

# Extensions, Frameworks & Integrations Used with Zeek

---

## Identifying Zeek Integrations



**Joe Abraham**

Cybersecurity Consultant

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



# Zeek Integrations

**Security Onion**

**Arkime**

**RockNSM**



# Zeek

**Zeek is a passive, open-source network traffic analyzer**

<https://docs.zeek.org/en/current/about.html>



# What You'll Learn Here

**Zeek Integration  
Capabilities**

**Integrating Zeek  
with Security Onion**

**Zeek with ELK and  
Arkime**

**Zeek and RockNSM**

**Zeek Intelligence  
Framework**

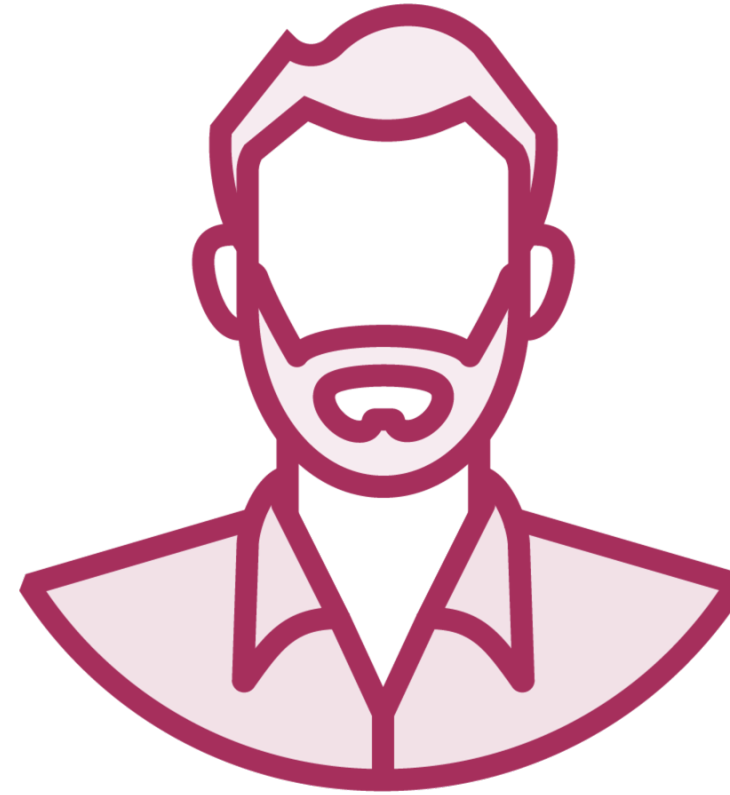


# Meet the Team



**Katrina**

Globomantics' Security Engineer



**Chris**

Globomantics SOC Analyst





## More information

### Utilizing Zeek in an Enterprise Environment or for Distributed Operations

Michael Edie



# Customizing Zeek Using Integrations

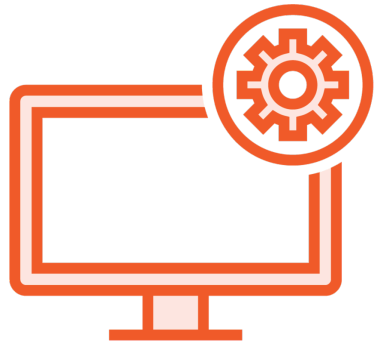
---



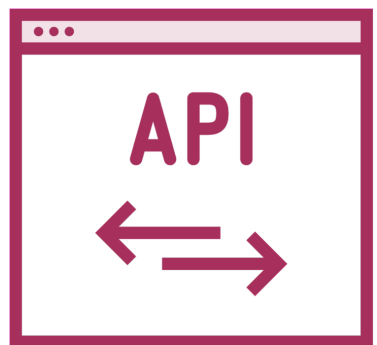
# Additional Frameworks in Zeek



**Input framework reads data from sources into events or tables**



**Configuration framework allows us to change the runtime configuration without modify scripts directly**



**Netcontrol framework provides the API functionality for Zeke**





Zeek add-ons can include  
packages, scripts and tools, or  
other projects



# The Framework's Components

## Projects

Larger add-ons and packages that provide new features

## Extension Scripts

Additional scripts to write or download that expand the Zeek capabilities



# Adding Zeek Packages

---



# Zeek Package Downloads

## **Zeek Package Browser**

<https://packages.zeek.org/packages>

## **Zeek Package GitHub**

<https://github.com/zeek/packages>



# Interesting Zeek Packages



**ukncsc/zeek-plugin-ikev2**  
IKEv2 analyzer



**corelight/got\_zoom**  
Detects Zoom meeting information



**amarokinc/bad-asn**  
Performs ASN lookups on remote connection IP addresses

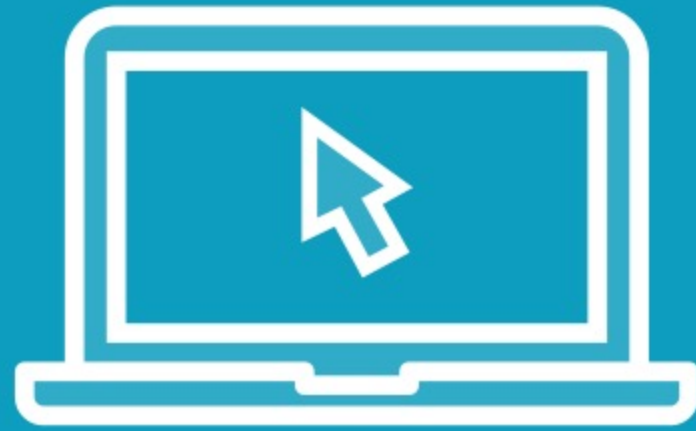


# Zeek Package Installation

**<https://docs.zeek.org/projects/package-manager/en/stable/quickstart.html>**



# Demo



**Explore extensions and frameworks**

**Install packages using package manager**



# Additional Zeek Projects

---





# Placeholder for package scrolling



# Zeek Agent

**For Linux and macOS**

**Reports endpoint information to Zeek**

- **File events**
- **Socket events**
- **Process events**

**Can interface with `osquery`**

- **Provides additional endpoint information for Zeek to use**
- **Uses API to connect to Zeek**



# What is Spicy?

A custom parser generator

Uses C++ to create parsers

Provides new protocol and file analyzers

No need to know or learn C++

Package manager can install new Spicy-based analyzers



# Demo



**Explore Spicy's installation**

**Validate Spicy analyzers**





## Module Review

**We can expand Zeek's capabilities with or without integrating other technologies**

**Extensions can be added through scripts, packages, projects, and other add-ons**



Up Next:

Deploying Zeek with Security Onion

---

