

Bedrijfsdetails

Baltimore Aircoil Company, BAC, is a global manufacturer of **heat transfer products and services**. We specialize in developing resource-saving evaporative cooling equipment that conserves water and energy. The products of BAC Europe are distributed across Europe, the Middle – East and North Africa

Functie

To strengthen our EMEA HQ in Belgium, we're recruiting an Global Senior Manager – Cybersecurity

This role leads the BAC's day-to-day security program inclusive of protecting corporate IT, the products the company builds, and the AI capabilities now being introduced across the business. This role covers the full traditional security mandate (operations, architecture, identity, vulnerability management, incident response, compliance) plus product security for the company's engineered products, and AI security for the growing footprint of AI and self-service data tools. BAC operates globally, including in complex regions such as China, and this role is expected to bring a seasoned perspective about running a security program in those environments.

This is a hands-on leadership role reporting into the Infrastructure, Operations and Security organization, balancing strategic program ownership with execution, partnering with peers across the team to plan and implement actions to progress the company's cybersecurity posture and compliance. This role is expected to collaborate directly with the Amsted group Security Operations Center (SOC) and other Amsted entity security leaders to define and execute the multi-year security roadmap.

Principal Accountabilities

Core Cybersecurity:

- **Security Operations:** in collaboration with the Amsted SOC, owns BAC's security monitoring, detection, and response across the enterprise and the tools that support it (SIEM, EDR, XDR).
- **Incident Response:** owns creation and execution of the incident response program (i.e., plans, playbooks, tabletop exercises, and live response); leads incident response readiness, security incident investigations, crisis coordination, and executive communications in partnership with legal, compliance, and business stakeholders.
- **Vulnerability & Threat Management:** in collaboration with the Amsted SOC, runs the enterprise vulnerability management program, including scanning, patch prioritization, penetration testing, and red/purple team exercises, with clear metrics on time-to-remediate.
- **Identity & Access Security:** in collaboration with the Amsted SOC and Amsted security council, design and implement a comprehensive security program spanning identity and access management (IAM), endpoint protection, data loss prevention (DLP), and threat intelligence. Application-level governance, including SAP roles, profiles, and segregation of duties, is owned by the Digital Applications & Product Delivery team.
- **Security Architecture:** partner with Enterprise Architecture and Infrastructure to embed security requirements into network, cloud, and application architecture decisions.
- **Governance, Risk, and Compliance:** owns the security policy framework and leads the enterprise through relevant audits and certifications (e.g., SOC 2, ISO 27001, NIST CSF) and supports customer and regulatory security questionnaires.
- **Security Awareness:** runs the company's security awareness and phishing simulation program, including establishment and publishing of metrics.
- **Third-Party & Vendor Risk:** in collaboration with the Amsted SOC, owns the vendor security risk assessment process for new and existing suppliers, systems integrators, and SaaS platforms.

Product Security:

- **Secure Development Lifecycle:** build and run a secure SDLC program for internally developed applications and configuration/product engineering tools, including threat modeling, secure code review, and security testing gated into the release process.
- **Product & Connected Systems Security:** own the security requirements for the company's engineered products and any connected/embedded components, including coordination with engineering on secure-by-design practices for products that ship with software or connectivity.
- **Application Security Testing:** run static and dynamic application security testing (SAST/DAST) and manage remediation of findings across custom-developed applications and the broader integration landscape.

AI Security:

- **AI Security Risk:** in collaboration with the Amsted SOC, own the security review process for AI tools and use cases, including Microsoft 365 Copilot and any custom or third-party AI/LLM deployments, covering risks such as data leakage, prompt injection, model access controls, and unsafe output.
- **AI Governance Partnership:** partner directly with the Director, AI, Data, and Emerging Tech Advancement to ensure AI governance policy is followed and enabled by security controls.
- **Emerging Risk Monitoring:** track the evolving AI threat landscape (adversarial AI, model theft, data poisoning) and translate it into practical controls embedded into the organizational way of working.

Global Considerations:

- **Global Security Strategy:** design and execute cybersecurity strategy across the company's global footprint, adapting controls and program design to local regulatory requirements.
- **Global Region Regulations Experience:** ensure cybersecurity strategy incorporates operation in highly regulated regions such as China, including practical handling of data localization, cross-border transfer restrictions, and state-level regulatory frameworks (e.g., China's Cybersecurity Law, PIPL, and Data Security Law).
- **Global Complexity and Risk Awareness:** advise IT and business leadership on the security and data risk implications of operating in, or expanding into, higher-risk regions.

Profiel

Knowledge & Skills

- Experience: 8+ years in cybersecurity, with 3+ years in a leadership or senior management role owning a security program end to end.
- CISSP certification required; additional certifications such as CISM, OSCP, GIAC (GCIH/GPEN/GWAPT), or CCSP are a strong plus.
- Direct experience running core security operations, including SOC oversight, incident response, vulnerability management, in a corporate IT environment of comparable scale.
- Hands-on secure SDLC / application security experience: demonstrated experience embedding security into software development and deployment.
- Working knowledge of AI security risk (LLM/AI-specific threats) and application of proportionate controls to a self-service AI program that is still maturing.
- Direct, hands-on experience building or executing a cybersecurity program in a complex multinational environment, China specifically preferred, including familiarity with local regulatory frameworks and cross-border data requirements.
- Manufacturing, industrial, or engineer-to-order environment experience, including OT/connected product security exposure, is a strong plus.
- Experience operating within an SAP or major ERP landscape is a plus, given the tight coupling between security and the company's core systems.
- A direct, clear communication style, ability to objectively explain cyber risk and trade-offs to executives, leading with facts and presenting recommendations with clear outcomes and risks.

Aanbod

What we offer you?

- An exciting job within an international environment at a market leading company.
- You'll work in an enthusiastic company and global team where we stimulate training and personal development.
- An international company with a strong focus on sustainability.
- A competitive salary added with fringe benefits.

Locatie:

België, Heist-Op-den-Berg

BALTIMORE AIRCOIL

Industriepark Zone A
2220 Heist-op-den-Berg
België

Tel:

+32 15 25 77 00

Url:

<https://www.baltimoreaircoil.eu/>

Interesse?

Voor meer informatie:

Bel **ELISA GOOSSENS**

op het nummer: **+3215237674**