



OT Security Services

August 2024

Breakfast Briefing

This presentation may contain confidential information and is intended only for the individual or entity stated above.

Agenda

1/ Introduction

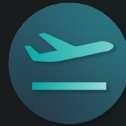
1. Personal introduction
2. About CSIS

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



Founded in **2003**

Independent **Danish** Cyber Security House



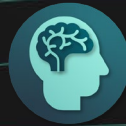
Acknowledged by **Gartner Group**



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-iiot-product-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/LOGKXDWJ>

³ <https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-global-report-finds-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

Wireshark | Pivot from Panorama

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: !!(erf.type.type == META)

No.	Time	Source	Destination	Protocol	Length	Info
1365	2020-03-11 00:45:25.2130537	10.9.130.154	10.9.130.12	SSL	1514	Continuation Data
1365	2020-03-11 00:45:25.2130549	10.9.17.7	10.9.17.158	TCP	78	56618 -> 443 [ACK] Seq=1 Ack=33936 Win=64668 Len=0 TSval=380779482 TSecr=38076...
1365	2020-03-11 00:45:25.2130550	10.9.17.198	10.9.17.6	TCP	1514	80 -> 51623 [PSH, ACK] Seq=61220 Ack=1 Win=7228 Len=1436 TSval=380779479 TSecr=...
1365	2020-03-11 00:45:25.2130562	10.9.34.170	10.9.34.6	TCP	1514	80 -> 32993 [PSH, ACK] Seq=53133 Ack=1 Win=7228 Len=1436 TSval=4195746565 TSecr=...
1365	2020-03-11 00:45:25.2130574	10.9.66.162	10.9.66.4	TCP	1514	80 -> 50884 [PSH, ACK] Seq=10053 Ack=1 Win=7228 Len=1436 TSval=3715746337 TSecr=...
1365	2020-03-11 00:45:25.2130587	10.9.131.167	10.9.131.13	TCP	1514	80 -> 60887 [PSH, ACK] Seq=22977 Ack=1 Win=7228 Len=1436 TSval=3235746081 TSecr=...
1365	2020-03-11 00:45:25.2130599	10.9.37.5	10.9.37.196	TCP	78	49772 -> 443 [ACK] Seq=1 Ack=87068 Win=64668 Len=0 TSval=4195746576 TSecr=4195...
1365	2020-03-11 00:45:25.2130600	10.9.37.7	10.9.37.200	TCP	78	[TCP Dup ACK 136383#5] 34509 -> 443 [ACK] Seq=1 Ack=31593 Win=64668 Len=0 TSva...
1365	2020-03-11 00:45:25.2130600	10.9.65.176	10.9.65.11	TCP	1514	80 -> 55786 [PSH, ACK] Seq=25320 Ack=1 Win=7228 Len=1436 TSval=3715746347 TSecr=...
1365	2020-03-11 00:45:25.2130613	10.9.18.12	10.9.18.204	TCP	78	46572 -> 80 [ACK] Seq=1 Ack=33936 Win=64668 Len=0 TSval=380779503 TSecr=380771...
1365	2020-03-11 00:45:25.2130613	10.9.37.13	10.9.37.159	TCP	78	57036 -> 8313 [ACK] Seq=1 Ack=4309 Win=64668 Len=0 TSval=4195746589 TSecr=4195...
1365	2020-03-11 00:45:25.2130614	10.9.131.167	10.9.131.13	TCP	1514	80 -> 60887 [PSH, ACK] Seq=24413 Ack=1 Win=7228 Len=1436 TSval=3235746091 TSecr=...

Frame 1: 609 bytes on wire (4872 bits), 609 bytes captured (4872 bits) on interface 1

Extensible Record Format

Ethernet II, Src: 02:00:01:04:00:05 (02:00:01:04:00:05), Dst: MS-NLB-PhysServer-26_c5:04:00:61 (02:1a:c5:04:00:61)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 400

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 14

Internet Protocol Version 4, Src: 10.9.68.6, Dst: 10.9.68.247

Transmission Control Protocol, Src Port: 58853, Dst Port: 445, Seq: 1, Ack: 1, Len: 531

NetBIOS Session Service

SMB2 (Server Message Block Protocol version 2)

```
0000 02 1a c5 04 00 61 02 00 01 04 00 05 81 00 01 90 .....E:G4F@
0010 81 00 00 0e 08 00 45 00 02 47 34 46 40 00 20 06 .....D.....
0020 87 5c 0a 09 44 06 0a 09 44 77 e5 e5 01 bd 22 ea .....X.....h
0030 9b ac 3c 22 7b 58 80 18 21 d8 bc 68 00 00 01 01 .....V.....S
0040 08 0a dd 5f c8 e1 dd 56 81 e0 00 00 02 0f fe 53 .....M.....
0050 4d 42 40 00 00 00 00 00 00 00 01 00 01 00 00 00 .....A.....
0060 00 00 00 00 00 00 02 00 00 00 00 00 00 41 ca .....a.....
0070 00 00 00 00 00 00 61 00 00 00 00 04 00 00 00 00 .....a.....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 .....X.....
0090 00 81 01 00 00 00 00 00 00 00 58 00 b7 91 00 00 .....X.....
00a0 00 00 00 00 00 00 a1 82 01 b3 30 82 01 af a0 03 .....0.....
00b0 0a 01 01 a2 82 01 92 04 82 01 8e 4e 54 4c 4d 53 .....NTLMS
00c0 53 50 00 03 00 00 00 18 00 18 00 86 00 00 e0 .....SP.....
00d0 00 e0 00 9e 00 00 10 00 10 00 58 00 00 00 0e .....X.....
00e0 00 0e 00 68 00 00 10 00 10 00 76 00 00 00 10 .....h.....
```

wiresharkUntitled_64a683ae-ddb9-4a13-b16d-06f2ba9be1b3.pcap_20200430210728_DHWfDw.pcap Packets: 136558 · Displayed: 136558 (100.0%) Profile: Default



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

Secure production continuity.

Something you sell:

- Hearing aids
- Radars
- Smart meters
- Software

How to harden your products.
Actionable recommendations.

20+ CVE
found during
these tests.

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.

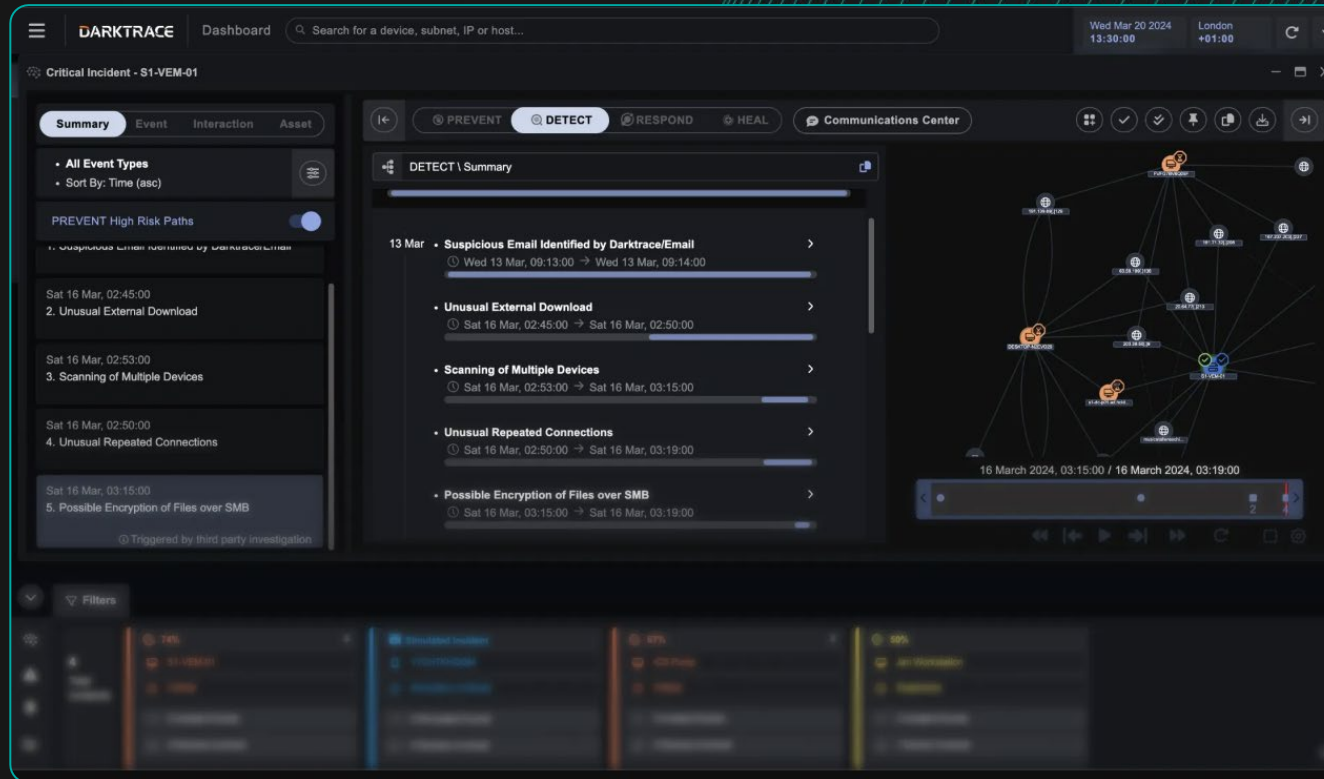
Cross-Technology insights between
your IT and OT infrastructure.

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

