OT Security Services

August 2024

Breakfast Briefing

Agenda

1/ Introduction

1. Personal introduction
2. About CSIS

2/ OT Services

1. Asset Discovery
2. Security Assessment
3. Purple Teaming
4. OT Emergency Response Retainer
5. 24/7 Monitoring

3/ Wrap up

1. Open discussion Q/A

CSIS

Founded in **2003**
Independent **Danish** Cyber Security House

Acknowledged by **Gartner Group**

Trusted adviser for the **FBI**, **NCA**, and **Europol**

Regularly called upon as **expert commentators**

Hundreds of incident response cases

Cyber security **professionals** across Europe.

Industrial modernization has made OT integral to companies

OT and IT are no longer segregated

51% have the OT network connected to their IT network. [1]

81% of client environments had 3+ CVEs with known exploits – many of which cannot be patched. [2]

56% have OT devices connected to the Internet. [1]

46% have detected malicious cyber activity in their OT networks. [3]

1 https://www2.deloitte.com/us/en/pages/risk/solutions/industrial-iot-otproduct-security-cybersecurity.html

2 Percentage of client environments with Critical CVEs or CVEs with known exploits. Source: Red Hat Insights: https://www.ibm.com/downloads/cas/L0GKXDWJ

3 https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-global-reportfinds-75-percent-ot-organizations-experienced-intrusion-last-year

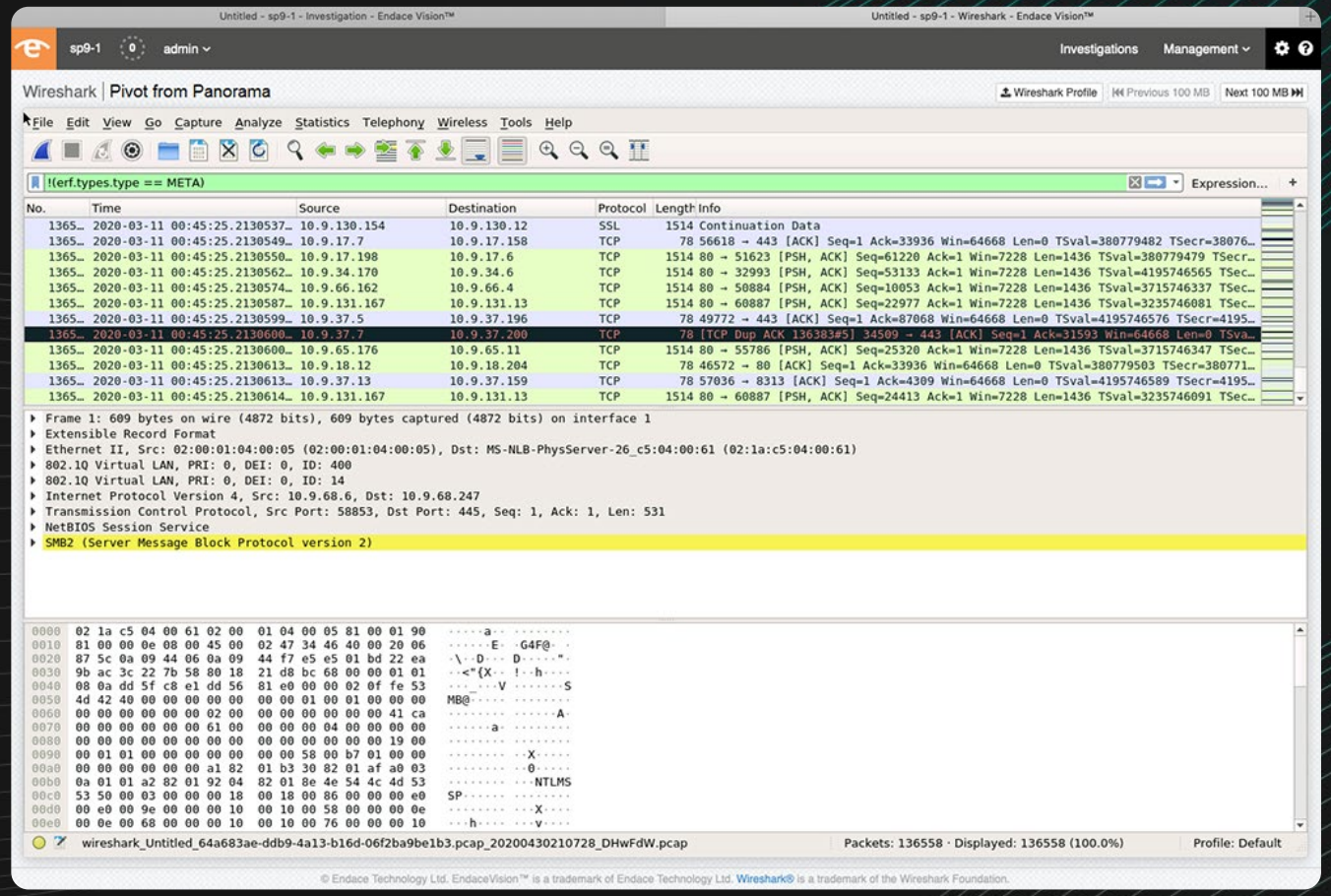
Asset Discovery

Asset Discovery

Why is it needed?

- You can only protect **what you know**.
- Companies have up to 20% unknown devices.
- For us an asset is a Device, model and firmware

Asset Discovery



- Only PCAP file needed
- Discover potential rogue devices
- Prioritized list of risks
- Step-by-step mitigation

FAQ – Asset Discovery

Does it affect my setup?

No. We are **passively** collecting the **PCAP** file.

What value am I getting?

Finding unknown devices and vulnerabilities and comprehensive mapping of devices and network-identifying anomalies.

How long does it take?

The assessment is running over period of 1 week.

Involvement needed

Minimal (2 hours).

What is included in the report?

A detailed devices and prioritised risks found and how to mitigate these risks.

Why CSIS?

CSIS is combining a range of commercial tools to optimize output quality.

OT Purple Team

Purple team testing

Why is it needed?

- Testing resilience.
- Simulation based training.
- Enhance your detection capabilities.

OT Purple team

Tried and tested approach

Mapped in against ICS MITRE ATT&CK

SOC aware / unaware

Reduce your attack surface

FAQ – Purple Team

What is needed?

We need access to 6 devices that are assessed as **non-critical**

What value am I getting?

Enhancement of detection capabilities. And all PCAP files from the test pc.

How long does it take?

The Purple-Team test a one day workshop.

Involvement needed

SOC team will have to be involved if that is the type of purple-team selected.

What is include?

A detailed report, containing all findings from all attacks and improvement recommendations.

How many attack phases?

We are running 12 different attack phases, with increasing complexity.

Why CSIS?

Based on our Incident response, and offensive experience we know what tools and processes by the malicious actors

OT Security Assessment

OT Security Assessment

Why is it needed?

- Testing your products – Less risk for your costumers.
- Can save your cost at the production floor level.
- Testing of critical and or expensive units.

OT Security Assessment

Something you invest in:

- Factory assets.
- Product components

Something you sell:

- Hearing aids
- Radars
- Smart meters
- Software

20+ CVE found during these tests.

Secure production continuity.

How to harden your products.

Actionable recommendations.

FAQ – OT Security Assessment

What is needed?

We require access to a device with the same brand and version as the one running in production.

What value am I getting?

Blackbox Testing.
Greybox Testing.
Whitebox Testing.

How long does it take?

Yes, we have 9 CVE´s + 15 not credited directly.

Involvement needed

Minimal (only devices needed).

What is include?

A detailed report containing all vulnerabilities found, and recommendation on product hardening + a presentation meeting.

How many attack phases?

We are scoping everything on an ad-hoc basis, contact your sales representee for more info.

Why CSIS?

Drawing on our extensive OT research experience and with the only person globally awarded with 4/4 technical challenge coins by SANS on board.

OT 24/7 Monitoring

The Service

24/7 Monitoring and Non-Invasive.
Escalation of Potential Threats.

Enhanced compliance for Multi-Layered Protection.

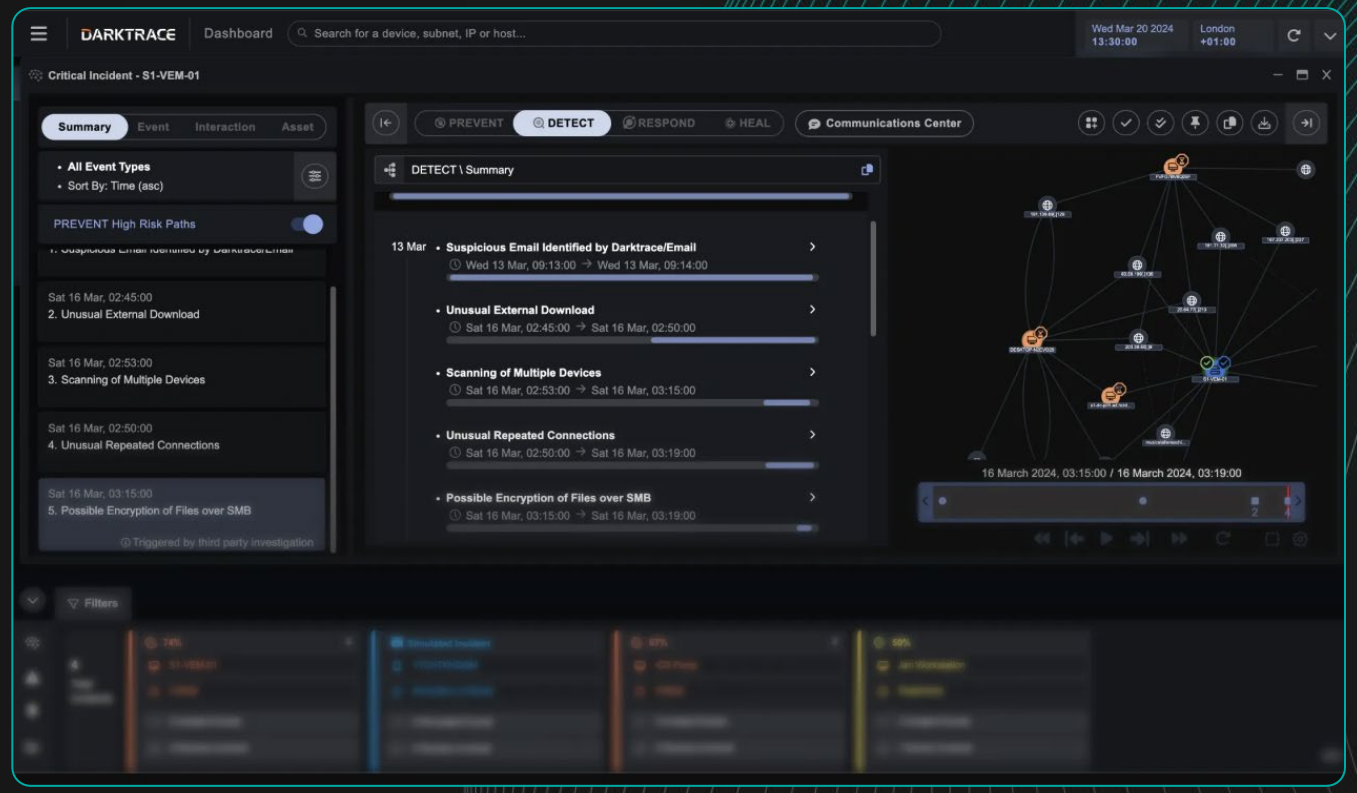
Cross-Technology insights between your IT and OT infrastructure.

The Team

Europe-based Cyber Security Analyst team.

20+ Full-Time Analysts with Expertise in Identifying and managing Cyber Incidents.

Convergence of OT and IT



- Unify IT and OT teams via a single communication platform.
- Ensure the protection of all interconnected production-driving devices within a trusted platform.
- Blend comprehensive coverage of industrial protocols/devices with top-tier IT activity analysis.
- Execute effective risk mitigation with or without patch implementation.
- Utilize MITRE mitigations and Darktrace guidance for executing preventative measures and reducing risks.

OT Incident Response Retainer

OT Incident Response Retainer

Why?

- Breaches can, do, and will happen.
- Can be targeted for OT or come from IT.
- No organization can consider itself impervious to a breach.
- Hackers do not operate on a '9 to 5' schedule.

What is included

- 24/7 Support Hotline
- Incident response start-up < 4 hours
- Threat Intelligence Portal Access
- Quarterly Threat Landscape Webinars

Have a trusted partner

- You need to know whom to call
- You need to know what will happen next
- You need to trust that you are in the expert hands

OT Incident Response Retainer

Access to experts 24/7

4 Hour Service Level Agreement (SLA)

PCAP files needed

2 Day Onboarding workshop

Participated in 200+ cases during last year.

Thank you!

Lars Henriksen – lhe@csis.com