APPLIED PURPLE TEAMING

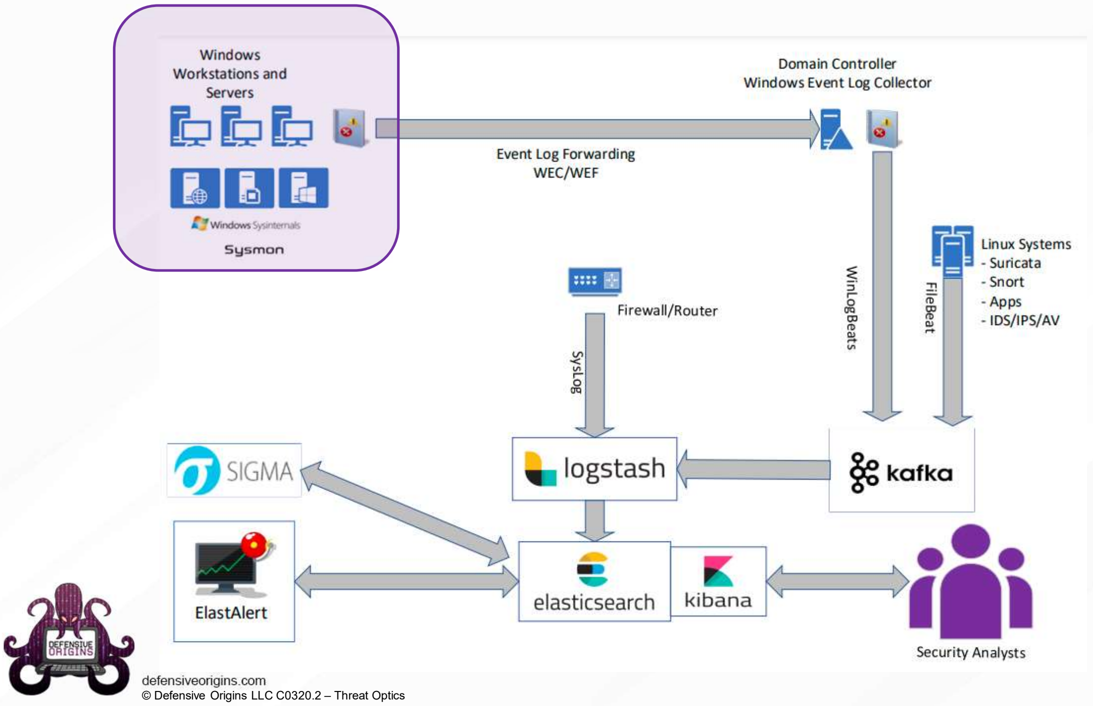
C0320

Threat Optics – Event Logs

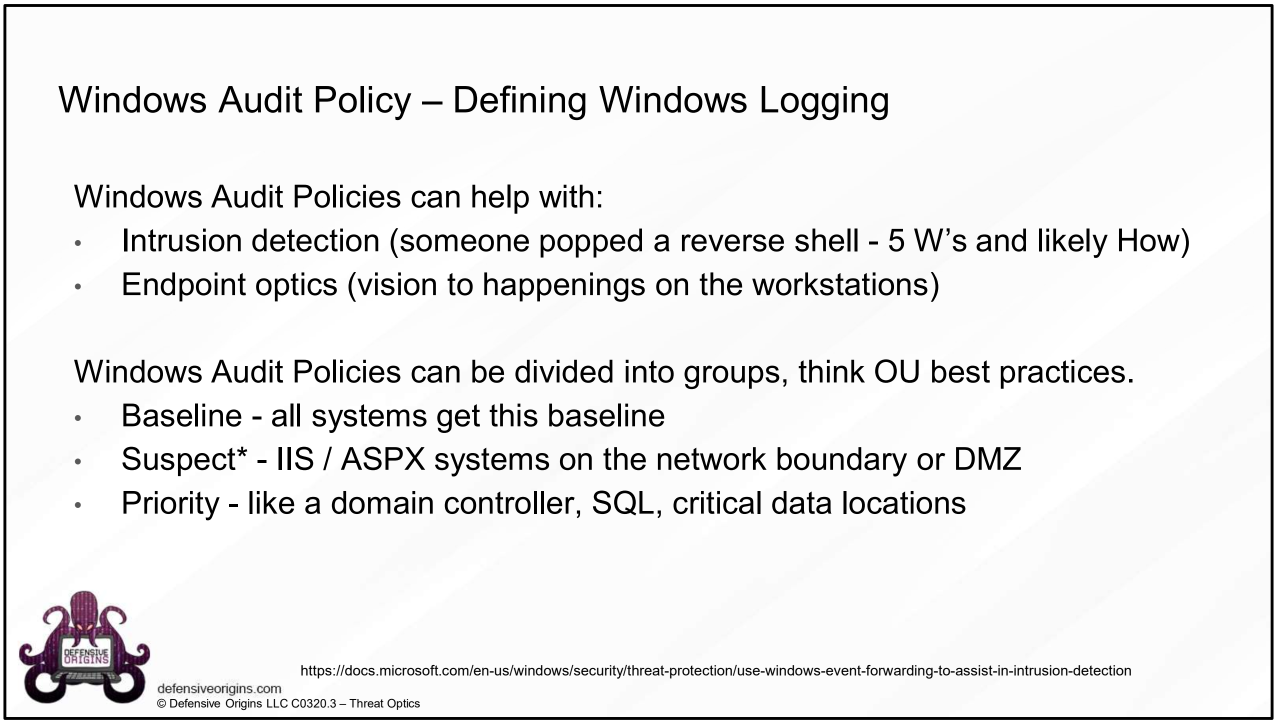
Windows Audit Policies
Windows Event Viewer
Web Apps on IIS

defensiveorigins.com

Applied Purple Teaming – C0320 Threat Optics – Event Logs
Windows Audit Policies
Windows Event Viewer
Web Apps on IIS



defensiveorigins.com
© Defensive Origins LLC C0320.2 – Threat Optics



Windows Audit Policy – Defining Windows Logging

Windows Audit Policies can help with:

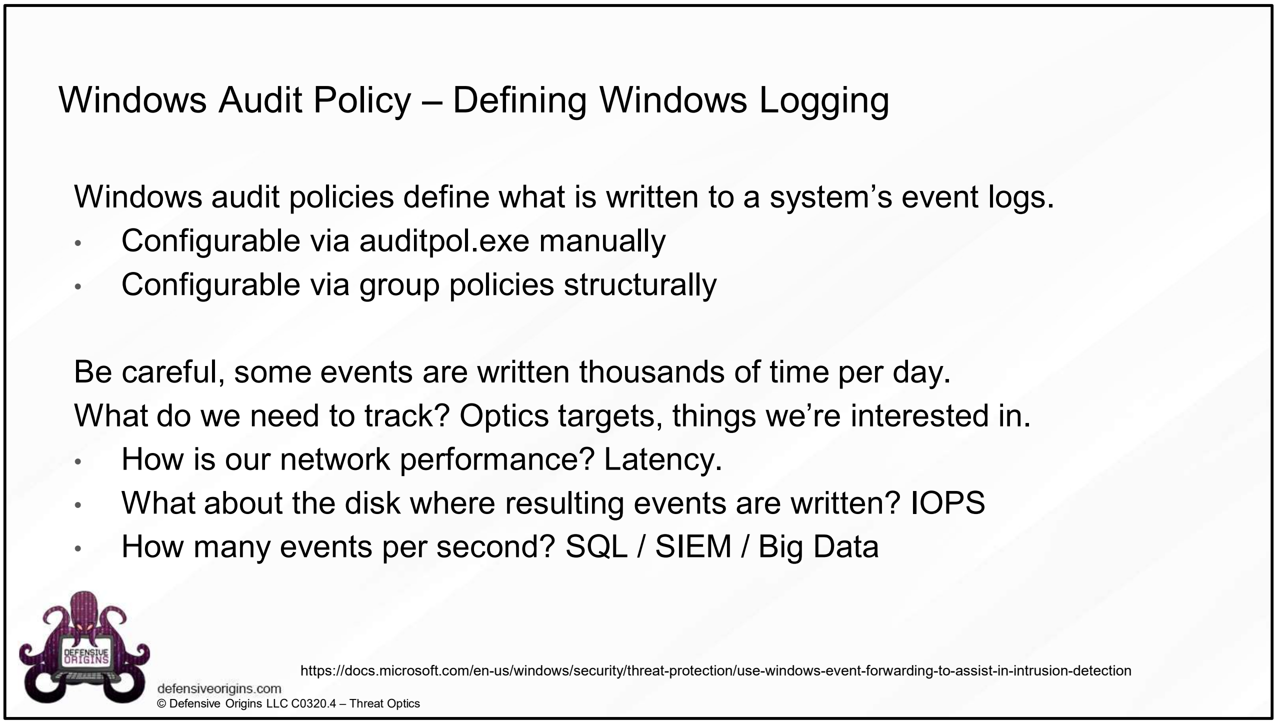
- Intrusion detection (someone popped a reverse shell - 5 W’s and likely How)
- Endpoint optics (vision to happenings on the workstations)

Windows Audit Policies can be divided into groups, think OU best practices.

- Baseline - all systems get this baseline
- Suspect* - IIS / ASPX systems on the network boundary or DMZ
- Priority - like a domain controller, SQL, critical data locations

https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

defensiveorigins.com



Windows Audit Policy – Defining Windows Logging

Windows audit policies define what is written to a system’s event logs.

- Configurable via auditpol.exe manually
- Configurable via group policies structurally

Be careful, some events are written thousands of time per day.

What do we need to track? Optics targets, things we’re interested in.

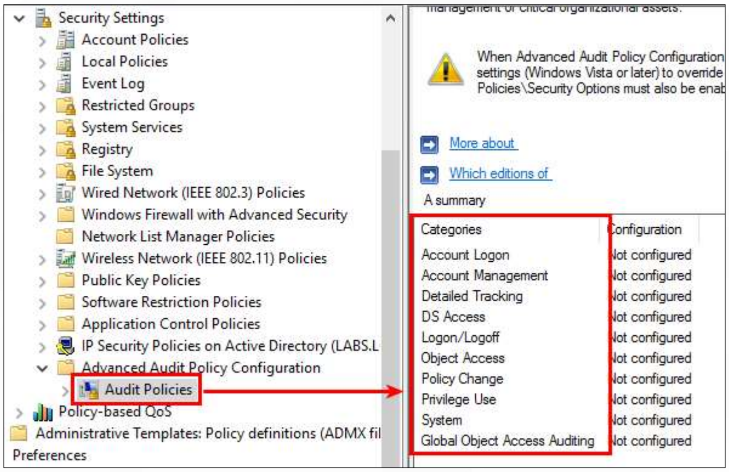
- How is our network performance? Latency.
- What about the disk where resulting events are written? IOPS
- How many events per second? SQL / SIEM / Big Data

https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

Windows Audit Policy – Defining Windows Logging

Audit Policy Configuration is Categorized.

- Account Logon
- Account Management
- Detailed Tracking
- DS Access
- Logon/Logoff
- Object Access
- Policy Change
- Privilege Use
- System
- Global Object Access Auditing


Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
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 (LABS.L
Advanced Audit Policy Configuration
Audit Policies
Policy-based QoS
Administrative Templates: Policy definitions (ADMX fil
Preferences
More about
Which editions of

management of critical organizational assets.

When Advanced Audit Policy Configuration settings (Windows Vista or later) to override Policies\Security Options must also be enab

A summary

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

defensiveorigins.com

Windows Audit Policy – Baseline Policy

Microsoft claims the items here:
1. Should be considered a baseline set of events.
2. Will provide a ton of useful information in log form.

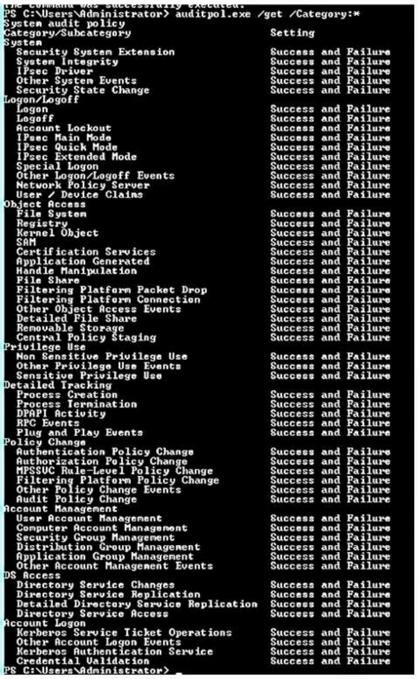
@Microsoft:
We’re tired of configuring these everywhere. Can you just turn them on for us? By default?

Category	Subcategory	Audit settings
Account Logon	Credential Validation	Success and Failure
Account Management	Security Group Management	Success
Account Management	User Account Management	Success and Failure
Account Management	Computer Account Management	Success and Failure
Account Management	Other Account Management Events	Success and Failure
Detailed Tracking	Process Creation	Success
Detailed Tracking	Process Termination	Success
Logon/Logoff	User/Device Claims	Not configured
Logon/Logoff	IPsec Extended Mode	Not configured
Logon/Logoff	IPsec Quick Mode	Not configured
Logon/Logoff	Logon	Success and Failure
Logon/Logoff	Logoff	Success
Logon/Logoff	Other Logon/Logoff Events	Success and Failure
Logon/Logoff	Special Logon	Success and Failure
Logon/Logoff	Account Lockout	Success
Object Access	Application Generated	Not configured
Object Access	File Share	Success
Object Access	File System	Not configured
Object Access	Other Object Access Events	Not configured
Object Access	Registry	Not configured
Object Access	Removable Storage	Success
Policy Change	Audit Policy Change	Success and Failure
Policy Change	MPSSVC Rule-Level Policy Change	Success and Failure
Policy Change	Other Policy Change Events	Success and Failure
Policy Change	Authentication Policy Change	Success and Failure
Policy Change	Authorization Policy Change	Success and Failure
Privilege Use	Sensitive Privilege Use	Not configured
System	Security State Change	Success and Failure
System	Security System Extension	Success and Failure
System	System Integrity	Success and Failure

Audit Policy

The **command prompt** way.

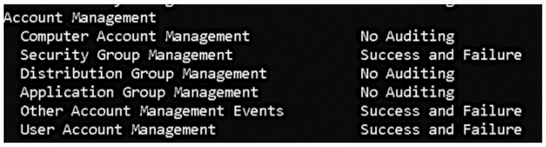
```
auditpol.exe /set /Category:* /success:enable
auditpol.exe /set /Category:* /failure:enable
auditpol.exe /get /Category:*
```



```
The command was successfully executed.
PS C:\Users\Administrator> auditpol.exe /get /Category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            Success and Failure
  Other System Events                     Success and Failure
  Security State Change                   Success and Failure
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         Success and Failure
  IPsec Main Mode                         Success and Failure
  IPsec Quick Mode                        Success and Failure
  IPsec Extended Mode                     Success and Failure
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   Success and Failure
  User / Device Claims                    Success and Failure
Object Access
  File System                             Success and Failure
  Registry                                Success and Failure
  Kernel Object                           Success and Failure
  SAM                                     Success and Failure
  Certification Services                  Success and Failure
  Application Generated                   Success and Failure
  Handle Manipulation                     Success and Failure
  File Share                              Success and Failure
  Filtering Platform Packet Drop          Success and Failure
  Filtering Platform Connection           Success and Failure
  Other Object Access Events              Success and Failure
  Detailed File Share                     Success and Failure
  Removable Storage                       Success and Failure
  Central Policy Staging                  Success and Failure
Privilege Use
  Non Sensitive Privilege Use             Success and Failure
  Other Privilege Use Events              Success and Failure
  Sensitive Privilege Use                 Success and Failure
Detailed Tracking
  Process Creation                        Success and Failure
  Process Termination                     Success and Failure
  DPAPI Activity                          Success and Failure
  RPC Events                              Success and Failure
  Plug and Play Events                    Success and Failure
Policy Change
  Authentication Policy Change            Success and Failure
  Authorization Policy Change             Success and Failure
  MPSSVC Rule-Level Policy Change         Success and Failure
  Filtering Platform Policy Change        Success and Failure
  Other Policy Change Events              Success and Failure
  Audit Policy Change                     Success and Failure
Account Management
  User Account Management                 Success and Failure
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
DS Access
  Directory Service Changes               Success and Failure
  Directory Service Replication           Success and Failure
  Detailed Directory Service Replication  Success and Failure
  Directory Service Access                Success and Failure
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure
PS C:\Users\Administrator> _
```

Configurable via GPO

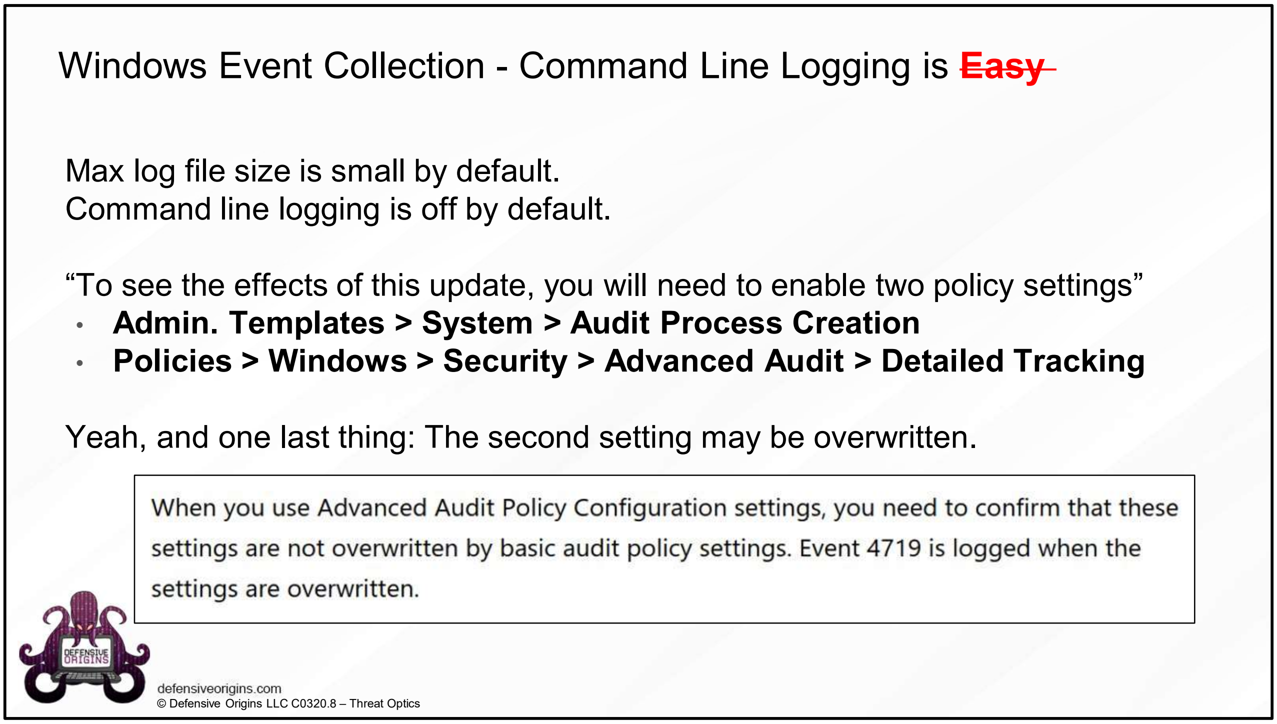
- More difficult, settings in a few different places
- BUT – granular controls are nice



```
Account Management
  Computer Account Management             No Auditing
  Security Group Management               Success and Failure
  Distribution Group Management           No Auditing
  Application Group Management            No Auditing
  Other Account Management Events         Success and Failure
  User Account Management                 Success and Failure
```

Commands:

```
auditpol.exe /set /Category:* /success:enable
auditpol.exe /set /Category:* /failure:enable
auditpol.exe /get /Category:*
```



Windows Event Collection - Command Line Logging is ~~Easy~~

Max log file size is small by default.
Command line logging is off by default.

“To see the effects of this update, you will need to enable two policy settings”

- **Admin. Templates > System > Audit Process Creation**
- **Policies > Windows > Security > Advanced Audit > Detailed Tracking**

Yeah, and one last thing: The second setting may be overwritten.

When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. Event 4719 is logged when the settings are overwritten.

defensiveorigins.com

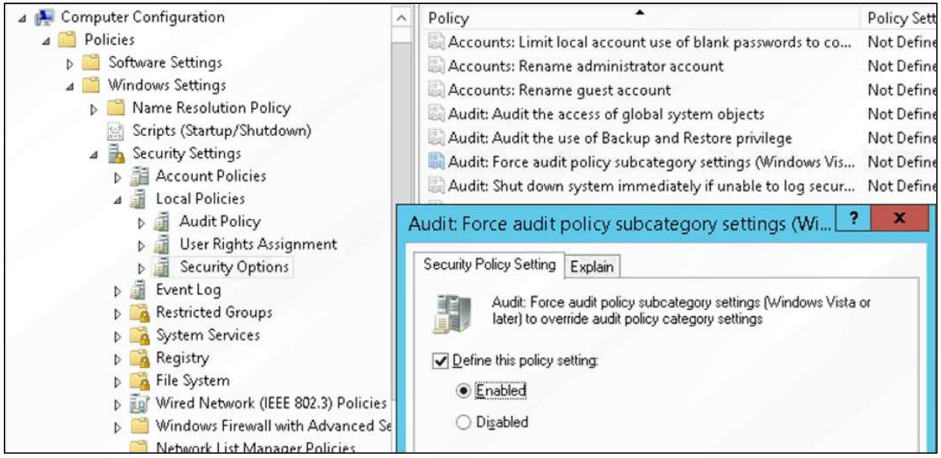
Group Policy Object Policy Paths:

```
Admin. Templates > System > Audit Process Creation
Policies > Windows > Security > Advanced Audit > Detailed Tracking
```

Windows Event Collection - Command Line Logging is ~~Easy~~

To avoid the overwriting of Advanced Audit settings, a *third* setting is required.
Computer Configuration > Policies > Windows Settings > Security > Local > Security

- Setting – **Audit: Force Audit Policy Subcategory Settings = *Enabled***



Policy	Policy Sett
Accounts: Limit local account use of blank passwords to co...	Not Define
Accounts: Rename administrator account	Not Define
Accounts: Rename guest account	Not Define
Audit: Audit the access of global system objects	Not Define
Audit: Audit the use of Backup and Restore privilege	Not Define
Audit: Force audit policy subcategory settings (Windows Vis...	Not Define
Audit: Shut down system immediately if unable to log secur...	Not Define

Audit: Force audit policy subcategory settings (Wi...

Security Policy Setting | Explain

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

☑ Define this policy setting:

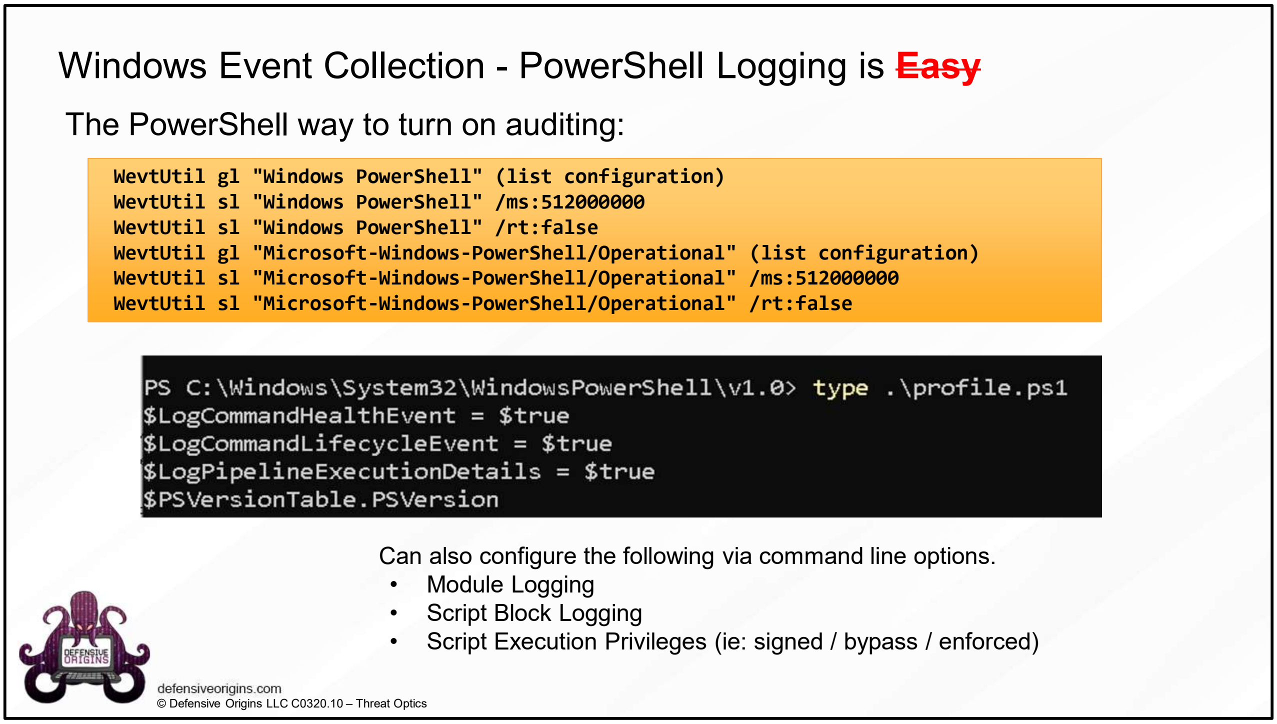
● Enabled

○ Disabled

Group Policy Object Policy Paths:

```
Computer Configuration > Policies > Windows Settings > Security >
Local > Security
```

Setting: Audit: Force Audit Policy Subcategory Settings = *Enabled*



Windows Event Collection - PowerShell Logging is ~~Easy~~

The PowerShell way to turn on auditing:

```
WevtUtil gl "Windows PowerShell" (list configuration)
WevtUtil sl "Windows PowerShell" /ms:512000000
WevtUtil sl "Windows PowerShell" /rt:false
WevtUtil gl "Microsoft-Windows-PowerShell/Operational" (list configuration)
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false
```

```
PS C:\Windows\System32\WindowsPowerShell\v1.0> type .\profile.ps1
$LogCommandHealthEvent = $true
$LogCommandLifecycleEvent = $true
$LogPipelineExecutionDetails = $true
$PSVersionTable.PSVersion
```

Can also configure the following via command line options.

- Module Logging
- Script Block Logging
- Script Execution Privileges (ie: signed / bypass / enforced)

defensiveorigins.com

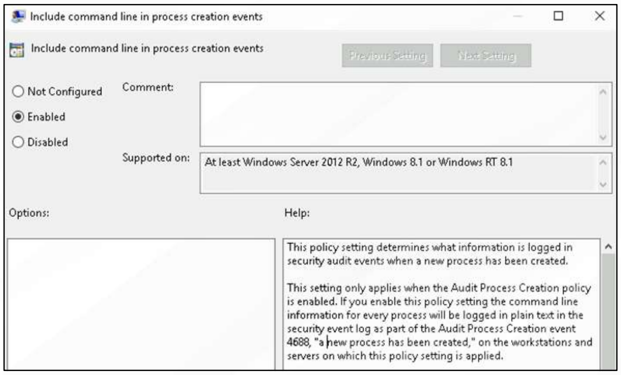
© Defensive Origins LLC C0320.10 – Threat Optics

Commands:

```
WevtUtil gl "Windows PowerShell" (list configuration)
WevtUtil sl "Windows PowerShell" /ms:512000000
WevtUtil sl "Windows PowerShell" /rt:false
WevtUtil gl "Microsoft-Windows-PowerShell/Operational" (list
configuration)
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false
```

Windows Event Collection - PowerShell Logging is ~~Easy~~

The Group Policy way to turn on PowerShell auditing:
Policies > Admin Templates > System > Audit Process Creation



Include command line in process creation events

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Help:

This policy setting determines what information is logged in security audit events when a new process has been created.

This setting only applies when the Audit Process Creation policy is enabled. If you enable this policy setting the command line information for every process will be logged in plain text in the security event log as part of the Audit Process Creation event 4688, "a new process has been created," on the workstations and servers on which this policy setting is applied.

Can also configure more granular things under the PowerShell config section.
Admin Templates > Windows Components > Windows PowerShell

- Module Logging
- Script Block Logging
- Script Execution Privileges (ie: signed / bypass / enforced)

Group Policy Object Policy Paths:

```
Policies > Admin Templates > System > Audit Process Creation
Admin Templates > Windows Components > Windows PowerShell
```

Windows Event Collection
What About IIS Logging?

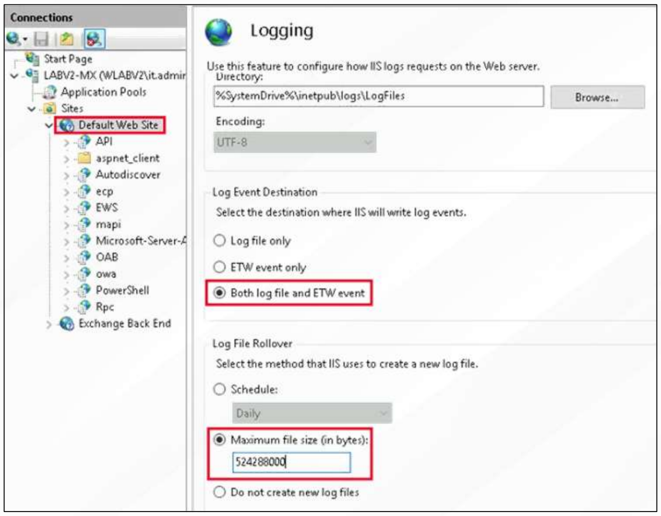
Yeah, that's not on by default either.
LogFiles (text) written by default…
Nothing to event log.

Enable:

- Both log file and ETW event
- Maximum file size

And then you can catch:

- MailSniper
- Burp Suite sprays
- Hydra
- Authentication interactions with Exchange



Logging

Use this feature to configure how IIS logs requests on the Web server.

Directory: %SystemDrive%\inetpub\logs\LogFiles

Encoding: UTF-8

Log Event Destination

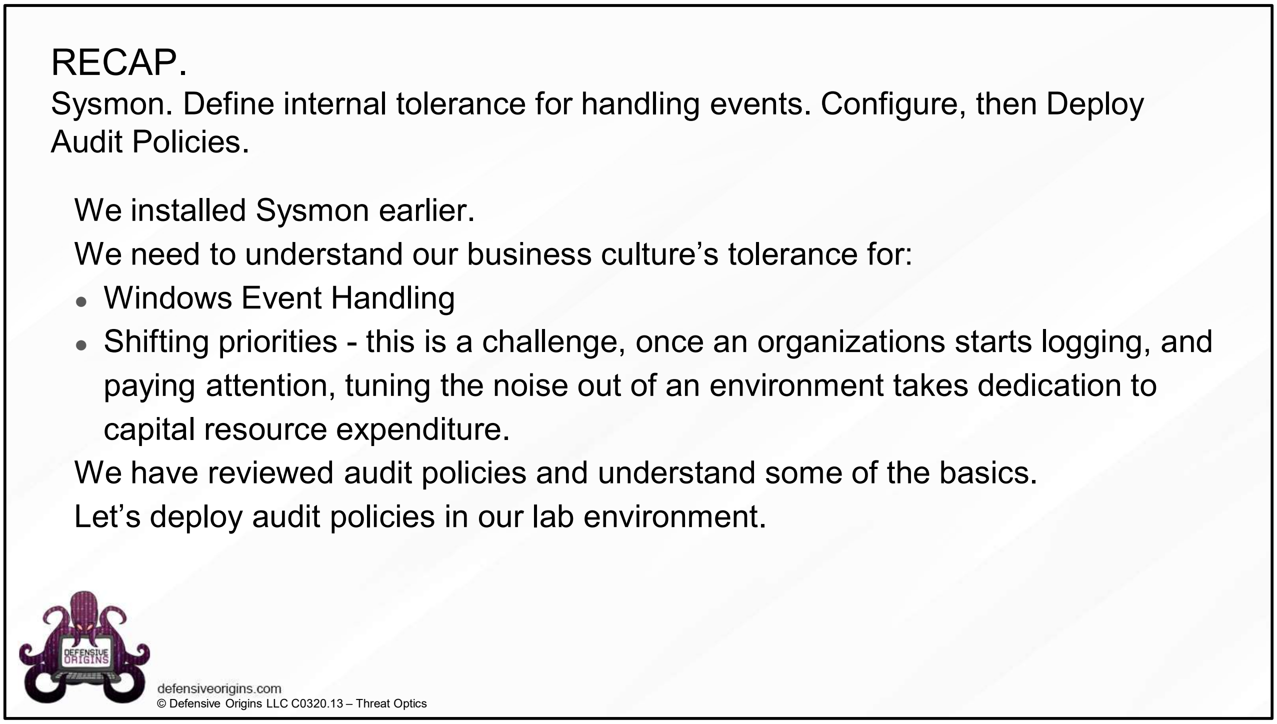
Select the destination where IIS will write log events.

○ Log file only
○ ETW event only
● Both log file and ETW event

Log File Rollover

Select the method that IIS uses to create a new log file.

○ Schedule: Daily
● Maximum file size (in bytes): 524288000
○ Do not create new log files



RECAP.

Sysmon. Define internal tolerance for handling events. Configure, then Deploy Audit Policies.

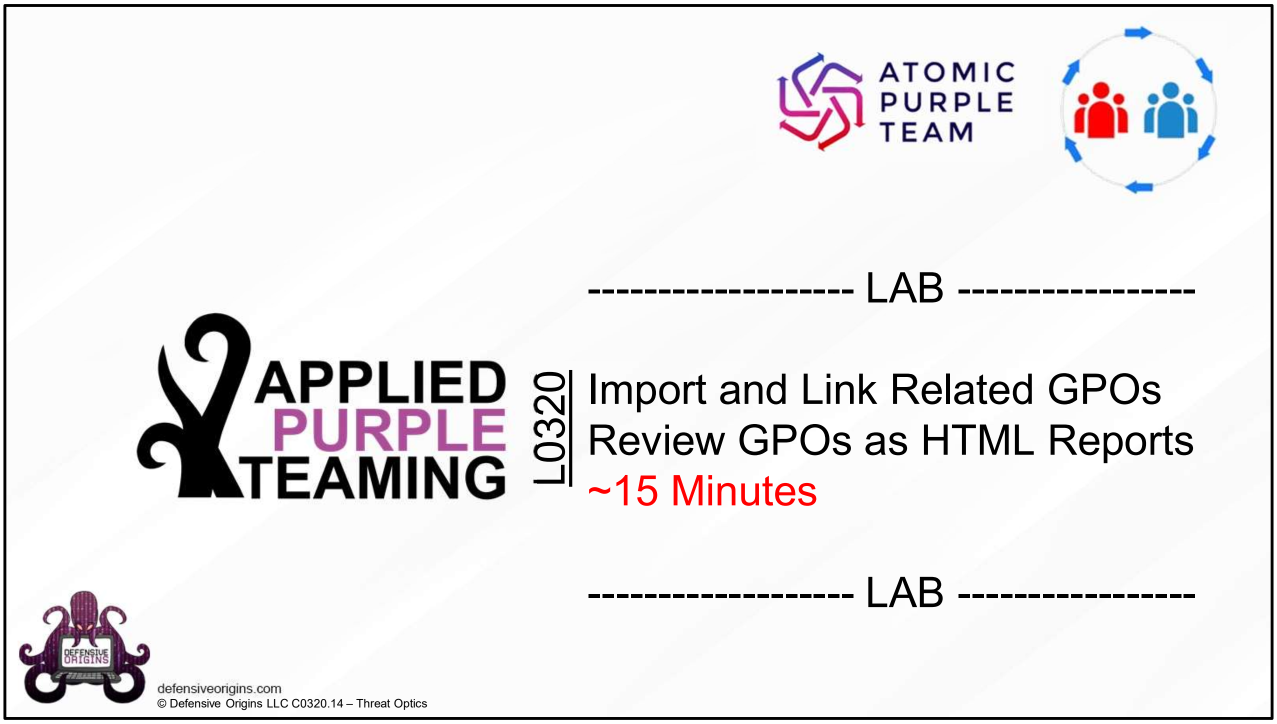
We installed Sysmon earlier.

We need to understand our business culture’s tolerance for:

- Windows Event Handling
- Shifting priorities - this is a challenge, once an organizations starts logging, and paying attention, tuning the noise out of an environment takes dedication to capital resource expenditure.

We have reviewed audit policies and understand some of the basics.

Let’s deploy audit policies in our lab environment.



ATOMIC PURPLE TEAM

APPLIED PURPLE TEAMING

------------------- LAB -----------------

L0320

Import and Link Related GPOs
Review GPOs as HTML Reports
~15 Minutes

------------------- LAB -----------------

defensiveorigins.com

Applied Purple Teaming – L0320 Threat Optics Lab 2
Group Policy Configuration and Import
15 Minutes