

Security-Centric Traffic Analysis

Luca Deri <deri@ntop.org>
@lucaderi

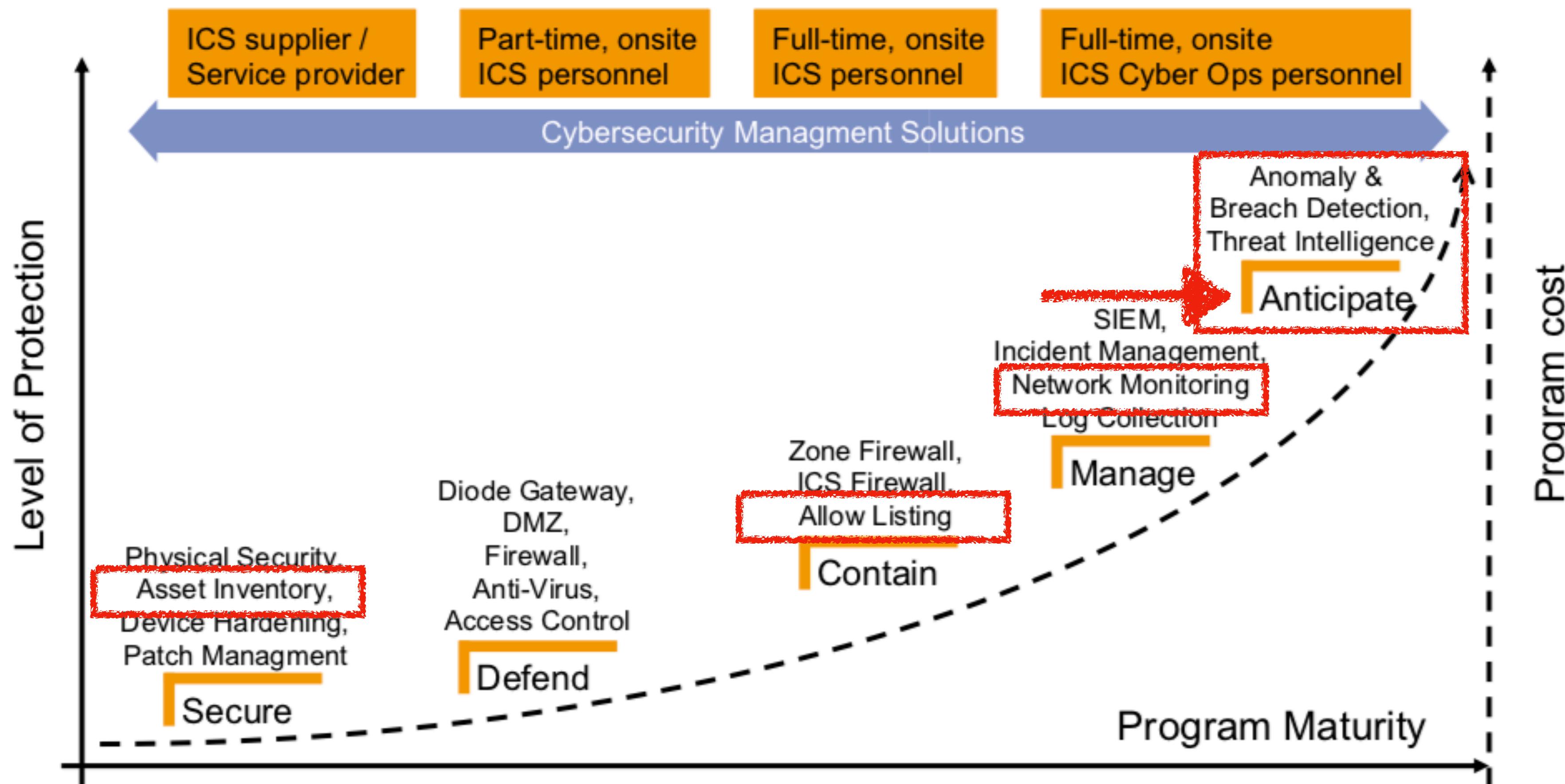


Part I: Introduction

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

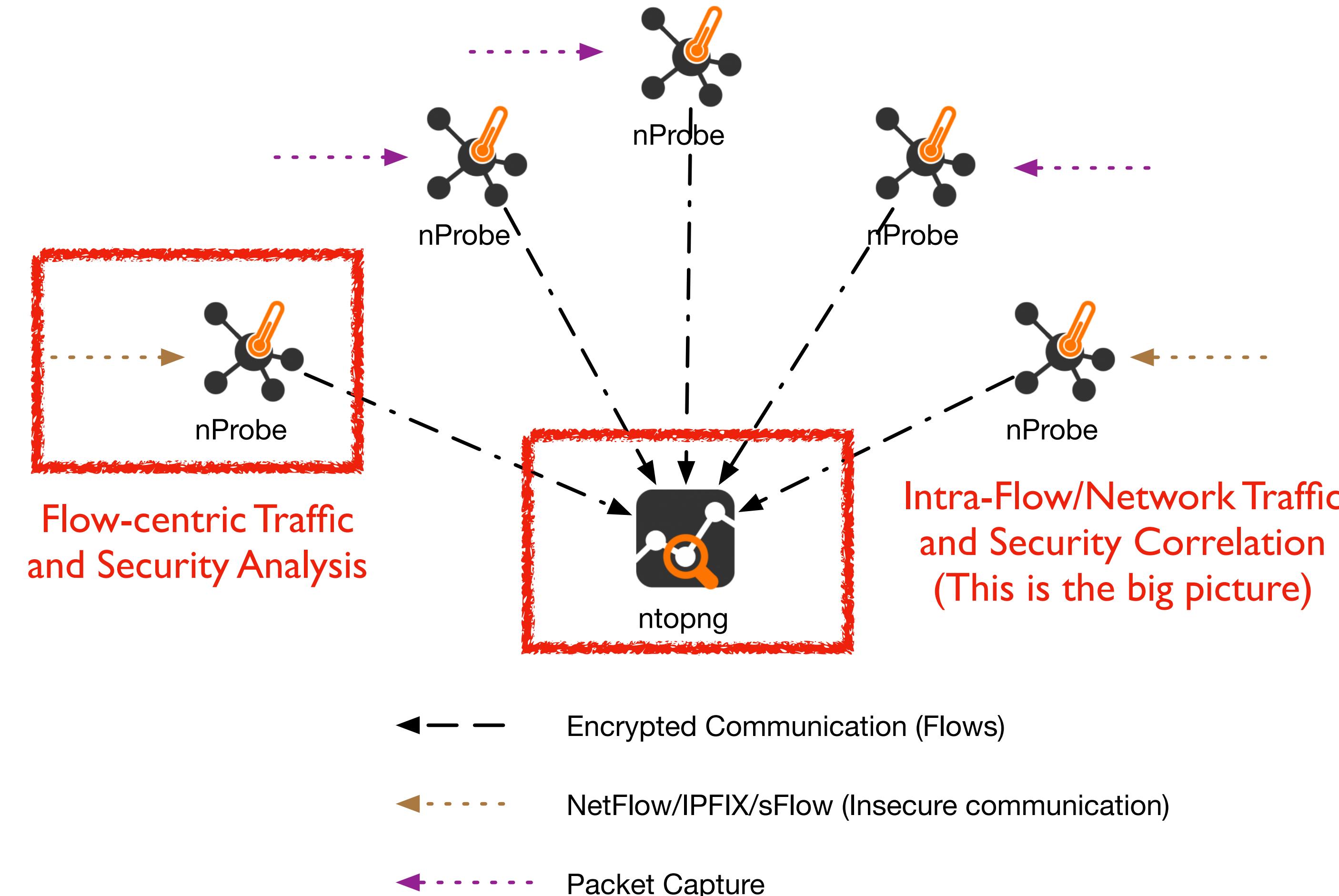


Picture courtesy of [switch.ch](#)

Cybersecurity Monitoring: Requirements

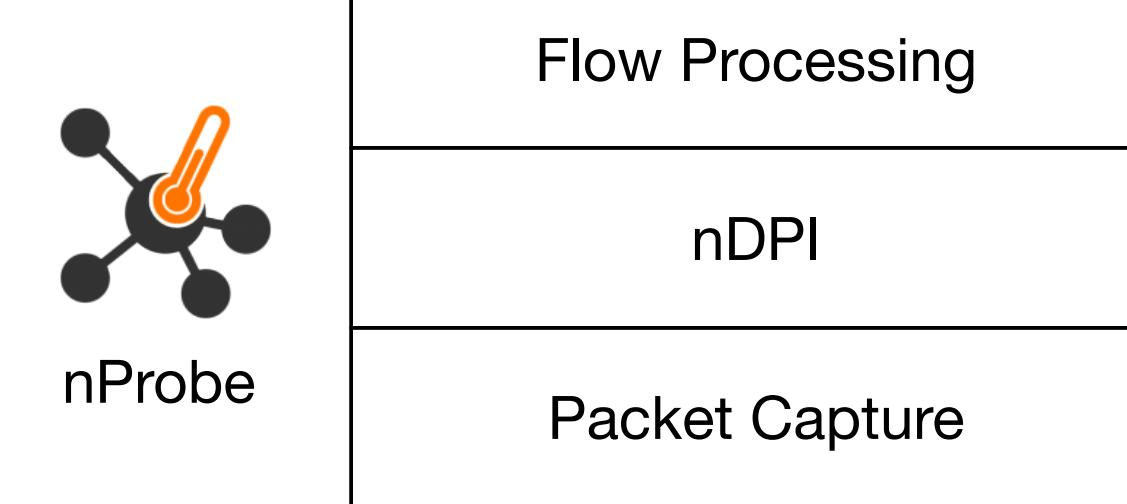
- Distributed monitoring platform
 - Network edge traffic monitoring + centralised analysis
- Deep network traffic dissection to also inspect encrypted traffic (more and more popular).
- Interpret traffic monitoring data to create alarms from raw signals and trigger actionable insights (e.g. mitigate 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).



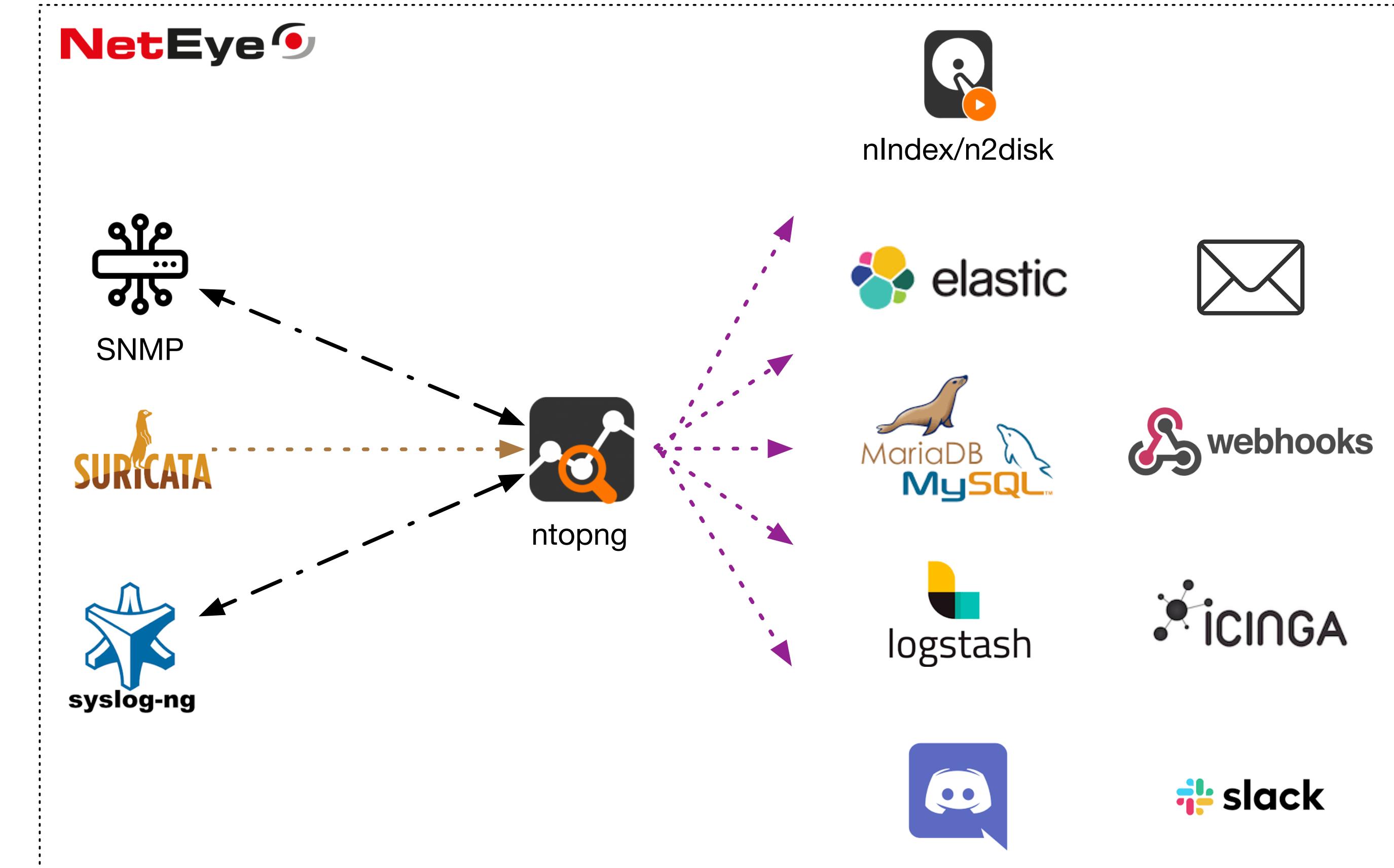
nDPI: Identified Flow Risks

- 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]



Ingress/Egress data



Ingress (Security Events)



Egress (Alerts/Long-Term Data Storage)

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:	Client ← Server:
	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

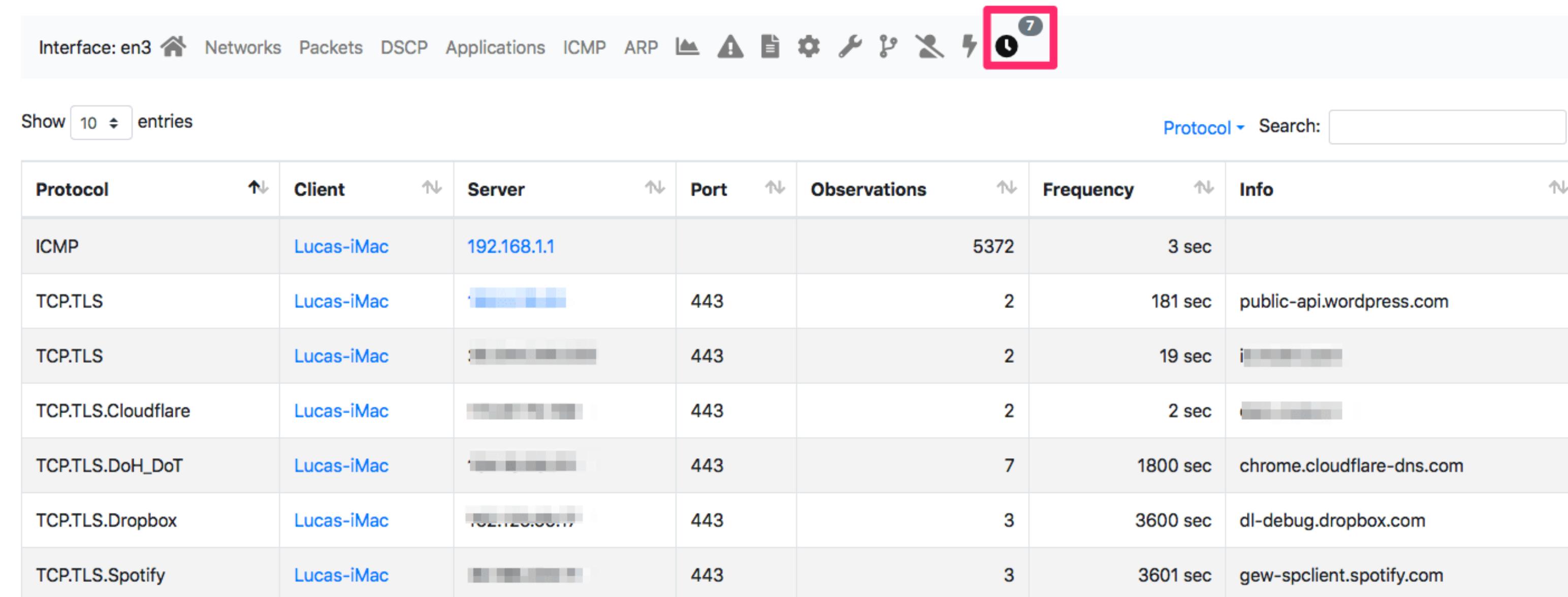
Threat Detection via User Scripts

The screenshot shows the ntop web interface with the following details:

- Header:** en3, 11.10 kbit/s, 2 Flows, 12 Devices, 51 Flows, 9 Devices, 39 Flows.
- Breadcrumbs:** User Scripts / Flows / Config Default.
- Filter Buttons:** All (22), Enabled (19) (highlighted in blue), Disabled (3).
- Search:** Security, Search Script: [empty input field].
- Table Headers:** Name, Category, Description, Values, Action.
- Table Rows:**
 - Blacklisted Flow:** Trigger an alert when a blacklisted host or domain is detected.
 - Data Exfiltration:** Trigger alerts when a possible data exfiltration activity is detected.
 - Device Application Not Allowed:** Trigger an alert when an unusual application is detected for a device. R...
 - DNS Data Exfiltration:** Trigger alerts when a DNS data exfiltration activity is detected.
 - Elephant Flows:** Trigger an alert when a flow exchanges more than the configured bytes. > 1 GB (L2R), > 1 GB (R2L). Exce...
 - Flow Risk:** Evaluate flow risks reported by nDPI.
 - Invalid DNS Query:** Trigger an alert when a possibly malicious DNS query is detected. sophosxl.net
 - Long Lived:** Trigger an alert when a flow lasts more than the configured duration. > 12:00:00. Exceptions: Database...
 - Malicious Signature:** Trigger an alert when a possibly malicious signature is detected.
 - Old TLS Version:** Trigger an alert when an old (and possibly unsecure) TLS version is dete...
- Pagination:** Showing 1 to 10 of 16 rows, page 1 of 2.

Searching Mice in Noise Traffic

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



The screenshot shows the ntopng web interface for monitoring network traffic on interface en3. The top navigation bar includes links for Home, Networks, Packets, DSCP, Applications, ICMP, ARP, and various configuration and status icons. A search bar and a protocol dropdown are also present. The main content is a table of network connections:

Protocol	Client	Server	Port	Observations	Frequency	Info
ICMP	Lucas-iMac	192.168.1.1		5372	3 sec	
TCP.TLS	Lucas-iMac	[REDACTED]	443	2	181 sec	public-api.wordpress.com
TCP.TLS	Lucas-iMac	[REDACTED]	443	2	19 sec	[REDACTED]
TCP.TLS.Cloudflare	Lucas-iMac	[REDACTED]	443	2	2 sec	[REDACTED]
TCP.TLS.DoH_DoT	Lucas-iMac	[REDACTED]	443	7	1800 sec	chrome.cloudflare-dns.com
TCP.TLS.Dropbox	Lucas-iMac	102.128.88.11	443	3	3600 sec	dl-debug.dropbox.com
TCP.TLS.Spotify	Lucas-iMac	[REDACTED]	443	3	3601 sec	gew-spclient.spotify.com

The ntop logo is visible at the bottom left, and a copyright notice for 2020 is at the bottom center. The page number 14 is at the bottom right.

Industrial IoT/Scada Monitoring [1/2]

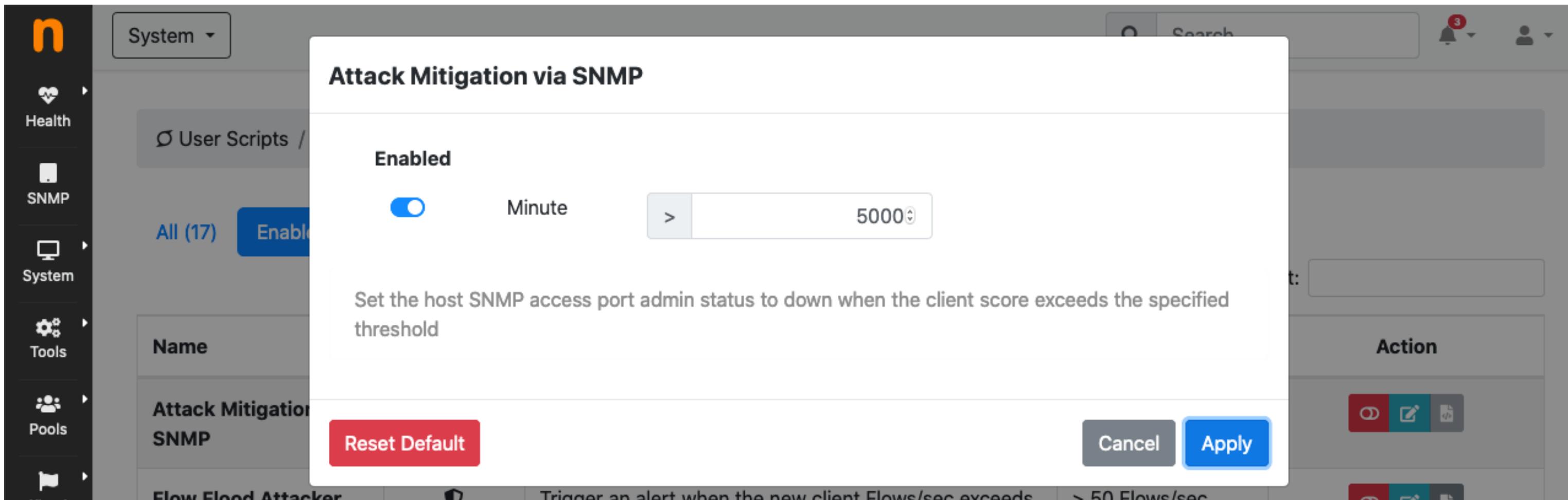
- nDPI supports some popular IoT/Scada protocols including modbus, DNP3 and IEC 60870.
- IEC 60870 is very important as it can be used to detect issues such as
 - Unknown telemetry addresses
 - Connection loss and restore
 - Loss of data coming from remote systems
- ntopng features permanent IEC 60870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

Industrial IoT/Scada Monitoring [2/2]

Flow:  Overview	
VLAN ID	21
Flow Peers [Client / Server]	
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 	<ul style="list-style-type: none">M_ME_NA_1 (9)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:   Client ← Server:  
	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]

The screenshot displays two views of the ntopng web interface.

Top View: All Hosts

- Left Sidebar:** Shows navigation links: Dashboard, Alerts, Flows, Hosts (selected).
- Header:** Interface eno1, Up/Down arrows, Bandwidth: 448.80 kbit/s (Up) / 278.30 kbit/s (Down), Alert count: 5, 5,761 Flows, 13 Devices, 16 Devices, 13,939 Flows.
- Table:** Headers: IP Address, Location, Flows, Score (sorted), Name. Data row: Flows (192.168.2.149), Local (green), 12,519, 39,650, apu. Details: Seen Since 46:54, Breakdown (Sent: 332.44 kbit/s, Rcvd: 19.07 MB), Throughput ↑.

Bottom View: Alerts

- Left Sidebar:** Shows navigation links: Dashboard, Alerts (selected), Flows, Hosts, Interface.
- Header:** Interface eno1, Up/Down arrows, Bandwidth: 37.90 kbit/s (Up) / 38.80 kbit/s (Down), Alert count: 4, 15 Devices, 22 Devices, 17 Devices, 76 Flows.
- Tab Selection:** Engaged Alerts (selected), Past Alerts, Flow Alerts.
- Table:** Headers: Date/Time, Duration, Count, Severity, Alert Type, Drilldown, Description, Actions. Data row: 00:19 ago, 1, Error, Attack Mitigation via SNMP, Drilldown, Description: Interface 63 admin status on SNMP device 192.168.2.168 set to Down: minute score crossed by host 192.168.2.149 [apu] [42360 > 5000], Actions: Disable, Delete.

<https://github.com/ntop/>

