

# Deploying Zeek with Security Onion

---



**Joe Abraham**

Cybersecurity Consultant

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



# Viewing Zeek Logs

## Kibana

Front end tool for Elasticsearch,  
providing search and visualization  
support

## Hunt

Security Onion Console interface,  
allowing you to hunt through the data in  
Elasticsearch



Zeek Intelligence Framework  
can be used to add context or  
intel data



# Zeek Custom Scripts

**Can add custom scripts to so-zeek deployment**

**Add additional configuration parameters such as:**

- New scripts**
- Modify local.zeek script**
- Turn on/off protocol analyzers**



# Salt



**Manages Zeek Configurations**

**Documentation:**

**<https://docs.saltstack.com/en/latest/>**

**Used for infrastructure management**

- Filebeat**
- Firewalls**
- Alerting**
- Suricata**
- Zeek**

**YAML format**



# Zeek Salt Configurations



Salt manages **local.zeek**, **node.cfg**, and **zeekctl.cfg** files



Local .sls file: `/opt/so/saltstack/local`



Default .sls file: `/opt/so/saltstack/default/pillar/zeek/init.sls`



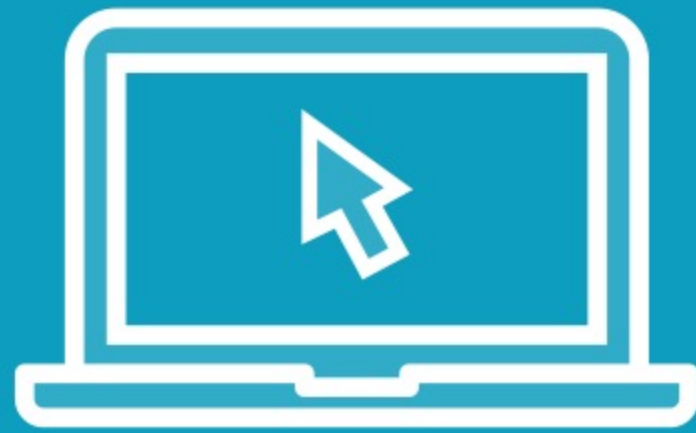


# Zeek Logs in Security Onion

Logs will be in /nsm/zeek/logs/ within Security Onion



# Demo



**Identify Zeek default configurations**

**Modify Zeek salt configurations**



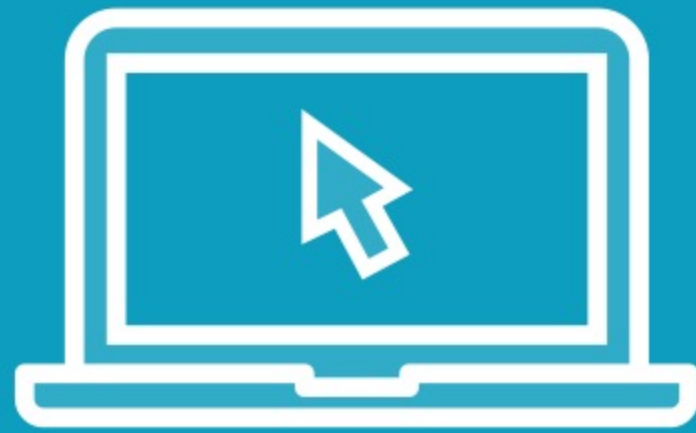
# Demo



## Validate Zeek data ingestion using Kibana



# Demo



## Validate Zeek data ingestion using Hunt



# Module Summary



**Zeek is a container within Security Onion**

**Configuration changes use salt**

- YAML-based

**Hunt and Kibana are used to view the Zeek logs**



# Security Onion Documentation

<https://docs.securityonion.net/en/2.3/zeek.html>



Up Next:

Ingesting and Enriching Zeek Logs

---

