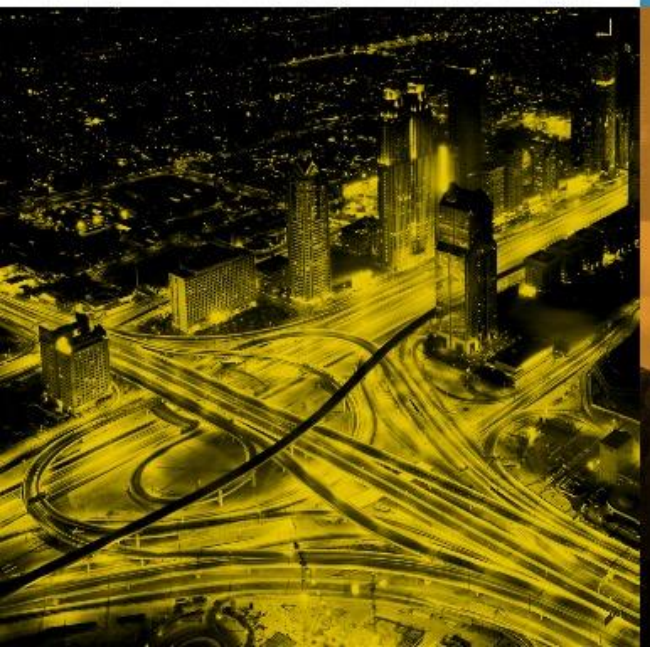
NIL




**Tom Kern**
Cyber security analyst, SIEM expert

# Complete Network Visibility on Budget

# C:\> whoami

- NIL\Tom_Kern
- living and breathing infosec for the past 2 years
- roots in network engineering

# Agenda

- Security operations
- Network visibility approaches
- Extracting metadata from the network traffic
- Data processing and storage
- About pcaps
- Correlating network and endpoint data

# Security Operations

- Detect and respond to threats in corporate environment
- **FACT**: You can't protect what you can't see!


- Proprietrary detection rules
- Threat hunting
- Security analytics
- Automation

DATA
(a lot of it)

- Incident response procedures
- Forensic investigations
- Remediation

# Network (data) monitoring

**Approaches:**

- Syslog from perimeter / inside firewalls
- IPFIX | Netflow
- Full packet capture

Best option? Somewhere in between.

Metadata.

# Bro (now Zeek)

Parsing metadata from network traffic:

- HTTP
- TLS
- SMB
- Kerberos
- NTLM
- DNS
- DHCP
- X508
- SMTP
- SNMP
- SIP

... and many others

# Bro log example - HTTP


```
{
  "ts":"2019-04-15T20:21:38.084972Z",
  "uid":"Ci6Smz3PZQUBQMz2Wl",
  "id.orig_h":"192.168.100.10",
  "id.orig_p":50238,
  "id.resp_h":"192.168.88.158",
  "id.resp_p":80,
  "trans_depth":1,
  "method":"GET",
  "host":"192.168.88.158",
  "uri":"/msf.docm",
  "version":"1.1",
  "user_agent":"Mozilla/5.0 (Windows NT; Windows NT 10.0; sl-SI) WindowsPowerShell/5.1.17134.590",
  "request_body_len":0,
  "response_body_len":200497,
  "status_code":200,
  "status_msg":"OK",
  "resp_mime_types":[
    "application/vnd.openxmlformats-officedocument.wordprocessingml.document"
  ]
}
```

# Bro log example - DNS


```
{
  "ts":"2019-04-15T18:30:45.113295Z",
  "uid":"CFM9bN2BV1sX7Wadef",
  "id.orig_h":"192.168.100.10",
  "id.orig_p":61298,
  "id.resp_h":"192.168.70.11",
  "id.resp_p":53,
  "proto":"udp",
  "trans_id":14078,
  "rtt":0.071271,
  "query":"login.live.com",
  "qclass":1,
  "qclass_name":"C_INTERNET",
  "qtype":1,
  "qtype_name":"A",
  "rcode":0,
  "rcode_name":"NOERROR",
  "AA":false,
  "TC":false,
  "RD":true,
  "RA":true,
  "Z":0,
  "answers":[
    "login.msa.akadns6.net",
    "vs.login.msa.akadns6.net",
    "207.46.26.12",
    "65.54.187.132",
    "207.46.26.14"
  ],
  "rejected":false
}
```

# Storage options

Bro logs are saved into multiple rotating text files.

What to do with them?

Forward them to:

- syslog server
- SIEM
- Elasticsearch
- .. any other database

# I don‘t have time/energy :|

Security Onion distro has it all:

- Bro
- Snort / Surricata
- Syslog ingestion
- Full packet capture (yey!)


Logs are parsed/processed/saved in ELK stack (elasticsearch, logstash, kibana).

Monitoring up to 100 Mbps using evaluation single VM or
up to multiple 10 Gbps using distributed production deployment.

kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout

## Navigation

Home
Help

**Alert Data**
Bro Notices
ElastAlert
HIDS
NIDS

**Bro Hunting**
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE
RADIUS
RDP
RFB
SIP
SMB
SMTP
SNMP
Software
SSH
SSL
Syslog
Tunnels
Weird
X.509

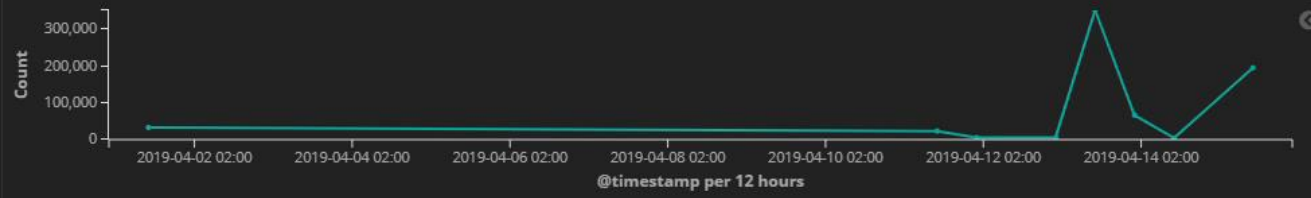
**Host Hunting**
Autoruns
Beats
OSSEC
Sysmon

**Other**

## Total Number of Logs

681,361

## Total Log Count Over TIme




## All Sensors - Log Type

| Log Type(s) | Count |
|---|---|
| sysmon | 612,806 |
| ossec_archive | 24,560 |
| CRON | 9,891 |
| bro_conn | 8,597 |
| bro_http | 5,601 |
| bro_dce_rpc | 3,553 |
| bro_files | 3,458 |
| bro_dns | 3,203 |
| firewall | 2,586 |
| bro_ssl | 1,171 |

Export: Raw Formatted

1 2 3 4 5 »

## Sensors - Count

1

## Devices - Count

2

## Devices - Log Count By Device

| Device | Count |
|---|---|
| seconi | 65,245 |
| gateway | 2,586 |

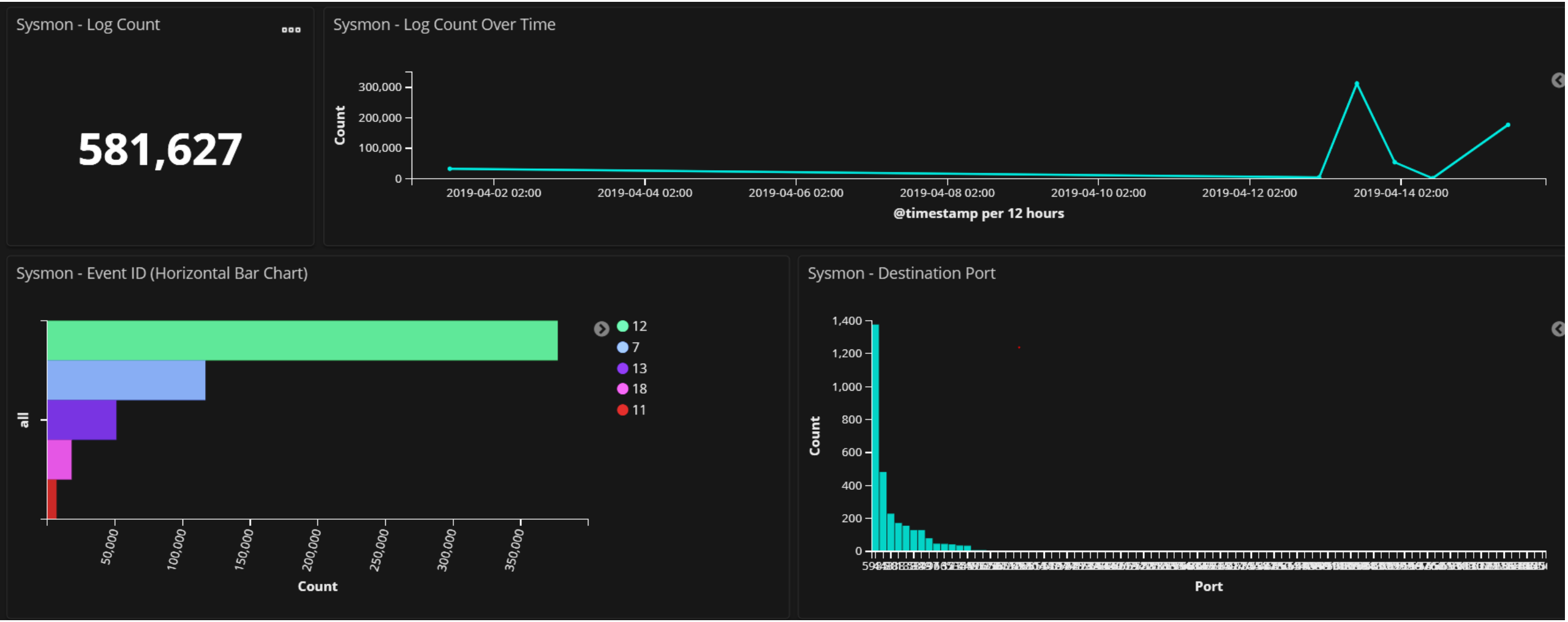
## Log Type Per Sensor/Device

# How about endpoint monitoring?

- Sysinternals Sysmon offers in-depth Windows endpoint monitoring:
  - process creation including execution arguments
  - network connections
  - registry modifications
  - file modifications
  - loaded DLLs
  - installed drivers
  - WMI events
  - .. and more!

- Installed as Windows service, logs to Windows Events
- Central log collection with WEF service
- Forwarding to Security Onion (Elastic Beats → Logstash)

# Sysmon - Overview



# Sysmon - Processes

Sysmon - Image

| Image | Parent Image | Count |
|---|---|---|
| C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe | 464 |
| C:\Program Files\Microsoft Office\Office15\WINWORD.EXE | C:\Windows\explorer.exe | 6 |
| C:\Program Files\Microsoft Office\Office15\WINWORD.EXE | C:\Program Files\Microsoft Office\Office15\WINWORD.EXE | 5 |
| C:\Program Files\Microsoft Office\Office15\WINWORD.EXE | C:\Program Files (x86)\Google\Chrome\Application\chrome.exe | 4 |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe | C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe | 262 |
| C:\Windows\System32\svchost.exe | C:\Windows\System32\services.exe | 167 |
| C:\Windows\System32\backgroundTaskHost.exe | C:\Windows\System32\svchost.exe | 220 |
| C:\Windows\System32\RuntimeBroker.exe | C:\Windows\System32\svchost.exe | 102 |
| C:\Program Files (x86)\Google\Chrome\Application\chrome.exe | C:\Program Files (x86)\Google\Chrome\Application\chrome.exe | 97 |
| C:\Program Files (x86)\Google\Chrome\Application\chrome.exe | C:\Windows\explorer.exe | 2 |

Export: Raw Formatted

1 2 3 4 5 ··· 11 »

# Sysmon – Network connections

Sysmon - Summary

| Image | Source IP Address | Source Hostname | Destination IP Address | Destination Hostname | Destination Port | Count |
|---|---|---|---|---|---|---|
| C:\Windows\System32\svchost.exe | 192.168.100.10 | pc-test13.tom.si | 92.123.5.107 | a92-123-5-107.deploy.static.akamaitechnologies.com | 443 | 30 |
| C:\Windows\System32\svchost.exe | 192.168.100.10 | pc-test13.tom.si | 104.103.107.203 | a104-103-107-203.deploy.static.akamaitechnologies.com | 443 | 17 |
| C:\Windows\System32\svchost.exe | 192.168.100.10 | pc-test13.tom.si | 104.96.141.107 | a104-96-141-107.deploy.static.akamaitechnologies.com | 80 | 17 |
| C:\Windows\System32\svchost.exe | 192.168.100.10 | pc-test13.tom.si | 205.185.216.42 | map2.hwcdn.net | 80 | 11 |
| C:\Windows\System32\svchost.exe | 192.168.100.10 | pc-test13.tom.si | 205.185.216.10 | map2.hwcdn.net | 80 | 10 |
| C:\Windows\System32\svchost.exe | ::1 | pc-test13.tom.si | ::1 | pc-test13.tom.si | 5985 | 8 |
| C:\Windows\System32\svchost.exe | 192.168.100.10 | pc-test13.tom.si | 104.103.81.93 | a104-103-81-93.deploy.static.akamaitechnologies.com | 443 | 5 |
| C:\Program Files\Microsoft Office\Office15\WINWORD.EXE | 192.168.100.10 | pc-test13.tom.si | 92.123.4.47 | a92-123-4-47.deploy.static.akamaitechnologies.com | 443 | 5 |
| System | ::1 | pc-test13.tom.si | ::1 | pc-test13.tom.si | 445 | 4 |
| C:\Windows\System32\backgroundTaskHost.exe | 192.168.100.10 | pc-test13.tom.si | 204.79.197.200 | a-0001.a-msedge.net | 443 | 4 |

Export: Raw Formatted

1 2 3 4 5 »

# Q&A

# ENABLING IT FOR BUSINESS

nil.com