# Security-Centric Traffic Analysis

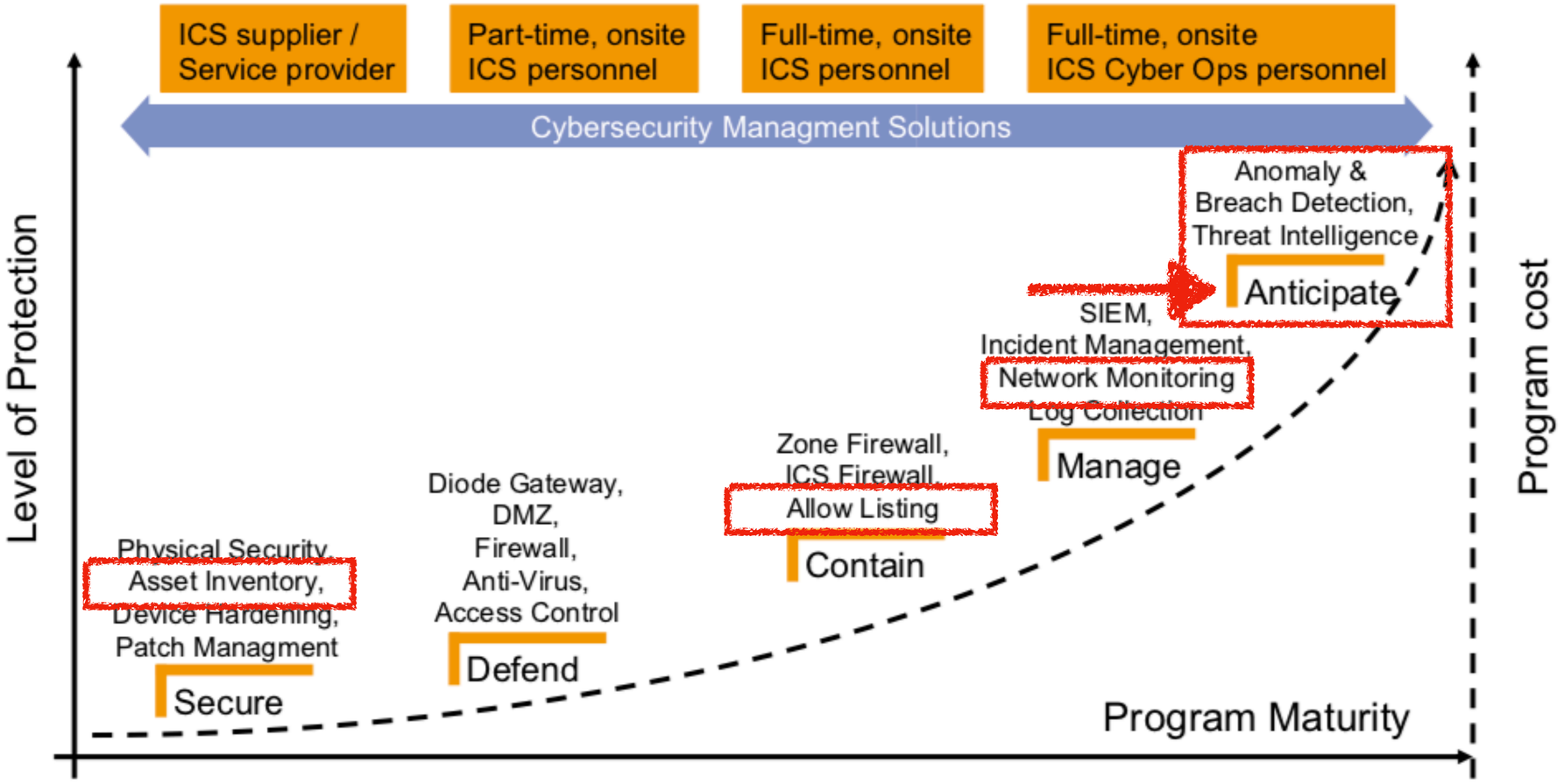
Luca Deri <deri@ntop.org>
@lucaderi

# Part I: Introduction

# Why Is Security-Centric Traffic Analysis Important?

- Constant increase of cyber-attacks required NTAs to focus on security aspects in addition to traditional monitoring (i.e. latency monitoring, service availability, …).
- In particular new challenges include:
  - Encrypted traffic analysis.
  - Detection of vulnerable protocols and ciphers.
  - Complete visibility including IoT devices (e.g. badge readers) that can create serious issues.
  - Realtime identification of threats and suspicious events.

# Cybersecurity Taxonomy

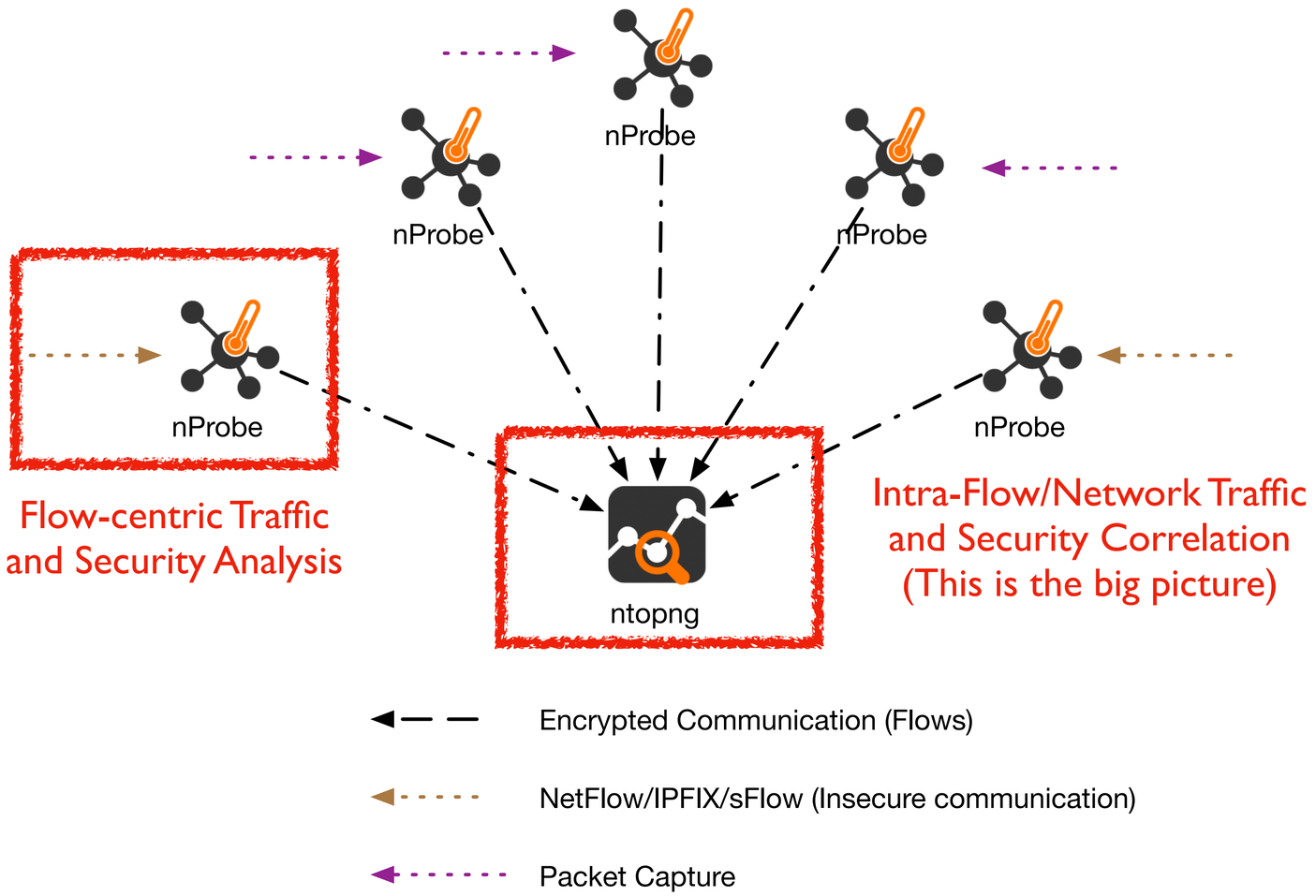



Picture courtesy of switch.ch

# Cybersecurity Monitoring: Requirements

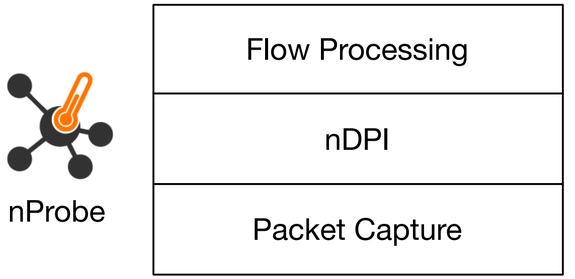
- Distributed monitoring platform
  - Network edge traffic monitoring + centralised analysis
- Deep network traffic dissection to also inspect encrypted traffic (more and more popular).
- Interpret traffic monitoring data to create alarms from raw signals and trigger actionable insights (e.g. mitigate the problem identified).
- Export monitoring information in an open format towards multiple consumers/subscribers.

# Typical Deployment: Traffic Processing [1/2]



# Typical Deployment: Traffic Processing [2/2]

- nDPI is an open source DPI toolkit on top of which nProbe computes flows statistics. It:
  - Decodes the initial flow packets detecting the application protocol (e.g. Google Maps).
  - Analyses encrypted traffic to detect issues hidden but un-inspectable payload content.
  - Extracts metadata from selected protocols (e.g. DNS, HTTP, TLS..) and matches it against known algorithms for detecting selected threats (e.g. DGA hosts, Domain Generated Algorithm).



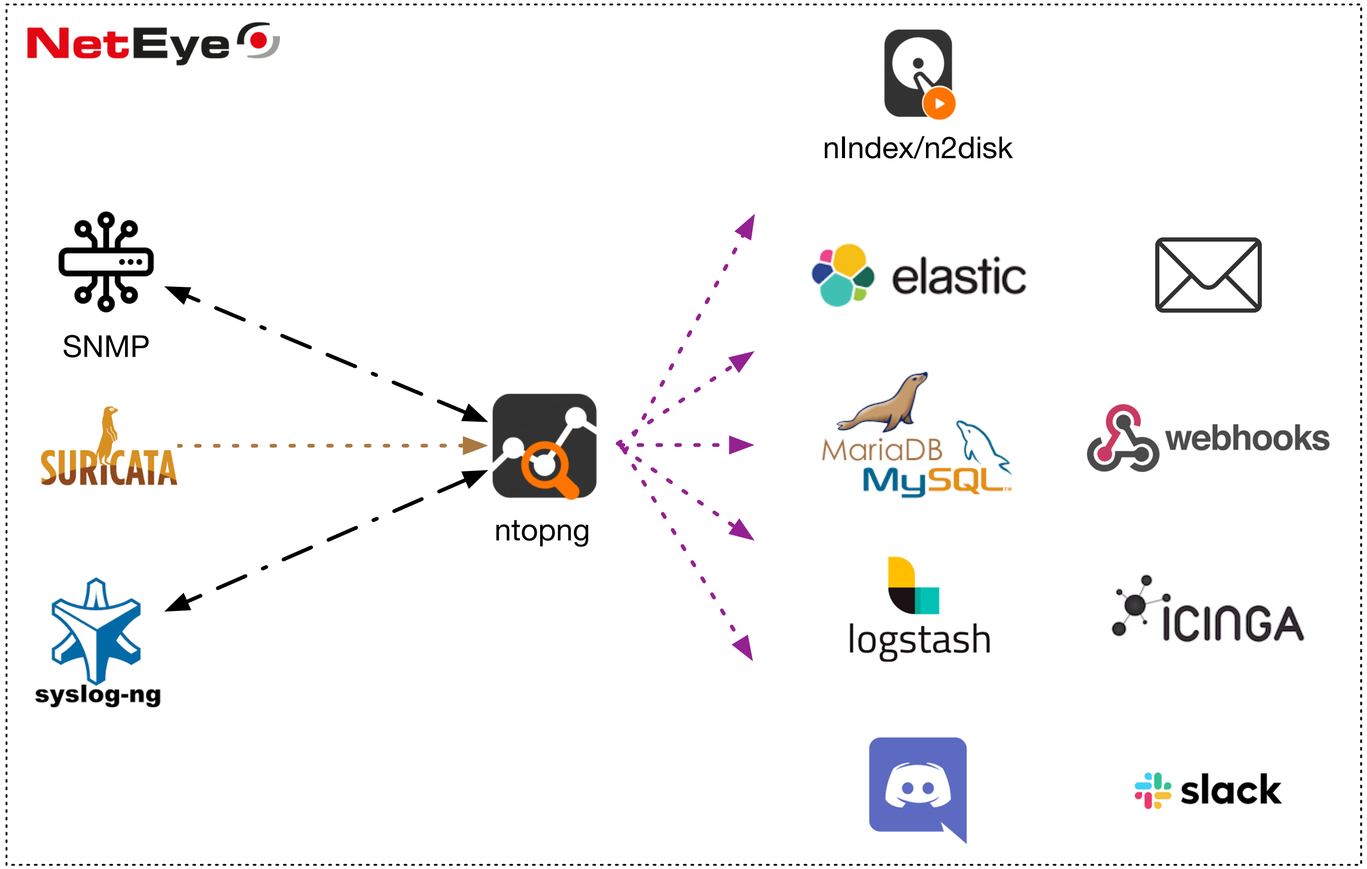
# nDPI: Identified Flow Risks

- XSS (Cross Site Scripting)
- SQL Injection
- Arbitrary Code Injection/Execution
- Binary/.exe application transfer (e.g. in HTTP)
- Known protocol on non standard port
- TLS self-signed certificate
- TLS obsolete version
- TLS weak cipher
- TLS certificate expired
- TLS certificate mismatch
- HTTP suspicious user-agent
- HTTP numeric IP host contacted
- HTTP suspicious URL
- HTTP suspicious protocol header
- TLS connections not carrying HTTPS (e.g. a VPN over TLS)
- Suspicious DGA domain contacted
- Malformed packet
- SSH/SMB obsolete protocol/application version
- TLS suspicious ESNI usage
- Unsafe Protocol used

# ntopng Traffic Consolidation [1/2]

- While nProbe is a flow-oriented probe that monitors traffic at the edge, ntopng is a data collector that correlates signals coming from distributed probe and:
  - Intra-flow correlation at host, AS, Network Interface level to spot higher-level threats.
  - Ability to trigger alerts based on user-defined scripts that are executed on collected data after consolidation.
  - Actionable insights to react to detected issues.
  - Web-based report and export to external systems.

# ntopng Traffic Consolidation [2/2]



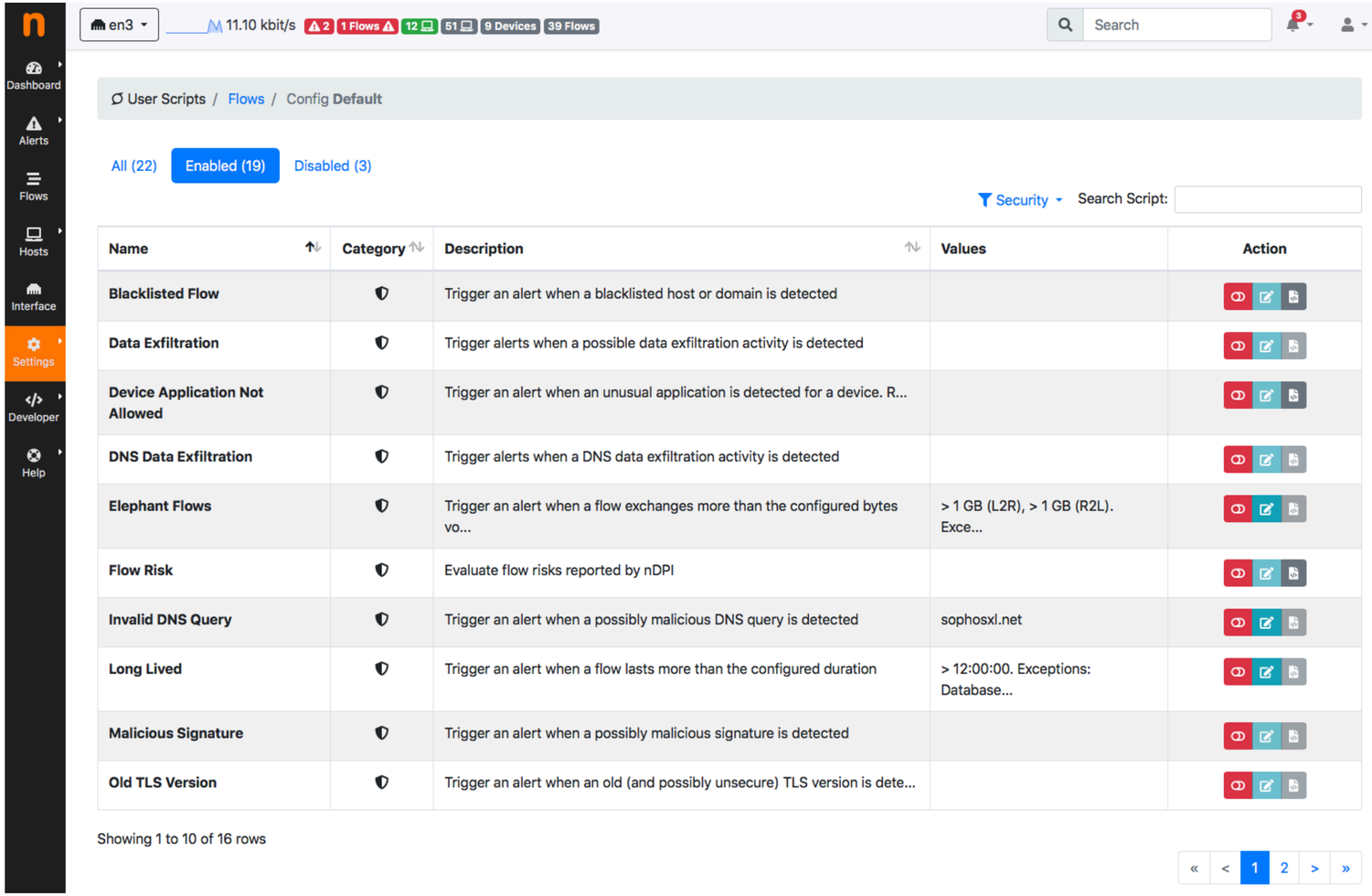
# Part II: Use Cases

# ETA (Encrypted Traffic Analysis)

Flow: 192.168.1.168:58196 ⇄ 167.99.215.164:4434 Overview

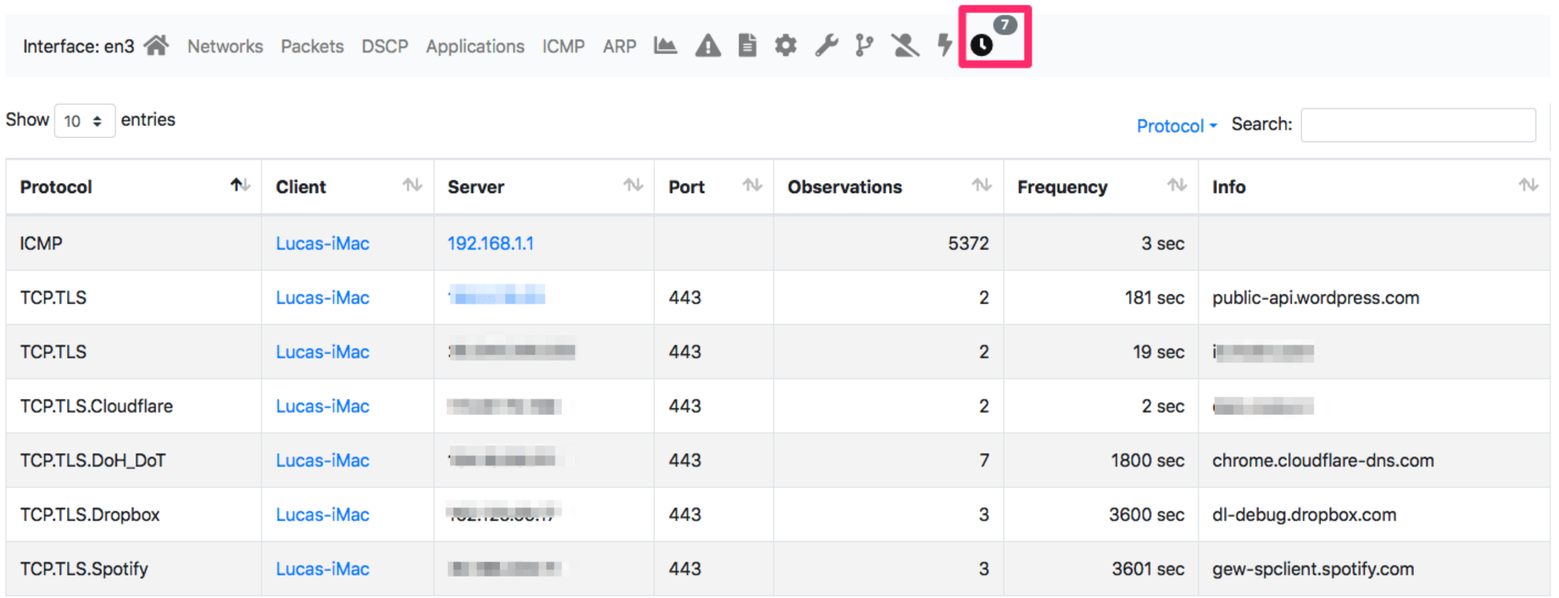
| | | |
|---|---|---|
| **Flow Peers [ Client / Server ]** | 192.168.1.168 :58196 [ 28:37:37:00:6D:C8 ] ⇄ 167.99.215.164 :4434 [ 10:13:31:F1:39:76 ] | |
| **Protocol / Application** | TCP / TLS.ntop (Network) [ TLSv1.3 ] | |
| **First / Last Seen** | 09/09/2020 22:14:00 [00:28 ago] | 09/09/2020 22:14:12 [00:16 ago] |
| **Total Traffic** | Total: 12.92 KB | Goodput: 10.63 KB (82.29 %) |
| | Client → Server: 18 Pkts / 5.42 KB | Client ← Server: 17 Pkts / 7.5 KB |
| | 192.168.1.168:58196 | 167.99.215.164:4434 |
| **TLS Certificate** | Client Requested: dati.ntop.org | |
| **JA3** | 7120d65624bcd2e02ed4b01388d84cdb | 15af977ce25de452b96affa2addb1036 |
| **TLS ALPN** | h2,http/1.1 | |
| **Client Supported TLS Protocols** | TLSv1.3,TLSv1.2,TLSv1.1,TLSv1 | |
| **Max (Estimated) TCP Throughput** | Client → Server: 199.53 kbit/s | Client ← Server: 1.63 Mbit/s |
| **TCP Flags** | Client → Server: FIN SYN PUSH ACK | Client ← Server: FIN SYN PUSH ACK |
| | Flow is closed. | |
| **Detected Flow Risks** | Known Application on Non-Standard Port | |
| **Flow Alerted** | Known application ntop detected on non-standard port 4434 [Score: 100] | |
| **Flow Score** | 100 | |
| **Entropy** | Client → Server: 7.689 | Client ← Server: 7.694 |

# Threat Detection via User Scripts



# Searching Mice in Noise Traffic

Low-bandwidth periodic connections might hide misuse (e.g. periodic tasks), botnet command-and-control communications, unauthorised monitoring.




| Protocol | Client | Server | Port | Observations | Frequency | Info |
|---|---|---|---|---|---|---|
| ICMP | Lucas-iMac | 192.168.1.1 | | 5372 | 3 sec | |
| TCP.TLS | Lucas-iMac | | 443 | 2 | 181 sec | public-api.wordpress.com |
| TCP.TLS | Lucas-iMac | | 443 | 2 | 19 sec | |
| TCP.TLS.Cloudflare | Lucas-iMac | | 443 | 2 | 2 sec | |
| TCP.TLS.DoH_DoT | Lucas-iMac | | 443 | 7 | 1800 sec | chrome.cloudflare-dns.com |
| TCP.TLS.Dropbox | Lucas-iMac | | 443 | 3 | 3600 sec | dl-debug.dropbox.com |
| TCP.TLS.Spotify | Lucas-iMac | | 443 | 3 | 3601 sec | gew-spclient.spotify.com |

# Industrial IoT/Scada Monitoring [1/2]

- nDPI supports some popular IoT/Scada protocols including modbus, DNP3 and IEC 60870.
- IEC 60870 is very important as it can be used to detect issues such as
  - Unknown telemetry addresses
  - Connection loss and restore
  - Loss of data coming from remote systems
- ntopng features permanent IEC 60870 monitoring to detect industrial anomalies in addition to traditional traffic monitoring.

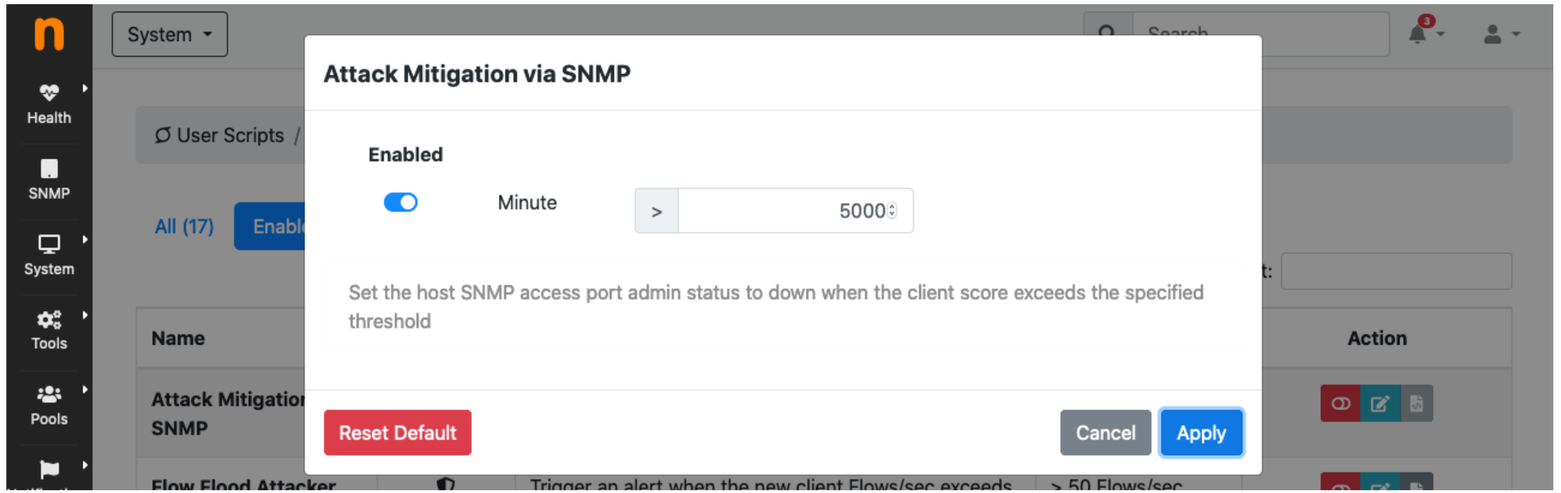
# Industrial IoT/Scada Monitoring [2/2]

Flow: [redacted] ⇄ [redacted] Overview

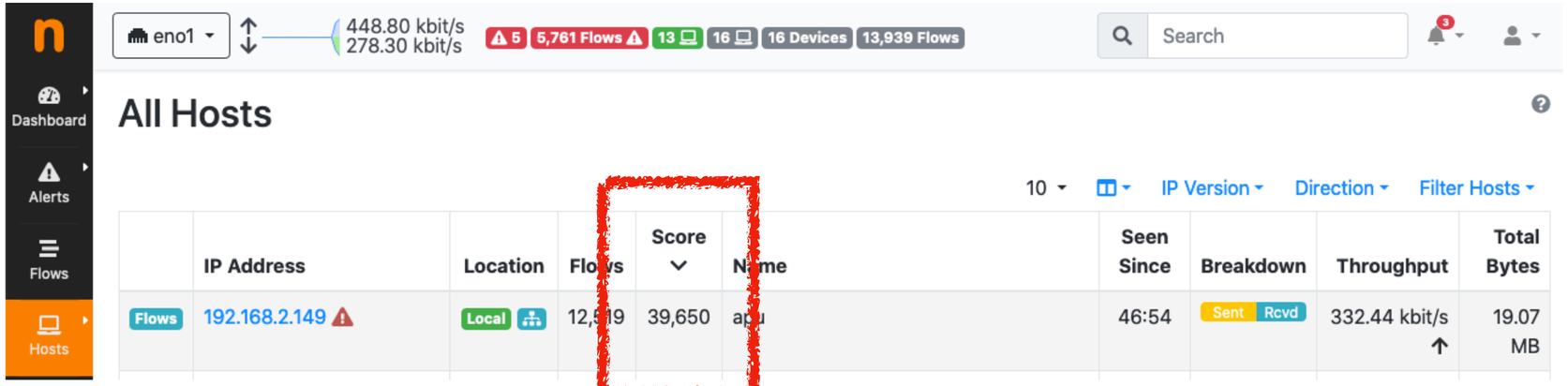
| | | |
|---|---|---|
| **VLAN ID** | 21 | |
| **Flow Peers [ Client / Server ]** | [redacted] | |
| **Protocol / Application** | TCP / IEC60870 (IoT-Scada) 👍 | |
| **First / Last Seen** | 02/09/2020 06:21:28 [6 Days, 14:02:24 ago] | 02/09/2020 06:26:29 [6 Days, 13:57:23 ago] |
| **Total Traffic** | Total: 508.8 KB — | Goodput: 120.5 KB (23.7 %) — |
| | Client → Server: 3,920 Pkts / 340.8 KB — | Client ← Server: 2,688 Pkts / 168 KB — |
| | 110.244.197.126@21:2404 | 110.244.190.197@21:44740 |
| **IEC 60870-5-104 TypeIDs** | • M_ME_NA_1 (9)<br>• ASDU_TYPE_41 (41) | |
| **DSCP / ECN [ Client / Server ]** | Best Effort (CS0) / Disabled (0) | Best Effort (CS0) / Disabled (0) |
| **Application Latency** | < 1 ms | |
| **Packet Inter-Arrival Time [ Min / Avg / Max ]** | Client → Server: 1 ms / 76.39 ms / 200 ms | Client ← Server: < 1 ms / 111.62 ms / 299 ms |
| **TCP Flags** | Client → Server: PUSH ACK | Client ← Server: PUSH ACK |
| | Flow is active, however, the beginning of the flow has not been seen and peer roles (client/server) might be inaccurate | |
| **Additional Flow Status** | Remote client and remote server [Score: 10] ⚙ | |
| **Flow Score** | 10 | |
| **Entropy** | Client → Server: 6.763 | Client ← Server: 4.892 |
| **Actual / Peak Throughput** | 0 bit/s — / 16.76 kbit/s | |

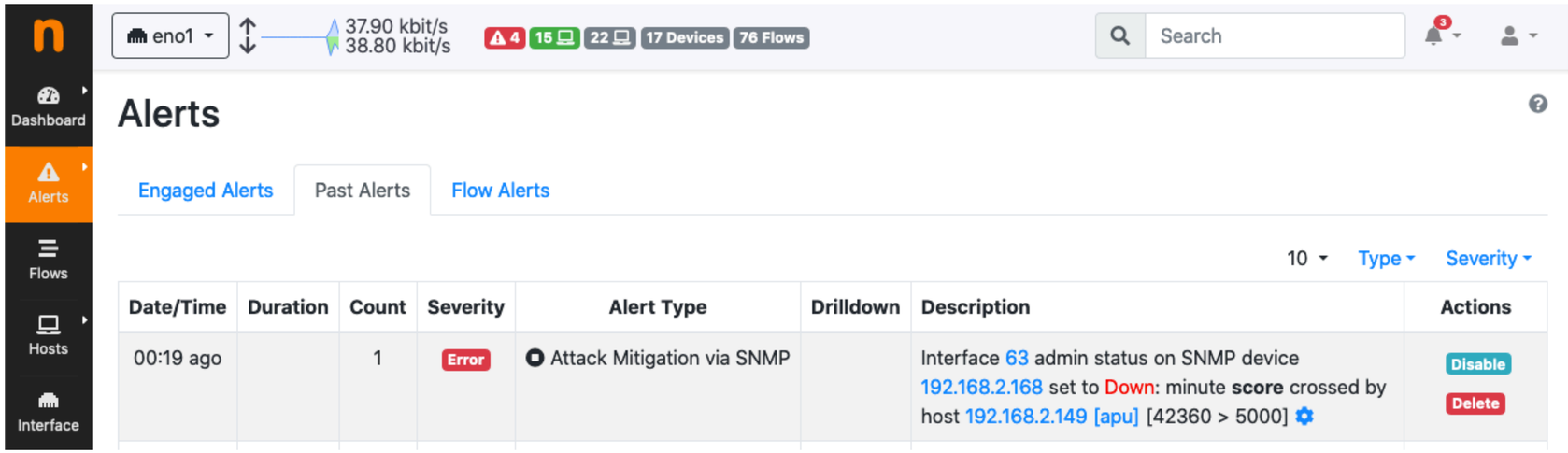
# Actionable Insights: Attack Mitigation via SNMP [1/2]

- Score is a metric used to detect issues on entities such as hosts, AS, networks.
- SNMP can be used to poll but also to modify devices configuration



# Actionable Insights: Attack Mitigation via SNMP [2/2]




https://github.com/ntop/