Maximize Security

Comprehensive Techniques for Boosting Protection and Accelerating Forensics

Industrial Cyber Security

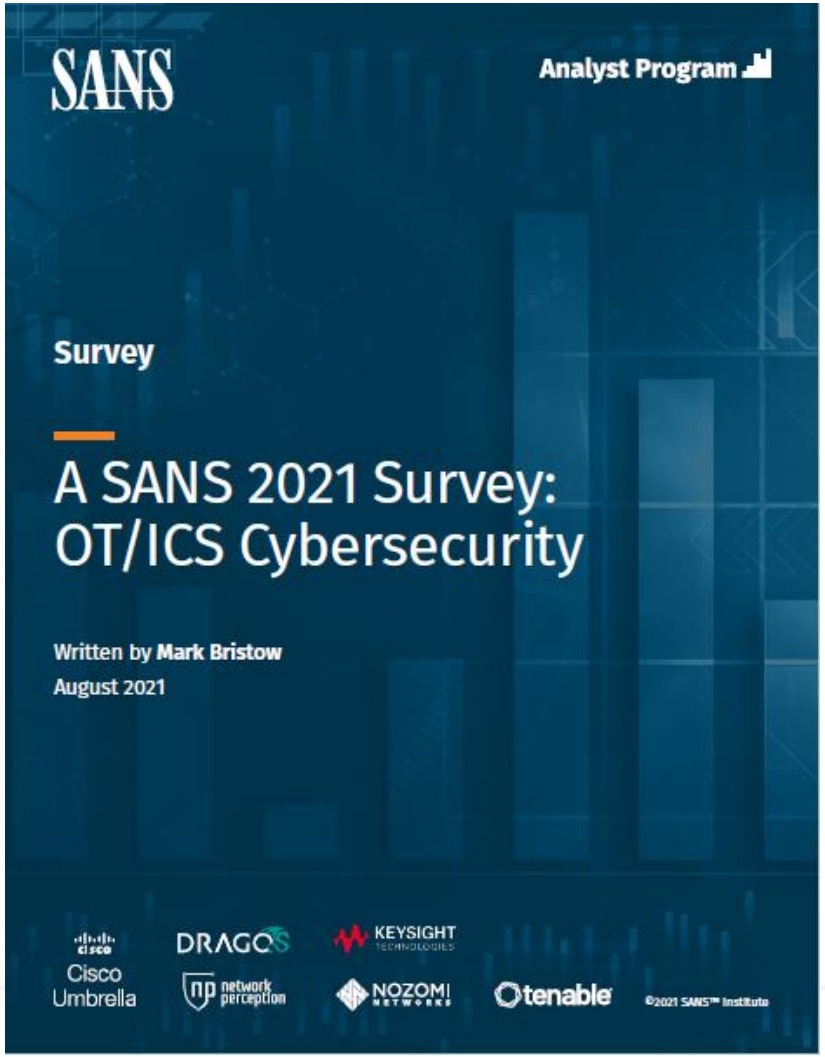
10 oktober 2023 | Congrescentrum 1931, den Bosch

Roxana Magdo, GICSP
Director, Business Development
KEYSIGHT TECHNOLOGIES

What is happening today in the industrial world?

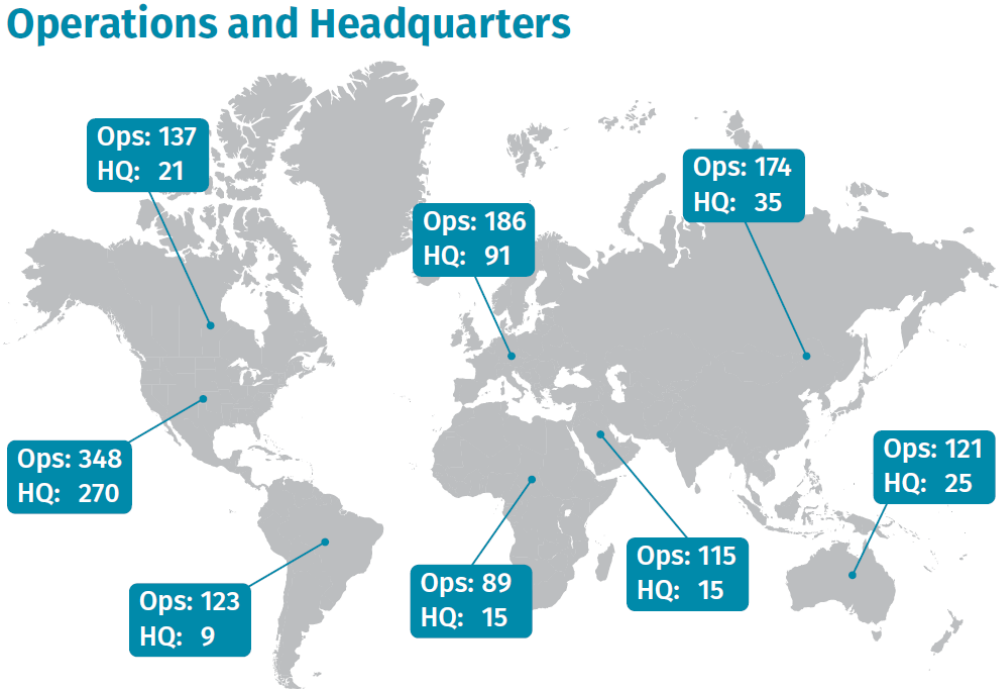
- The survey had over 480 responses.
- 12.5% of respondents confident they had not experienced a compromise in the past year
- 48% of survey participants not knowing whether they suffered an incident

SANS SURVEY FROM 2021 ON OT/ICS CYBERSECURITY



Are the industrial companies in the world secured?

- Almost all respondents indicated having at least one incident in the last year
- 90% of the incidents had some level of impact on the Process.

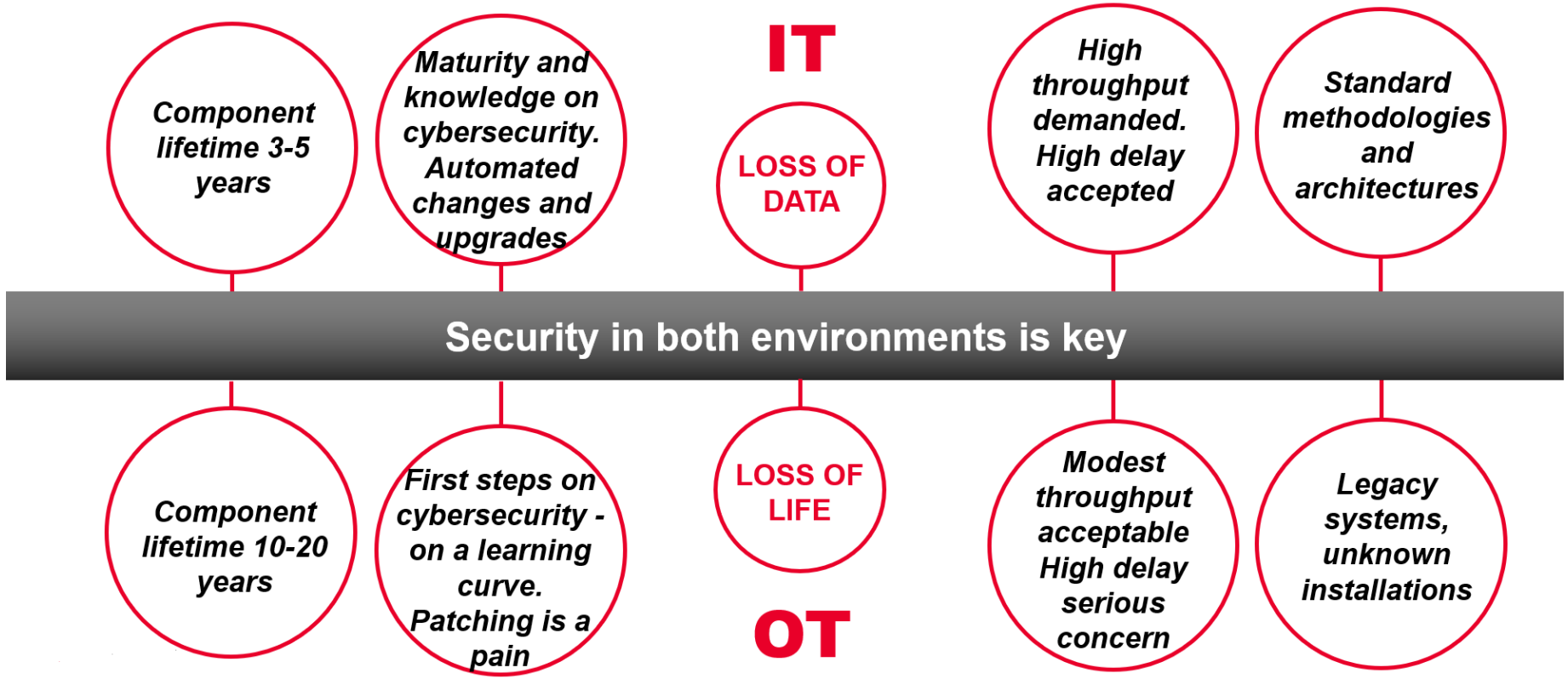


- Asset inventories continue to challenge most organizations.
- Biggest challenge:

59.4% Technical integration of legacy and aging OT technology with modern IT systems

- Yet only high-profile incidents such as Colonial attack make headlines.

What is the difference with IT world?



Some of the challenges in securing OT world. Techniques we can use.

- Lack of available ports that could be used in mirroring mode

USE CASE:

NEED TO ANALYZE PACKETS FROM A SWITCH THAT HAS NO FREE PORTS FOR MIRRORING

One important way to keep the OT network secure is to use different Security tools. These tools need to analyze the data that flows through the network to see if there are breaches or risks for being breached.

SOLUTION:

USE TAPS TO GET A COPY OF THE TRAFFIC FROM THE SWITCH PORT

Connecting the TAP into the switch port is a rapid and safe solution, which does not require planning a long maintenance window.

Some of the challenges in securing OT world. Techniques we can use.

- Legacy equipment is always a challenge to manage and secure

USE CASE:

ANALYZE PACKETS FROM A SWITCH THAT "WE DO NOT WANT TO TOUCH" ☺

We all heard of this situation: there are old switches in the network, installed in the past, by 3rd parties, we do not have the possibility to upgrade or change them now and they work just fine. We do not want to change the config on them to add SPAN ports.

SOLUTION:

CONNECT TAPS IN THE EXISTING PORTS AND RETREIVE A COPY OF TRAFFIC

A copy of the traffic can be retrieved from the switch without configuring a SPAN port. Adding a TAP does not involve any change on the switch configuration.

Some of the challenges in securing OT world. Techniques we can use.

- Adding a HW probe in the network incurs adding more risk

USE CASE:

ADDING A HARDWARE RUNNING SOFTWARE ON IT, AS AN APPLIANCE BRINGS ADITIONAL SECURITY RISKS

Many security solutions function via appliances that are deployed in the OT network to collect a copy of the traffic from the switches and then forward it to a centralized analyzing server. These appliances pose a risk as any other HW and SW element

SOLUTION:

TAPS:
* **ARE NOT IP ADDRESSABLE**
* **DO NOT HAVE MEMORY**
* **FAIL OPEN**

One of the main concern when adding lower SCADA level elements is the introduction of additional risks. The use of TAPs provide visibility without having to compromise

Some of the challenges in securing OT world. Techniques we can use.

- Multiple TOOLS need the same traffic for security and monitoring analysis

USE CASE:

THE SAME TRAFFIC NEEDS TO BE ANALYSED BY DIFFERENT TOOLS SIMULTANEOUSLY. ALSO PORTS ARE AT DIFFERENT SPEEDS.

The challenge of getting access to all of the traffic in multiple instances is always there. Several tools are needed to have concurent access to the same OT data, so that different types of analysis can be performed.

SOLUTION:

AGREGATE THE TRAFFIC COLLECTED FROM THE OT NETWORK THROUGH TAPS AND SPAN PORTS INTO A PACKET BROKER

A packet broker placed at Level 4 in SCADA model architecture can collect the traffic copied by the TAPs and SPAN ports and replicate it in real time such that several tools can use it. Packet brokers have multiple ports with multiple speeds

Some of the challenges in securing OT world. Techniques we can use.

- Need to filter which traffic is sent to what security tool

USE CASE:

NOT ALL THE TRAFFIC FROM THE OT NETWORK NEEDS TO BE SENT TO ALL TOOLS

In many cases, there is traffic that runs through the OT network and does not need to be subjected to security tools inspection. Sending such traffic to the tools, increases the bandwidth (ports) needs and overwhelms the tools with additional non needed tasks such as filtering.

SOLUTION:

AGREGATE THE TRAFFIC COLLECTED FROM THE OT NETWORK THROUGH TAPS AND SPAN PORTS INTO A PACKET BROKER

A packet broker can, in addition to gathering and replicating traffic in real time, to also filter traffic based of different criteria. The most performant packet brokers can filter traffic based on application OSI level.

Some of the challenges in securing OT world. Techniques we can use.

- Maintenance windows are always hard to plan

USE CASE:

SCHEDULING MAINTENANCE WINDOWS FOR ALL THE TOOLS THAT ANALYZE THE TRAFFIC IS A CHALLENGING.

Using more tools improves the security posture but it increases the challenge of maintaining them, as well as changing configurations or upgrading them without interrupting the network.

SOLUTION:

WHEN TOOLS ARE CONNECTED TO A PACKET BROKER, THEY CAN BE SAFELY INDIVIDUALLY DISCONNECTED WITHOUT AFFECTING NETWORK FUNCTION

The packet broker will continue to send the traffic to the relevant tools even if one of the tools gets disconnected is up for maintenance or configuration changes.

Some of the challenges in securing OT world. Techniques we can use.

- Industrial networks are often subjected to extreme temperatures and humidity

USE CASE:

THE OT NETWORK IS SUBJECTED TO SPECIAL ENVIRONMENTAL CONDITIONS SUCH AS EXTREME HEAT OR HUMIDITY

Many of the industrial network elements are either running in small rack spaces or in DIM mountable racks. However, even with these limitations, traffic needs to be retrieved to be sent to the security tools.

SOLUTION:

THERE ARE SPECIFIC INDUSTRIAL TAPS AND PACKET BROKERS WHICH ARE RESITENT TO HEAT AND HUMIDITY

For the challenging environment, the hardened TAPs and Packet Brokers can withstand temperatures of 85C and humidity up to 95%

Some of the challenges in securing OT world. Techniques we can use.

- Secure a network where the rack space is very limited

USE CASE:

THE OT NETWORK IS SUBJECTED TO LIMITATIONS IN RACK SPACE

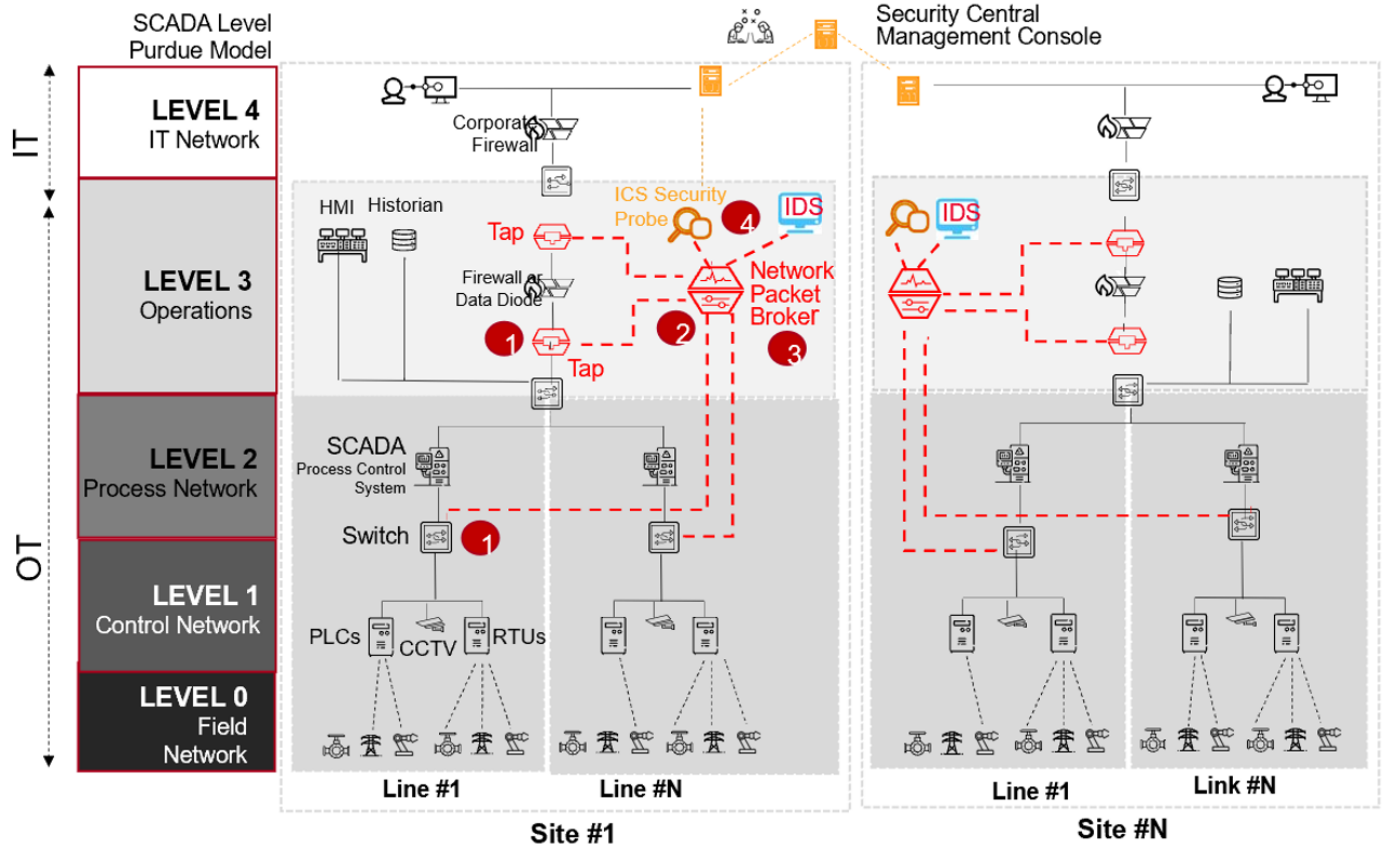
Many of the industrial networks are either running in factories or in outside places where the weather can bring a challenging condition for regular hardware equipment. But even is such conditions, the traffic that runs through the network needs to be collected and then analysed.

SOLUTION:

THERE ARE SPECIFIC INDUSTRIAL TAPS WHICH ARE DIN MOUNTABLE

Same way as industrial specific TAPs are build to resist extreme conditions, there are as well such TAPs that are DIN mountable and have specific PSU.

Visibility from OT design is they key to overcome many challenges

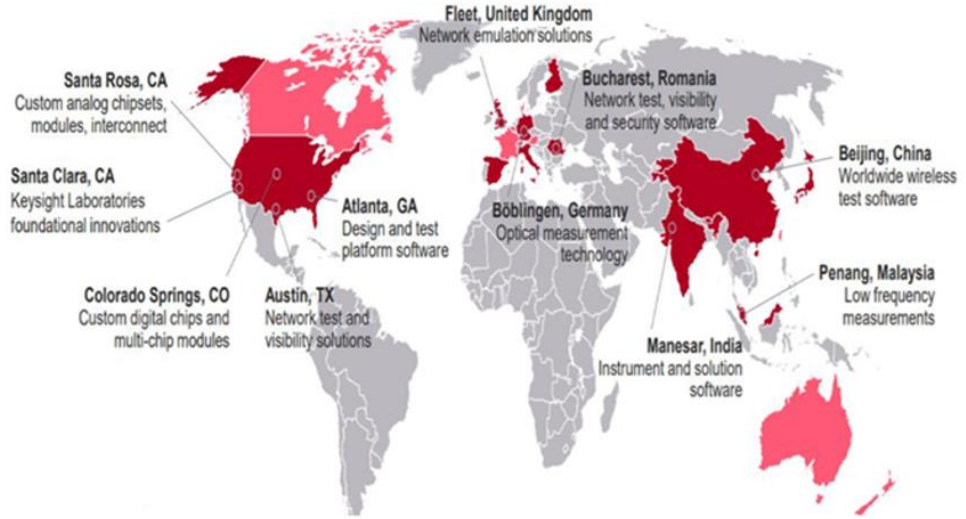


1. Tap or SPAN traffic in Layers 2/3/4 for full visibility
2. Aggregate traffic to NPM in Layer 3 to simplify security tool deployment
3. Filter out unneeded traffic (ex. CCTV) to maximize tools
4. Share traffic with multiple tools

NOZOMI NETWORKS · DRAGOS · armis · DARKTRACE · FORESCOUT · Indegy · SCADAfence · CLAROTY · corelight

Why Keysight?

- What drives our customers to trust and work with Keysight for OT visibility



5.4Bn USD revenue
33Bn market capitalisation
14,300 employees
32,000 customers in 100+ countries

- 25 of 25 Top Auto electronics suppliers
- 25 of 25 Top Semiconductor suppliers
- 25 of 25 Top Engineering & Tech Uni's
- 29 of 30 Top Technology companies
- 24 of 25 Top Telecom equipment co's
- 23 of 25 Top Aerospace and Defence contractors.

- $700m annual R&D investment
- 13 R&D centres around the world
- 3,000 patents
- Strategic University Research

- Network and Mobile 5G, WIFI 6, 6G
- Driverless Vehicles and IoT
- Aerospace and Defence
- Quantum and next gen security