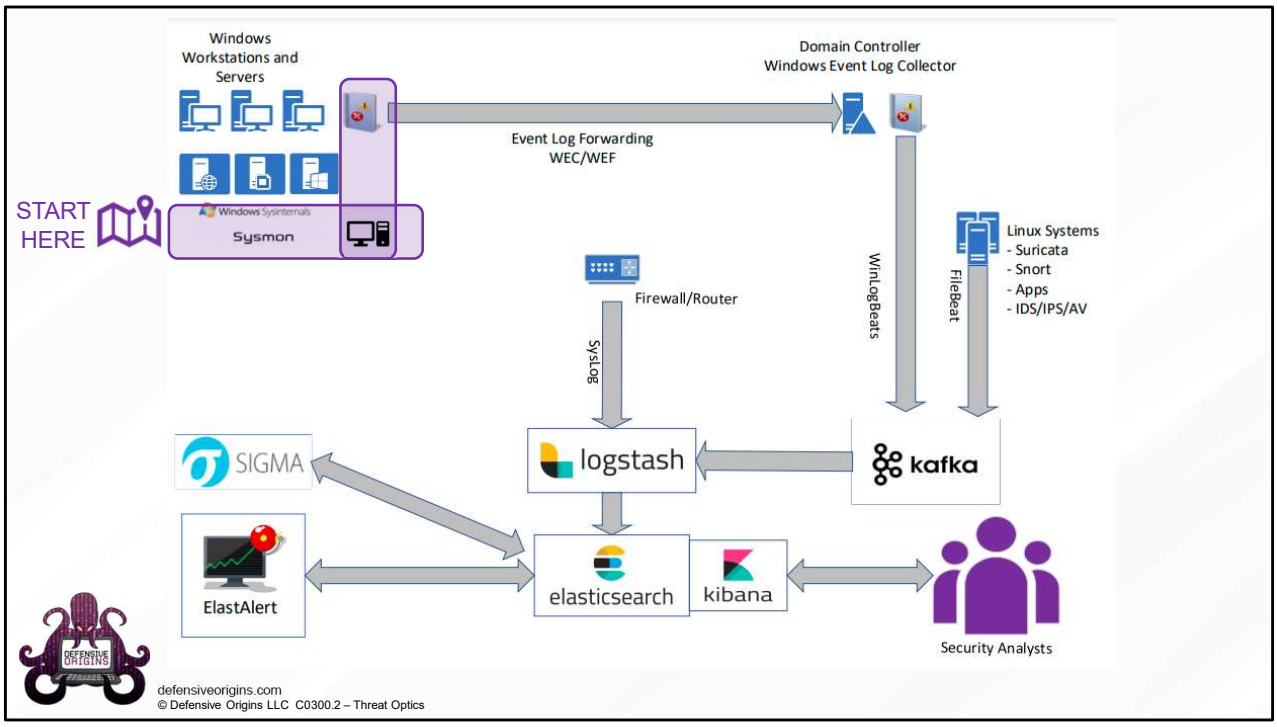
Applied Purple Teaming – C0300 Threat Optics Overview
Sysmon, Audit Policies, WEC/WEF, Log Shipping


Windows
Workstations and
Servers
Domain Controller
Windows Event Log Collector
Event Log Forwarding
WEC/WEF
START
HERE
Windows Sysinternals
Sysmon
Firewall/Router
Syslog
WinLogBeats
FileBeat
Linux Systems
- Suricata
- Snort
- Apps
- IDS/IPS/AV
SIGMA
logstash
kafka
ElastAlert
elasticsearch
kibana
Security Analysts
DEFENSIVE ORIGINS
defensiveorigins.com
© Defensive Origins LLC C0300.2 – Threat Optics

Threat Optics – Important Items

Some of you will not love the depth of this section.
OR
The amount of time we spend on it.

For some of you the labs will be easy and will take two minutes.

For others who have not deployed event logging, we are going to be patient.

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

Threat Optics – Our Perspective

We consider threat optics to be the following:

- A “present” where forensic investigators ask for and get everything they need
- A baseline of event monitoring across a Windows domain
- A pane of glass where analysts can query event log datasets
- An event log repository with useful data and limited blind spots
- A basis for functional relationships across disparate stakeholders
- More, so much more.

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