HMS

24-03-2026

Automation Company A

INTRODUCTION

Welcome to the HMS OT Cybersecurity Assessment report for Automation Company A. This comprehensive report provides a detailed analysis of the cybersecurity maturity level within your organization's operational technology (OT) environment. By completing the assessment questionnaire, you have enabled us to evaluate the current state of your OT cybersecurity practices and provide tailored recommendations for improvement.

Start date	20-03-2026
End date	24-03-2026
Contributor(s)	Thomas
Partner	HMS

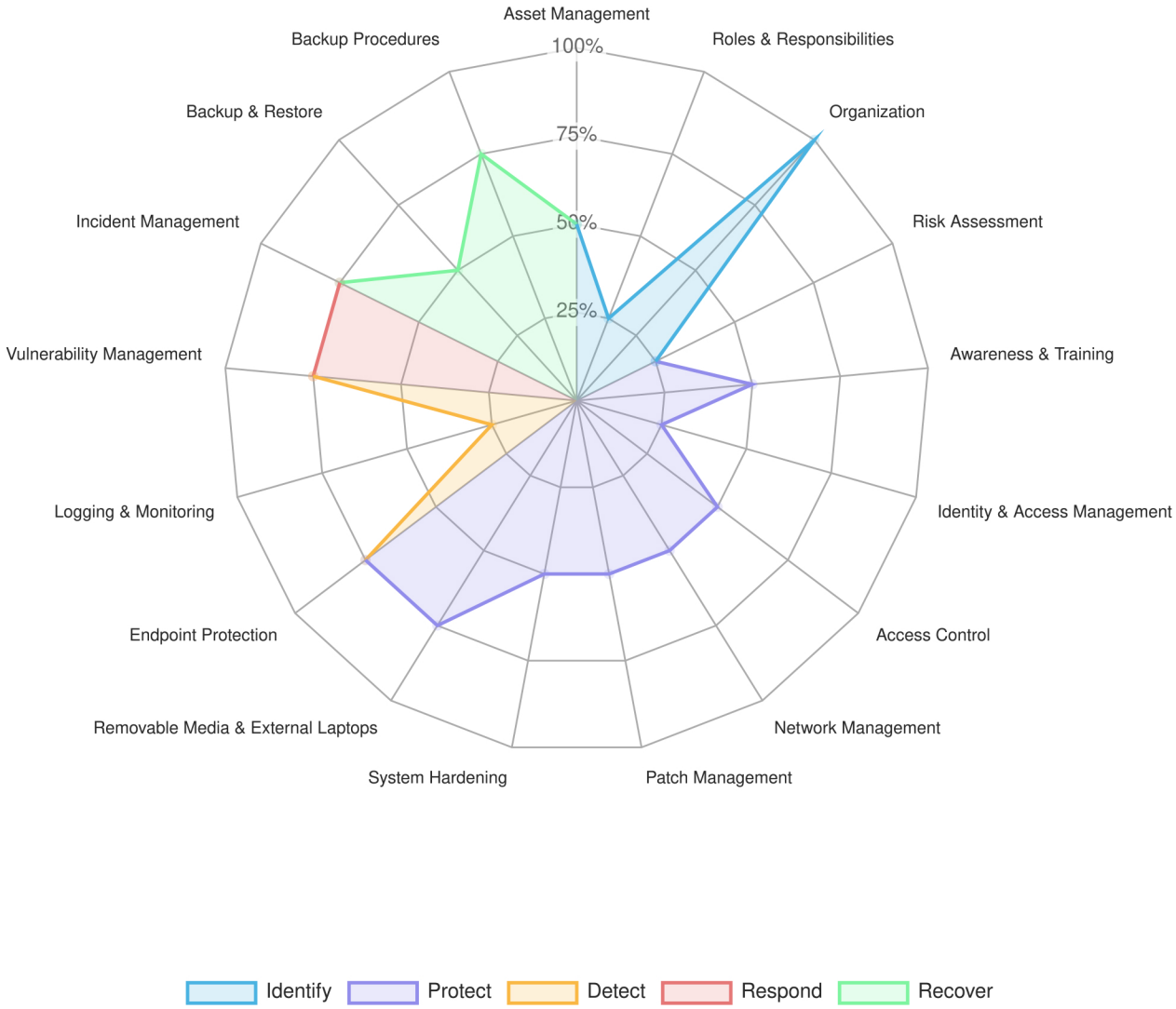
The insights gathered from this assessment serve as a foundation for developing a robust cybersecurity strategy to enhance your organization's resilience against cyber threats. This report enables your organization to identify strengths as well as areas for improvement in managing OT cybersecurity risks. In addition to this report, you will find a graphical representation of the assessment results, offering a clear visual overview of your OT cybersecurity maturity across the different NIST categories. For each category, detailed and tailored recommendations are provided to support structured and effective security improvements within your operational environment.

By implementing the recommended actions, Automation Company A can strengthen its defenses, mitigate potential threats, and foster a culture of cybersecurity resilience. Together, we safeguard your critical operations against evolving cyber threats.

We appreciate your commitment to securing your operational environment and thank you for your participation in this important evaluation.

sales@ot-secure.nl
www.ot-secure.nl

MATURITY OVERVIEW



sales@ot-secure.nl
www.ot-secure.nl

MATURITY OVERVIEW LEGEND

In this assessment, the cybersecurity maturity of your organization's OT environment has been evaluated across four maturity levels:

- Maturity Level 1
- Maturity Level 2
- Maturity Level 3
- Maturity Level 4

For each maturity level, specific recommendations have been provided to help your organization progress towards higher maturity levels and enhance its cybersecurity posture.

Identification:

- Asset Management: Evaluates the extent to which your organization identifies and manages its assets, including OT systems and infrastructure.
- Roles & Responsibilities: Assesses the clarity and effectiveness of roles and responsibilities within your OT cybersecurity team, with strong support from senior leadership.
- Organization: Examines the standardization of cybersecurity measures across both existing and new systems within your organization.
- Risk Assessment: Evaluates the thoroughness and effectiveness of risk assessment processes in identifying and mitigating cybersecurity risks.

Protection:

- Awareness & Training: Evaluates the level of cybersecurity awareness and training programs within your organization, tailored to different roles and responsibilities.
- Identity & Access Management: Assesses the effectiveness of identity and access management practices in controlling access to OT systems.
- Access Control: Evaluates the security of access to OT systems within your organization, including automated verification of access privileges.
- Network Management: Assesses the management and security of your organization's network infrastructure to prevent unauthorized access.
- Patch Management: Evaluates the effectiveness of patch management processes in addressing vulnerabilities within OT systems.
- System Hardening: Assesses the level of system hardening practices implemented to minimize attack vectors and vulnerabilities.
- Removable Media & External Laptops: Evaluates measures to secure against threats from external devices such as USB sticks and external laptops.
- Endpoint Protection: Assesses the security measures implemented to protect endpoints within your OT systems.

Detection:

- Logging & Monitoring: Evaluates the effectiveness of logging and monitoring practices for detecting and responding to cybersecurity incidents.
- Vulnerability Management: Assesses the effectiveness of vulnerability management processes in identifying and addressing security vulnerabilities.

Response:

- Incident Management: Evaluates the preparedness and effectiveness of incident management processes in responding to cybersecurity incidents.

Recovery:

- Backup & Restore: Assesses the resilience of backup and restore processes for recovering OT systems after a cybersecurity incident, including backup procedures.

sales@ot-secure.nl
www.ot-secure.nl

RESULTS AND RECOMMENDED ACTIONS

IDENTIFY

MATURITY LEVEL 1

Asset Management
Advice: The recommendation for achieving the next maturity level, would be to expand the Asset Management document by including security zones within which assets with similar security requirements are grouped. This will provide a more detailed insight into the security aspects of the assets and enable the development and implementation of a more targeted security policy.

Roles & Responsibilities
Advice: Consider expanding your OT Cybersecurity team to effectively address various aspects of cybersecurity. A single employee cannot bear all responsibilities.

Organization
Advice: Ensure that new systems are designed from the outset with the highest standards of cybersecurity in mind. This requires integrating security measures into both the design and development phases, followed by continuous monitoring and maintenance to ensure the effectiveness of these measures.

Risk Assessment
Advice: It is essential to conduct a thorough risk assessment to understand the risks in the field of OT Cybersecurity for your organization. Start by identifying and evaluating potential risks to achieve a basic level of control.

RESULTS AND RECOMMENDED ACTIONS

PROTECT

MATURITY LEVEL 1

Awareness & Training
Advice: To take the next step, it is crucial to enhance Cybersecurity Training with interactive elements such as scenario-based training and simulations of real cyberattacks. Additionally, the Awareness program should be continuously updated with the latest threats and best practices to keep staff alert.

Identity & Access Management
Advice: It is essential to implement an identity and access management program to ensure the security of your OT systems. Start by establishing clear procedures for registering, managing, and revoking user accounts and their access rights to systems and data. This can be achieved, for example, by implementing a centralized identity management system that automates user identity, authentication, and authorization management.

Access Control
Advice: To enhance your access control process, consider implementing a more centralized approach to managing user identities and rights. This could involve implementing an IAM system that provides a uniform and automated method for assigning and managing access rights across all IACS systems.

Network Management
Advice: To improve your network management, consider expanding your inventory with more detailed information about network configurations and topologies. This can help identify potential single points of failure and optimize network performance and security. Also, consider implementing network management tools for continuous monitoring and analysis of network activities.

Patch Management
Advice: To improve your patch management process, it is recommended to transition to a more proactive approach. Implement a patch management plan that includes regular vulnerability assessments and applies patches on a predefined schedule, taking into account the criticality of the patches and their impact on operations. Aim to reduce the time between patch release and implementation to minimize exposure to potential threats.

System Hardening
Advice: While it is positive that firewalls and antivirus software are utilized, it is important to further enhance system hardening measures. This involves implementing specific configurations and guidelines to secure servers and endpoints against known attack methods and vulnerabilities.

Removable Media & External Laptops
Advice: To further strengthen your security against external assets, it is important to take proactive measures to scan and check such devices for malware and other threats before they are used on systems within your network. Implement automated scanning tools and conduct regular manual checks to ensure that all external assets are secure before accessing sensitive systems or data.

Endpoint Protection
Advice: To elevate your endpoint protection, consider implementing advanced technologies such as machine learning and behavioral analysis for detecting zero-day attacks and advanced malware. Additionally, consider integrating endpoint protection with your network security systems for a coordinated and integrated approach to cyber threats.

sales@ot-secure.nl
www.ot-secure.nl

RESULTS AND RECOMMENDED ACTIONS

DETECT

MATURITY LEVEL 1

[illegible]

RESPOND

MATURITY LEVEL 3

[illegible]

RECOVER

MATURITY LEVEL 2

[illegible]