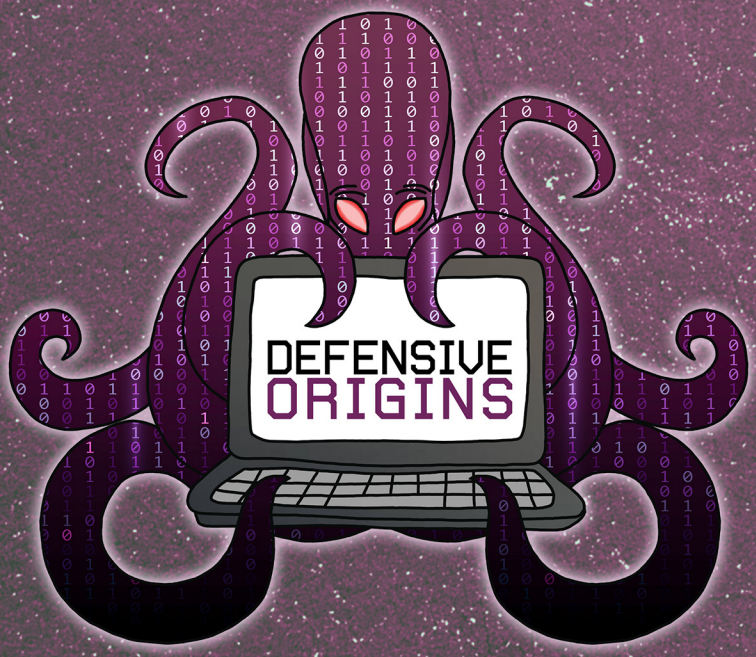
APPLIED PURPLE TEAMING

by jordan drysdale & kent ickler



Applied Purple Teaming: Infrastructure, Threat Optics, and Continuous Improvement

Are Excerpts From

Atomic Purple Teaming

First Edition

Printed in the United States of America

Defensive Origins LLC

ISBN 978-0-578-65979-4

Library of Congress Control Number: 2020904534

Defensive Origins LLC
Rapid City, SD 57702
https://www.defensiveorigins.com
info@defensiveorigins.com

Authors: Jordan Drysdale, Kent Ickler

Atomic Purple Teaming

Applied Purple Teaming (June 2020)

Applied Purple Teaming

Infrastructure, Threat Optics, and Continuous Improvement

June 6, 2020

C0100

Course Interview and Overview

Instructors

Jordan Drysdale
@Rev10D

Kent Ickler
@Krelkci

Course Objectives

- Implement Sysmon with the modular configuration
- Configure and launch meaningful audit policies
- Deploy the WEF / WEC model of event collection
- Install and configure WinLogBeat
- The Hunting ELK (HELK) Docker-based Elastic install
- Catch some basic command line execution
- Bonus: Build a Continuous Improvement Purple Team Environment

Course Components

- C0100-1: Course Introduction
- C0300-1: Event Baselines and Sysmon
- C0320-1: Event Handlers and Subscriptions
- C0330-1: Log Shipping and Event Ingests
- C0150-1: Purple Team Lifecycle / Continuous Improvement

- Course Git Repo: https://github.com/DefensiveOrigins/APT06202001

Have everything?

- Lab Environment (Optional!)
- Applied Purple Team Courseware (Git Repo!)

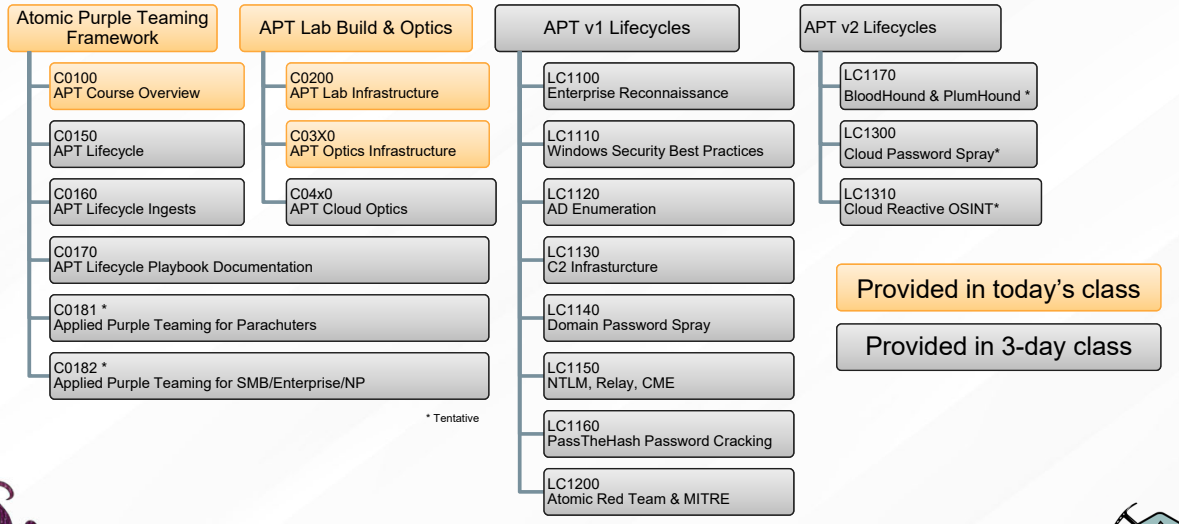
https://github.com/DefensiveOrigins/APT06202001

Course Information

- 4-5 Hours
- Breaks will be announced, approximately hourly.
- Course Git Repo

https://github.com/DefensiveOrigins/APT06202001

Applied Purple Teaming Course Matrix



Applied Purple Teaming Full (3-Day) Course

3 Day Session

- Tue, June 30 – 10:30 a.m. to 5 p.m. EST
- Wed, July 1 – 11:30 a.m. to 5 p.m. EST
- Thu, July 2 – 11:30 a.m. to 5 p.m. EST

Instructors: Kent Ickler & Jordan Drysdale

Price: $395

Scholarships available and will be discussed at the end of todays session.

- Three days of fast-paced interactive learning
- Continuous security hardening framework (Applied Purple Teaming)
- APT for Parachuters, SMB, Enterprise, and NP
- Discussion of Design and implementation network optics and logging
- A Review of Enterprise OSINT Awareness
- Active Directory Best Practices for Securing your Environment
- Interactive Exercises (Labs)
- Plan, Attack, Defend, Hunt, Document Lifecycle-Driven Methodology
- Live-fire attack tactics such as SMB/NTLM Relay, Command and Control, and BloodHound!
- Life hunt-detection methodology using Logstash, Elasticsearch, and Kibana!
- Implementation of continuous security improvement by leveraging MITRE ATT&CK
- Integration of the Atomic Red Team framework in Purple Teaming exercises
- Defensive Origins Hosted Lab Environment
- 6 Months of BHIS AntiSiphon Cyber Range Included!

https://wildwesthackinfest.com/online-training/applied-purple-teaming/

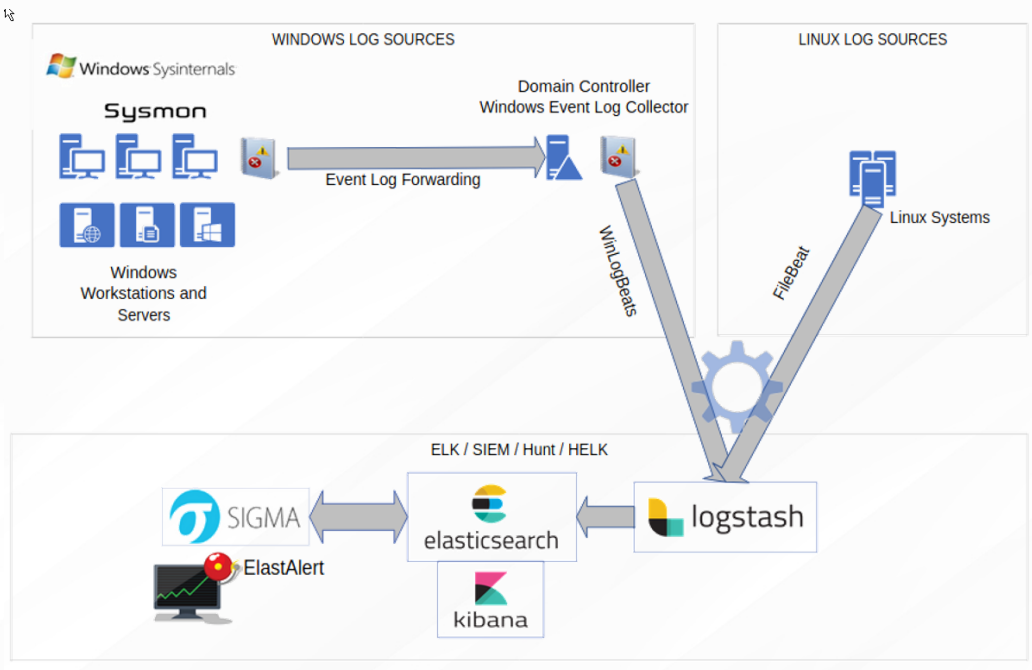
Applied Purple Teaming

Infrastructure, Threat Optics, and Continuous Improvement

June 6, 2020

LC0310

Endpoint Optics
Sysmon
Audit Policy



Sysmon – Assisting with Endpoint Logging

Biased opinion: Sysmon is the best free endpoint logging tool available.
Nuanced opinion: Sysmon can create a lot of noise.
Sysmon-modular: A configurable way to help parse and limit the noise.

- Also, as seen below, can help map events to MITRE techniques

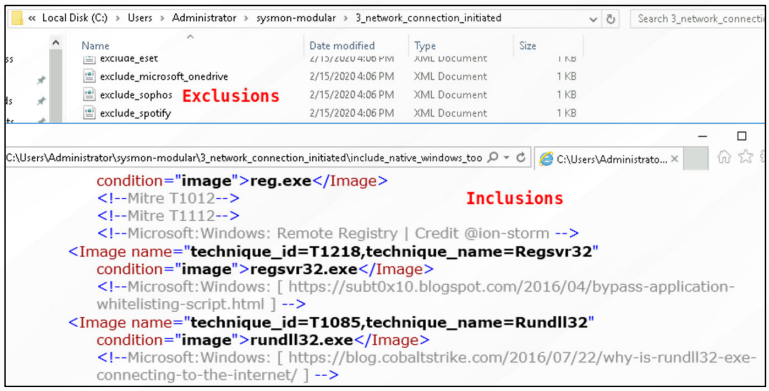
Sysmon v11.0

04/28/2020 • 13 minutes to read •

By Mark Russinovich and Thomas Garnier

Published: April 28, 2020

https://github.com/olafhartong/sysmon-modular
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

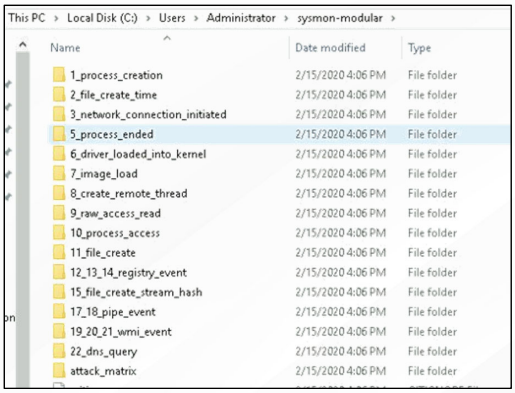


Sysmon – Assisting with Endpoint Logging

Create a configuration file using the sysmon-modular repository.
The containers to the right include configurable options.

The process below generates a custom config file for Sysmon.

- Parses directories as listed for includes/excludes
- It can be adjusted and re-installed easily




```
PS C:\Users\Administrator> cd .\sysmon-modular\
PS C:\Users\Administrator\sysmon-modular> Import-Module .\Merge-SysmonXml.ps1
PS C:\Users\Administrator\sysmon-modular> Merge-AllSysmonXml -Path ( Get-ChildItem '[0-9]*\*.xml') -AsString
  | Out-File sysmonconfig.xml
```

https://github.com/olafhartong/sysmon-modular

Sysmon – Assisting with Endpoint Logging

The install process is easy.

sysmon64.exe -accepteula -i sysmonconfig.xml

```
Z:\lab.defensiveorigins.com\CourseWare\Sysmon>sysmon64.exe -accepteula -i sysmonconfig.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.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
Z:\lab.defensiveorigins.com\CourseWare\Sysmon>
```

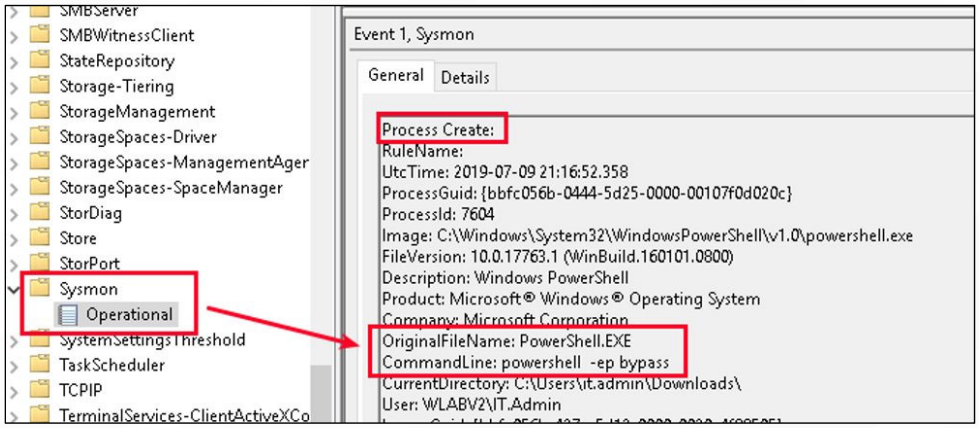
The config update process is easy too.
Update the config directory from the previous slide in accordance with lifecycle changes.
Re-generate the sysmonconfig.xml with the modular tool.

sysmon.exe -c sysmonconfig-update.xml

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon – Assisting with Endpoint Logging

Catches things accurately.

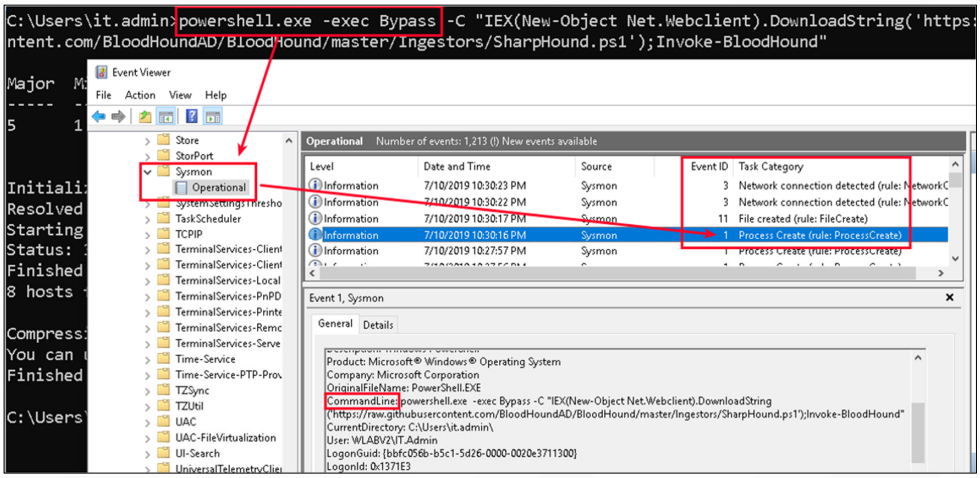


https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon – Assisting with Endpoint Logging

Catches things accurately.

https://github.com/olafhartong/sysmon-modular



Windows Audits the CLI and PowerShell Natively, Right?

Wrong.

Domain controllers? Nope.

Workstations? Nope.

Anything? Nope.

https://github.com/olafhartong/sysmon-modular

Audit Policy

The command prompt way.

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

```
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
```

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

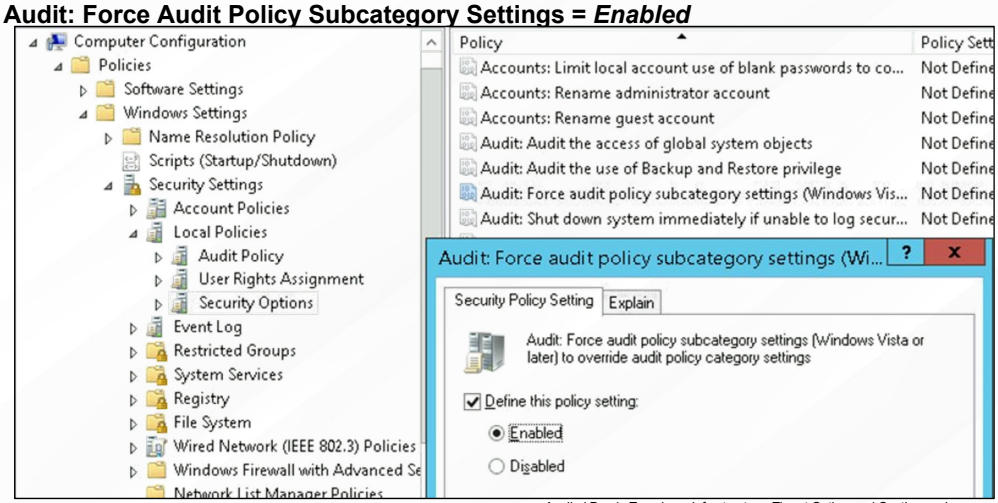
Yeah, and one last thing: The second setting may be overwritten.

> 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.

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***



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
```

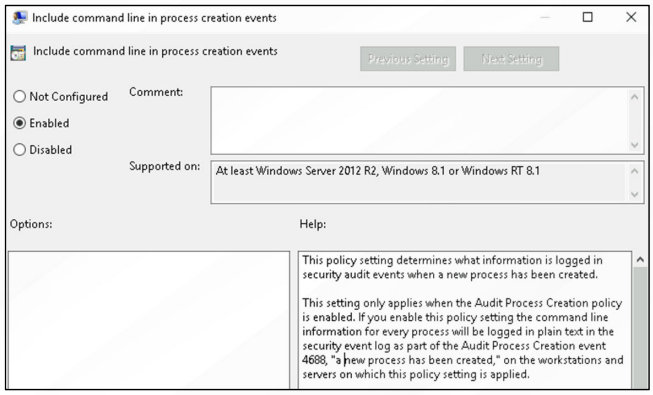
Can also configure the following via command line options.

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

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

The Group Policy way to turn on PowerShell auditing:

Policies > Admin Templates > System > Audit Process Creation



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)

Windows Event Collection
What About IIS Logging?

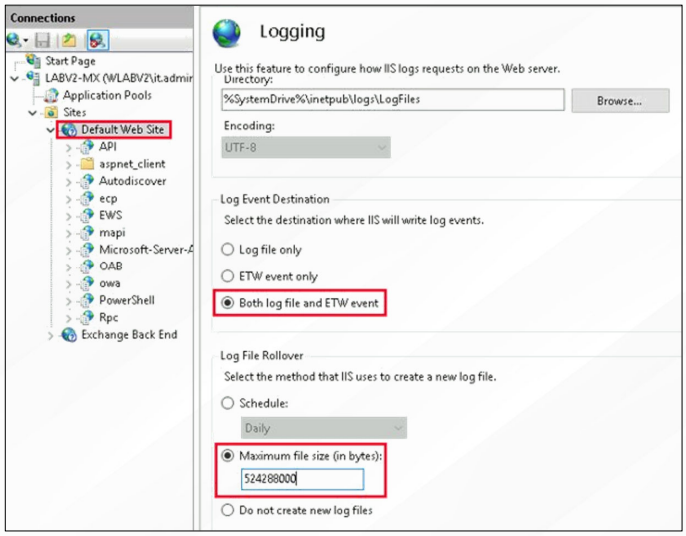
Yeah, that's not on by default either.
LogFiles (text) written by default…
Nothing to event log.

Enable:

- Both log file and ETW event
- Maximum file size

And then you can catch:

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



Windows Event Collection - Making Sense Out of it All.

1. Sysmon can help, a lot. This is not a silver bullet, nothing is.
2. Command line auditing should be configured to capture process creation events.
3. PowerShell module logging and transcription should be configured via Group Policy.
4. IIS doesn't log to Event Viewer without configuration.
5. Logging and auditing can be a challenge, and we're up to the task.

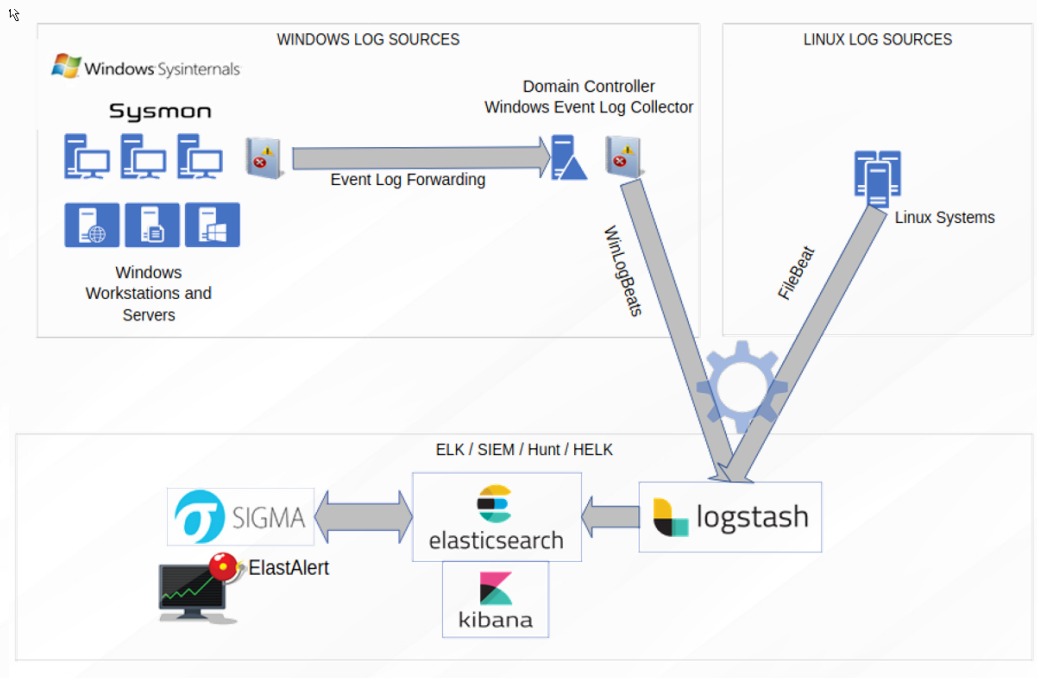
Applied Purple Teaming

Infrastructure, Threat Optics, and Continuous Improvement

June 6, 2020

LC0320

Event Handlers
WEC / WEF
Event Subscriptions



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

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

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)

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

Policy	Setting
Manage auditing and security log	NT AUTHORITY\ NETWORK SERVICE

Restricted Groups

Group	Members	Member of
BUILTIN\ Event Log Readers	NT AUTHORITY\ NETWORK SERVICE	

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/ Event Forwarding

Policy	Setting	Comment
Configure forwarder resource usage	Enabled	
The maximum forwarding rate (events/ sec) allowed for the forwarder:	5	

Policy	Setting	Comment
Configure target Subscription Manager	Enabled	

SubscriptionManagers
Server=http:// dc01.lab.defensiveorigins.com:5985/ wsman/ SubscriptionManager/ WEC,Refresh=60

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

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 qc

Remote systems must also support the WS-Management protocol!

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

Log Forwarding Performance Considerations

- Frequency of connections **(Refresh)**
- Number of subscriptions
- Number of clients
- Operating system of the clients

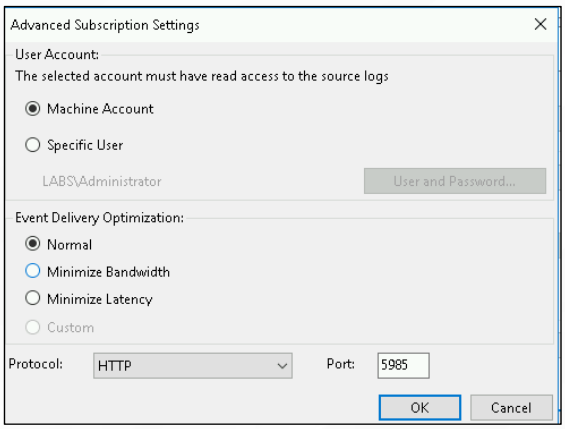
Policy	Setting	Comment
Configure target Subscription Manager	Enabled	
SubscriptionManagers		
Server=http://dc01.lab.defensiveorigins.com:5985/wsman/SubscriptionManager/WEC,Refresh=60		

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

Log Forwarding Performance Considerations

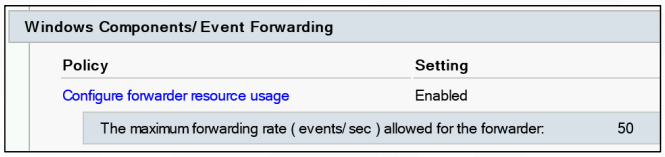
Delivery Optimization (Subscription Parameter)

- Normal
- Minimize Bandwidth
- Minimize Latency



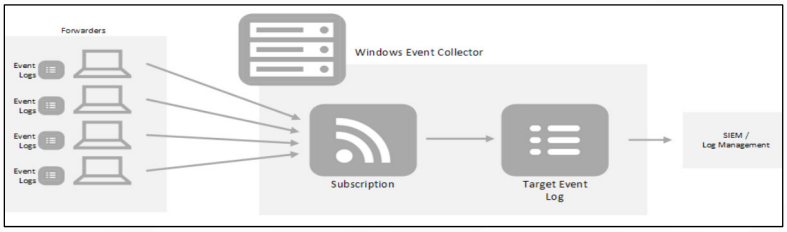
Resource Restrictions

- Events per second



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

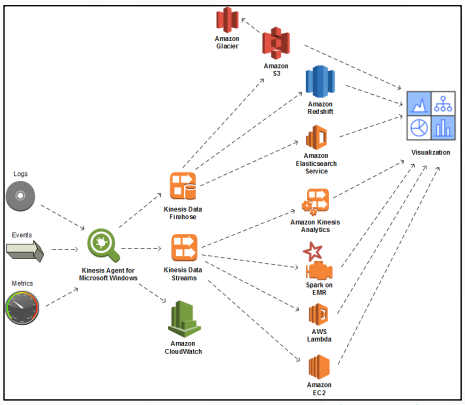
Windows Event Collection



Maintains registry stamp of last heartbeat
No more than 10k WEF clients
No more than 10k events/sec (remember EMR?)

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.**

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

Windows Event Collection

Two commands on the collector.

- **winrm qc** (remote mgmt quick config)
- **wecutil qc** (event collector utility)

(or pre-deploy winrm via GPO)

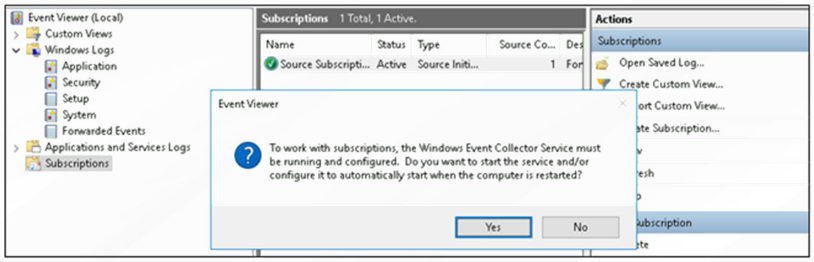
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>winrm qc
WinRM service is already running on this machine.
WinRM is already set up for remote management on this comput
C:\Users\Administrator>
```

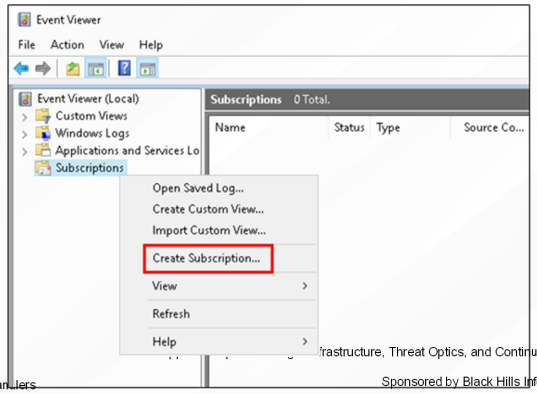
```
C:\Users\Administrator>wecutil qc
The service startup mode will be changed to Delay-Start.
   Would you like to proceed ( Y- yes or N- no)?Y
Windows Event Collector service was configured successfully.
```

Windows Event Collection

If prompted, as seen here, click **Yes.**



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



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

Event Channels

Or, just "channels"
Event channel = log bucket

Working with Event Subscriptions

Grouping event IDs in meaningful ways.
This XML filter, when applied to a subscription:

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

```
<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>
```

https://github.com/palantir/windows-event-forwarding
https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Subscriptions/NT6

Working with Event Subscriptions
Security Insight Baselines

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

- 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
- Palantir's Event Baselines are used for APT lab

<u>This is just a baseline.</u>

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
ExpCreds.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

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….

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-sept2019update-for-windows-10-v1903-and/ba-p/890940

Working with Event Subscriptions
Audit Policy

You must have Audit Process Creation auditing enabled
You must enable the policy setting:

- Include command line in process creation events

> "When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings." (cit. *MSFT, see links)

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://github.com/MotiBa/Sysmon/
https://github.com/SwiftOnSecurity/sysmon-config
https://www.malwarearchaeology.com/cheat-sheets
https://adsecurity.org/?p=3458
http://www.stuffithoughtiknew.com/2019/02/detecting-bloodhound.html

Working with Event Subscriptions
Audit Policy Baselines

Y

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://github.com/MotiBa/Sysmon/
https://github.com/SwiftOnSecurity/sysmon-config
https://www.malwarearchaeology.com/cheat-sheets
https://adsecurity.org/?p=3458
http://www.stuffithoughtiknew.com/2019/02/detecting-bloodhound.html

RECAP.

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

Enable Windows Collection
- Plan appropriately for scaling

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

Plan, configure, and deploy Audit Policies
- This is critical to the success of this project
- You cannot see that which you do not audit

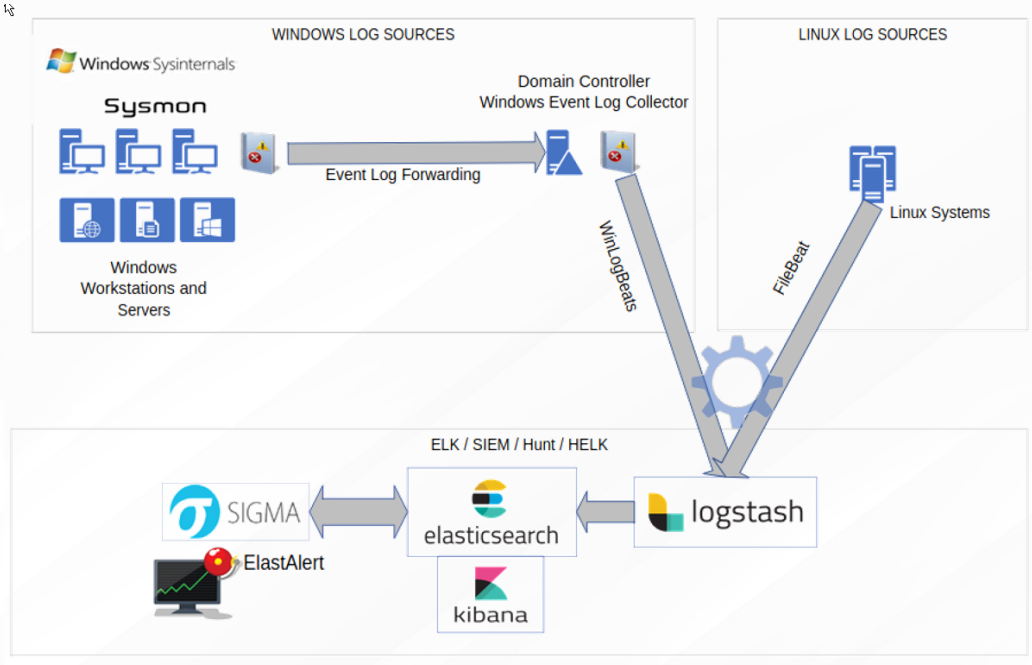
Applied Purple Teaming

Infrastructure, Threat Optics, and Continuous Improvement

June 6, 2020

LC0330

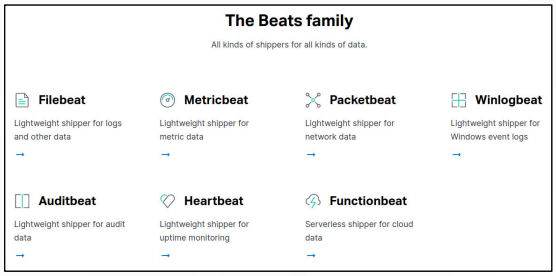
Log Shipping Event Ingestors



Beats (by Elastic)

"Lightweight Data Shippers for Everything"
Installing WinLogBeat is relatively easy.

- Pick your Beats flavor
- Configure the yaml file (to the right)
- Install on your platform
  - Windows
  - Linux
  - Router / Firewall / Network
  - App Servers
  - Web Servers




```
#================== Winlogbeat specific options =================
winlogbeat.event_logs:
  - name: Application
    ignore_older: 30m
  - name: Security
    ignore_older: 30m
  - name: System
    ignore_older: 30m
  - name: Microsoft-windows-sysmon/operational
    ignore_older: 30m
  - name: Microsoft-windows-PowerShell/Operational
    ignore_older: 30m
    event_id: 4103, 4104
  - name: Windows PowerShell
    event_id: 400,600
    ignore_older: 30m
  - name: ForwardedEvents
    ignore_older: 30m
  - name: Microsoft-Windows-WMI-Activity/Operational
    event_id: 5857,5858,5859,5860,5861

#-------------------- Logstash output -------------------
output.logstash:
  # The Logstash hosts
  hosts: ["elk.lab.defensiveorigins.com:5044"]
```


Beats (by Elastic)

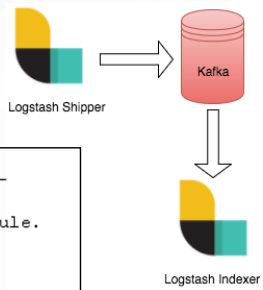
```
#----------------- Kafka output ---┼-------------------
#output.kafka:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # The list of Kafka broker addresses from which to fetch the
cluster metadata.
  # The cluster metadata contain the actual Kafka brokers events
are published
  # to
  #hosts: ["localhost:9092"]
```

Configuring Beats for Your Environment – the WinLogBeats config file.

Pick your remote ingestor:

- **Elastisearch** can consume logs directly or accept either of the following
- **Logstash** is a collector, parser, and transformer of logs
- **Kafka** is a "publish-subscribe-topic" or "an event broker"
  - Can sit in between Logstash and *Logstash?*
- **Redis**
- **File output**...



And....configure it.

```
#----------------- File output ---------┼------------
#output.file:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # Configure JSON encoding
  #codec.json:
    # Pretty-print JSON event
    #pretty: false
```

Beats (by Elastic) - Logstash Ingest for Elastic Stack

APT lab utilizes Logstash (two lines of config)

Your environment will differ.
Splunk – Universal Forwarder
ManageEngine – Syslog Relay Tool
ArcSight – Smart Connector and Logger Management
AlienVault – USM Anywhere Sensor
Et cetera, et cetera.

There are like 3,000 commercial solutions as of the date of writing.

```
#-------------------- Logstash output -------------------
output.logstash:
  # The Logstash hosts
  hosts: ["elk.lab.defensiveorigins.com:5044"]
```

Beats (by Elastic)

Installing WinLogBeat is relatively easy (Windows install below)

- **powershell -Exec bypass -File .\install-service-winlogbeat.ps1**
- **Set-Service -Name "winlogbeat" -StartupType automatic**
- **Start-Service -Name "winlogbeat"**
- **Get-Service winlogbeat**

```
C:\Users\...\winlogbeat-7.5.1-windows-x86_64>powershell -ep bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\...\winlogbeat-7.5.1-windows-x86_64> powershell -Exec bypass -File .\install-service-winlogbeat.ps1

Status   Name               DisplayName
------   ----               -----------
Stopped  winlogbeat         winlogbeat

PS C:\Users\...\winlogbeat-7.5.1-windows-x86_64> Set-Service -Name "winlogbeat" -StartupType automatic
PS C:\Users\...\winlogbeat-7.5.1-windows-x86_64> Start-Service -Name "winlogbeat"
PS C:\Users\...\winlogbeat-7.5.1-windows-x86_64> Get-Service winlogbeat

Status   Name               DisplayName
------   ----               -----------
Running  winlogbeat         winlogbeat
```

RECAP.

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

Enable Windows Collection
- Plan appropriately for scaling

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

Plan, configure, and deploy Audit Policies
- This is critical to the success of this project
- You cannot see that which you do not audit

Install the log shipper on the Windows Event Collector
- Configure WinLogBeat to ship to your SIEM / Logging Tool / Cloud Destination / Third-Party / Wherever

Applied Purple Teaming

Infrastructure, Threat Optics, and Continuous Improvement

June 6, 2020

C0120
C0150

Atomic Purple Team
APT Lifecycle Lifecyle

Ok, NIST? Blue Team.

- Responsible for **defending** an enterprise's use of information systems by maintaining its security posture…
- **Identifies** security threats and risks in the operating environment, **analyzes** the network environment and its current state of security readiness.
- **Provides recommendations** … to increase the customer's cyber security readiness posture.

https://csrc.nist.gov/Glossary/Term/Red-Team-Blue-Team-Approach

Ok, NIST? Red Team.

- **Emulate** a potential adversary's **attack** or **exploitation**
- Improve enterprise Information Assurance by **demonstrating the impacts** of successful attacks
- **Demonstrating** what works for the defenders

https://csrc.nist.gov/Glossary/Term/Red-Team-Blue-Team-Approach

https://csrc.nist.gov/Glossary/Term/Red-Team-Blue-Team-Approach

Red Team, Blue Team, Purple Team

- Red Team: Offense. Attack. Pillage.
- Blue Team: Defense. Block. Build.

- Purple Team: Collaboration of Red and Blue Teams.
  - Attack, Defend, Pillage, Build.
  - Use both Blue Team and Red Team tactics to increase efficiency of Security Posture improvement programs.

Who/What is APT? Where does it fit?

- Some organizations have Blue and Red Teams.
- Some organizations have just Blue, or Red teams.
- Some organizations have neither Blue or Red teams…
- Consider Network Analysts and a Help Desk.
- MSP's, MSSP's

The **Purple Team** can be an independent team, multiple teams, a few employees, or single employee; It works best as a team of **collaborative effort** from **Information Security** related departments and roles.

It can fall under Information Security, Information Technology, or cross organizational unit to leverage collaborative effort..

Applied Purple Teaming

What does an APT accomplish?

- Build a more secure business infrastructure
- Align Information Technology infrastructure to best practices
- Keep businesses protected by monitoring current threats
- Assess risk and threats of vulnerabilities
- Build and implement effective defenses and alerting methods

Applied Purple Team & Production - Lifecycle

The APT does not operate in production environments.

- Lab Environment used to test attacks, test defenses, test changes.

The goal of APT is to:

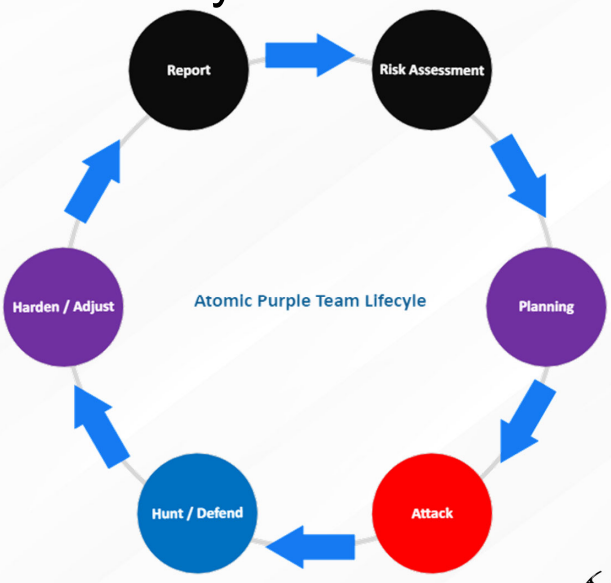
- Produce proven methods to defeat attacks
- Identify/alert threats
- Continually improve the security posture of the organization

DO NOT TEST IN PRODUCTION.

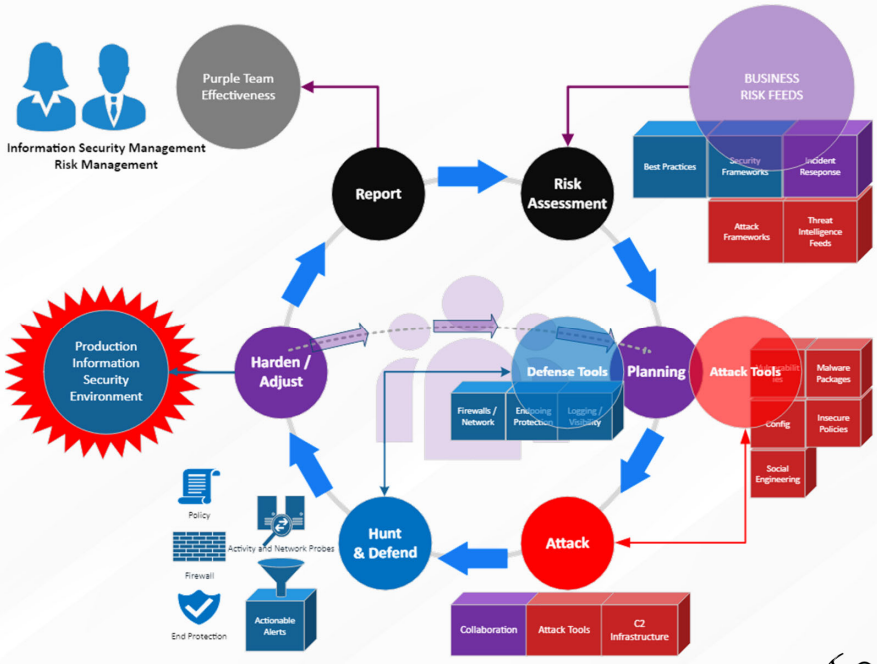
APT produces proven methodologies with empirical evidence for production Change Management by testing in a lab/simulated environment!

Applied (Atomic) Purple Team Lifecycle

1. Risk and Threat Assessment (Attack Ingest)
2. Planning
3. Attack Execution / Simulation
4. Detection / Build Defenses
5. Optimize / Harden / Adjust
6. Report



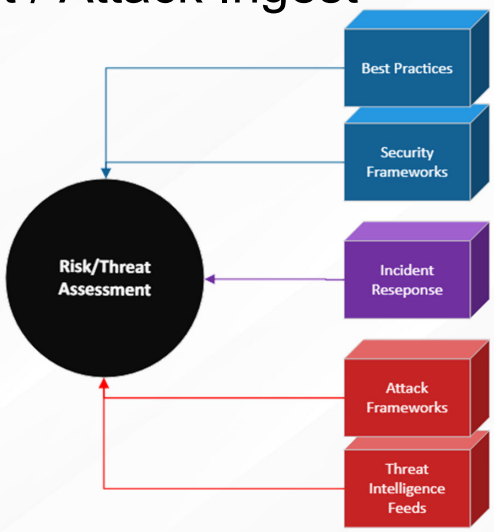
APTLC Big (Macro) Picture



1. Risk and Threat Assessment / Attack Ingest

Goal: Find an attack.
Goal: Determine if defending and/or hunting
How: Use an ingest:

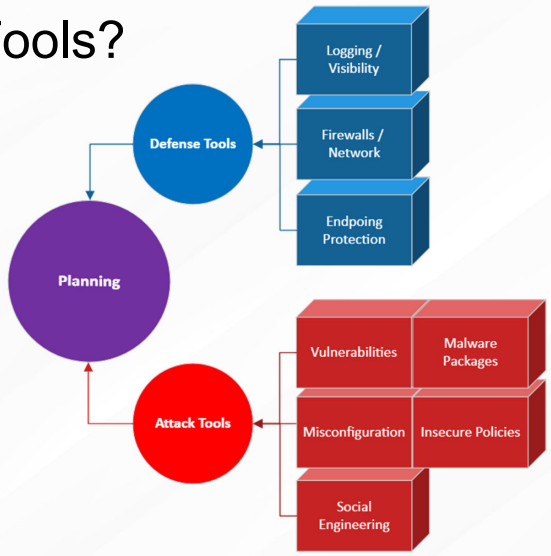
- Best Practices (audit)
- Security Framework
- Current Events
- Incident Response
- Threat Intelligence
- etc.



2. Planning – What are the Tools?

Goal: Identify the Attack Tools
Goal: Identify the Defense Tools

How:
- Provided by Threat Assessment
- Research
- New tools?? Great!!

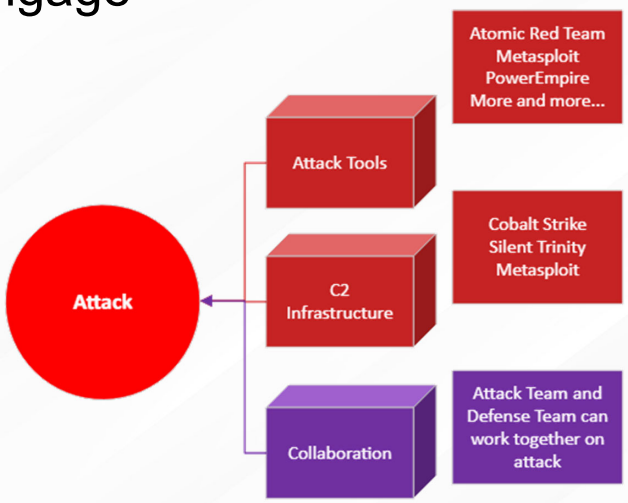


3. Attack / Execute / Engage

Goal: Execute the attack.

What attacks were successful?
What data could be found?
Was a pivot possible?
Could a C2 be achieved?

Did the attack achieve its goal?
Why? Why not?



4: Hunt and Defend

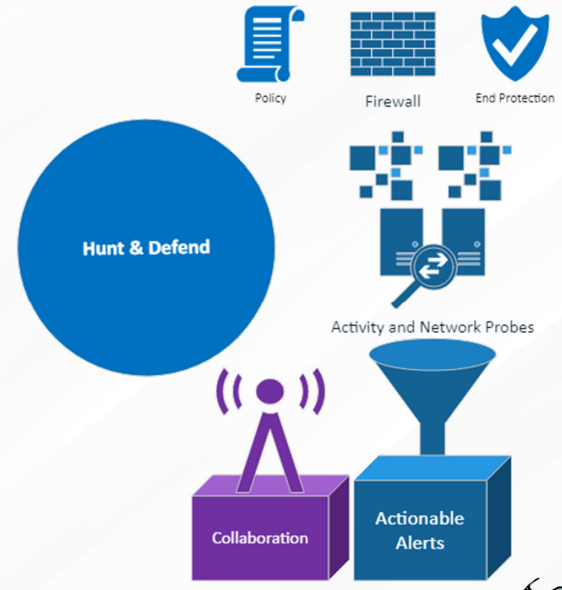
Goal: Find and Defend/Stop the Attack

How:

- Hunt Team Skills!
- Search Logs
- Review Endpoint Protection

Determine:

- New Tools Needed?
- Logs Need Adjusted?



5. Adjust & Harden

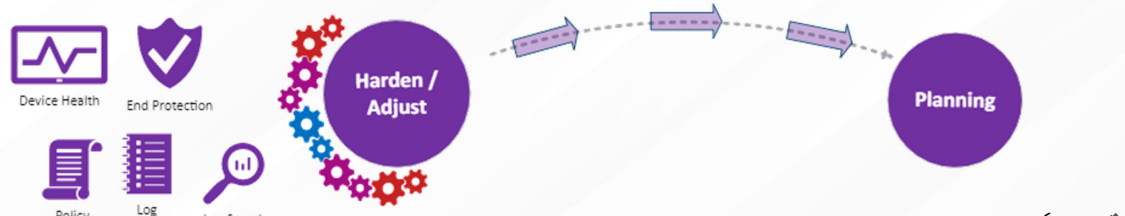
GOAL: Identify the changes necessary to be able to achieve the goals identified in planning.

- Stop attacks / Identify Attacks / Alert

How: Modify policies, protections, logging to achieve goal.

- After changing, go to Planning phase and verify that you can achieve the goal (Stop/Identify/Alert)

Success: Move to Reporting Phase



Reporting and Request for Deployment

GOAL: Finalize the documentation of the Lifecycle engagement.

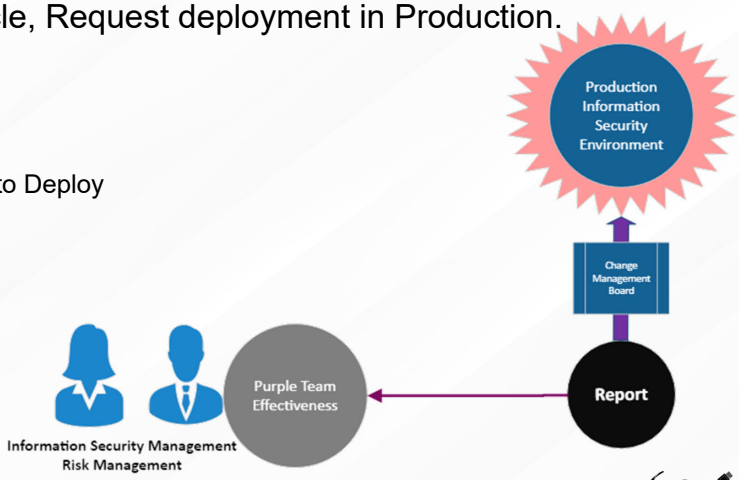
GOAL: With Success of the Lifecycle, Request deployment in Production.

How:

- Review Lifecycle Documentation
- Produce Change Management Request to Deploy

Done?

On to the next Lifecycle Rotation!



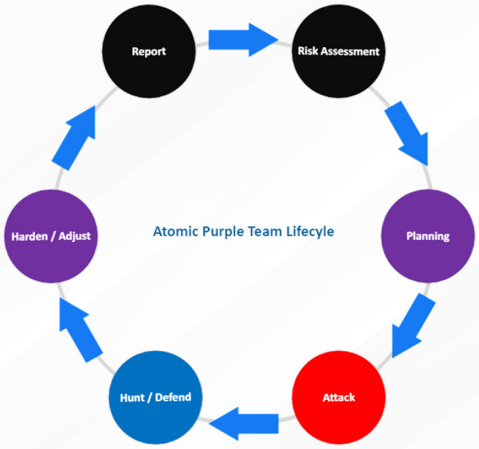
Lessons Learned

What can be done differently next time?

Were new techniques learned?

Do you feel you gained experience in “x”?

Has the organizations security posture improved?



Jordan Drysdale was around for the inception of Napster and the explosion of P2P networks. This drove his fascination with network systems and led him toward a career in IT. Jordan's first gig in the industry included supporting Latin American networking customers for Hewlett Packard's network support division. After five years of support, engineering, training, and stress, Jordan became a wireless escalations team lead and multi-vendor certified problem solver. With kids in tow, Jordan headed back toward the Dakotas to be nearer extended family and friends where he learned Citrix, VMware, VDI, supported Cisco gear, implemented profile management solutions, deployed remote networks at scale, and ensured performance across infrastructure. Before becoming a penetration tester, Jordan supported multiple (50+) domains as part of an MSSP's rock star team. Solutions utilized included HP Networking, FortiGate/FortiManager/FortiWeb/FortiAnalyzer et al., Cisco ASA, HP DL/GL/ML, Dell, VMware, NetApp, and the list goes on. Since 2014, Jordan has been a penetration tester with the Black Hills InfoSec team.

Kent Ickler started his Information Technology career working for an Internet Service Provider supporting the MidWest's broadband initiatives of the early 2000s. His interest in technology and business operations drove his career to working for multiple Fortune 500 companies and equipping their organizational leadership with business analytical data that would support their technology initiatives. With his continued interest in Business Operations, Kent completed his postgraduate education in Business Management. With an understanding of Information Technology, System Administration, Accounting, and Business Law, Kent has helped businesses leverage technology for competitive advantage while balancing the risks associated with today's dynamic network environments. Kent has been with Black Hills Information Security since 2016 in security and administration roles.

Jordan Drysdale, Kent Ickler

We know what it's like to have limited resources and staff with huge responsibilities looming overhead. We're focused on helping you save time and your sanity.

Applied Purple Team

info@defensiveorigins.com

https://www.defensiveorigins.com

Applied Purple Teaming

Atomic Purple Team

info@defensiveorigins.com

https://www.defensiveorigins.com