

Ingesting and Enriching Zeek Logs



Joe Abraham

Cybersecurity Consultant

@joeabrah www.defendthenet.com



ELK Stack



Elasticsearch is the search engine



Logstash ingests, stashes, and parses the data



Kibana provides GUI searches and visualizations



Beats are the data shippers for the stack



Our Uses for ELK Tools



ELK is installed on a virtual machine

Filebeat will gather and ship Zeek logs

Logstash will receive them

Kibana will be used for data validation

Logstash will parse and enrich the data for Arkime



What's Next?

Pluralsight Courses for ELK

Elastic Stack Fundamentals Path

**Getting Started with Endpoint Log
Analysis**

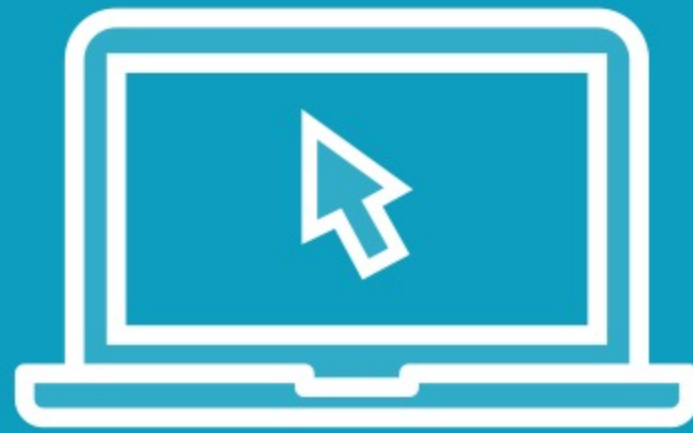
Configure the Components

**Logstash and Filebeat will be the focus
for the configurations in this module**

Use Kibana for data validation



Demo



**Configure and validate Zeek log ingestion
using Elastic Stack**



Stashing and Parsing Logs with Logstash





Logstash Capabilities

Multiple input formats and sources

Parse and transform data “on the fly”

Stash or send data

Uses plugins and extensions



Logstash.yml

```
# Settings file in YAML
#   pipeline:
#     batch:
#       size: 125
#       delay: 5
# Or as flat keys:
#
#   pipeline.batch.size: 125
#   pipeline.batch.delay: 5
#
# ----- Node identity -----
#
# Use a descriptive name for the node:
#
# node.name: test
#
# If omitted the node name will default to the machine's host name
#
# ----- Data path -----
#
# Which directory should be used by logstash and its plugins
# for any persistent needs. Defaults to LOGSTASH_HOME/data
#
path.data: /var/lib/logstash
#
# ----- Pipeline Settings -----
#
# The ID of the pipeline.
#
# pipeline.id: main
```


Sample Logstash Pipeline Configuration

```
input {
  file {
    path => "/home/ubuntu/apache-daily-access.log"
    start_position => "beginning"
    sincedb_path => "/dev/null" }
}
filter {
  grok {
    match =>
    { "message" => "%{COMBINEDAPACHELOG}" }
  }
  date {
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
  geoip {
    source => "clientip"
  }
}
output {
  elasticsearch {
    hosts => ["localhost:9200"]
  }
}
```



Integrating Zeek Log Data with Arkime



Arkime and Zeek can work
together to help close visibility
gaps



Maps Zeek fields to Arkime
Enrich data
View and search Zeek
logs in Arkime
Correlate data between
tools

Views			
Saved views provide an easier method to specify common base queries and can be activated in the search bar.			
Share	Name	Expression	Sessions Columns
<input type="checkbox"/>	Public IP Addresses	(country.dst == EXISTS!) (country.src == EXISTS!	
<input type="checkbox"/>	Zeek conn.log	zeek.logType == conn	
<input type="checkbox"/>	Zeek Exclude conn.log	zeek.logType == EXISTS! && zeek.logType != conn	
<input type="checkbox"/>	Zeek Logs	zeek.logType == EXISTS!	
<input type="checkbox"/>	PCAP Files	zeek.logType != EXISTS!	



What Do We Need?

Zeek instance running

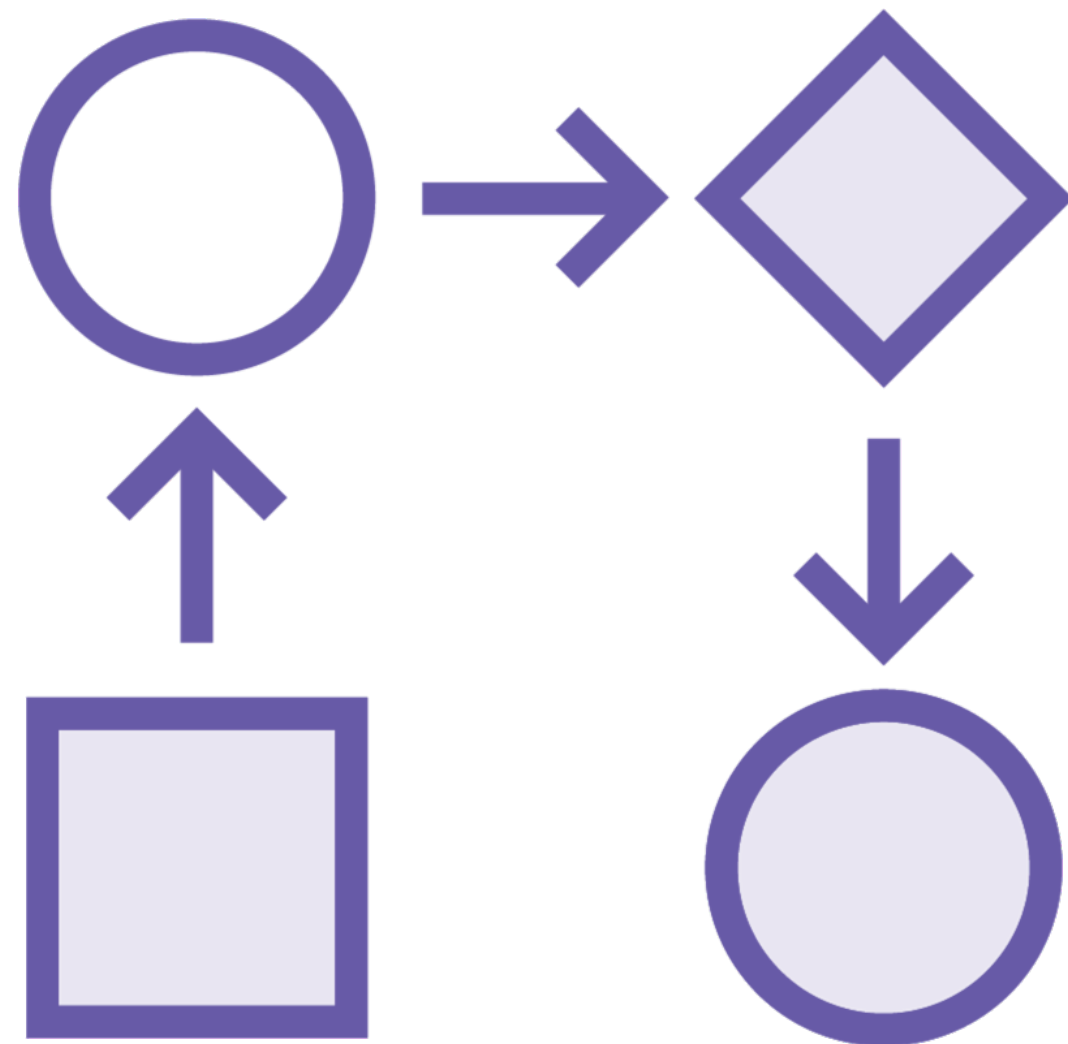
Elastic Stack ingesting Zeek logs

Arkime installed and running

- <https://arkime.com/learn>
- **Network Analysis with Arkime**



What Will We Do?



Malcolm

- Developed by CISA and INL
- Platform with many tools pre-packaged
 - Zeek, Arkime, ELK, etc.

Steps:

- View and configure Logstash for parsing
- Map Zeek's fields to Arkime's
- Enrich Zeek logs
- Create Arkime WISE data source
- Validate the integration

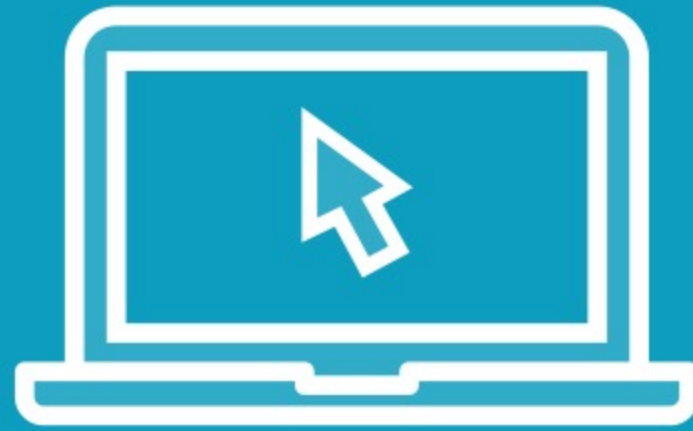
Follow Along with Malcolm or Your Install

<https://malcolm.fyi/>

<https://github.com/cisagov/Malcolm#ArkimeZeek>



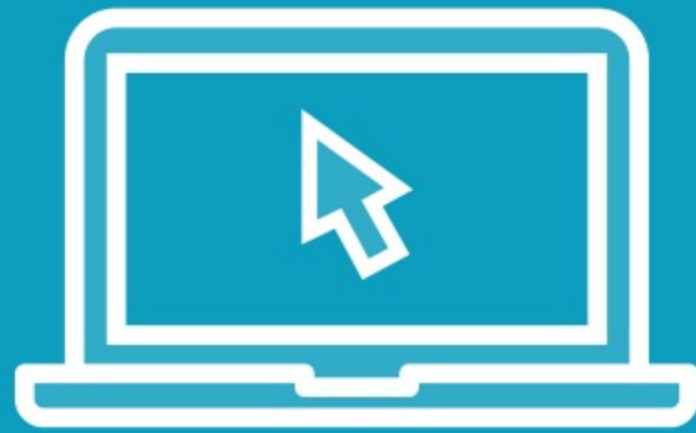
Demo



Configure Logstash for parsing and enriching Zeek logs



Demo



Configure Zeek data source in Arkime

Validate Zeek-Arkime integration



Up Next:
Integrating Zeek with RockNSM

