

Event IDs, Logging, & SIEMs

09 January 2023 12:00

4.1 Introduction

In the days of Windows XP, we knew of event logs, but it was something that we rarely referenced. It was only referenced when there was a software or hardware problem, and users were intimidated by the type of information they had to sift through to figure out the cause of the problem.

4.1 Introduction

As incident response gained popularity, so did event logs. The incident response process proved that these artifacts within the operating system were an invaluable source of information to determine what actions took place on the machine. So, event logs were no longer looked at as a troubleshooting tool but were looked at more for what they were designed to be.

4.1 Introduction

As hunters, if we're not accustomed or trained to look at event log data, then that needs to change. If we're hunting for evil on the endpoints, the information we need to look at is in those logs. The upcoming slides will help you determine which logs are more significant than others when we're hunting for specific attack signatures.

Windows Event Logs

4.2 Windows Event Logs

Windows Event Logs are built into all versions of Windows. They allow us to audit and monitor software and hardware events on the machine. These events come from various sources, such as applications or the operating system itself. All of these events are stored in a collection known as the event log.

4.2 Windows Event Logs

All versions of Windows maintain 3 core event logs:

- Application
- System
- Security



Application logs

4.2 Windows Event Logs

The **Application** event log contains events logged by various applications and/or user programs.

These events include any errors or information that an application is designed to report.

Host-based security tools, such as antivirus, often report to the Application event log.

System Logs

4.2 Windows Event Logs

The **System** event log contains events logged by various Windows system components.

These events can include drivers being loaded and unloaded, network configurations, Windows service events, etc.

Any events that are logged from Windows system components are predetermined.

Security Event Logs

4.2 Windows Event Logs

The **Security** event log contains events related to Windows authentication and security processes.

These events include valid and invalid logon attempts, account creations, changes to user privileges, etc.

Local or Group Policy settings can configure exactly which security events are logged.

Old version of Windows event logs path.

4.2 Windows Event Logs

On Windows XP, Windows 2003, and any prior versions of Windows, the default event log paths are as follows:

Event Log	Event Log Path
Application	%SYSTEMROOT%\System32\Config\AppEvent.evt
System	%SYSTEMROOT%\System32\Config\SysEvent.evt
Security	%SYSTEMROOT%\System32\Config\SecEvent.evt

4.2 Windows Event Logs

With modern versions of Windows, beginning with Windows Vista and Windows Server 2008, Microsoft made significant changes to the event logging system.

The EVT format was eliminated for a XML-based format using the EVTX extension.

The location of the event logs was changed as well.

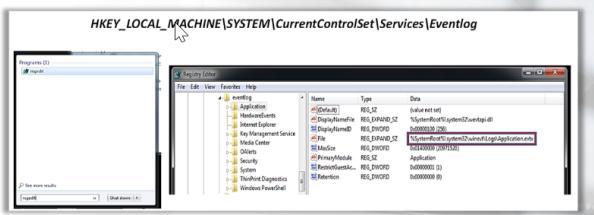
New Update location of the windows event logs path

4.2 Windows Event Logs

Event Log	Event Log Path
Application	%SYSTEMROOT%\System32\Winevt\Logs\Application.evtx
System	%SYSTEMROOT%\System32\Winevt\Logs\System.evtx
Security	%SYSTEMROOT%\System32\Winevt\Logs\Security.evtx

4.2 Windows Event Logs

Each event log location is also present within the registry.



4.2 Windows Event Logs

Under Windows Logs, you will see 2 additional sets of logs:

- **Setup:** logs contain events related to application setup.
- **Forwarded Events:** logs used to store events collected from remote computers.

4.2 Windows Event Logs

It's also worth mentioning that Microsoft added a new category of event logs, a second set of logs, called **Applications and Services**.

These logs are used by individual applications or system components.

4.2 Windows Event Logs

These logs are saved in the same location as the 3 core logs previously mentioned.

A few examples of Windows components that maintain their own logs: *UAC, Windows Firewall with Advanced Security, AppLocker, Sysmon, Windows Defender, and PowerShell*.

4.2 Windows Event Logs

Why are event logs important?

- Monitor logons that failed or that were successful.
- Monitor system services that were created, started, or stopped.
- Monitor specific application usage.
- Monitor changes to the audit policy.
- Monitor changes to user permissions.
- Monitor events generated by installed applications, such as AV.

4.2 Windows Event Logs

So by now, you should know what event logs are, where they are located, and why they are important, but how do we access and view them?

The answer to that is the **Event Viewer**.

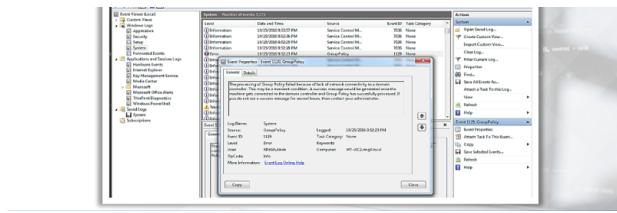
4.2 Windows Event Logs

You can access the Event Viewer by either double clicking the evtx file directly, by typing "eventvwr" in the Search box, or by navigating to **Control Panel > Administrative Tools > Event Viewer**.

4.2 Windows Event Logs

Below is a snapshot of the event viewer.





4.2 Windows Event Logs

In the previous slide, we saw an error recorded within the System event log related to Group Policy.

This particular event had an **ID** value of **1129**. In the properties for this particular event, we were fortunate enough to get some clear information as to why this error occurred. But what happens when the information is not clear?

Luckily for us, Microsoft has documented the Event IDs [here](#).

Advanced security auditing FAQ

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq>



If we use the search engine to research the recently discussed error, ID 1129, below are the results.

The screenshot shows a search result for "Event ID 1129" on the Microsoft TechNet website. The result is titled "Event ID 1129 - Group Policy Preprocessing (Networking)". It includes a brief description: "Event ID 1129 occurs when the Group Policy service fails to connect to a domain controller. This can happen if there is no network connectivity between the client and the domain controller." Below the description is a link to the full article: "Event ID 1129 - Microsoft-Windows-GroupPolicy".

The screenshot shows the full Microsoft Knowledge Base article for Event ID 1129, Microsoft-Windows-GroupPolicy. The page title is "Event ID 1129 — Microsoft-Windows-GroupPolicy". The article contains sections such as "Table of Contents", "Applies To", "Event Details", "Resolve", "Event Details", and "Message". The "Resolve" section provides troubleshooting steps: "Correct network connectivity" and "Verify". The "Event Details" section lists the product as "Windows Operating System", the event ID as "1129", the source as "Microsoft-Windows-GroupPolicy", the version as "6.0", the symbolic name as "gpEventNO_NETWORK", and the message as "The processing of Group Policy failed because of lack of network connectivity to a domain controller. This may be a transient condition. A success message would be generated once the machine gets connected to the domain controller and Group Policy has successfully processed. If you do not see a success message for several hours, then contact your administrator." The "Message" section also includes a note about the processing of Group Policy failing due to lack of network connectivity to a domain controller.

Resolve

Correct network connectivity

To correct network connectivity:

1. Open a command prompt window on the computer, and then type **ipconfig /all**.
2. Make sure that the computer has an IP address in the correct IP address range and does not have an Automatic Private IP Addressing (APIPA) address (an IP address in the 169.254.x.x range).
3. Ping the loopback address of 127.0.0.1 to verify that TCP/IP is installed and correctly configured on the local computer. If the ping is unsuccessful, this may indicate a corrupt TCP/IP stack or a problem with the network adapter.
4. Test whether you can ping the local IP address. If you can ping the loopback address but not the local IP address, there may be an issue with the routing table or with the network adapter driver.
5. Ping the IP address of a domain controller in the users' and computers' domain. Failing to ping the these domain controllers indicates a potential problem with the network in between the computer and the domain.

controllers. Diagnose the problem further using Network troubleshooting procedures.

6. Ping the fully qualified name of a domain controller in the users' and computers' domain. Failing to ping the name of these domain controllers indicates a potential problem with name resolution between the computer and the domain controllers.

7. Follow Network troubleshooting procedures to diagnose the problem further (<http://go.microsoft.com/fwlink/?LinkId=92706>).

Note:

The steps listed above may have varying results if your network constrains or blocks ICMP packets.

Verify

Group Policy applies during computer startup and user logon. Afterward, Group Policy applies every 90 to 120 minutes. Events appearing in the event log may not reflect the most current state of Group Policy. Therefore, you should always refresh Group Policy to determine if Group Policy is working correctly.

To refresh Group Policy on a specific computer:

1. Open the **Start** menu. Click **All Programs** and then click **Accessories**.
2. Click **Command Prompt**.
3. In the command prompt window, type **gpupdate** and then press **ENTER**.
4. When the gpupdate command completes, open the Event Viewer.

Group Policy is working correctly if the last Group Policy event to appear in the System event log has one of the following event IDs:

- 1500
- 1501
- 1502
- 1503

Windows event IDs

Hunting suspicious Accounts

Event IDs:

4624	Successful logon
4625	Failed logon
4634	Successful logoff
4647	User-initiated log off
4648	Logon using explicit credentials
4672	Special privileges assigned
4768	Kerberos ticket (TGT) requested
4769	Kerberos service ticket requested
4771	Kerberos pre-auth failed
4776	Attempt to validate credentials
4778	Session reconnected
4779	Session disconnected

Event IDs specific to Account Management

4720	Account created
4722	Account enabled
4724	Attempt to reset password
4728	User added to global group
4732	User added to local group
4756	User added to universal group

Finding the Elusive Active Directory Threat Hunting

<https://adsecurity.org/wp-content/uploads/2017/04/2017-BSidesCharm-DetectingtheElusive-ActiveDirectoryThreatHunting-Final.pdf>

At this point, it's worth discussing Logon Types.

In Event Logs, we'll see a numerical value referring to the Logon type, which will let us know how the account logged

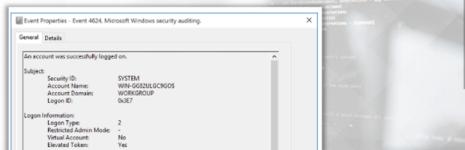
into the system, such as an RDP session or interactive logon.



4.3.1 Hunting Suspicious Accounts

Logon Type 2 is an interactive login (a user physically logged into the computer).

- <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624>



Logon Type 2 is an interactive login (a user physically logged into the computer)

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624>

4.3.1 Hunting Suspicious Accounts

Logon Type	Logon Title	Description
2	Interactive	A user physically logged onto this computer.
3	Network	A user or computer logged on from the network.
4	Batch	Used by batch servers where processes may be executing on behalf of a user, like scheduled tasks.
5	Service	A service started by the Service Control Manager.
7	Unlock	The workstation was unlocked.
8	NetworkClear text	Network credentials sent in cleartext.
9	NewCredentials	A caller cloned its current token and specified new credentials (runas command).
10	RemoteInteractive	A user logged onto computer using Terminal Services or RDP.
11	CachedInteractive	A user logged onto computer using network credentials which were stored locally on the computer.

4.3.1 Hunting Suspicious Accounts

Another piece of information to note regarding Event IDs specific to accounts is the **Logon ID**.

The Logon ID will let us know which Event ID is part of which logon session.

4.3.1 Hunting Suspicious Accounts

Start of session, **Event ID 4624**, and sessions ends, **Event ID 4634 or 4647**.



4.3.1 Hunting Suspicious Accounts

We will know the duration of the session by the timestamps at logon and at logoff by looking at the **Logged** field.

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4625
Level:	Information
User:	N/A
OpCode:	Info
More Information:	Event Log Online Help

4.3.1 Hunting Suspicious Accounts

Another Event ID (also mentioned earlier) to hunt for would be **Event ID 4672** (Special privileges assigned to new logon).

We would like to see if there are any unusual accounts logged into machines with admin rights when they shouldn't have admin rights, or hunting for privileged local accounts being used to log into other machines remotely, instead of using legitimate network accounts.

4672

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4672>

4.3.1 Hunting Suspicious Accounts

Keep in mind that we will have to look at different sources to determine logon/session information via event logs.

Some event logs might be local to the workstation, but some might be on the server, such as the domain controller, or other machine that was accessed.

This outlines the importance of having a central logging server, which we discuss more in the upcoming slides.

THPV2: Section 03, Module 04 - Caendra Inc. © 2020 | p.43

Hunting for the Password Attacks

4.3.2 Hunting Password Attacks

We will be looking for **Event ID 4625** (failed logon) and **Logon Type 3** (network logon).

Overall, looking for a rapid succession of failed attempts to the same machine, or multiple machines, repeatedly in a small amount of time with each attempt, may indicate Password Spraying/Guessing attack. Of course, we know the attacker can change the timing between each attempt to make it look less suspicious.

Hunting for the Pass the Hash

4.3.3 Hunting Pass The Hash

In a blog post, David Kennedy (ReL1K) shares a technique to hunt for PTH attacks with a low false positive rate.

The Event ID to hunt for is **Event ID 4624** with **Logon Type 3**. We should also look for the Logon Process to be NtLmSsP and the key length to be set to 0.

You can read more about this technique, [here](#).

Hunting Golden Tickets

4768(S, F): A Kerberos authentication ticket (TGT) was requested.

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4768>

4.3.4 Hunting Golden Tickets

Oftentimes, attackers leverage native Kerberos functionality. For example, this is the case when a golden ticket is created. A golden ticket is a forged Ticket-Granting Ticket that provides the attacker with access to every network asset. You should therefore be familiar with Kerberos-related Event IDs, like [4768](#), when hunting for this type of attack.

More in-depth research about detecting pass-the-ticket and Golden Tickets can be found [here](#) and [here](#), respectively.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4768>
<https://blog.shashibitz.com/detect-pass-the-ticket-attacks>
https://cert.europa.eu/static/WhitePapers/UPDATED - CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf

Researches about the detecting the ticket and golden tickets can be found

<https://blog.netwrix.com/2022/09/28/how-to-detect-pass-the-ticket-attacks/>

Hunting RDP sessions

4.3.5 Hunting RDP Sessions

If your network environment is accustomed to a lot of RDP connections into other machines, then this can be difficult to hunt for.

When hunting for RDP sessions, we're looking for **Event IDs 4624 & 4778** with **Logon Type 10** (Terminal Services or RDP). Also, note the expected Event IDs after successful or failed authentication attempts. You can also check out resources from the Threat Hunting Project, [here](#).

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624>
<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4778>
https://github.com/TheHuntingProject/ThreatHunting/blob/main/assets/windows_rdp_extrime_access.md

4624(S): An account was successfully logged on.

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624>

4778(S): A session was reconnected to a Window Station.

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4778>

Resources from threat hunting project
[ThreatHuntingProject/ThreatHunting](#)

Hunting PsExec

4.3.6 Hunting PsExec

PsExec, part of the [SysInternals Suite](#), is one of the common lateral movement tools, which provides the capability to execute remote commands. Due to the way that PsExec works, we can utilize the following Event IDs to hunt for it:

- [5145](#) (captures requests to shares, we are interested in ADMIN\$ and IPC\$)
- [5140](#) (share successfully accessed)
- [4697 / 7045](#) (service creation)
- [4688](#) / Sysmon EID 1

https://docs.microsoft.com/en-us/sysinternals/
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5145
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5140
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4697
https://www.manageengine.com/products/activity-directory-audit-kb/system-audit/events/event-id-7045.html
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4688

Sysinternals

<https://learn.microsoft.com/en-us/sysinternals/>

We can use this event IDs to hunt for PsExec

5145	Captures requests to shares, we are interested in ADMIN\$ and IPC\$
5140	Share successfully accessed
4679/7045	Service creation
4688	Sysmon EID 1

4.3.6 Hunting PsExec

While you can certainly look for the default indicators, such as a service with the name "PSEXECsvc" being created on the remote machine, much of the behavior is customizable. As Endgame points out in their [guide to threat hunting](#)*^{*}, you may get more complete results if you look for any executable that uses "\\" and the "-accepteula" prefix.

Tools like PsExec are common. Red Canary released a detailed blog post on ways of hunting for them [here](#).

*Click the resources drop-down menu in the appropriate module line to access 'The Endgame Guide to Threat Hunting - ebook' pdf attachment.
https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/

Threat Hunting for PsExec, Open-Source Clones, and Other Lateral Movement Tools

<https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/>

Hunting WMI Persistence

4.3.7 Hunting WMI Persistence

Hunting WMI usage for persistence involves the creation of a WMI subscription. Therefore, our goal is to search for and identify any newly registered subscriptions.

One way to achieve this is by utilizing WMI itself to monitor for that activity. Full details of this technique are available from FireEye [here](#).

WMI vs. WMI: Monitoring for Malicious Activity

<https://www.mandiant.com/resources/blog/wmi-vs-wmi-monitor>

Hunting for scheduled Tasks

4.3.8 Hunting Scheduled Tasks

Event ID 4698 (a scheduled task was created) is what we'll hunt for. Also, **Event IDs 106, 200, and 201** all relate to scheduled tasks. Here is an example log entry.

Event Properties - Event 4698, Microsoft Windows security auditing.
General [Details]
A scheduled task was created.
Subject: Security ID: CONTOSO\administrator
Account Name: administrator
Logon ID: 0x3E8
Task:
Task Name: MyNewStartUpTask
Task Content:
<Task xmlns="http://schemas.microsoft.com/windows/2004/02/ns/Default">
 <TaskGuid>{221983D8-B268-4C61-90B1-000000000000}</TaskGuid>
 <Author>CONTOSO\administrator</Author>
 <Priority>1</Priority>
 <Triggers />
 <Principals>
 <Principal id="Author">
 <UserId>CONTOSO\administrator</UserId>
 <UserLogonName>CONTOSO\administrator</UserLogonName>
 </Principal>
 </Principals>
<Settings>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4698>
[https://technet.microsoft.com/en-us/library/dd363640\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd363640(v=ws.10).aspx)
[https://technet.microsoft.com/en-us/library/cc775088\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc775088(v=ws.10).aspx)
[https://technet.microsoft.com/en-us/library/cc774861\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc774861(v=ws.10).aspx)

4698(S): A scheduled task was created.

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4698>

Event ID 106 — General Task Registration

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd363640\(v=ws.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd363640(v=ws.10)?redirectedfrom=MSDN)

Event ID 200 — Task Monitoring and Control

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc775088\(v=ws.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc775088(v=ws.10)?redirectedfrom=MSDN)

Event ID 201 — Task Monitoring and Control

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc774861\(v=ws.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc774861(v=ws.10)?redirectedfrom=MSDN)

Hunting For service creation

4.3.9 Hunting Service Creations

Event ID 4697 (a service was installed in the system) is what we'll be hunting for to find the creation of suspicious services.

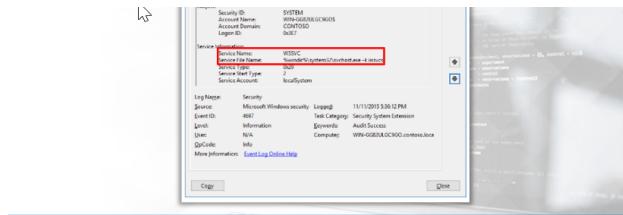
Event Properties - Event 4697, Microsoft Windows security auditing.
General [Details]
A service was installed in the system.
Subject:

EventID 4697

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4698>

4.3.9 Hunting Service Creations

Event Properties - Event 4697, Microsoft Windows security auditing.
General [Details]
A service was installed in the system.
Subject:



Hunting for Network shares

4.3.10 Hunting Network Shares

Event ID **4776** is specific to the NTLM protocol and notifies us of successful or failed authentication attempts.

Under Keywords, we should see either Audit Success or Audit Failure. Error Code will also give us information about the authentication attempt.

4777(F): The domain controller failed to validate the credentials for an account.

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4777>

4.3.10 Hunting Network Shares

Other Event IDs specific to network shares are **Event IDs 5140 and 5145**.

Note: In order to see these event logs, a policy setting must be enabled. This setting is within the **Advanced Audit Policy Configuration > Object Access > Audit File Share**.

5140(S, F): A network share object was accessed

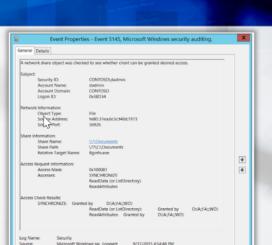
<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5140>

5148(F): The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5148>

4.3.10 Hunting Network Shares

A log entry of event ID 5145 is shown on the image to the right.





Hunting for lateral movement

4.3.11 Hunting Lateral Movement

When hunting for lateral movement, we'll refer to research performed by the Japan Computer Emergency Response Team Coordination Center - the results of the research are available [here](#).

You can also check out resources from the Threat Hunting Project [here](#), [here](#), and [here](#).

<https://jpcertcc.github.io/ToolAnalysisResultSheet/>
<https://github.com/ThreatHuntingProject/ThreatHunting/blob/master/hunts/lateral-movement-via-explicit-credentials.md>
<https://github.com/ThreatHuntingProject/ThreatHunting/blob/master/hunts/lateral-movement-windows-authentication-logs.md>
https://github.com/ThreatHuntingProject/ThreatHunting/blob/master/hunts/lateral_movement_detection_via_process_monitoring.md

Research paper from Japan Computer Emergency Response Team.

<https://jpcertcc.github.io/ToolAnalysisResultSheet/>

Windows Lateral Movement via Explicit Credentials

[ThreatHuntingProject/ThreatHunting](https://github.com/ThreatHuntingProject/ThreatHunting/blob/master/hunts/lateral-movement-via-explicit-credentials.md)

Detecting Lateral Movement in Windows Event Logs

<https://github.com/ThreatHuntingProject/ThreatHunting/blob/master/hunts/lateral-movement-windows-authentication-logs.md#detecting-lateral-movement-in-windows-event-logs>

#Lateral Movement Detection via Process Monitoring

https://github.com/ThreatHuntingProject/ThreatHunting/blob/master/hunts/lateral_movement_detection_via_process_monitoring.md

Windows Event Forwarding

4.4 Windows Event Forwarding

As you can see, event logs are extremely useful, but they're only useful if you have them.

These logs shouldn't stay on the endpoint, but rather should be forwarded to a central server immediately.

4.4 Windows Event Forwarding

If this capability is not enabled currently in your environment, enabling it is something you should consider immediately.

Please read these additional resources from Microsoft regarding Windows Event Forwarding [here](#) and [here](#).



Use Windows Event Forwarding to help with intrusion detection

<https://learn.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection>

Windows Event Collector

<https://learn.microsoft.com/en-in/windows/win32/wec/windows-event-collector?redirectedfrom=MSDN>

Windows Log Rotation & Clearing

4.5 Windows Log Rotation & Clearing

If event logs are not forwarded, then they are at risk of being cleared (deleted) or rotated from the endpoint device.

To clear event logs, administrative rights are needed.

It is possible to clear the event logs without admin rights by flooding the endpoint with events to generate logs that will rotate the logs that can be seen within tools such as Event Viewer.

4.5 Windows Log Rotation & Clearing

Event IDs to hunt for regarding log clearing are **Event IDs 1102** and **104**.

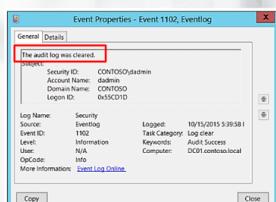
<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-1102>
<http://www.eventid.net/display-eventid-104-source-Microsoft-Windows-Eventlog-eventno-11441-phase-1.htm>

1102(S): The audit log was cleared.

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-1102>

4.5 Windows Log Rotation & Clearing

A log entry of event ID 1102 is shown on the image to the right.



General	Details
The audit log was cleared	
Access	
Security	Event ID: 1102
Source:	EventLog
Event ID:	1102
Level:	Information
User:	N/A
Opcode:	Info
More Information Event Log Online	

4.5 Windows Log Rotation & Clearing

Note that Event Logs are extremely difficult, if not impossible, to tamper with.

This means an attacker can't just modify an event log, which is good to know.

Again, to avoid the logs being cleared or rotated on the endpoint, they need to be forwarded to a central location.

4.5 Windows Log Rotation & Clearing

Once these logs are at the central location, then you need to consider log retention.

Do you keep 1 week of logs, 1 month, 6 months, etc.?

Tools

Sysmon

4.6.1 Sysmon

We're going to look at a tool from Sysinternals called [Sysmon](#).

System Monitor (**Sysmon**) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

<https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

4.6.1 Sysmon

"It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network."

4.6.1 Sysmon

Sysmon collects activity for 22 different events that may occur on the system, including an additional one which

indicates an error within Sysmon itself.

A list of all Event IDs is shown on the next slide.

4.6.1 Sysmon	
Event description	Event ID
Process Create	1
File creation time changed	2
Network connection detected	3
Sysmon service state change	4
Process terminated	5
Driver loaded	6
Image loaded	7
CreateRemoteThread detected	8
RawAccessRead detected	9
Process accessed	10
Event description	Event ID
File created	11
Registry object added or deleted	12
Registry value set	13
Registry object renamed	14
File stream created	15
Sysmon configuration change	16
Named pipe created	17
Named pipe connected	18
WMI filter	19
WMI consumer	20
Event description	Event ID
WMI consumer filter	21
DNS query	22
Error	255

4.6.1 Sysmon

Sysmon should be installed on all systems, which will ensure that data from them is available when you need it, either for Threat Hunting or for digital forensics and incident response (DFIR).

The events should be forwarded to a SIEM (discussed later in the module) to prevent deletion by adversaries, and for utilizing them centrally to detect anomalous activity on both single systems and also across multiple systems.

4.6.1 Sysmon

Sysmon requires configuration to be set, which tells it what events to capture, and whether to exclude certain events which are “known good”, for example.

The most widespread and recommended base configuration is the one from [SwiftOnSecurity](#), available [here](#). It can be used as a baseline, but additional configuration for your specific environment is also necessary and recommended.

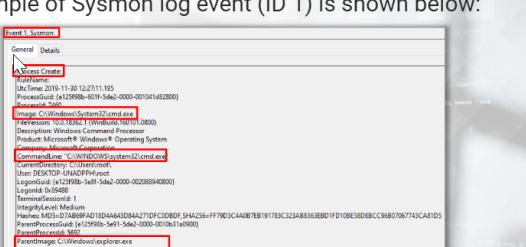
sysmon-config | A Sysmon configuration file for everybody to fork

[SwiftOnSecurity/sysmon-config](#)

Example

4.6.1 Sysmon

An example of Sysmon log event (ID 1) is shown below:



The screenshot shows a detailed view of a Sysmon log entry for a Process Create event (ID 1). The event details are as follows:

- UtcTime: 2019-11-30 12:27:11.195
- ProcessGuid: {41299B-0015-40d0-8000-000000000000}
- CommandLine: "C:\Windows\System32\cmd.exe"
- User: DESKTOP-UHADPHV\root
- LogonGuid: {41299B-5eef-5e6c-0000-000000000000}
- TerminalSessionId: 1
- Image: C:\Windows\System32\cmd.exe
- Hemu: M05=07A89FAD1D4A61D9AA271FC0080F54A256+FF79D1C4A0B7E19178C123AB3638BD1D108E50D8BC36807067742CA1D5
- ParentProcessGuid: {41299B-5eef-5e6c-0000-000000000000}
- ParentImage: C:\Windows\explorer.exe
- ParentCommandline: C:\Windows\Explorer.exe

4.6.1 Sysmon

We can use Sysmon to search/alert for certain malicious behaviors related to:

- Image paths
- Command line arguments
- Process injection
- Process parent-child relationships
- Network connections to certain domain names
- Lateral movement
- Etc.

SIEM

4.6.2 SIEM

Another invaluable item used within our hunts is a **SIEM**, **Security Information and Event Management**, platform.

This appliance will ingest various logs from different types of security equipment, such as firewalls, IPS systems, and even threat intelligence feeds.

We can then create alerts, dashboards, and perform queries to sift through thousands upon thousands of log entries.

4.6.2 SIEM

There are various commercial SIEM products you can look at and invest in, such as LogRhythm, ArcSight, Splunk, QRadar, and USM to name a few.

ELK Stack

4.6.3 ELK Stack

In this course, we'll be looking at **ELK Stack** to sift through Windows Event Logs and PowerShell Logs to hunt for evil.

It's a good choice, because we're not looking at any other types of logs, such as firewall, proxy, etc., just Windows logs.

4.6.3 ELK Stack

The ELK Stack is comprised of 3 open source products: **Elasticsearch**, **Logstash**, and **Kibana**.

All three of these open source products are from [Elastic](#).

You can read more about the ELK Stack, including tutorials on how to implement and use these products [here](#).

THE COMPLETE GUIDE TO THE ELK STACK

<https://logz.io/learn/complete-guide-elk-stack/>

CHOOSING THE RIGHT SIEM SOLUTION FOR YOUR NEEDS

<https://www.netsurion.com/EventTracker/media/EventTracker/Files/whitepapers/WP-SIEM-Choosing.pdf>

Splunk vs ELK: Which Works Best For You?

<https://www.upguard.com/blog/splunk-vs-elk>

a