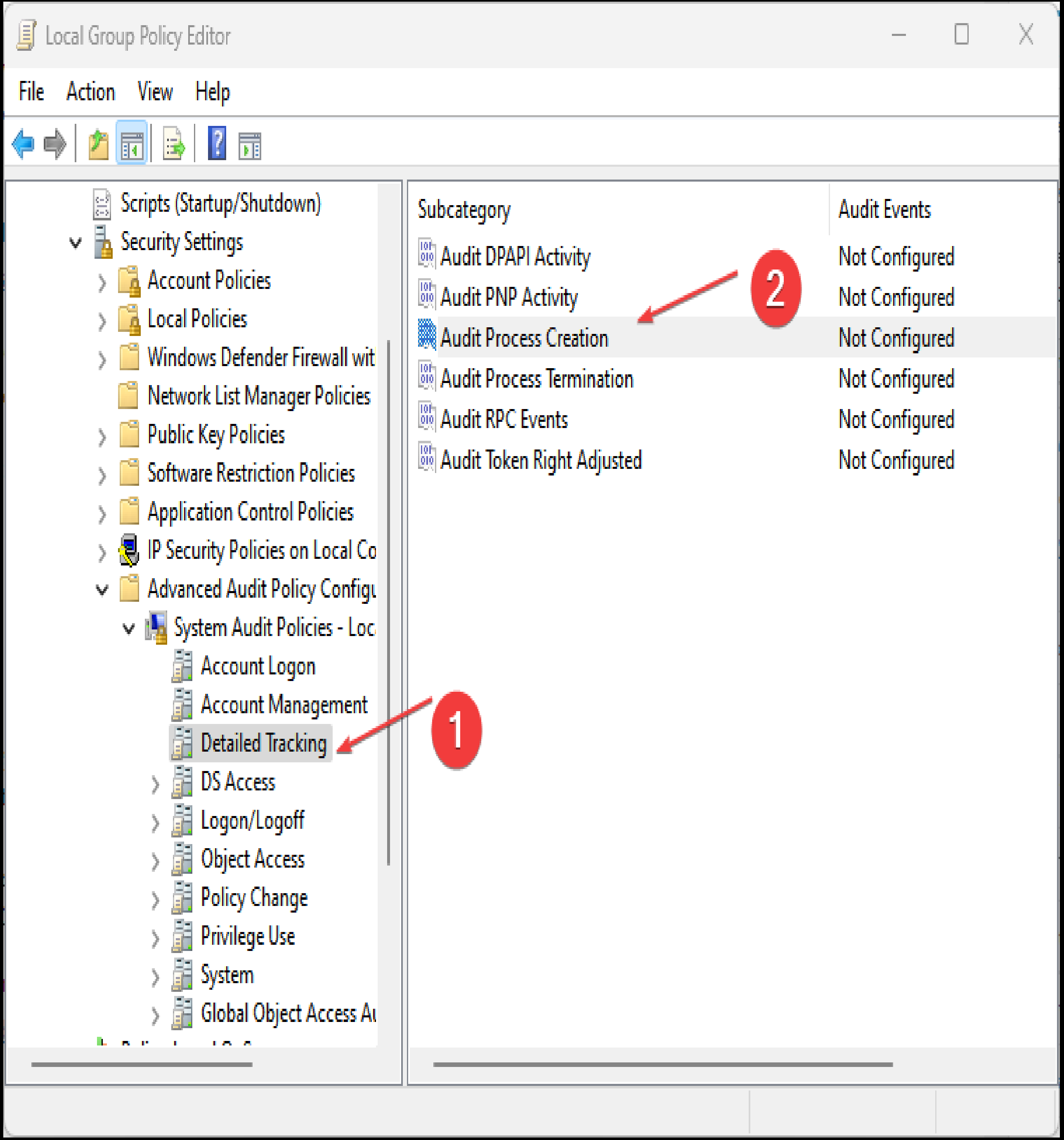
❑ Event Code **4688** (**new process**)

It's possible that this **is the most significant event code in existence**. Event Code **4688** is defined by Windows as "A new process has been created " but it can mean much more than that. It is associated with any program or process that a user starts, or even spawns from another process.

freshly formed processes and, if they were produced by a parent process, their Parent Process ID.

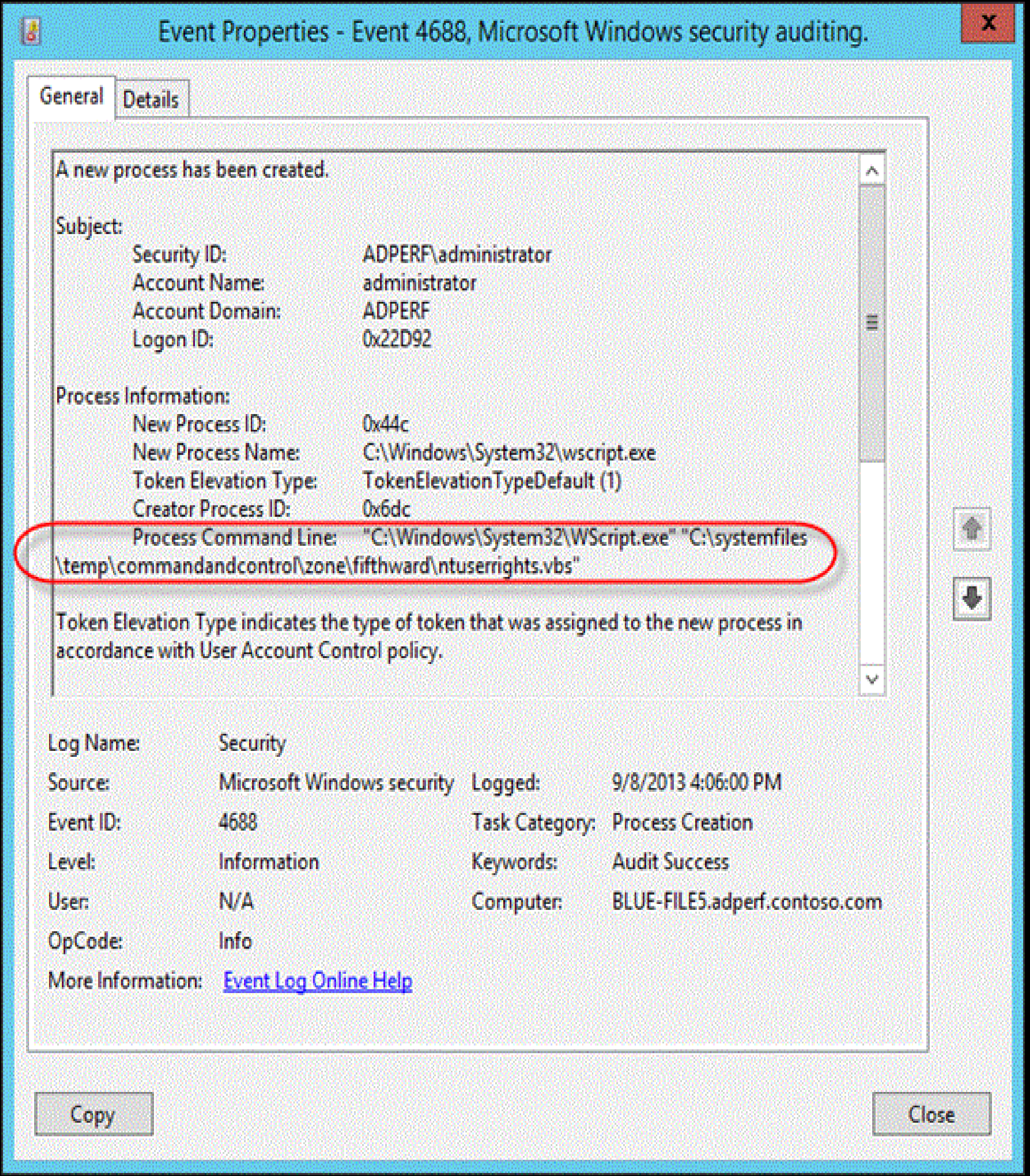
❑ Why is this information relevant ?

- ➢The Parent Process ID of a child process is always the same as that of the parent process. This gives you the information you need to remove the infection and aids in locating any malicious processes that may have been spawned.



- Scripts (Startup/Shutdown)
- Security Settings
  - Account Policies
  - Local Policies
  - Windows Defender Firewall wit
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Co
  - Advanced Audit Policy Configu
    - System Audit Policies - Loc
      - Account Logon
      - Account Management
      - Detailed Tracking
      - DS Access
      - Logon/Logoff
      - Object Access
      - Policy Change
      - Privilege Use
      - System
      - Global Object Access Au

Subcategory	Audit Events
Audit DPAPI Activity	Not Configured
Audit PNP Activity	Not Configured
Audit Process Creation	Not Configured
Audit Process Termination	Not Configured
Audit RPC Events	Not Configured
Audit Token Right Adjusted	Not Configured

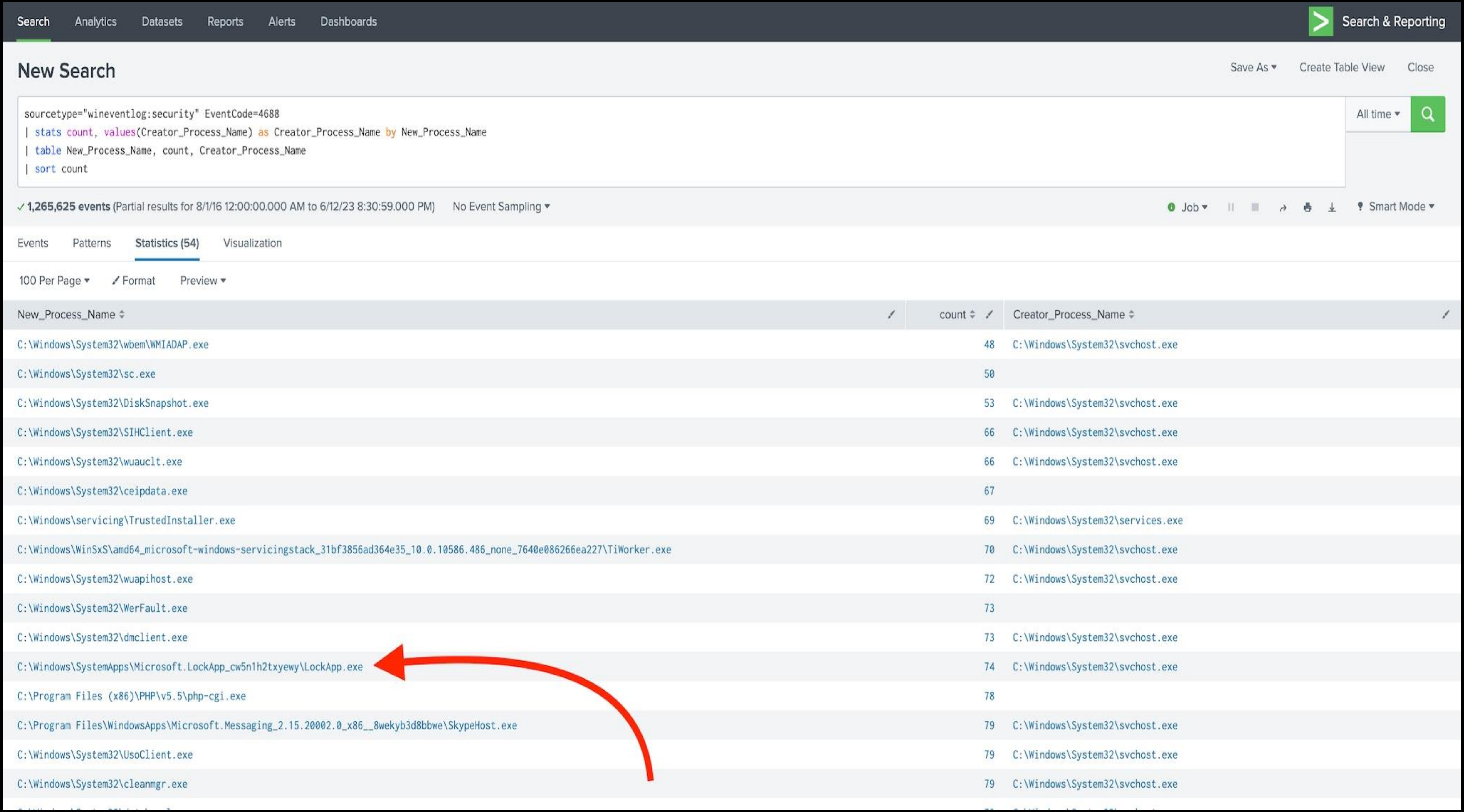

Event Properties - Event 4688, Microsoft Windows security auditing.
General
Details
Copy
Close

```
A new process has been created.

Subject:
        Security ID:            ADPERF\administrator
        Account Name:           administrator
        Account Domain:         ADPERF
        Logon ID:               0x22D92

Process Information:
        New Process ID:         0x44c
        New Process Name:       C:\Windows\System32\wscript.exe
        Token Elevation Type:   TokenElevationTypeDefault (1)
        Creator Process ID:     0x6dc
        Process Command Line:   "C:\Windows\System32\WScript.exe" "C:\systemfiles
\temp\commandandcontrol\zone\fifthward\ntuserrights.vbs"

Token Elevation Type indicates the type of token that was assigned to the new process in
accordance with User Account Control policy.
```

Log Name: Security
Source: Microsoft Windows security
Logged: 9/8/2013 4:06:00 PM
Event ID: 4688
Task Category: Process Creation
Level: Information
Keywords: Audit Success
User: N/A
Computer: BLUE-FILE5.adperf.contoso.com
OpCode: Info
More Information: Event Log Online Help

❑ Splunk query for hunting this event

```
sourcetype="wineventlog:security"EventCode=4688

| stats count, values(Creator_Process_Name) as Creator_Process_Name by
New_Process_Name

| table New_Process_Name, count, Creator_Process_Name

| sort count
```



```
sourcetype="wineventlog:security" EventCode=4688
| stats count, values(Creator_Process_Name) as Creator_Process_Name by New_Process_Name
| table New_Process_Name, count, Creator_Process_Name
| sort count
```

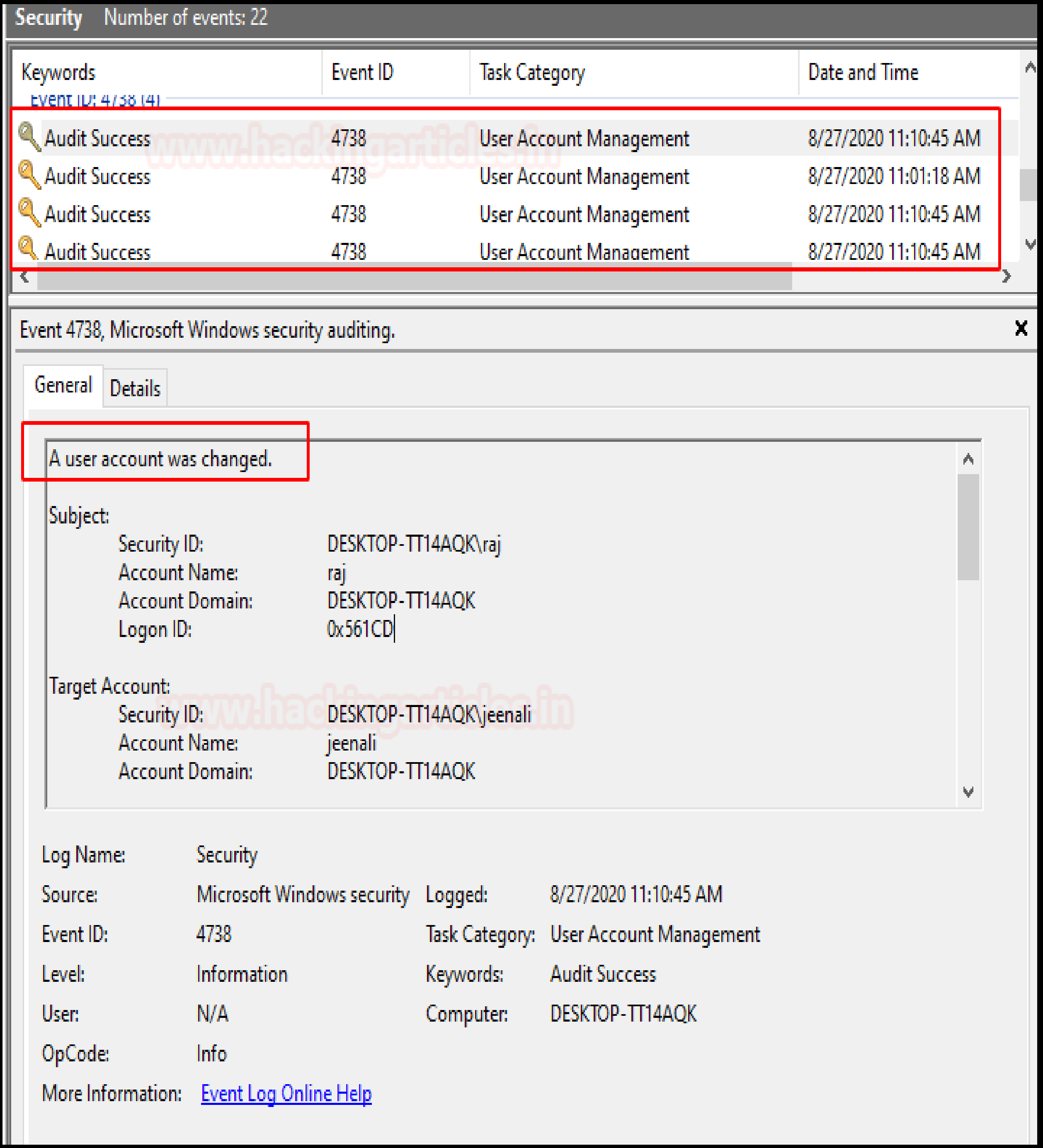
✓ 1,265,625 events (Partial results for 8/1/16 12:00:00.000 AM to 6/12/23 8:30:59.000 PM) No Event Sampling ▾

New_Process_Name	count	Creator_Process_Name
C:\Windows\System32\wbem\WMIADAP.exe	48	C:\Windows\System32\svchost.exe
C:\Windows\System32\sc.exe	50	
C:\Windows\System32\DiskSnapshot.exe	53	C:\Windows\System32\svchost.exe
C:\Windows\System32\SIHClient.exe	66	C:\Windows\System32\svchost.exe
C:\Windows\System32\wuauclt.exe	66	C:\Windows\System32\svchost.exe
C:\Windows\System32\ceipdata.exe	67	
C:\Windows\servicing\TrustedInstaller.exe	69	C:\Windows\System32\services.exe
C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.10586.486_none_7640e086266ea227\TiWorker.exe	70	C:\Windows\System32\svchost.exe
C:\Windows\System32\wuapihost.exe	72	C:\Windows\System32\svchost.exe
C:\Windows\System32\WerFault.exe	73	
C:\Windows\System32\dmclient.exe	73	C:\Windows\System32\svchost.exe
C:\Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy\LockApp.exe	74	C:\Windows\System32\svchost.exe
C:\Program Files (x86)\PHP\v5.5\php-cgi.exe	78	
C:\Program Files\WindowsApps\Microsoft.Messaging_2.15.20002.0_x86__8wekyb3d8bbwe\SkypeHost.exe	79	C:\Windows\System32\svchost.exe
C:\Windows\System32\UsoClient.exe	79	C:\Windows\System32\svchost.exe
C:\Windows\System32\cleanmgr.exe	79	C:\Windows\System32\svchost.exe

❑ Event Code 4738 (User account change)

- Now for my personal favorite, 4738 : "A user account was changed." Every time a user account is modified, this event is recorded, and it is particularly significant when an account is given Administrator rights in a domain or on a stand-alone Windows computer.

- **I enjoy** searching for this occasion and seeing anything that happens two minutes later. Malicious adversaries, **such as** hackers or your own staff, frequently try to "elevate" user account permissions.



Security Number of events: 22

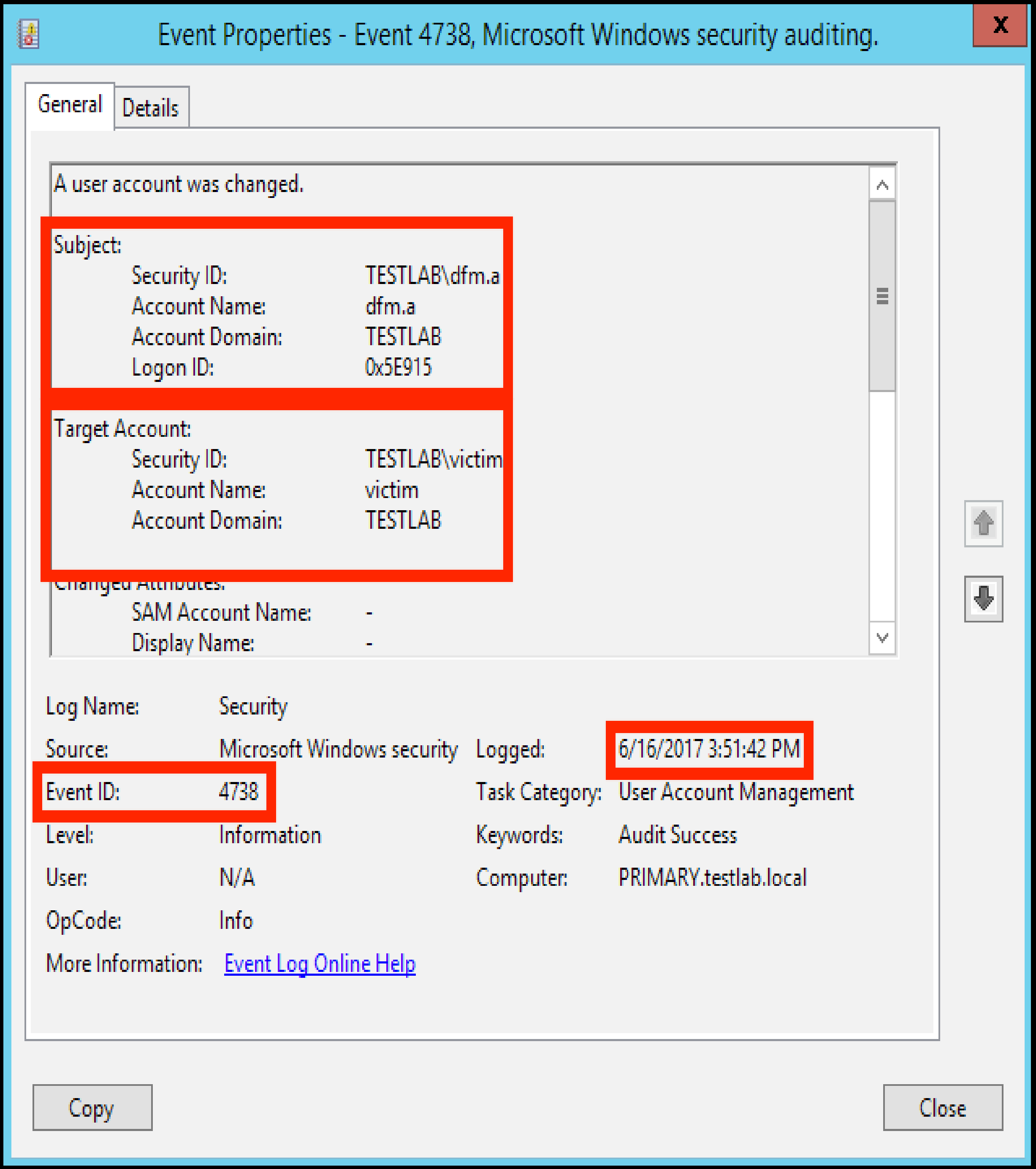
Event ID: 4738 (4)

Keywords	Event ID	Task Category	Date and Time
Audit Success	4738	User Account Management	8/27/2020 11:10:45 AM
Audit Success	4738	User Account Management	8/27/2020 11:01:18 AM
Audit Success	4738	User Account Management	8/27/2020 11:10:45 AM
Audit Success	4738	User Account Management	8/27/2020 11:10:45 AM

Event 4738, Microsoft Windows security auditing.

```
A user account was changed.

Subject:
        Security ID:        DESKTOP-TT14AQK\raj
        Account Name:       raj
        Account Domain:     DESKTOP-TT14AQK
        Logon ID:           0x561CD

Target Account:
        Security ID:        DESKTOP-TT14AQK\jeenali
        Account Name:       jeenali
        Account Domain:     DESKTOP-TT14AQK
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/27/2020 11:10:45 AM
Event ID:	4738	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-TT14AQK
OpCode:	Info		
More Information:	Event Log Online Help		



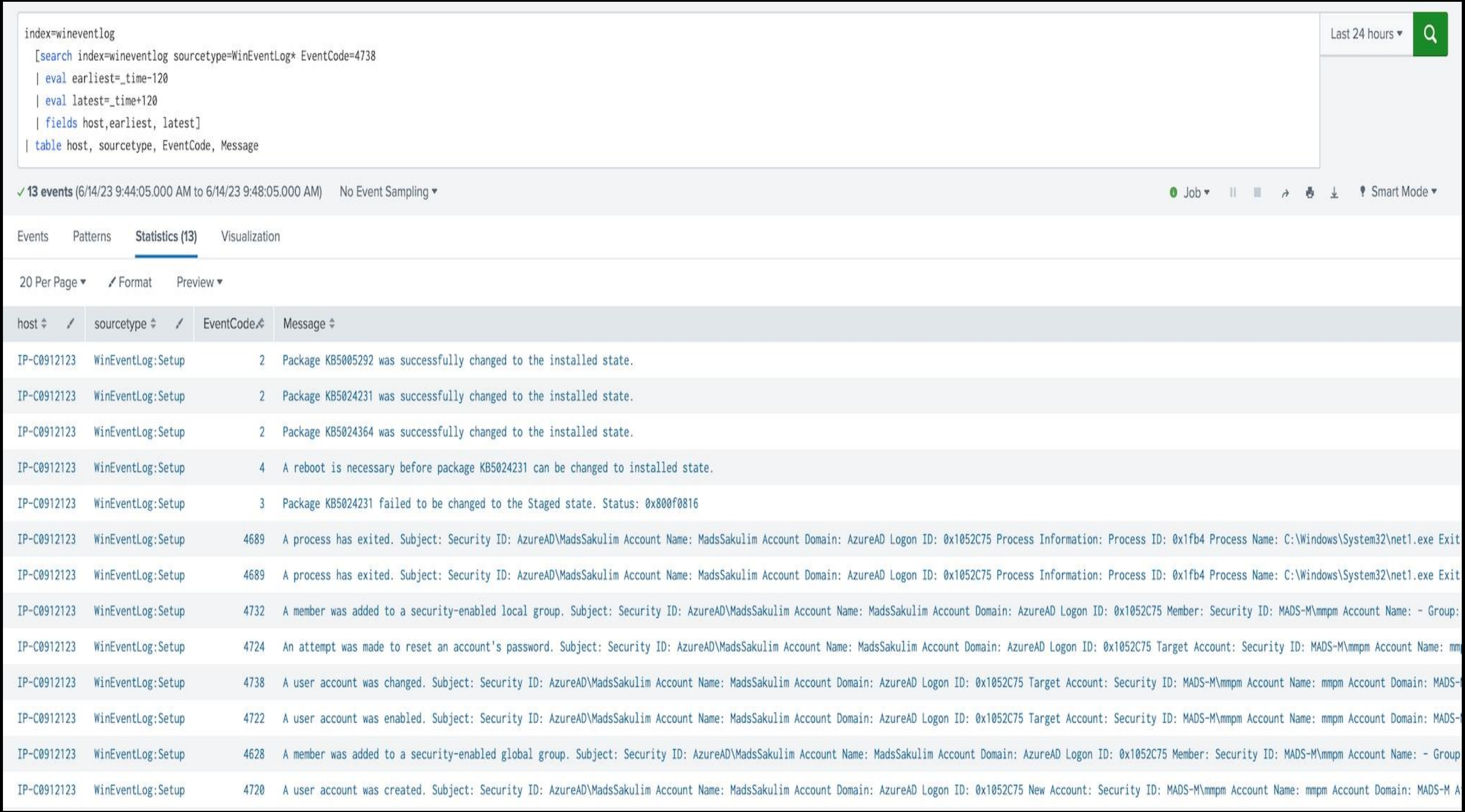
Event Properties - Event 4738, Microsoft Windows security auditing.

```
A user account was changed.

Subject:
        Security ID:        TESTLAB\dfm.a
        Account Name:       dfm.a
        Account Domain:     TESTLAB
        Logon ID:           0x5E915

Target Account:
        Security ID:        TESTLAB\victim
        Account Name:       victim
        Account Domain:     TESTLAB

Changed Attributes:
        SAM Account Name:   -
        Display Name:       -
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	6/16/2017 3:51:42 PM
Event ID:	4738	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	PRIMARY.testlab.local
OpCode:	Info		
More Information:	Event Log Online Help		

❑ Splunk query for hunting this event

```
index=wineventlog

        [search index=wineventlog sourcetype=WinEventLog* EventCode=4738

        | eval earliest=_time-120

        | eval latest=_time+120

        | fields host, earliest, latest]

| table host, sourcetype, EventCode, Message
```



```
index=wineventlog
  [search index=wineventlog sourcetype=WinEventLog* EventCode=4738
   | eval earliest=_time-120
   | eval latest=_time+120
   | fields host,earliest, latest]
| table host, sourcetype, EventCode, Message
```

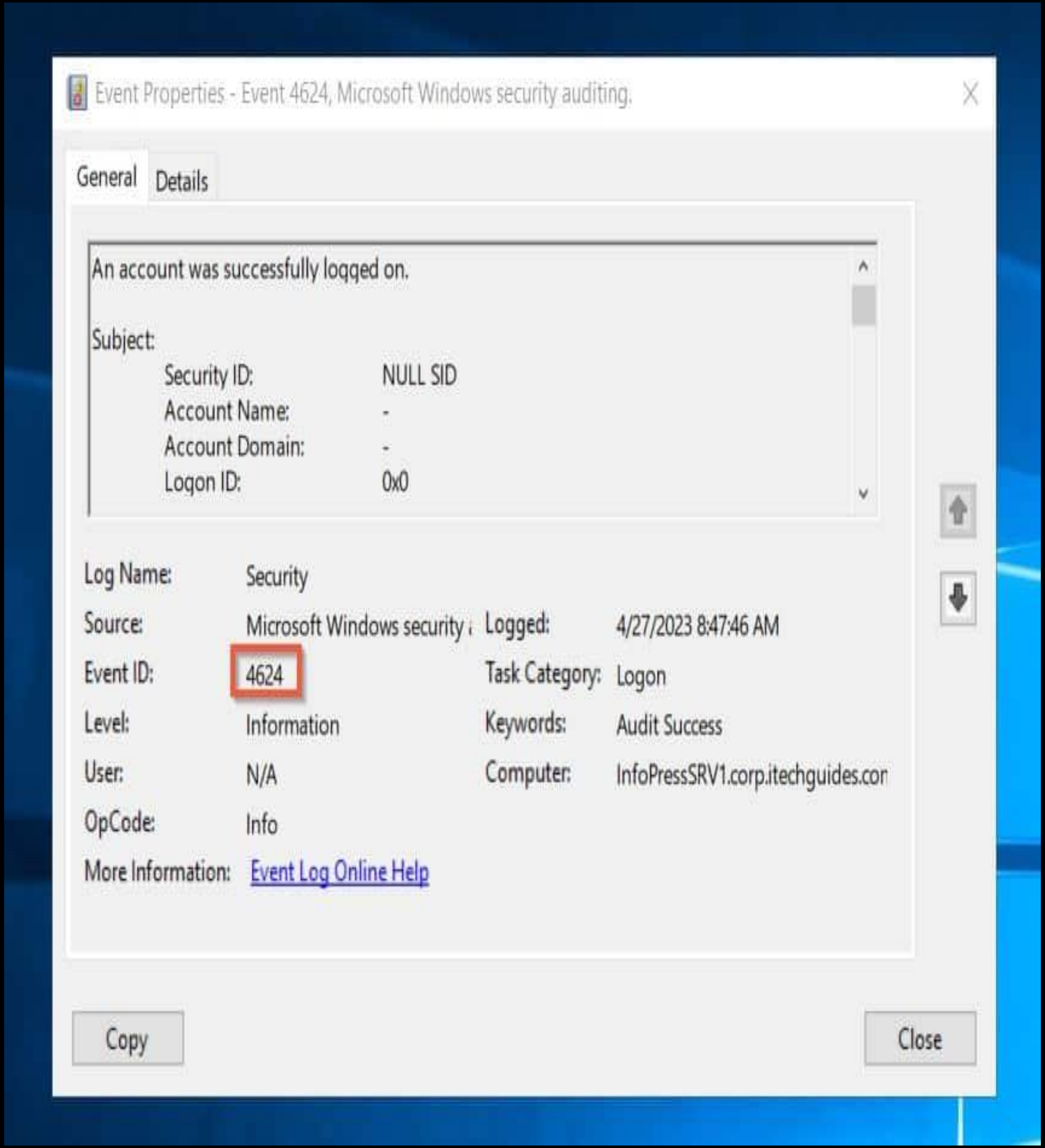
✓ 13 events (6/14/23 9:44:05.000 AM to 6/14/23 9:48:05.000 AM)

host	sourcetype	EventCode	Message
IP-C0912123	WinEventLog:Setup	2	Package KB5005292 was successfully changed to the installed state.
IP-C0912123	WinEventLog:Setup	2	Package KB5024231 was successfully changed to the installed state.
IP-C0912123	WinEventLog:Setup	2	Package KB5024364 was successfully changed to the installed state.
IP-C0912123	WinEventLog:Setup	4	A reboot is necessary before package KB5024231 can be changed to installed state.
IP-C0912123	WinEventLog:Setup	3	Package KB5024231 failed to be changed to the Staged state. Status: 0x800f0816
IP-C0912123	WinEventLog:Setup	4689	A process has exited. Subject: Security ID: AzureAD\MadsSakulim Account Name: MadsSakulim Account Domain: AzureAD Logon ID: 0x1052C75 Process Information: Process ID: 0x1fb4 Process Name: C:\Windows\System32\net1.exe Exit
IP-C0912123	WinEventLog:Setup	4689	A process has exited. Subject: Security ID: AzureAD\MadsSakulim Account Name: MadsSakulim Account Domain: AzureAD Logon ID: 0x1052C75 Process Information: Process ID: 0x1fb4 Process Name: C:\Windows\System32\net1.exe Exit
IP-C0912123	WinEventLog:Setup	4732	A member was added to a security-enabled local group. Subject: Security ID: AzureAD\MadsSakulim Account Name: MadsSakulim Account Domain: AzureAD Logon ID: 0x1052C75 Member: Security ID: MADS-M\mmpm Account Name: - Group:
IP-C0912123	WinEventLog:Setup	4724	An attempt was made to reset an account's password. Subject: Security ID: AzureAD\MadsSakulim Account Name: MadsSakulim Account Domain: AzureAD Logon ID: 0x1052C75 Target Account: Security ID: MADS-M\mmpm Account Name: mm
IP-C0912123	WinEventLog:Setup	4738	A user account was changed. Subject: Security ID: AzureAD\MadsSakulim Account Name: MadsSakulim Account Domain: AzureAD Logon ID: 0x1052C75 Target Account: Security ID: MADS-M\mmpm Account Name: mmpm Account Domain: MADS-
IP-C0912123	WinEventLog:Setup	4722	A user account was enabled. Subject: Security ID: AzureAD\MadsSakulim Account Name: MadsSakulim Account Domain: AzureAD Logon ID: 0x1052C75 Target Account: Security ID: MADS-M\mmpm Account Name: mmpm Account Domain: MADS-
IP-C0912123	WinEventLog:Setup	4628	A member was added to a security-enabled global group. Subject: Security ID: AzureAD\MadsSakulim Account Name: MadsSakulim Account Domain: AzureAD Logon ID: 0x1052C75 Member: Security ID: MADS-M\mmpm Account Name: - Group
IP-C0912123	WinEventLog:Setup	4720	A user account was created. Subject: Security ID: AzureAD\MadsSakulim Account Name: MadsSakulim Account Domain: AzureAD Logon ID: 0x1052C75 New Account: Security ID: MADS-M\mmpm Account Name: mmpm Account Domain: MADS-M A

❑ Event Code 4624 (Successful login)

- When an account logs into a Windows environment successfully, Event Code 4624 is generated. By using this data, a user baseline of login times and locations can be established.

- Additionally, Event Code 4624 logs the various logon types, such as network and local. You can use this data to identify outliers in your network filtering by logon type or even time



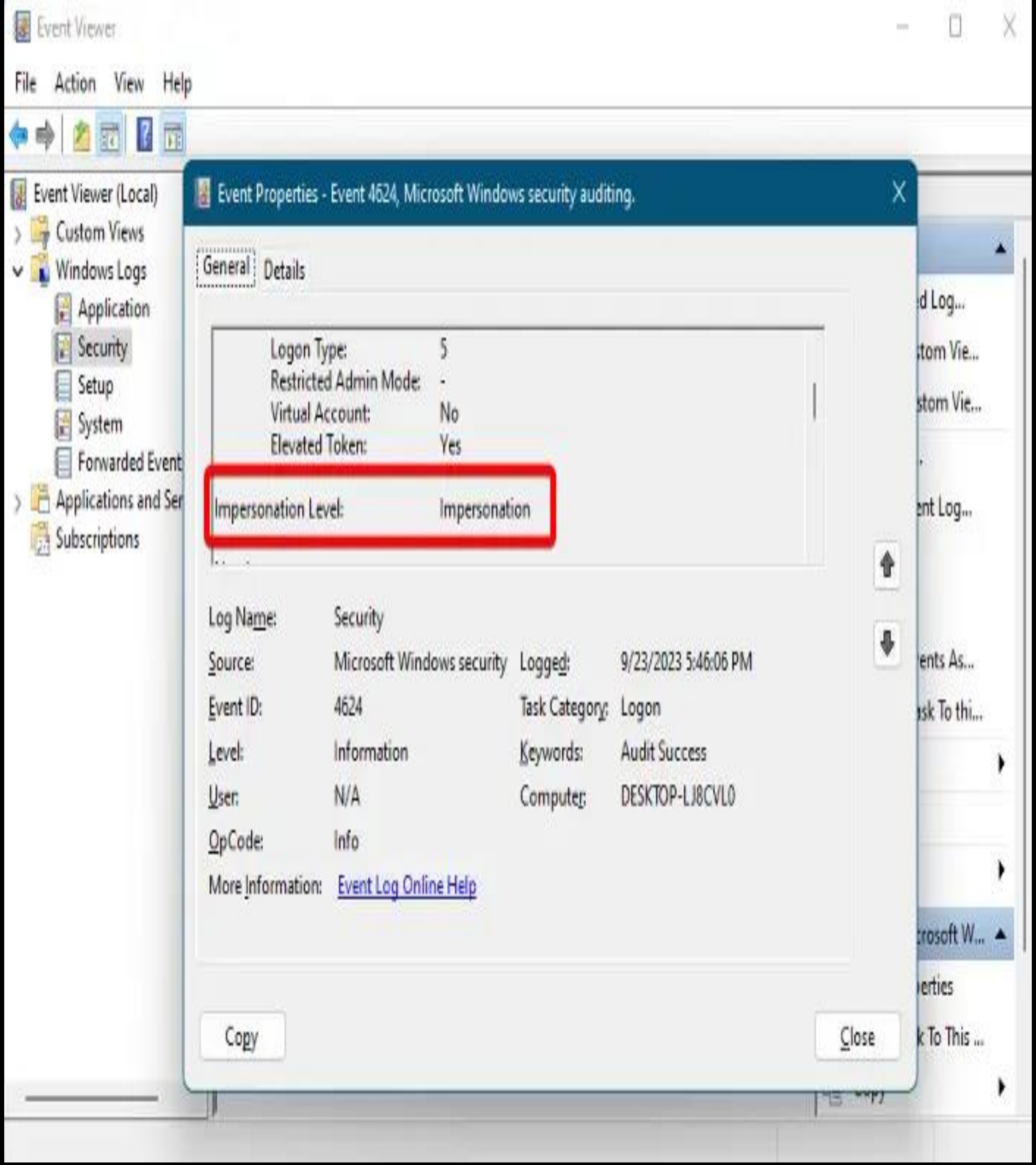
Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Copy
Close

An account was successfully logged on.

Subject:

```
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0
```

```
Log Name:      Security
Source:        Microsoft Windows security a   Logged:         4/27/2023 8:47:46 AM
Event ID:      4624                           Task Category:  Logon
Level:         Information                    Keywords:       Audit Success
User:          N/A                            Computer:       InfoPressSRV1.corp.itechguides.cor
OpCode:        Info
More Information:  Event Log Online Help
```

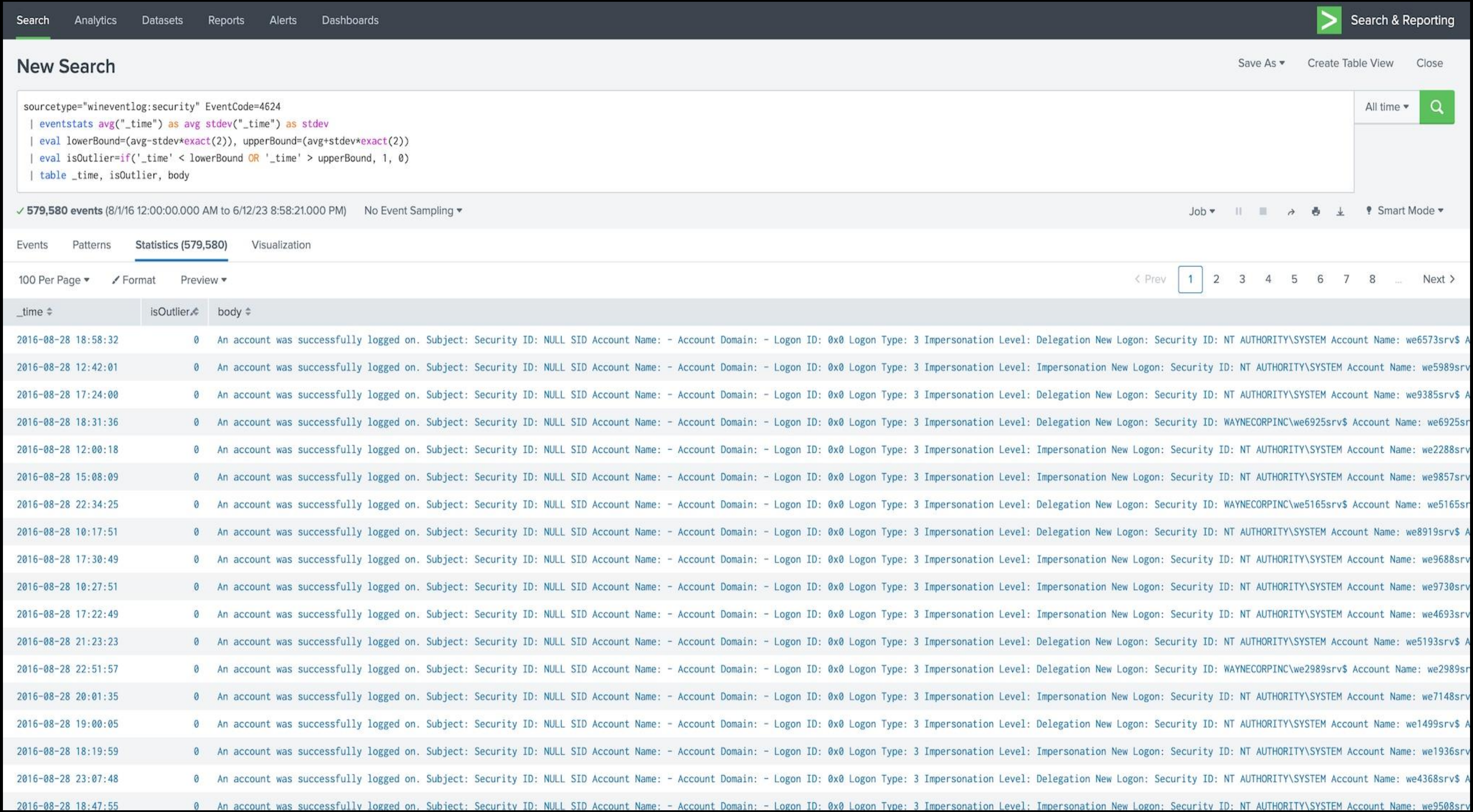


```
        Logon Type:             5
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation
```

```
Log Name:      Security
Source:        Microsoft Windows security   Logged:         9/23/2023 5:46:06 PM
Event ID:      4624                         Task Category:  Logon
Level:         Information                  Keywords:       Audit Success
User:          N/A                          Computer:       DESKTOP-LJ8CVL0
OpCode:        Info
More Information:  Event Log Online Help
```

❑ Splunk query for hunting this event

```
sourcetype="wineventlog:security" EventCode=4624

 | eventstats avg("_time") as avg stdev("_time") as stdev

 | eval lowerBound=(avg-stdev*exact(2)),
upperBound=(avg+stdev*exact(2))

 | eval isOutlier=if('_time' < lowerBound OR '_time' > upperBound, 1, 0)

 | table _time, isOutlier, body
```



New Search

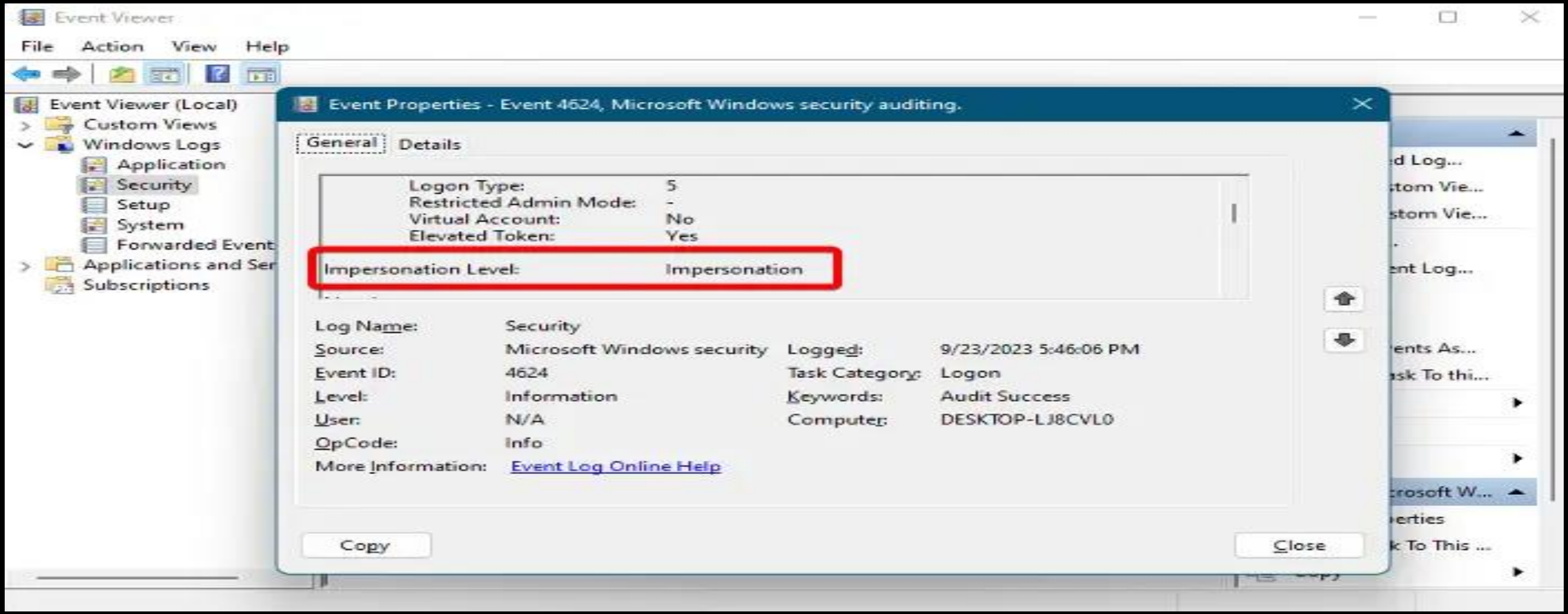
```
sourcetype="wineventlog:security" EventCode=4624
 | eventstats avg("_time") as avg stdev("_time") as stdev
 | eval lowerBound=(avg-stdev*exact(2)), upperBound=(avg+stdev*exact(2))
 | eval isOutlier=if('_time' < lowerBound OR '_time' > upperBound, 1, 0)
 | table _time, isOutlier, body
```

✓ **579,580 events** (8/1/16 12:00:00.000 AM to 6/12/23 8:58:21.000 PM) No Event Sampling ▾

_time	isOutlier	body
2016-08-28 18:58:32	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we6573srv$ A
2016-08-28 12:42:01	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we5989srv
2016-08-28 17:24:00	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we9385srv$ A
2016-08-28 18:31:36	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: WAYNECORPINC\we6925srv$ Account Name: we6925sr
2016-08-28 12:00:18	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we2288srv
2016-08-28 15:08:09	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we9857srv
2016-08-28 22:34:25	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: WAYNECORPINC\we5165srv$ Account Name: we5165sr
2016-08-28 10:17:51	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we8919srv$ A
2016-08-28 17:30:49	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we9688srv
2016-08-28 10:27:51	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we9730srv
2016-08-28 17:22:49	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we4693srv
2016-08-28 21:23:23	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we5193srv$ A
2016-08-28 22:51:57	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: WAYNECORPINC\we2989srv$ Account Name: we2989sr
2016-08-28 20:01:35	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we7148srv
2016-08-28 19:00:05	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we1499srv$ A
2016-08-28 18:19:59	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we1936srv
2016-08-28 23:07:48	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we4368srv$ A
2016-08-28 18:47:55	0	An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: we9508srv

❑ Event Code 1102 (Audit log clearing)

- When a Windows administrator or administrative account clears the audit log, Event Code **1102** is triggered. It should not be used frequently, and if it is, it may be done to hide something.



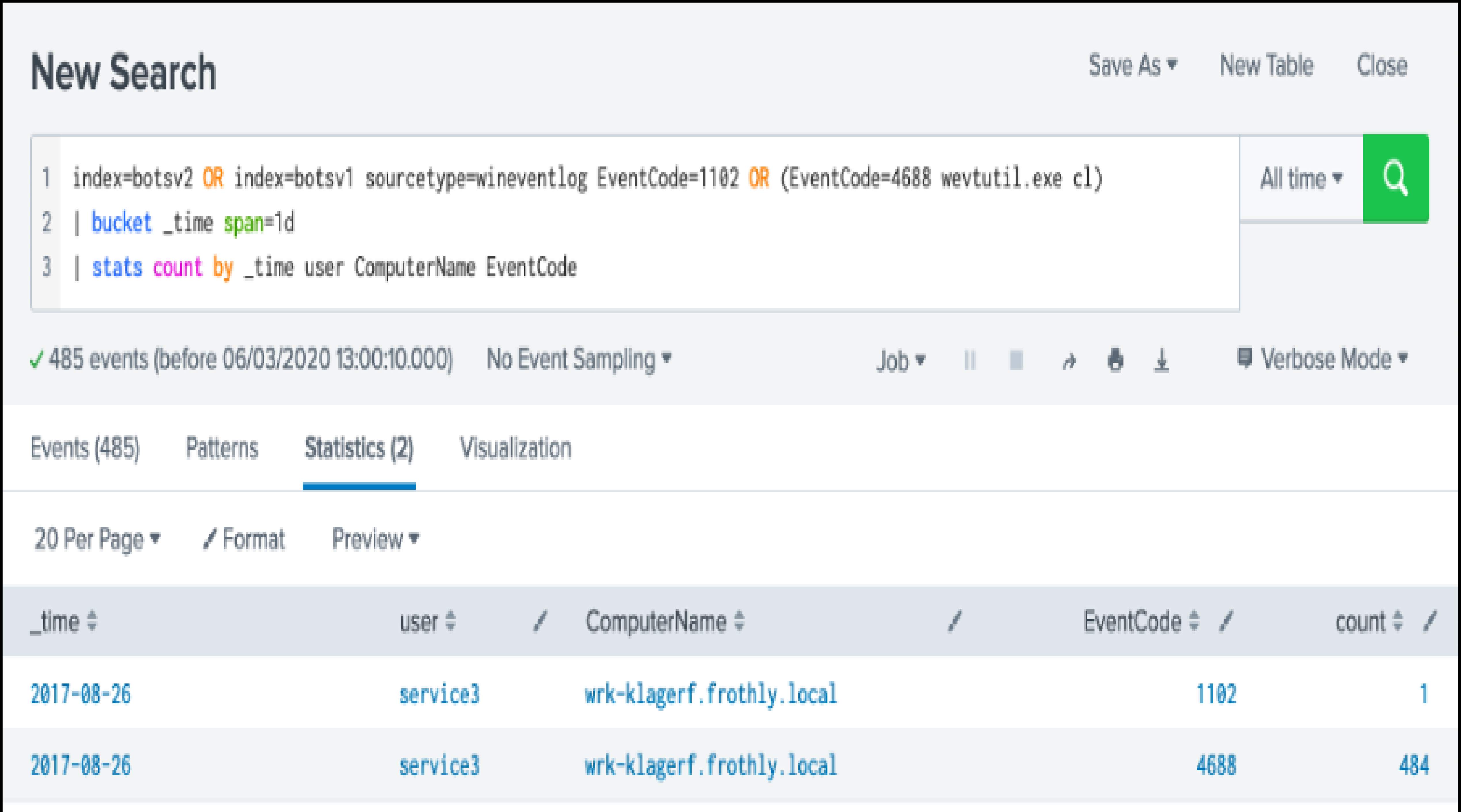
Event Properties - Event 4624, Microsoft Windows security auditing.

```
Logon Type:                 5
Restricted Admin Mode:      -
Virtual Account:            No
Elevated Token:             Yes

Impersonation Level:        Impersonation
```

```
Log Name:          Security
Source:            Microsoft Windows security    Logged:          9/23/2023 5:46:06 PM
Event ID:          4624                          Task Category:   Logon
Level:             Information                   Keywords:        Audit Success
User:              N/A                           Computer:        DESKTOP-LJ8CVL0
OpCode:            Info
More Information:  Event Log Online Help
```

❑ Splunk query for hunting this event

```
(`wineventlog_security` EventCode=1102) OR (`wineventlog_system`
EventCode=104)

| stats count min(_time) as firstTime max(_time) as lastTime by dest name
EventCode

| `security_content_ctime(firstTime)`

| `security_content_ctime(lastTime)`

| `windows_event_log_cleared_filter`
```



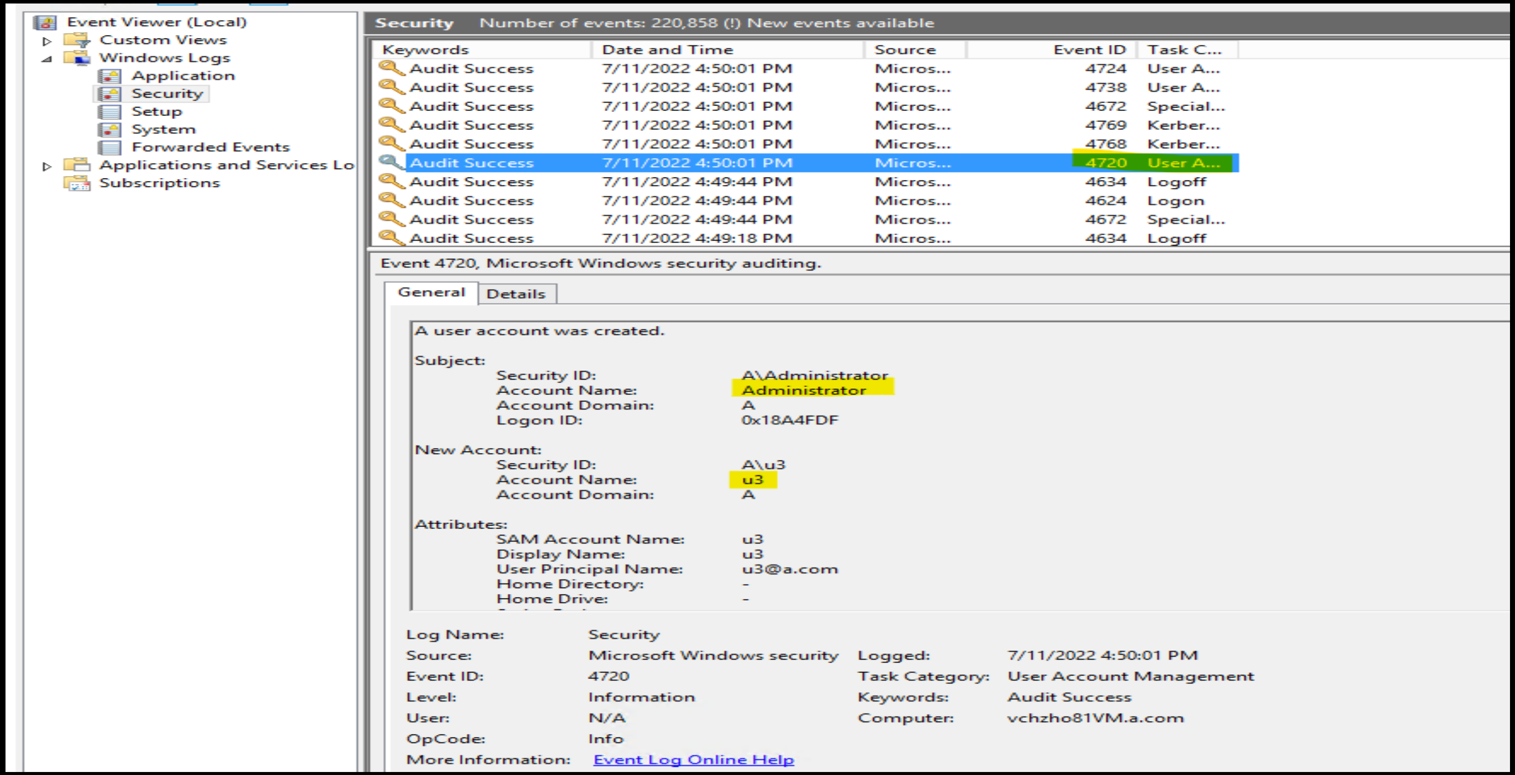
```
index=botsv2 OR index=botsv1 sourcetype=wineventlog EventCode=1102 OR (EventCode=4688 wevtutil.exe cl)
| bucket _time span=1d
| stats count by _time user ComputerName EventCode
```

✓ 485 events (before 06/03/2020 13:00:10.000)

_time	user	ComputerName	EventCode	count
2017-08-26	service3	wrk-klagerf.frothly.local	1102	1
2017-08-26	service3	wrk-klagerf.frothly.local	4688	484

❑ Event Code 4720 user account created

- An event log with ID 4720 will be present on a Windows workstation upon the creation of a new user account. Considering that most accounts are created via Active Directory, this can be a sign of a persistent attempt.



Security Number of events: 220,858 (!) New events available

Keywords	Date and Time	Source	Event ID	Task C...
Audit Success	7/11/2022 4:50:01 PM	Micros...	4724	User A...
Audit Success	7/11/2022 4:50:01 PM	Micros...	4738	User A...
Audit Success	7/11/2022 4:50:01 PM	Micros...	4672	Special...
Audit Success	7/11/2022 4:50:01 PM	Micros...	4769	Kerber...
Audit Success	7/11/2022 4:50:01 PM	Micros...	4768	Kerber...
Audit Success	7/11/2022 4:50:01 PM	Micros...	4720	User A...
Audit Success	7/11/2022 4:49:44 PM	Micros...	4634	Logoff
Audit Success	7/11/2022 4:49:44 PM	Micros...	4624	Logon
Audit Success	7/11/2022 4:49:44 PM	Micros...	4672	Special...
Audit Success	7/11/2022 4:49:18 PM	Micros...	4634	Logoff

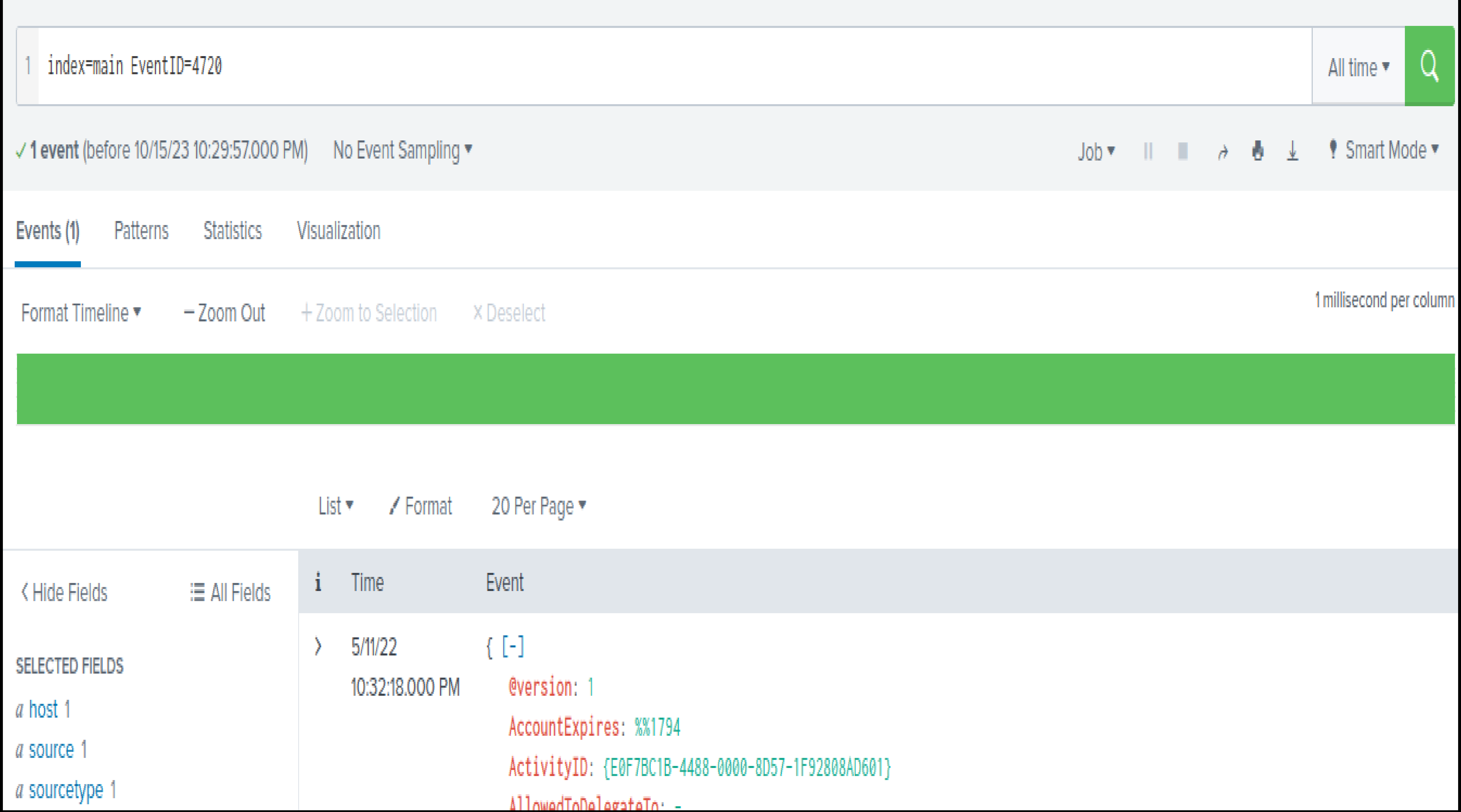
Event 4720, Microsoft Windows security auditing.

```
A user account was created.

Subject:
        Security ID:            A\Administrator
        Account Name:           Administrator
        Account Domain:         A
        Logon ID:               0x18A4FDF

New Account:
        Security ID:            A\u3
        Account Name:           u3
        Account Domain:         A

Attributes:
        SAM Account Name:       u3
        Display Name:           u3
        User Principal Name:    u3@a.com
        Home Directory:         -
        Home Drive:             -
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	7/11/2022 4:50:01 PM
Event ID:	4720	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	vchzho81VM.a.com
OpCode:	Info		
More Information:	Event Log Online Help		

❑ Splunk query for hunting this event

```
index=* source="WinEventLog:Security" (EventCode=4720 OR
EventCode=624)
    | eval CreatedBy = mvindex(Account_Name,0)
    | eval New_User = mvindex(Account_Name,1)
    | search CreatedBy=*
    | table _time EventCode CreatedBy New_User
```



```
index=main EventID=4720
```

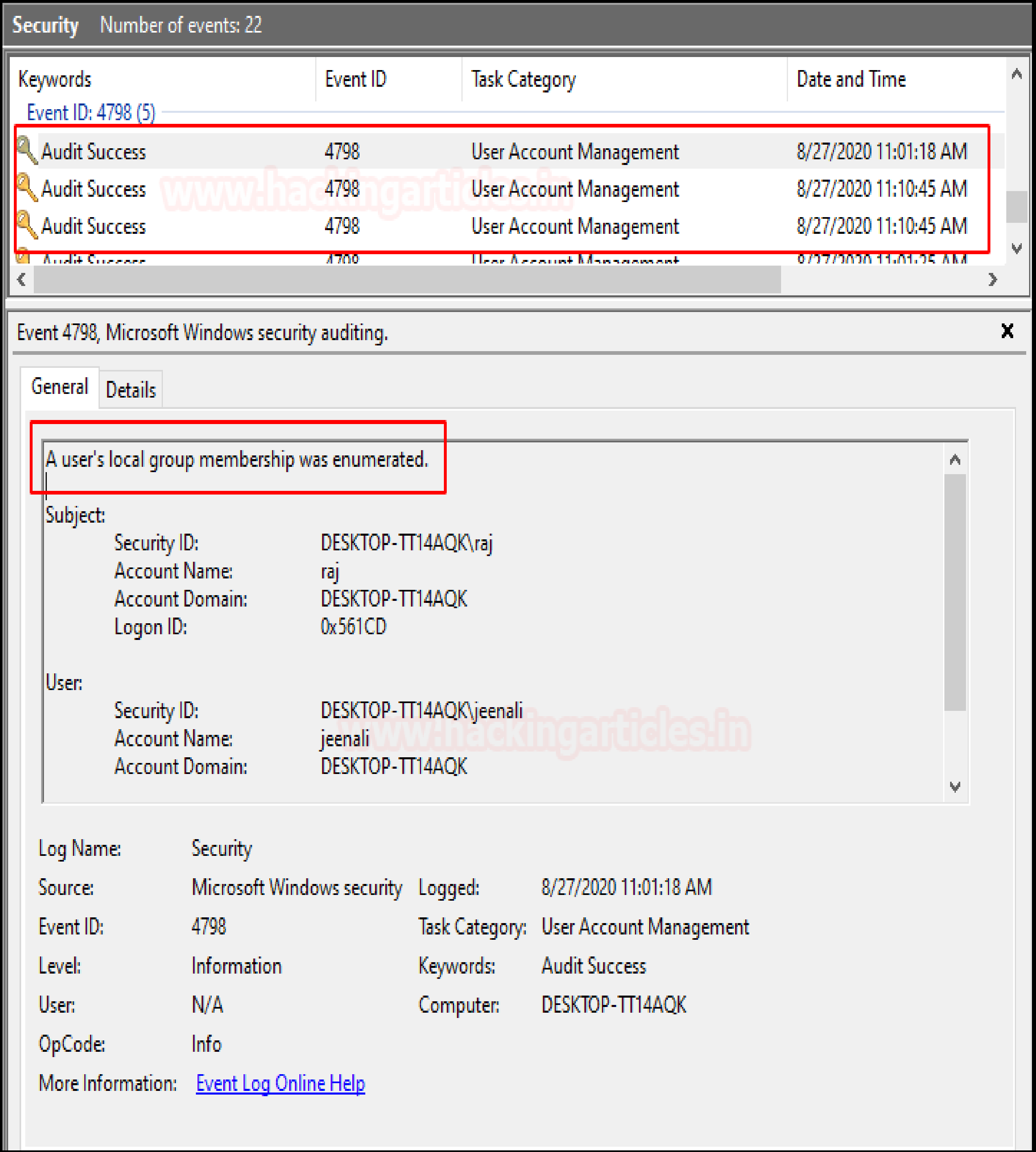
✓ 1 event (before 10/15/23 10:29:57.000 PM) No Event Sampling ▾

```
> 5/11/22            { [-]
  10:32:18.000 PM      @version: 1
                       AccountExpires: %%1794
                       ActivityID: {E0F7BC1B-4488-0000-8D57-1F92808AD601}
                       AllowedToDelegateTo: -
```

❑ Event Code **4798** (The user's local group membership was analyzed).

- The membership of a user in local groups was listed: When a process lists all the local groups that the specified user is a member of on that computer, Windows records this event.

- This event is important to identify and apprehend so-called **APT** actors that are extending their horizontal kill chain by investigating the local accounts on a compromised system.



Security Number of events: 22

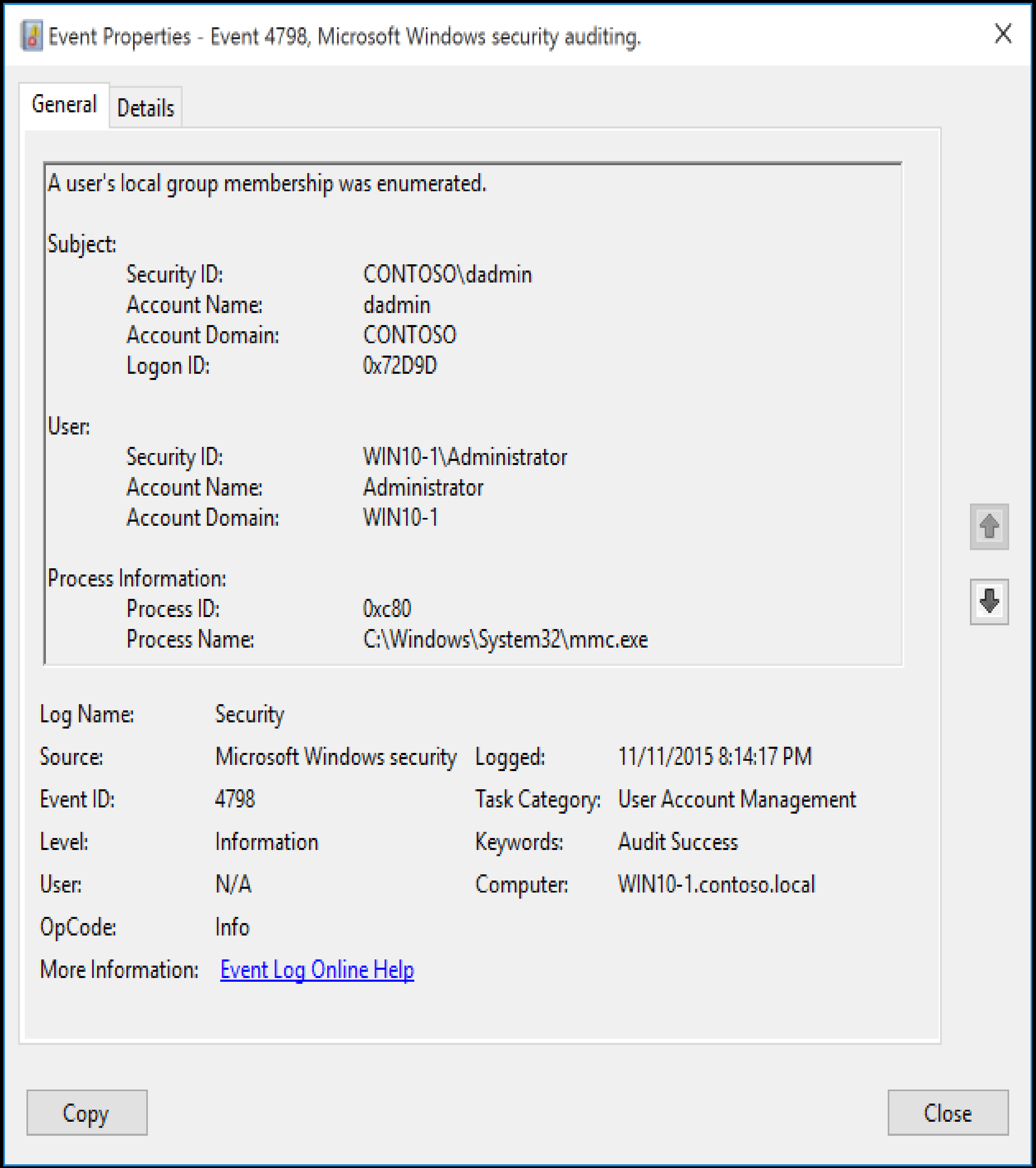
Keywords	Event ID	Task Category	Date and Time
Event ID: 4798 (5)			
Audit Success	4798	User Account Management	8/27/2020 11:01:18 AM
Audit Success	4798	User Account Management	8/27/2020 11:10:45 AM
Audit Success	4798	User Account Management	8/27/2020 11:10:45 AM
Audit Success	4798	User Account Management	8/27/2020 11:01:25 AM

Event 4798, Microsoft Windows security auditing.

A user's local group membership was enumerated.

```
Subject:
	Security ID:		DESKTOP-TT14AQK\raj
	Account Name:		raj
	Account Domain:		DESKTOP-TT14AQK
	Logon ID:		0x561CD

User:
	Security ID:		DESKTOP-TT14AQK\jeenali
	Account Name:		jeenali
	Account Domain:		DESKTOP-TT14AQK
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/27/2020 11:01:18 AM
Event ID:	4798	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-TT14AQK
OpCode:	Info		
More Information:	Event Log Online Help		



Event Properties - Event 4798, Microsoft Windows security auditing.

A user's local group membership was enumerated.

```
Subject:
	Security ID:		CONTOSO\dadmin
	Account Name:		dadmin
	Account Domain:		CONTOSO
	Logon ID:		0x72D9D

User:
	Security ID:		WIN10-1\Administrator
	Account Name:		Administrator
	Account Domain:		WIN10-1

Process Information:
	Process ID:		0xc80
	Process Name:		C:\Windows\System32\mmc.exe
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	11/11/2015 8:14:17 PM
Event ID:	4798	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN10-1.contoso.local
OpCode:	Info		
More Information:	Event Log Online Help		

THANK YOU