

Integrating Zeek with RockNSM



Joe Abraham

Cybersecurity Consultant

@joeabrah www.defendthenet.com



What's RockNSM?



Network sensor

Response Operation Collection Kit

Used for threat hunting and incident response

Integrates multiple tools like other platforms



RockNSM Tools

Zeek

Suricata

Google Stenographer

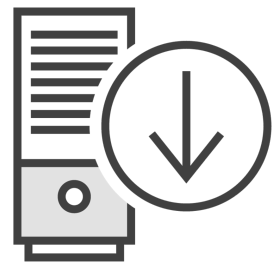
Docket

Apache Kafka

Elastic Stack



How Does Zeek Fit In?



Zeek is deployed using RockNSM and Zeek default configurations



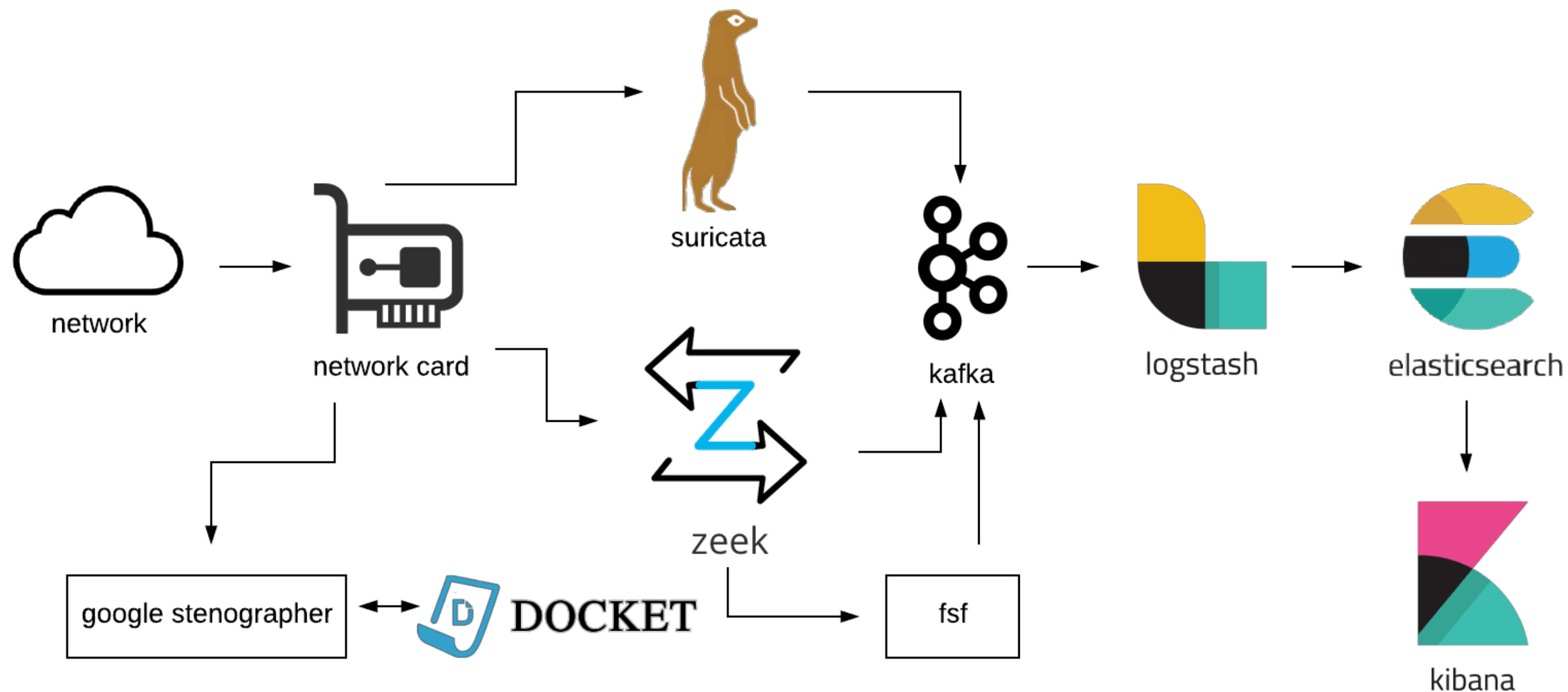
Zeek logs are sent to Kafka and Logstash



Zeek provides protocol analysis, metadata, alerting, and more



RockNSM Architecture



RockNSM Configuration

local.zeek

```
...
# Detect SHA1 sums in Team Cymru's Malware Hash Registry.
@load frameworks/files/detect-MHR

# Extend email alerting to include hostnames
@load policy/frameworks/notice/extend-email/hostnames

# Uncomment the following line to enable detection of the heartbleed attack. Enabling
# this might impact performance a bit.
# @load policy/protocols/ssl/heartbleed

# Uncomment the following line to enable logging of connection VLANs. Enabling
# this adds two VLAN fields to the conn.log file.
# @load policy/protocols/conn/vlan-logging

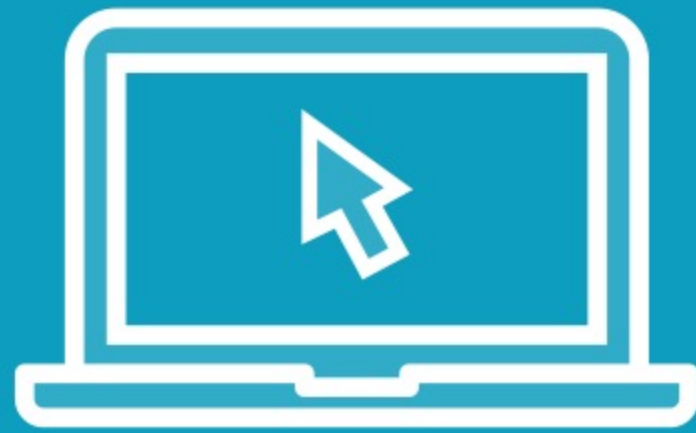
# Uncomment the following line to enable logging of link-layer addresses. Enabling
# this adds the link-layer address for each connection endpoint to the conn.log file.
# @load policy/protocols/conn/mac-logging
@load scripts/rock # ROCK NSM customizations
@load scripts/rock/plugins/kafka
```



Ansible is used for deployment
configurations



Demo



[View RockNSM implementation of Zeek](#)



File Carving with Zeek



File Carving

The reconstruction of computer files that takes place without helpful metadata indicators or other specific guidance



Why Use File Carving?

Conduct additional analysis on the files being transmitted

Keeping a record of the files or to use with digital forensic investigations

File recovery in case of storage failure





File Analysis Framework





File analysis framework presents and passes file information to other frameworks or tools to be used



Zeek File Extraction Package

file-extraction

<https://github.com/hosom/file-extraction>

 12  84  43  0 Last Push 3/17/20, 12:51 PM

Module for File Extraction

This is a Zeek package that provides convenient extraction of files.

As a secondary goal, this script performs additional commonly requested file extraction and logging tasks, such as naming extracted files after their calculated file checksum or naming the file with its common file extension.

Installing with zkg (preferred)

This package can be installed through the [zeek package manager](#) by utilizing the following commands:

```
zkg install zeek/hosom/file-extraction

# you must separately load the package for it to actually do anything
zkg load zeek/hosom/file-extraction
```

Installing manually

While not preferred, this package can also be installed manually. To do this, follow the tasks below:

```
cd <prefix>/share/zeek/site

git clone git://github.com/hosom/file-extraction file-extraction

echo "@load file-extraction" >> local.zeek
```

Configuration

The package installs with the **extract-common-exploit-types.zeek** policy, however, additional functionality may be desired.

Configuration must **always be done within the config.zeek** file. Failure to isolate configuration to **config.zeek** will result in your configuration being overwritten.

To download to your Zeek instance: `zkg install zeek/hosom/file-extraction`



Demo



Configure Zeek to extract and save files



Module Summary



Detailed RockNSM configurations for Zeek

- Configurations
- Uses
- Dashboards

File carving with Zeek

- Custom scripts
- Prebuilt packages



Up Next:
Using Intelligence in Zeek

