APPLIED PURPLE TEAMING

C0340

Threat Optics – Log Shipping

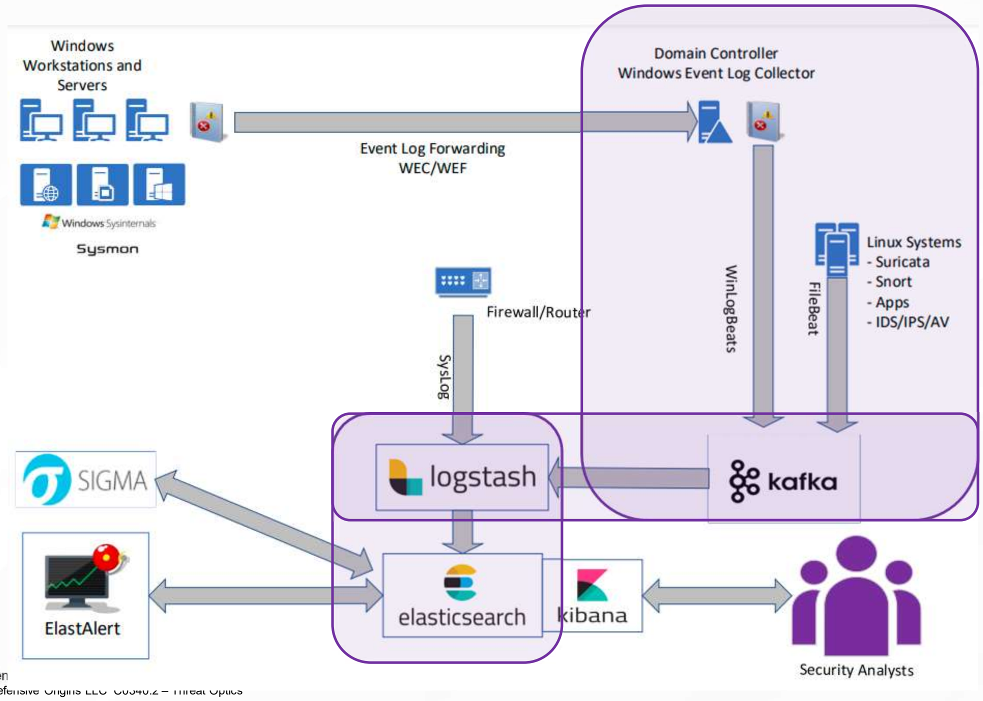
Elastic Ecosystem

Log Shipping

defensiveorigins.com

© Defensive Origins LLC C0340.1 – Threat Optics

Applied Purple Teaming – C0340 Threat Optics – Log Shipping
Elastic Ecosystem
Log Shipping

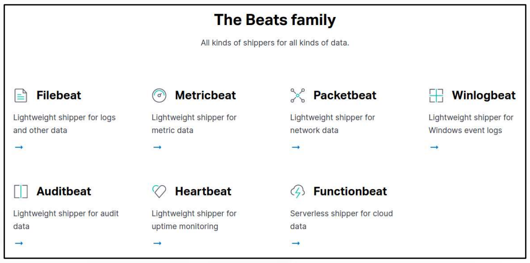


defen
© Defensive Origins LLC C0340.2 – Threat Optics

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



The Beats family

All kinds of shippers for all kinds of data.

Filebeat
Lightweight shipper for logs and other data
→

Metricbeat
Lightweight shipper for metric data
→

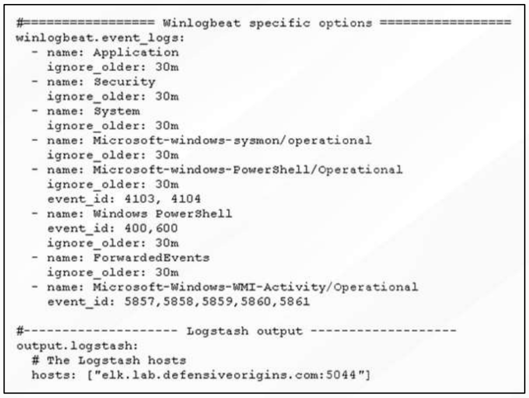
Packetbeat
Lightweight shipper for network data
→

Winlogbeat
Lightweight shipper for Windows event logs
→

Auditbeat
Lightweight shipper for audit data
→

Heartbeat
Lightweight shipper for uptime monitoring
→

Functionbeat
Serverless shipper for cloud data
→



```
#================= 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"]
```

The Elastic Ecosystem

ELK = Elasticsearch, Logstash, Kibana

- Event generated somewhere, shipped through one of the “Beats”
- […] into Logstash (or kafka) for parsing and transformation (pipelining)
- Which is then indexed by Elasticsearch
- And presented visually by Kibana

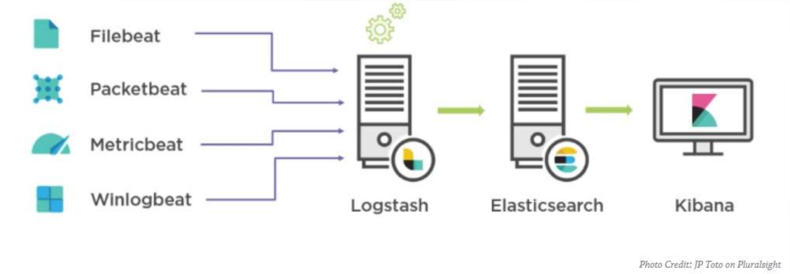


Photo Credit: JP Toto on Pluralsight

Various Log Shippers for SIEMs

Your environment will differ.

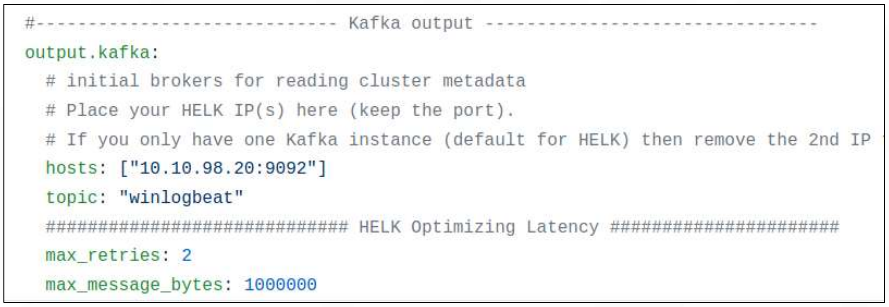
Splunk – Universal Forwarder

ManageEngine – Syslog Relay Tool

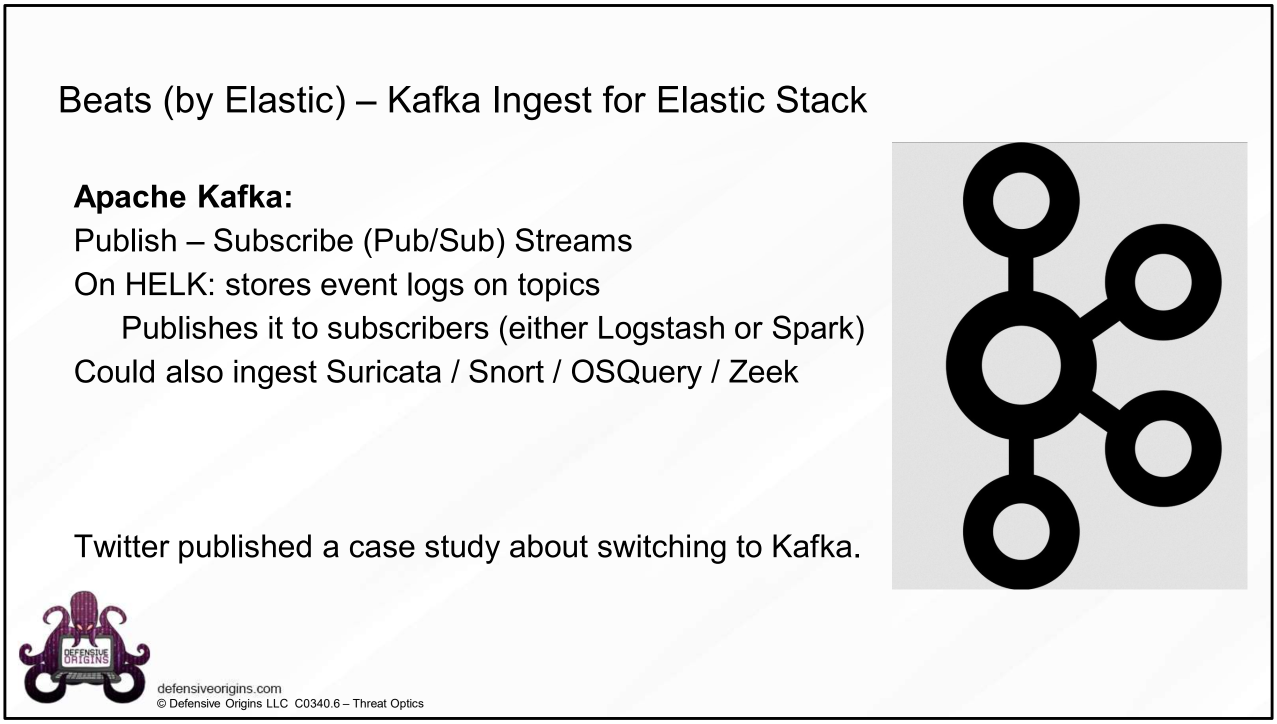
ArcSight – Smart Connector and Logger Management

AlienVault – USM Anywhere Sensor

APT lab utilizes Kafka (few lines of config)



```
#----------------------------- 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
```



Beats (by Elastic) – Kafka Ingest for Elastic Stack

Apache Kafka:

Publish – Subscribe (Pub/Sub) Streams

On HELK: stores event logs on topics

- Publishes it to subscribers (either Logstash or Spark)

Could also ingest Suricata / Snort / OSQuery / Zeek

Twitter published a case study about switching to Kafka.

Links:

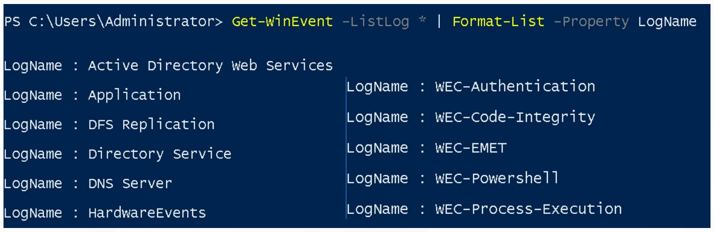
https://blog.twitter.com/engineering/en_us/topics/insights/2018/twitters-kafka-adoption-story.html

WinLogBeat Config Options

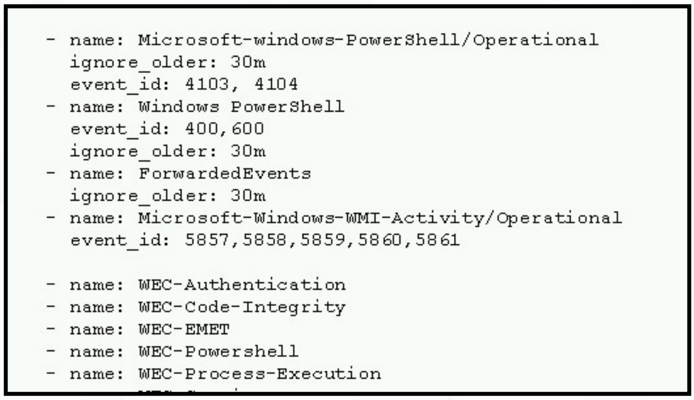
Configuring Beats for Your Environment
The WinLogBeats config parameters.

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



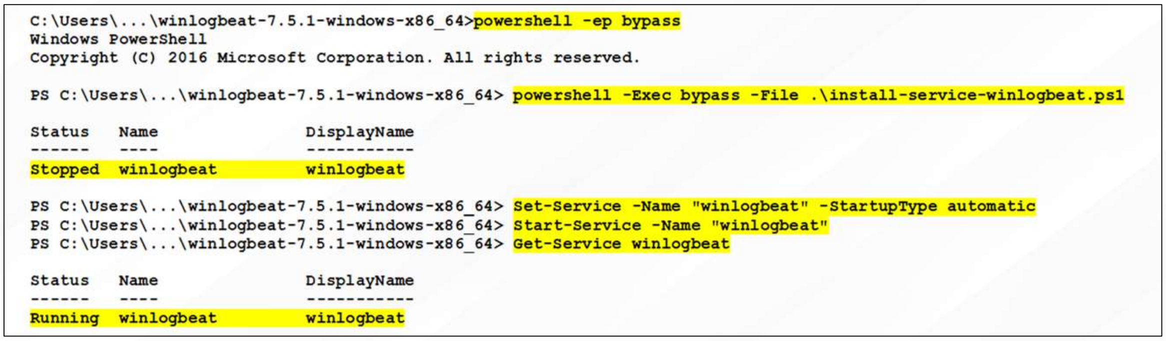
```
  - name: Microsoft-windows-PowerShell/Operational
    ignore_older: 30m
    event_id: 4103, 4104
  - name: Windows PowerShell
    event_id: 400,600
    ignore_older: 30m
  - name: ForwardedEvents
    ignore_older: 30m
  - name: Microsoft-Windows-WMI-Activity/Operational
    event_id: 5857,5858,5859,5860,5861

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

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

Deploy WinLogBeats

Installing WinLogBeat is relatively easy (Windows install below)

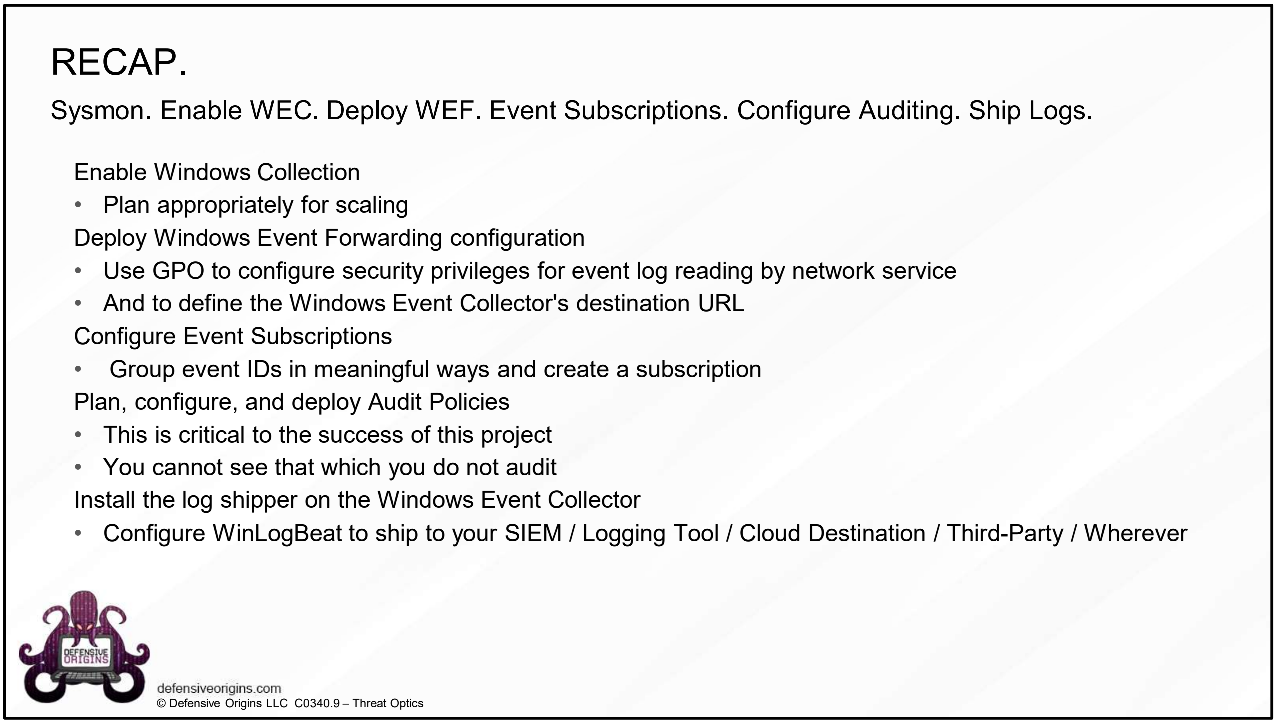
- **powershell -Exec bypass -File .\install-service-winlogbeat.ps1**
- **Set-Service -Name "winlogbeat" -StartupType automatic**
- **Start-Service -Name "winlogbeat"**
- **Get-Service winlogbeat**



```
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
```

defensiveorigins.com

© Defensive Origins LLC C0340.8 – Threat Optics



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

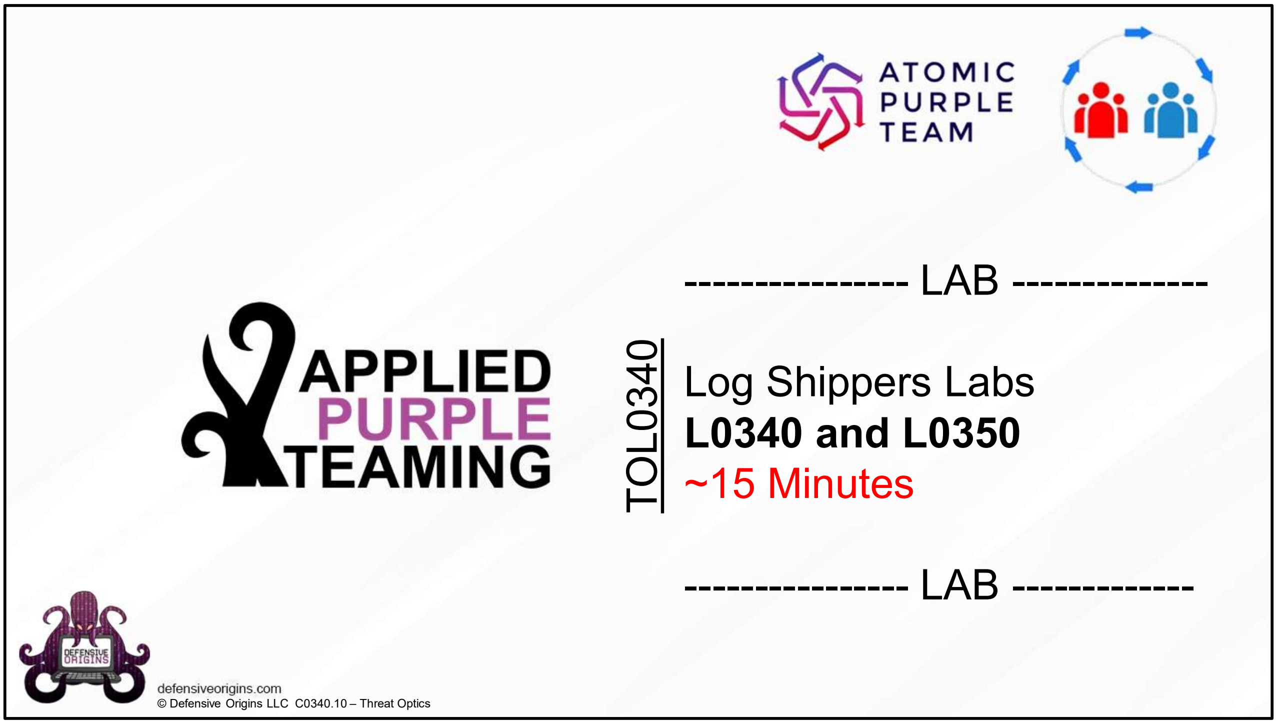
Configure Event Subscriptions
- Group event IDs in meaningful ways and create a subscription

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

defensiveorigins.com

© Defensive Origins LLC C0340.9 – Threat Optics


ATOMIC
PURPLE
TEAM
APPLIED
PURPLE
TEAMING
DEFENSIVE ORIGINS

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

TOL0340

Log Shippers Labs

L0340 and L0350

~15 Minutes

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

defensiveorigins.com

© Defensive Origins LLC C0340.10 – Threat Optics

Applied Purple Teaming – TOL340 Log Shippers Lab
L0340 & L0350
15 Minutes