



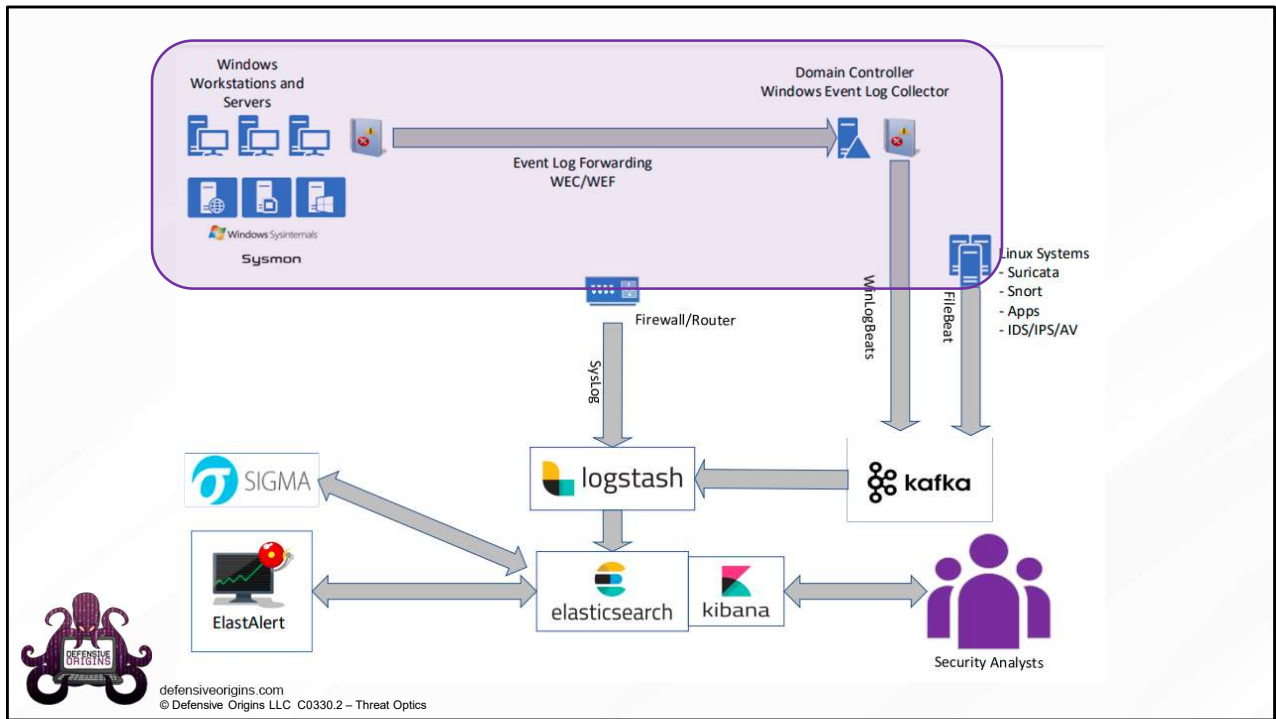
C0330

Threat Optics – Event Handling
WEC / WEF
Event Subscriptions and Channels



defensiveorigins.com
© Defensive Origins LLC C0330.1 – Threat Optics

Applied Purple Teaming – C0330 Threat Optics – Event Handling
Windows Event Collector / Windows Event Forwarder
Event Subscriptions and Channels



What's an Admin to do with all those Logs?

Windows Event Forwarding (WEF) to the rescue!

- Configuration tells an endpoint where to send its logs (Push)
- OR
- Configuration tells an endpoint who is coming for them (Pull)

Pushed out via GPO

Here's an approximate scaling guide for WEF events:

Events/second range	Data store
0 - 5,000	SQL or SEM
5,000 - 50,000	SEM
50,000+	Hadoop/HDInsight/Data Lake



defensiveorigins.com
© Defensive Origins LLC C0330.3 – Threat Optics

Links:

<https://social.technet.microsoft.com/wiki/contents/articles/33895.windows-event-forwarding-survival-guide.aspx>

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

<https://github.com/nsacyber/Event-Forwarding-Guidance>

Windows Event Forwarding

- Push or pull - not both
- Will queue events (size, see next bullet)
- Client buffer is size of windows event log
- Increase buffer by bumping log size
- Delivery timing options are configurable
- IPv4 / IPv6 ready
- Encrypted via Kerberos on domain
- WEF Servers can be HA'd

Deploy via GPO

- Define collector server[s]
- Provide necessary privileges
- Define resource usage (events/sec)



The screenshot displays the Windows Event Forwarding configuration console. It shows the following sections:

- Windows Event Forwarding** (Data collected on: 2/29/2020 10:47:32 AM)
- Computer Configuration (Enabled)**
- Policies**
- Windows Settings**
- Security Settings**
- Local Policies/ User Rights Assignment**
- Restricted Groups**
- Administrative Templates**
- Windows Components/ Event Forwarding**

Policy	Setting	Comment
Configure forwarder resource usage	Enabled	
The maximum forwarding rate (events/ sec) allowed for the forwarder:		
	5	
Configure target Subscription Manager	Enabled	
SubscriptionManagers		
Server=http://dc01.lab.defensiveorigins.com:5985/wsmapi/SubscriptionManager/WEF;Refresh=60		



defensiveorigins.com
© Defensive Origins LLC C0330.4 – Threat Optics

Links:

<https://social.technet.microsoft.com/wiki/contents/articles/33895.windows-event-forwarding-survival-guide.aspx>

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

<https://github.com/nsacyber/Event-Forwarding-Guidance>

Log Forwarding Performance Considerations

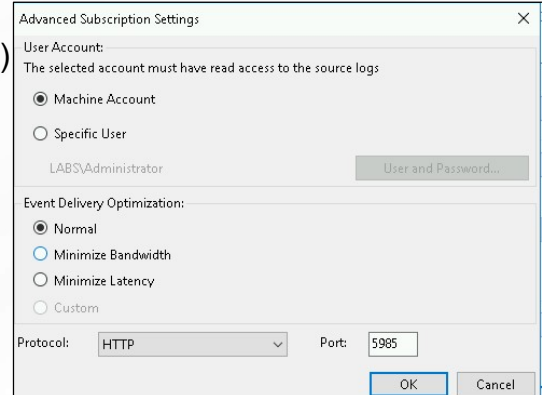
Delivery Optimization (Subscription Parameter)

- Normal
- Minimize Bandwidth
- Minimize Latency

Resource Restrictions

- Events per second

Windows Components/ Event Forwarding	
Policy	Setting
Configure forwarder resource usage	Enabled
The maximum forwarding rate (events/ sec) allowed for the forwarder: 50	



The dialog box 'Advanced Subscription Settings' contains the following configuration:

- User Account:** Machine Account (selected), Specific User (unselected). The text below states: 'The selected account must have read access to the source logs'. The user field is 'LABS\Administrator' and the password field is 'User and Password...'. There is a 'User and Password...' button next to the password field.
- Event Delivery Optimization:** Normal (selected), Minimize Bandwidth (unselected), Minimize Latency (unselected), Custom (unselected).
- Protocol:** HTTP (selected in dropdown), Port: 5985.
- Buttons: OK, Cancel.



defensiveorigins.com
© Defensive Origins LLC C0330.5 – Threat Optics

Links:

<https://support.microsoft.com/en-us/help/4494356/best-practice-eventlog-forwarding-performance>

Who's Listening? The Windows Event Collector (WEC)

Windows Event Collector to the rescue!

Windows remote management is required (quick CLI config below)

```
winrm qc
```

Windows event collector service allows creation and management of event subscriptions

```
wecutil qx
```

Remote systems must also support the WS-Management protocol!



defensiveorigins.com
© Defensive Origins LLC C0330.6 – Threat Optics

Commands:

```
winrm qc  
wecutil qx
```

Links:

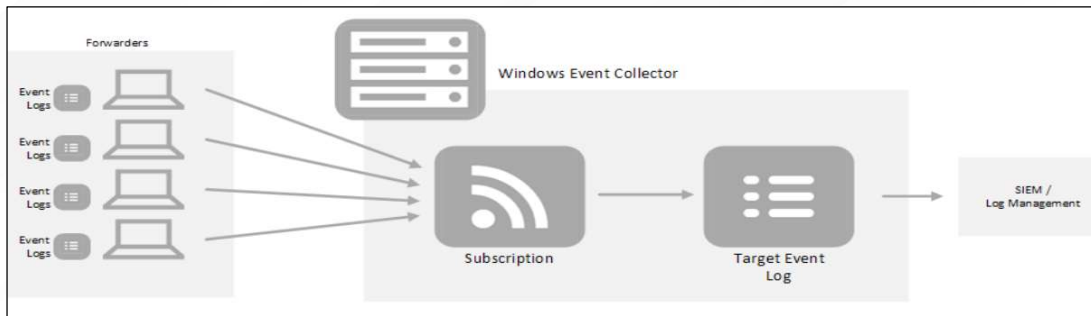
<https://docs.microsoft.com/en-us/windows/win32/wec/windows-event-collector>

Windows Event Collector

Maintains registry stamp of last heartbeat

No more than 10k WEF clients

No more than 10k events/sec (Hadoop? EMR?)



defensiveorigins.com
© Defensive Origins LLC C0330.7 – Threat Optics

Windows Event Collection

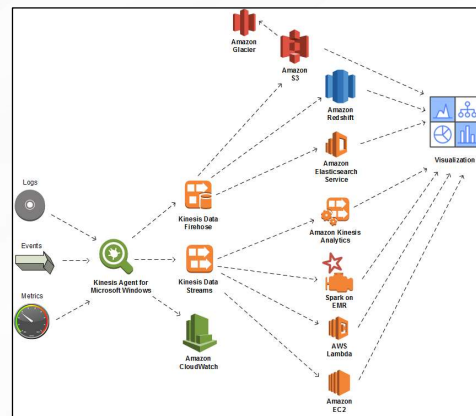
MapReduce on AWS

Relatively Inexpensive and Auto-Scaling Option for Log Ingests

AWS Kinesis Agents

- Amazing data pipelining for almost anything
 - Video and data streams
 - Metric information
 - Logs of all types

Picture here sourced from AWS Kinesis article below.



defensiveorigins.com
© Defensive Origins LLC C0330.8 – Threat Optics

Links:

<https://aws.amazon.com/blogs/big-data/collect-parse-transform-and-stream-windows-events-logs-and-metrics-using-amazon-kinesis-agent-for-microsoft-windows/>

<https://docs.aws.amazon.com/kinesis-agent-windows/latest/userguide/directory-source-to-s3-tutorial.html>

Windows Event Collection

Three considerations to achieve maximum numbers.

- Disk I/Ops
- Resilient network infrastructure
- Registry size (lifetime subscription numbers below)
 - >1,000 subscriptions event viewer will slow down noticeably
 - >50,000 subscriptions event viewer is no longer an option (wecutil.exe instead)
 - >100,000 subscriptions registry becomes unreadable



defensiveorigins.com
© Defensive Origins LLC C0330.9 – Threat Optics

Windows Event Collection Configuration

Two commands on the collector.

- **winrm qc** - remote management quick config
- **wecutil qc** - event collector utility (or pre-deploy winrm via GPO)

```
C:\Users\itadmin>winrm qc
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.
C:\Users\itadmin>
C:\Users\itadmin>wecutil qc
The service startup mode will be changed to Delay-Start. Would you like to proceed ( Y- yes or N- no)?y
Windows Event Collector service was configured successfully.
```

```
winrm qc
```

```
wecutil qc
```



defensiveorigins.com
© Defensive Origins LLC C0330.10 – Threat Optics

Commands:

```
Winrm qc
wecutil qc
```

Working with Event Subscriptions

Security Insight Baselines – Optics Configurations

Audit Policy – Which events on the domain are we going to capture?

Windows Event Forwarding Configuration

- Baseline WEF config on all systems
- Suspect WEF config on targeted / high risk systems

Subscriptions then define the following:

- Event IDs grouped in meaningful ways (example on next slide) we wish to collect
- Source computer groups

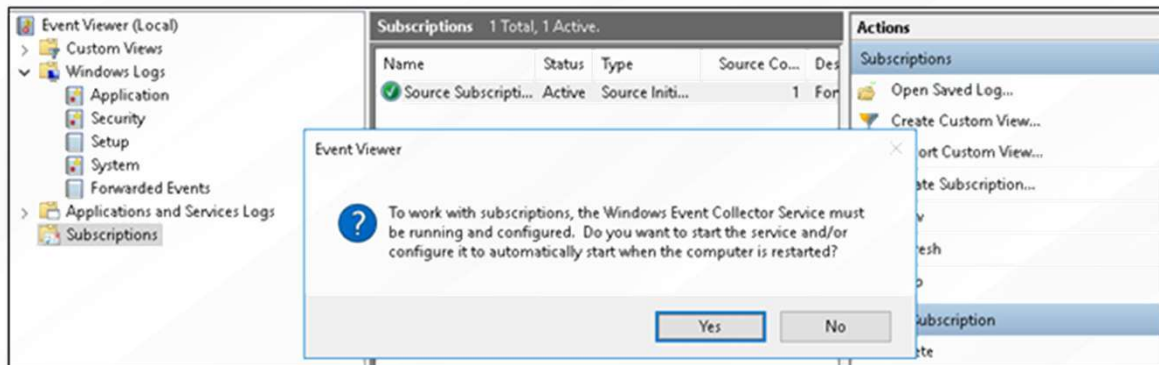


defensiveorigins.com
© Defensive Origins LLC C0330.11 – Threat Optics

Windows Event Collection - Event Subscriptions

From the Event Viewer window, right (alternate) click on **Subscriptions** and click to **Create Subscription...**

Subscription = Channel = Related Events \leftrightarrow Xpath Query



defensiveorigins.com
© Defensive Origins LLC C0330.12 – Threat Optics

Xpath Query: Privilege Group Adds

Grouping event IDs in meaningful ways.

- Event ID 4728: Member added to security enabled global group
- 4732: Member added to security enabled local group
- 4756: Member added to security enabled universal group
- 4735: Security enabled local group was changed

Thus **4728 or 4732 or 4756 and 4735** == An important group type was changed

Additional filters maybe? Tune out noise and focus efforts.

- Group = domain admins / server admins / desktop admins



defensiveorigins.com
© Defensive Origins LLC C0330.13 – Threat Optics

Working with Event Subscriptions

Grouping event IDs in meaningful ways.

This XML filter, when applied to a subscription:

- Called an "XPath query" and can be constructed as a custom event log "view"
- Check the security logs for 4728 **or** 4732 **or** 4756 **and** 4735
- This one identifies users added to privileged groups

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*[System[Provider[@Name='Microsoft-Windows-Security-
    Auditing'] and (EventID=4728 or EventID=4732 or EventID=4756)]]</Select>
    <Select Path="Security">*[System[Provider[@Name='Microsoft-Windows-Security-
    Auditing'] and EventID=4735]]</Select>
  </Query>
</QueryList>
```



defensiveorigins.com
© Defensive Origins LLC C0330.14 – Threat Optics

Working with Event Subscriptions Security Insight Baselines

You want event subscription xml templates?
The NSA has your subscriptions XMLs linked here.

- NSA Cyber's guidance (IADGov)
- Account Lockouts
- Problems with Defender
- Group Policy Errors
- USB Drives Plugged In
- Users Added to Privileged Groups
- Problems with Windows Updates
- Each of these is just an XPath query

This is just a baseline.



defensiveorigins.com
© Defensive Origins LLC C0330.15 – Threat Optics

AccountLocked.xml	initial commit of Event Forwarding scripts
AccountLogons.xml	initial commit of Event Forwarding scripts
AppCrash.xml	initial commit of Event Forwarding scripts
BsodErr.xml	initial commit of Event Forwarding scripts
DefenderErr.xml	Fixed crucial spelling error in DefenderErr.xml query
EMETLogs.xml	initial commit of Event Forwarding scripts
ExpCredits.xml	initial commit of Event Forwarding scripts
GrpPolicyErr.xml	initial commit of Event Forwarding scripts
KernelDriverDetect.xml	initial commit of Event Forwarding scripts
LogDel.xml	initial commit of Event Forwarding scripts
MsiPackages.xml	initial commit of Event Forwarding scripts
PrintDetect.xml	initial commit of Event Forwarding scripts
ServiceManager.xml	Fix: Corrected invalid level
USBDetection.xml	initial commit of Event Forwarding scripts
UserToPriv.xml	initial commit of Event Forwarding scripts
WhitelistingLogs.xml	initial commit of Event Forwarding scripts
WifiActivity.xml	Fix bug in Wi-Fi security & authentication status XPath queries
WinFAS.xml	initial commit of Event Forwarding scripts
WinUpdateErr.xml	initial commit of Event Forwarding scripts

Links:

<https://github.com/palantir/windows-event-forwarding>

<https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Subscriptions/NT6>

The Palantir Event Handling Repo Security Insight Baselines

Palantir also has an awesome repo on Github!

Name	Date modified	Type	Size
AutorunsToWinEventLog	6/21/2020 4:56 PM	File folder	
group-policy-objects	6/21/2020 4:56 PM	File folder	
wef-subscriptions	6/21/2020 4:56 PM	File folder	
windows-event-channels	6/21/2020 4:56 PM	File folder	
.gitignore	6/21/2020 4:56 PM	GITIGNORE File	5 KB
LICENSE.md	6/21/2020 4:56 PM	MD File	2 KB
README.md	6/21/2020 4:56 PM	MD File	8 KB
WEF-Event-Mappings.md	6/21/2020 4:56 PM	MD File	47 KB



defensiveorigins.com
© Defensive Origins LLC C0330.16 – Threat Optics

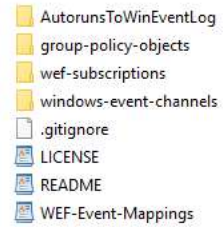
Links:

<https://github.com/palantir/windows-event-forwarding>

<https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Subscriptions/NT6>

The Palantir Event Handling Repo Security Insight Baselines

The repo is structured in this manner



The wef-subscriptions container has 51 xpath queries for related events.

```
<Query>
  <![CDATA[
    <QueryList>
      <!-- Inspired by Microsoft Documentation and/or IADGOV -->
      <Query Id="0" Path="Security">
        <!-- For Domain Accounts event is created on DC-->
        <!-- For Local Accounts event is created locally-->
        <!-- 4740: Account Lockouts -->
        <Select Path="Security"> *[System[Provider[@Name='Microsoft-Windows-S...
      </Query>
    </QueryList>
  ]]>
```



defensiveorigins.com
© Defensive Origins LLC C0330.17 – Threat Optics

Links:

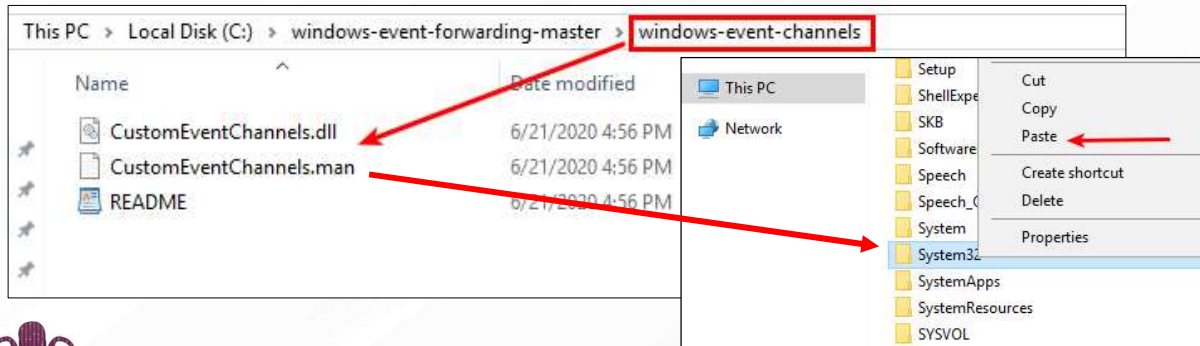
<https://github.com/palantir/windows-event-forwarding>

<https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Subscriptions/NT6>

The Palantir Event Handling Repo

Order of Operations Step 1.

The windows-event-channels directory has the pre-configured event channels files. These files need to be dropped in c:\Windows\system32\



defensiveorigins.com
© Defensive Origins LLC C0330.18 – Threat Optics

Links:

<https://github.com/palantir/windows-event-forwarding>

<https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Subscriptions/NT6>

The Palantir Event Handling Repo

Order of Operations Step 2.

The windows-event-channels directory has the pre-configured event channels files. These files need to be dropped in c:\Windows\system32\

The following commands then deploy the new event channels:

```
net stop wecsvc
(stop event collector service)

wevtutil um C:\windows\system32\CustomEventChannels.man
(unloads manifest)

wevtutil im C:\windows\system32\CustomEventChannels.man
(imports manifest)
```



defensiveorigins.com
© Defensive Origins LLC C0330.19 – Threat Optics

Commands

```
net stop wecsvc
wevtutil um C:\windows\system32\CustomEventChannels.man
wevtutil im C:\windows\system32\CustomEventChannels.man
```

Links:

<https://github.com/palantir/windows-event-forwarding>

<https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Subscriptions/NT6>

The Palantir Event Handling Repo

Order of Operations Step 3.

The windows-event-channels directory has the pre-configured event channels files. These files need to be dropped in c:\Windows\system32\. The following commands then deploy the new event channels. And, finally, resize them.

From a PS prompt:

```
$xml = wevtutil el | select-string -pattern "WEC"  
foreach ($subscription in $xml) {  
    wevtutil sl $subscription /ms:4194304  
}
```

Restart the wec service (wecsvc) from the CMD prompt or services console.



defensiveorigins.com
© Defensive Origins LLC C0330.20 – Threat Optics

Commands:

```
$xml = wevtutil el | select-string -pattern "WEC"  
foreach ($subscription in $xml) {  
    wevtutil sl $subscription /ms:4194304  
}
```

Links:

<https://github.com/palantir/windows-event-forwarding>

<https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Subscriptions/NT6>

The Palantir Event Handling Repo Order of Operations Step 4.

Once we're satisfied with our subscription container configuration, per the repo's instructions, a quick for loop will install these subscriptions.

From a CMD prompt:

```
net stop wecsvc
for /r %i in (*.xml) do wecutil cs %i
net start wecsvc
```



defensiveorigins.com
© Defensive Origins LLC C0330.21 – Threat Optics

Subscriptions 51 Total, 51 Inactive.			
Name	Status	Type	
Account-Lockout	Inactive	Source Initiated	
Account-Manag...	Inactive	Source Initiated	
Active-Directory	Inactive	Source Initiated	
ADFS	Inactive	Source Initiated	
Application-Cras...	Inactive	Source Initiated	
Applocker	Inactive	Source Initiated	
Authentication	Inactive	Source Initiated	
Autoruns	Inactive	Source Initiated	
Bits-Client	Inactive	Source Initiated	
Certificate-Auth...	Inactive	Source Initiated	
Code-Integrity	Inactive	Source Initiated	
Device-Guard	Inactive	Source Initiated	
DNS	Inactive	Source Initiated	
Drivers	Inactive	Source Initiated	
Duo-Security	Inactive	Source Initiated	
EMET	Inactive	Source Initiated	
Event-Log-Diagn...	Inactive	Source Initiated	
Explicit-Credenti...	Inactive	Source Initiated	

Commands:

```
net stop wecsvc
for /r %i in (*.xml) do wecutil cs %i
net start wecsvc
```

Working with Event Subscriptions Audit Policy

Microsoft recommends the following:

- Anti-Malware
- Process Creation
- Registry Changes
- OS Startup / Shutdown
- Service Installs
- CA Audit Events
- User Profile Events
- Service Start / Failure
- Network Share Events (*sans* IPC\$ events)
- RDS Session Events
- EMET Events

...and so much more...**as a baseline**...plus the "suspect system/server" baselines

A Few Important Event IDs

4624 and 4634 (Logon / Logoff)
4662 (ACL'd object access - Audit req.)
4688 (process launch and usage)
4698 and 4702 (tasks + XML)
4740 and 4625 (Acct Lockout + Src IP)
5152, 5154, 5156, 5157 (FW - Noisy)
4648, 4672, 4673 (Special Privileges)
4769, 4771 (Kerberoasting)
5140 with *\IPC\$ and so many more....



defensiveorigins.com
© Defensive Origins LLC C0330.22 – Threat Optics

Links:

<https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-sept2019update-for-windows-10-v1903-and/ba-p/890940>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings>

RECAP.

Sysmon. Configure Auditing. Enable WEC. Deploy WEF. Deploy Event Subscriptions.

Enable Windows Collection

- Plan appropriately for scaling

Plan, configure, and deploy Audit Policies

- This is critical to the success of this project
- You cannot see that which you do not audit

Deploy Windows Event Forwarding configuration

- Use GPO to configure security privileges for event log reading by network service
- And to define the Windows Event Collector's destination URL

Configure Event Subscriptions

- Group event IDs in meaningful ways and create a subscription



defensiveorigins.com
© Defensive Origins LLC C0330.23 – Threat Optics



----- LAB -----



L0330

Configuring Event Collection
Configuring Event Forwarding
<20 Minutes

----- LAB -----



defensiveorigins.com
© Defensive Origins LLC C0330.24 – Threat Optics

Applied Purple Teaming – L0330 Configuring Event Collection & Forwarding 20 Minutes