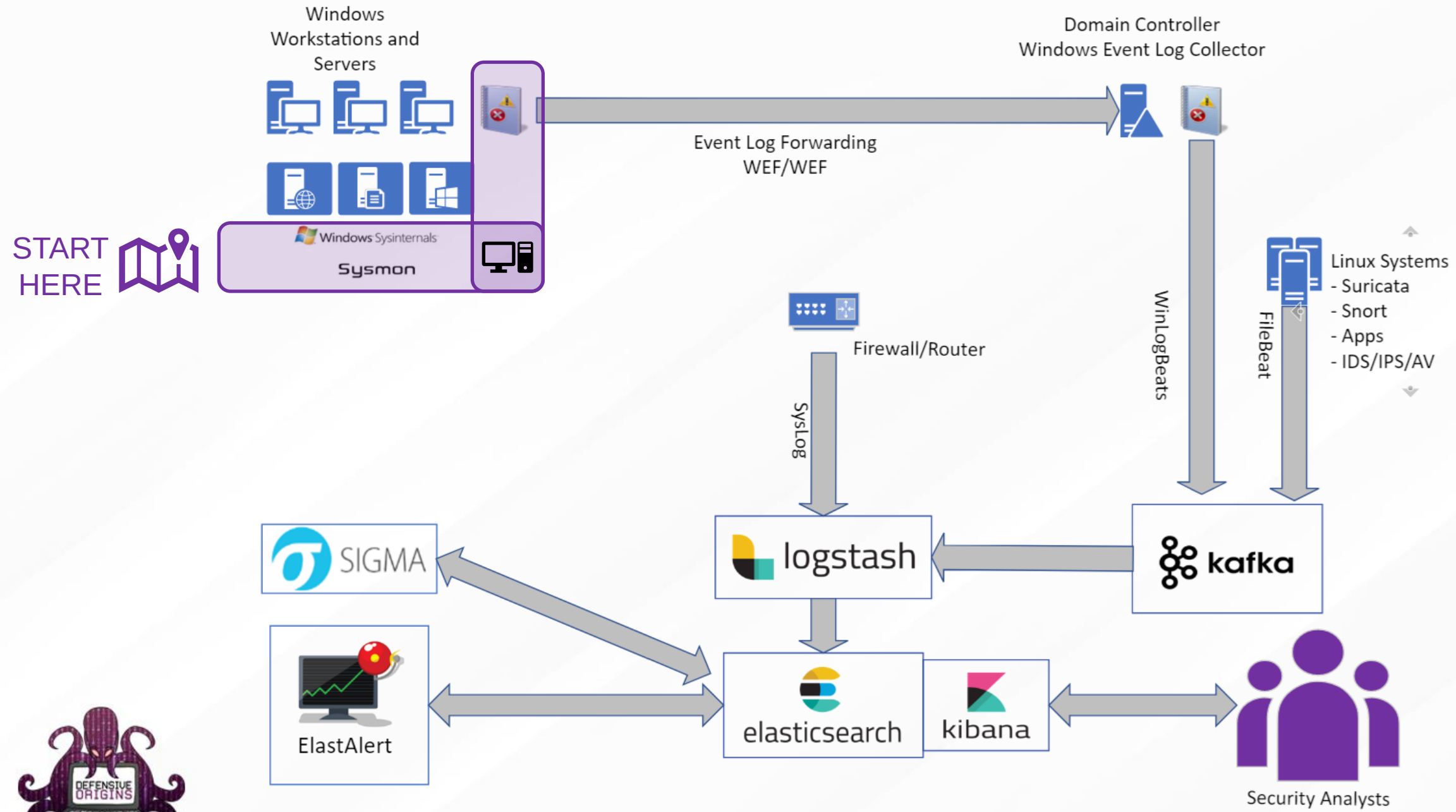
Building Threat Optics Infrastructure

APT0020

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

APT0021

Endpoint Optics
Sysmon and Sysmon-Modular



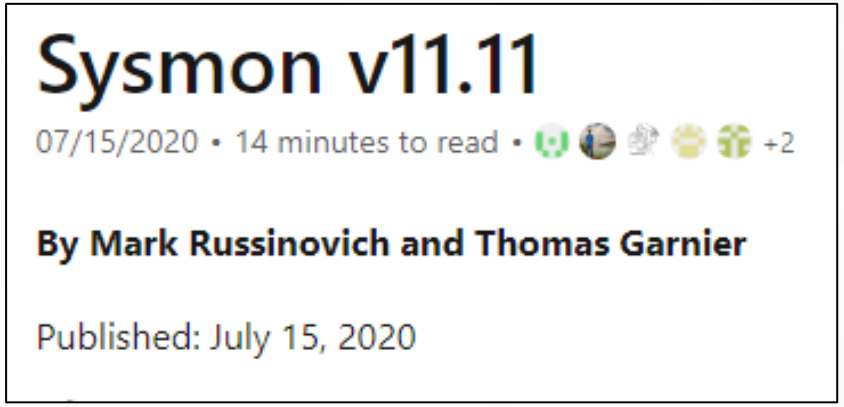
Sysmon – System Monitor?

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

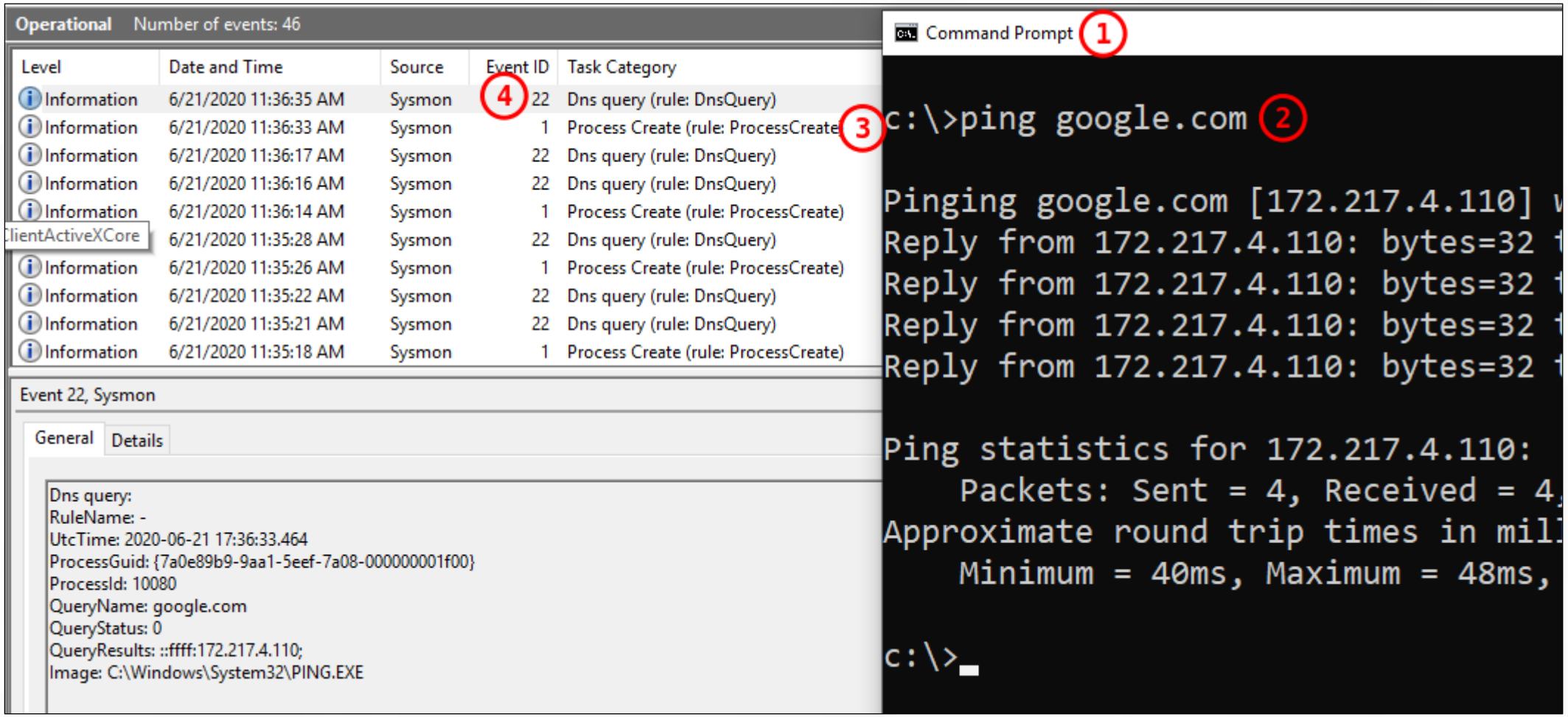
- Better organized
- Logs full command line
- Records hash of process executables (makes global searching easier)
- DLL load operations
- Raw disk reads (file.exe opened by process)
- Network connections
- Process Access



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

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

Evidence of Sysmon's Abilities – Just a ping.



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

Evidence of Sysmon's Abilities – Just a ping.

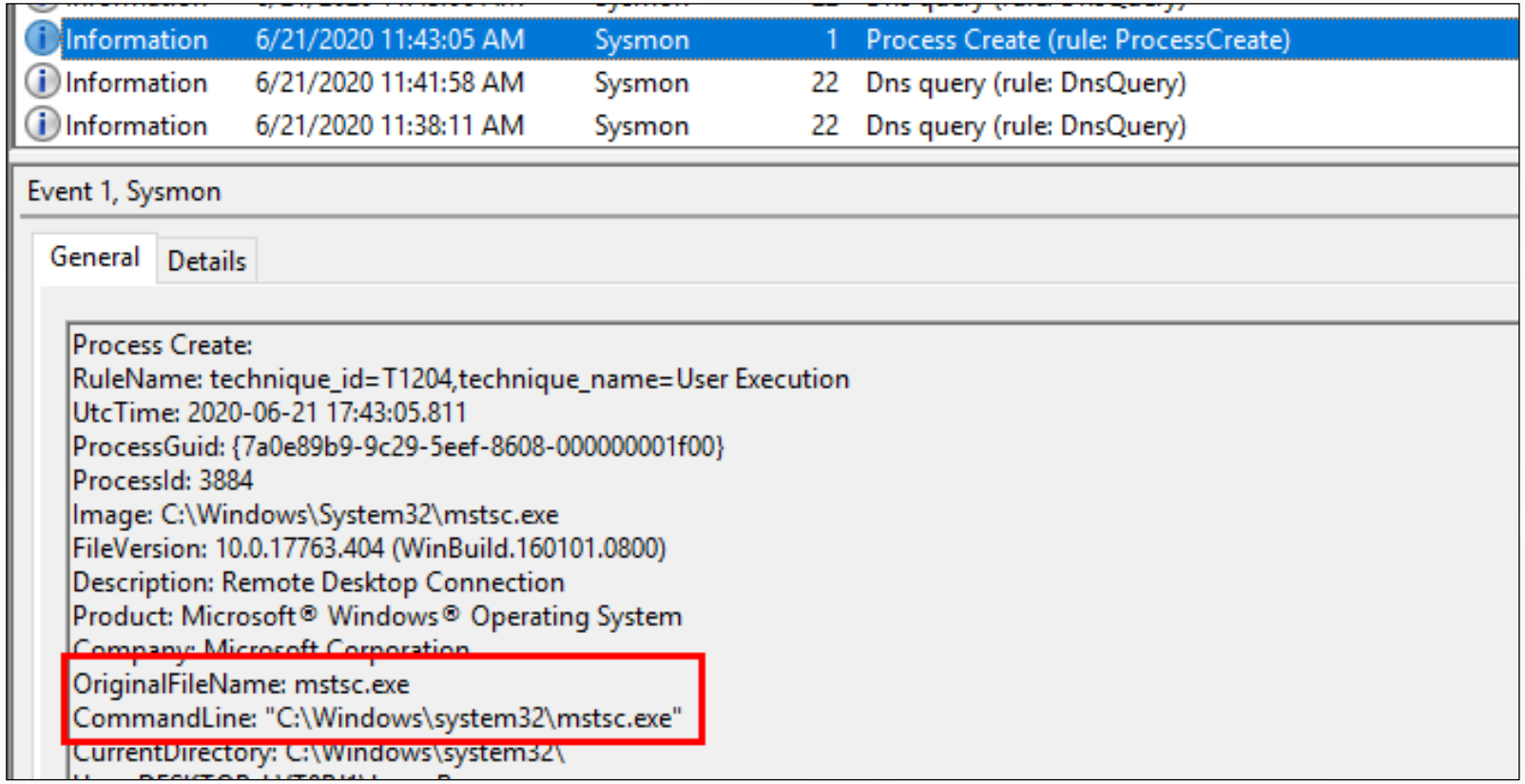
1. User instantiates a command prompt (cmd.exe)
   - Sysmon event ID 1: Process creation (number 3 in screenshot)
2. User issues command to "ping google.com"
   - Sysmon event ID 22: DNS lookup (number 4 in screenshto
3. Sysmon logs user access ping.exe
4. Ping.exe asks for DNS resolution of google.com

All of this takes 10 seconds to get logged to disk

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

Evidence of Sysmon's Abilities – RDP Session

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



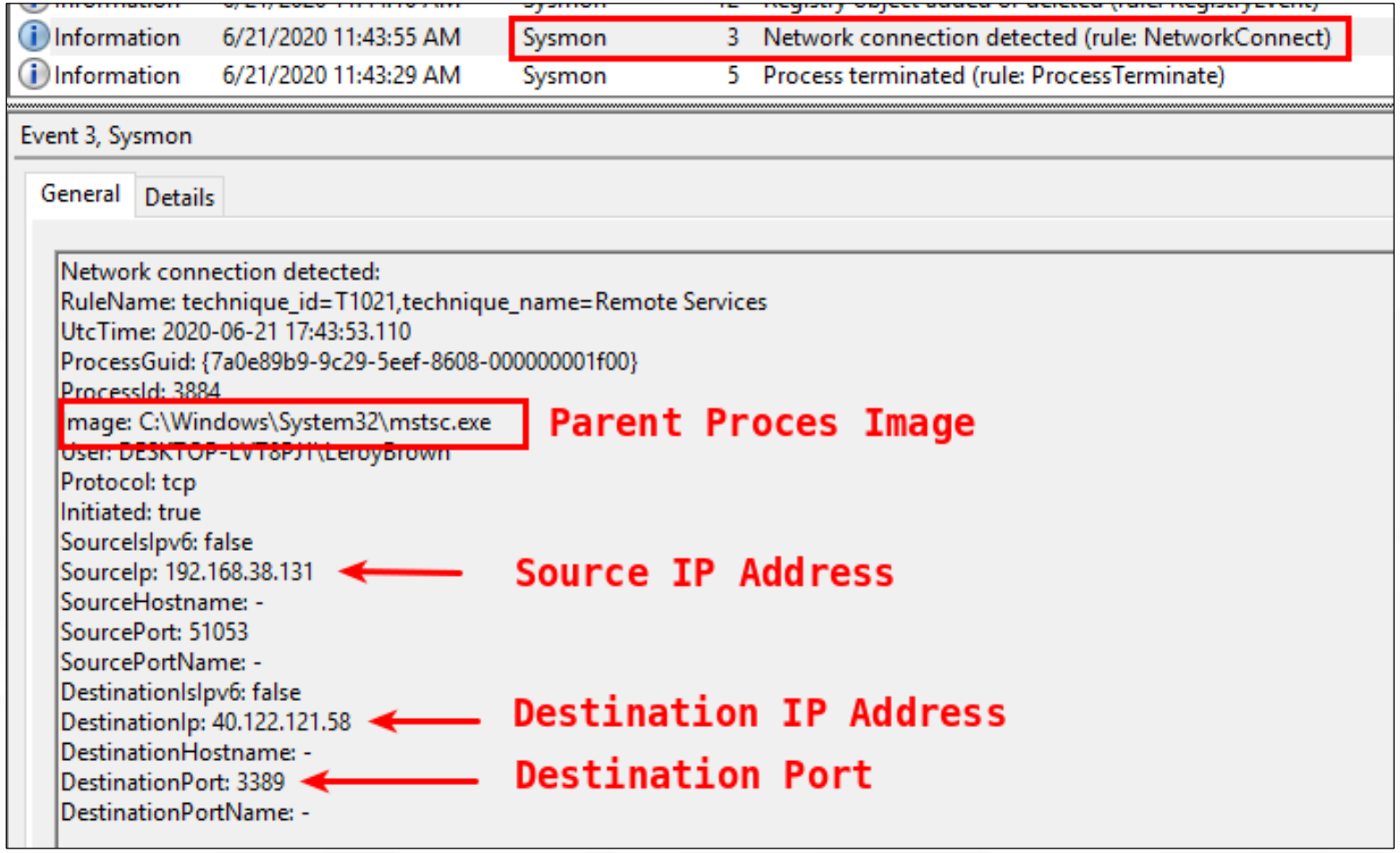
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

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.



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

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.

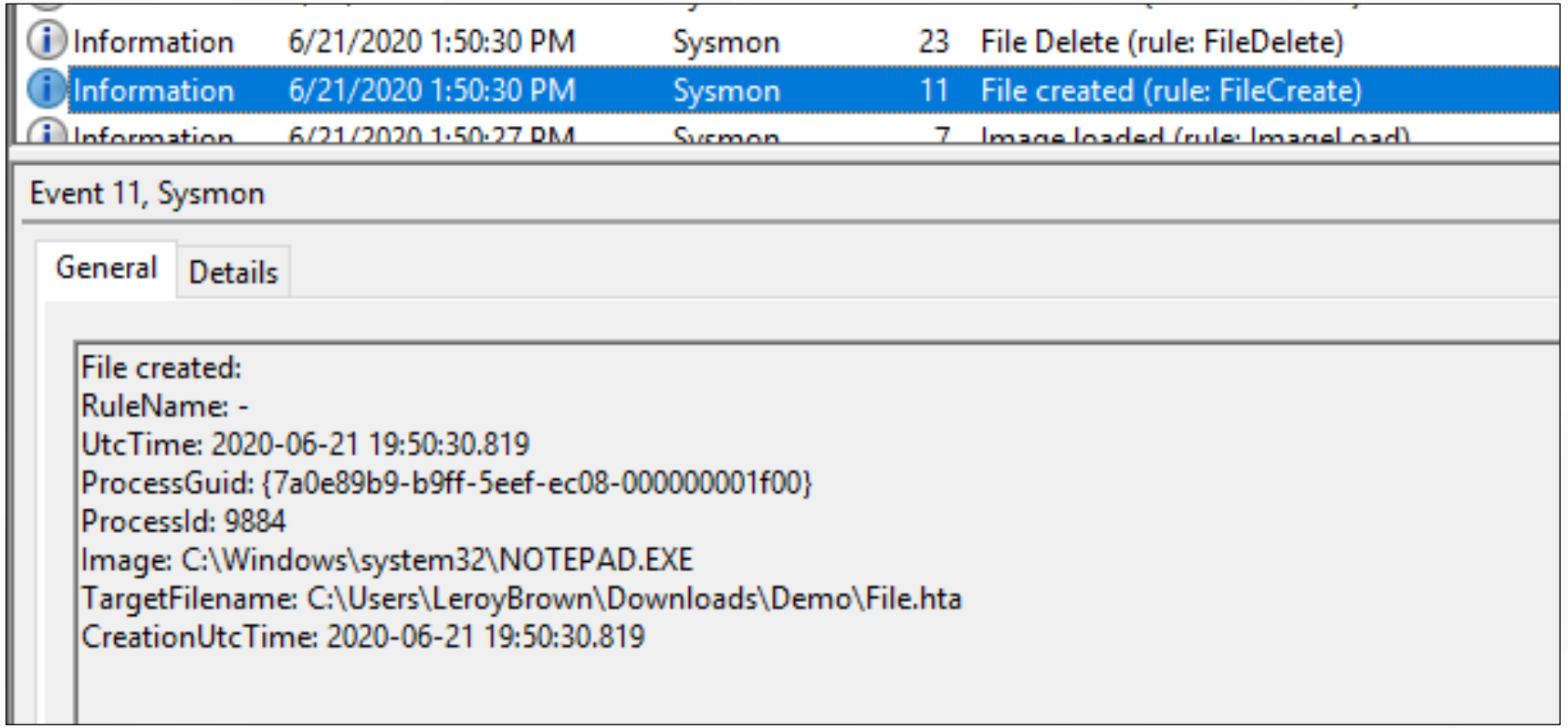
https://youtu.be/_MUP4tgdM7s (Mark Russinovich's Explanation)

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

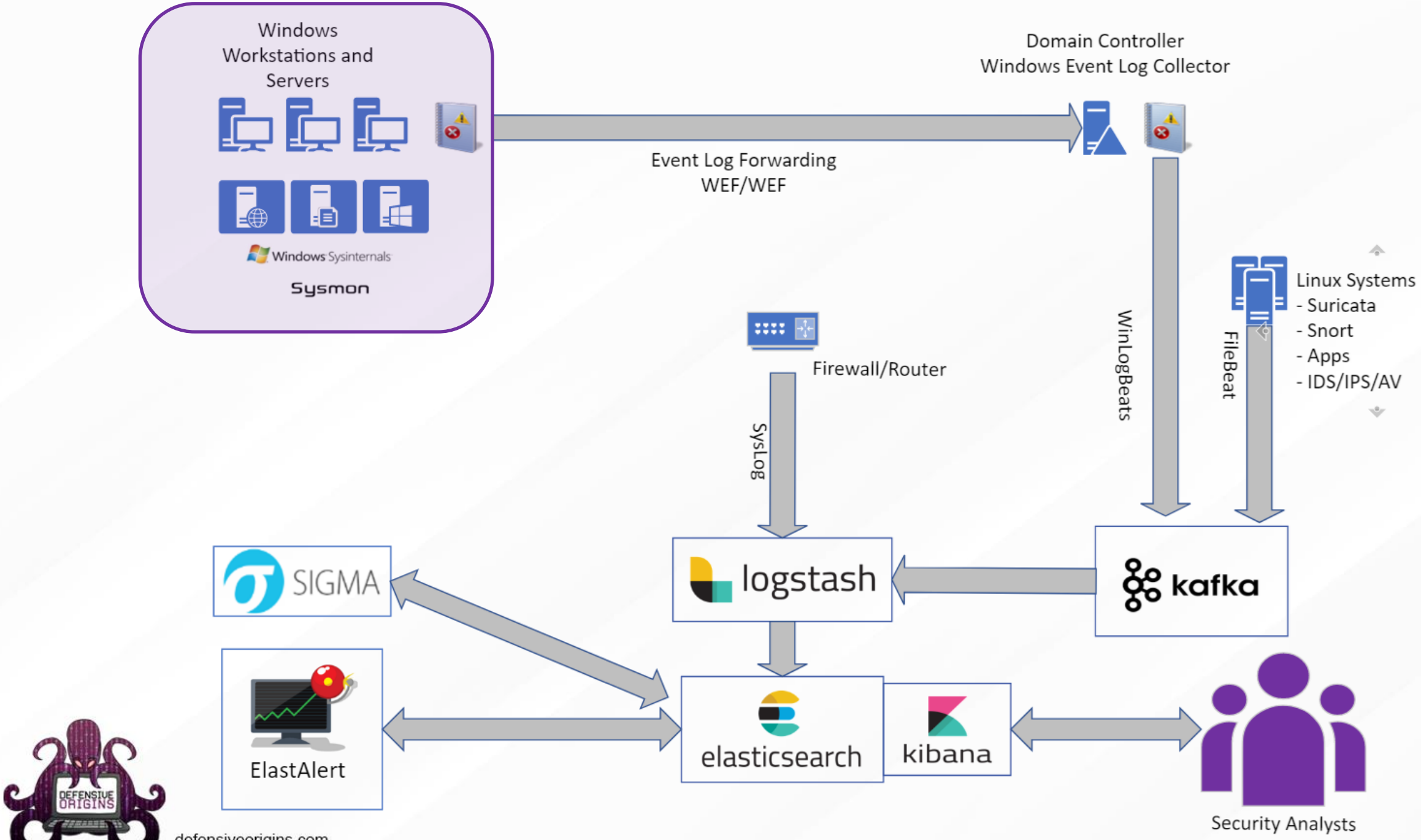
Event ID 23: FileDelete Rule with file hash



https://youtu.be/_MUP4tgdM7s (Mark Russinovich's Explanation)

APT0022

Windows Audit Policies
Windows Event Viewer
IIS Logging



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

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

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 time per day.

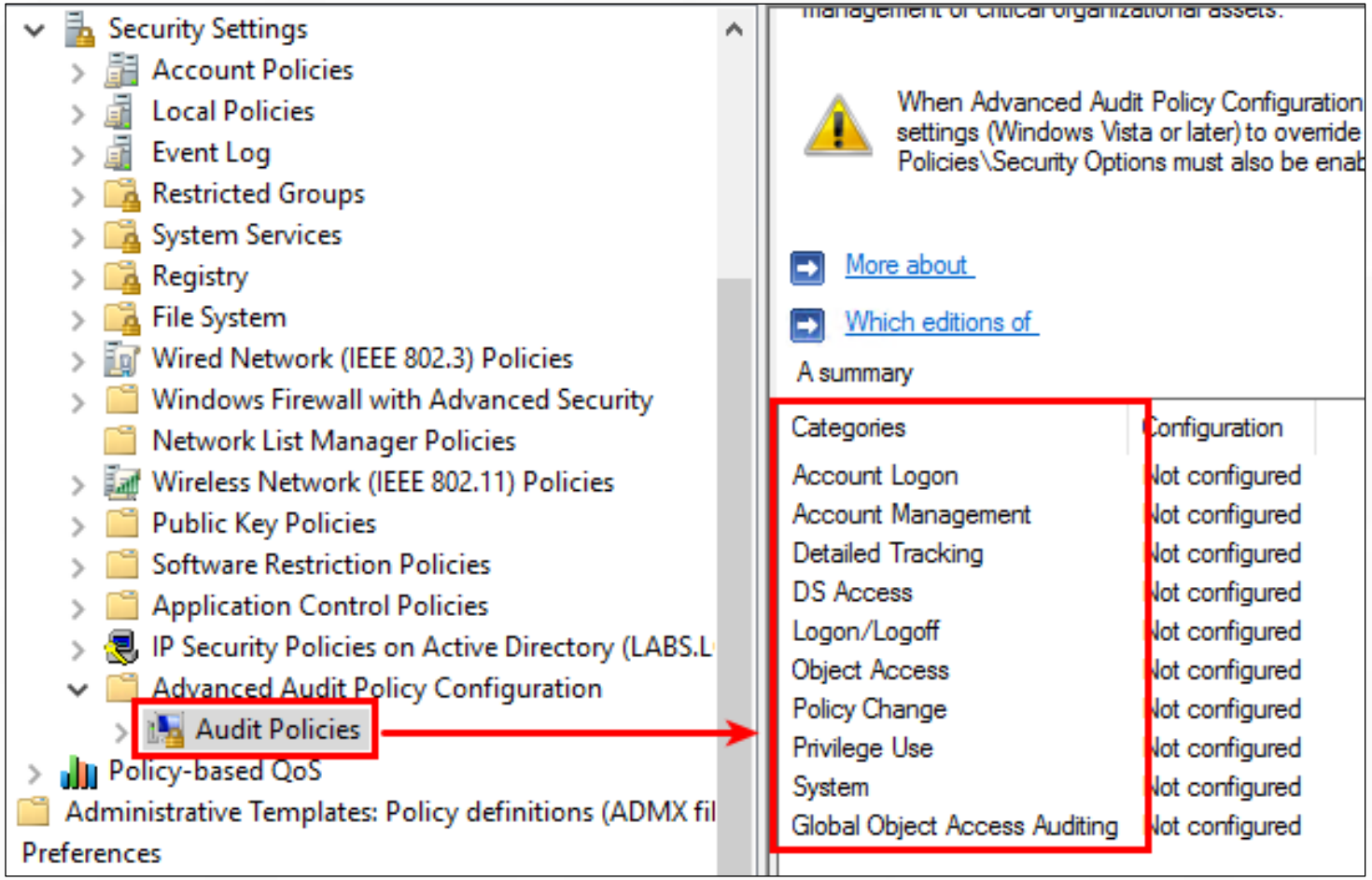
- What do we need to track? Optics targets, things we're interested in.
- How is our network performance? Latency.
- What about the disk where resulting events are written? IOPS
- How many events per second? SQL / SIEM / Big Data

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

Windows Audit Policy – 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



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:

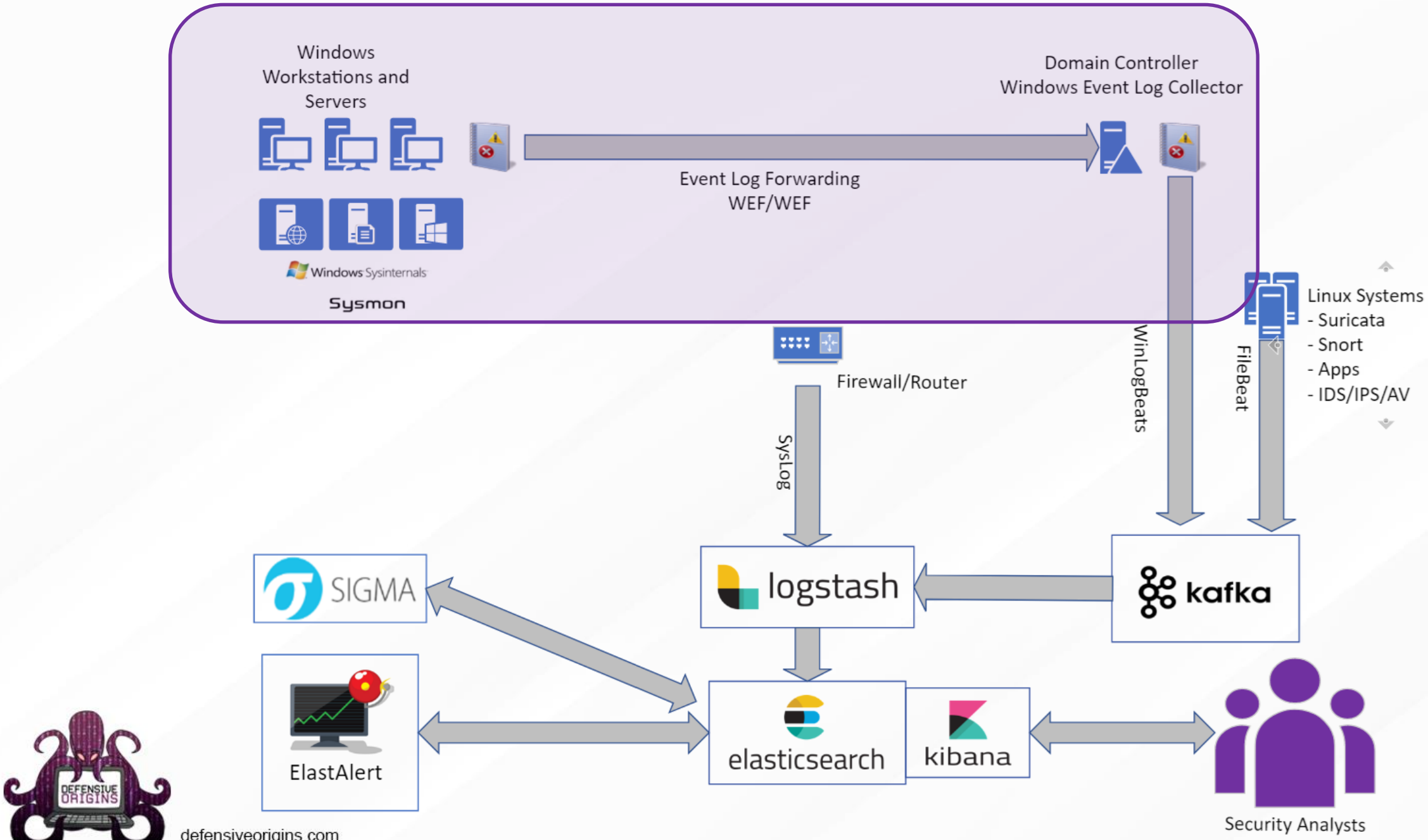
We’re tired of configuring these everywhere. Can you just turn them on for us? By default?

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

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

APT0023

WEC / WEF
Event Subscriptions and Channels



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

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

<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

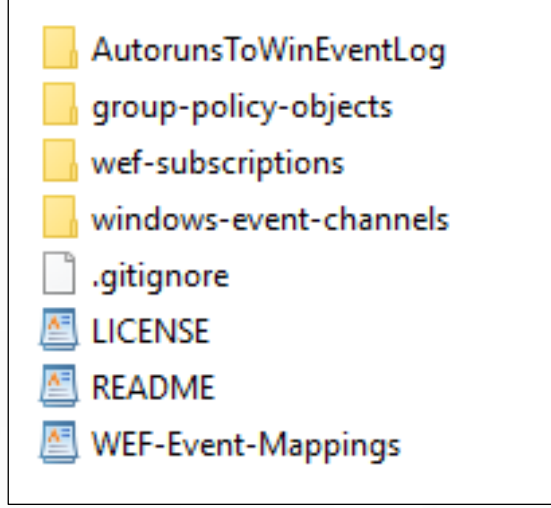
https://github.com/palantir/windows-event-forwarding

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

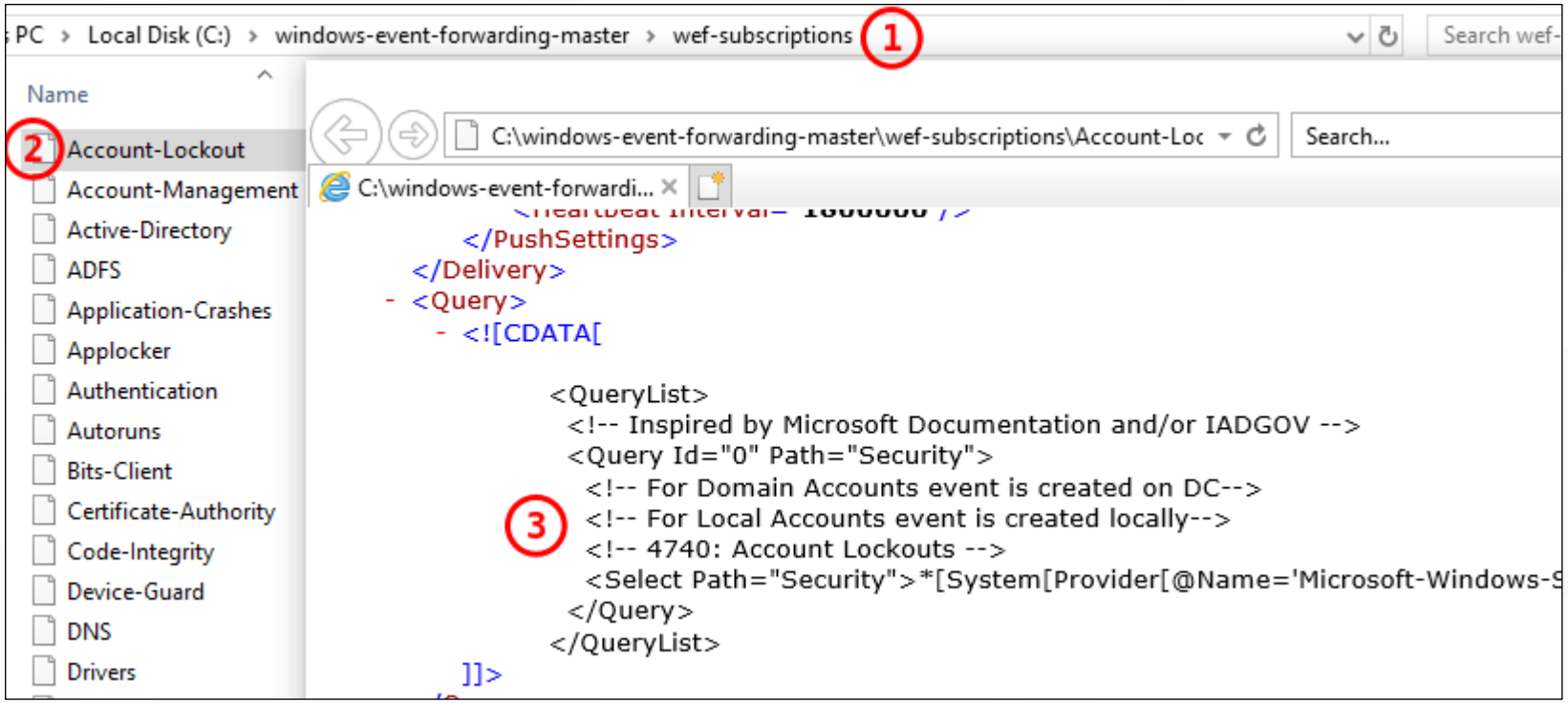
The Palantir Event Handling Repo

Security Insight Baselines

The repo is structured in this manner



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



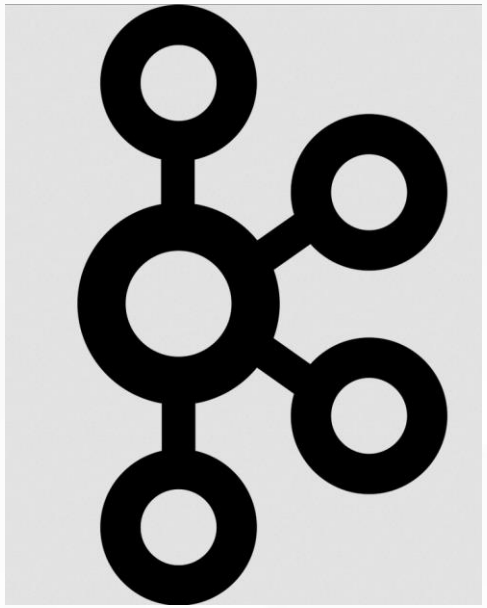
https://github.com/palantir/windows-event-forwarding

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

APT0024

Log Shipping
Event Ingestors

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
```

https://www.elastic.co/guide/en/beats/winlogbeat/current/configuration-winlogbeat-options.html#configuration-winlogbeat-options-event_logs-name

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