



APT0020

Building Threat Optics Infrastructure

- APT0021 – Sysmon and Sysmon Modular
- APT0022 – Audit Policies, WEC / WEF
- APT0023 – Event Ingestors (Logstash + Kafka)
- APT0024 – Log Shipping with WinLogBeat



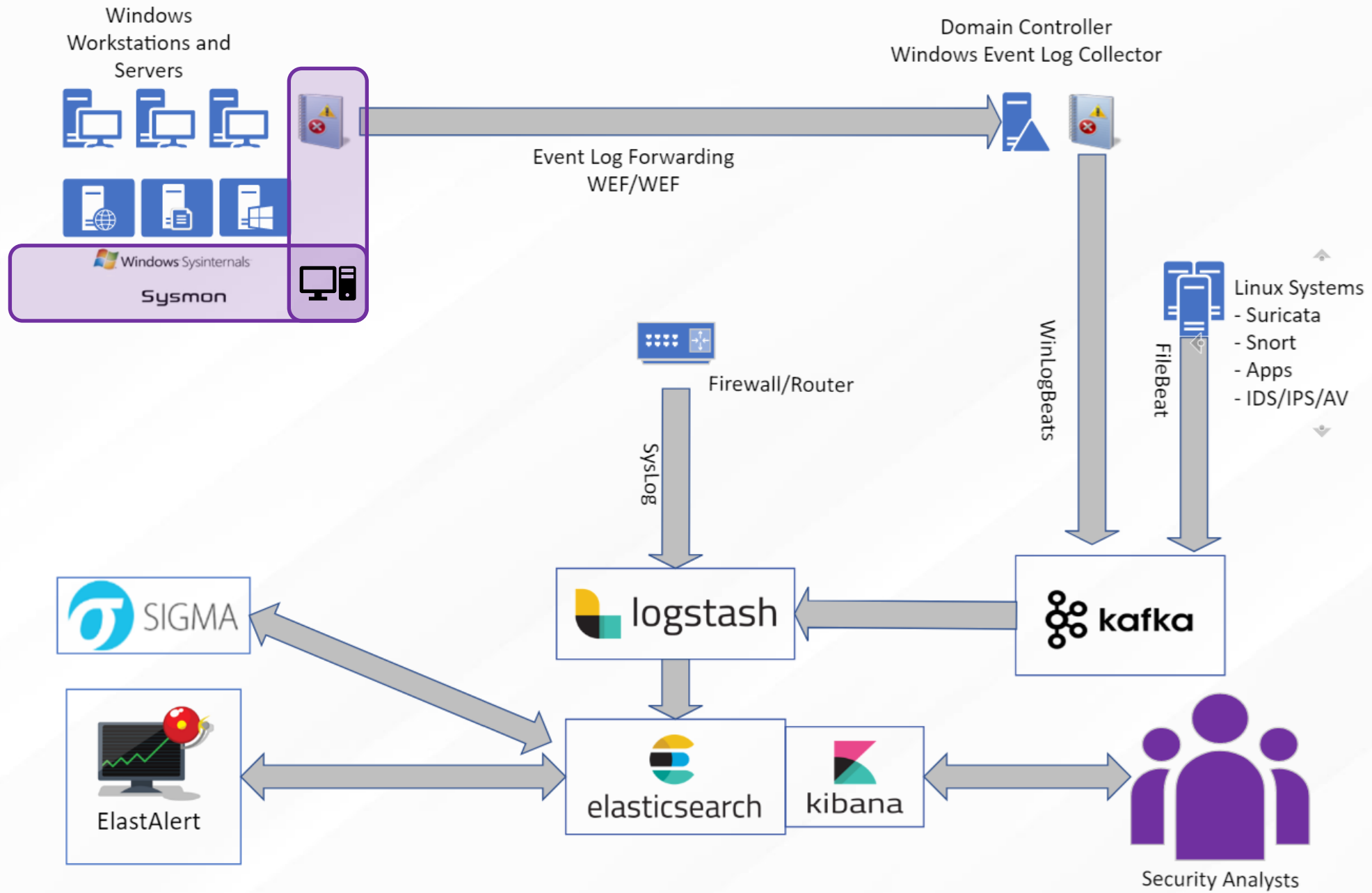


APT00021

Endpoint Optics Sysmon and Sysmon-Modular



START
HERE



Sysmon – System Monitor?






Biased opinion: Sysmon is the best free endpoint logging tool available.

Nuanced opinion: Sysmon can create a lot of noise.

Significantly fewer event IDs than standard Windows logging

- Better organized
- Logs full command line
- Records hash of process executables (makes global searching easier)
- DLL load operations
- Raw disk reads (file.exe opened by process)
- Network connections
- Process Access

Sysmon v11.11

07/15/2020 • 14 minutes to read •      +2

By Mark Russinovich and Thomas Garnier

Published: July 15, 2020



defensiveorigins.com

© Defensive Origins LLC APT0020.4 – APT Optics Infrastructure – Sysmon

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

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

Evidence of Sysmon's Abilities – Just a ping.

Operational Number of events: 46

Level	Date and Time	Source	Event ID	Task Category
Information	6/21/2020 11:36:35 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:36:33 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/21/2020 11:36:17 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:36:16 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:36:14 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/21/2020 11:35:28 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:35:26 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/21/2020 11:35:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:35:21 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:35:18 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 22, Sysmon

General Details

Dns query:
RuleName: -
UtcTime: 2020-06-21 17:36:33.464
ProcessGuid: {7a0e89b9-9aa1-5eef-7a08-000000001f00}
ProcessId: 10080
QueryName: google.com
QueryStatus: 0
QueryResults: ::ffff:172.217.4.110;
Image: C:\Windows\System32\PING.EXE

Command Prompt

```
c:\>ping google.com

Pinging google.com [172.217.4.110] with 32 bytes of data:
Reply from 172.217.4.110: bytes=32 time=40ms TTL=64
Reply from 172.217.4.110: bytes=32 time=40ms TTL=64
Reply from 172.217.4.110: bytes=32 time=40ms TTL=64
Reply from 172.217.4.110: bytes=32 time=40ms TTL=64

Ping statistics for 172.217.4.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 40ms, Maximum = 48ms, Average = 40ms

c:\>
```



Evidence of Sysmon's Abilities – Just a ping.

1. User instantiates a command prompt (cmd.exe)
 - Sysmon event ID 1: Process creation (number 3 in screenshot)
2. User issues command to “ping google.com”
 - Sysmon event ID 22: DNS lookup (number 4 in screenshot)
3. Sysmon logs user access ping.exe
4. Ping.exe asks for DNS resolution of google.com

All of this takes 10 seconds to get logged to disk



Evidence of Sysmon's Abilities – RDP Session

1. User instantiates launches mstsc.exe
 - Sysmon event ID 1: Process creation

Information	6/21/2020 11:43:05 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/21/2020 11:41:58 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:38:11 AM	Sysmon	22	Dns query (rule: DnsQuery)

Event 1, Sysmon	
General	Details
<p>Process Create: RuleName: technique_id= T1204, technique_name= User Execution UtcTime: 2020-06-21 17:43:05.811 ProcessGuid: {7a0e89b9-9c29-5eef-8608-000000001f00} ProcessId: 3884 Image: C:\Windows\System32\mstsc.exe FileVersion: 10.0.17763.404 (WinBuild.160101.0800) Description: Remote Desktop Connection Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: mstsc.exe CommandLine: "C:\Windows\system32\mstsc.exe" CurrentDirectory: C:\Windows\system32\</p>	

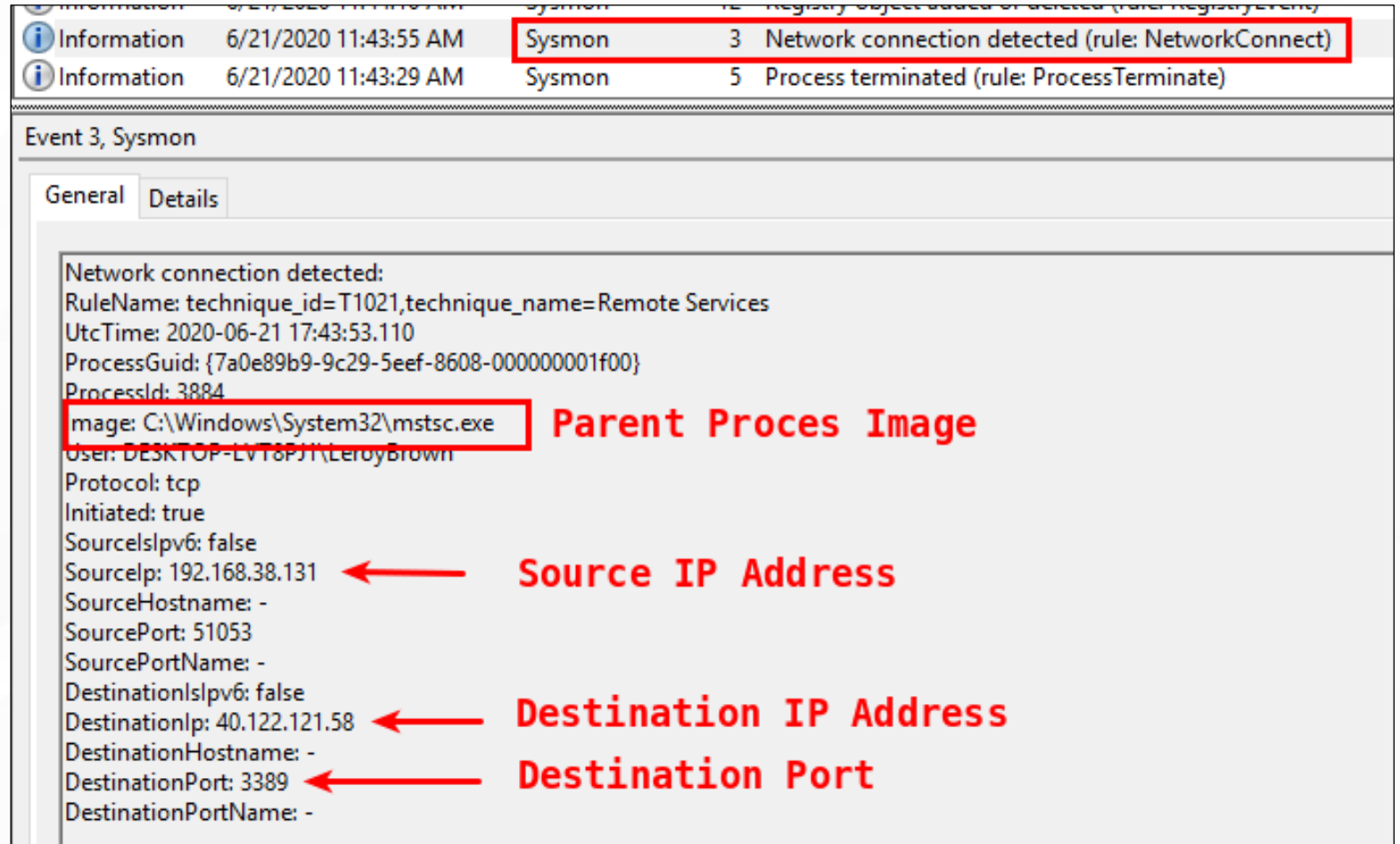


Evidence of Sysmon's Abilities – RDP Session

Finally something interesting: Network Connection Detected

- Event ID 3!
 - Image name
 - Src IP
 - Dst IP
 - Dst port

This is important.



Level	Date and Time	Source	Event ID	Task Category	Task Name
Information	6/21/2020 11:43:55 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)	
Information	6/21/2020 11:43:29 AM	Sysmon	5	Process terminated (rule: ProcessTerminate)	

Event 3, Sysmon

General Details

Network connection detected:
RuleName: technique_id=T1021,technique_name=Remote Services
UtcTime: 2020-06-21 17:43:53.110
ProcessGuid: {7a0e89b9-9c29-5eef-8608-000000001f00}
ProcessId: 3884
Image: C:\Windows\System32\mstsc.exe
User: DESKTOP-LVT8PJI\LeroyBrown
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.38.131
SourceHostname: -
SourcePort: 51053
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 40.122.121.58
DestinationHostname: -
DestinationPort: 3389
DestinationPortName: -

Parent Proces Image

Source IP Address

Destination IP Address

Destination Port



Sysmon's Newest Event ID: 23 FileDelete

1. Archive Directory location, can be a network share.
 - This can provide forensic investigators the evidence they need.
 - Example: System compromised, malware downloaded, executed, and deleted.
 - Sysmon will create an archive of the deleted file.
2. FileDelete option to *include* or *exclude*
3. Rule filters as they apply to each other *and ...or... or*
4. File descriptors of interest (.exe, .bat, .ps1, .aspx, .vbs, and so on)

Sysmon has a marketing problem though.



Sysmon's Newest Event ID: 23 FileDelete

At this point, the test file create and delete was caught.

Event ID 11: Notepad (parent process) created File.hta

Event ID 23: FileDelete Rule with file hash

Information	6/21/2020 1:50:30 PM	Sysmon	23	File Delete (rule: FileDelete)
Information	6/21/2020 1:50:30 PM	Sysmon	11	File created (rule: FileCreate)
Information	6/21/2020 1:50:27 PM	Sysmon	7	Image loaded (rule: ImageLoad)

Event 11, Sysmon

General Details

File created:
RuleName: -
UtcTime: 2020-06-21 19:50:30.819
ProcessGuid: {7a0e89b9-b9ff-5eef-ec08-000000001f00}
ProcessId: 9884
Image: C:\Windows\system32\notepad.exe
TargetFilename: C:\Users\LeroyBrown\Downloads\Demo\File.hta
CreationUtcTime: 2020-06-21 19:50:30.819





ATOMIC
PURPLE
TEAM



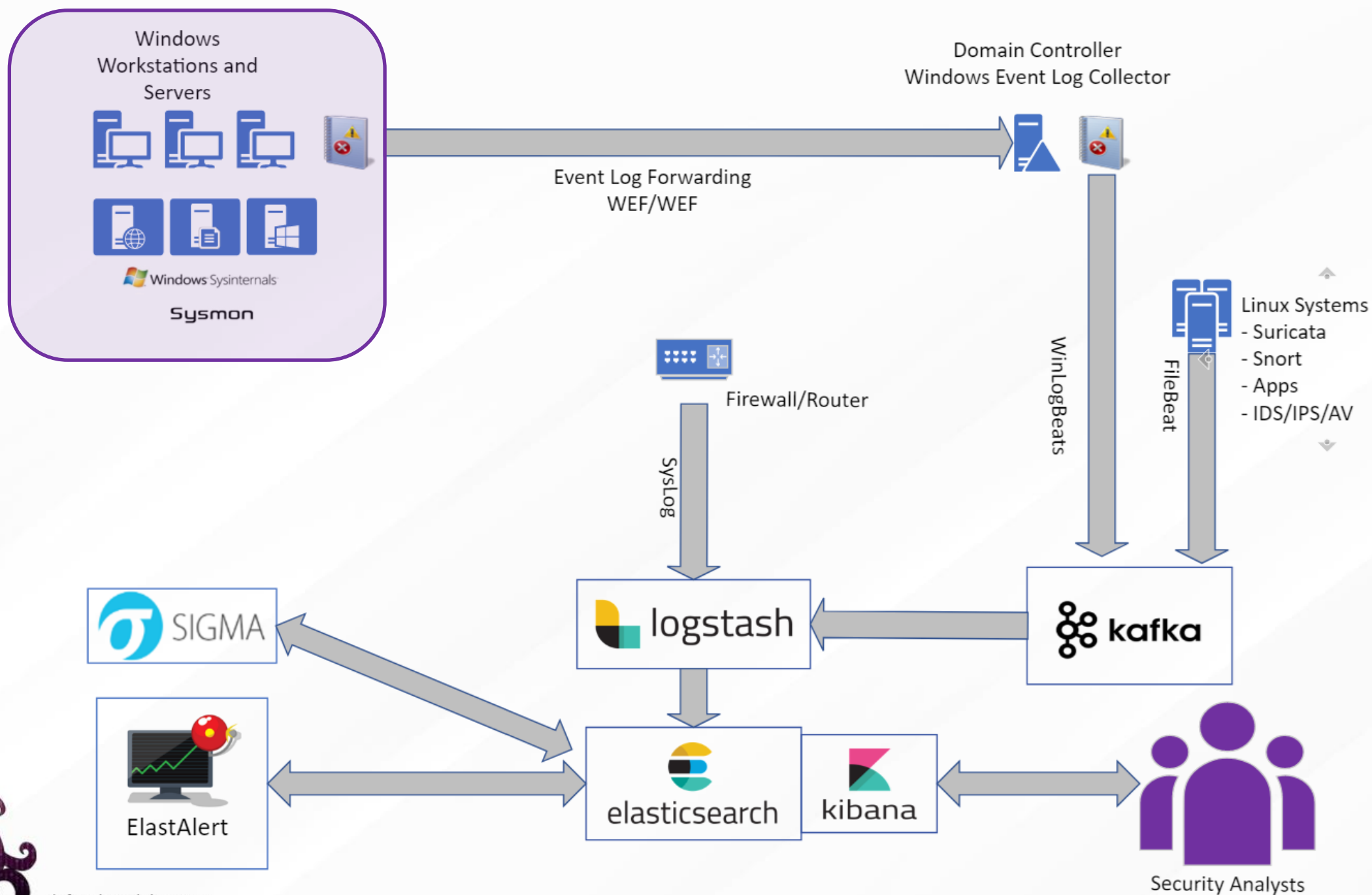
APT0022

Windows Audit Policies
Windows Event Viewer
IIS Logging



defensiveorigins.com

© Defensive Origins LLC APT002111 – APT Optics Infrastructure – Event Handlers



Windows Audit Policy – The Complicated Process of 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



Windows Audit Policy – The Complicated Process of 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 times per day.

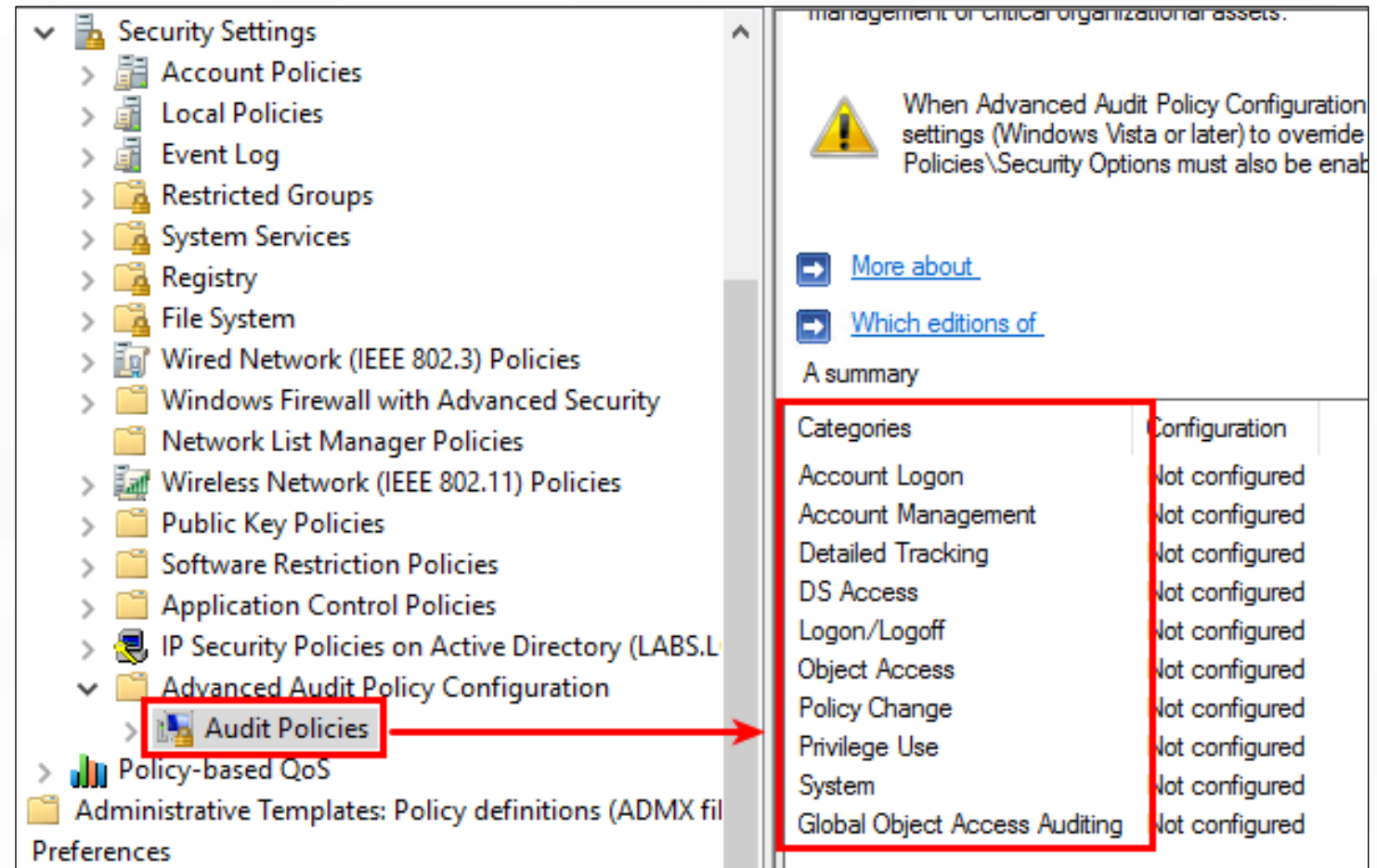
- What do we need to track? Optics targets, things we're interested in.
- How is our network performance? Latency.
- What about the disk where resulting events are written? IOPS
- How many events per second? SQL / SIEM / Big Data



Windows Audit Policy – The Complicated Process of 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



management of critical organizational assets.

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

[More about](#)

[Which editions of](#)

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



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

Account Logon
Account Management
Account Management
Account Management
Account Management
Detailed Tracking
Detailed Tracking
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Object Access
Object Access
Object Access
Object Access
Object Access
Object Access
Policy Change
Policy Change
Policy Change
Policy Change
Policy Change
Policy Change
Privilege Use
System
System
System

Subcategory

Credential Validation
Security Group Management
User Account Management
Computer Account Management
Other Account Management Events
Process Creation
Process Termination
User/Device Claims
IPsec Extended Mode
IPsec Quick Mode
Logon
Logoff
Other Logon/Logoff Events
Special Logon
Account Lockout
Application Generated
File Share
File System
Other Object Access Events
Registry
Removable Storage
Audit Policy Change
MPSSVC Rule-Level Policy Change
Other Policy Change Events
Authentication Policy Change
Authorization Policy Change
Sensitive Privilege Use
Security State Change
Security System Extension
System Integrity

Audit settings

Success and Failure
Success
Success and Failure
Success and Failure
Success and Failure
Success
Success
Not configured
Not configured
Not configured
Success and Failure
Success
Success and Failure
Success and Failure
Success
Not configured
Success
Not configured
Not configured
Not configured
Success
Success and Failure
Success and Failure
Success and Failure
Success and Failure
Success and Failure
Not configured
Success and Failure
Success and Failure
Success and Failure





ATOMIC
PURPLE
TEAM



APT0023

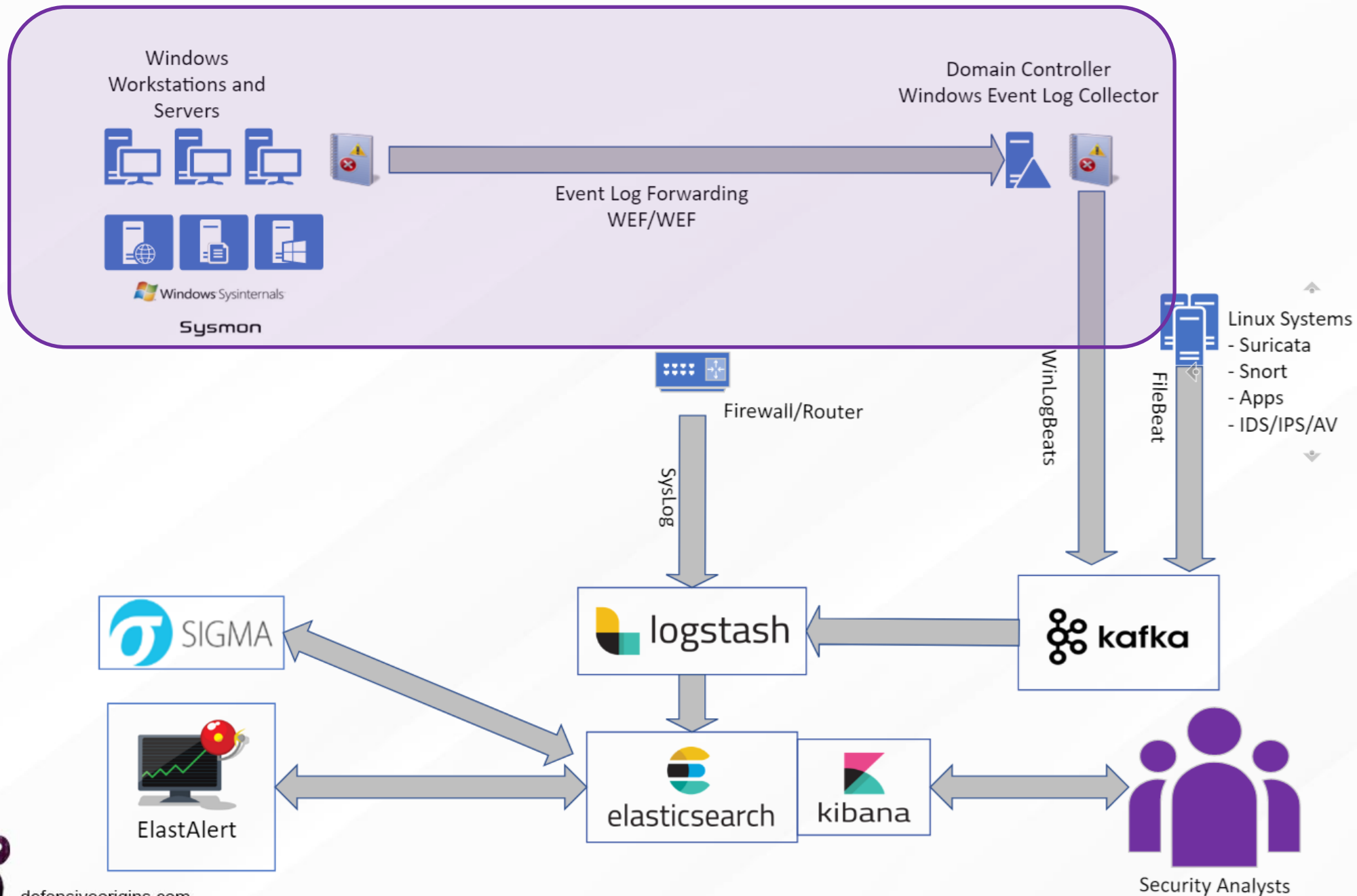
WEC / WEF

Event Subscriptions and Channels



defensiveorigins.com

© Defensive Origins LLC APT0023.17 – APT Optics Infrastructure – Event Handlers



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>



defensiveorigins.com

© Defensive Origins LLC APT0022.19 – APT Optics Infrastructure – Event Handlers

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



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>
```



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

This is just a baseline.



defensiveorigins.com

© Defensive Origins LLC APT0022.22 – APT Optics Infrastructure – Event Handlers

 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

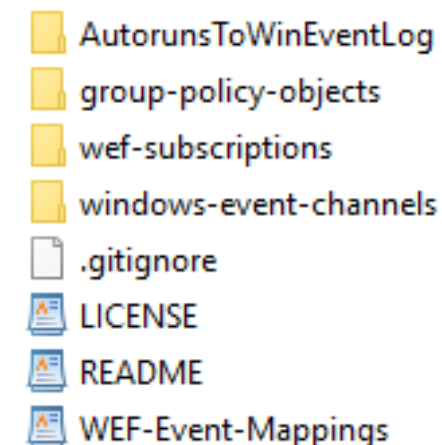
<https://github.com/palantir/windows-event-forwarding>

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

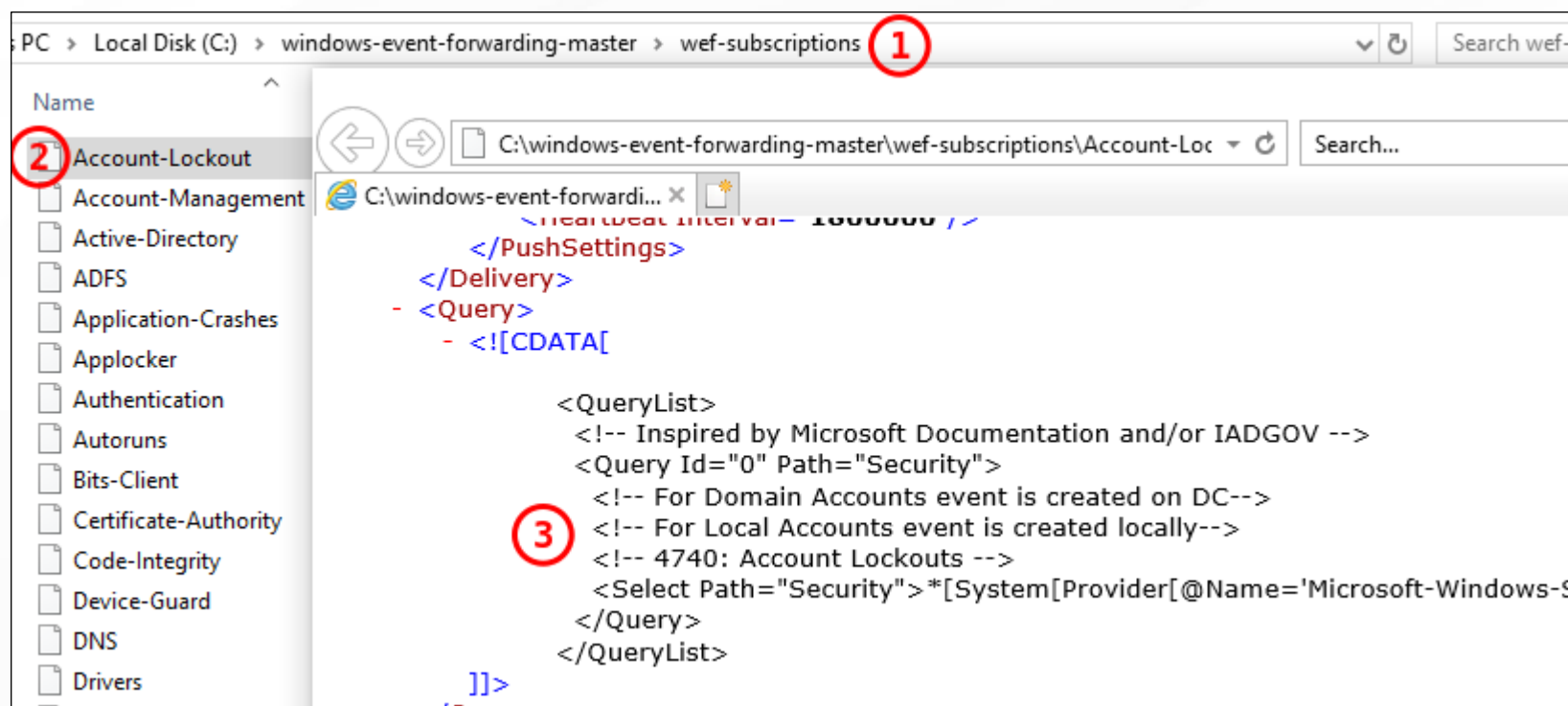
The Palantir Event Handling Repo

Security Insight Baselines

The repo is structured in this manner



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





ATOMIC
PURPLE
TEAM



APT0024

Log Shipping Event Ingestors



defensiveorigins.com

© Defensive Origins LLC APT0024.24 – APT Optics Infrastructure – Log Shipping

Beats (by Elastic) - Kafka Ingest for Elastic Stack

APT lab utilizes Kafka (few lines of config)

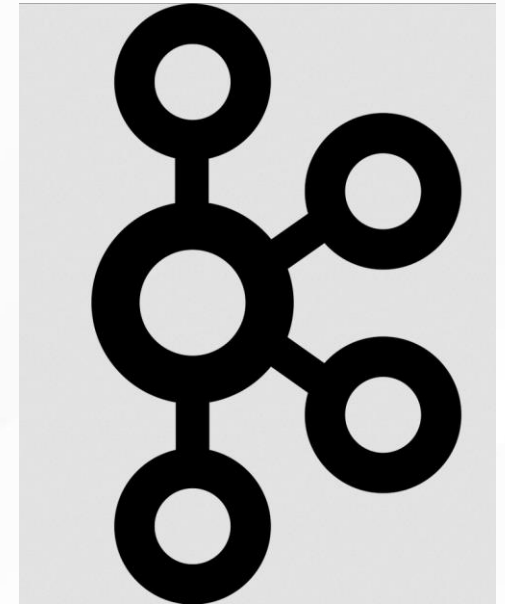
Your environment will differ.

Splunk – Universal Forwarder

ManageEngine – Syslog Relay Tool

ArcSight – Smart Connector and Logger Management

AlienVault – USM Anywhere Sensor



```
#----- Kafka output -----  
output.kafka:  
  # initial brokers for reading cluster metadata  
  # Place your HELK IP(s) here (keep the port).  
  # If you only have one Kafka instance (default for HELK) then remove the 2nd IP  
  hosts: ["10.10.98.20:9092"]  
  topic: "winlogbeat"  
##### HELK Optimizing Latency #####  
  max_retries: 2  
  max_message_bytes: 1000000
```



WinLogBeat Config Options

Configuring Beats for Your Environment
The WinLogBeats config parameters.

event_logs

- name: (full channel name required in config)
- ignore_older: (filter events older than)
- event_id: (id's go here)
- tags: (string value here, easy to search)
- fields:
 - custom_thing: (string / int / etc)

LogName from PS becomes - name in WinLogBeat config -->

```
PS C:\Users\Administrator> Get-WinEvent -ListLog * | Format-List -Property LogName

LogName : Active Directory Web Services
LogName : Application
LogName : DFS Replication
LogName : Directory Service
LogName : DNS Server
LogName : HardwareEvents
LogName : WEC-Authentication
LogName : WEC-Code-Integrity
LogName : WEC-EMET
LogName : WEC-Powershell
LogName : WEC-Process-Execution
```

```
- 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

- name: WEC-Authentication
- name: WEC-Code-Integrity
- name: WEC-EMET
- name: WEC-Powershell
- name: WEC-Process-Execution
```



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

