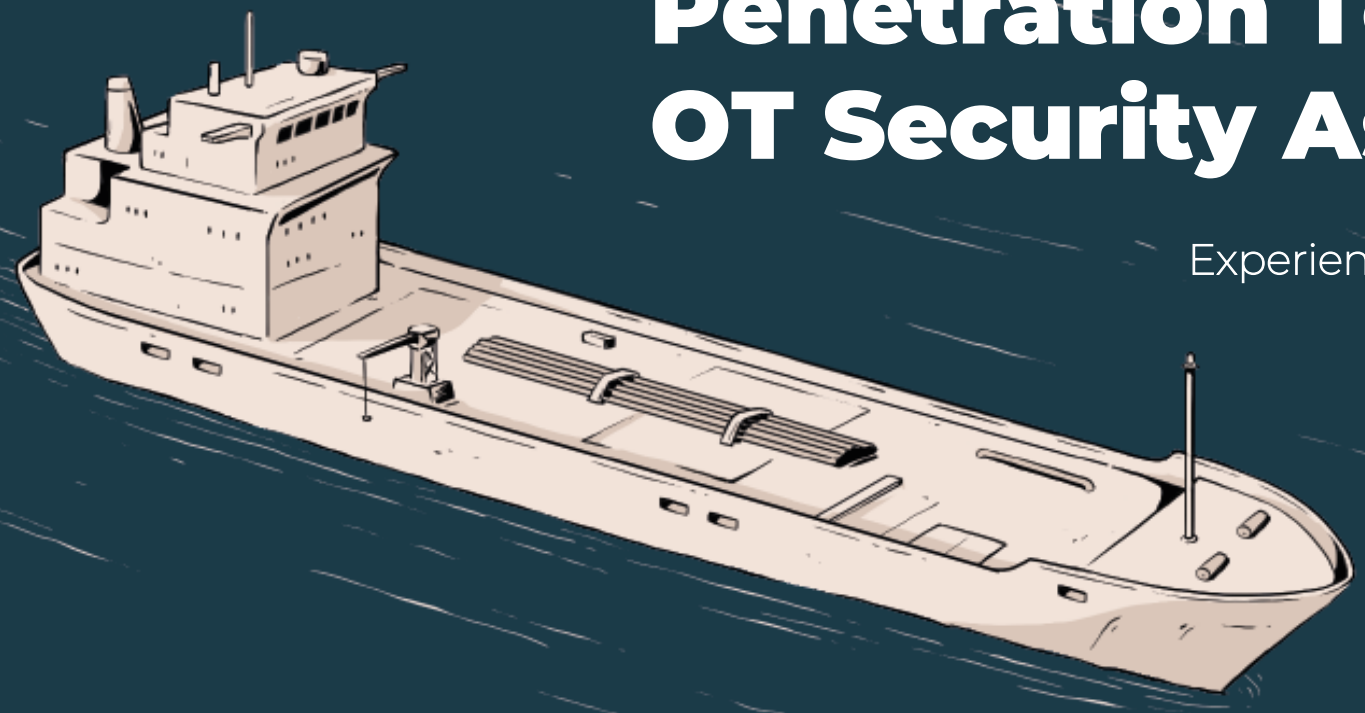
TLP:CLEAR

NORMA CYBER

Penetration Test and OT Security Assessment

Experience Sharing - NORMA Cyber



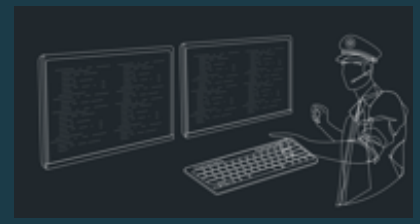
TLP:CLEAR

Nordic Maritime Cyber Resilience Centre

190+ Member organisations

Represented with 3000+ Vessels

16 Employees



Offices and Operations Room in Oslo, Norway

Threat Intelligence

Incident and Crisis Response

External Monitoring

Network

Managed Security Operations Centre

Penetration Testing

NORMACYBER



$whoami

John Velo, 27 years old

Lead Penetration Tester at NORMA Cyber

Cyber Security Analyst

Bachelors in Entrepreneurship and Cybersecurity

Currently taking Masters in NTNU Gjøvik

CTF player, FPS games, Some running

OSCP+ (Offensive Security Certified Penetration Tester)

GIAC - GPEN (Enterprise Pentest, SANS SEC560)

Other Pentest Certifications Includes:

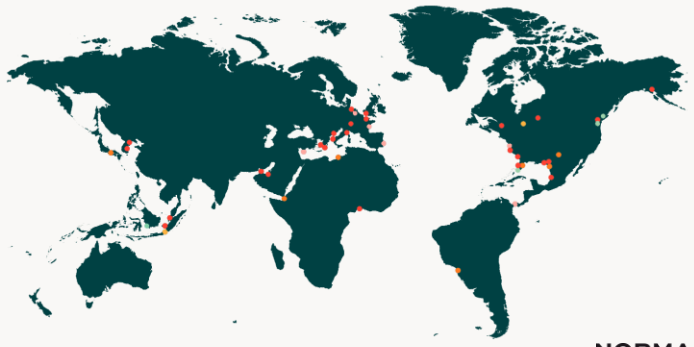
eCPPT, eWPT, eJPT, and **PT1**





Experiences

- Passenger vessels
- Car ferries
- Offshore Construction Vessels
- Offshore energy vessels
- Cloud & IT-Infrastructure
- WebApp



NORMACYBER

Scope and method

The 4-method-approach

IT and Configurations

- Directory forests
- Certificate services
- Mail and webmail
- Single sign-on and MFA
- Virtualization and storage
- Firewalls and gateways

Vessel and site systems

- Card payment
- Cabin access control
- CCTV and video
- Telephony
- Crew and guest wireless
- Out-of-band management

Applications and exposure

- Web applications
- APIs and middleware
- Master-data services
- External attack surface
- Transport security
- Detection platforms

Operational technology

- Integrated automation
- Check for outdated documents
- Interview with crew
- Bridge, navigation, ECDIS
- HMI and SCADA front-ends
- Gas, fire and safety systems
- Power and energy management

Tested from four positions

1. **External**
   No access. Internet only.
2. **Guest**
   On the network. No login.
3. **Assumed breach**
   One normal user account.
4. **Post-exploitation**
   After admin. How far it spreads.

TLP:CLEAR

The numbers

Findings with a severity rating

136
Rated findings

26
Critical

49
High

61
Medium and Low

5
ways to full admin, one site

Domain, forest and infrastructure.

<30
minutes to full domain control

One setting. No exploit. No patch.

100+
partners behind one hub

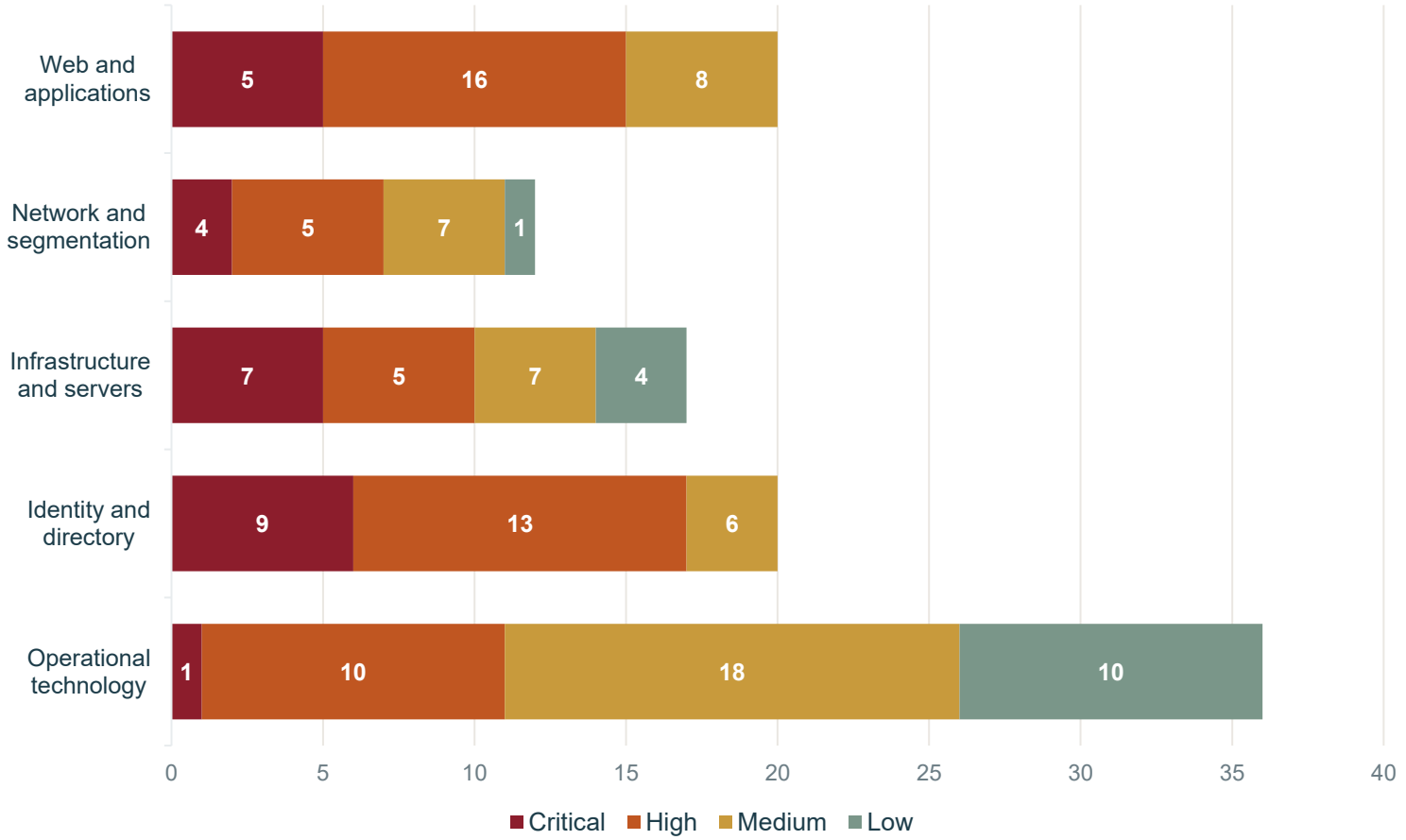
Taken over from a normal user account.

0
attacks that reached OT

Tested from a hacked PC. Being reachable is a separate issue.

Counts cover findings given a severity rating.

Where the findings sit



Read it this way

- **Identity is worst.** Fewest systems, most Criticals. It unlocks everything else.
- **Apps are close behind.** Missing permission checks, not firewall gaps.
- **Infrastructure surprises.** Storage, servers and admin interfaces. Rarely tested.
- **OT is volume, not severity.** A different shape. See the OT section.

Typical Vulnerabilities

01

Identity is the fastest way in

Templates, built-in admins, vendor accounts. They beat any firewall.

02

Credentials that never expire

Passwords well over a decade old. Shared templates. Defaults published online.

03

Data exposed, and alterable

Door locks, payments, personal data. One could be changed from the internet.

04

Known flaws left exposed

Public exploits exist. Even on the kit meant to defend you.

05

Legacy never retired

Systems years past support. Still running in production.

06

Detection gaps, not tool gaps

The tools worked. Logging, outbound blocking and watching did not.

07

OT risk arrives by hand (physically)

Not over the network. USB sticks, service laptops, vendor access.

08

Exposure nobody intended

Admin pages and control screens, put online by accident.

TLP:CLEAR

Identity is the fastest way in

1
Ordinary user
What a new joiner or contractor has.

2
Misconfigured template
Any user could get a certificate as anyone else.

3
Forest administrator
Full identity control in under 30 minutes.

4
Everything downstream
Harvest passwords, then take servers and storage.

Five paths to Admin

- **Domain Admin.** A certificate template. Three commands.
- **Full forest.** A renamed built-in administrator account.
- **Full forest.** A service account password over a decade old. One cracked hash.
- **Privileged groups.** A shared helpdesk password template.
- **Infrastructure.** Cleartext credentials from domain controllers.

Why this matters

These are settings and privileges, not patches.

Fixed by changing settings and removing rights. No purchase needed.

Fixing one certificate template would close over half the Criticals there.

Vendor accounts with too many rights were another recurring path.

Credentials that never expire

15+ years

since the oldest service account password changed

50+ accounts

sharing one predictable password template

All accounts

cracked in a single guessing run – worked with their email addresses as well

5 servers

sharing one local administrator password

In practice

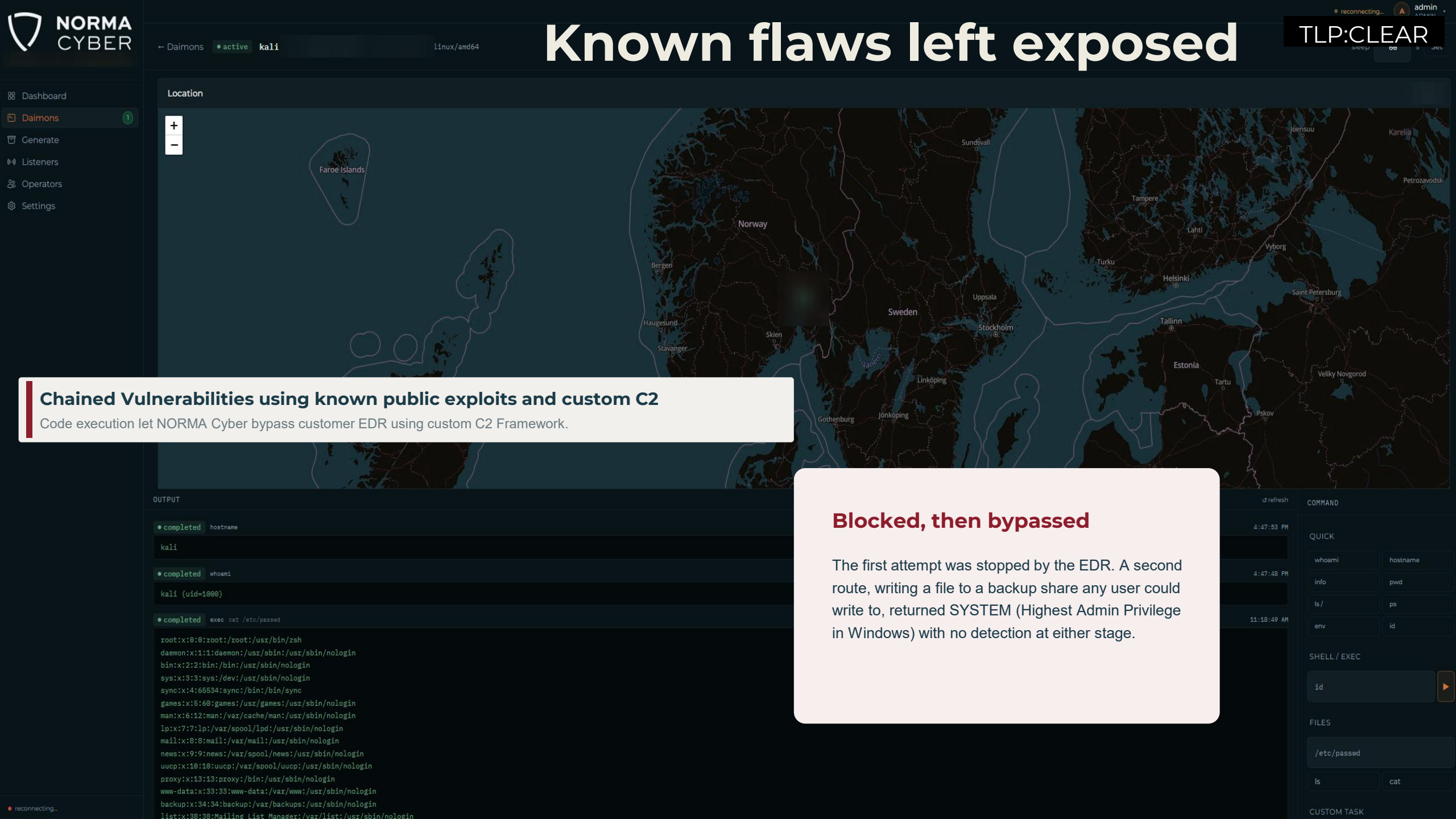
- **Service accounts as permanent keys.** Often a decade or more unchanged. Some are admin everywhere.
- **Vendor defaults, published online.** Admin pages anyone can look up in a manual.
- **No lockout policy.** Every crew account on one ship fell in one run. Alerts fired. Nobody acted.

Typical Passwords = Easy Access

Norma1	Norma2022	NormaCyber1
Norma12	Norma2023	NormaCyber123
Norma123	Norma2024	NormaCyber2024
Norma1234	Norma2025	NormaCyber2025
Norma12345	Norma2026	NormaCyber2026
Norma123456	Norma2027	NormaCyber2026!
Norma123!	Norma2024!	Normacyber2026
Norma123!!	Norma2025!	NORMACYBER2026

Known flaws left exposed

TLP:CLEAR



Chained Vulnerabilities using known public exploits and custom C2

Code execution let NORMA Cyber bypass customer EDR using custom C2 Framework.

Blocked, then bypassed

The first attempt was stopped by the EDR. A second route, writing a file to a backup share any user could write to, returned SYSTEM (Highest Admin Privilege in Windows) with no detection at either stage.

TLP:CLEAR

Detection gaps, not tool gaps

The products worked. The setup around them did not.

✓ What fired

- Endpoint protection blocked the standard payload first time.
- Memory password theft blocked every time on one ship.
- A perimeter firewall was patched against the year's big flaw.
- A remote access portal enforced five separate checks.
- Message signing on domain controllers stopped relay attacks.
- Tamper protection held. The agent could not be stopped or removed.

! What passed in silence

- A full copy of the password database taken from a domain controller. No alert.
- Certificate abuse, the step that gave admin. No security event at all.
- A password sweep across dozens of hosts in minutes. No signal.
- Traffic out to attacker servers from several internal hosts, including domain controllers.
- Alerts did fire. Nobody acted on them.
- A blocked payload got in by a second route and returned SYSTEM, unseen.
- An audit log the attacker could read and delete.

Every item on the right is fixed by a setting, a rule, outbound blocking, or someone watching. Not by buying anything.

IT and OT are not the same problem

Same attacker. Different rules. We test both.

	IT	OT
What is at stake	Data, money and reputation.	Safety and staying in operation.
What we found	96 findings. 25 Critical.	40 findings. 1 Critical.
How we test it	We attack it. Assumed breach.	We inspect and interview. Attacking live systems is unsafe.
Fastest way in	Identity. Templates and admin accounts.	Physical. USB sticks, service laptops, vendor visits.
Patching	Weeks. You control it.	Years. The vendor controls it.
A Medium finding	Moderate business impact.	Could be steering or propulsion.
Biggest single gap	Missing permission checks.	Segmentation that has drifted.

One boundary between them. It is the control that stops a cyber incident becoming a safety incident.

The OT Assessment

How OT risk arrives

1. **A technician boards with a laptop**
   It has been on other ships, other networks, and the internet.
2. **It connects straight to automation**
   Often below the firewall everything depends on.
3. **Files arrive on removable media**
   No scanning step. No approval record.
4. **Nobody logs the visit**
   No record of what connected or changed. Nothing to investigate.

What the assessments asked for

1. **A portable media policy that exists in practice**
   Issued, scanned, controlled USB. Approval before anything connects.
2. **One standard for vendor remote access**
   Started onboard. Jump host. Time-limited. Logged. Off by default.
3. **An OT security management system**
   Named owners, change control, asset list, incident plan.
4. **Maintain the segmentation deliberately**
   Your strongest control. Check it after every vendor visit.

What is working

Controls that held. Do not fix what is working.

✓

IT and OT separation

Where we tested it directly, the firewall kept office networks fully separate from navigation and safety, even from a fully hacked PC.

✓

Endpoint protection

Blocked memory password theft every time. Blocked standard payloads. Could not be removed.

✓

External perimeter

No internet-exposed service had a public exploit. Gateway attacks failed.

✓

Network design on newer vessels

Strong segmentation, encrypted wireless, no open networks, few risky services exposed.

✓

Directory hardening where applied

Message signing stopped relay attacks. On one ship there was no route to Domain Admin at all.

✓

Layered remote access

Done properly: source limits, device certificate, password, single sign-on, second factor.

TLP:CLEAR



NORMA CYBER

Questions

John Velo - NORMA Cyber

Connect with me @ LinkedIn