

CYBERSECURITY ENGINEER

Are you interested in joining an organization that:

- Plays a significant role in global airspace safety?
- Has over 35 years of experience providing industry leading Air Traffic Control (ATC) simulation training systems and state-of-the-art Air Traffic Management (ATM) solutions?
- Offers a job-related training tuition reimbursement program and access to various professional development opportunities?
- Has work/life balance programs in place and offers a holistic benefits package that is fully customizable based on your specific needs?

If this sounds interesting, continue reading about our job opportunity below.

Position Summary:

The ATM **Cybersecurity Engineer** supports the design, assessment, integration, and lifecycle assurance of secure and resilient Air Traffic Management systems, engineering environments, and customer-deployed operational platforms. The role combines hands-on vulnerability analysis with security architecture and systems engineering aligned with ATM Cybersecurity regulations. The engineer identifies and validates vulnerabilities, assesses information security risk in the context of operational continuity and system safety, translates information security obligations into verifiable technical requirements, and works with software, systems, network, infrastructure, safety, quality, project, and IT/OT teams to develop practical remediation and mitigation measures. The position contributes from analysis of proposals and requirements through architecture, implementation, integration, verification, deployment, maintenance, and controlled change.

Essential Duties and Responsibilities:

- **Vulnerability assessment and authorized validation:**
 - Identify, validate, and score vulnerabilities across ATM platforms and applications
 - Assess, exposure, asset criticality, compensating controls, operational continuity, recovery, and potential safety impact.
- **Security requirements and architecture assessment:**

- Translate customer, product, contractual, regulatory, and organizational information security and cybersecurity obligations into clear, testable, and traceable requirements
- **Secure design and remediation engineering:**
 - Working with systems engineers and solutions architect, develop security controls and remediation with software, systems, network, infrastructure, customer-site.
 - Address root causes proportionate measures such as segmentation, secure communications, privileged-access control, hardening, logging and monitoring, backup and recovery, resilience, and least privilege, while maintaining ATM performance, availability, interoperability, maintainability, and safety.
- **Verification, closure, and traceability:**
 - Define and validate closure evidence for corrective actions.
 - Verify implementation using appropriate verification activities.
 - Maintain traceability across requirements, findings, corrective actions, baselines, and verification records.
 - Record compensating controls and accepted residual risks.
- **Technical reporting and stakeholder communication:**
 - Produce concise, actionable assessments for technical and non-technical stakeholders.
- **Support of Proposal:**
 - Collaborate with engineering, product, and safety teams to develop competitive and compliant proposals.
- **ATM security and safety co-engineering:**
 - Work with system safety and engineering specialists to identify cyber conditions that could affect safety, integrity, availability, timing, redundancy, or operational service.

Competencies:

Conceptual Analysis: Considers a variety of factors; has different interests; wants to understand several different areas; likes theory as well as conceptual and abstract topics.

Systems thinking: Think long term; develop strategies that take a wide array of factors into account, including how the organization and market are changing; can take a step back and see the big picture in any situation.

Communication: Explains complex technical issues clearly and adapts the level of detail for implementers, engineering leaders, project teams, and management.

Team Consultation: Accepts having his opinions questioned; consults with team

members when making decisions that affect them; realizes that team members team members have valuable opinions that should be sought.

Conflict Management: Deals with disagreements that arise; defends his positions; gives in when appropriate; seeks an acceptable compromise and, ideally, “win-win” solutions.

Qualifications:

Required

- Bachelor's degree in Cybersecurity, Information Security Computer Science, Computer Engineering, Systems Engineering, Software Engineering, or a related technical discipline, or equivalent relevant experience
- 3 to 6 years of experience in cybersecurity engineering, vulnerability assessment, security architecture, network security, systems engineering, or a related field.
- Experience with risk management process (Risk Analysis, Risk Assessment and Risk Treatment)
- Strong analytical judgment, collaboration, communication, and reporting skills, with the ability to work independently and escalate complex architecture, exploitation, or risk-acceptance decisions for senior review.
- Ability to evaluate information security and cybersecurity changes in relation to system availability, redundancy, performance, interoperability, maintainability, and safety constraints across product and customer deployment environments.
- Ability to review system and network architectures, interfaces, data flows, and technical requirements, and translate identified risks into practical remediation.
- Working knowledge of vulnerability management, secure architecture, threat modeling, secure configuration, network security, authentication and authorization, cryptography fundamentals, and risk-based decision making.
- Hands-on experience with vulnerability assessment, configuration and security reviews, evidence analysis, and validation of technical findings.

Desired

- Experience securing mixed Windows and Linux environments, virtualized infrastructure, network appliances, and third-party integrated systems.
- Experience in aviation, ATM, industrial control, transportation, defense, or another high-availability operational domain is strongly valued.
- Experience with operational technology, industrial control, real-time systems,

aerospace, air navigation services, Air Traffic Management, or other mission- or safety-critical environments.

- Familiarity with security frameworks and guidance such as the NIST Cybersecurity Framework, NIST Risk Management Framework, NIST Secure Software Development Framework, ISO/IEC 27001, ISO/IEC 27005 or any risk management methodology, IEC 62443, MITRE ATT&CK, OWASP, Part IS (EU 2022/1645 and EU 2023/203), and recognized secure architecture practices.
- Experience with vulnerability lifecycle tracking, risk registers, security verification evidence, and exception or residual-risk documentation.
- Relevant certifications such as Security+, CySA+, CISSCP, GSEC, GIAC vulnerability assessment or penetration testing credentials, OSCP, or equivalent practical training. Core Competencies.

Other Qualifications:

- Ability to adhere to Adacel's Drug Free Workplace Policy.
- Ability to pass an Adacel background check while employed.

Physical Requirements:

- Occasional lifting – up to 50 lbs.
- Repetitive wrist, hand, and finger movement.

Work Environment:

- Location: Montreal.
- Job Status: Permanent, Full Time.
- Hybrid teleworking environment
- Alternative work schedules (9/80 with every other Friday off).
- Typically sitting at a desk

Benefits:

- Up to 26 three-day weekends annually with 9/80 schedule.
- Four weeks of vacation
- Company RRSP, SPSP (employer contribution), and TFSA.
- Full (100%) employer-paid insurance program from day one of employment.

How to Apply:

- You may apply by emailing your resumé to careers@adacel.com
- Include the position title in the subject line of your message.

Disclaimer:

Adacel is an Equal Opportunity/Affirmative Action employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, and protected veteran status.

This job description reflects management's assignment of essential duties and responsibilities. It does not restrict the duties and responsibilities that may be assigned. Reasonable accommodations may be made to enable individuals with disabilities to perform essential duties and responsibilities. If this job has a travel requirement, note that the frequency of travel may increase at any time due to adjustments in Adacel's business needs.