

Building the Panopticon:

Centralized Logging and Alerting With Free Tools

Matthew Gracie

Information Security Engineer



BlueCross BlueShield
of Western New York

Who Am I?

What is the Panopticon?



Attackers view

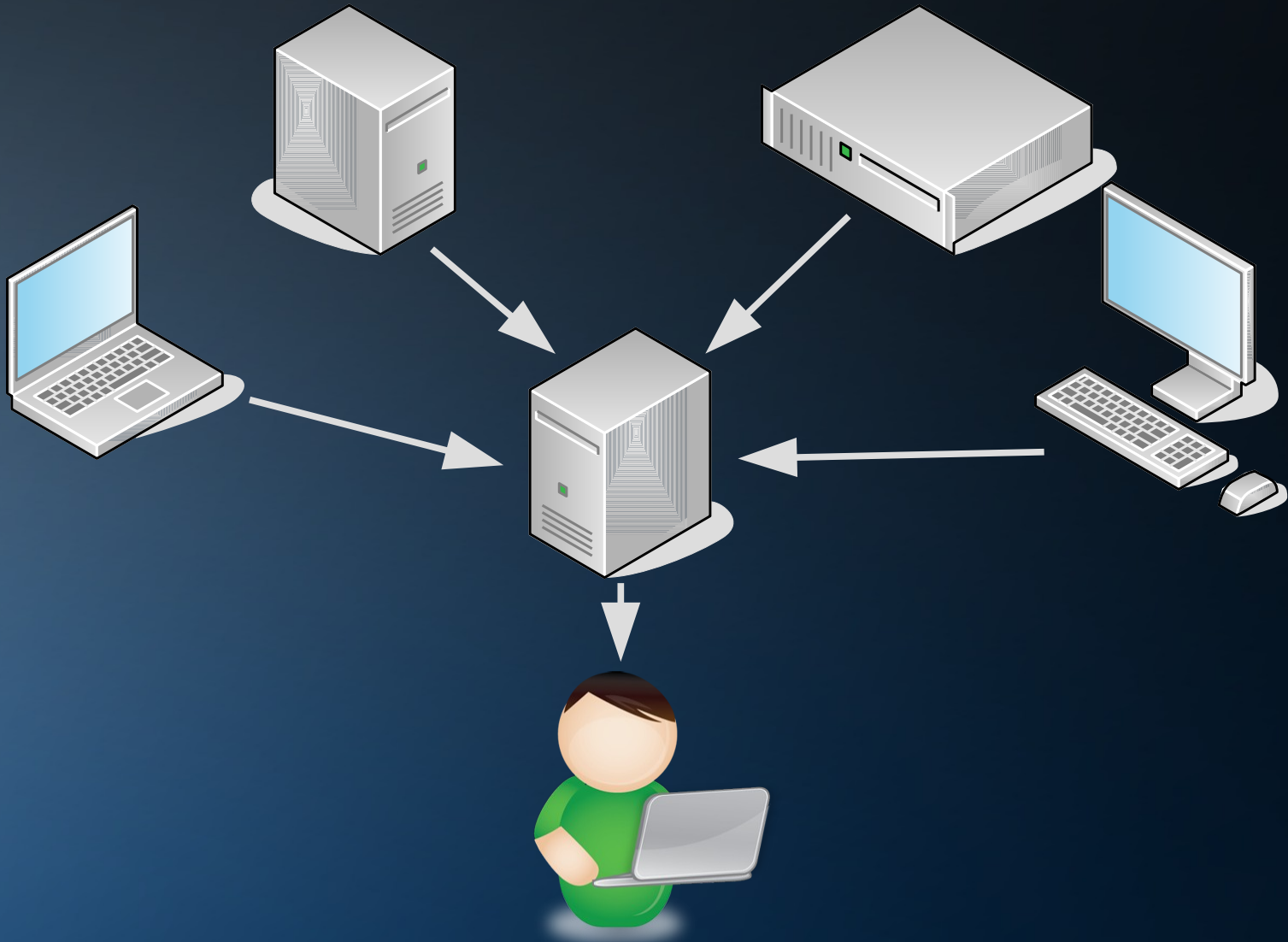


Defenders view

Interior View of Cell House, new Illinois State Penitentiary at Stateville, near Joliet, Ill.—23







Assumptions

- This is primarily a Windows environment, running a modern version of Active Directory (2008R2 or better).
- You have already enabled Advanced Audit Policy on your domain to activate deeper logging of security events.
- There is enough buy-in from your system administrators to make some wide-ranging infrastructure changes.
- Your organization is amenable to using free or open source software.

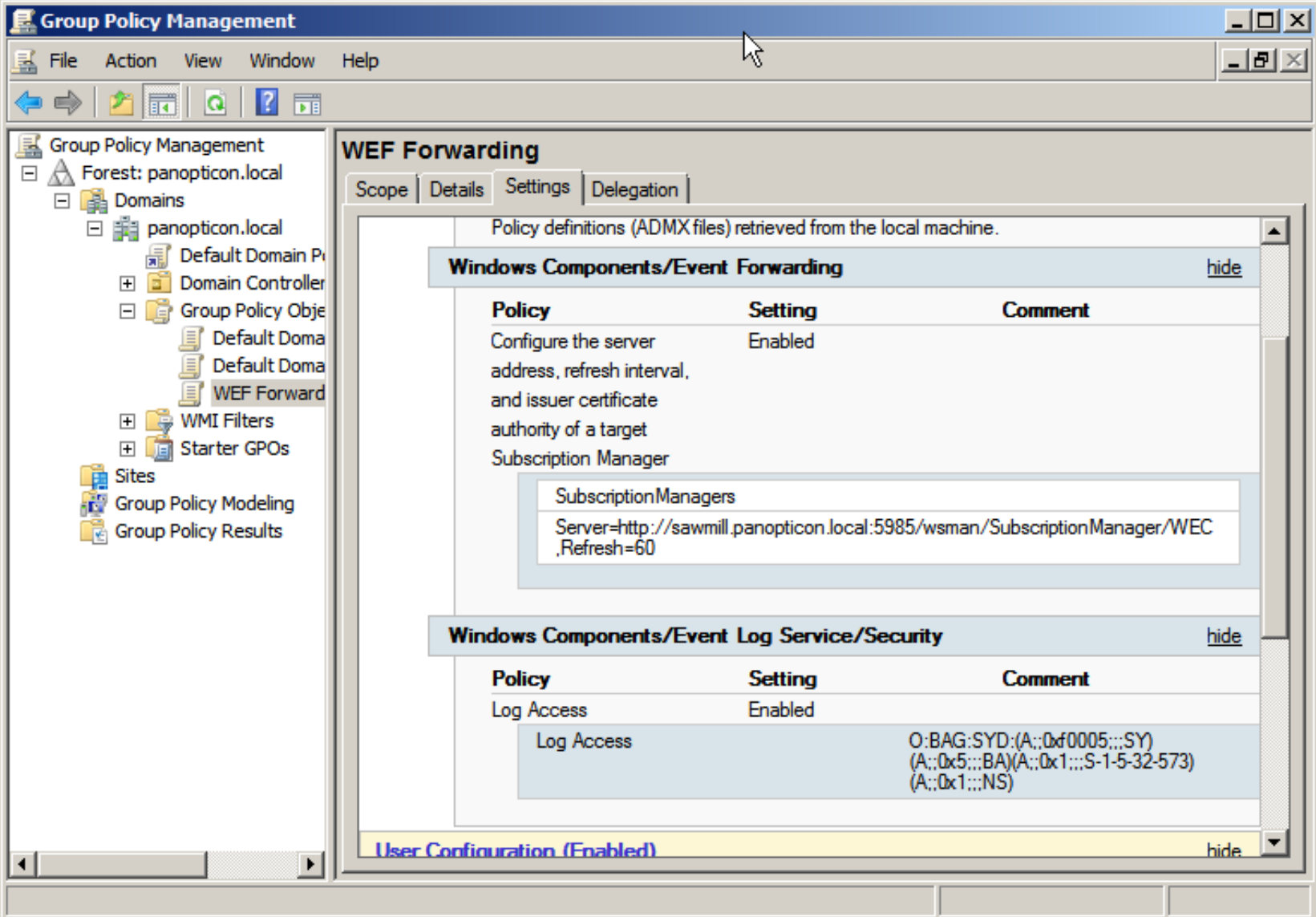
Tools

- Windows Event Forwarding (WEF)
- OSSEC HIDS
- Security Onion



Windows Event Forwarding

- A server on the domain is designated as a log collector.
- This collector server is configured with subscriptions.
- A GPO tells domain computers to subscribe.
- Events designated in the subscriptions are now forwarded.



Group Policy Management

File Action View Window Help



- Group Policy Management
 - Forest: panopticon.local
 - Domains
 - panopticon.local
 - Default Domain Policy
 - Domain Controller
 - Group Policy Objects
 - Default Domain Policy
 - Default Domain Policy
 - WEF Forwarding
 - WMI Filters
 - Starter GPOs
 - Sites
 - Group Policy Modeling
 - Group Policy Results

WEF Forwarding

Scope Details Settings Delegation

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

Windows Components/Event Forwarding [hide](#)

| 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 [hide](#)

| 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) [hide](#)

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 Select Computers...

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

Source computer initiated Select Computer Groups...

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: Select Events...

Configure advanced settings: Advanced...

OK Cancel

C:\Windows\system32\cmd.exe

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>

File Machine View Input Devices Help

Event Viewer



File Action View Help



- Event Viewer (Local)
 - Custom Views
 - Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
 - Applications and Services Logs
 - Subscriptions

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

Actions

Security

Open Saved ...

Create Custo...

Import Custo...

Clear Log...

Filter Current...

Properties

Find...

Save All Eve...

Attach a Tas...

View

Refresh

Help

Event 1102, Eve...

Event Proper...

Attach Task ...

Copy

Save Selecte...

Start

9:01 AM
8/25/2018

Right Ctrl

File Machine View Input Devices Help

Event Viewer

File Action View Help



- Event Viewer (Local)
 - Custom Views
 - Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events**
 - Applications and Services Logs
 - Subscriptions

Forwarded Events Number of events: 1,929

| Time | 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

Event ID: 1102

Level: Information

User: N/A

Logged: 8/25/2018 8:58:57 AM

Task Category: Log clear

Keywords: Audit

Computer: MEMBER.panop

Actions

Forwarded Even... ▲

Open Saved ...

Create Custo...

Import Custo...

Clear Log...

Filter Current...

Properties

Find...

Save All Eve...

Attach a Tas...

View ▶

Refresh

Help ▶

Event 1102, Eve... ▲

Event Proper...

Attach Task ...

Copy ▶

Save Selecte...

Start



9:02 AM

8/25/2018

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-13-1004-00

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](#)

File Machine View Input Devices Help

Event Viewer

File Action View Help

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

General Details

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

Log Name: Microsoft-Windows-Sysmon/Operational

Actions

Operational

- Open Save...
- Create Cust...
- Import Cus...
- Clear Log...
- Filter Curre...
- Properties
- Disable Log
- Find...
- Save All Eve...
- Attach a Ta...
- View
- Refresh
- Help
- Event 1, Sysmon
- Event Prop...
- Attach Task...

9:30 AM
8/25/2018

File Machine View Input Devices Help

Untitled - Notepad

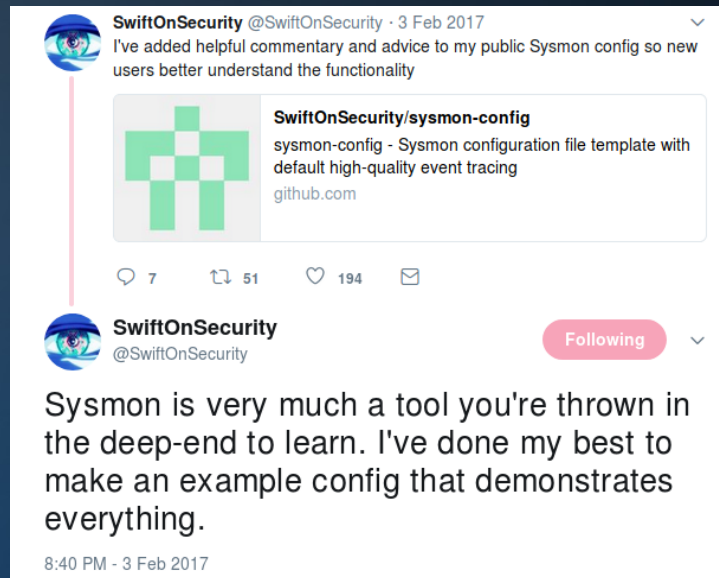
File Edit Format View Help

```
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
```

9:33 AM
8/25/2018

Sysmon

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



The image is a screenshot of a tweet from the user @SwiftOnSecurity, posted on February 3, 2017. The tweet text reads: "I've added helpful commentary and advice to my public Sysmon config so new users better understand the functionality". Below the text is a link to a GitHub repository named "SwiftOnSecurity/sysmon-config", with a description: "sysmon-config - Sysmon configuration file template with default high-quality event tracing" and the URL "github.com". The repository's logo, a green and white checkerboard pattern, is shown to the left of the link. Below the tweet are icons for replies (7), retweets (51), likes (194), and a direct message icon. Below the tweet is the user's profile information: "SwiftOnSecurity @SwiftOnSecurity" with a "Following" button. The user's text reads: "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." The timestamp "8:40 PM - 3 Feb 2017" is at the bottom.

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

7 51 194

SwiftOnSecurity @SwiftOnSecurity **Following**

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

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

OSSEC

- OSSEC is an agent-based HIDS software platform.
- Agents installed on endpoints monitor files and report changes and events to a central server.
- Incoming events are evaluated using rules.
- Rules that are triggered can raise alerts.
- Alerts can be handled in a variety of ways.

OSSEC

- For this architecture, we can install the OSSEC Agent on the WEF Collector server and have it report to the OSSEC Server in Security Onion.
- Rules on the Security Onion server can then be written to evaluate incoming OSSEC events and raise alerts.

Security Onion

- Security Onion is an Ubuntu-based platform for threat hunting and Network Security Monitoring.
- It includes many useful tools for data gathering and analysis.
- It uses a server / sensor architecture.
- For this use case, we only need the server components.
- That said, the sensor components are *fantastically useful* and if you have the budget for a couple boxes full of disk, you should look into deploying them.

Security Onion - OSSEC

- The OSSEC Agent on the WEF Collector server forwards the collected logs to the OSSEC Server on Security Onion.
- Rules on the Security Onion server parse the logs and raise alerts as necessary.

OSSEC Rules

```
Terminal - root@onion: /var/ossec/rules
File Edit View Terminal Tabs Help
<if_sid>18104</if_sid>
<id>^4702$</id>
<description> Scheduled Task Updated </description>
</rule>

<rule id="101002" level="10">
  <if_sid>18104</if_sid>
  <id>^4698$</id>
  <description> New Scheduled Task Created </description>
</rule>

<rule id="101003" level="10">
  <if_sid>18101</if_sid>
  <id>^1102$</id>
  <description> Security Event Log Cleared </description>
</rule>

<rule id="101004" level="10">
  <if_sid>18104</if_sid>
  <id>^4724$</id>
  <description> AD password reset by administrator </description>
</rule>
"local_rules.xml" 73L, 1771C written                22,1                41%
```

SGUIL

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: matt UserID: 2 2018-08-25 13:24:40 GMT

RealTime Events Escalated Events

| ST | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|----|-----|----------|----------|---------------------|---------|-------|-------------|-------|----|------------------------------------|
| RT | 2 | so-ossec | 1.630 | 2018-08-25 13:13:59 | 0.0.0.0 | | 10.10.10.10 | | | [OSSEC] Service Installation |
| RT | 3 | so-ossec | 1.632 | 2018-08-25 13:23:54 | 0.0.0.0 | | 10.10.10.10 | | | [OSSEC] Security Event Log Cleared |

IP Resolution Agent Status Snort Statistics System Msgs User Msgs

Reverse DNS Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: None Src IP Dst IP

Display Detail

User: (no user)
2018 Aug 25 09:08:51 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: 0x11a4e8

Squert

squert (5) - matt - Mozilla Firefox

squert (5) - matt

https://10.10.10.25/squert/index.php?id=2097bba661ad46477fcde5c226f106

EVENTS SUMMARY VIEWS

INTERVAL: 2018-08-25 00:00:00 -> 2018-08-25 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 100.0%

TOGGLE

queue only on

grouping on

SUMMARY

queued events 5

total events 5

total signatures 2

PRIORITY

high -

medium -

low -

other 5 (100.0%)

CLASSIFICATION

- compromised L1-
- compromised L2-
- attempted access -
- denial of service-
- policy violation -
- reconnaissance -
- malicious -
- no action req'd. -
- escalated event -

TAGS

no tags

HISTORY

no history

20

10

0

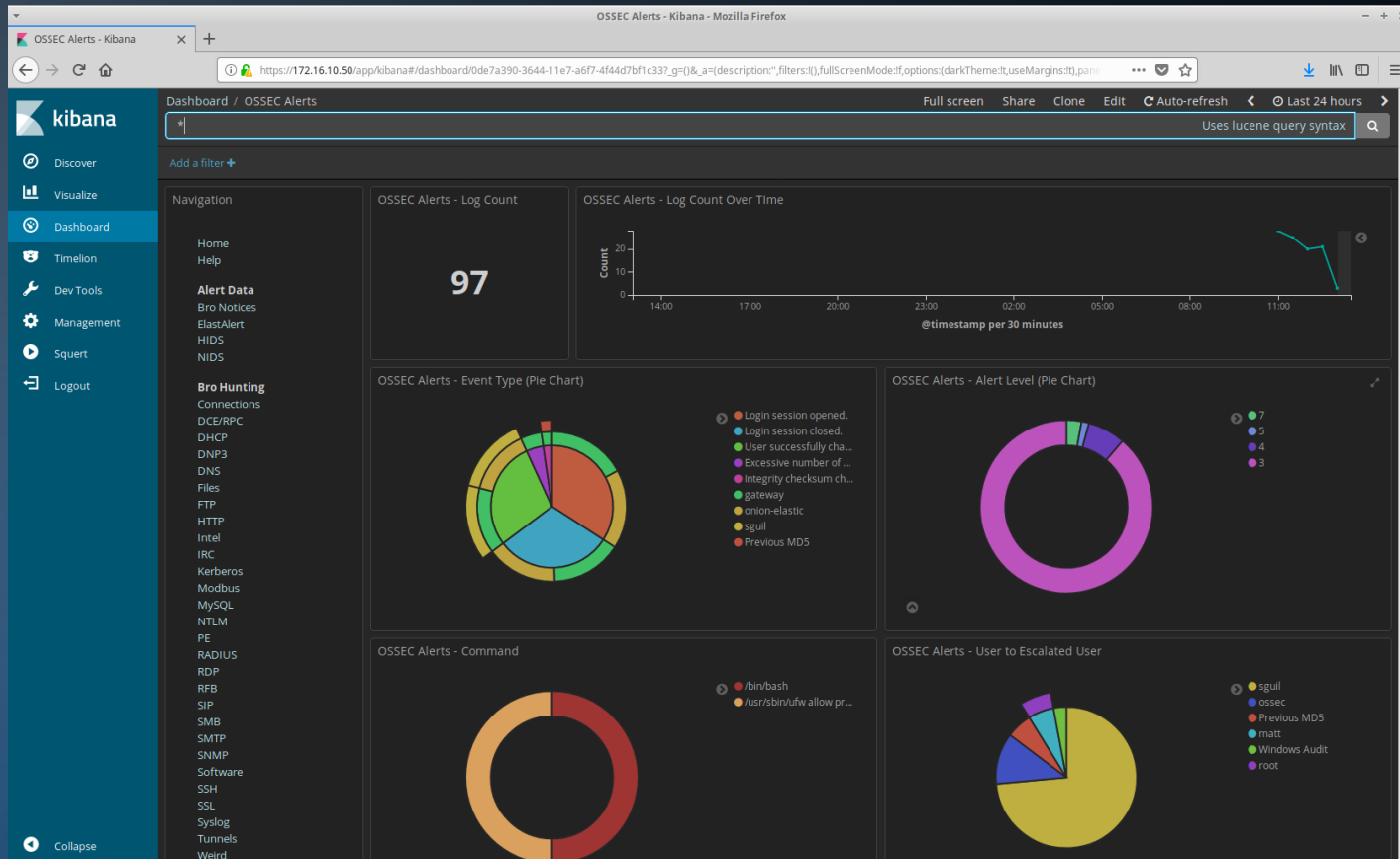
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23

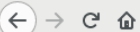
| QUEUE | SC | DC | ACTIVITY | LAST EVENT | SIGNATURE | ID | PROTO | % TOTAL |
|-------|----|----|----------|------------|------------------------------------|--------|-------|---------|
| 3 | 10 | 1 | 1 | 13:23:54 | [OSSEC] Security Event Log Cleared | 101003 | 0 | 60.000% |
| 2 | 10 | 1 | 1 | 13:13:59 | [OSSEC] Service Installation | 101006 | 0 | 40.000% |

WELCOME matt | LOGOUT

UTC 13:25:24

Kibana





kibana

15 hits

New Save Open Share Auto-refresh Last 24 hours

1102

[Uses lucene query syntax](#)

Discover

Add a filter +

Visualize

:logstash-

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

Auto

Dashboard

Selected Fields

Timelion

? _source

Dev Tools

Available Fields

Management

@timestamp

Squert

t @version

Logout

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

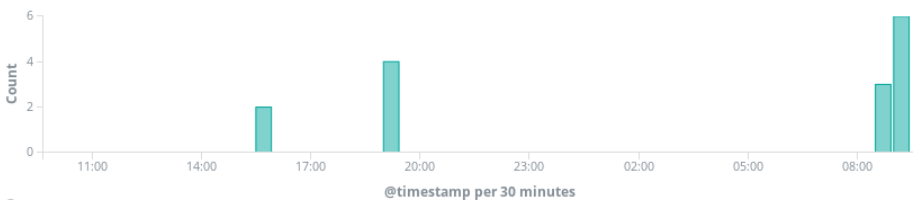
t message

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: S security ID: S-1-5-21-521924874-2335322756-2749444801-1104 Account Name: matt Do main Name: PANOPTICON Logon ID: 0x11bd96 **details:** 10.10.10.10->WinEvtLog 2018

Table JSON

[View surrounding documents](#)[View single document](#)

| | |
|------------|---|
| @timestamp | August 25th 2018, 09:23:54.828 |
| @version | 1 |
| _id | UqVBcWUB0m3uR2gpYW3E |
| _index | so:logstash-syslog-2018.08.25 |
| _score | - |
| _type | doc |
| 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 |
| event_type | ossec_archive |
| host | gateway |
| location | (SAWMILL) |

Collapse

Discover - Kibana - Mozilla Firefox

Discover - Kibana

https://10.10.10.25/app/kibana#/discover?_g=()&_a=(columns:!(_source),index:*.logstash!)

1 hit

458F4590F80563EB2A0A72709BFC2BD9

Uses lucene query syntax

Discover

Visualize

Dashboard

Timeline

Dev Tools

Management

Squert

Logout

:logstash-

August 24th 2018, 09:42:28.468 - August 25th 2018, 09:42:28.468 — Auto

Count

@timestamp per 30 minutes

Time

_source

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): Microsoft-Windows-Sysmon: SYSTEM: NT AUTHORITY: DESKTOP.panopticon.local: Process Create: RuleName: UtcTime: 2018-08-25 16:28:45.667 ProcessGuid: {C8610E3E-83BD-5B81-0000-001027DB7C00} ProcessId: 2588 Image: C:\Windows\System32\mspaint.exe FileV

Table JSON

View surrounding documents

View single document

| Field | Value |
|-------------------|---|
| @timestamp | August 25th 2018, 09:28:59.204 |
| @version | 1 |
| _id | IqVGcWJB0m3uR2gpB28v |
| _index | so:logstash-syslog-2018.08.25 |
| _score | - |
| _type | doc |
| current_directory | C:\Windows\system32\ |
| 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: DESKTOP.panopticon.local: Process Create: RuleName: UtcTime: 2018-08-25 16:28:45.667 ProcessGuid: {C8610E3E-83BD-5B81-0000-001027DB7C00} ProcessId: 2588 Image: C:\Windows\System32\mspaint.exe FileVersion: 6.1.7600.16385 (win7_rtm.090713-1255) Description: Paint Product: Microsoft® Windows® Operating System Company: Microsoft Corporation CommandLine: "C:\Windows\system32\mspaint.exe" CurrentDirectory: C:\Windows\system32\ User: PANOPTICON\matt LogonGuid: {C8610E3E- |

Collapse

- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management
- Squert
- Logout

Visualize / New Visualization (unsaved)
Search... (e.g. status:200 AND extension:PHP)

Add a filter +

:logstash-

Data Options

Metrics

Slice Size Count

Buckets

Split Slices

Aggregation

Terms

Field
process_name.keyword

Order By
metric: Count

Order Descendi Size 15

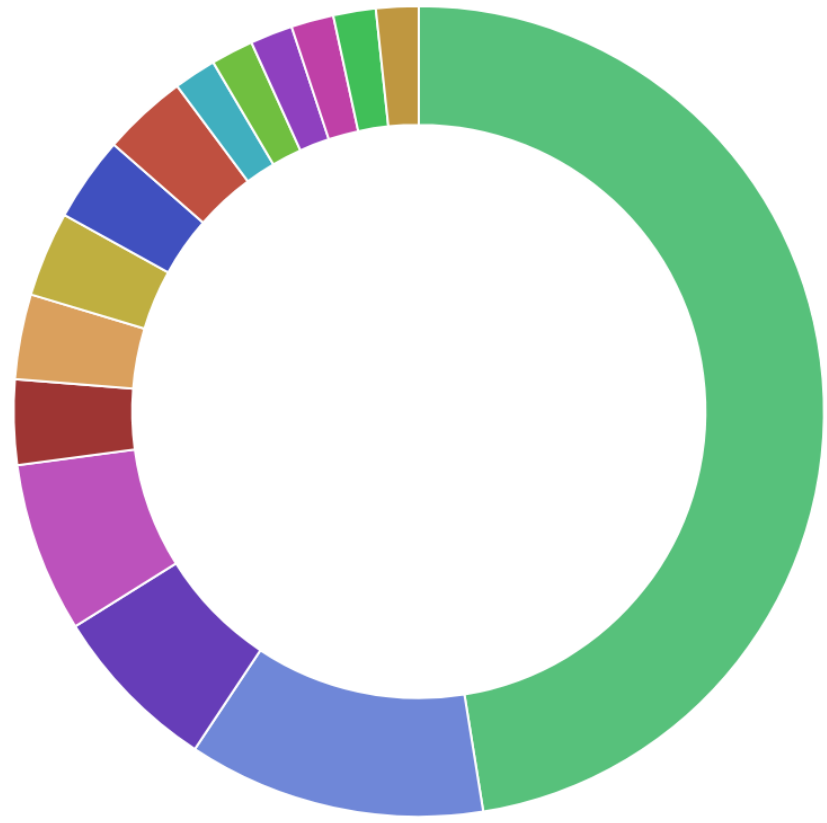
Group other values in separate bucket

Show missing values

Custom Label

Add sub-buckets

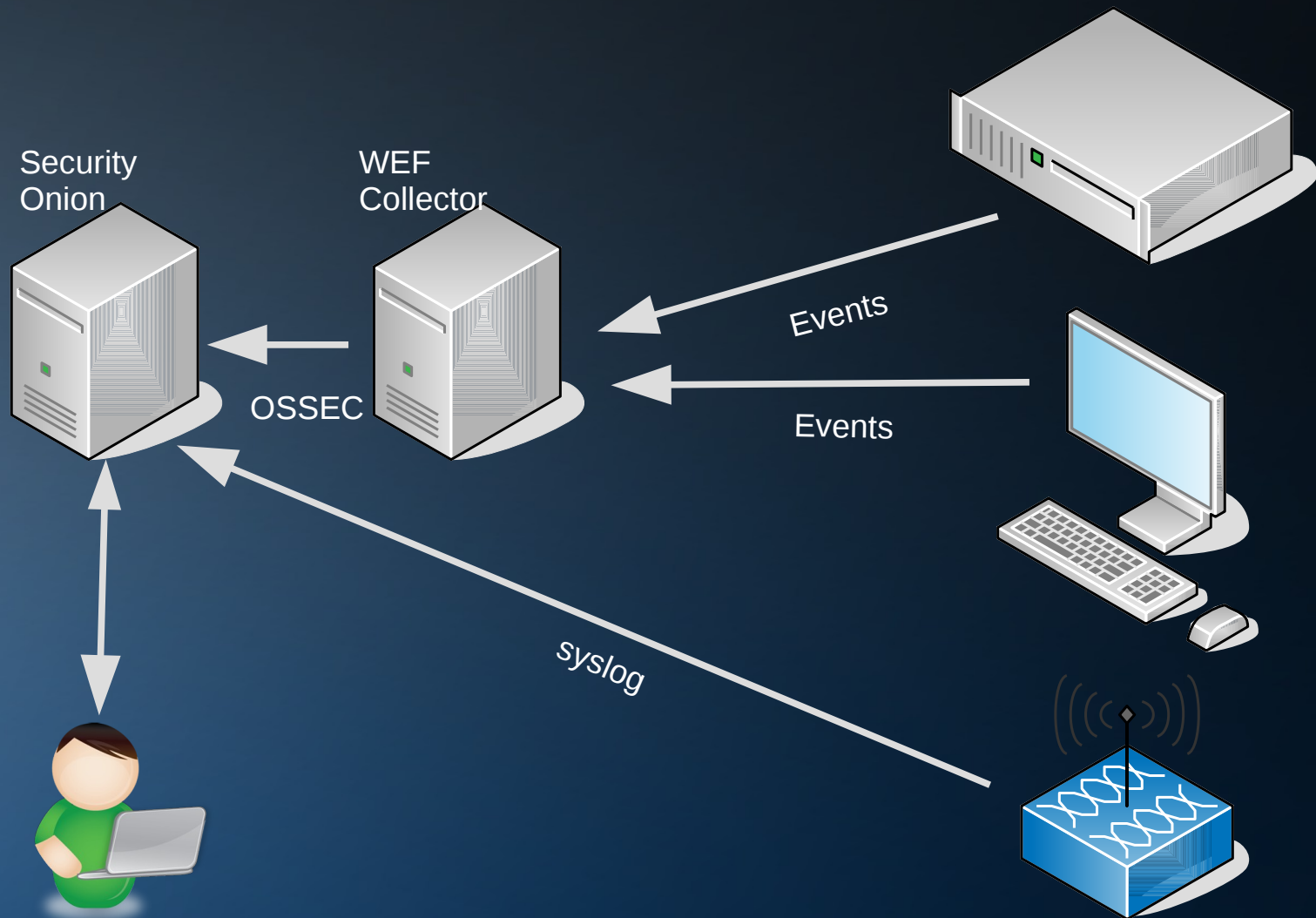
Advanced



- taskhost.exe
- C:\Program
- C:\Windows\System32
- PSTools\PsExec64.exe
- C:\Windows\SysNativ...
- C:\Windows\explorer...
- C:\Windows\System32
- C:\Windows\system32
- C:\Windows\system32
- C:\Windows\system32
- C:\Windows\system32
- C:\Windows\system32
- C:\Windows\system32
- C:\Windows\system32
- C:\Windows\system32

Syslog

- Clearly, not all devices speak Windows Event natively.
- Security Onion can also accept log information via syslog.
- Syslog data becomes searchable via Kibana.
- Syslog-ng can be configured to write data to a text file for OSSEC monitoring.
- The OSSEC server is then configured to look at that file and parsing rules are written in local_rules.xml.



Conclusions/ Questions

For More Information



@InfosecGoon



infosecgoon@roadflares.org



<https://github.com/InfosecGoon/panopticon/>