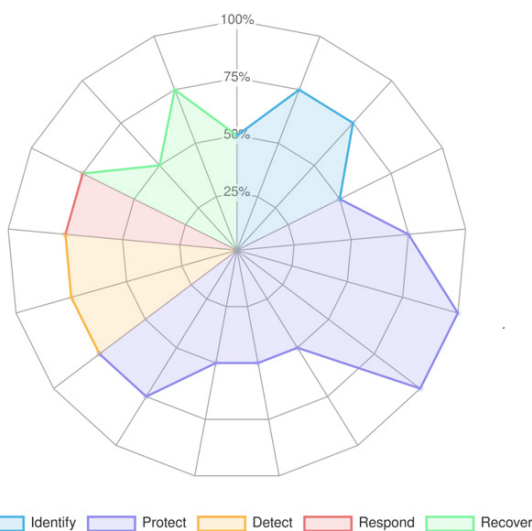




SERVICE OVERVIEW

OT CYBERSECURITY ASSESSMENT

Is your OT environment as secure as you think?



[A visual snapshot of a typical OT Cybersecurity Maturity diagram across the 5 key areas - highlighting your strengths and priority improvement areas.]



“How ready are you for NIS2?”
“Where are our biggest risks?”
“Which improvements should we prioritise first?”

If questions like these are on your mind and you're tired of long, drawn-out consulting engagements, then this service is for you.

The HMS OT Cybersecurity Assessment gives you a clear, visual overview of your OT security maturity, paired with tailored, actionable recommendations that help you focus on what matters most.

WHAT YOU WILL GAIN

- **Clarity** on your OT cybersecurity maturity across 5 key areas
- **Prioritised next steps** you can act on immediately
- **Alignment** across OT/IT and leadership to support decisions
- **Momentum** towards a structured, repeatable improvement plan

SPECIFICALLY DESIGNED FOR

MANUFACTURERS & INDUSTRIAL

Single-site factories or multi-plant operations that need clarity on OT risk exposure.

CRITICAL INFRASTRUCTURE OPERATORS

Always-on operators needing consistent OT security across distributed sites.

IT & OT TEAMS

In-house teams that need a clear starting point without deep OT specialisation required.

KEY BENEFITS

01 ALIGNED WITH INDUSTRY STANDARDS

Mapped to leading cybersecurity frameworks in OT including NIST and ISA/IEC 62443

02 INSTANT OT SECURITY SCORE

Receive a clear maturity score across 5 domains and 17 subcategories immediately upon completion.

03 ACTIONABLE RECOMMENDATIONS

Each subcategory produces targeted improvement points - not just findings, but a concrete action plan.

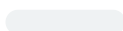



04 FAST-TRACK TO DEFEND UPTIME

Forget lengthy consulting cycles. One concise, expert-led conversation gives you fast, practical outcomes.

ASSESSMENT PROCESS

- 1 SET SCOPE**
Choose a site on where you need the assessment to focus. Get IT and OT responsible together for the interview. Questions map directly to maturity levels 1-4.
- 2 INTERVIEW**
Guided by HMS Networks OT Cybersecurity Specialist, you and your team completes the structured OT cybersecurity questionnaire in approx. 2 hours.
- 3 EXPERT ANALYSIS**
Responses are analysed by HMS Networks OT Cybersecurity specialists and translated into a cybersecurity maturity score per domain.
- 4 ASSESSMENT REPORT**
You receive a detailed report: identified risks, maturity scores, and a prioritised improvement roadmap.

4 MATURITY LEVELS

-  **Level 1** - Initial / Ad Hoc
-  **Level 2** - Defined
-  **Level 3** - Managed
-  **Level 4** - Optimising



Implement the prioritised recommendations and run follow-up assessments to track your maturity progression over time - across one site or many.

IDENTIFY YOUR WEAKPOINTS

Results are presented across the 5 NIST domains mapped to IEC: Identify, Protect, Detect, Respond & Recover - covering all 17 OT-specific subcategories below.

- Asset Management
- Identity & Access Mgmt
- Network Management
- Patch Management
- Vulnerability Management
- Incident Management
- Roles & Responsibilities
- +10 more subcategories

IEC 62443-3-3 ALIGNED

Every domain maps directly to IEC 62443-3-3 Security Requirements (SR 1-7), ensuring your assessment results translate directly into compliance evidence.

WHY HMS + OT CYBERSECURITY ASSESSMENT

HMS Networks is a global leader in industrial communication and ICT solutions, enabling industries to securely connect and manage their equipment and data. With extensive OT cybersecurity expertise and thousands of installations worldwide, HMS helps customers in manufacturing, energy, and infrastructure protect their operations. Our automated OT Cybersecurity Assessment platform delivers actionable insights and transparent costs, while our scalable solutions and trusted expertise support businesses of any size.



✉ otc-marketing@hms.se

🌐 hms-networks.com