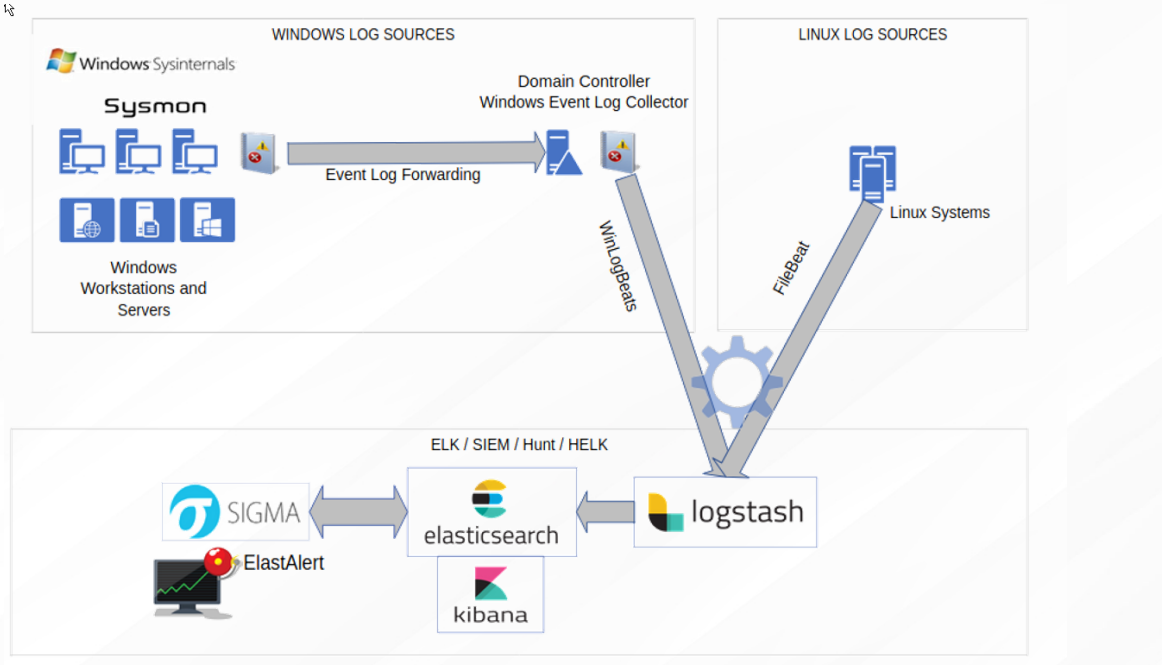
Applied Purple Teaming

Infrastructure, Threat Optics, and Continuous Improvement

June 6, 2020

LC0330

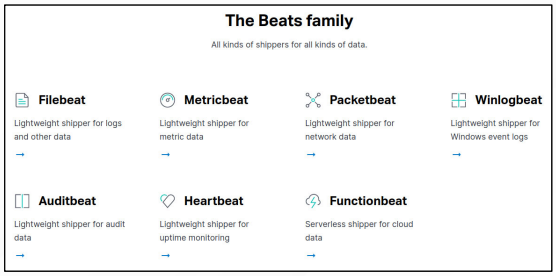
Log Shipping Event Ingestors



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)

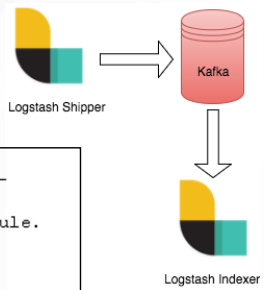
```
#----------------- Kafka output ---┼-------------------
#output.kafka:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # 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