

Using Zeek for Continuous Monitoring



Michael Edie

Security Engineer

@tankmek blog.edie.io

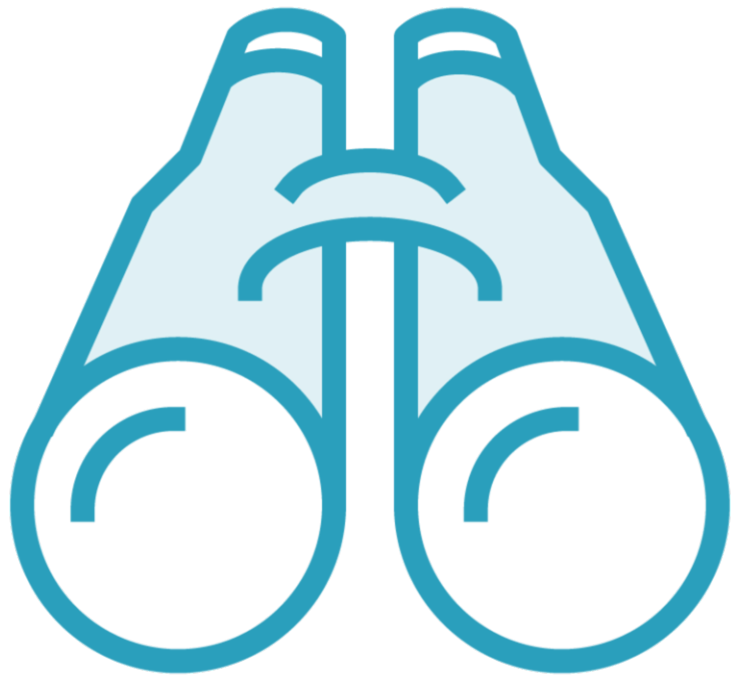


Continuous Monitoring (CM)

Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.



Continuous Monitoring



Maintaining situational awareness

Understanding of threats and threat activities

Assessing all security controls

Collecting, correlating, and analyzing security-related information

Asset Inventory

Actively manage all enterprise assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments.



Asset Inventory



Automated discovery

DHCP logging

Portable devices

New equipment acquisition

Software and versions

Continuous Monitoring Gaps

**Rogue server
detection**

**SSL Certificate
auditing**

DNS auditing



Rogue Server Detection



Authorized servers list and subnet(s)



Zeek connection log



Zeek DHCP log



```
"ts": 1621553236.650258,  
"uid": "ClVE2f4xsC2qjfIBgl",  
"id.orig_h": "192.168.50.14",  
"id.orig_p": 44880,  
"id.resp_h": "192.168.28.6",  
"id.resp_p": 8089,  
"proto": "tcp",  
"orig_pkts": 16,  
"orig_ip_bytes": 1216,  
"resp_pkts": 0,  
"resp_ip_bytes": 0
```

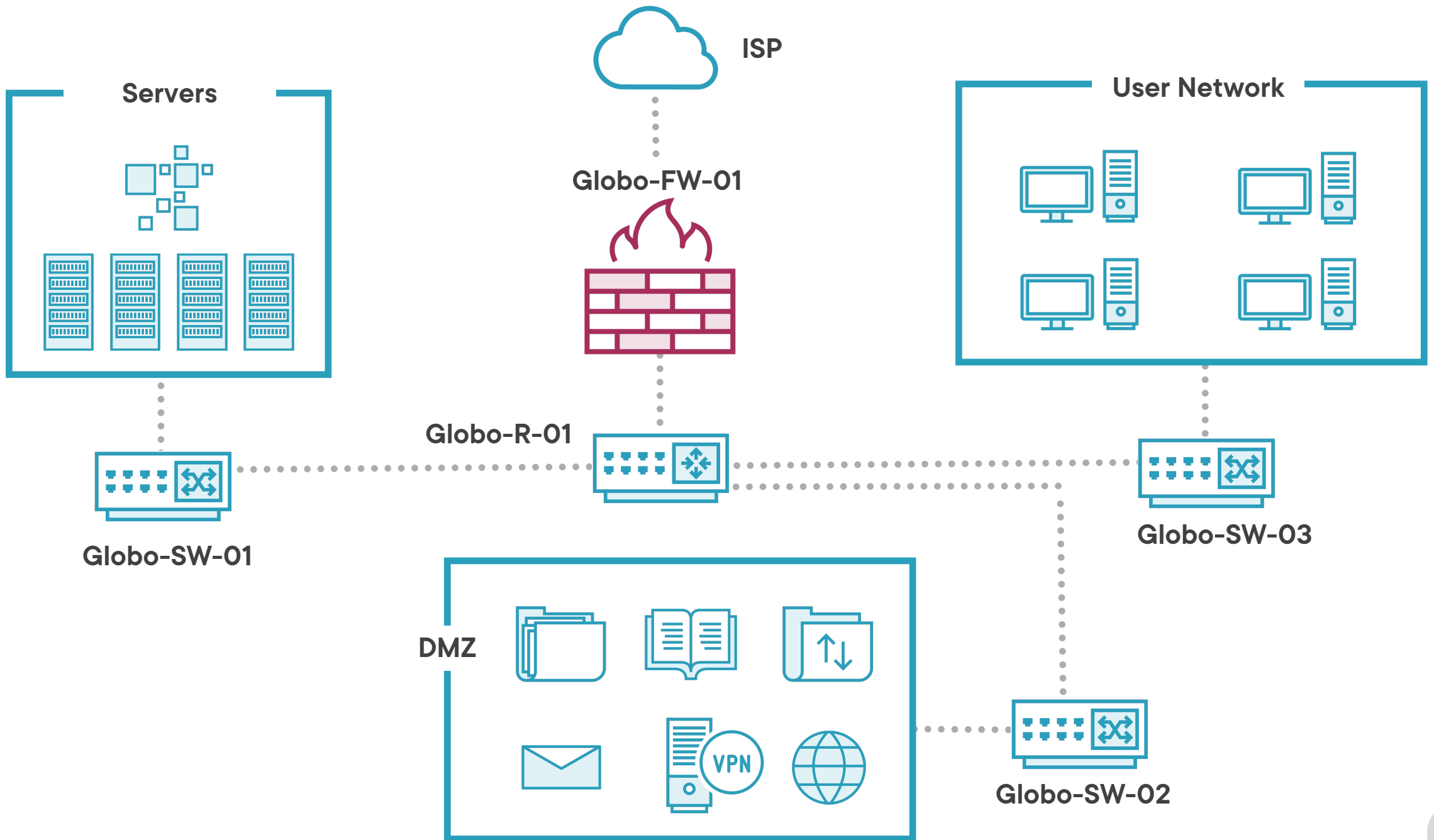
conn.log

Holds layer 3 and layer 4 metadata from the network traffic captured. Can also be viewed as the information about which systems are communicating on the monitored network.


```
"uids": [  
    "CW2Gvu1o8Cim5WWAS1"  
],  
"mac": "56:6f:b6:f3:00:88",  
"host_name": "HINATA",  
"client_fqdn": "HINATA.globomantics.com",  
"requested_addr": "192.168.27.15",  
"msg_types": [  
    "REQUEST",  
    "REQUEST"  
],  
"duration": 2.4080276489257812e-05
```

dhcp.log

Provides IP and MAC address mappings for systems utilizing the DHCP Protocol. The Discover, Offer, Release, and Acknowledge (DORA) message types are all captured along with any DHCP Servers providing leases on the network.



Servers



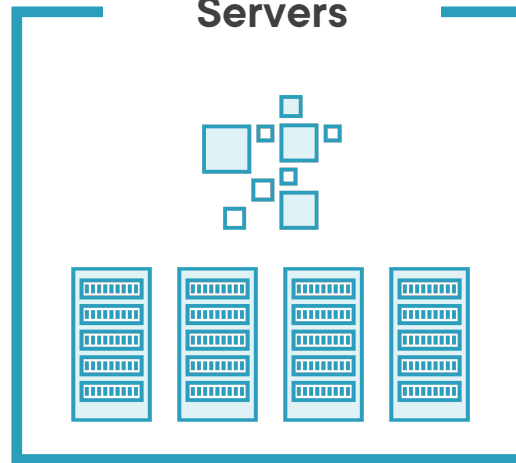
DMZ



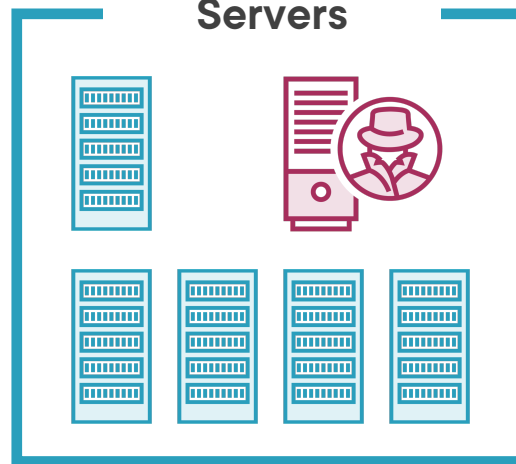
User Network



Servers



Servers



```
PUT _watcher/watch/cm_rogue-srv01
{
  "trigger": {
    "schedule": {"interval": "1h"}
  },
  "input": {
    "search": { "request": { "indices": [ "filebeat*" ],
    "body": {
      "query": { "bool": {
        "must": { "term": { "source.ip": "192.168.28.0/27" } } },
        "must_not": { "terms": { "source.ip":
          [ "192.168.28.10", "192.168.28.7", "192.168.28.2",
            "192.168.28.12", "192.168.28.15", "192.168.28.18" ] } } } } }
```

Watcher API

You add watches to automatically perform an action when certain conditions are met. The conditions are generally based on data you've loaded into the watch, also known as the Watch Payload.

```
}, "extract": ["hits.total.value"]}  
},  
"condition": {  
  "compare" : { "ctx.payload.hits.total" : { "gt" : 0 } }  
}, "actions" : {  
  "send_email" : {  
    "throttle_period": "2h",  
    "email" : {  
      "to" : "security@globomantics.com",  
      "from": "watcher@globomantics.com",  
      "subject" : "Watcher Notification",  
      "body" : "{{ctx.payload.hits.total}} error logs found"    }    }
```

Watcher API

Actions have access to the payload in the execution context. They can use it to support their execution in any way they need. For example, the payload might serve as a model for a templated email body.

SSL Certificate Auditing



SSL Certificate Auditing



Authorized SSL/TLS certificates list



Zeek SSL/TLS log



Zeek x509 log



```
"ts": 1621562247.877147,  
"id.orig_h": "192.168.27.14",  
"id.orig_p": 62393,  
"id.resp_h": "8.43.72.113",  
"id.resp_p": 443,  
"version": "TLSv12",  
"cipher": "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",  
"curve": "secp256r1",  
"cert_chain_fuids": [  
    "FhBDiv3bpJlrXbRrs1",  
    "F0EoBtZWAMZ52PcE5"],  
"validation_status": "ok"
```

ssl.log

This log will parse the various version of TLS and store the metadata from the encrypted traffic. The Secure Sockets Layer (SSL) name is a carry over from the now deprecated protocol.

```
"ts": 1621563013.8525,  
"certificate.serial": "049DA07D908F3A4C2509CDB1C38F26220119",  
"certificate.subject": "CN=gnu.org",  
"certificate.issuer": "CN=R3,O=Let's Encrypt,C=US",  
"certificate.not_valid_before": 1619726196,  
"certificate.not_valid_after": 1627502196,  
"certificate.key_alg": "rsaEncryption",  
"certificate.sig_alg": "sha256WithRSAEncryption",  
"certificate.key_type": "rsa",  
"certificate.key_length": 2048,  
"san.dns": ["archive.gnewsense.org", "www.playogg.net", "www6.gnu.org"],  
"basic_constraints.ca": false
```

x509.log

Captures details on certificates exchanged during certain TLS negotiations. There will be no x509 log for TLS 1.3 connections.

SSL Certificate Auditing

Certificates provide a lot of details that can be inventoried and monitored.



Certificate Authority

Monitor for certificates not signed by a trusted third party.



Ciphers or hashes

Avoid weak, insecure or deprecated versions

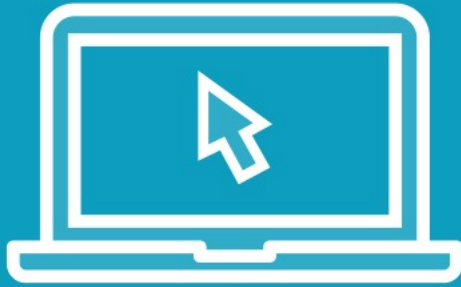


Expired certificates

Should not exist.



Demo



SSL Certificate Auditing

- Enumerate SSL fields in Elasticsearch
- Generate certificate baseline
- Create alert for new certificates
- Trigger alert with unauthorized certificate



DNS Auditing



DNS Auditing



Authorized domains and subdomains list



Zeek DNS log



Zeek connection log



```
"ts": 1621560879.911037,  
"id.orig_h": "192.168.50.14",  
"id.orig_p": 52400,  
"id.resp_h": "192.168.50.1",  
"id.resp_p": 53,  
"proto": "tcp",  
"query": "ntp.ubuntu.com",  
"answers": [  
    "91.189.89.198",  
    "91.189.91.157",  
    "91.189.89.199",  
    "91.189.94.4" ]
```

dns.log

All unencrypted Domain Name System (DNS) resolution queries and responses are captured in this file from a monitored network.

DNS Auditing



Authoritative DNS

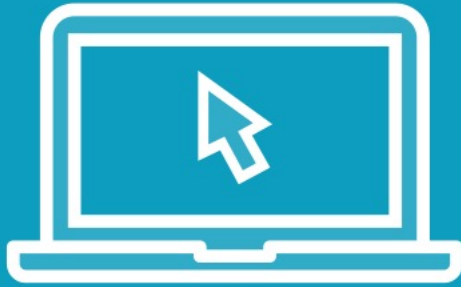
All query requests should be sourced by local DNS server



Encrypted DNS

DNS over HTTPS (DoH) and DNS over TLS (DoT) are not captured by Zeek logs

Demo



DNS Auditing

- Enumerate DNS fields in Elasticsearch
- Generate DNS baseline
- Create alert for unauthorized subdomains
- Create alert for third party DNS server
- Trigger alert with anomalous DNS request



Zeek Limitations



Zeek Limitations



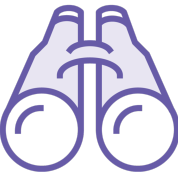
Only network data. No host-based visibility.



TLS v1.3 and other IETF standards



No TLS inspection. Only limited metadata on encrypted traffic.



Only captures what it can monitor.



Proprietary protocols



Summary



Continuous Monitoring

- Rogue server detection
- SSL certificate auditing
- DNS auditing
- Limitations of Zeek