

# Tracking Zeek's Discoveries

---



**Joe Abraham**

NETWORK SECURITY CONSULTANT

@joeabrah [www.joeabrahamtech.com](http://www.joeabrahamtech.com)

# Overview

**Review of previous modules**

**Discussing Zeek outputs**

**Course wrap up!**

What's up  
with Zeek?

**Uses scripts as its policy engine**

**Use default or custom scripts**

**Can install as standalone or cluster**

**Passive tool!**

**Looks for protocol behavior, file  
content, and much more**

# Zeek Deployments

## Standalone

Only node in the deployment

No other Zeek instances

## Cluster

Multiple Zeek nodes

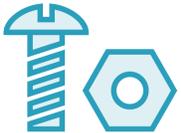
One manager, multiple  
sensors

Uses ZeekControl

# Zeek Capabilities



Frameworks allow us to do specific things within the Zeek system and each one has its purpose



Subcomponents give Zeek specific functionality and efficiency, and make up the Zeek ecosystem



Plugins add functionality to the system that isn't already built in. Adds APIs and scripts as needed.

# Signature Framework



**Gives Zeek signature analysis/rule-based functionality**



**Write specific criteria for events or traffic to match; alert or other action invoked after signature is tripped**

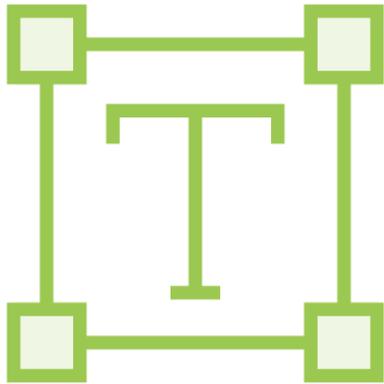


**More like typical IDS with rules based on type of traffic, header information, contents of payload**

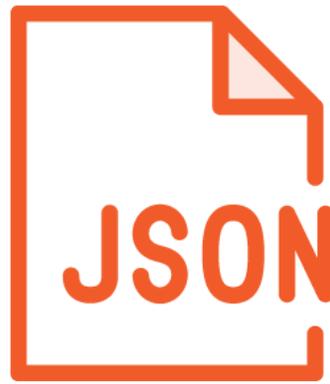
# Zeek Outputs

---

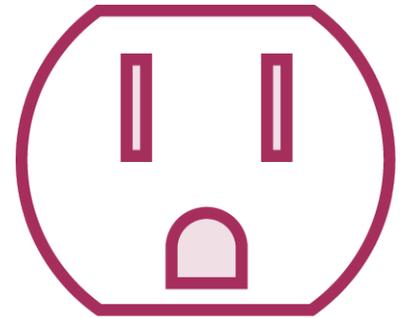
# Logging Framework



ASCII Logs



JSON Format



Expanded Using  
Plugins

# Notice Framework



**Alerts and Logs**



**Emailed Notifications**

# Demo

**Look at ASCII log in Splunk**

**Configure JSON format**

**Look at JSON log in Splunk**

# Summary

**Reviewed previous modules**

**Logging and notice frameworks**

**Demo converting ASCII to JSON**

**Course wrap up!**

Thank You!