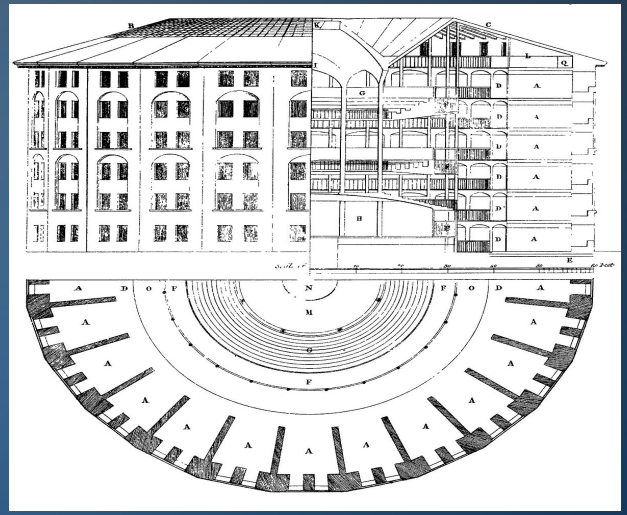
Building the Panopticon:

Centralized Logging and Alerting With Free Tools



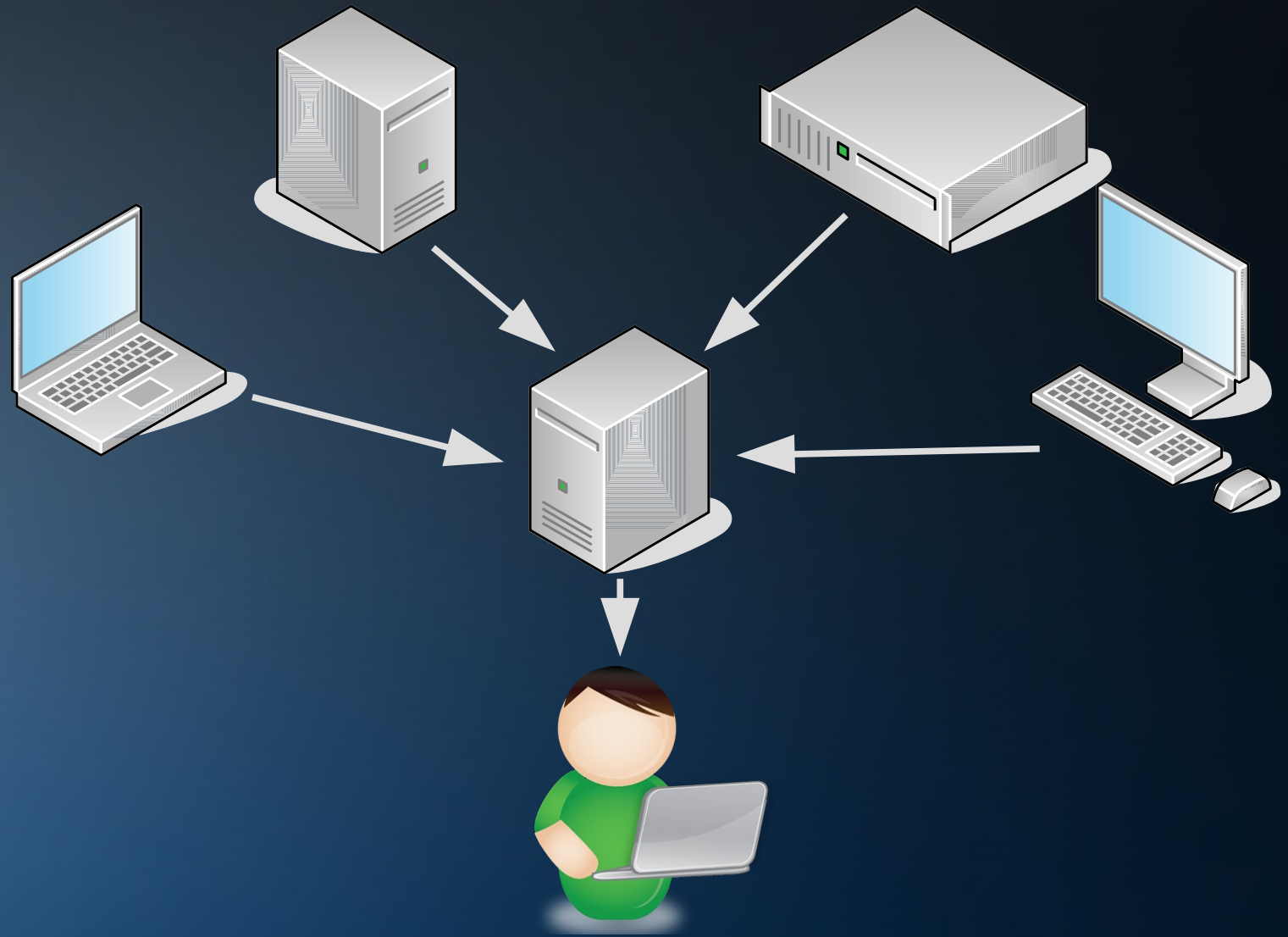
Matthew Gracie

Security Analyst

Who Am I?

What is the Panopticon?

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



Assumptions

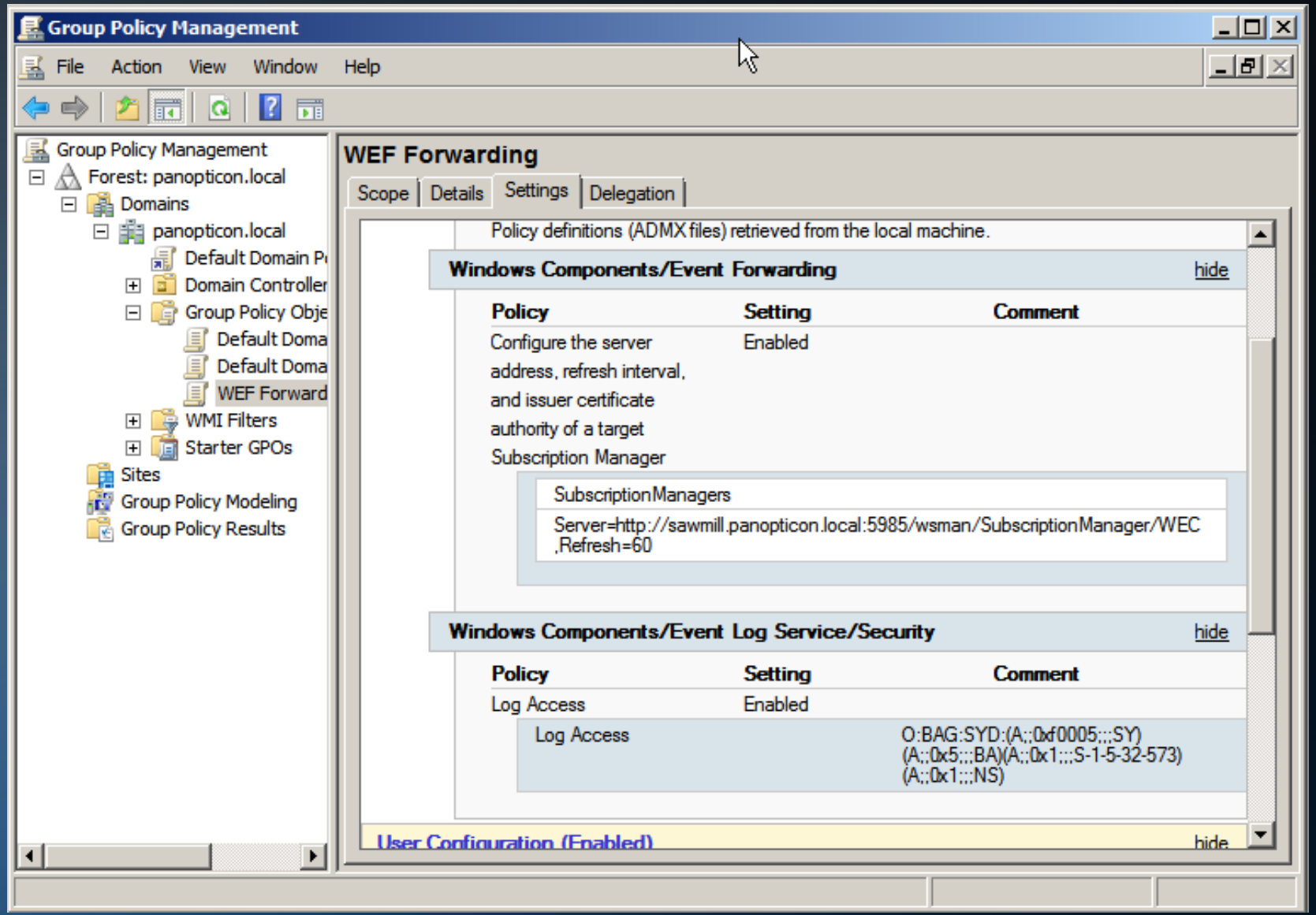
- This is primarily a Windows environment, running a modern version of Active Directory (2008R2 or better).
- You have already enabled Advanced Audit Policy on your domain to activate deeper logging of security events.
- There is enough buy-in from your system administrators to make some wide-ranging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

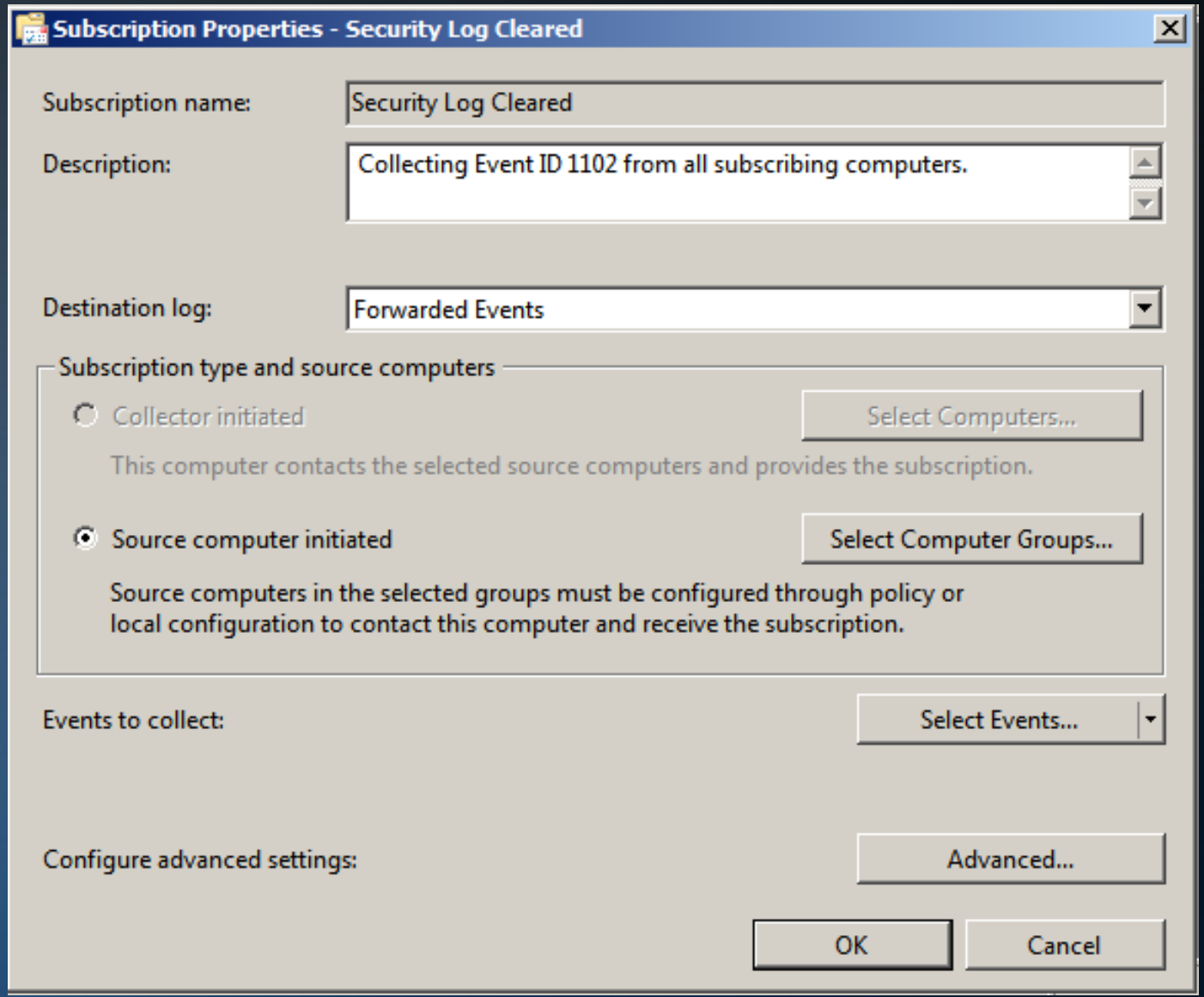
Tools

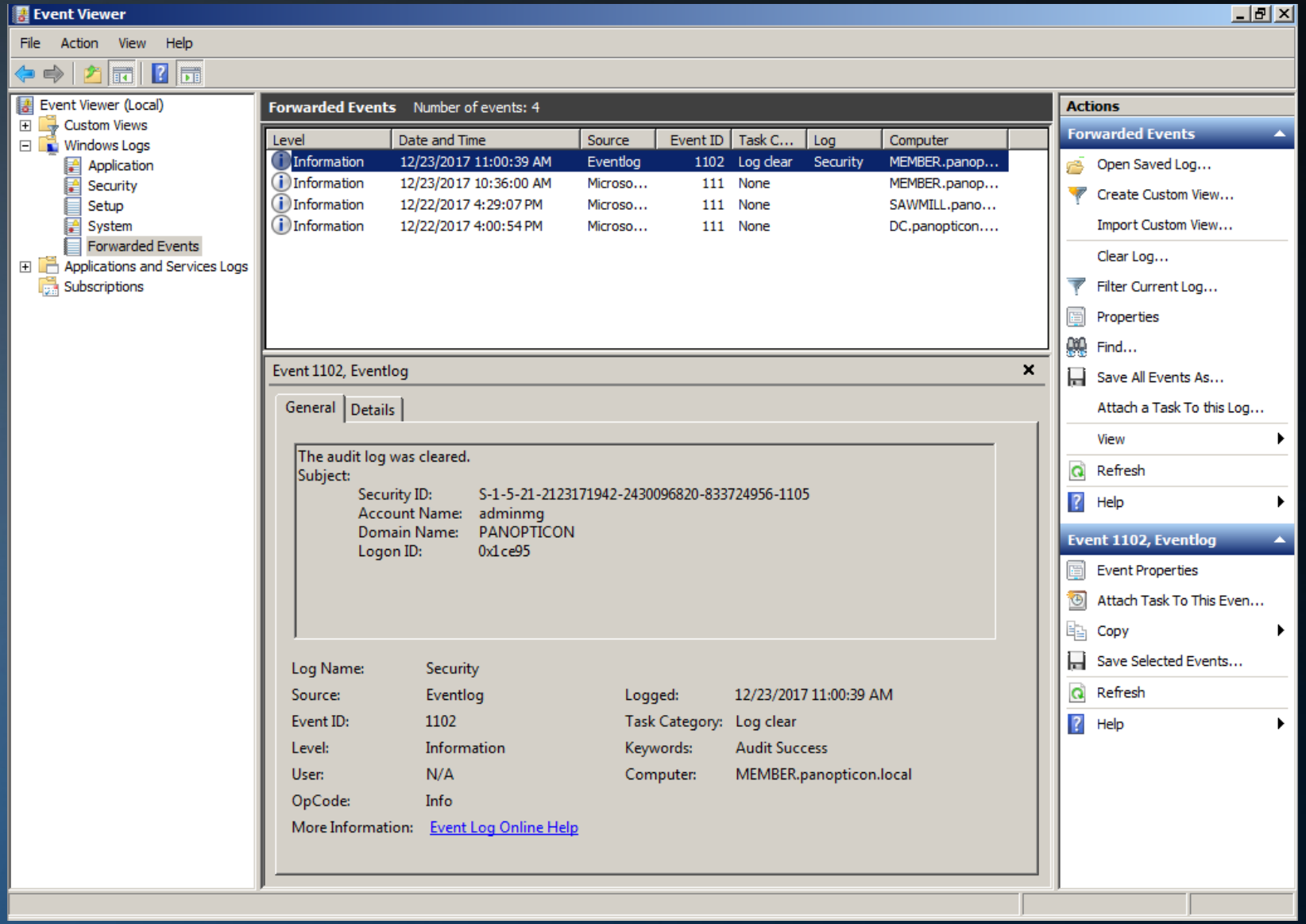
- Windows Event Forwarding (WEF)
- OSSEC HIDS
- Security Onion

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 P
Domain Controller
Group Policy Obje
Default Doma
Default Doma
WEF Forward
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


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: 4
Level Date and Time Source Event ID Task C... Log Computer
Information 12/23/2017 11:00:39 AM Eventlog 1102 Log clear Security MEMBER.panop...
Information 12/23/2017 10:36:00 AM Microso... 111 None MEMBER.panop...
Information 12/22/2017 4:29:07 PM Microso... 111 None SAWMILL.pano...
Information 12/22/2017 4:00:54 PM Microso... 111 None DC.panopticon....
Event 1102, Eventlog
General Details
The audit log was cleared.
Subject:
Security ID: S-1-5-21-2123171942-2430096820-833724956-1105
Account Name: adminmg
Domain Name: PANOPTICON
Logon ID: 0x1ce95
Log Name: Security
Source: Eventlog
Logged: 12/23/2017 11:00:39 AM
Event ID: 1102
Task Category: Log clear
Level: Information
Keywords: Audit Success
User: N/A
Computer: MEMBER.panopticon.local
OpCode: Info
More Information: Event Log Online Help
Actions
Forwarded Events
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 1102, Eventlog
Event Properties
Attach Task To This Even...
Copy
Save Selected Events...
Refresh
Help

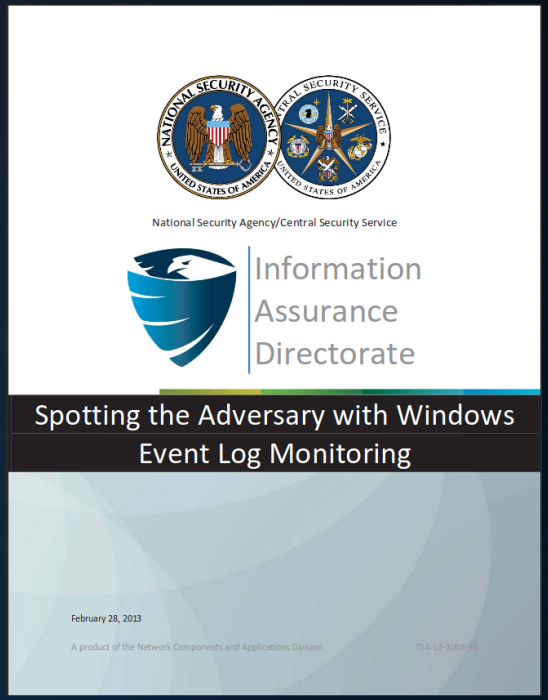
What Events to Monitor?

- 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.

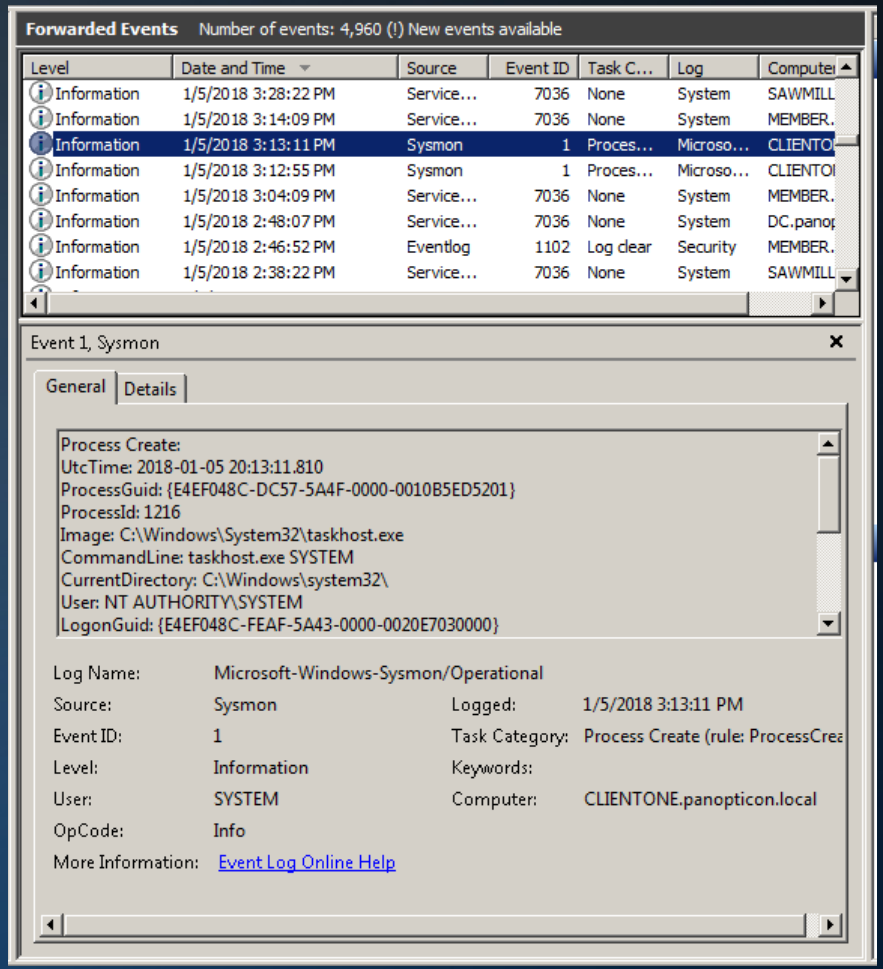


Sysmon

“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


Forwarded Events
Number of events: 4,960 (!) New events available
Level
Date and Time
Source
Event ID
Task C...
Log
Computer
Information 1/5/2018 3:28:22 PM Service... 7036 None System SAWMILL
Information 1/5/2018 3:14:09 PM Service... 7036 None System MEMBER.
Information 1/5/2018 3:13:11 PM Sysmon 1 Proces... Microso... CLIENTO
Information 1/5/2018 3:12:55 PM Sysmon 1 Proces... Microso... CLIENTO
Information 1/5/2018 3:04:09 PM Service... 7036 None System MEMBER.
Information 1/5/2018 2:48:07 PM Service... 7036 None System DC.panop
Information 1/5/2018 2:46:52 PM Eventlog 1102 Log clear Security MEMBER.
Information 1/5/2018 2:38:22 PM Service... 7036 None System SAWMILL
Event 1, Sysmon
General
Details
Process Create:
UtcTime: 2018-01-05 20:13:11.810
ProcessGuid: {E4EF048C-DC57-5A4F-0000-0010B5ED5201}
ProcessId: 1216
Image: C:\Windows\System32\taskhost.exe
CommandLine: taskhost.exe SYSTEM
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {E4EF048C-FEAF-5A43-0000-0020E7030000}
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 1/5/2018 3:13:11 PM
Event ID: 1
Task Category: Process Create (rule: ProcessCrea
Level: Information
Keywords:
User: SYSTEM
Computer: CLIENTONE.panopticon.local
OpCode: Info
More Information: Event Log Online Help

Sysmon

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

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.

OSSEC

- The WEF Collector server must be whitelisted in the firewall rules on the Security Onion server.
- The OSSEC agent on the WEF collection server must be configured to watch the ForwardedEvents log.

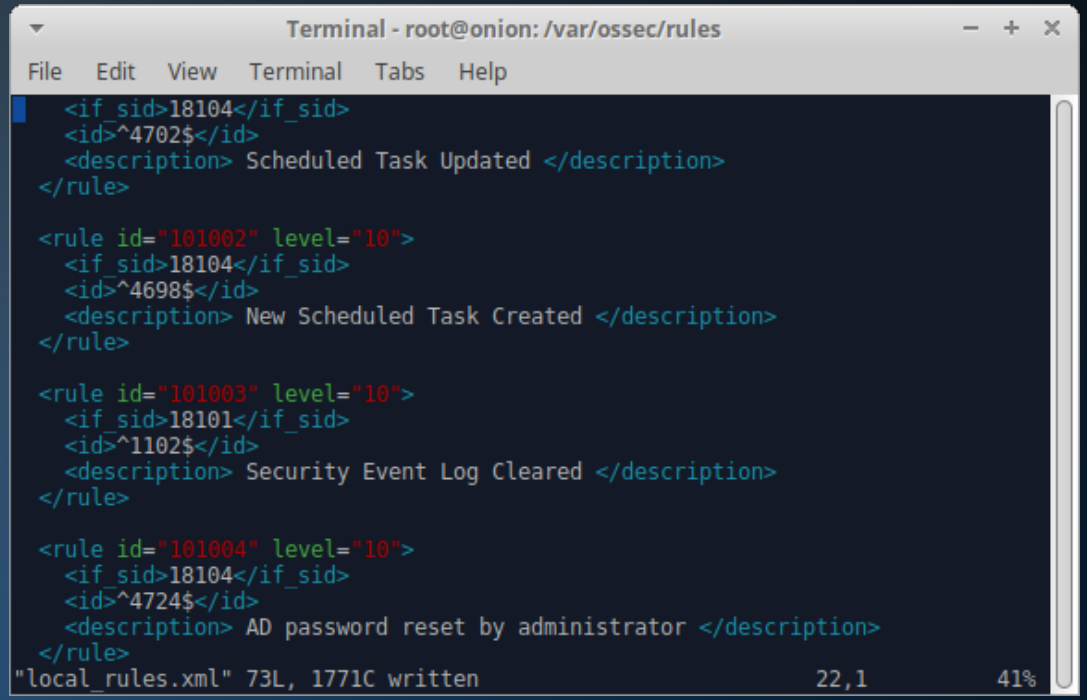
Security Onion

- 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.

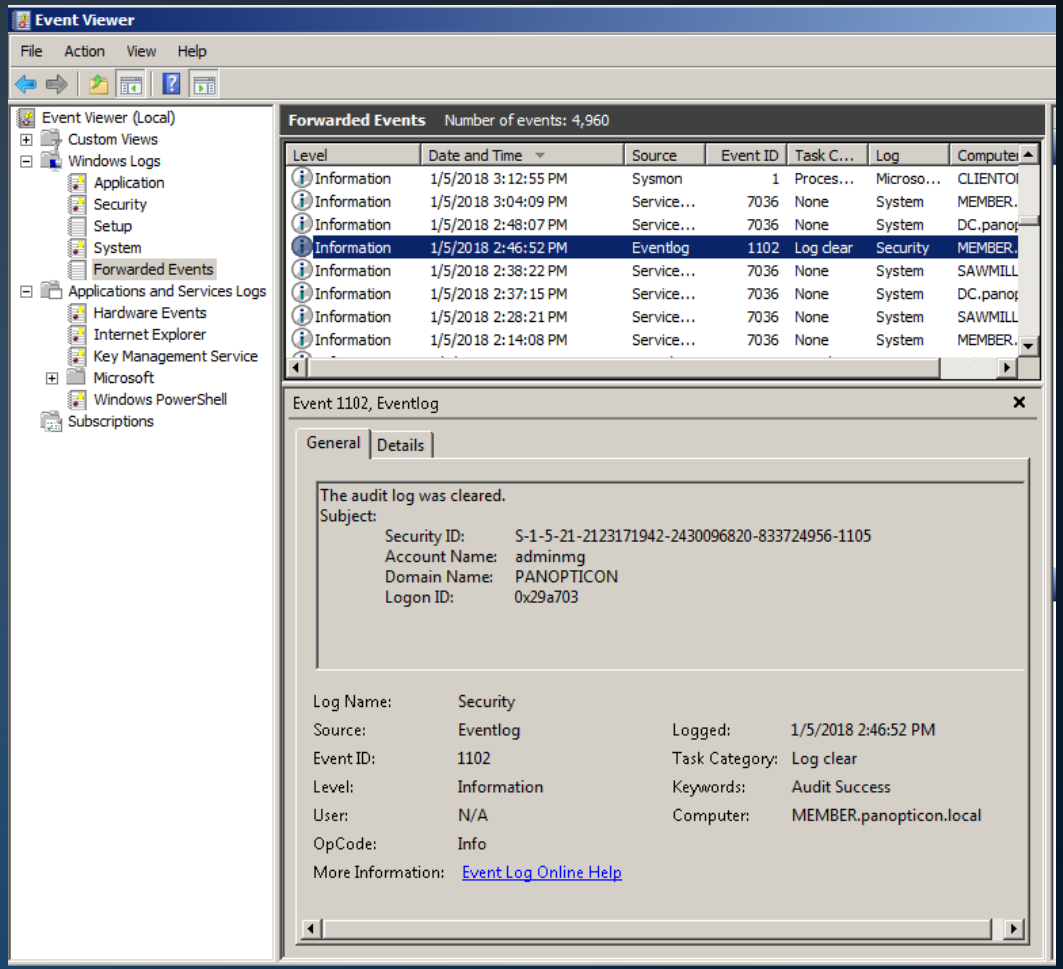
Security Onion - OSSEC

- 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.

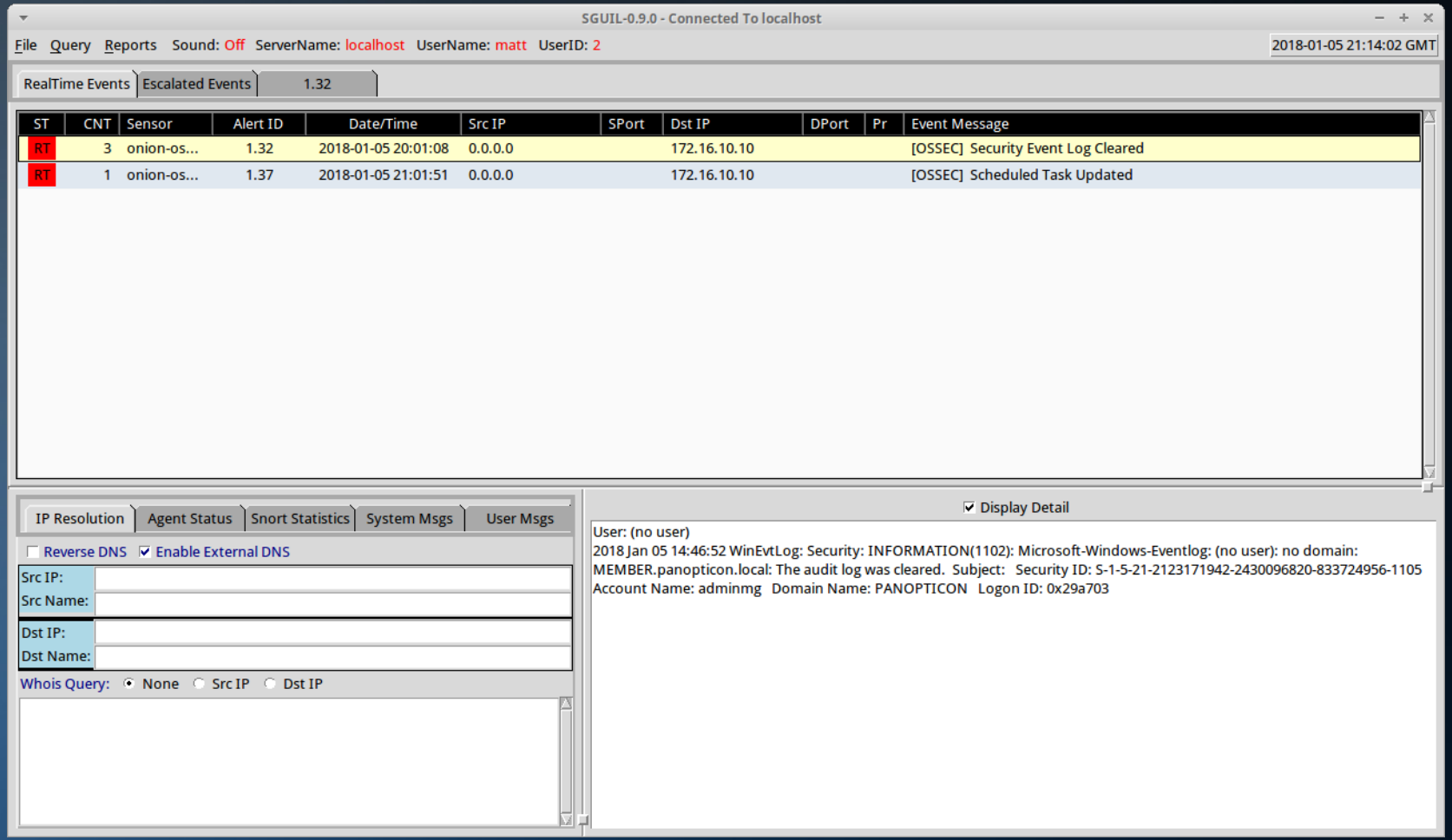
OSSEC Rules


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%

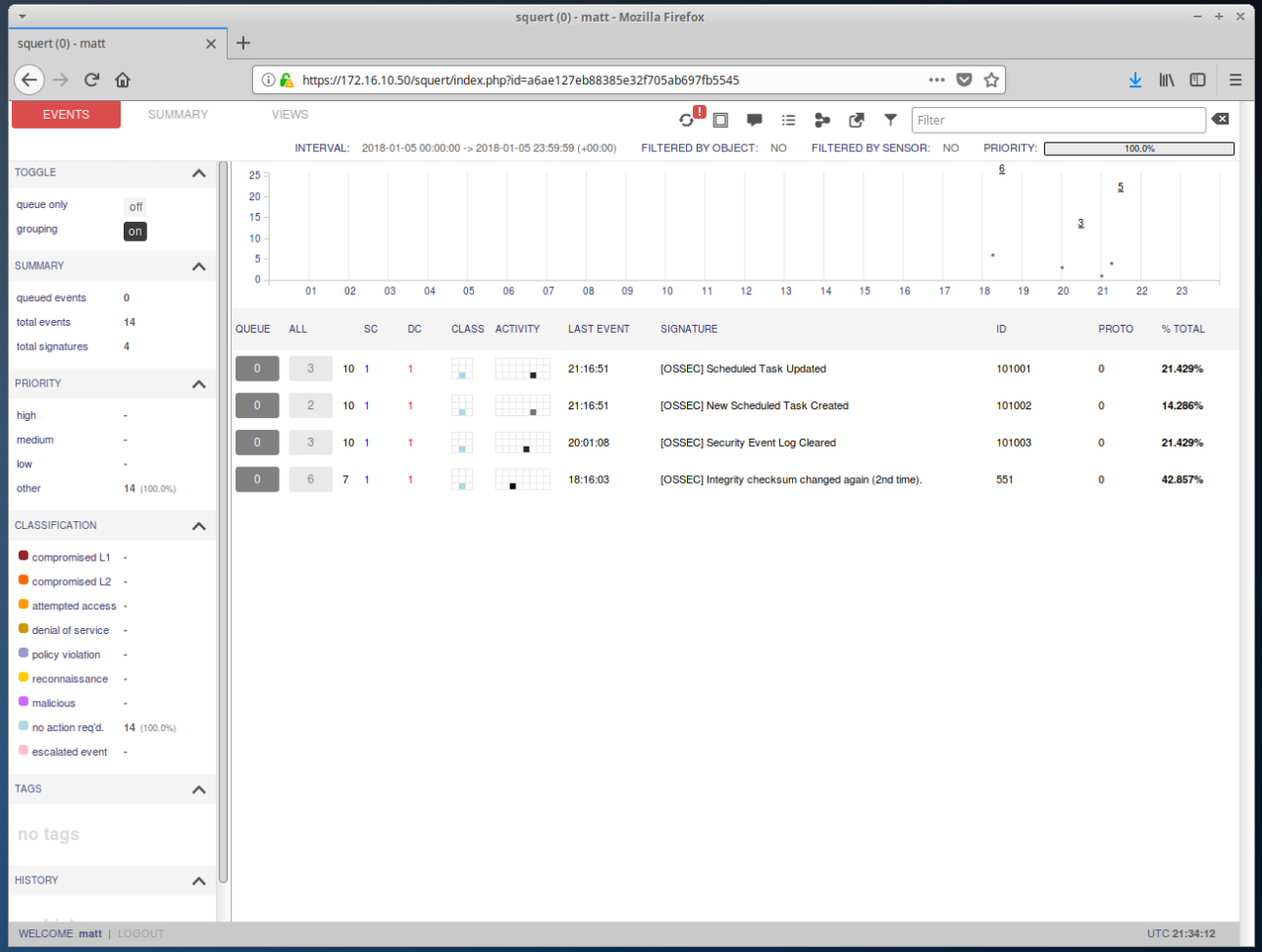
Event Viewer



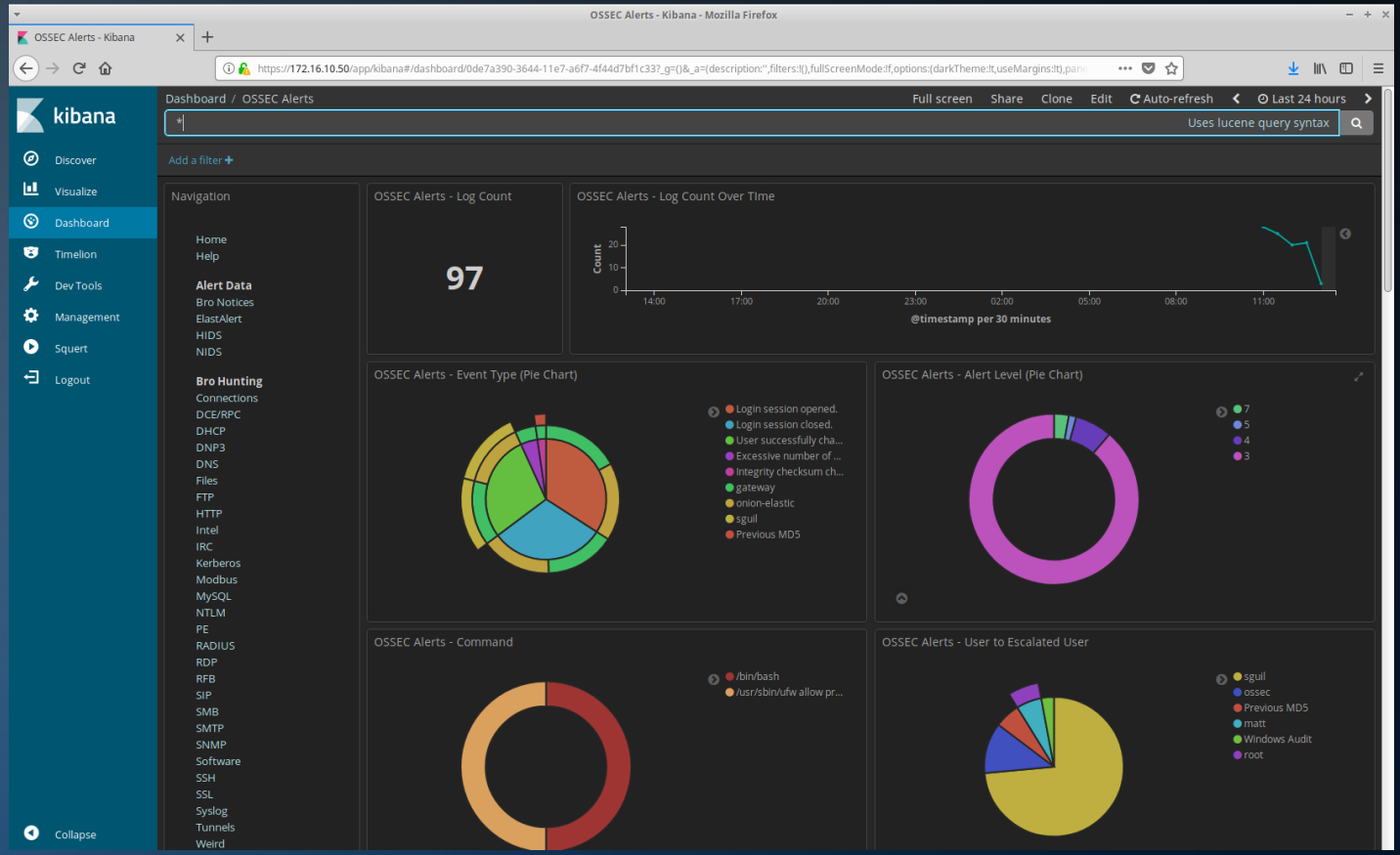
SGUIL


SGUIL-0.9.0 - Connected To localhost
File Query Reports Sound: Off ServerName: localhost UserName: matt UserID: 2
2018-01-05 21:14:02 GMT
RealTime Events
Escalated Events
1.32
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 3 onion-os... 1.32 2018-01-05 20:01:08 0.0.0.0 172.16.10.10 [OSSEC] Security Event Log Cleared
RT 1 onion-os... 1.37 2018-01-05 21:01:51 0.0.0.0 172.16.10.10 [OSSEC] Scheduled Task Updated
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 Jan 05 14:46:52 WinEvtLog: Security: INFORMATION(1102): Microsoft-Windows-Eventlog: (no user): no domain: MEMBER.panopticon.local: The audit log was cleared. Subject: Security ID: S-1-5-21-2123171942-2430096820-833724956-1105 Account Name: adminmg Domain Name: PANOPTICON Logon ID: 0x29a703

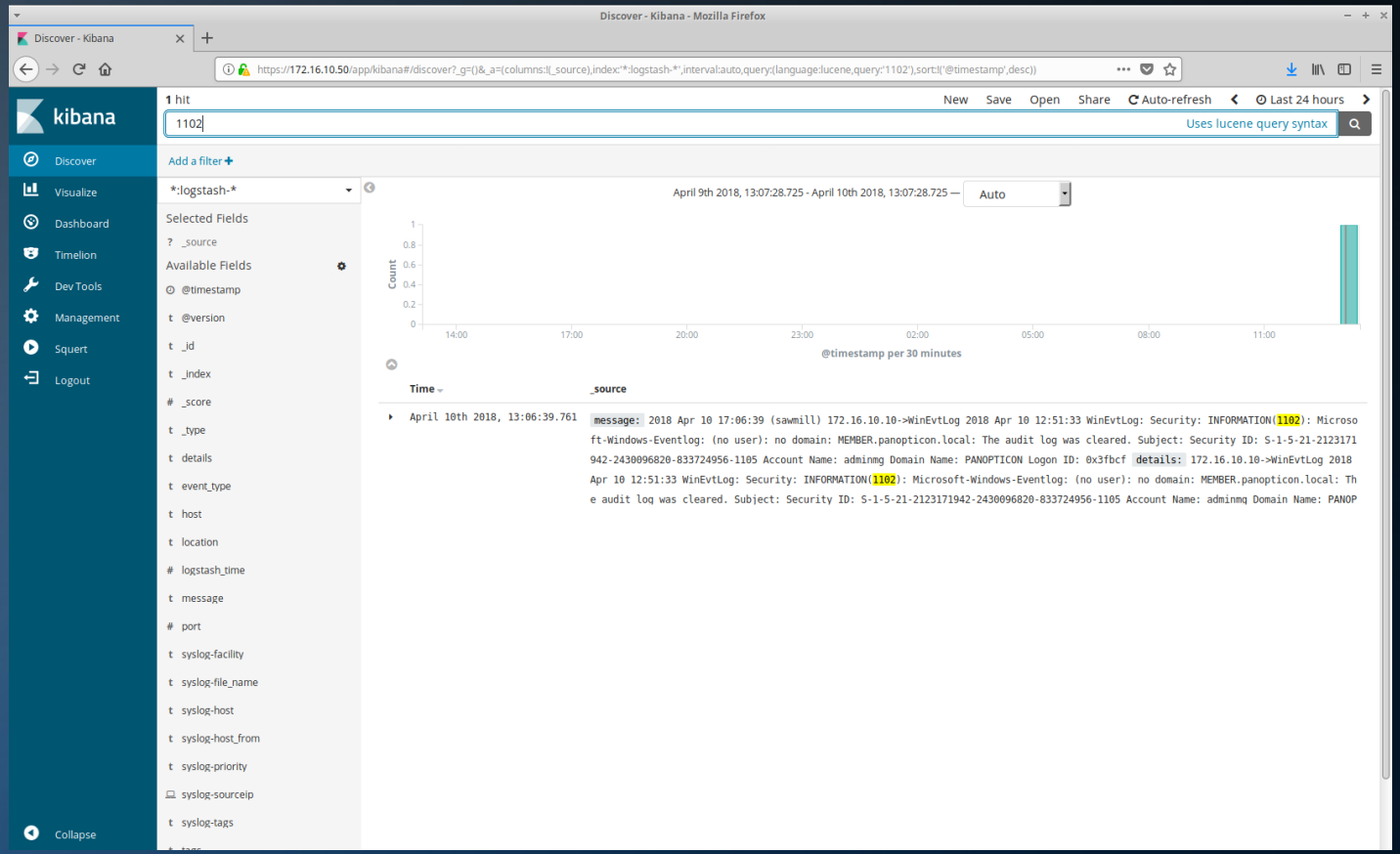
Squert


squert (0) - matt - Mozilla Firefox
squert (0) - matt
https://172.16.10.50/squert/index.php?id=a6ae127eb88385e32f705ab697fb5545
EVENTS
SUMMARY
VIEWS
Filter
INTERVAL: 2018-01-05 00:00:00 -> 2018-01-05 23:59:59 (+00:00)
FILTERED BY OBJECT: NO
FILTERED BY SENSOR: NO
PRIORITY:
100.0%
TOGGLE
queue only off
grouping on
SUMMARY
queued events 0
total events 14
total signatures 4
PRIORITY
high -
medium -
low -
other 14 (100.0%)
CLASSIFICATION
compromised L1 -
compromised L2 -
attempted access -
denial of service -
policy violation -
reconnaissance -
malicious -
no action req'd. 14 (100.0%)
escalated event -
TAGS
no tags
HISTORY
QUEUE ALL SC DC CLASS ACTIVITY LAST EVENT SIGNATURE ID PROTO % TOTAL
0 3 10 1 1 21:16:51 [OSSEC] Scheduled Task Updated 101001 0 21.429%
0 2 10 1 1 21:16:51 [OSSEC] New Scheduled Task Created 101002 0 14.286%
0 3 10 1 1 20:01:08 [OSSEC] Security Event Log Cleared 101003 0 21.429%
0 6 7 1 1 18:16:03 [OSSEC] Integrity checksum changed again (2nd time). 551 0 42.857%
WELCOME matt | LOGOUT
UTC 21:34:12

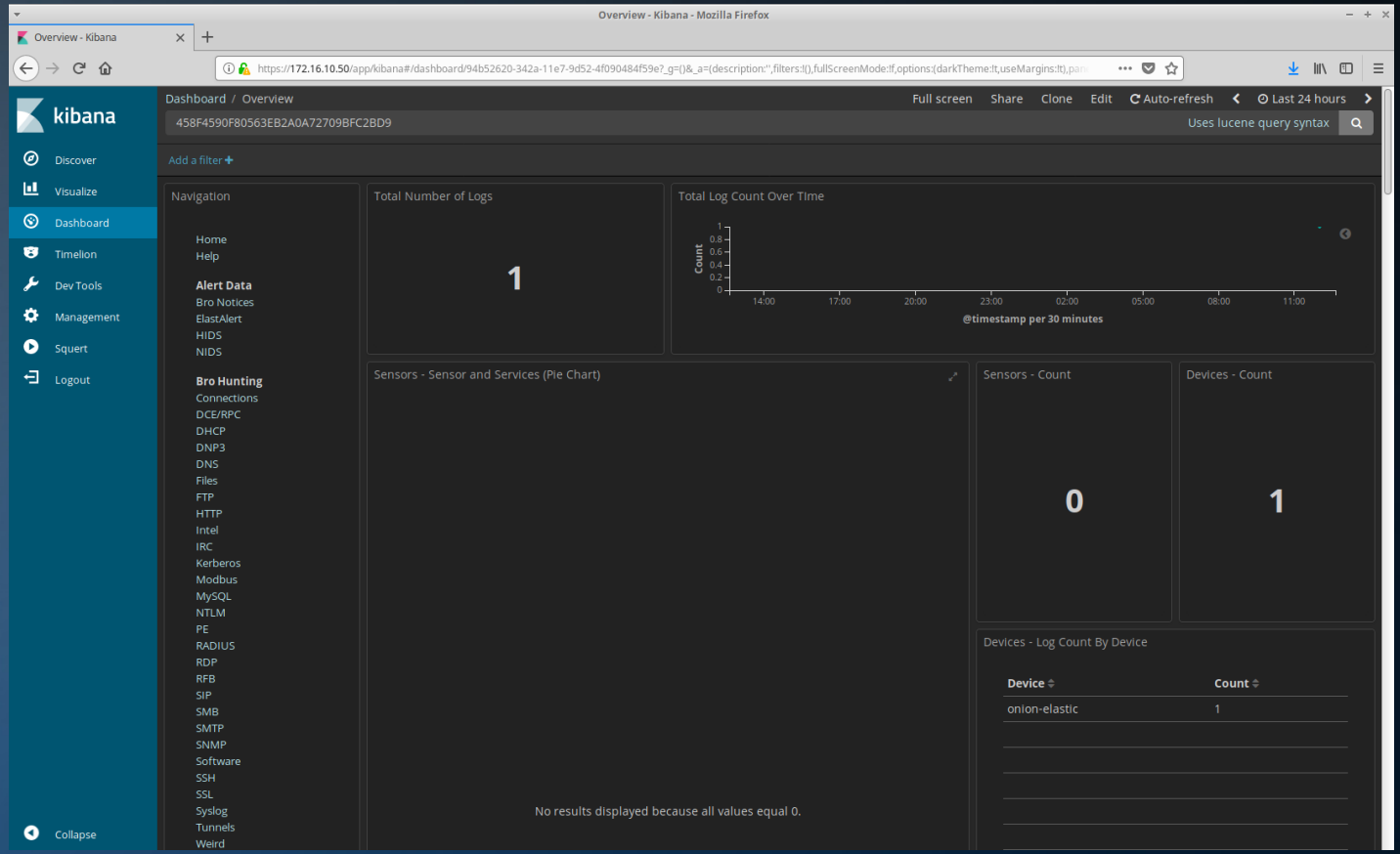
Kibana


OSSEC Alerts - Kibana - Mozilla Firefox
OSSEC Alerts - Kibana
https://172.16.10.50/app/kibana#/dashboard/0de7a390-3644-11e7-a6f7-4f44d7bf1c33?_g=()&_a=(description:'',filters:!(),fullScreenMode:!f,options:(darkTheme:!t,useMargins:!t),pane
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
Dashboard / OSSEC Alerts
Full screen
Share
Clone
Edit
Auto-refresh
Last 24 hours
*
Uses lucene query syntax
Add a filter
Navigation
Home
Help
Alert Data
Bro Notices
ElastAlert
HIDS
NIDS
Bro Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE
RADIUS
RDP
RFB
SIP
SMB
SMTP
SNMP
Software
SSH
SSL
Syslog
Tunnels
Weird
OSSEC Alerts - Log Count
97
OSSEC Alerts - Log Count Over TIme
Count
20
10
0
14:00
17:00
20:00
23:00
02:00
05:00
08:00
11:00
@timestamp per 30 minutes
OSSEC Alerts - Event Type (Pie Chart)
Login session opened.
Login session closed.
User successfully cha...
Excessive number of ...
Integrity checksum ch...
gateway
onion-elastic
sguil
Previous MD5
OSSEC Alerts - Alert Level (Pie Chart)
7
5
4
3
OSSEC Alerts - Command
/bin/bash
/usr/sbin/ufw allow pr...
OSSEC Alerts - User to Escalated User
sguil
ossec
Previous MD5
matt
Windows Audit
root

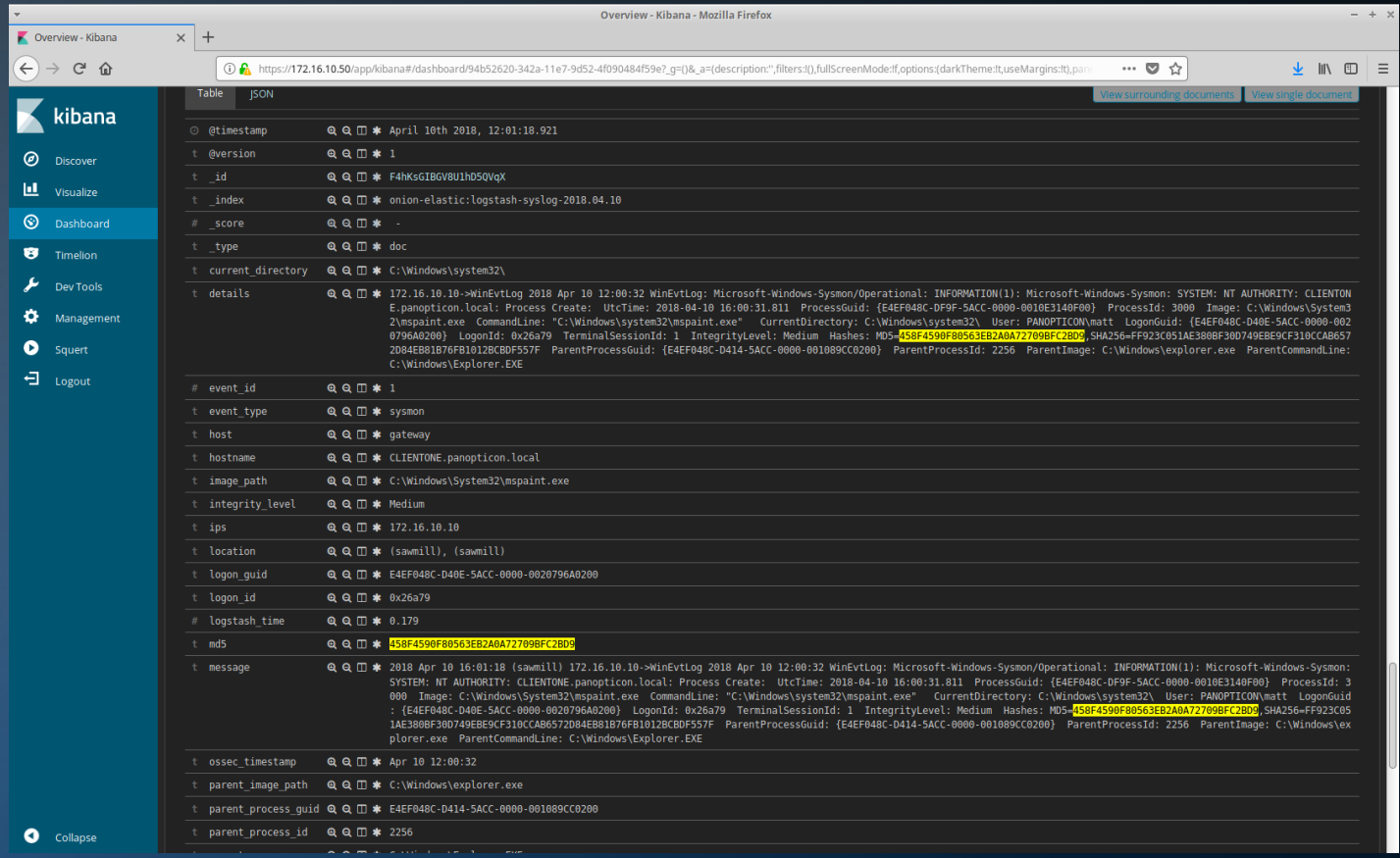
Kibana


Discover - Kibana - Mozilla Firefox
Discover - Kibana
https://172.16.10.50/app/kibana#/discover?_g=()&_a=(columns:!(_source),index:'*:logstash-*',interval:auto,query:(language:lucene,query:'1102'),sort:!('@timestamp',desc))
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
1 hit
New
Save
Open
Share
Auto-refresh
Last 24 hours
1102
Uses lucene query syntax
Add a filter
:logstash-
Selected Fields
? _source
Available Fields
@timestamp
t @version
t _id
t _index
_score
t _type
t details
t event_type
t host
t location
logstash_time
t message
port
t syslog-facility
t syslog-file_name
t syslog-host
t syslog-host_from
t syslog-priority
syslog-sourceip
t syslog-tags
April 9th 2018, 13:07:28.725 - April 10th 2018, 13:07:28.725 —
Auto
Count
@timestamp per 30 minutes
Time
_source
April 10th 2018, 13:06:39.761
message: 2018 Apr 10 17:06:39 (sawmill) 172.16.10.10->WinEvtLog 2018 Apr 10 12:51:33 WinEvtLog: Security: INFORMATION(1102): Microsoft-Windows-Eventlog: (no user): no domain: MEMBER.panopticon.local: The audit log was cleared. Subject: Security ID: S-1-5-21-2123171942-2430096820-833724956-1105 Account Name: adminmg Domain Name: PANOPTICON Logon ID: 0x3fbcf details: 172.16.10.10->WinEvtLog 2018 Apr 10 12:51:33 WinEvtLog: Security: INFORMATION(1102): Microsoft-Windows-Eventlog: (no user): no domain: MEMBER.panopticon.local: The audit log was cleared. Subject: Security ID: S-1-5-21-2123171942-2430096820-833724956-1105 Account Name: adminmg Domain Name: PANOP

Hash Hunting With Kibana

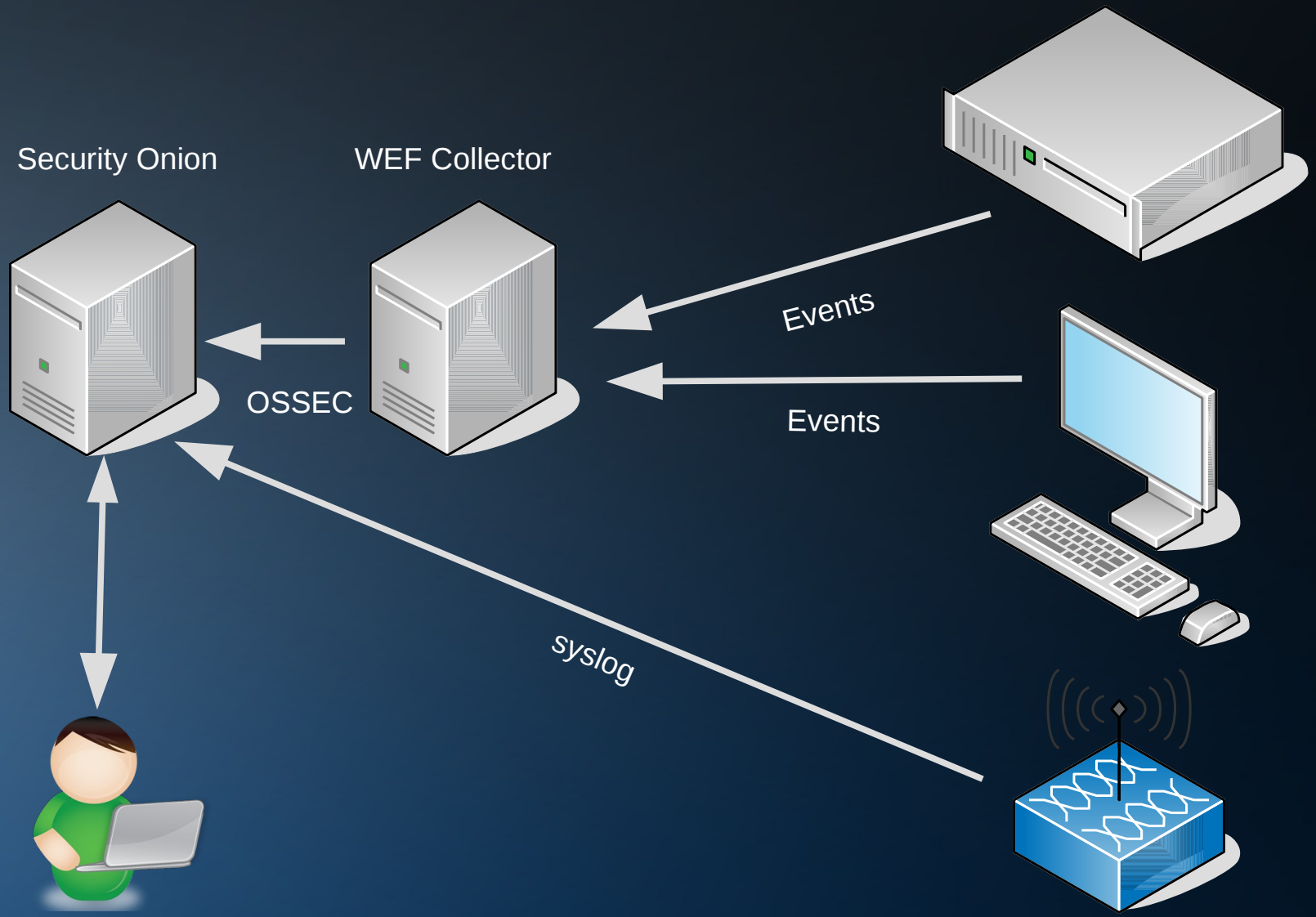


Hash Hunting With Kibana



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.


Security Onion
WEF Collector
Events
OSSEC
Events
syslog

Conclusions/ Questions

For More Information


@InfosecGoon


infosecgoon@roadflares.org


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