Investigating Windows Endpoints With Free Tools

Matthew Gracie
BsidesROC 2022

Who Am I And What Am I Talking About?

The Virtuous Detection Cycle

- Collect Logs From Windows Endpoints
- Write Detections For IOCs In Those Logs
- Use Detection Alerts To Launch Investigation
- Use Investigation Results To Define New IOCs

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

Step One: Collecting Logs

Windows Event Logs

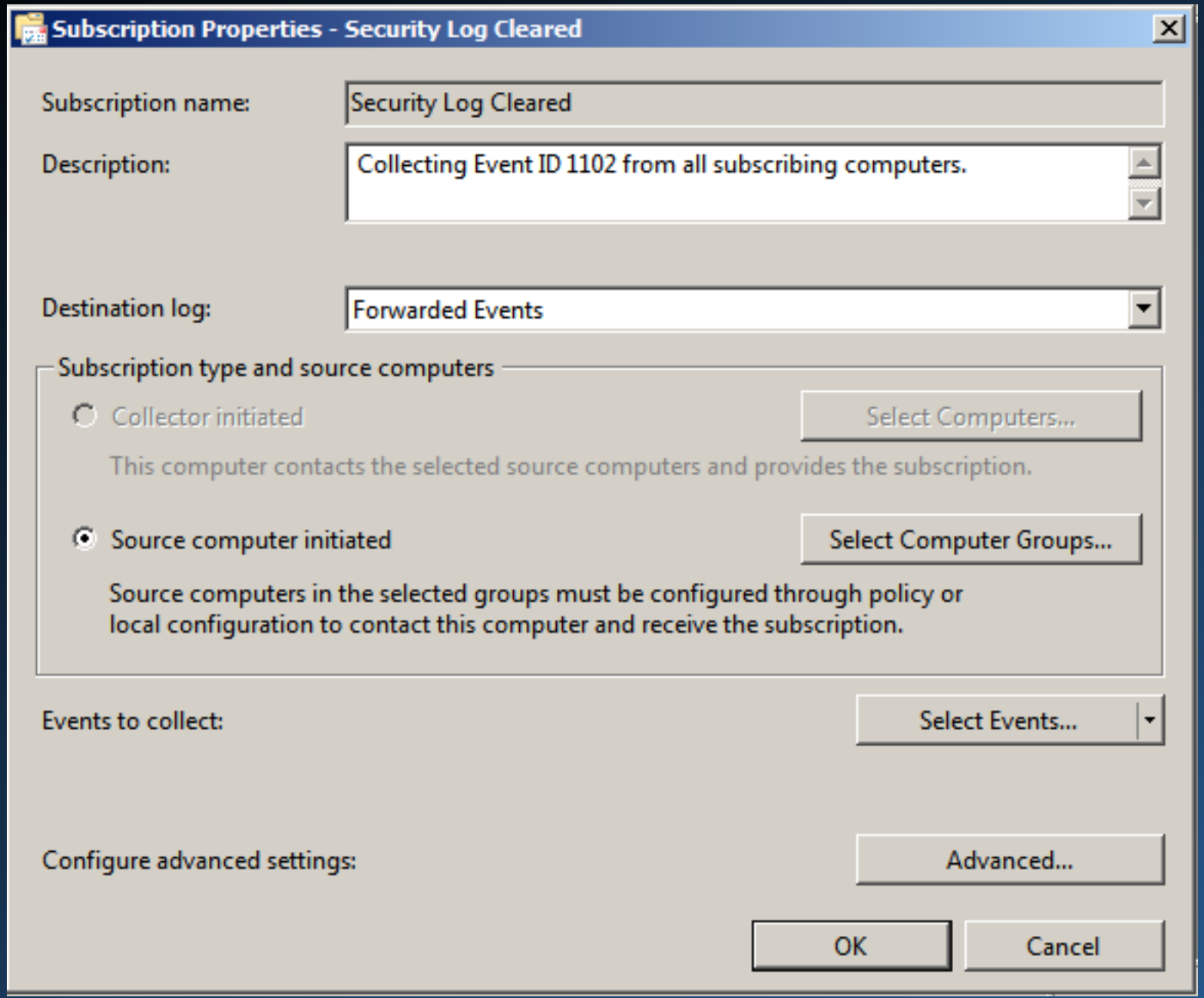
- Windows records system events in local Event Log files, including the classics: Application, Setup, System, and Security.
- Windows 2000 introduced per-application log files.
- Windows Vista rewrote everything with an XML event definition standard.
- Every Event has a standard numeric Event ID.

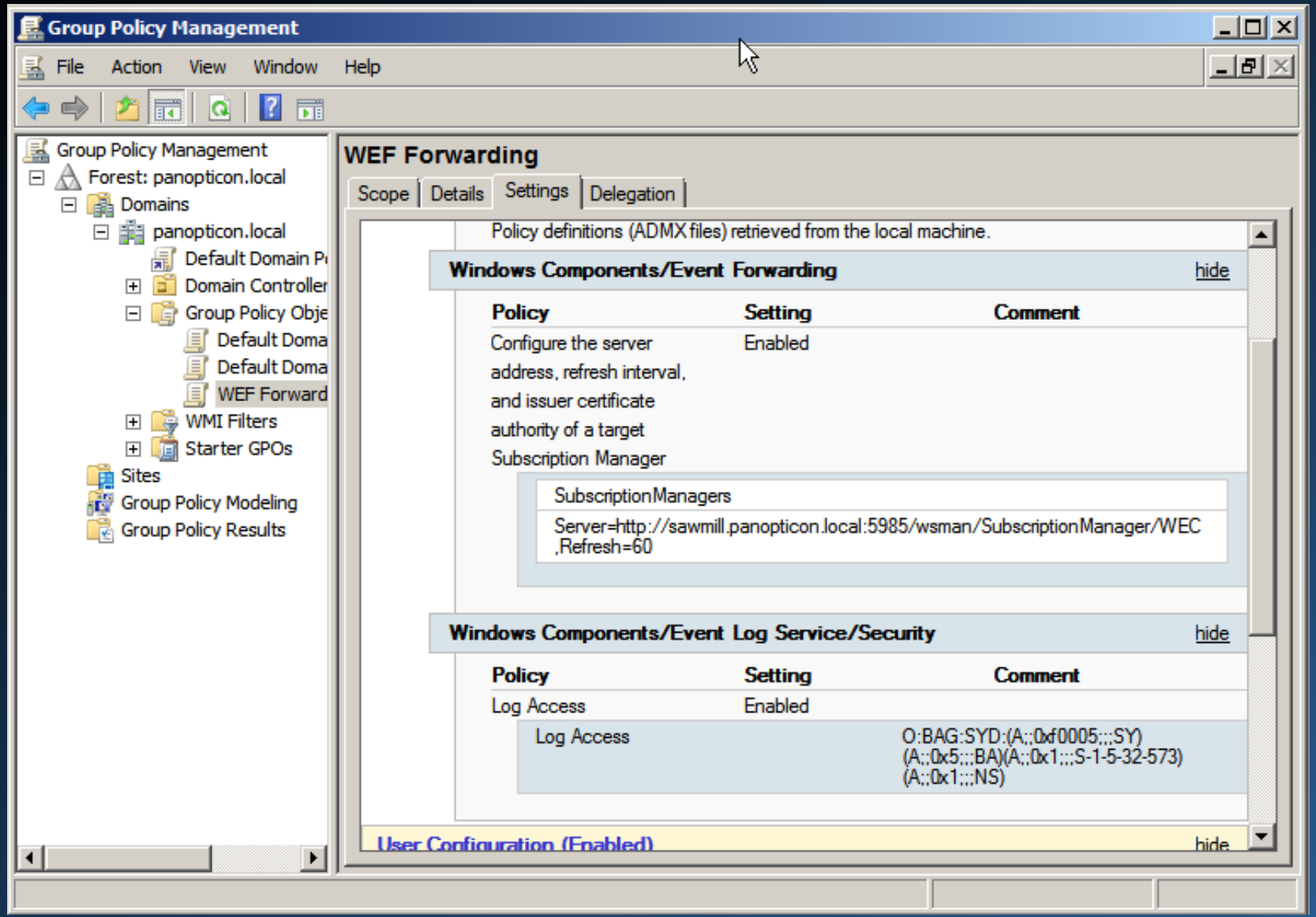

Event Properties - Event 4802, Microsoft Windows security auditi...
General
Details
The screen saver was invoked.
Subject:
Security ID: CONTOSO\dadmin
Account Name: dadmin
Account Domain: CONTOSO
Logon ID: 0x759A9
Session ID: 3
Log Name: Security
Source: Microsoft Windows se
Logged: 9/10/2015 5:16:32 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
Copy
Close

<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

- In an Active Directory environment, log collection is a built-in feature
- Requires a Subscription Server and a GPO


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


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

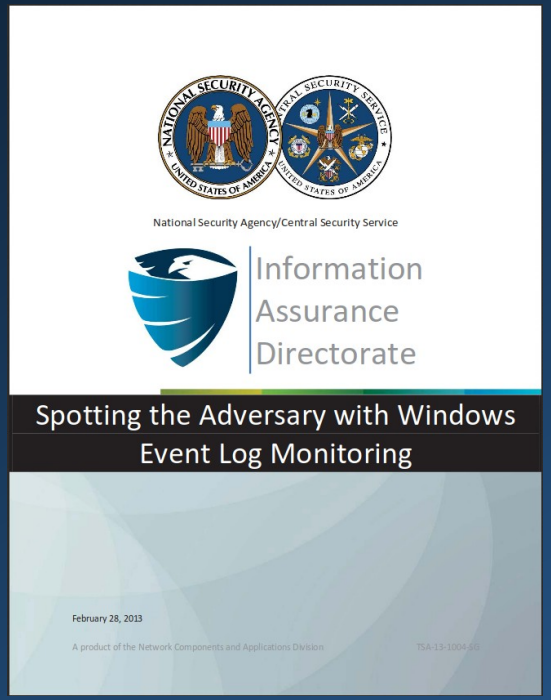
What Events to Monitor?

- 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).

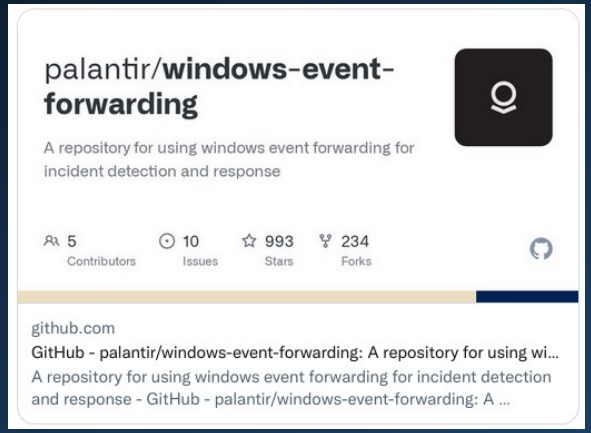
Jessica Payne
“Monitoring What Matters”

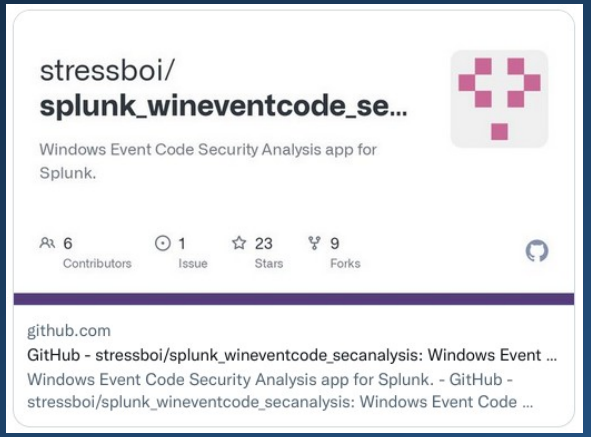
Any Other Suggestions?

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




nsacyber/Event-Forwarding-Guidance
Configuration guidance for implementing collection of security relevant Windows Event Log events by using Windows Event Forwarding. #nsacyber
8 Contributors
5 Issues
686 Stars
158 Forks
github.com
GitHub - nsacyber/Event-Forwarding-Guidance: Configuration guidan...
Configuration guidance for implementing collection of security relevant Windows Event Log events by using Windows Event Forwarding. ...


palantir/windows-event-forwarding
A repository for using windows event forwarding for incident detection and response
5 Contributors
10 Issues
993 Stars
234 Forks
github.com
GitHub - palantir/windows-event-forwarding: A repository for using wi...
A repository for using windows event forwarding for incident detection and response - GitHub - palantir/windows-event-forwarding: A ...


stressboi/splunk_wineventcode_se...
Windows Event Code Security Analysis app for Splunk.
6 Contributors
1 Issue
23 Stars
9 Forks
github.com
GitHub - stressboi/splunk_wineventcode_secanalysis: Windows Event ...
Windows Event Code Security Analysis app for Splunk. - GitHub - stressboi/splunk_wineventcode_secanalysis: Windows Event Code ...

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.

Powershell Logging

- Powershell is a common attacker tool – it should be logged 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
- OSQuery

Step Two: Writing Detections

Sigma

- Sigma is a metalanguage used for defining detections in a vendor agnostic way
- These detections are then compiled for a particular SIEM or platform
- Think of it as YARA, but for logs

Playbook

- Playbook is a Security Onion module that uses the Sigma detection metalanguage to search logs
- If something shows up in the log that matches a detection, an alert is raised

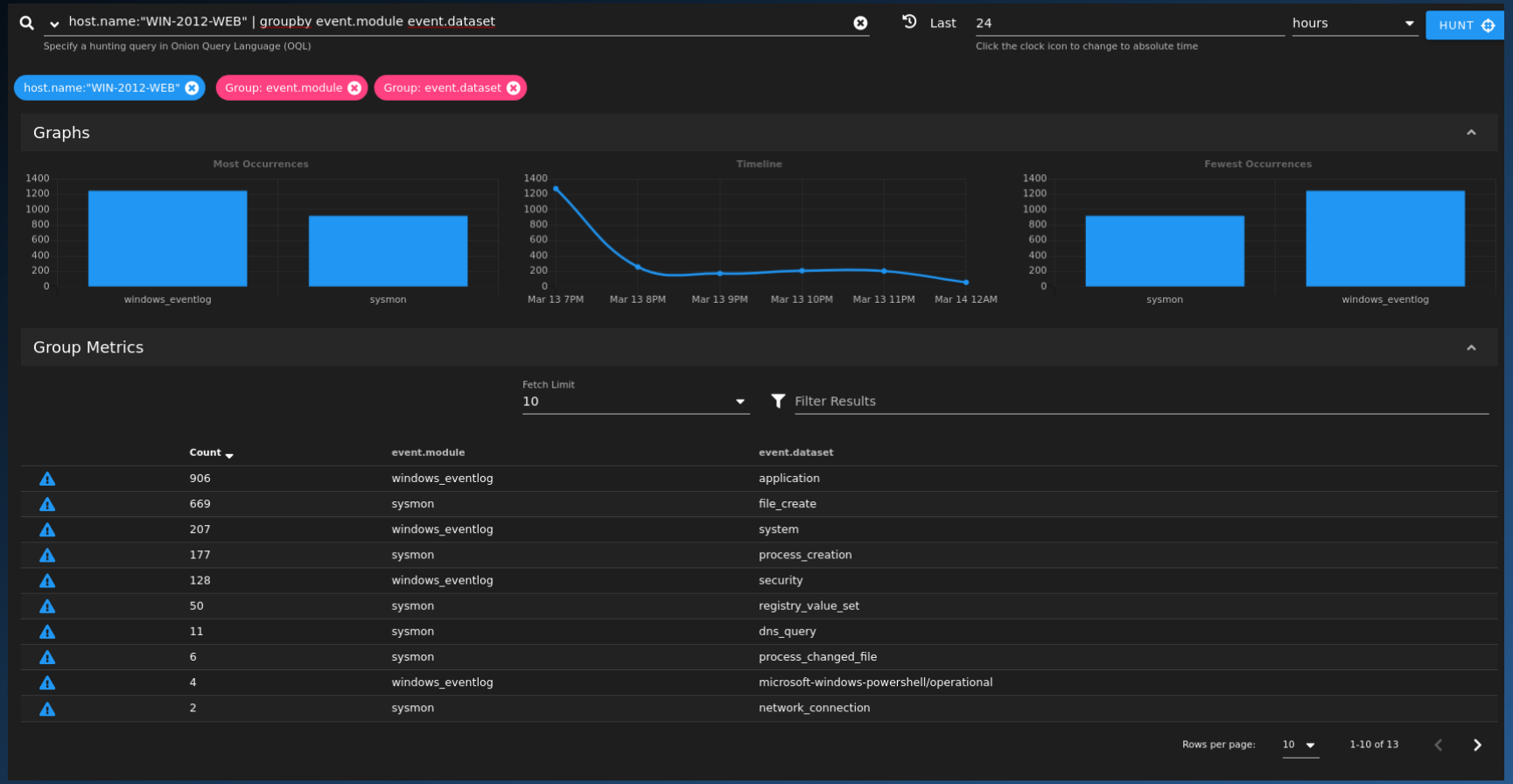
Sigma Edit **Preview**

View Sigma

```yaml
title: Whoami Execution
id: e28a5a99-da44-436d-b7a0-2afc20a5f413
status: experimental
description: Detects the execution of whoami, which is often used by attackers after
  exloitation / privilege escalation but rarely used by administrators
references:
- https://brica.de/alerts/alert/public/1247926/agent-tesla-keylogger-delivered-inside-a-power-iso-daa-archive/
- https://app.any.run/tasks/7eaba74e-c1ea-400f-9c17-5e30eee89906/
author: Florian Roth
date: 2018/08/13
tags:
- attack.discovery
- attack.t1033
- car.2016-03-001
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image: '*\whoami.exe'
  selection2:
    OriginalFileName: whoami.exe
  condition: selection or selection2
falsepositives:
- Admin activity
- Scripts and administrative tools used in the monitored environment
level: high
```

Step Three: Investigation

SOC Hunt


host.name:"WIN-2012-WEB" | groupby event.module event.dataset
Specify a hunting query in Onion Query Language (OQL)
Last
24
hours
Click the clock icon to change to absolute time
HUNT
host.name:"WIN-2012-WEB"
Group: event.module
Group: event.dataset
Graphs
Most Occurrences
1400
1200
1000
800
600
400
200
0
windows_eventlog
sysmon
Timeline
1400
1200
1000
800
600
400
200
0
Mar 13 7PM
Mar 13 8PM
Mar 13 9PM
Mar 13 10PM
Mar 13 11PM
Mar 14 12AM
Fewest Occurrences
1400
1200
1000
800
600
400
200
0
sysmon
windows_eventlog
Group Metrics
Fetch Limit
10
Filter Results
Count
event.module
event.dataset
906 windows_eventlog application
669 sysmon file_create
207 windows_eventlog system
177 sysmon process_creation
128 windows_eventlog security
50 sysmon registry_value_set
11 sysmon dns_query
6 sysmon process_changed_file
4 windows_eventlog microsoft-windows-powershell/operational
2 sysmon network_connection
Rows per page:
10
1-10 of 13

OSQuery

- OSQuery is a management technology from Facebook that allows you to query your endpoints using SQL syntax
- Search for a particular indicator across your fleet from a central console

Demonstration

Summary

- Windows has a robust logging infrastructure that not enough people take advantage of
- Forwarding those logs into another platform for digestion and analysis is free and effective
- Sigma allows for granular, platform-agnostic detections
- Deploying OSQuery agents across your fleet allows for easy investigation from your SOC

Questions?

 @InfosecGoon

 infosecgoon@roadflares.org

 https://github.com/InfosecGoon/