Seeing Through The Windows: Centralizing Windows Logs For Greater Visibility

Matthew Gracie
Packet Hacking Village
2021

Who Am I And What Am I Talking About?

So Why Do We Want To Centralize Our Windows Logs, Anyway?

Attackers view

Defenders view

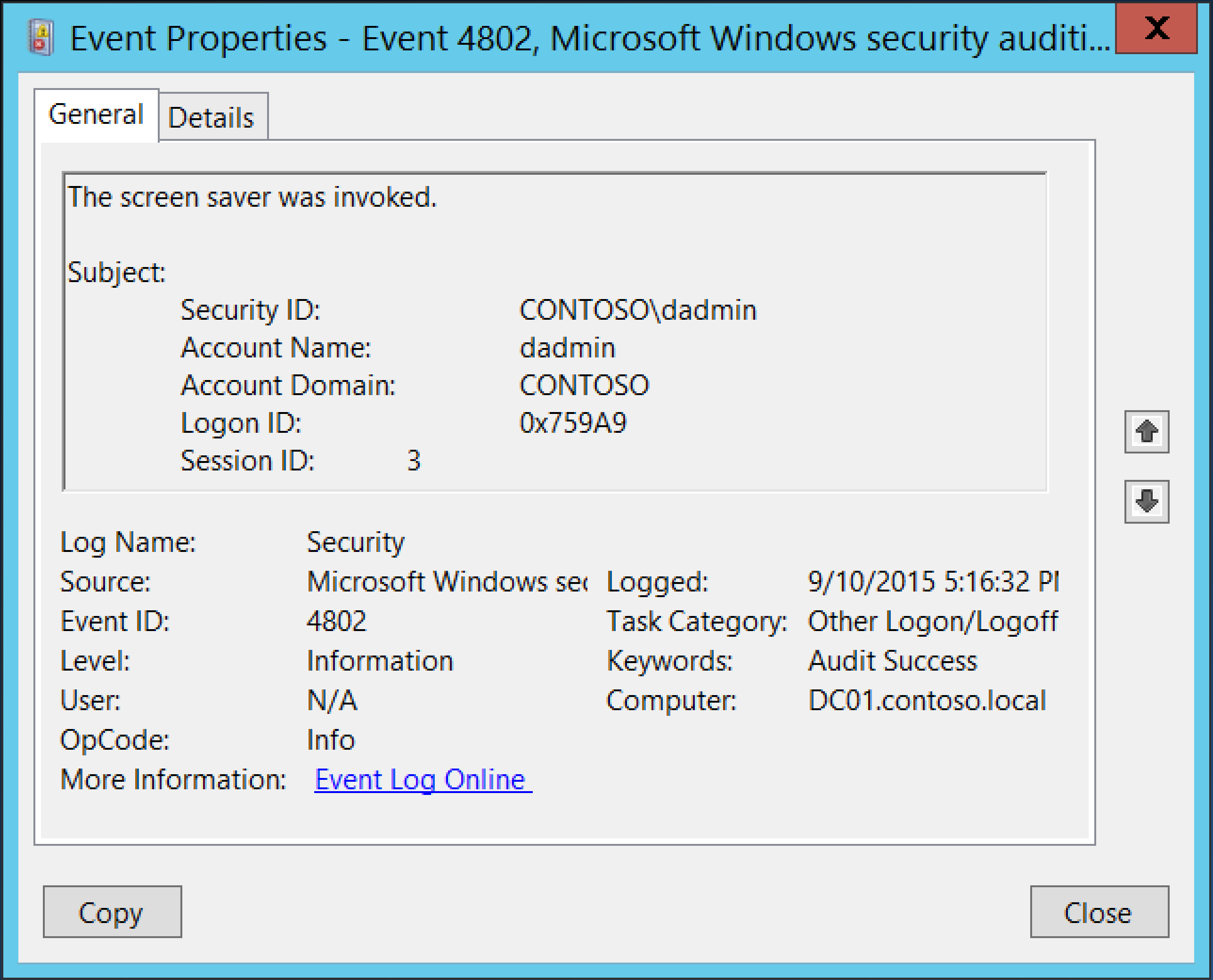
But Why Endpoint Logs?

“According to FortiGuard Labs, the total percentage of encrypted web traffic is now around 85%, up from just 55% in Q3 of 2017. This traffic is a larger and larger slice of a steadily increasing pie.” --Fortinet, August 2020

So How Do We Do It?

Windows Event Logs

- Windows records system events in local Event Log files, including the classics: Application, Setup, System, and Security.
- Windows 2000 introduced per-application log files.
- Windows Vista rewrote everything with an XML event definition standard.
- Every Event has a standard numeric Event ID.



Event Properties - Event 4802, Microsoft Windows security auditi...
X
General
Details

```
The screen saver was invoked.

Subject:
	Security ID:		CONTOSO\dadmin
	Account Name:		dadmin
	Account Domain:		CONTOSO
	Logon ID:		0x759A9
	Session ID:	3
```

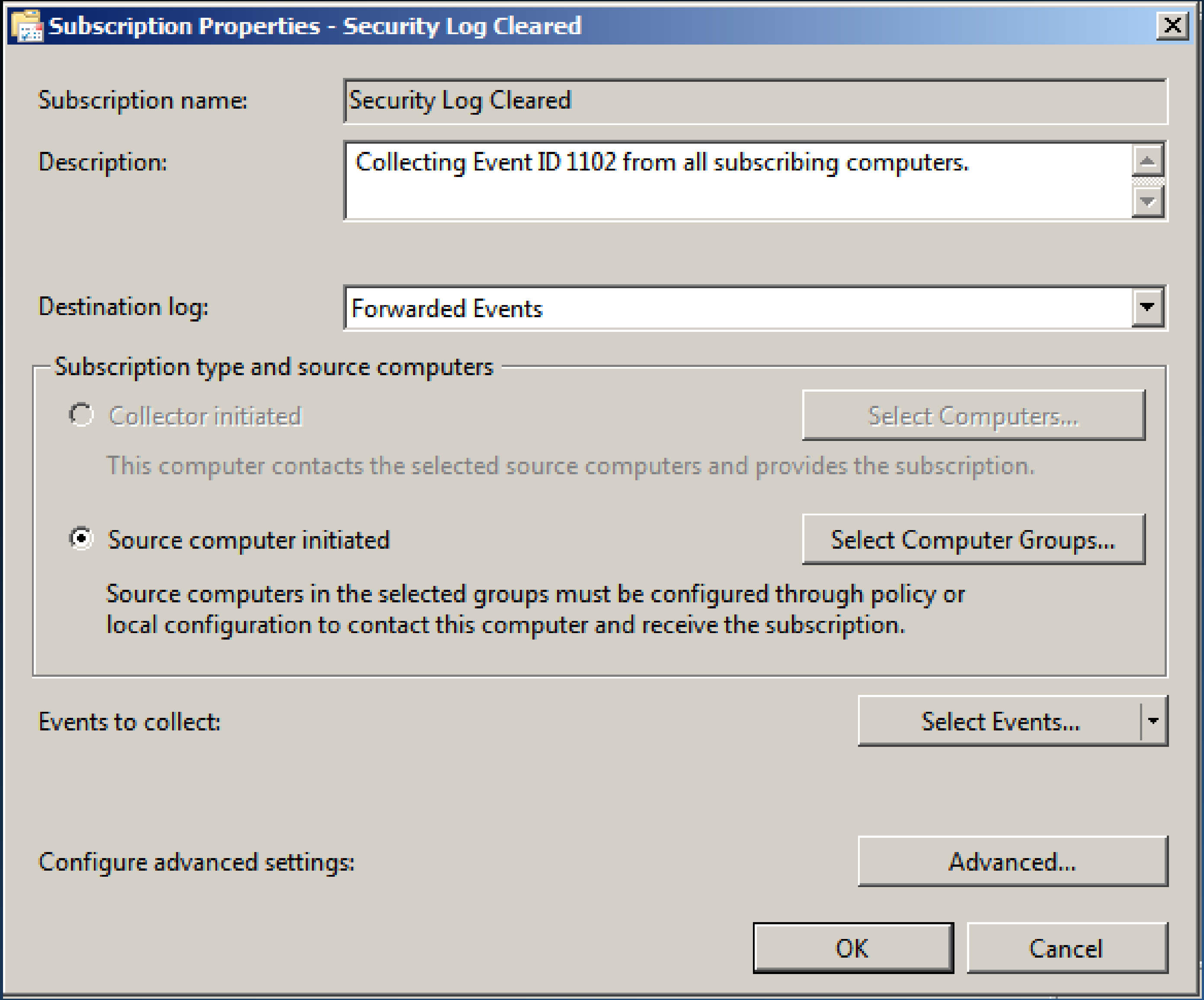
```
Log Name:          Security
Source:            Microsoft Windows sec   Logged:          9/10/2015 5:16:32 PI
Event ID:          4802                    Task Category:   Other Logon/Logoff
Level:             Information             Keywords:        Audit Success
User:              N/A                     Computer:        DC01.contoso.local
OpCode:            Info
More Information:  Event Log Online
```

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
 <EventID>4802</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12551</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-11T00:16:32.377883700Z" />
 <EventRecordID>237662</EventRecordID>
 <Correlation />
 <Execution ProcessID="504" ThreadID="1676" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="TargetUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
 <Data Name="TargetUserName">dadmin</Data>
 <Data Name="TargetDomainName">CONTOSO</Data>
 <Data Name="TargetLogonId">0x759a9</Data>
 <Data Name="SessionId">3</Data>
 </EventData>
 </Event>
```

Windows Event Forwarding

On an enterprise AD network, specific Event IDs can be forwarded to a central location by using Windows Event Forwarding.

This requires only a Windows Server to act as the “subscription server” and a GPO to tell the endpoints where to get their information.



Subscription Properties - Security Log Cleared

Subscription name: Security Log Cleared

Description: Collecting Event ID 1102 from all subscribing computers.

Destination log: Forwarded Events

Subscription type and source computers

○ Collector initiated

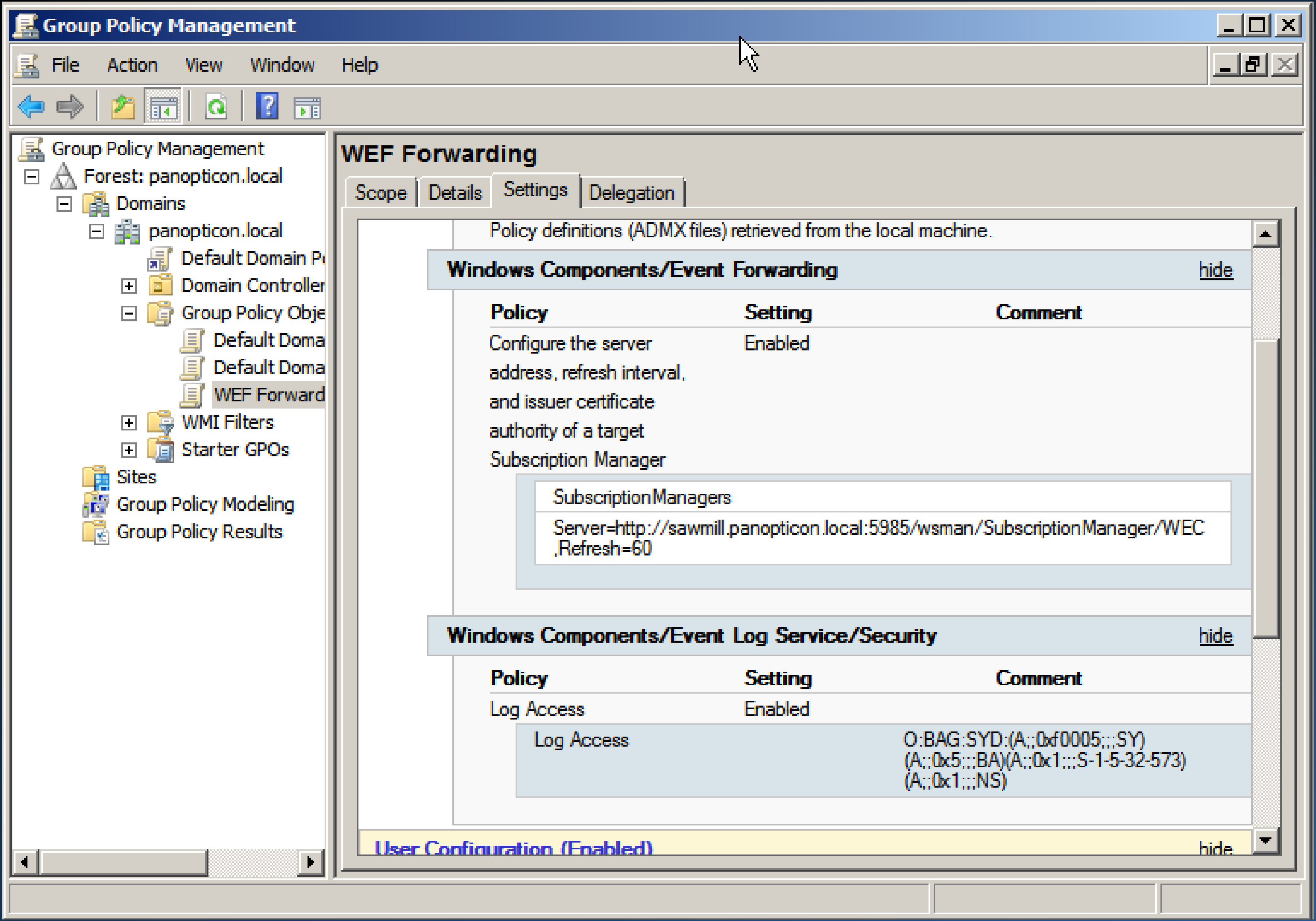
This computer contacts the selected source computers and provides the subscription.

● Source computer initiated

Source computers in the selected groups must be configured through policy or
local configuration to contact this computer and receive the subscription.

Events to collect:

Configure advanced settings:



WEF Forwarding

Policy definitions (ADMX files) retrieved from the local machine.

Windows Components/Event Forwarding

Policy	Setting	Comment
Configure the server address, refresh interval, and issuer certificate authority of a target Subscription Manager	Enabled	

SubscriptionManagers

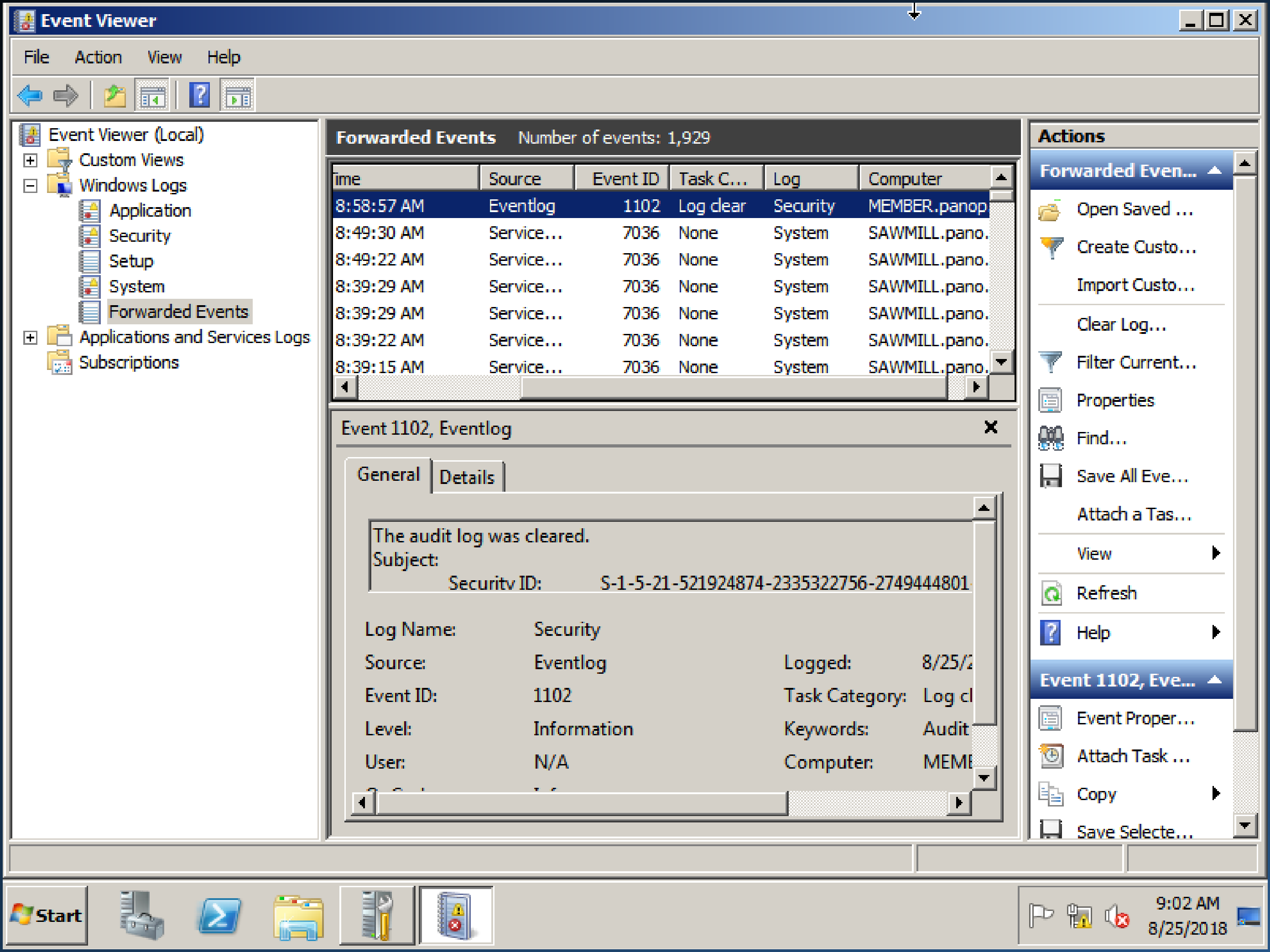
```
Server=http://sawmill.panopticon.local:5985/wsman/SubscriptionManager/WEC
,Refresh=60
```

Windows Components/Event Log Service/Security

Policy	Setting	Comment
Log Access	Enabled	

Log Access

```
O:BAG:SYD:(A;;0xf0005;;;SY)
(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
(A;;0x1;;;NS)
```



Forwarded Events   Number of events: 1,929

ime	Source	Event ID	Task C...	Log	Computer
8:58:57 AM	Eventlog	1102	Log clear	Security	MEMBER.panop
8:49:30 AM	Service...	7036	None	System	SAWMILL.pano.
8:49:22 AM	Service...	7036	None	System	SAWMILL.pano.
8:39:29 AM	Service...	7036	None	System	SAWMILL.pano.
8:39:29 AM	Service...	7036	None	System	SAWMILL.pano.
8:39:22 AM	Service...	7036	None	System	SAWMILL.pano.
8:39:15 AM	Service...	7036	None	System	SAWMILL.pano.

Event 1102, Eventlog

General   Details

The audit log was cleared.
Subject:
Security ID: S-1-5-21-521924874-2335322756-2749444801

Log Name:	Security		
Source:	Eventlog	Logged:	8/25/2
Event ID:	1102	Task Category:	Log cl
Level:	Information	Keywords:	Audit
User:	N/A	Computer:	MEMI

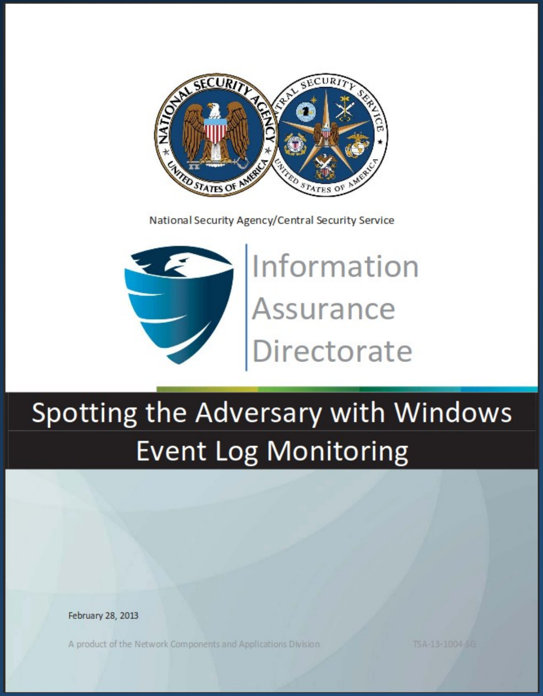
What Events to Monitor?

- Security Event Logs being cleared.
- High value groups like Domain Admins being changed.
- Local administrator groups being changed.
- Local users being created or deleted on member systems.
- New Services being installed, particularly on Domain Controllers (as this is often an indicator of malware or lateral movement behavior).

Jessica Payne
“Monitoring What Matters”

Any Other Suggestions?

- Changes to Scheduled Tasks.
- Password resets.
- Software installations.
- Account creation / enabling.
- Honeytokens.
- Legacy accounts.
- RDP logins.



National Security Agency/Central Security Service

Information Assurance Directorate

Spotting the Adversary with Windows Event Log Monitoring

February 28, 2013

A product of the Network Components and Applications Division

TSA-13-1004-SG

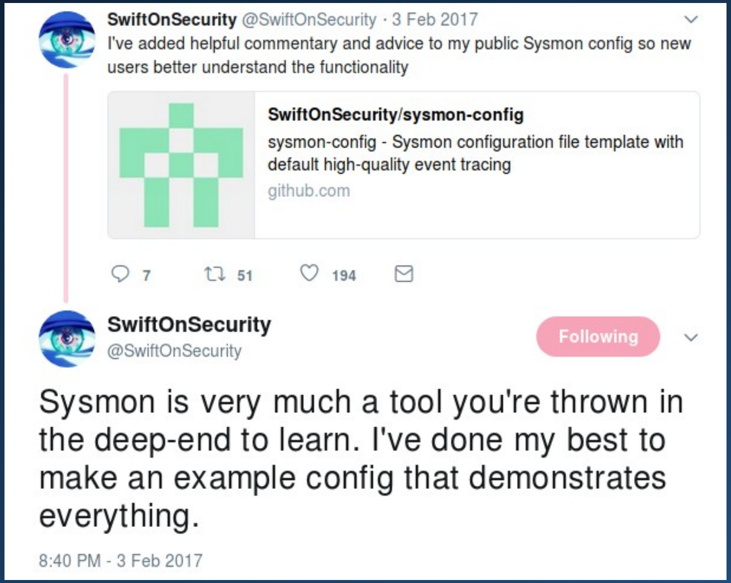
Sysmon

“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. 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.”

Sysmon Download Page

Sysmon

There are several freely available Sysmon configurations available on the Internet. One of the best is from @SwiftOnSecurity.



SwiftOnSecurity @SwiftOnSecurity · 3 Feb 2017

I've added helpful commentary and advice to my public Sysmon config so new users better understand the functionality

SwiftOnSecurity/sysmon-config

sysmon-config - Sysmon configuration file template with default high-quality event tracing

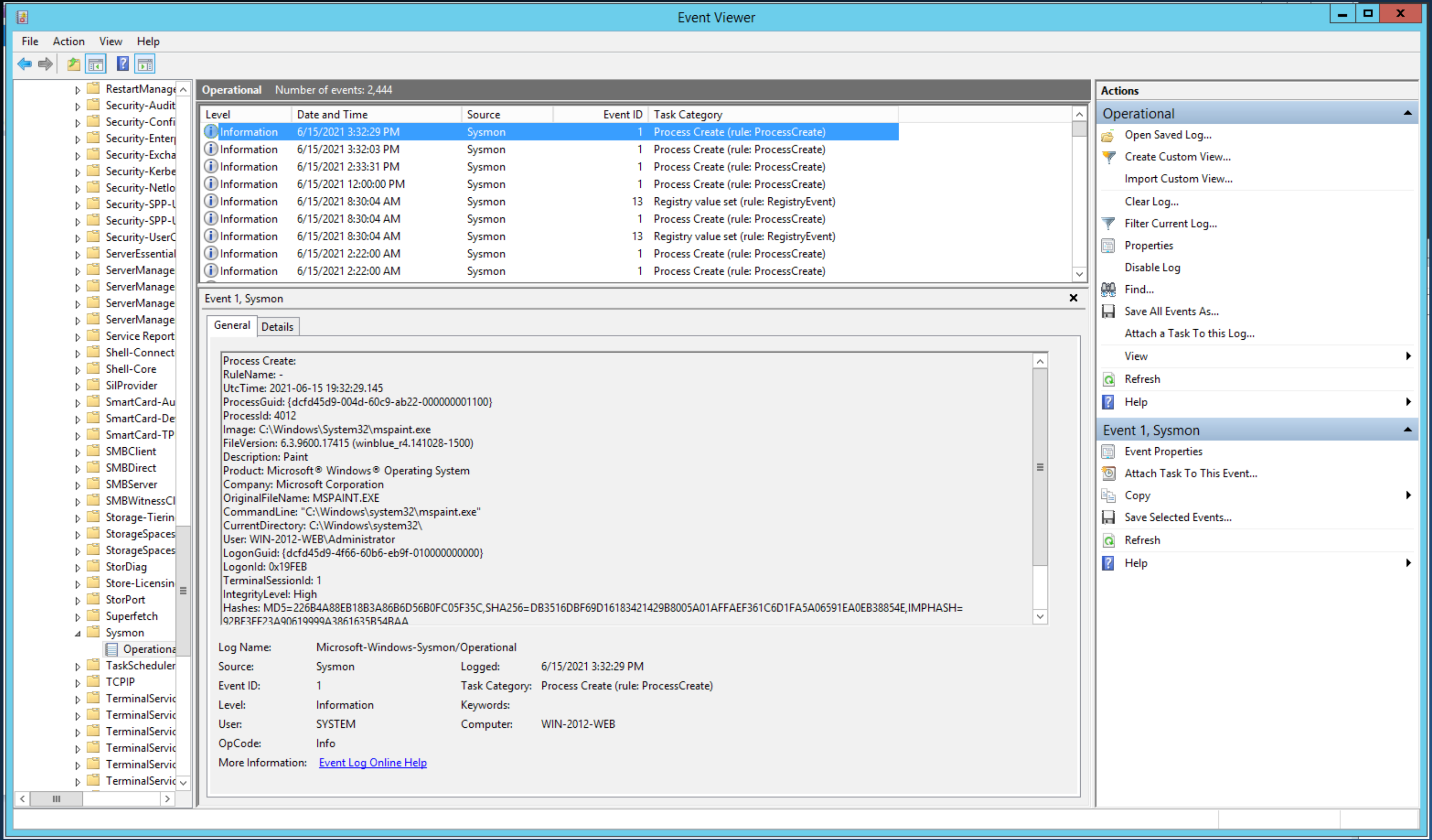
github.com

SwiftOnSecurity

@SwiftOnSecurity

Sysmon is very much a tool you're thrown in the deep-end to learn. I've done my best to make an example config that demonstrates everything.

8:40 PM - 3 Feb 2017



Operational Number of events: 2,444

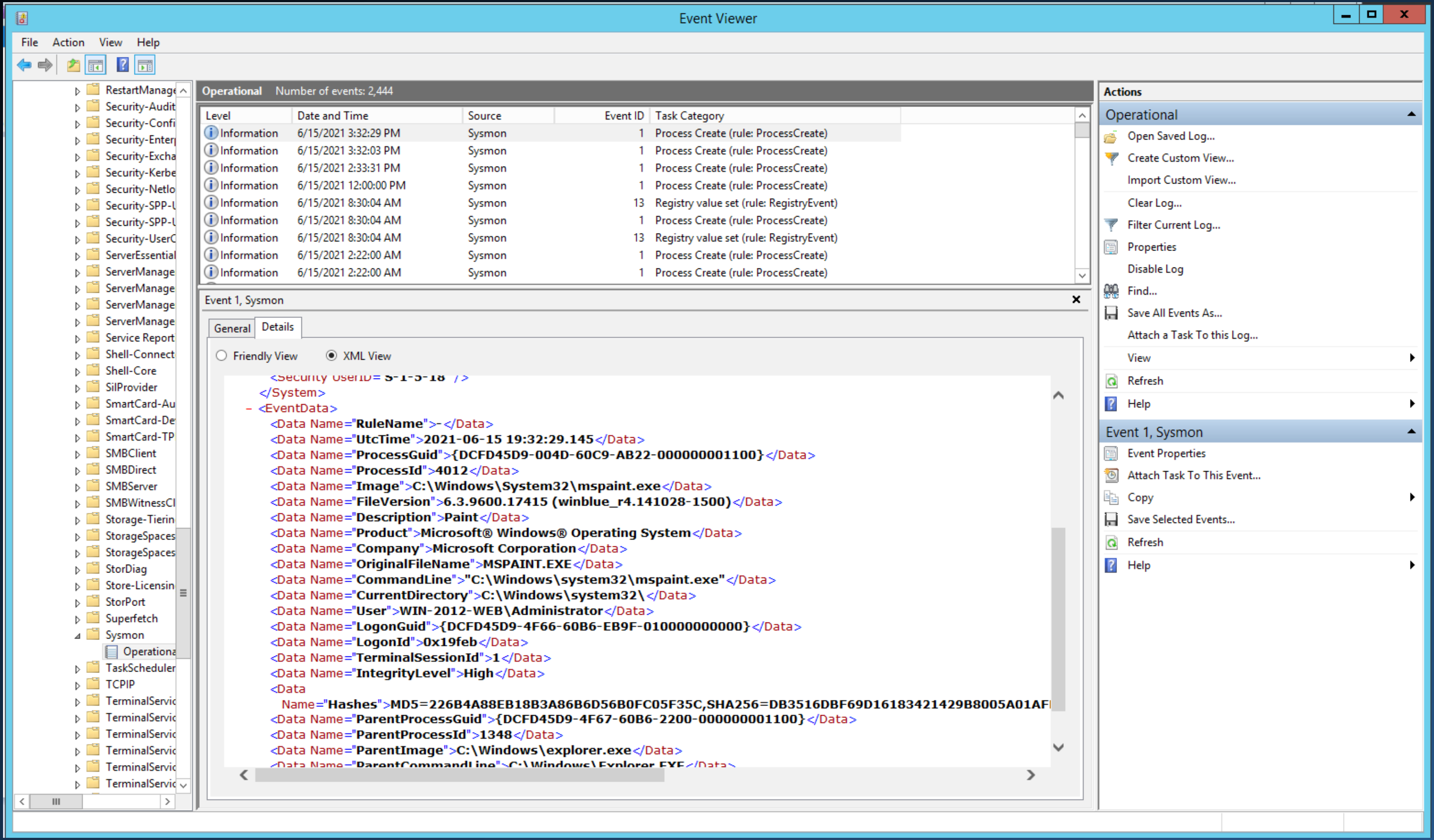
Level	Date and Time	Source	Event ID	Task Category
Information	6/15/2021 3:32:29 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 3:32:03 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 2:33:31 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 12:00:00 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 8:30:04 AM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	6/15/2021 8:30:04 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 8:30:04 AM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	6/15/2021 2:22:00 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 2:22:00 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

General Details

```
Process Create:
RuleName: -
UtcTime: 2021-06-15 19:32:29.145
ProcessGuid: {dcfd45d9-004d-60c9-ab22-000000001100}
ProcessId: 4012
Image: C:\Windows\System32\mspaint.exe
FileVersion: 6.3.9600.17415 (winblue_r4.141028-1500)
Description: Paint
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: MSPAINT.EXE
CommandLine: "C:\Windows\system32\mspaint.exe"
CurrentDirectory: C:\Windows\system32\
User: WIN-2012-WEB\Administrator
LogonGuid: {dcfd45d9-4f66-60b6-eb9f-010000000000}
LogonId: 0x19FEB
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=226B4A88EB18B3A86B6D56B0FC05F35C,SHA256=DB3516DBF69D16183421429B8005A01AFFAEF361C6D1FA5A06591EA0EB38854E,IMPHASH=
92BF3FF23A90619999A3861635B54BAA
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	6/15/2021 3:32:29 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WIN-2012-WEB
OpCode:	Info		
More Information:	Event Log Online Help		



Operational Number of events: 2,444

Level	Date and Time	Source	Event ID	Task Category
Information	6/15/2021 3:32:29 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 3:32:03 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 2:33:31 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 12:00:00 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 8:30:04 AM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	6/15/2021 8:30:04 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 8:30:04 AM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	6/15/2021 2:22:00 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2021 2:22:00 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

General Details

○ Friendly View ● XML View

```
      <Security UserID="S-1-5-18" />
    </System>
  - <EventData>
      <Data Name="RuleName">-</Data>
      <Data Name="UtcTime">2021-06-15 19:32:29.145</Data>
      <Data Name="ProcessGuid">{DCFD45D9-004D-60C9-AB22-000000001100}</Data>
      <Data Name="ProcessId">4012</Data>
      <Data Name="Image">C:\Windows\System32\mspaint.exe</Data>
      <Data Name="FileVersion">6.3.9600.17415 (winblue_r4.141028-1500)</Data>
      <Data Name="Description">Paint</Data>
      <Data Name="Product">Microsoft® Windows® Operating System</Data>
      <Data Name="Company">Microsoft Corporation</Data>
      <Data Name="OriginalFileName">MSPAINT.EXE</Data>
      <Data Name="CommandLine">"C:\Windows\system32\mspaint.exe"</Data>
      <Data Name="CurrentDirectory">C:\Windows\system32\</Data>
      <Data Name="User">WIN-2012-WEB\Administrator</Data>
      <Data Name="LogonGuid">{DCFD45D9-4F66-60B6-EB9F-010000000000}</Data>
      <Data Name="LogonId">0x19feb</Data>
      <Data Name="TerminalSessionId">1</Data>
      <Data Name="IntegrityLevel">High</Data>
      <Data
        Name="Hashes">MD5=226B4A88EB18B3A86B6D56B0FC05F35C,SHA256=DB3516DBF69D16183421429B8005A01AF
      <Data Name="ParentProcessGuid">{DCFD45D9-4F67-60B6-2200-000000001100}</Data>
      <Data Name="ParentProcessId">1348</Data>
      <Data Name="ParentImage">C:\Windows\explorer.exe</Data>
      <Data Name="ParentCommandLine">C:\Windows\Explorer.EXE</Data>
```

Powershell Logging

- With Powershell being such a common attacker tool, it might be best to enable enhanced logging in your environment.
- Powershell script block logging will record every Powershell command issued on an endpoint.
- Can be enabled via GPO or registry key.

Windows-Native Analysis Tools

With all the logs in one place, there are some freely available Windows tools for analysis.

- Event Viewer
- Log Parser (Studio)
- PowerBI Desktop

Log Shipping Mechanisms

If you prefer, there are a lot of options for moving them into another analysis platform.

- NXLog
- OSSEC / Wazuh
- Winlogbeat

Demonstration

Summary

- Centralizing the Event Logs in your environment can provide tremendous visibility into what’s happening on your network.
- As more network traffic is encrypted, endpoint logs become more important.
- Shipping those logs into an Elastic Stack makes them much easier to use for investigation.

For More Information

@InfosecGoon

infosecgoon@roadflares.org

https://github.com/InfosecGoon/

Resources

- On Encrypted Traffic: https://www.fortinet.com/blog/industry-trends/keeping-up-with-performance-demands-of-encrypted-web-traffic
- On Powershell Logging: https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- Monitoring What Matters: https://channel9.msdn.com/Events/Ignite/Australia-2015/INF327
- NSA Spotting The Adversary: https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm