

Detailing the Zeek Components



Joe Abraham

NETWORK SECURITY CONSULTANT

@joeabrah www.joeabrahamtech.com

Overview

Zeek frameworks

Zeek subcomponents

Plugins

Network Monitoring Solution



Security or network functionality monitoring

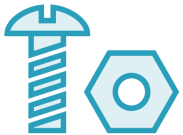
Many frameworks, components, and plugins to expand the tool

Modular solution to add features

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.



Configuration Framework

Change configuration without restarting

- Changes occur within files
- Zeek monitors configuration files
- Changes can be made at runtime

City or country
database from GeoLite2

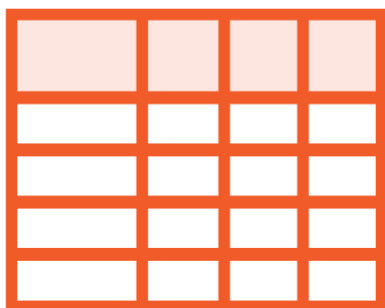
IP based

Intelligent policy
creation

Adds context to data



Input Framework



Tables

Define fields and values in tables
for Zeek to read



Data Streams

Dynamic data such as IP
blacklists and event streams for
ingestion

Logging Framework

ASCII logs sent to
SIEMs and other
syslog receivers

SQLite databases

External plugins
and APIs (JSON)

**Perform actions based on
events**

Drop connections

Stop routing/forwarding

Redirect flows

Many more!

NetControl Framework

Other Frameworks

**File Analysis
Framework**

**Intelligence
Framework**

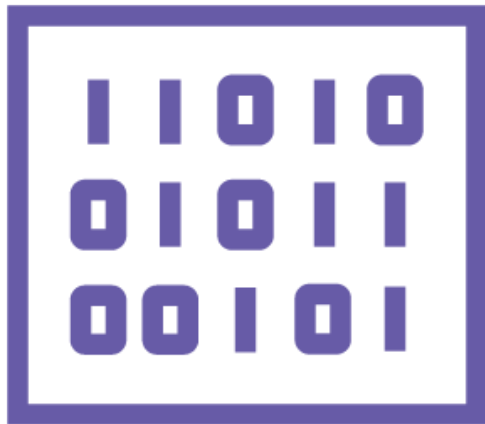
Notice Framework

**Signature
Framework**

**Summary Statistics
Framework**

**Broker-enabled
Communication and
Cluster Framework**

Zeek Subcomponents

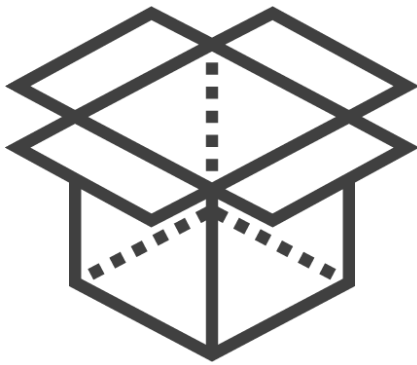


Capstats

Monitor network interface usage

- Analyze utilization and saturation
- Statistics (pps, bandwidth, data amount)
- Packets per protocol (TCP, UDP, etc.)

Zeek Package Manager



CLI tool to install/manage packages and scripts

Can automatically pull from Git repo

Anyone can request their code be uploaded to the repo!

Zeek Broker



Used for logging and alerting based on events and scripts



Distributes messages to subscribers based on publisher/subscriber model



Fine-tune messages and formats used within Zeek

Other Subcomponents

BinPAC

Zeek-aux

BTest

PySubnetTree

ParaGlob

Trace-summary

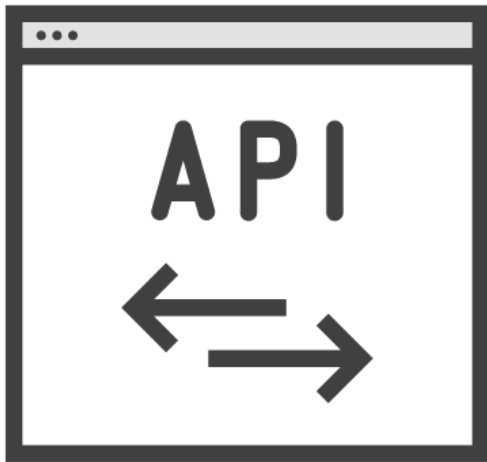
Zeek Plugins



Adds additional scripts, analyzers, logging formats, etc.

Pull in additional information for scripts to process

Add capabilities to the Zeek system

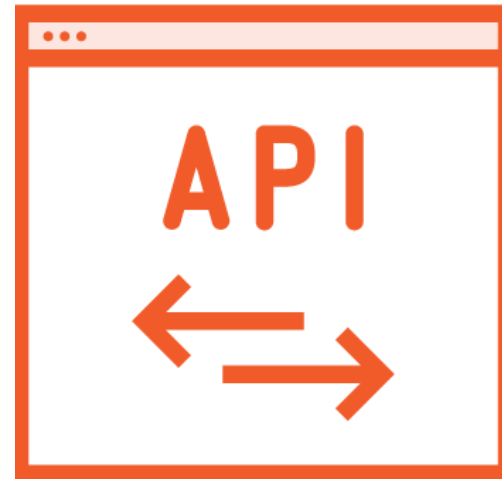


Integration and Sharing of Information

Write code according to Zeek standards

- Utilize python if desired!

What can you think of?
Custom attack detection
Look at signatures
Change alerting



Module Recap

Summary

Zeek frameworks

Zeek subcomponents

Plugins

Coming up: Learning Zeek's
Language