Job Title	Security Specialist

Organisation	**Challenge Airlines BE**
Reports to	CISO
Location	Liège, Belgium
Position Code	CHG114
Job Purpose	The Security Specialist is responsible for executing and improving technical security controls across the organization's infrastructure and cloud environments. This role includes advanced analysis of security incidents, conducting technical audits and vulnerability assessments, advising on secure architecture design, and supporting regulatory compliance initiatives. The position requires strong technical expertise, analytical capabilities, and the ability to operate effectively in a fast-paced, regulated environment.
Responsibilities	• Manage corporate-wide Information security projects. • Manage corporate-wide information security controls. • Perform and advanced level analysis on escalated security events, notifications, and alerts from various systems/sources including forensics. • Implement new and existing technologies and/or solutions for the organization and its platforms. Communicate and collaborate with business and IT staff. • Improve the information security operations processes and procedures, including incident response playbooks and workflows using automation tooling. • Work with other Departments and Business functions to resolve security events, incidents, and service requests. • Availability to provide reactive support to critical security incidents outside standard business hours. Provide feedback and recommendations on existing and new security tools/technology and techniques for improvement. • Work effectively as a member of a team, contribute to sharing information about new technologies, identified problems, and discovered solutions. • Advice on secure system architecture and design • Execute technical audits, vulnerability assessments, and configuration reviews • Support regulatory compliance initiatives related to information security • Other duties as assigned.
Job Requirements	
Education	• Strong technical understanding of IT, to be able to validate that an environment meets all security and compliance controls • Security and/or Technical Certification – Advantage

Experience, Skills, and Personal Attributes	• Minimum of 2-3 years of work experience in Information Security **Technical Competence** • Well versed in networking devices, firewalls, intrusion detection and prevention systems • Excellent technical knowledge of Microsoft Operating Systems • Excellent skills with Endpoint Protection (EDR/XDR, Anti-malware Solutions) Familiarity with Email Security Systems • Good Familiarity with IAM (Identity and Management) systems • A successful record of managing security tasks and/or projects. • Ability to perform complex tasks with limited supervision. • Understanding of IT security methods and solutions. • Familiarity with WAF – Advantage • Familiarity with WEB application architecture – Advantage • Familiarity with AI security methods - Advantage • Familiarity with Cloud Security Technologies (AWS Security Tools, Google Security, Azure Security) – Advantage **Occupational Personality** • Great problem solving/analytical skills • Curiosity with good attention to detail • Ability to work both independently and collaboratively • Self-motivated to learn and develop one's skills and knowledge in various fields Passionate about Technology • Work well under pressure • Good written and verbal communication skills (English)