A Series Of Unfortunate Windows Events

Matthew Gracie
IntroSecCon 2021

Who Am I And What Am I Talking About?

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

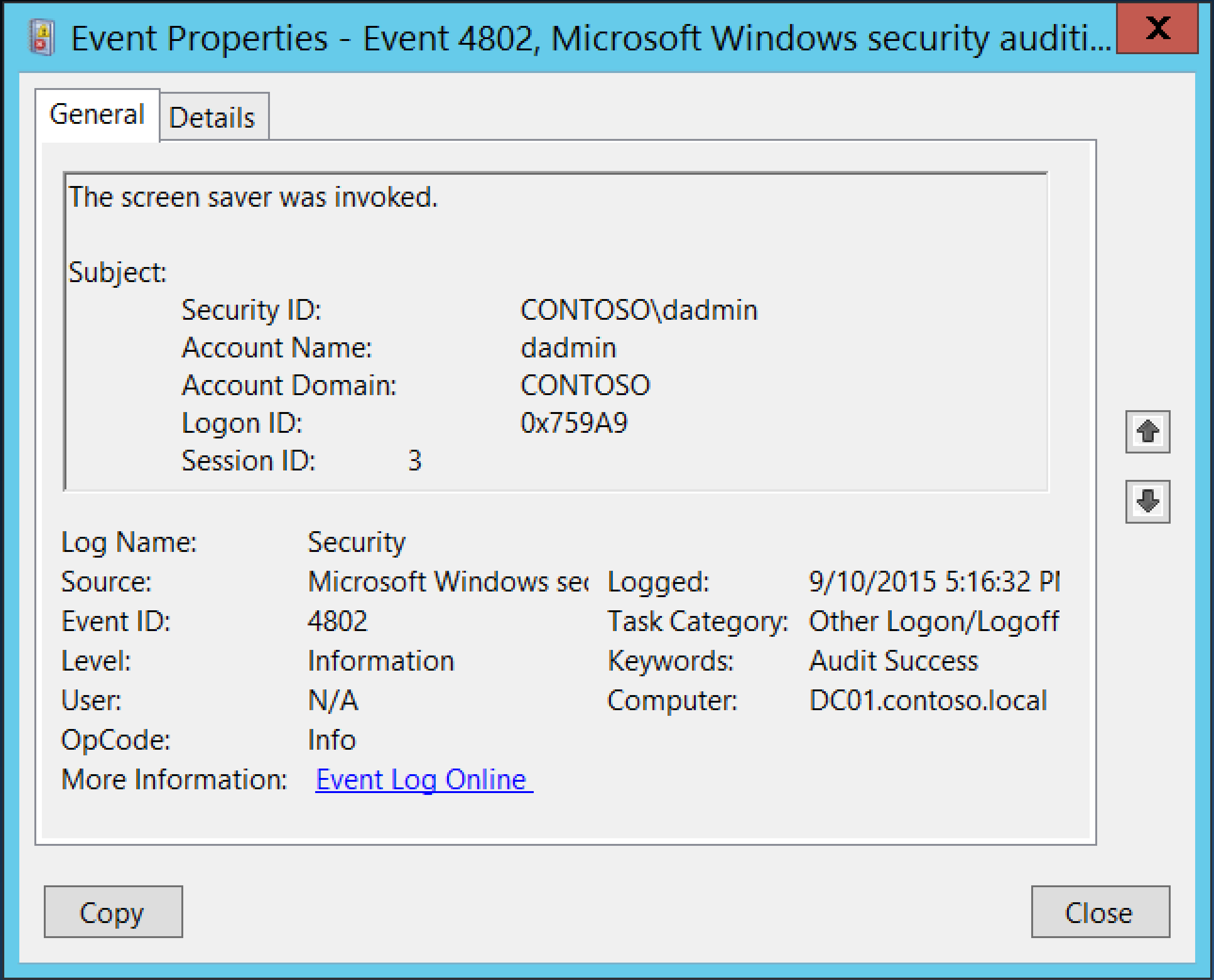
Attackers view

Defenders view

So How Do We Do It?

Windows Event Logs

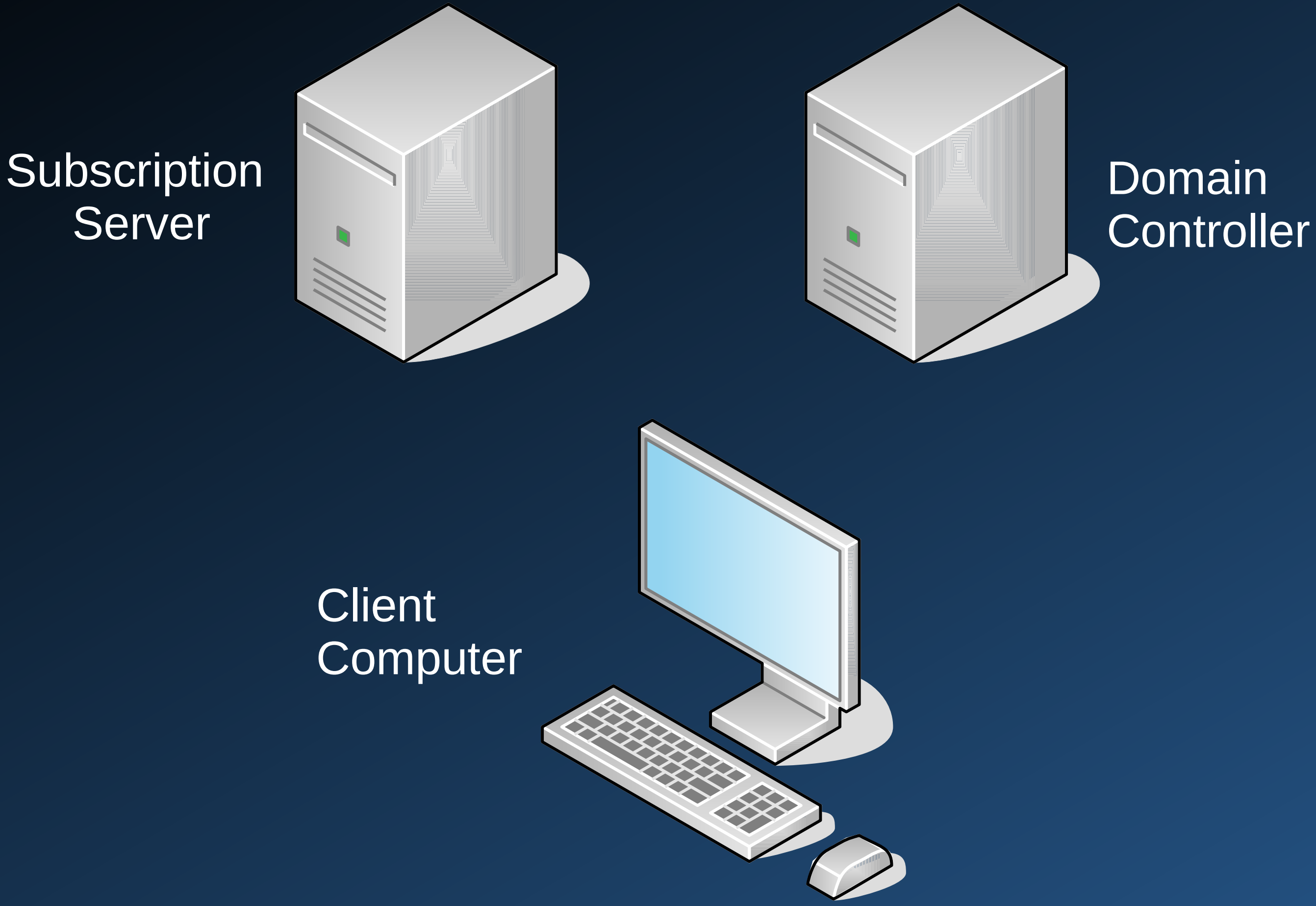
- Windows records system events in local Event Log files, including the classics: Application, Setup, System, and Security.
- Windows 2000 introduced per-application log files.
- Windows Vista rewrote everything with an XML event definition standard.
- Every Event has a standard numeric Event ID.


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

```
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 se    Logged:          9/10/2015 5:16:32 P
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
```

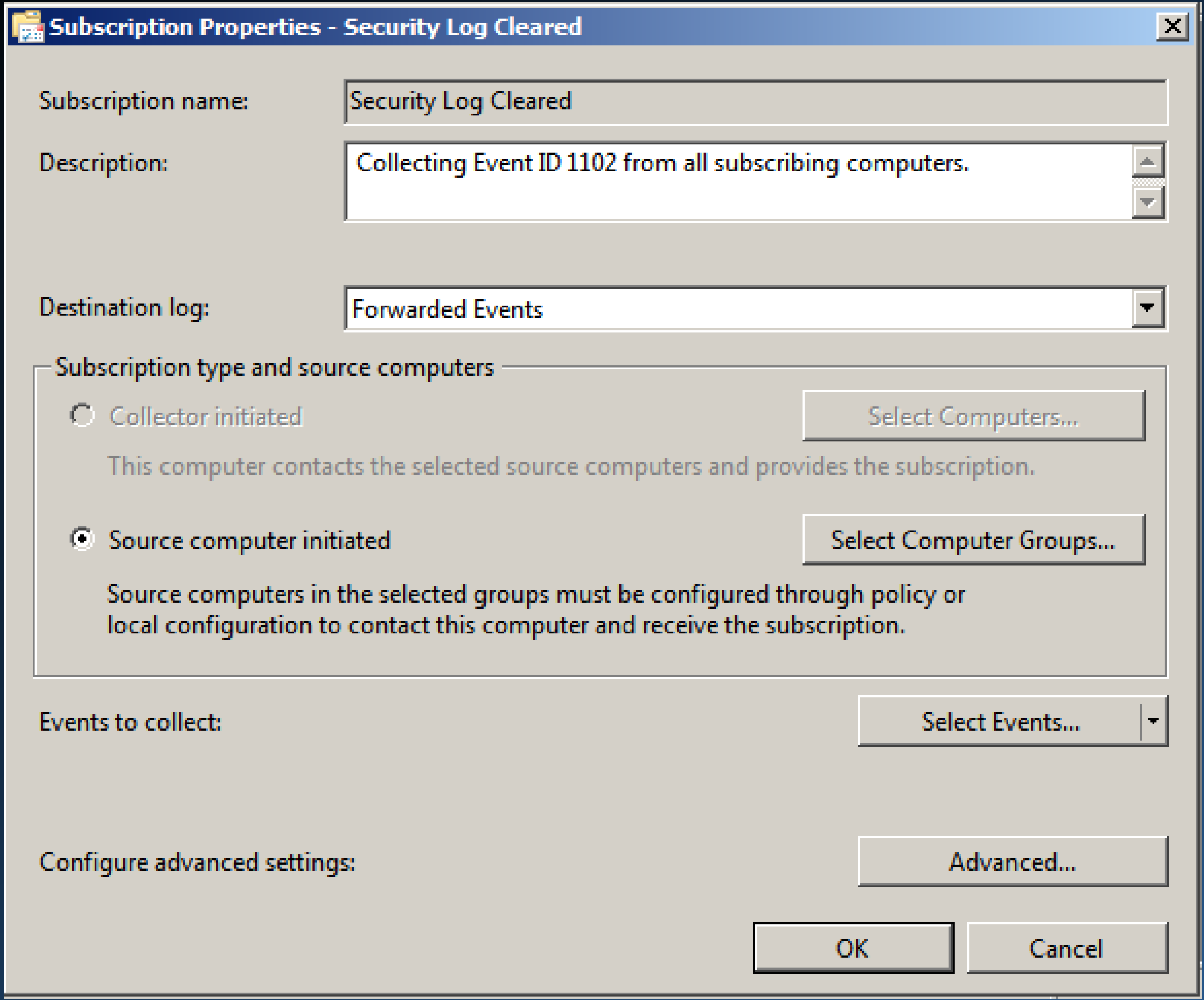
```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
  <EventID>4802</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>12551</Task>
  <Opcode>0</Opcode>
  <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>
```



Subscription Server

Domain Controller

Client Computer



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

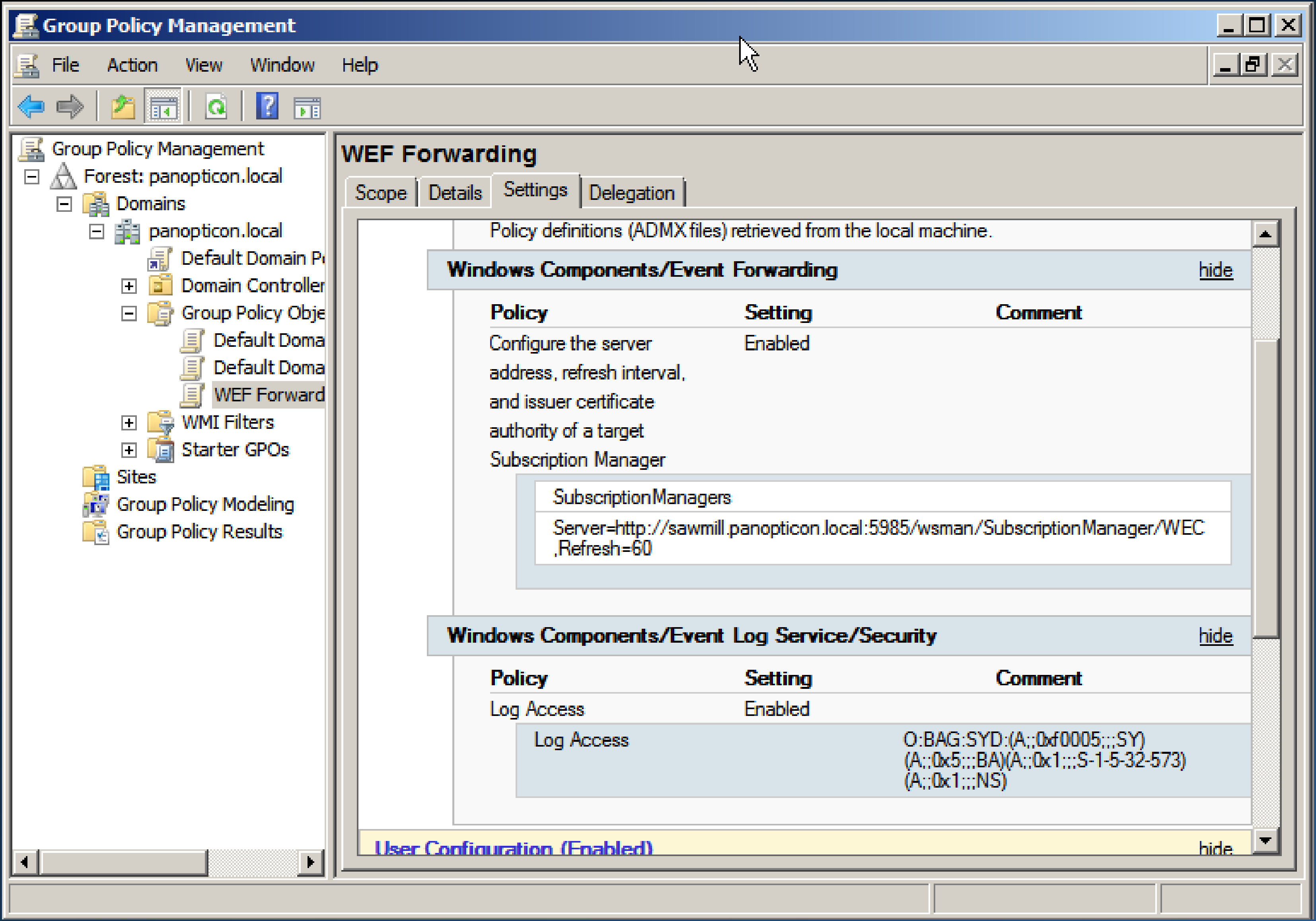
This computer contacts the selected source computers and provides the subscription.

● 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

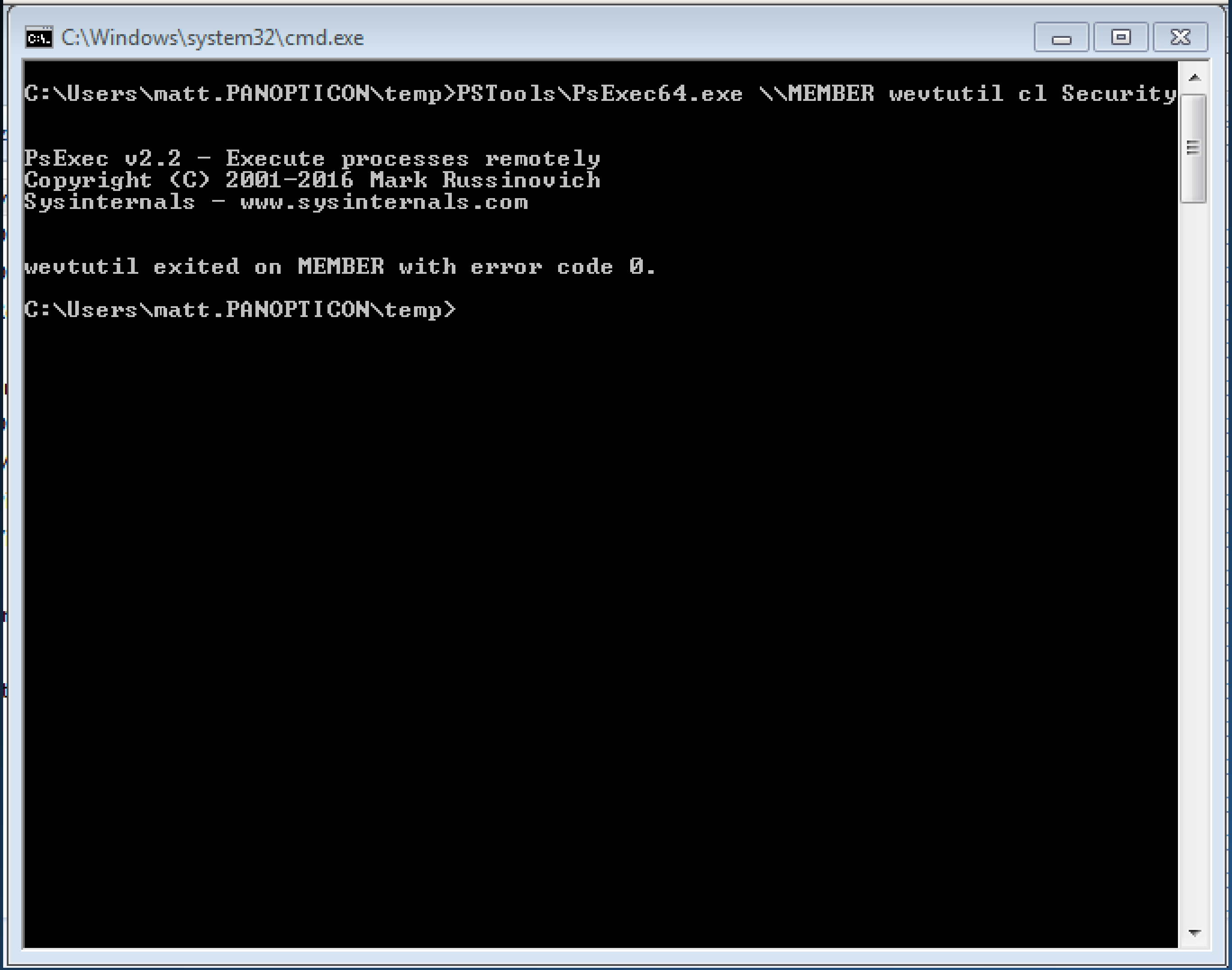
Server=http://sawmill.panopticon.local:5985/wsman/SubscriptionManager/WEC,Refresh=60

Windows Components/Event Log Service/Security

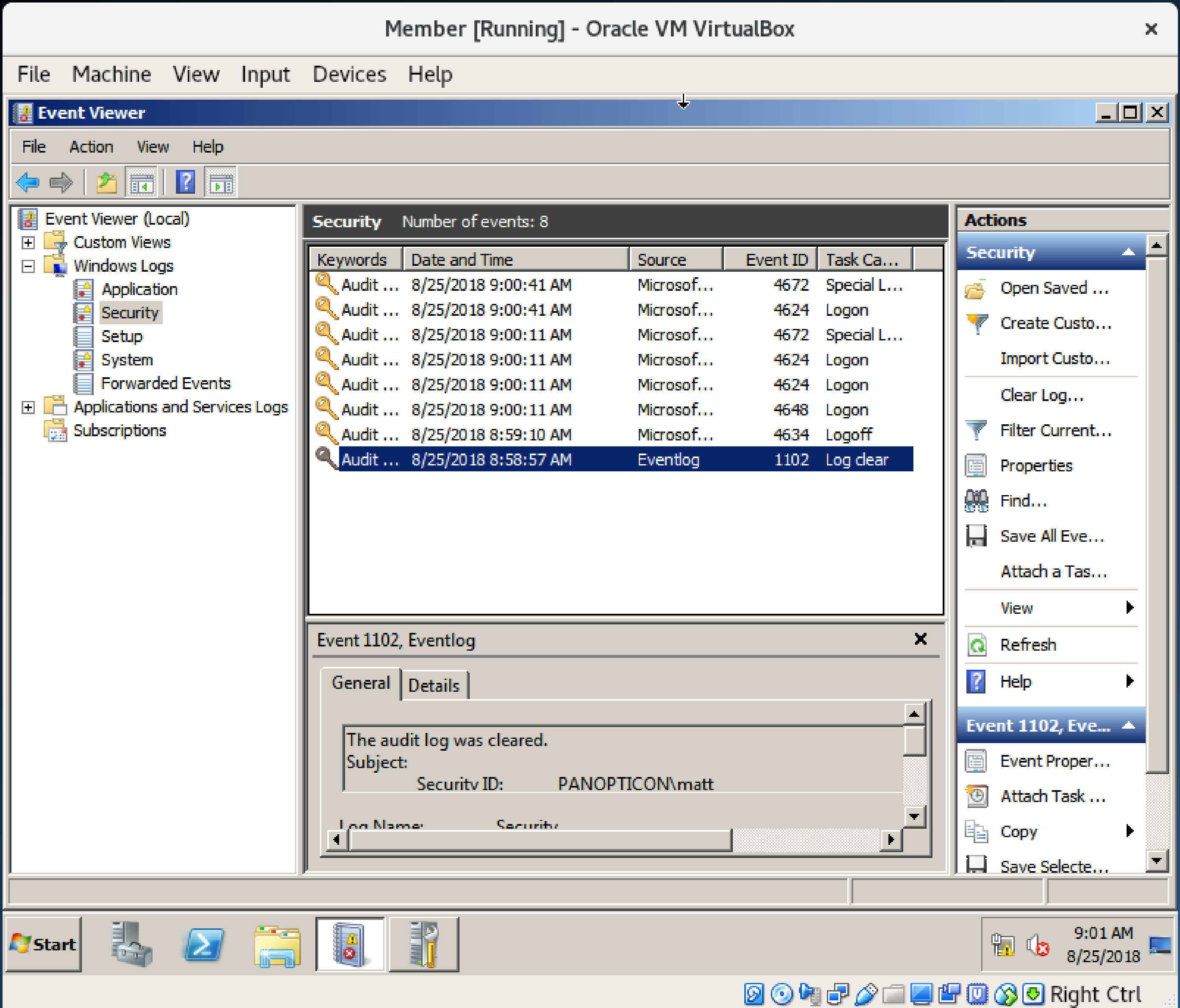
Policy	Setting	Comment
Log Access	Enabled	

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

User Configuration (Enabled)



```
C:\Users\matt.PANOPTICON\temp>PSTools\PsExec64.exe \\MEMBER wevtutil cl Security


PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


wevtutil exited on MEMBER with error code 0.

C:\Users\matt.PANOPTICON\temp>
```



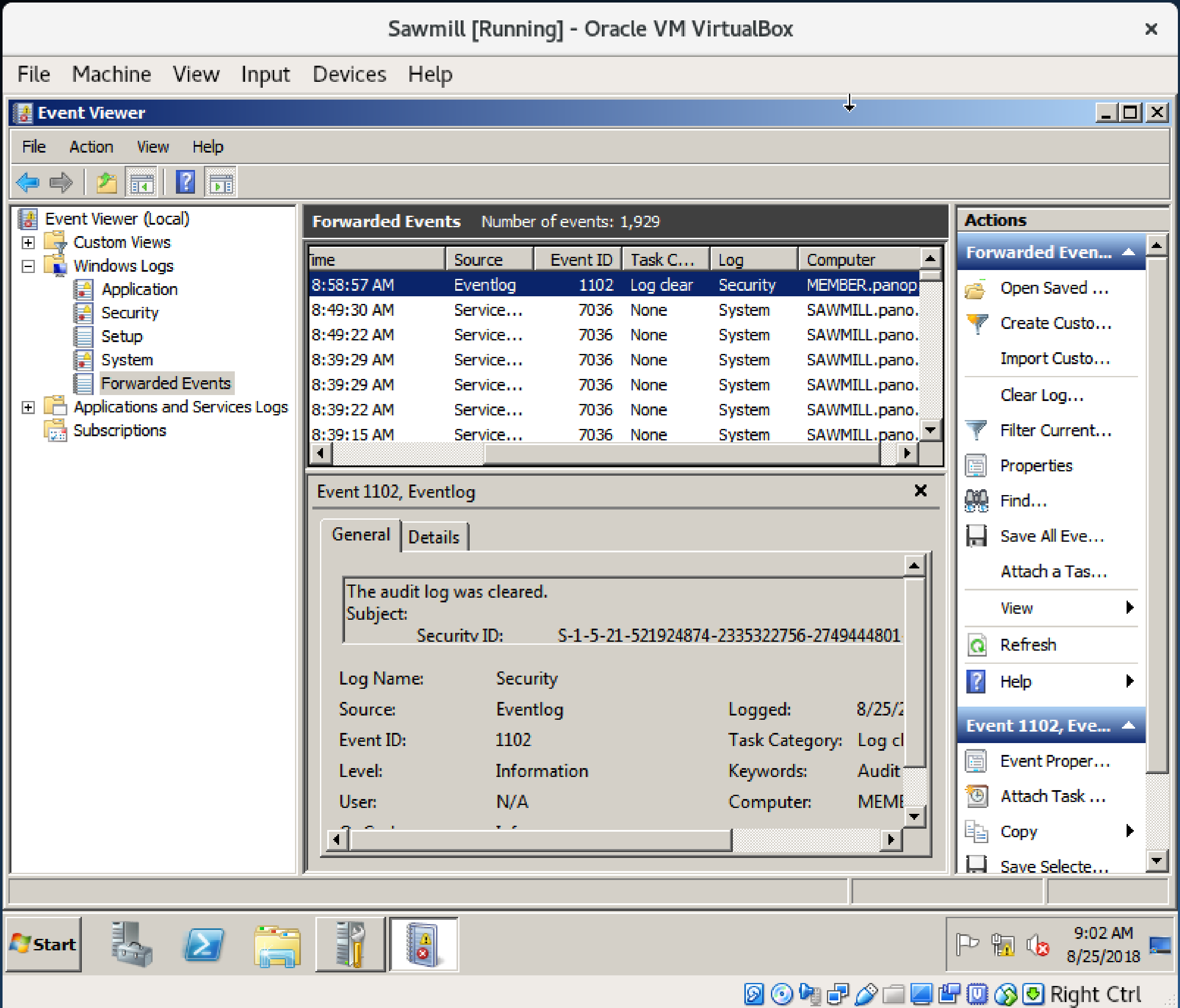
Security Number of events: 8

Keywords	Date and Time	Source	Event ID	Task Ca...
Audit ...	8/25/2018 9:00:41 AM	Microsof...	4672	Special L...
Audit ...	8/25/2018 9:00:41 AM	Microsof...	4624	Logon
Audit ...	8/25/2018 9:00:11 AM	Microsof...	4672	Special L...
Audit ...	8/25/2018 9:00:11 AM	Microsof...	4624	Logon
Audit ...	8/25/2018 9:00:11 AM	Microsof...	4624	Logon
Audit ...	8/25/2018 9:00:11 AM	Microsof...	4648	Logon
Audit ...	8/25/2018 8:59:10 AM	Microsof...	4634	Logoff
Audit ...	8/25/2018 8:58:57 AM	Eventlog	1102	Log clear

Event 1102, Eventlog

General Details

```
The audit log was cleared.
Subject:
        Security ID:        PANOPTICON\matt

Log Name:           Security
```



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

```
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

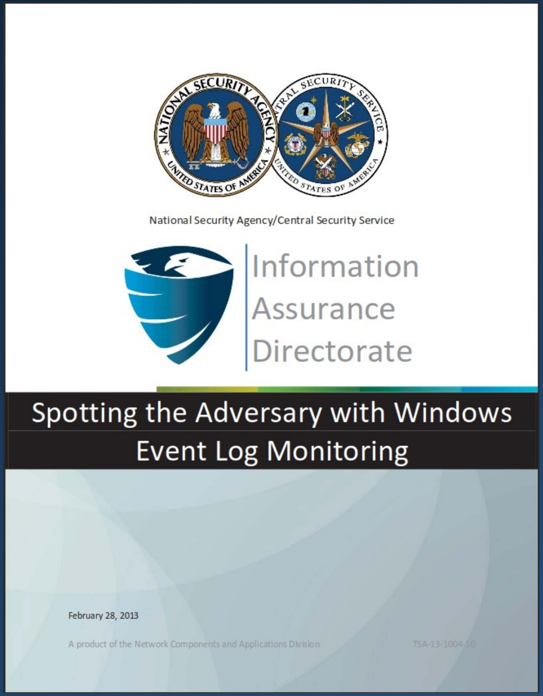
What Events to Monitor?

- 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

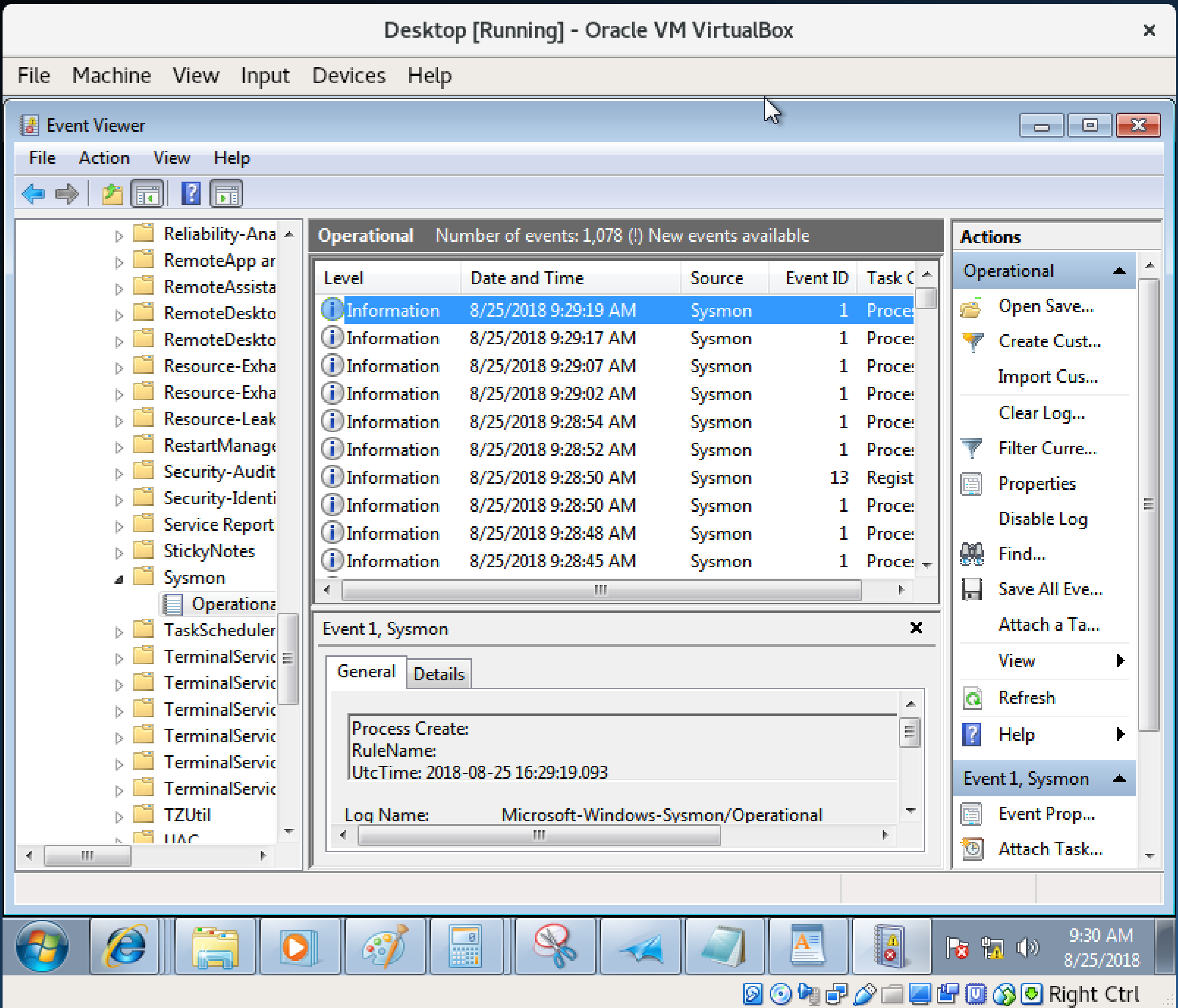
A product of the Network Components and Applications Division

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

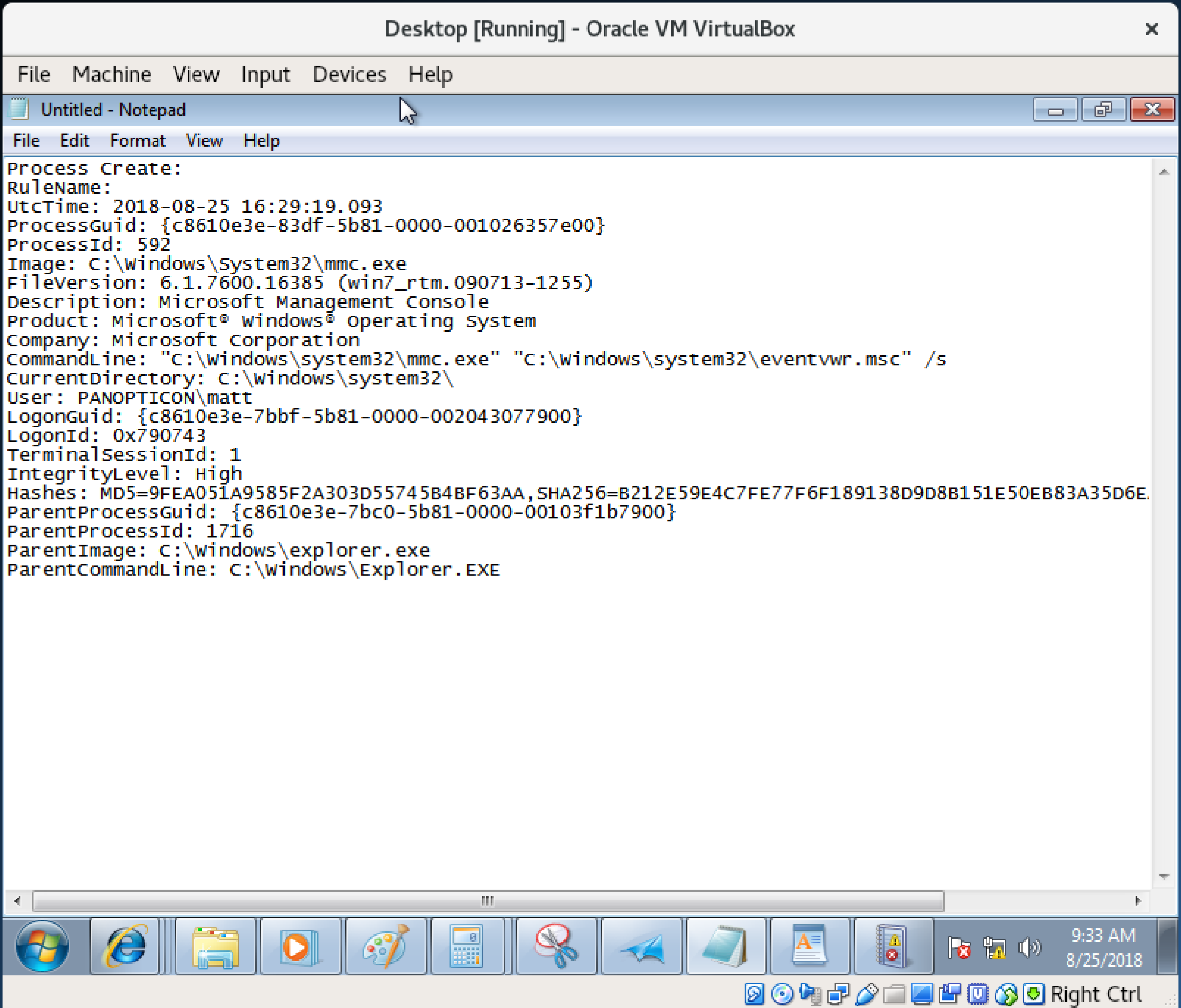


Operational Number of events: 1,078 (!) New events available

Level	Date and Time	Source	Event ID	Task C
Information	8/25/2018 9:29:19 AM	Sysmon	1	Proce
Information	8/25/2018 9:29:17 AM	Sysmon	1	Proce
Information	8/25/2018 9:29:07 AM	Sysmon	1	Proce
Information	8/25/2018 9:29:02 AM	Sysmon	1	Proce
Information	8/25/2018 9:28:54 AM	Sysmon	1	Proce
Information	8/25/2018 9:28:52 AM	Sysmon	1	Proce
Information	8/25/2018 9:28:50 AM	Sysmon	13	Regist
Information	8/25/2018 9:28:50 AM	Sysmon	1	Proce
Information	8/25/2018 9:28:48 AM	Sysmon	1	Proce
Information	8/25/2018 9:28:45 AM	Sysmon	1	Proce

Event 1, Sysmon

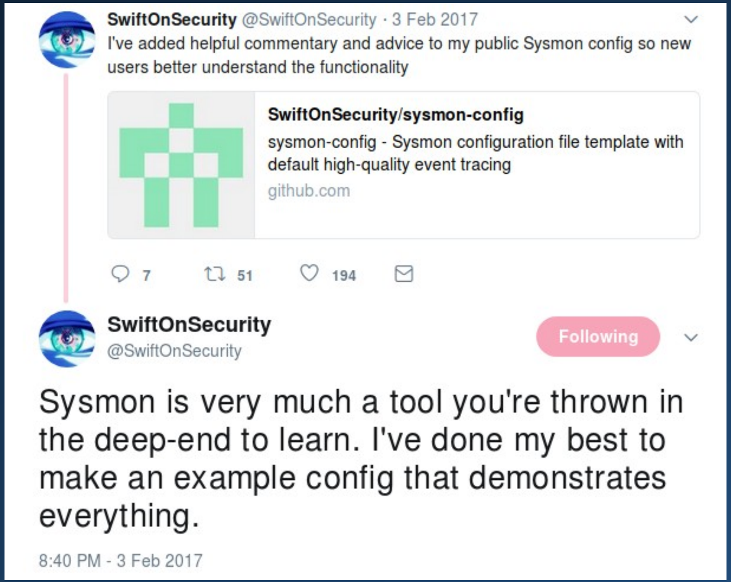
```
Process Create:
RuleName:
UtcTime: 2018-08-25 16:29:19.093

Log Name:          Microsoft-Windows-Sysmon/Operational
```



```
Process Create:
RuleName:
UtcTime: 2018-08-25 16:29:19.093
ProcessGuid: {c8610e3e-83df-5b81-0000-001026357e00}
ProcessId: 592
Image: C:\Windows\System32\mmc.exe
FileVersion: 6.1.7600.16385 (win7_rtm.090713-1255)
Description: Microsoft Management Console
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: "C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s
CurrentDirectory: C:\Windows\system32\
User: PANOPTICON\matt
LogonGuid: {c8610e3e-7bbf-5b81-0000-002043077900}
LogonId: 0x790743
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=9FEA051A9585F2A303D55745B4BF63AA,SHA256=B212E59E4C7FE77F6F189138D9D8B151E50EB83A35D6E
ParentProcessGuid: {c8610e3e-7bc0-5b81-0000-00103f1b7900}
ParentProcessId: 1716
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
```

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

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

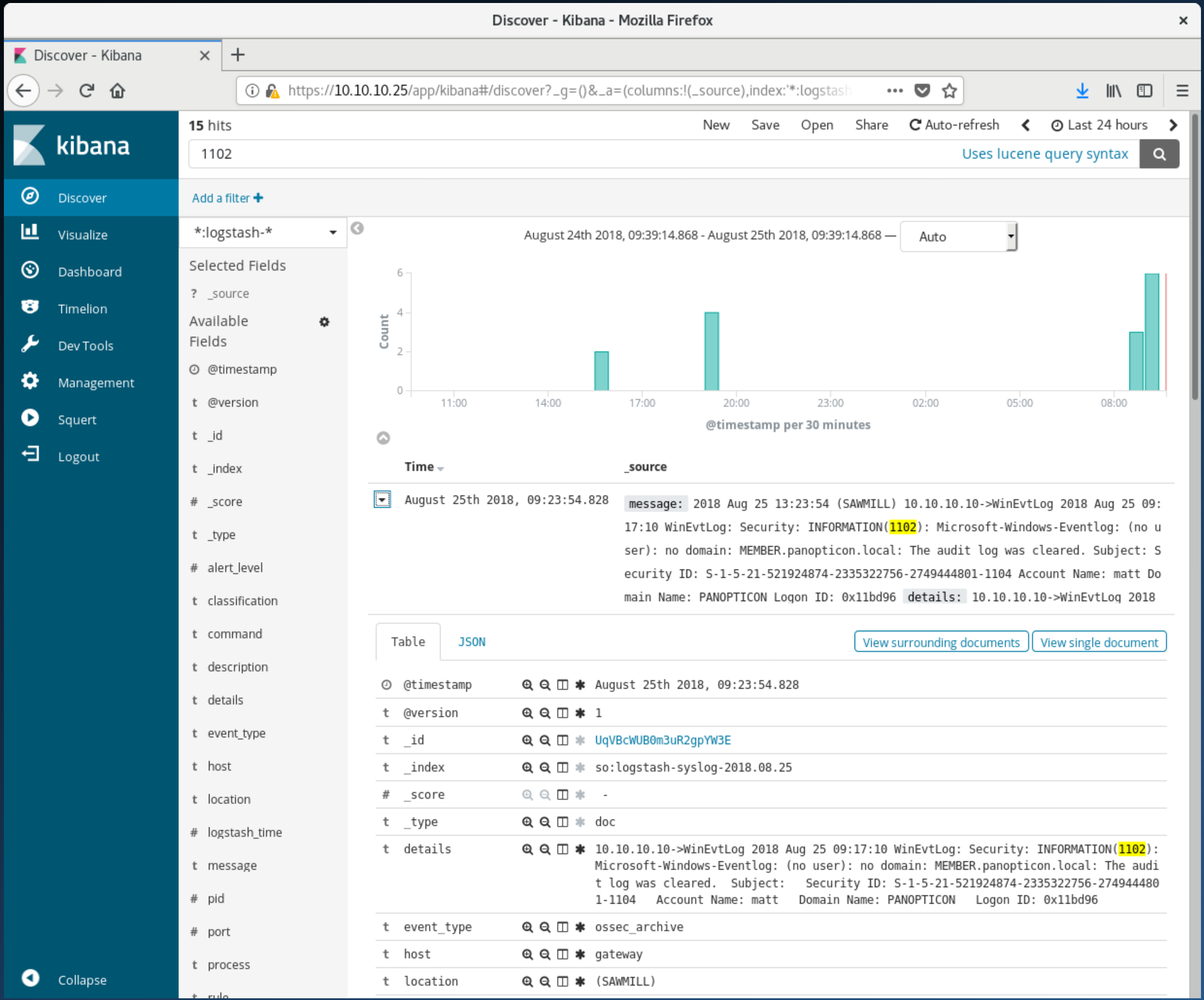
Log Shipping Mechanisms

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

- NXLog
- OSSEC / Wazuh
- Winlogbeat

Security Onion

- Project by Doug Burks (@dougburks)
- Prebuilt Dockerized stack of open source NSM tools
- Available as an appliance ISO
- Can be installed on top of vanilla Ubuntu and RHEL/CentOS
- Commercial support and training available
- Built around the Elastic Stack
- Includes parsing for Windows Event and Sysmon logs
- Includes Playbook and Elastalert for writing alarm rules



15 hits

1102

:logstash-

August 24th 2018, 09:39:14.868 - August 25th 2018, 09:39:14.868 —

Selected Fields

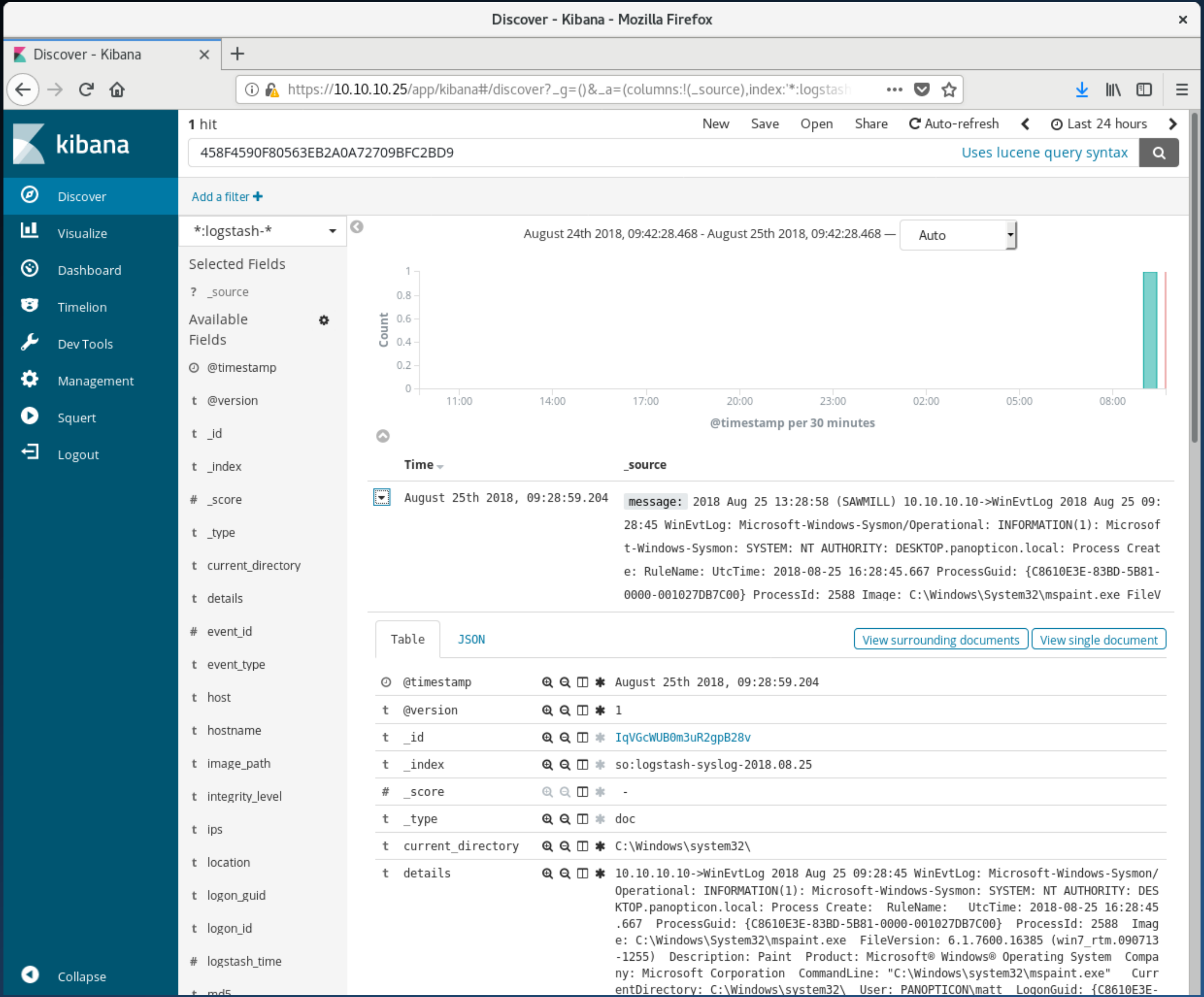
- ? _source

Available Fields

- @timestamp
- t @version
- t _id
- t _index
- # _score
- t _type
- # alert_level
- t classification
- t command
- t description
- t details
- t event_type
- t host
- t location
- # logstash_time
- t message
- # pid
- # port
- t process
- t rule

Time	_source
August 25th 2018, 09:23:54.828	message: 2018 Aug 25 13:23:54 (SAWMILL) 10.10.10.10->WinEvtLog 2018 Aug 25 09:17:10 WinEvtLog: Security: INFORMATION(1102): Microsoft-Windows-Eventlog: (no user): no domain: MEMBER.panopticon.local: The audit log was cleared. Subject: Security ID: S-1-5-21-521924874-2335322756-2749444801-1104 Account Name: matt Domain Name: PANOPTICON Logon ID: 0x11bd96 details: 10.10.10.10->WinEvtLog 2018

	@timestamp	August 25th 2018, 09:23:54.828
t	@version	1
t	_id	UqVBcWUB0m3uR2gpYW3E
t	_index	so:logstash-syslog-2018.08.25
#	_score	-
t	_type	doc
t	details	10.10.10.10->WinEvtLog 2018 Aug 25 09:17:10 WinEvtLog: Security: INFORMATION(1102): Microsoft-Windows-Eventlog: (no user): no domain: MEMBER.panopticon.local: The audit log was cleared. Subject: Security ID: S-1-5-21-521924874-2335322756-2749444801-1104 Account Name: matt Domain Name: PANOPTICON Logon ID: 0x11bd96
t	event_type	ossec_archive
t	host	gateway
t	location	(SAWMILL)

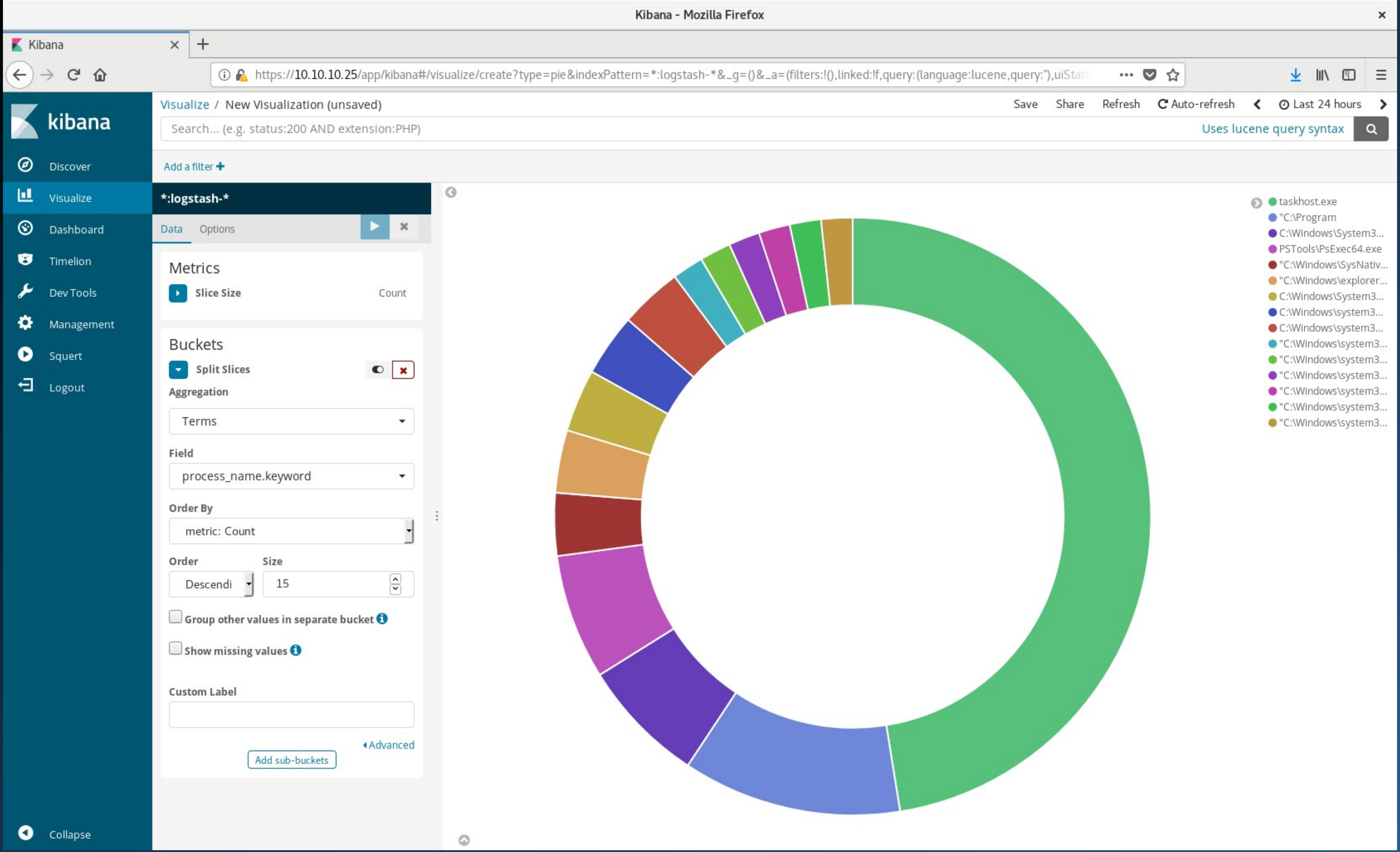


```
458F4590F80563EB2A0A72709BFC2BD9
```

August 25th 2018, 09:28:59.204

```
message: 2018 Aug 25 13:28:58 (SAWMILL) 10.10.10.10->WinEvtLog 2018 Aug 25 09:
28:45 WinEvtLog: Microsoft-Windows-Sysmon/Operational: INFORMATION(1): Microsof
t-Windows-Sysmon: SYSTEM: NT AUTHORITY: DESKTOP.panopticon.local: Process Creat
e: RuleName: UtcTime: 2018-08-25 16:28:45.667 ProcessGuid: {C8610E3E-83BD-5B81-
0000-001027DB7C00} ProcessId: 2588 Image: C:\Windows\System32\mspaint.exe FileV
```

```
@timestamp          August 25th 2018, 09:28:59.204
t @version          1
t _id               IqVGcWUB0m3uR2gpB28v
t _index            so:logstash-syslog-2018.08.25
# _score            -
t _type             doc
t current_directory C:\Windows\system32\
t details           10.10.10.10->WinEvtLog 2018 Aug 25 09:28:45 WinEvtLog: Microsoft-Windows-Sysmon/
                    Operational: INFORMATION(1): Microsoft-Windows-Sysmon: SYSTEM: NT AUTHORITY: DES
                    KTOP.panopticon.local: Process Create:  RuleName:   UtcTime: 2018-08-25 16:28:45
                    .667  ProcessGuid: {C8610E3E-83BD-5B81-0000-001027DB7C00}  ProcessId: 2588  Imag
                    e: C:\Windows\System32\mspaint.exe  FileVersion: 6.1.7600.16385 (win7_rtm.090713
                    -1255)  Description: Paint  Product: Microsoft® Windows® Operating System  Compa
                    ny: Microsoft Corporation  CommandLine: "C:\Windows\system32\mspaint.exe"   Curr
                    entDirectory: C:\Windows\system32\  User: PANOPTICON\matt  LogonGuid: {C8610E3E-
```



https://10.10.10.25/app/kibana#/visualize/create?type=pie&indexPattern=*:logstash-*&_g=()&_a=(filters:!(),linked:!f,query:(language:lucene,query:''),uiStat

Visualize / New Visualization (unsaved)

:logstash-

Metrics

Slice Size Count

Buckets

Split Slices

Aggregation: Terms

Field: process_name.keyword

Order By: metric: Count

Order: Descendi

Size: 15

□ Group other values in separate bucket

□ Show missing values

Custom Label

● taskhost.exe
● "C:\Program
● C:\Windows\System3...
● PSTools\PsExec64.exe
● "C:\Windows\SysNativ...
● "C:\Windows\explorer...
● C:\Windows\System3...
● C:\Windows\system3...
● C:\Windows\system3...
● "C:\Windows\system3...
● "C:\Windows\system3...
● "C:\Windows\system3...
● "C:\Windows\system3...
● "C:\Windows\system3...
● "C:\Windows\system3...

Summary

- Windows Event Forwarding (WEF) is available in every supported version of Windows.
- It requires one subscription server and one GPO.
- It can pull any event from the endpoints on your network with amazing granularity.

Questions?

For More Information

@InfosecGoon

infosecgoon@roadflares.org

https://github.com/InfosecGoon/