

Using Zeek in the Enterprise



Joe Abraham

NETWORK SECURITY CONSULTANT

@joeabrah www.joeabrahamtech.com

Overview

Zeek deployment types

The Zeek engine

ZeekControl

Installation and configuration

- **Demo**

Zeek Deployments

Standalone

Only node in the deployment

No other Zeek instances

Cluster

Multiple Zeek nodes

One manager, multiple
sensors

Uses ZeekControl



Cluster Deployment

Benefits include:

- Scalability
- Ease of management

ZeekControl

Interactive shell for easily operating/managing Zeek installations on a single system or even across multiple systems in a traffic-monitoring cluster.

-Zeek Documentation Library

ZeekControl

ZeekControl Version 2.0.0

capstats [<nodes>] [<secs>]	- Report interface statistics with capstats
check [<nodes>]	- Check configuration before installing it
cleanup [--all] [<nodes>]	- Delete working dirs (flush state) on nodes
config	- Print zeekctl configuration
cron [--no-watch]	- Perform jobs intended to run from cron
cron enable disable ?	- Enable/disable "cron" jobs
deploy	- Check, install, and restart
df [<nodes>]	- Print nodes' current disk usage
diag [<nodes>]	- Output diagnostics for nodes
exec <shell cmd>	- Execute shell command on all hosts
exit	- Exit shell
install	- Update zeekctl installation/configuration
netstats [<nodes>]	- Print nodes' current packet counters
nodes	- Print node configuration
peerstatus [<nodes>]	- Print status of nodes' remote connections
print <id> [<nodes>]	- Print values of script variable at nodes
process <trace> [<op>] [-- <sc>]	- Run Zeek with options and scripts on trace
quit	- Exit shell
restart [--clean] [<nodes>]	- Stop and then restart processing
scripts [-c] [<nodes>]	- List the Zeek scripts the nodes will load
start [<nodes>]	- Start processing
status [<nodes>]	- Summarize node status
stop [<nodes>]	- Stop processing
top [<nodes>]	- Show Zeek processes ala top

The Zeek Engine

Zeek's Event Engine



Takes raw packets and uses analyzers to look at traffic to identify events that may be occurring

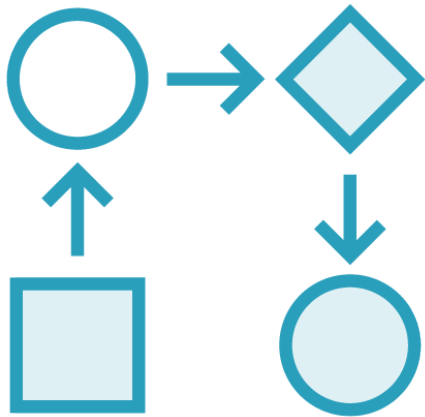


Only analyzes traffic; Analyzers include transport layer, application layer, and infrastructure analyzers



Also tracks connections to identify suspicious behavior

Policy Script Interpreter



Uses scripts to decide how to handle events

Can use defaults or customize as needed

Event-driven scripting language

Notification or alert is generated based on event criteria

Zeek Installation and Configuration

Zeek on Unix

**Linux Platforms such as Red
Hat, Debian, FreeBSD**

**Mac OS X with Xcode or
Command Line Tools**

Libpcap
OpenSSL libraries
BIND8 library
Libz
Bash
Python 2.6 or later



Use Security Onion to learn
Zeek and other network
security tools!

www.securityonion.net

Demo

Installing prerequisites and updating packages

User and group configuration

Zeek installation and verification

Module Recap

Summary

Zeek deployment options

ZeekControl

Zeek's event engine and policy script interpreter

Zeek installation and configuration

- **Demo**

Coming up: Zeek's
components