# Getting Started with Zeek

## DISCOVERING ZEEK'S CAPABILITIES

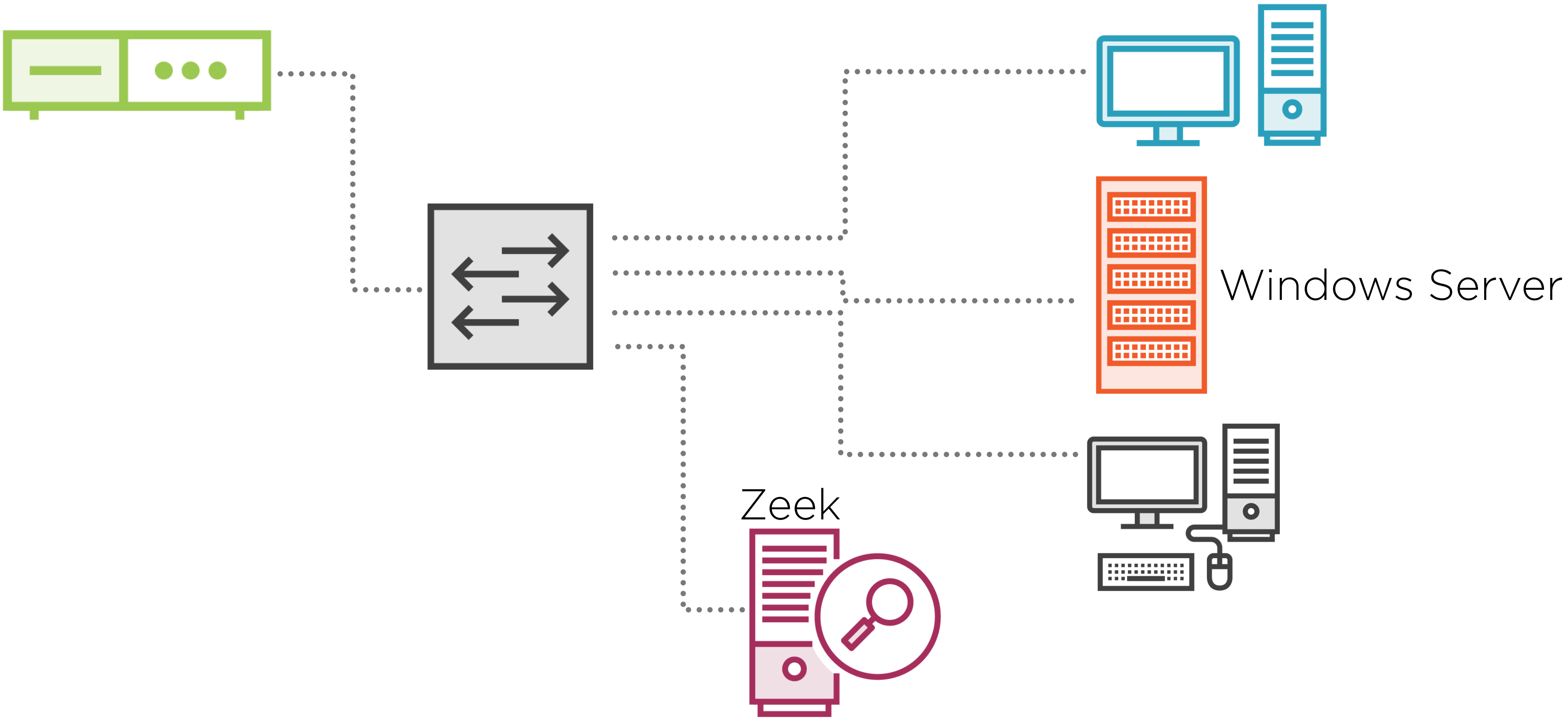
Joe Abraham
NETWORK SECURITY CONSULTANT
@joeabrah www.joeabrahamtech.com

# What is Zeek?

Formerly known as “Bro,” Zeek is an open-source network traffic analyzer inspecting all traffic on a link for signs of suspicious activity.

-Zeek Documentation Library

# Globomantics' Network



# Globomantics

You work for Globomantics

Improve networ es with open-source tools

Corrected the body again.

You need to learn Zeek so that you can determine its appropriateness and learn how to use it effectively

# Overview

**Introduction to Zeek**

- Features, benefits, uses, history

Using Zeek in the enterprise

- Engine and controlling the tool

Zeek components

- Frameworks, sub components, plugins

Zeek’s language

Zeek’s outputs and reporting

# Course Prerequisites

**Have good understanding of:**

Typical organization endpoints and devices

Network protocols

Desire to learn Zeek!

# How You Can Follow Along

Have operating system capable of

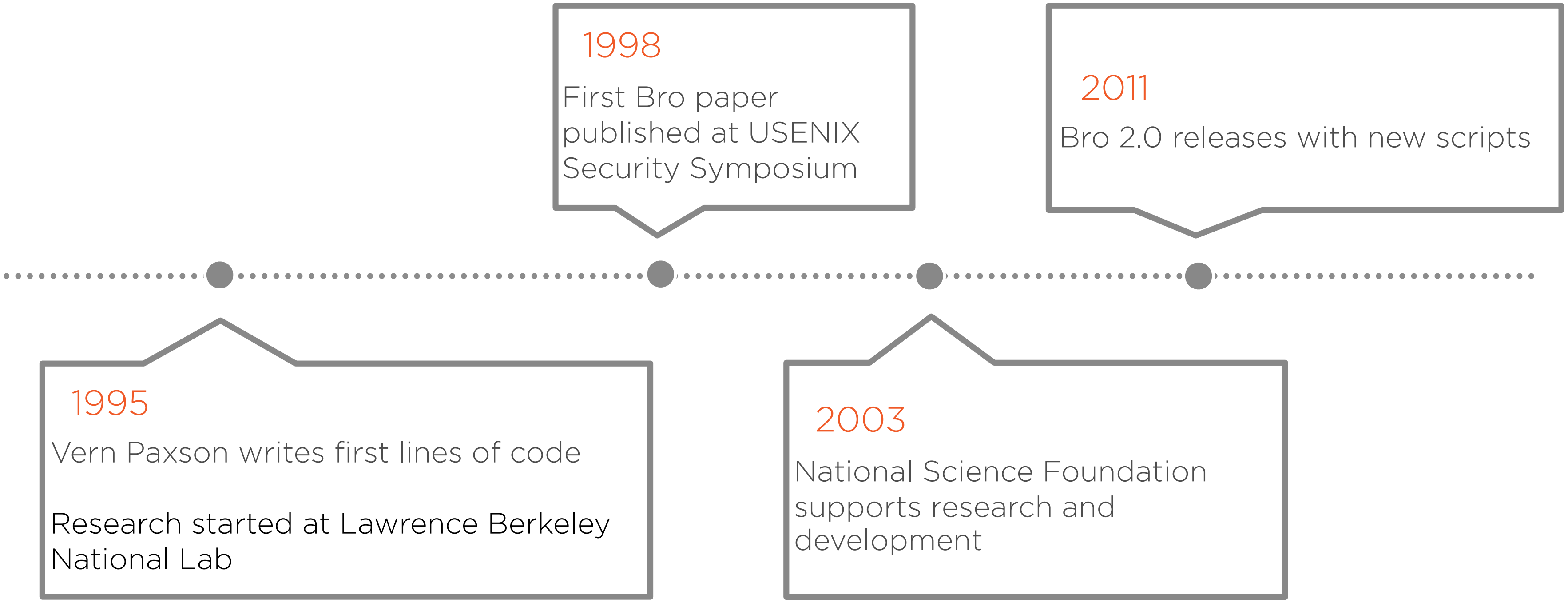
Zeek

traffic from at least one

I corrected this slide to better fit with the template. Please keep in mind that the main body of the slide should be Gotham medium. This makes it much easier to read for most learners, especially when printing.

# What Is Zeek?

# Short Zeek History



1995

Vern Paxson writes first lines of code

Research started at Lawrence Berkeley National Lab

1998

First Bro paper published at USENIX Security Symposium

2003

National Science Foundation supports research and development

2011

Bro 2.0 releases with new scripts

# 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 outputs:**

ASCII Logs

JSON

SQLite Databases

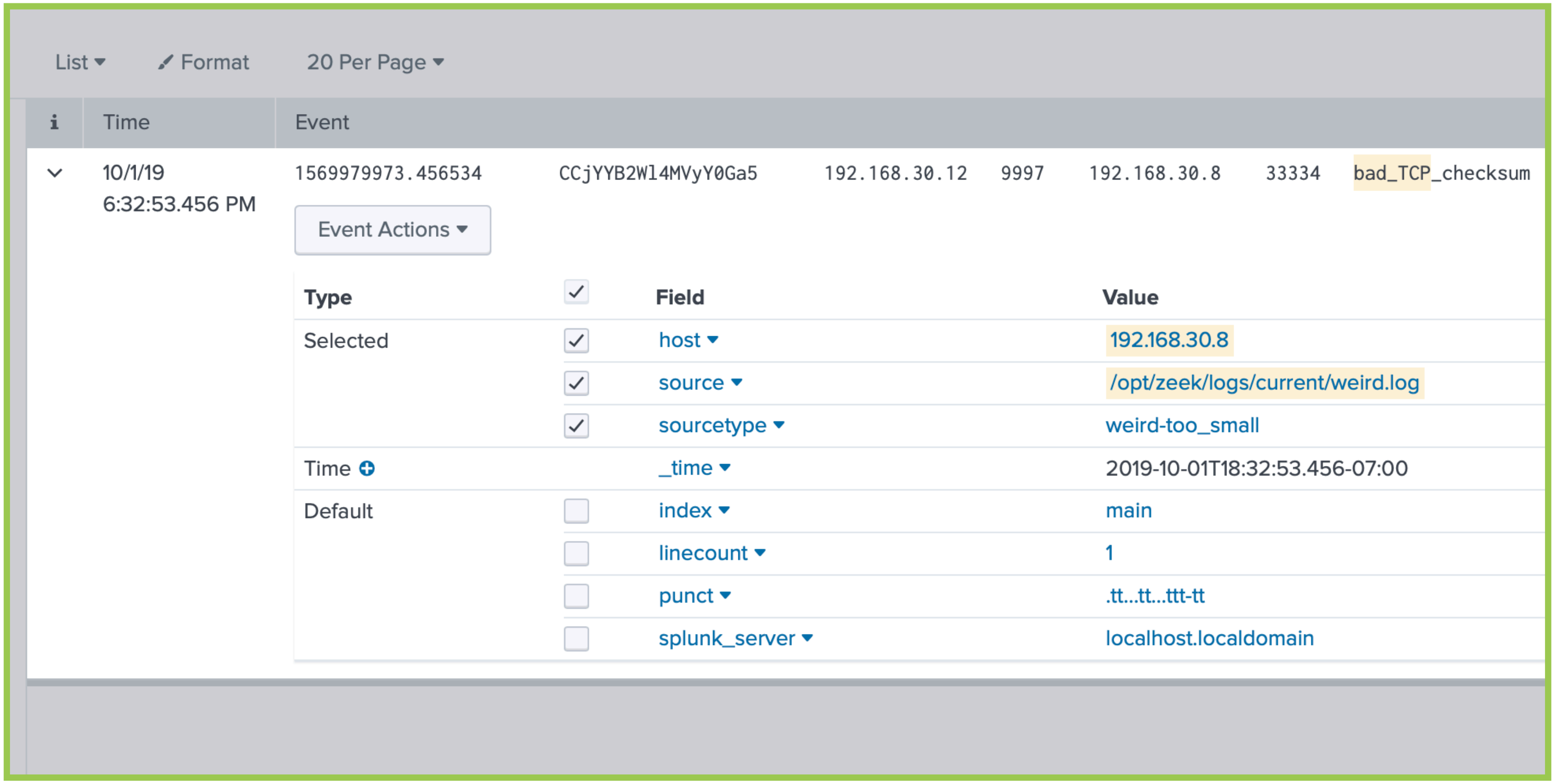
External Plugins

# Zeek Use Cases

# Network Monitoring

Looking at the protocols, files, conversations, and other components of your environment and the functionality of it all.

# Zeek’s weird.log



| Time | Event |
|---|---|
| 10/1/19 6:32:53.456 PM | `1569979973.456534    CCjYYB2Wl4MVyY0Ga5    192.168.30.12    9997    192.168.30.8    33334    bad_TCP_checksum` |

| Type | ✓ | Field | Value |
|---|---|---|---|
| Selected | ☑ | host ▾ | 192.168.30.8 |
| | ☑ | source ▾ | /opt/zeek/logs/current/weird.log |
| | ☑ | sourcetype ▾ | weird-too_small |
| Time ⊕ | | _time ▾ | 2019-10-01T18:32:53.456-07:00 |
| Default | □ | index ▾ | main |
| | □ | linecount ▾ | 1 |
| | □ | punct ▾ | .tt...tt...ttt-tt |
| | □ | splunk_server ▾ | localhost.localdomain |

# Zeek Documentation:

docs.zeek.org

# Summary

Course introduction and overview

What is Zeek?

Zeek demonstration