

Using Zeek for Defensive Cyber Operations



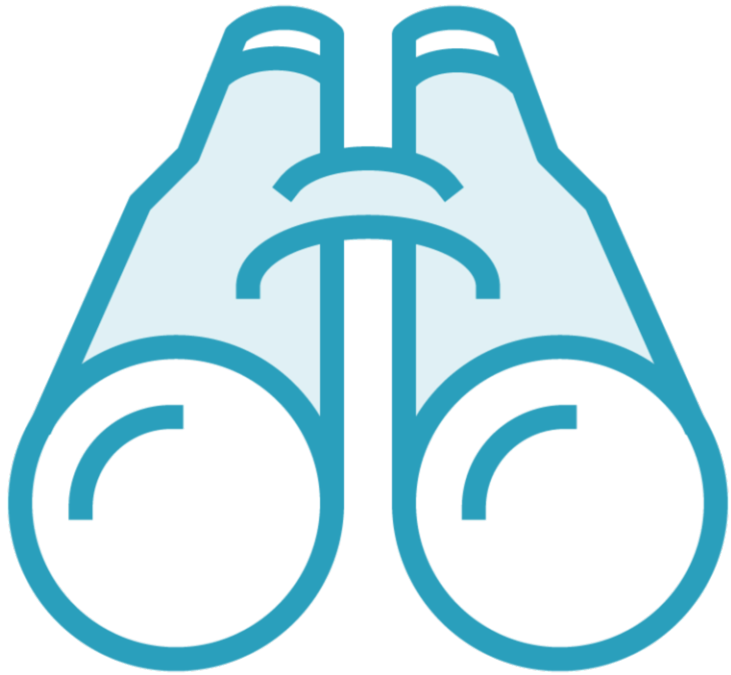
Michael Edie

Security Engineer

@tankmek blog.edie.io



Detecting Network Reconnaissance



DNS reconnaissance

Network scanning



Detecting DNS Reconnaissance



Asset List

Authorized DNS servers and authoritative zones.



DNS log

Filter on parent domain and use subdomain aggregation.



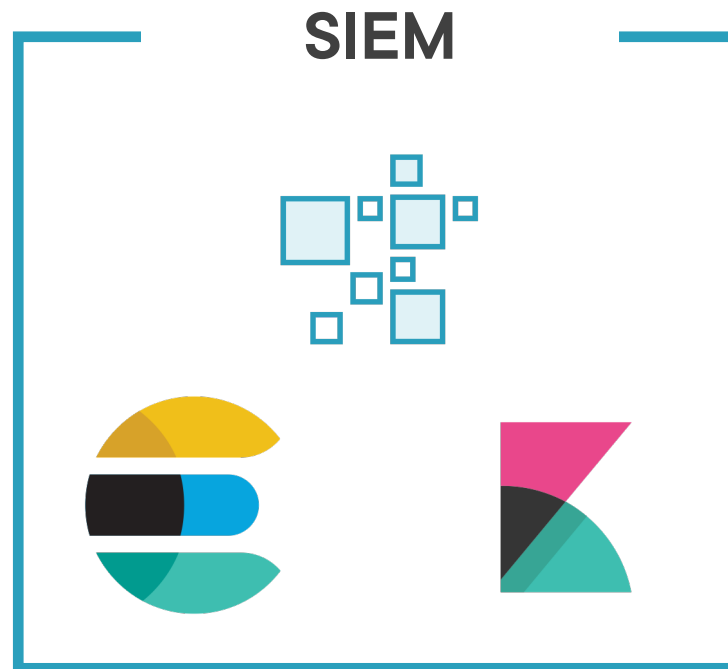
Detecting DNS Reconnaissance



Detecting DNS Reconnaissance



SERVER Sensor

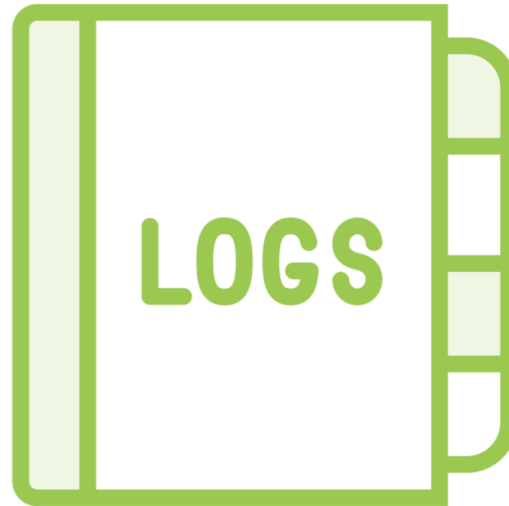


Detecting Network Scanning



Asset List

Identify vulnerability scanners in your environment



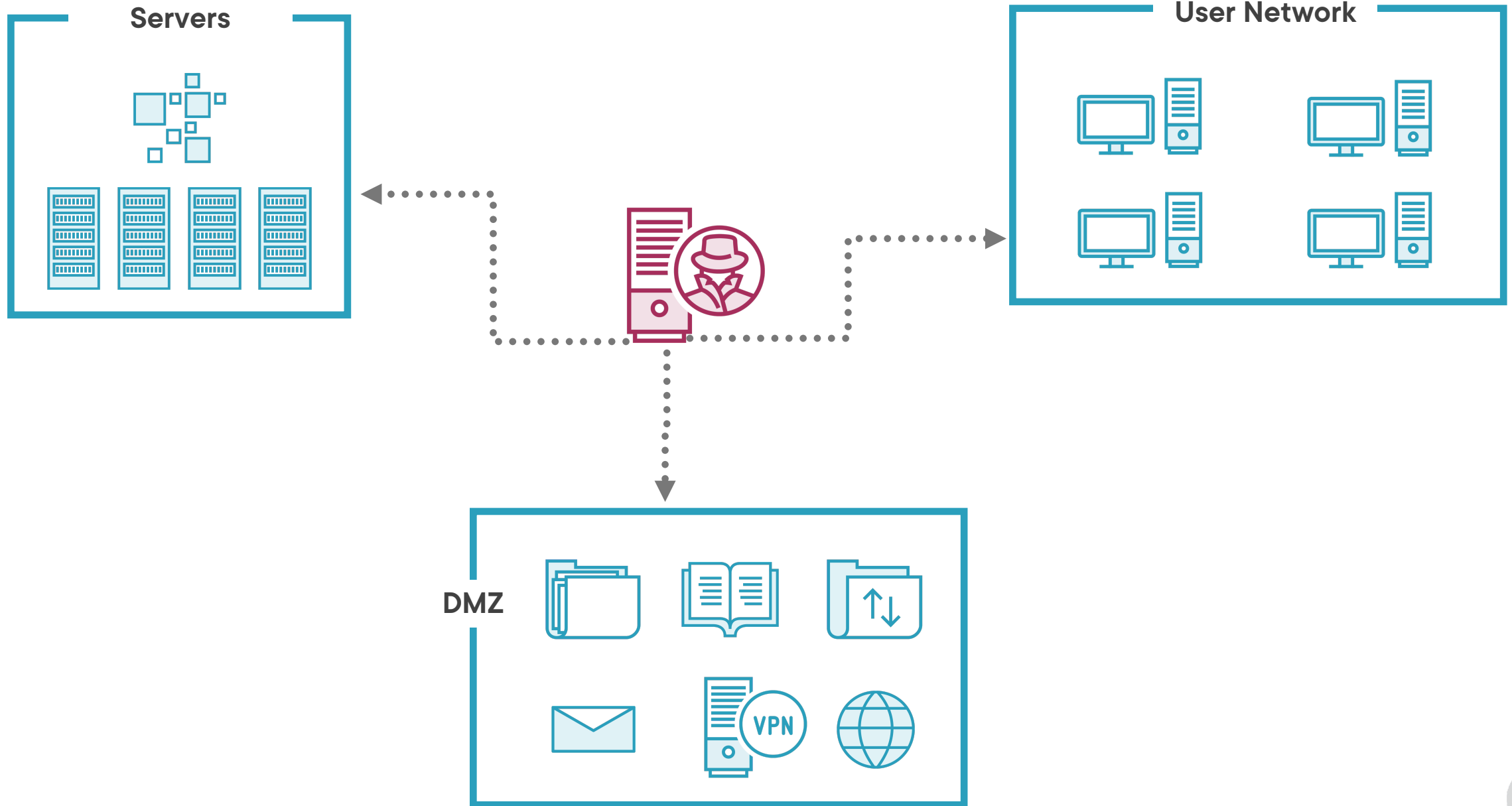
Connection log

Look for one-to-many relationships in across IP and ports.

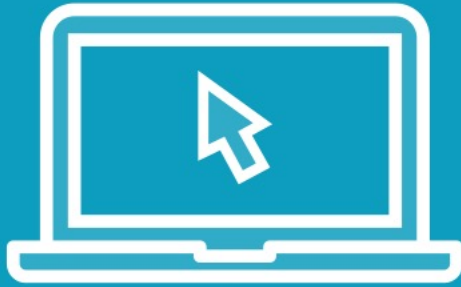


`misc/scan.zee`

Simple TCP scan detection script bundled with Zeek.



Demo



Detecting Network Reconnaissance

- Identify DNS servers
- Identify authoritative zones
- Find indicators of DNS recon
- Identify organic network scanners
- Enable bundled scan script
- Find indicators of network recon



Hunting Data Exfiltration



Hunting Data Exfiltration



Connection log analysis

DNS exfiltration

ICMP exfiltration

Long connection script

```
"uid": "CVkeu91nWacp0yYv16",  
"id.orig_h": "66.23.231.191",  
"id.orig_p": 8089,  
"id.resp_h": "192.168.28.7",  
"id.resp_p": 55622,  
"proto": "tcp",  
"duration": 4.851704835891724,  
"orig_bytes": 18100,  
"local_orig": false,  
"local_resp": true,  
"orig_pkts": 41,
```

conn.log

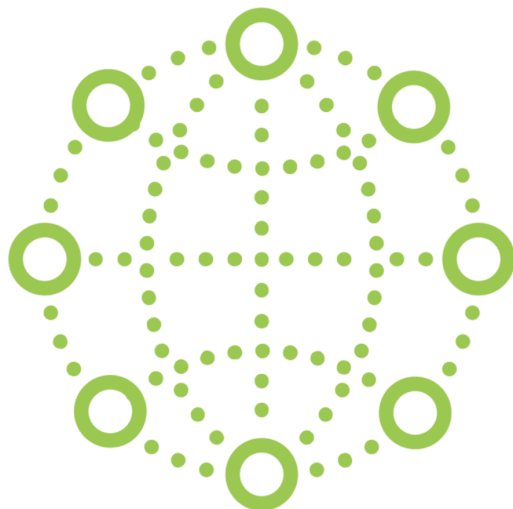
Holds layer 3 and layer 4 metadata from the network traffic captured. Can also be viewed as the information about which systems are communicating on the monitored network.

Hunting Data Exfiltration



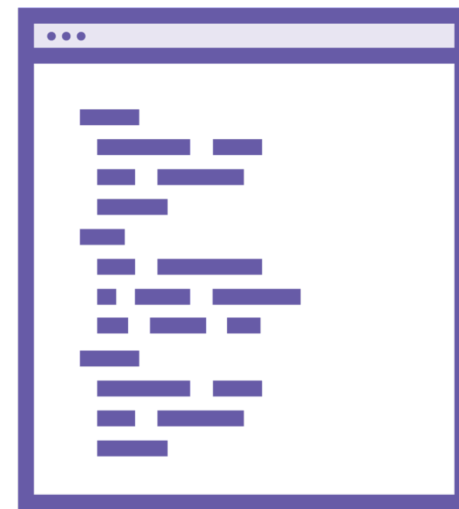
DNS Exfiltration

Query length allows
for 255 characters.



ICMP exfiltration

Several public
toolkits available that
allow data tunneling

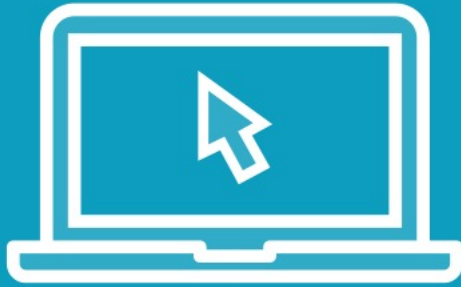


Long conn script

Will create
intermediate logs for
long connections.



Demo



Hunting Data Exfiltration

- General indicators of exfiltration
- Indicators of DNS exfiltration
- Install long connections script
- View Zeek notice log in Kibana



Malicious File Extraction



Malicious File Extraction



MIME types

Zeek file analyzers

Full Packet Capture (FPC)

Zeek file extraction policy

MIME types



application/x-dosexec



audio/mpeg



application/zip



application/msword



image/jpeg



text/json

Zeek Files

files.log

```
{  
  "ts": 1623121272.81747,  
  "fuid": "FBzKIu30EVtA3WMM14",  
  "tx_hosts": [  
    "192.168.4.188"  
  ],  
  "rx_hosts": [  
    "192.168.28.10"  
  ],  
  "conn_uids": [  
    "CPDDZ81GyIIjcSBFQ9"  
  ],  
  "source": "HTTP",  
  "mime_type": "text/json",  
  "is_orig": true,  
  "seen_bytes": 352,  
  "total_bytes": 352,  
  "md5": "566d2478ad3428d4292b46234167dace",  
  "sha1": "a0e7f8630661fb369cd308176a1f9cba564a4cc7"  
}
```

```
# Extract all files to disk.
```

```
@load base/files/extract
```

```
event file_new(f: fa_file)
{
    Files::add_analyzer(f, Files::ANALYZER_EXTRACT);
}
```

extract-all-files.zEEK

Default policy that will extract all files that have a corresponding MIME type known to zEEK. This can lead to a large volume of files and may have some privacy considerations.

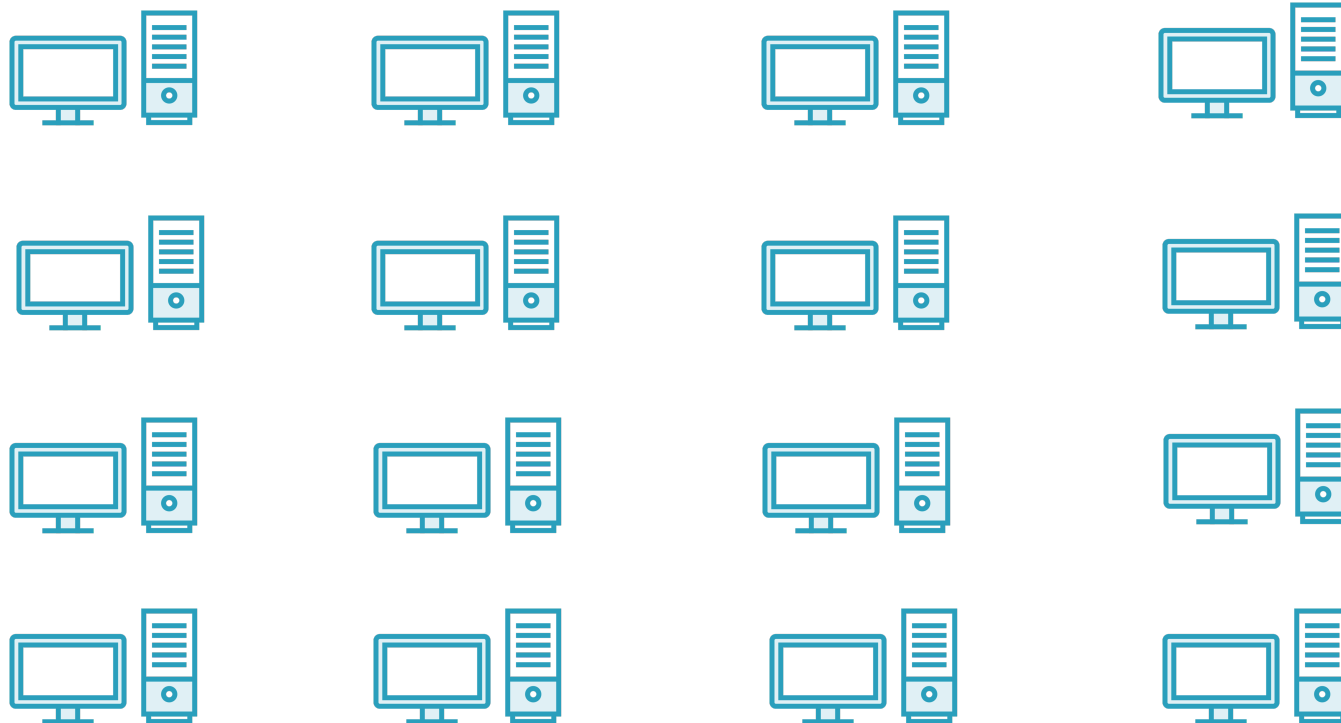
```
event file_sniff(f: fa_file, meta: fa_metadata)
{
    if (meta?$mime_type) {
        if (meta$mime_type == "application/x-dosexec")
            Files::add_analyzer(f, Files::ANALYZER_EXTRACT);
        else
            return;
    }
}
```

extract-pe-files.zEEK

Custom zEEK script to extract portable executables. This is a more targeted approach than the previous broad stroke.

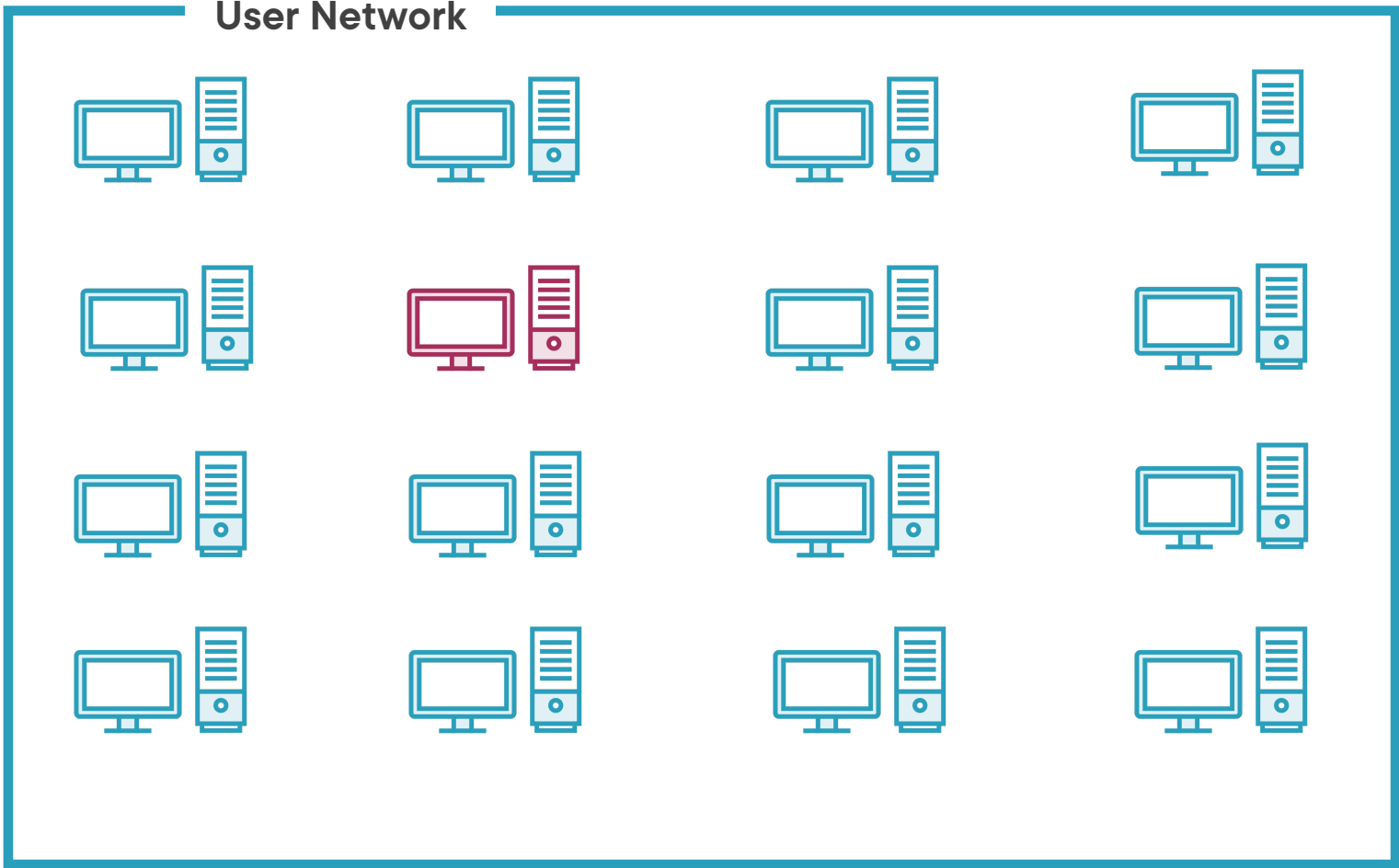


User Network

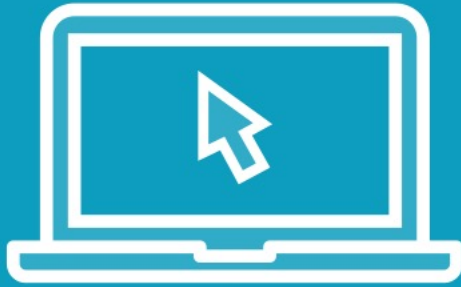




User Network



Demo



Malicious File Extraction

- Verify Zeek file extraction policy
- Browse extracted files directory
- Investigate system logs in Kibana
- Locate potential malware file



Post-Mortem Analysis



Post-Mortem Analysis



Compromised host

Network connections

DNS traffic

Encrypted Traffic

External connections

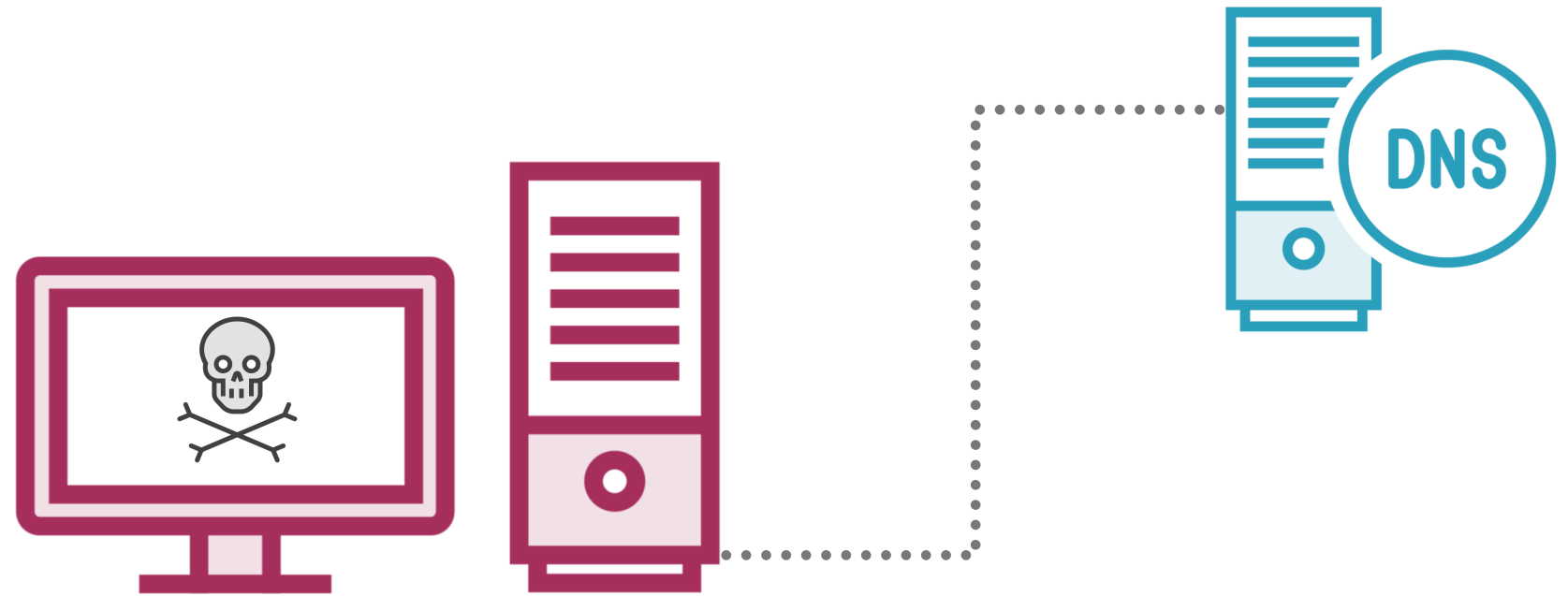
Post-Mortem Analysis



Post-Mortem Analysis



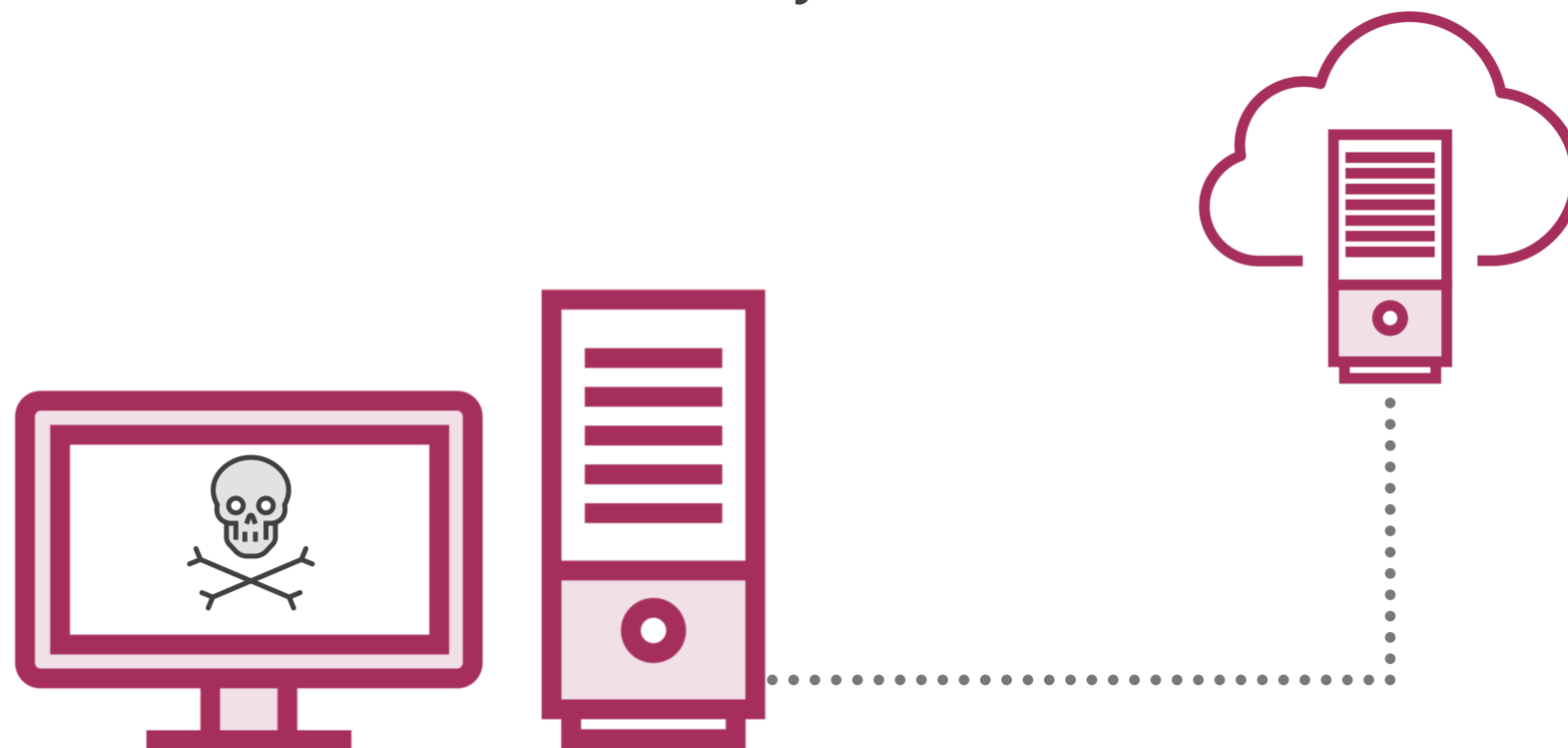
Post-Mortem Analysis



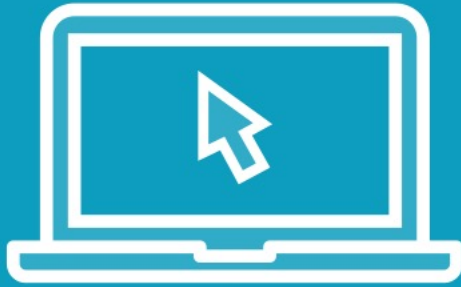
Post-Mortem Analysis



Post-Mortem Analysis



Demo



Post-Mortem Analysis

- Identify compromised host
- Identify lateral connections
- Identify DNS connections
- Identify encrypted connections
- Identify external connections



Course Review

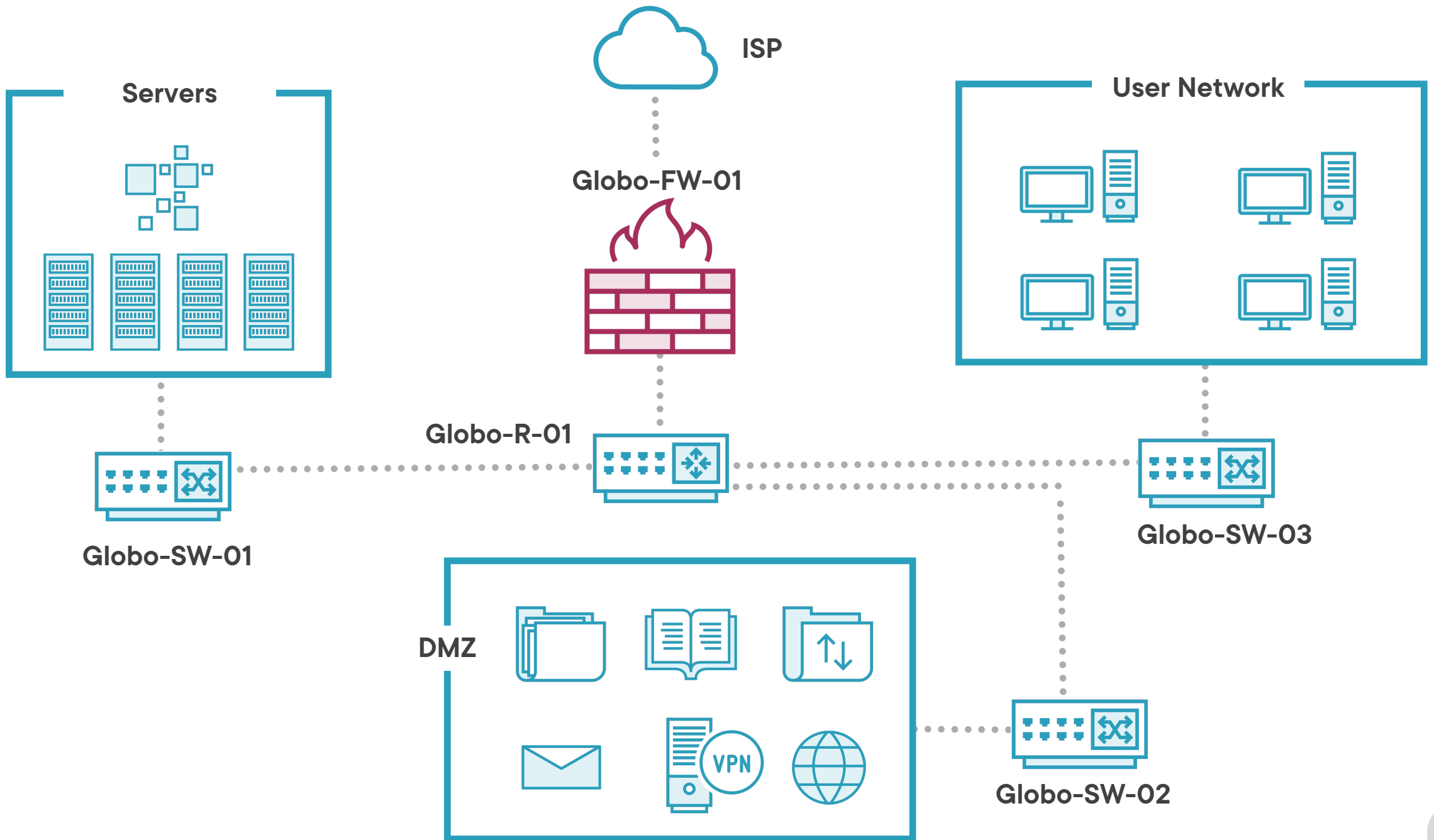


Summary



- Designing Zeek for enterprise monitoring





Summary



- Designing Zeek for enterprise monitoring
- Using Zeek for continuous monitoring



Continuous Monitoring Gaps

**Rogue server
detection**

**SSL Certificate
auditing**

DNS auditing

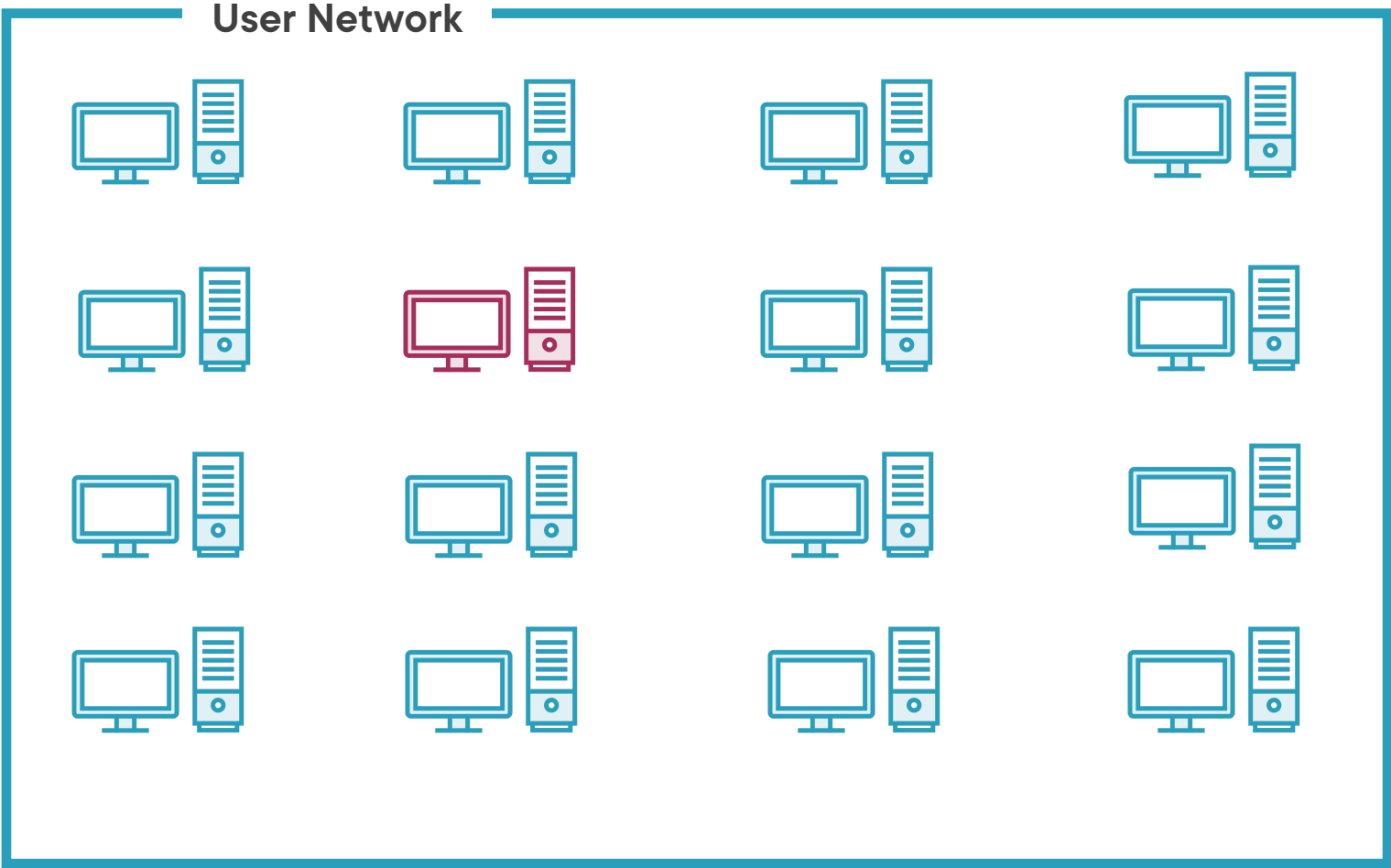


Summary



- Designing Zeek for enterprise monitoring
- Using Zeek for continuous monitoring
- Using Zeek for Defensive Cyber Ops





Thank you!

