



The impact from implementing Cybersecurity on Human Resources and Company Assets

Making sense of the cybersecurity jungle

Let's get to know each other

Speaker

Audience

- Vertical
- Roles
- Strategy

Today's agenda

Attacks

Regulations & Security Standards

Defence strategy

Compliance

Where to start?

Myths

Attacks on OT-infrastructure

Ransomware (encryption of files)

Phishing (Installation of Malware)

Social engineering (physical access & installation of Malware)

Regulations and Standards

nist

iec62443

iec27001

nis2

nerc cip

NIS2

Revision of European NIS Directive from 2016

Framework for protection of network & information systems

Focus on critical infrastructure, operators & service providers

Enhanced reporting requirements

Stronger security requirements (Authentication & Encryption)

Scope:

Energy Transport, Banking and finance, Health, Water, Digital infrastructure, Digital services

Defence and compliance

1. Realise you run many legacy systems that are hard to protect or to change
2. Know what you are defending (Inventory Management)
3. Monitor what you want to defend (don't automatically act IPS in OT-applications)
 - a. Behaviour Analytics
 - b. Custom signatures
4. Respond to attacks (via MSSP or own team(s))
5. Report attacks (timely) to authorities
6. Report attacks to customers

Dealing with legacy systems

Legacy systems (Lifespan 20-30 years)

Vendor support

(nearly) impossible to make changes, focus on future, while using a sensor (IDS)

Looking at the future, what you need, start replacing systems step-by-step over product life cycle.

Where to (re)start?

Do I need a system?

What type of system? NDR/XDR/SIEM/IDS/IPS?

Do I need Threat Intelligence?

- What leads to an actually actionable event
- False positives

Common myths

- Human is the weakest link
- Implementing cybersecurity is expensive
- We can't have enough threat Intelligence
- OT security specialists are impossible to find



Demo Bohemia Market follow-up

GREYCORTEX MENDEL
Dashboard Inventory Network OT Metrics Events Incidents
DEMO User

Date Time range

March 2023

S	M	T	W	T	F	S
26	27	28	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1

Attributes

Predefined filters:

Event visibility level:

Detection methods:

Subnet:

Host:

Service:

Traffic:

Event:

Severity:

Filter

Clear Filter Manager

Events by Severity Hosts by Risk

Filter Clear ?

Chart Map
Traffic

Y axis to linear

Events Export data Preferences

Event	Src Hosts	Dst Hosts	Events	Date
10 Exploitation: PLC CPU Crash attempt	2	1	3	Feb 21 15:08 – Feb 22 15:28

Signature: 1000005001 (information, created: 2023-02-20 17:58:01)

Signature ID: 1000005001

Created: 2023-02-20 17:58:01 (Modified: 2023-02-21 15:04:16)

Revision: 1

Severity: 10

Matched rule: alert top any any -> any any

Properties:

Top Src Hosts

- 172.28.252.98
- rherban-ntb (172.29.10.119)

Top Dst Hosts

- 172.29.20.30

Top Src Subnets

- Private B (172.16.0.0/12)
- Office Network (172.29.10.0/24)

Top Dst Subnets

- ICS Network (172.29.20.0/24)

Top Services

- HTTP (80)

To filter Action Report an incident Show more details

4 Scan: Internal Scan-like Behavior	4	4	25	Feb-17 11:36 – Feb-23 16:34
7 Exploit: ETERNALBLUE Exploit MS17-010 Win8+	1	1	190	Feb-15 10:03 – Mar-02 08:21
7 Discovery: New Host by MAC Address (forbidden by policies)		35	36	Feb-15 10:09 – Feb-21 15:45