Network Monitoring & Anomaly Detection in ISC/SCADA

SCADA Security Conference 2019 Prague

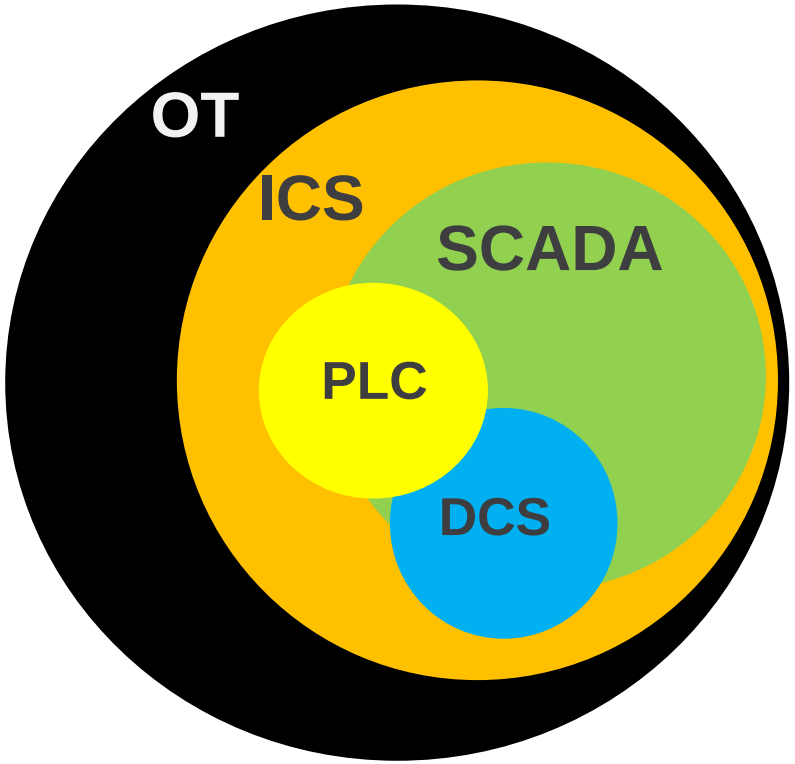
Pavel Minarik, Chief Technology Officer, Flowmon Networks

Flowmon
Driving Network Visibility

What is SCADA?

- **SCADA** is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management
- Cyber-physical system where **availability**, **performance** and **reliability** are the top concerns – **not security.**
- **Industrial Control Systems (ICS) –** geographically dispersed assets PLCs
- **Distributed Control Systems (DCS) –** locally significant controllers in a plant, they control batch-oriented (continuous) processes in refineries, petrochemical, and so on

Security Policies	IT Network	IoT Network
Focus	Protecting Intellectual Property and Company Assets	24/7 Operations, High OEE, Safety, and Ease of Use
Priorities	1. Confidentiality 2. Integrity 3. Availability	1. Availability 2. Integrity 3. Confidentiality
Types of Data Traffic	Converged Network of Data, Voice and Video (Hierarchical)	Converged Network of Data, Control Protocols, Information, Safety and Motion (P2P & Hierarchical)
Implications of a Device Failure	Continues to Operate	Could Stop Processes, Impact Markets, Physical Harm
Threat Protection	Shut Down Access to Detected Threat and Remediate	Potentially Keep Operating with a Detected Threat
Upgrades and Patch Mgmt	ASAP During Uptime	Scheduled During Downtime
Infrastructure Life Cycle	Equipment upgrades and refresh <5yr	Avoid Equipment upgrades (lifespan 15+ yrs)
Deployment conditions	Controlled physical environments	Harsh environments (temp, vibration, etc)



Flowmon
Driving Network Visibility

SCADA is Unsecure

“An important drawback derived from the connection to intranets and communication networks, is the increased vulnerability to computer network-based attacks.”

Source: European Union Agency for Network and Information Security

Non-secure / or few secure end points

Absence of network visibility

Absence of technological security design and processes

Irregular patching of IT systems

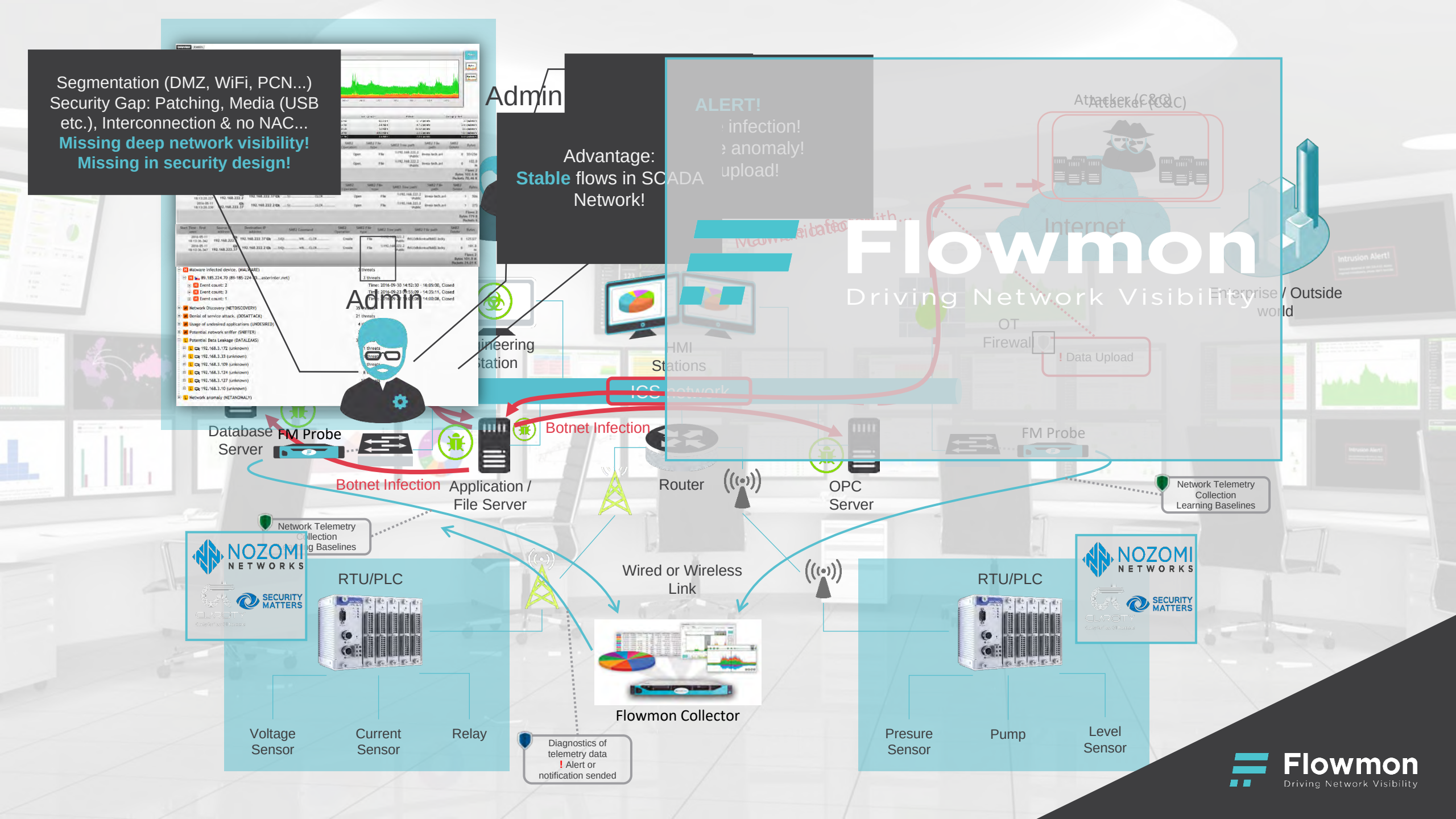
Obsolete equipment and OS

Flowmon
Driving Network Visibility

What’s inside SCADA?

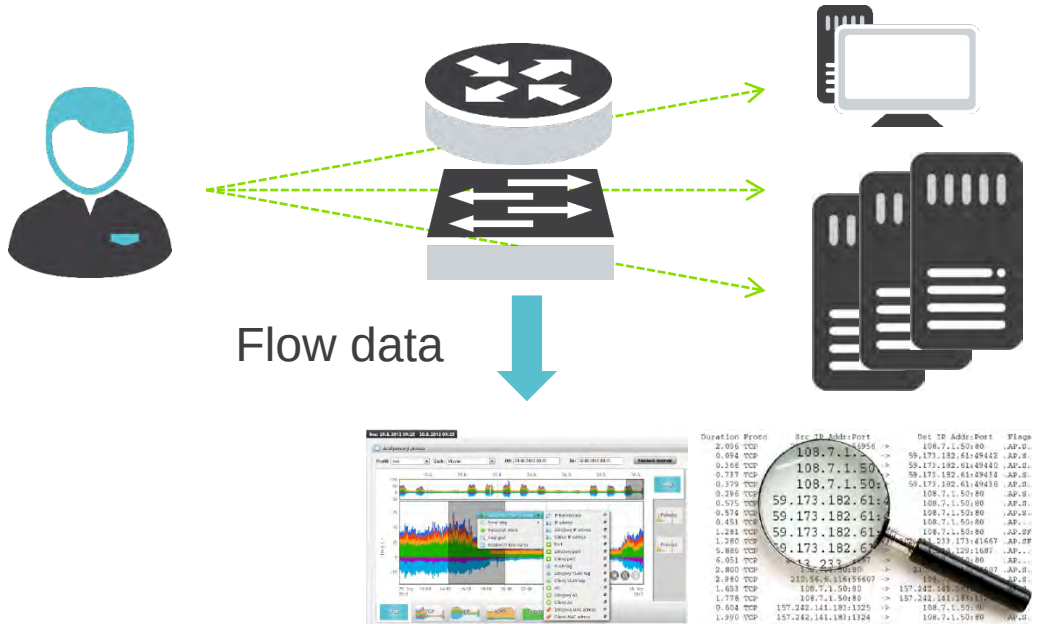
- Specialized devices with JeOS operating system
  - No password or only the default one
- "Industrial" computers with OS Windows / Linux
  - Obsolete
  - No updates/patches
  - No advanced security
- Endpoint security cannot be ensured
- Exposed to modern threats just like conventional IT environment
- Additionally, exposed to long forgotten threats

Flowmon
Driving Network Visibility

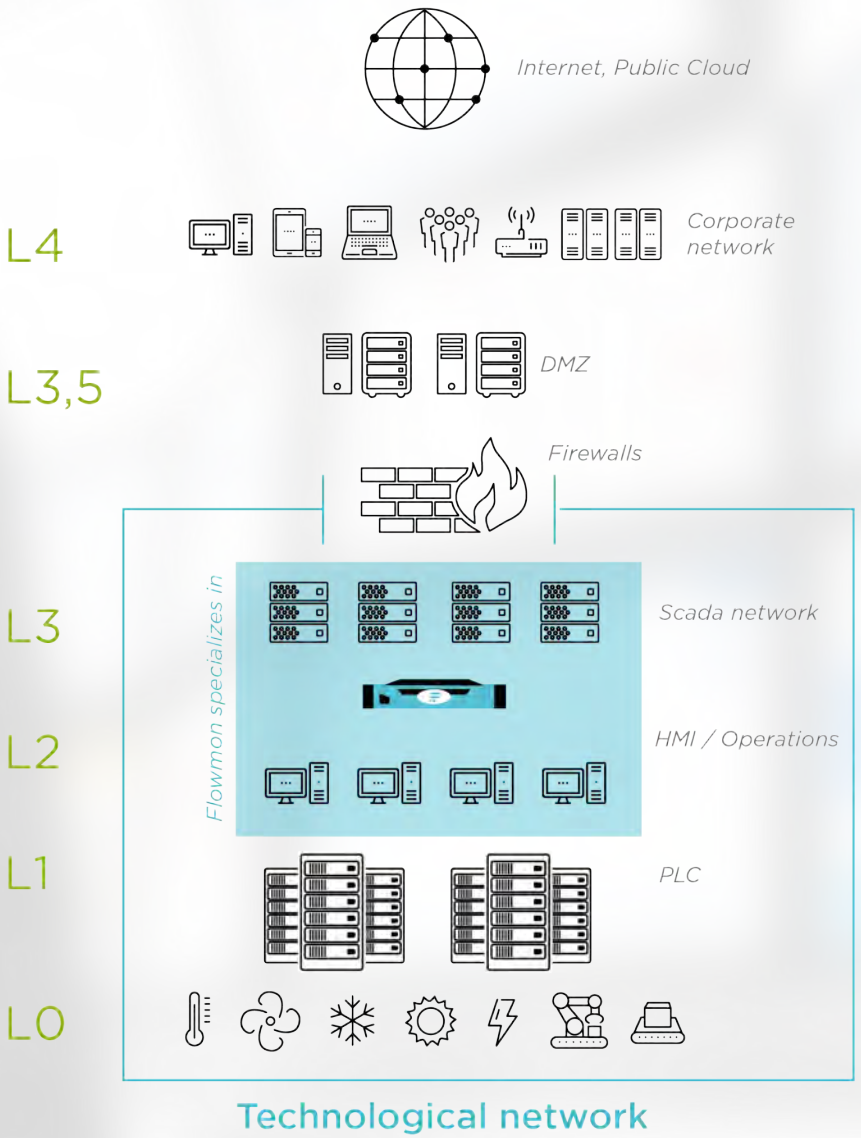

Segmentation (DMZ, WiFi, PCN...)
Security Gap: Patching, Media (USB etc.), Interconnection & no NAC...
Missing deep network visibility!
Missing in security design!
Admin
Advantage:
Stable flows in SCADA Network!
ALERT!
infection!
anomaly!
upload!
Attacker (C&C)
Internet
Flowmon
Driving Network Visibility
Enterprise / Outside world
OT Firewall
! Data Upload
Admin
Engineering Station
HMI Stations
ICS network
Database Server
FM Probe
Botnet Infection
Botnet Infection
Application / File Server
Router
OPC Server
FM Probe
Network Telemetry Collection Learning Baselines
Network Telemetry Collection Learning Baselines
NOZOMI NETWORKS
SECURITY MATTERS
CLARIOT
RTU/PLC
Wired or Wireless Link
Flowmon Collector
Voltage Sensor
Current Sensor
Relay
Diagnostics of telemetry data
! Alert or notification sended
Presure Sensor
Pump
Level Sensor
Flowmon
Driving Network Visibility

What is Passive Network Monitoring?

- Works with copy of the network traffic = no impact on network
- Provides rich network telemetry (IPFIX – IETF standard)
- Analyzes all the network layers from L2-L7
- Reduces amount of data for analysis (500:1)



Flowmon
Driving Network Visibility



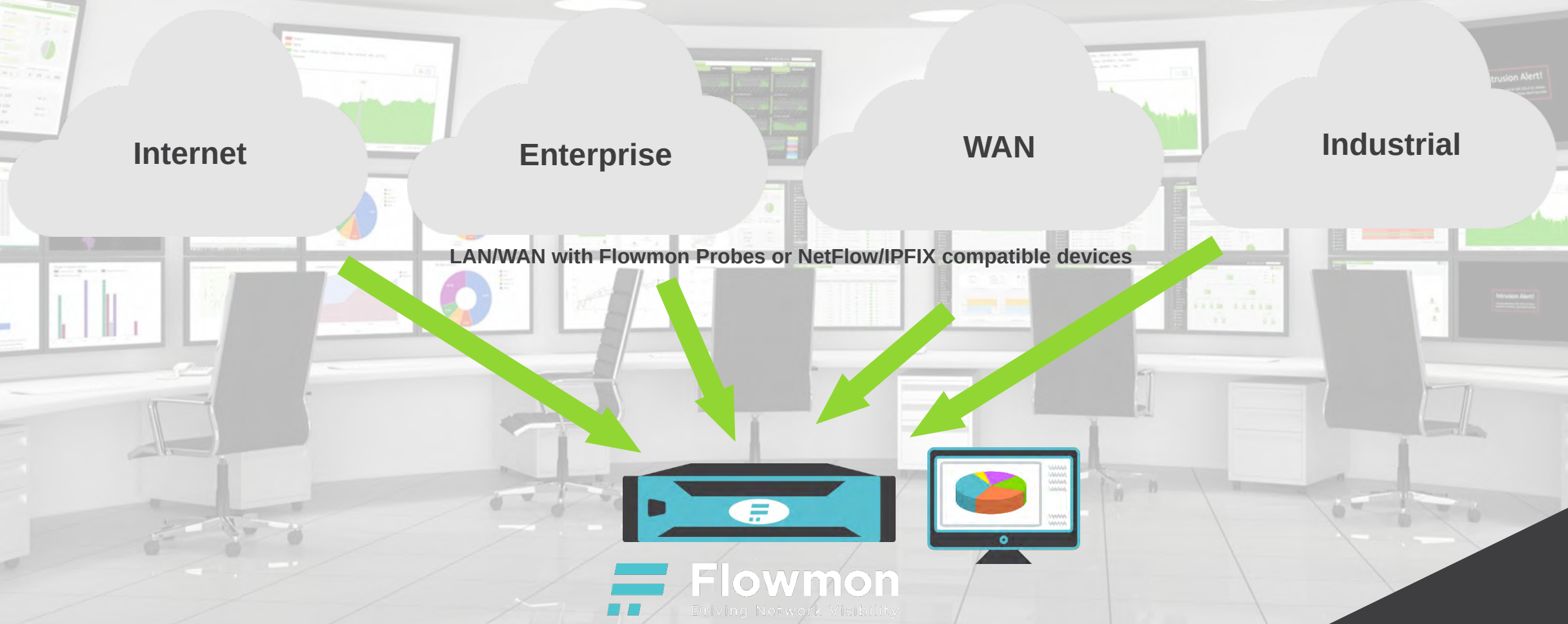
Firewalls protect communications between the perimeter of the network and the DMZ. However they do not provide any visibility and detection methods inside of the Scada environment. The easiest way to intrude and attack the Scada system is to bring an infected laptop and connect to the network e.g. during planned maintenance. Malicious activity will never be visible to the Firewall.

Flowmon specializes in the monitoring of communications inside IP networks. It provides a deep understanding of all communication between servers and end stations inside the Scada server as well as communications between Scada servers and HMIs. It provides comprehensive troubleshooting capability to tackle configurations issues, errors, as well as performance degradation. Leveraging machine learning and anomaly detection Flowmon can detect suspicious behaviour even if no signatures are available for that type of malicious behaviour.

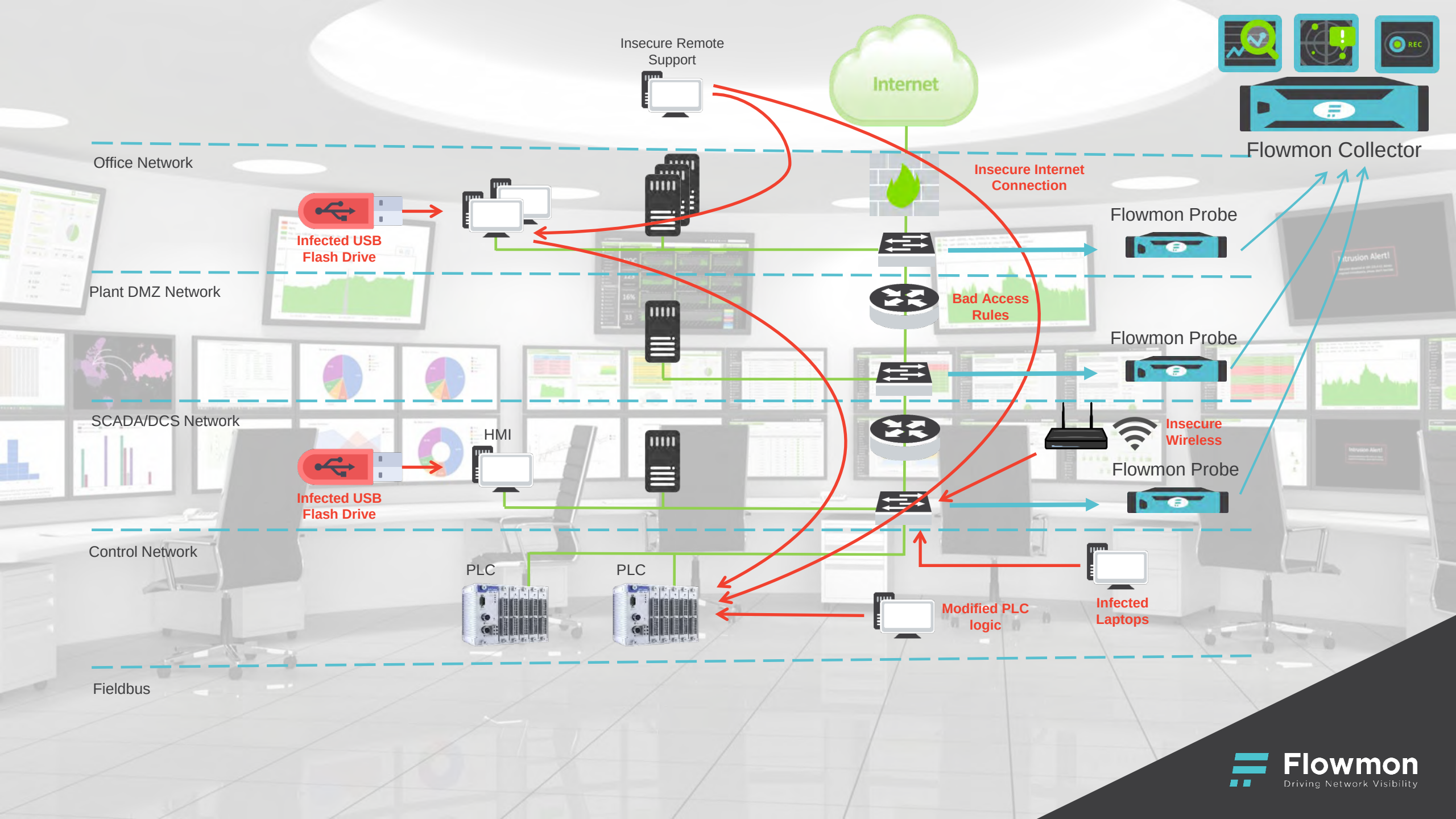
Flowmon
Driving Network Visibility

Monitoring of the Entire Attack Path

From Internet and VPN, business networks to OT environment



Flowmon
Driving Network Visibility

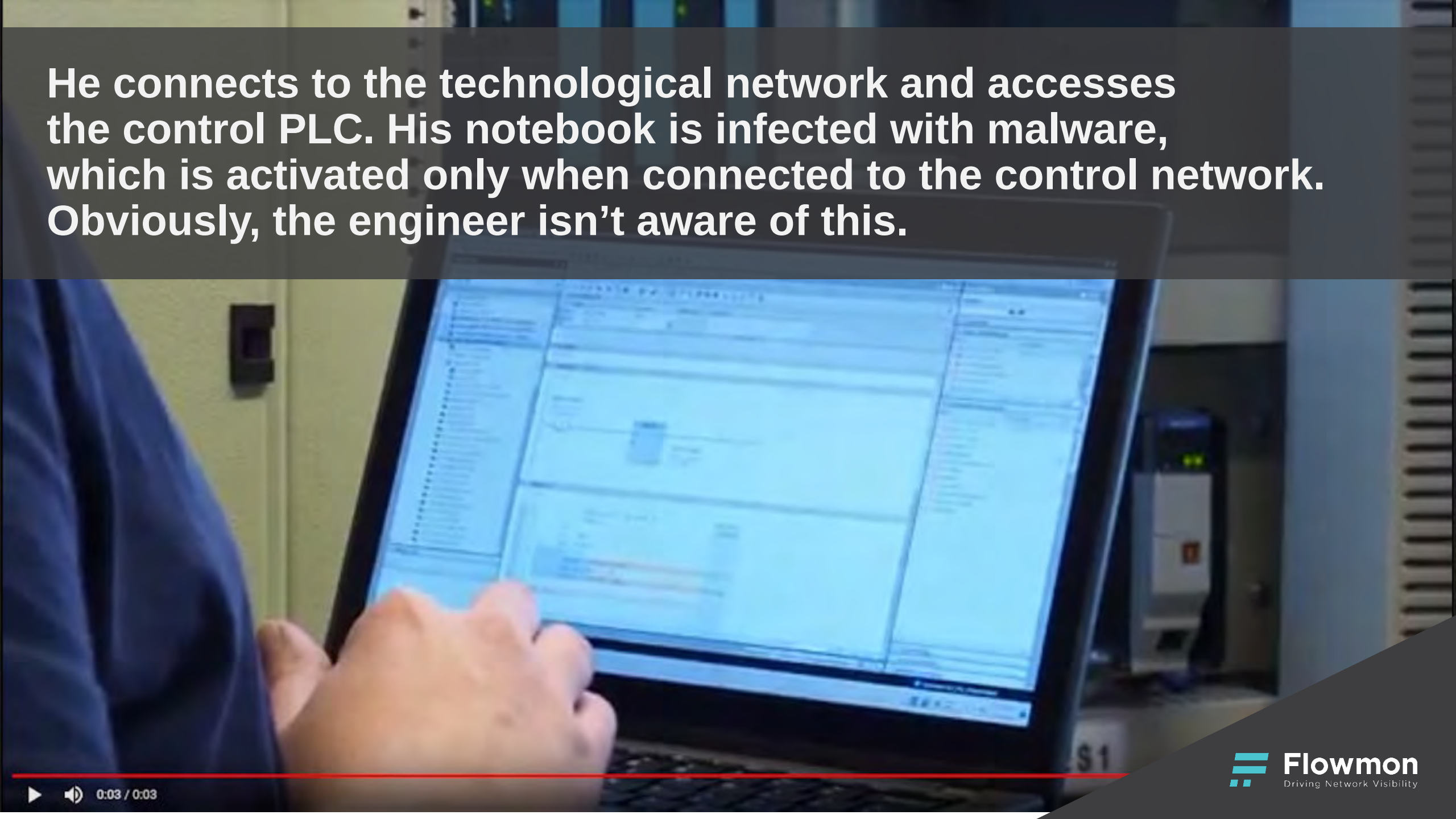

Insecure Remote Support
Internet
Flowmon Collector
Office Network
Insecure Internet Connection
Infected USB Flash Drive
Flowmon Probe
Plant DMZ Network
Bad Access Rules
Flowmon Probe
SCADA/DCS Network
HMI
Insecure Wireless
Infected USB Flash Drive
Flowmon Probe
Control Network
PLC
PLC
Modified PLC logic
Infected Laptops
Fieldbus
Flowmon
Driving Network Visibility

In this simulation we'll demonstrate a cyber attack targeting an ICS environment. ICS are systems that control industrial technologies. In our case it is a power plant. ICS/SCADA networks are generally very vulnerable to external influences, since any change can directly lead to a restriction or complete shutdown. Which subsequently leads to a huge damage to the organization and their customers. Even though we attempt to completely isolate ICS from the Internet and outsiders in general, it is never possible to contain all threats.

A suppliers service engineer enters the control system room to perform operations and maintenance checks beyond the scope of surveillance system.

Flowmon
Driving Network Visibility

He connects to the technological network and accesses the control PLC. His notebook is infected with malware, which is activated only when connected to the control network. Obviously, the engineer isn’t aware of this.



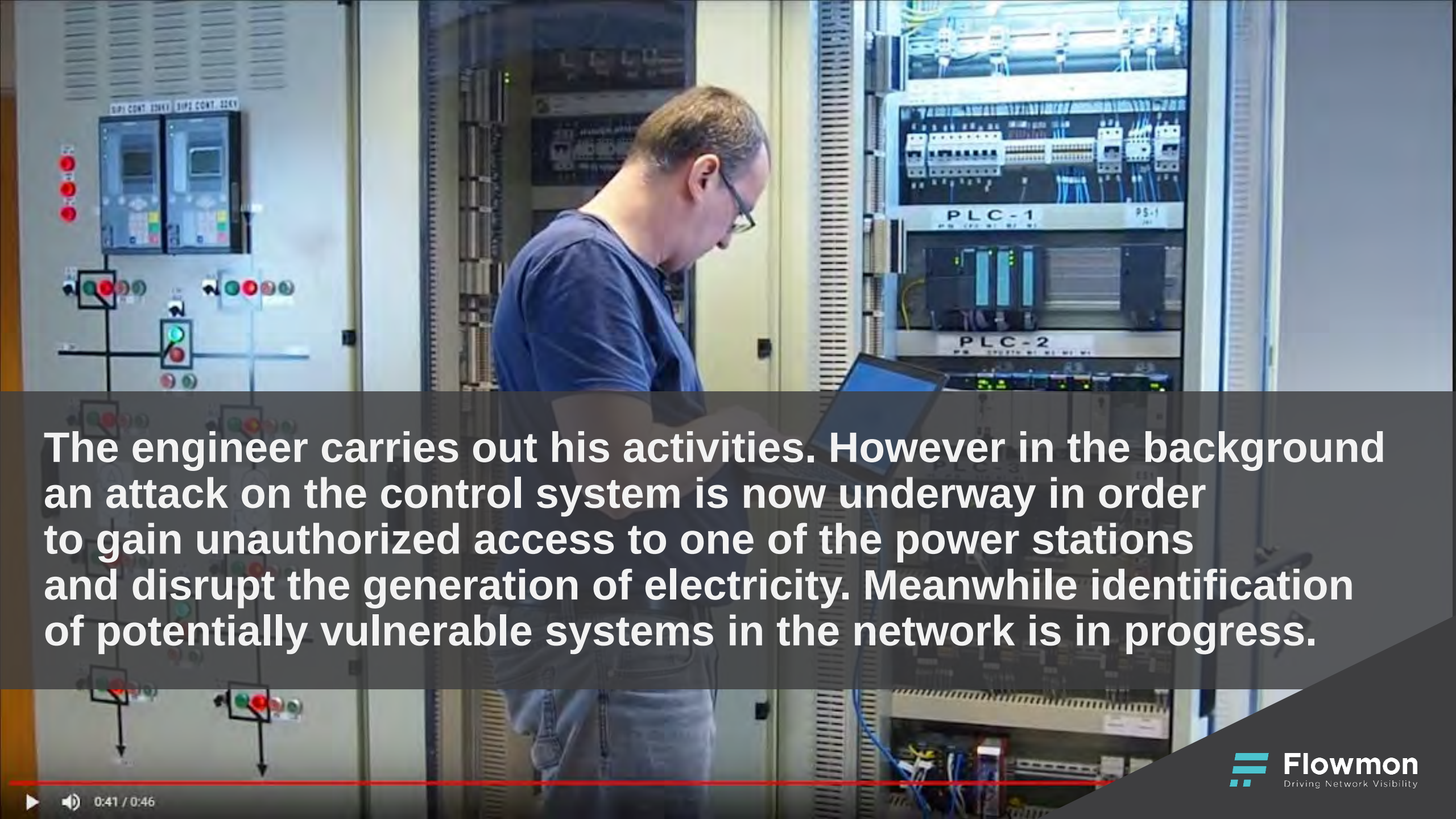
Flowmon
Driving Network Visibility

At the start of his maintenance activities, all indicators are normal. We're now looking at the temperature of the cooling medium in the tertiary circuit.

3:06 / 6:47

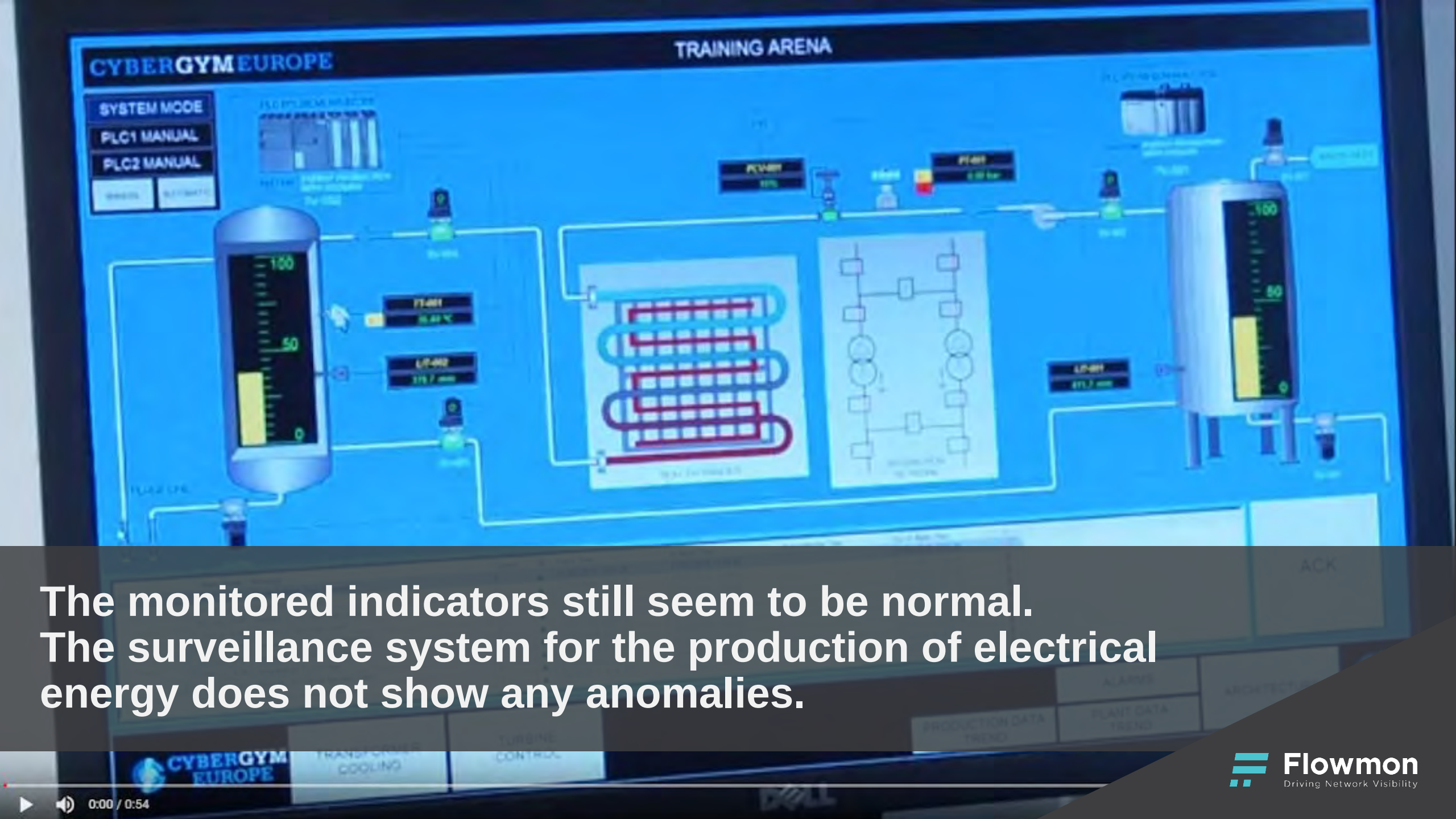
Flowmon
Driving Network Visibility


The state of the system and activities of the engineer are constantly monitored by the local surveillance center. Nothing suggests anything unusual yet.
0:01 / 0:29
Flowmon
Driving Network Visibility



The engineer carries out his activities. However in the background an attack on the control system is now underway in order to gain unauthorized access to one of the power stations and disrupt the generation of electricity. Meanwhile identification of potentially vulnerable systems in the network is in progress.

Flowmon
Driving Network Visibility



The monitored indicators still seem to be normal.
The surveillance system for the production of electrical energy does not show any anomalies.

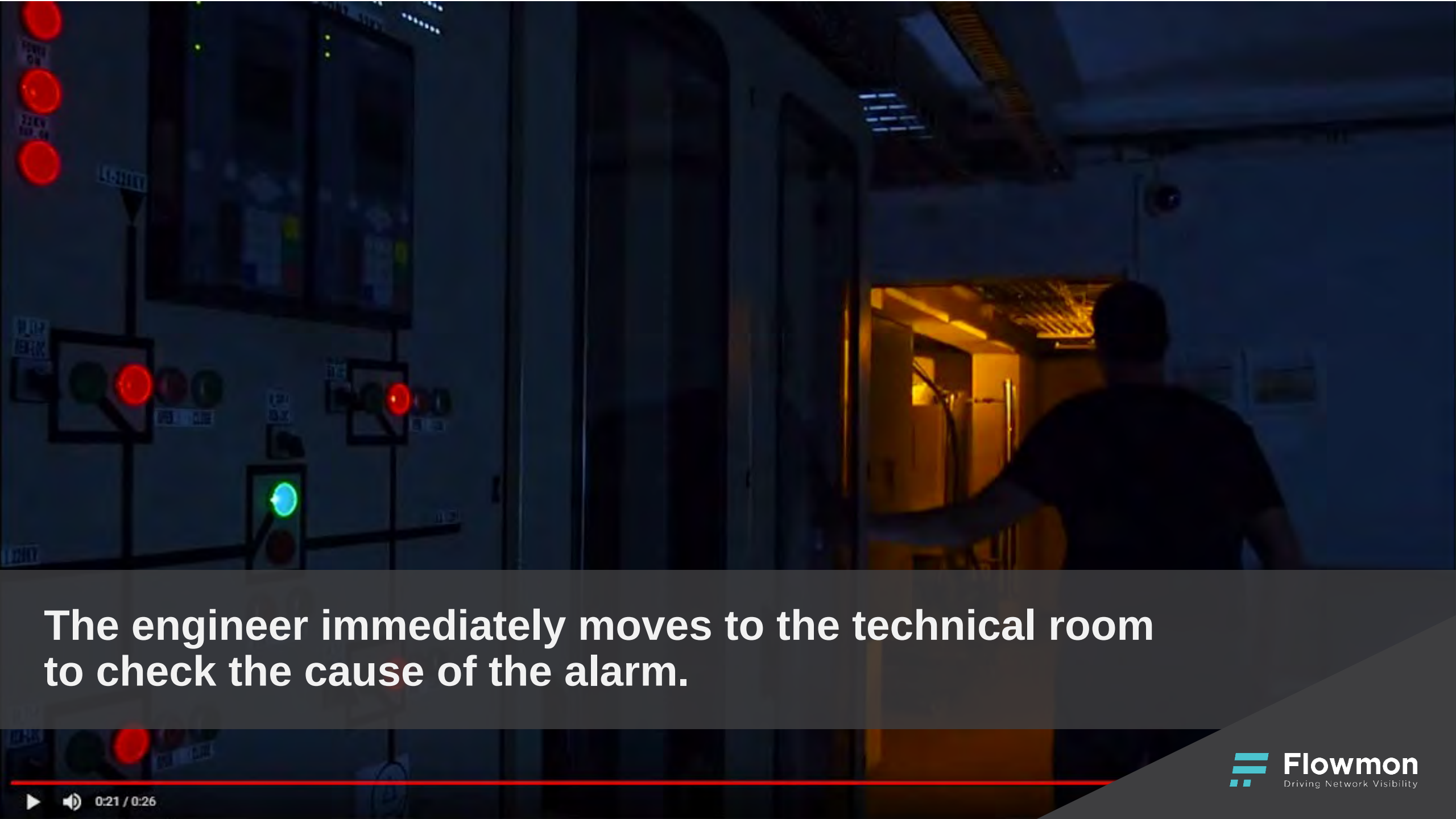
Flowmon
Driving Network Visibility

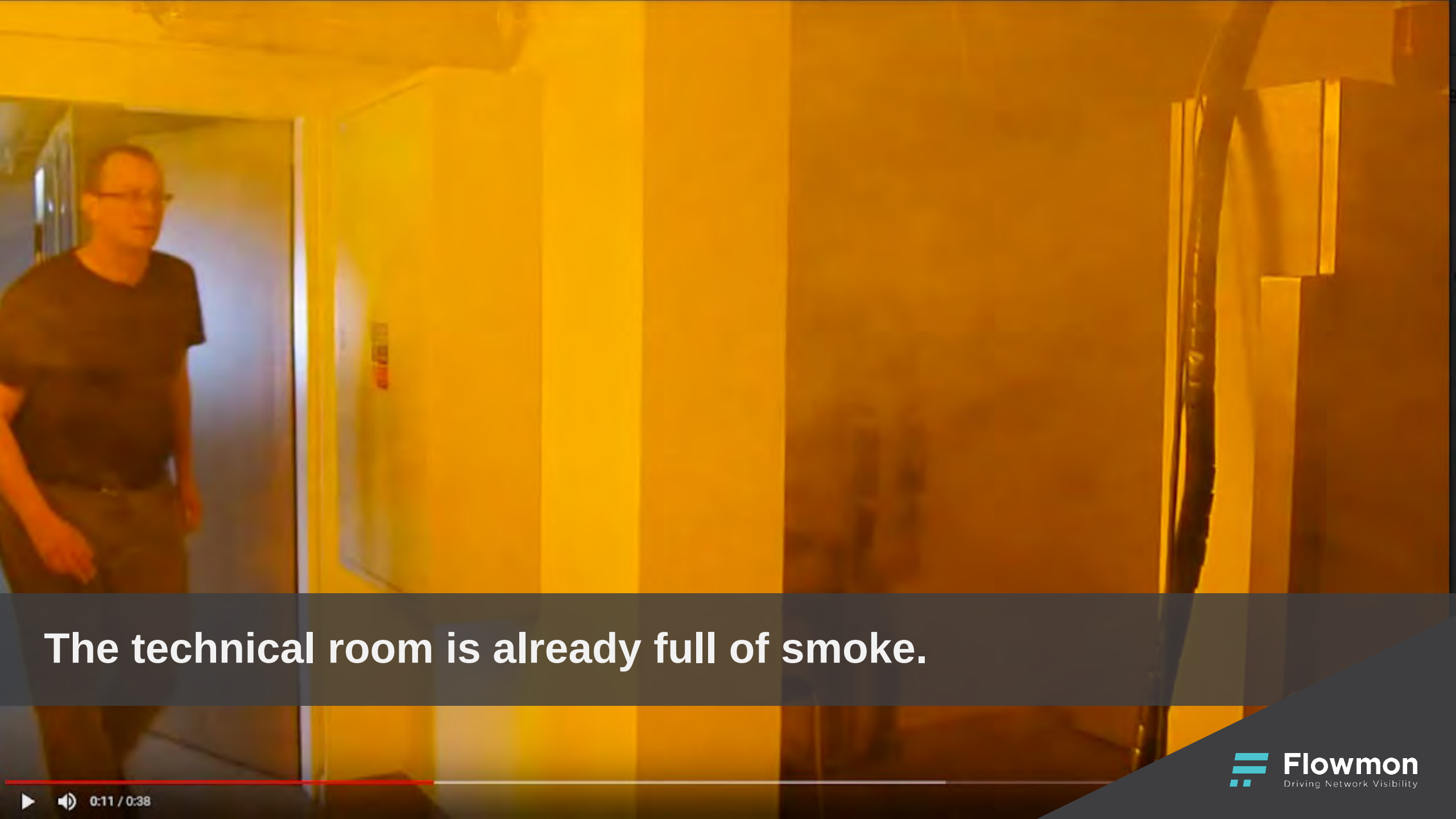

However, the system has been compromised and the temperature of the cooling medium is rising.
0:01 / 0:07
Flowmon
Driving Network Visibility


The engineer has finished his work, disconnected from the system and now leaving the facility.
0:02 / 0:05
Flowmon
Driving Network Visibility

When a critical temperature is reached and an alarm is triggered.

Flowmon
Driving Network Visibility


The engineer immediately moves to the technical room
to check the cause of the alarm.
0:21 / 0:26
Flowmon
Driving Network Visibility



The technical room is already full of smoke.

Flowmon
Driving Network Visibility

The engineer is manually shutting the system down to remediate the situation.

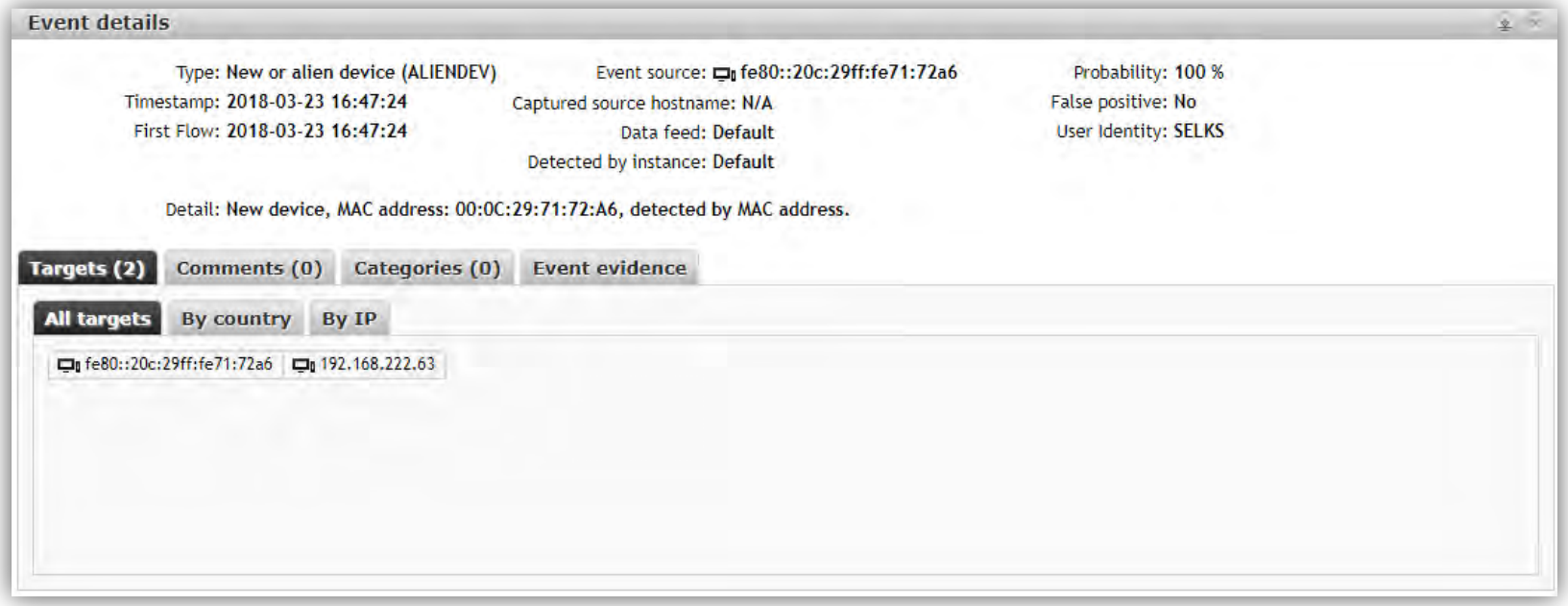
0:02 / 0:13

Flowmon
Driving Network Visibility

This power plant was fortunate to have an engineer on site who could manually intervene. If that hadn’t been the case, the damage would’ve been inevitable. Now let's take a look at how little it would take to detect and resolve the problem in timely manner.

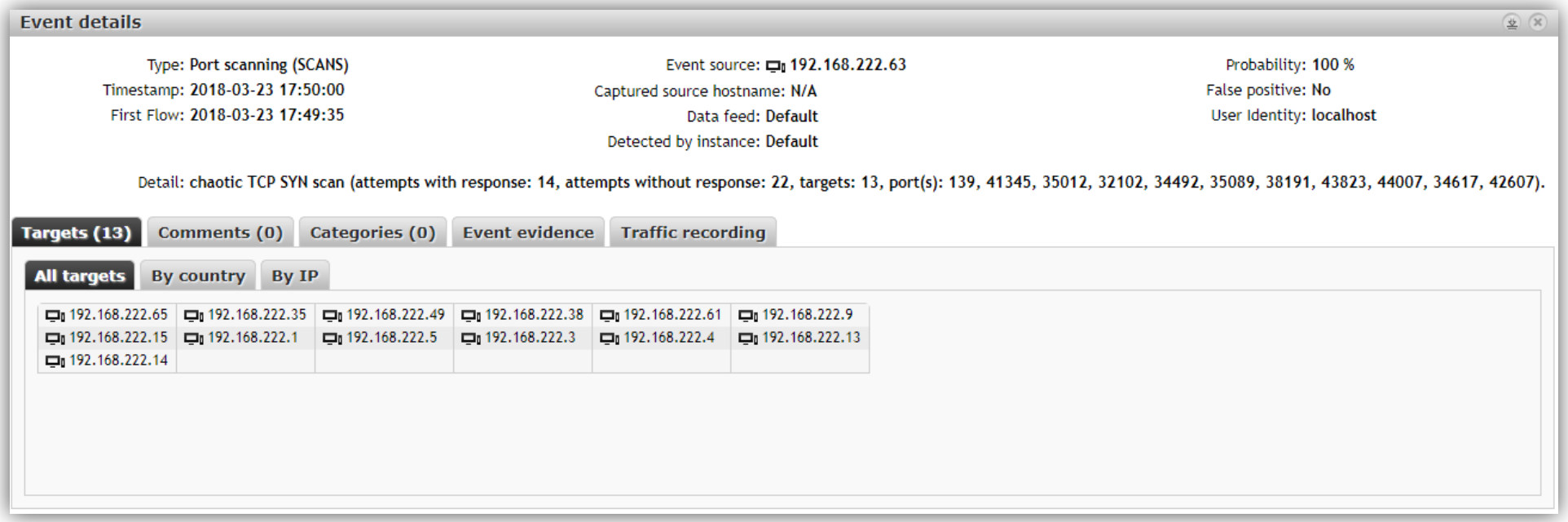
Flowmon
Driving Network Visibility

At the time of connecting to the control network, Flowmon ADS identified a new device in the network. This is expected behavior, because the new device was actually connected.



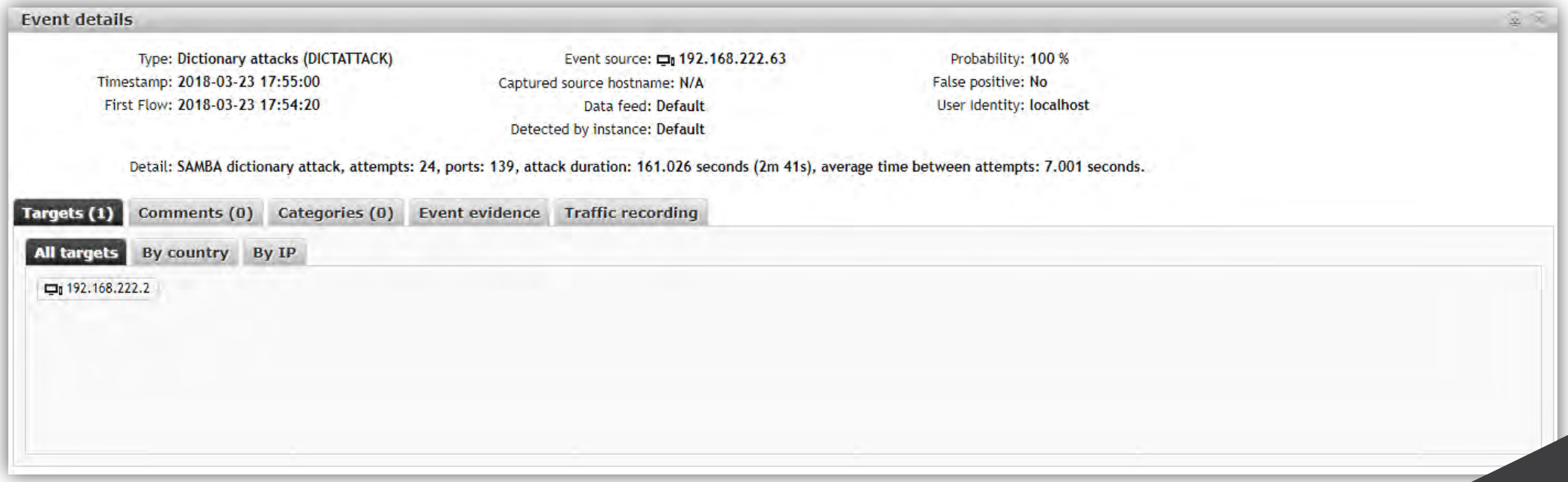
Flowmon
Driving Network Visibility

During the engineers activity, malware looks for devices in the network which can be attacked. The scan runs on port 139, the Samba protocol, which has a number of vulnerabilities.



Flowmon
Driving Network Visibility

Subsequently, malware attacks the vulnerable station in order to gain unauthorized access, escalate permissions, and damage the production process. We can see an event that represents the described attack.



Flowmon
Driving Network Visibility

Monitoring and early detection of security incidents is essential for the protection of SCADA/industrial control systems. Their independence and separation from the surrounding environment does not mean these systems cannot be the target of an attack. ICS systems are functional and reliable, but based on legacy technologies which goes hand in hand with their security. Imagine the possible consequences of this attack happening in a nuclear power plant. That said, visibility into network communication and early detection is vital.

Flowmon
Driving Network Visibility

Thank you

Performance monitoring, visibility and security
with a single solution

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Czech Republic
www.flowmon.com

Flowmon
Driving Network Visibility