Working with its partners, the Ottawa Macdonald-Cartier International Airport Authority will be a leader in providing quality, safe, secure, sustainable and affordable transportation facilities and services to the airport's customers and communities within the National Capital Region.

The Information Technology and Telecommunications team is accepting applications for the position of **Information Technology (IT) Security Analyst**.

Reporting to the Chief Information Security Officer and Director Information Technology, the successful candidate will take a lead role in IT security related technical planning, architecture design, installation and integration, monitoring and maintenance of IT information security systems including networking, computing, software and external SaaS components. He/she will also take a lead role in critical and complex intra and inter-organizational projects requiring high levels of coordination and an extreme breadth of knowledge. Overall, the successful candidate will be responsible for the efficiency, effectiveness, evaluation, utilization, modernization and interoperability of security systems with existing networking and computing environments. Flexibility to shift hours will be required in order to provide response to critical issues and events that occur outside of normal work hours.

Essential functions:

Security Deployment

- Designs, builds and maintains a Security Information and Event Management (SIEM) system in accordance with industry and chosen vendor best practices;
- Identifies and implements key monitoring security metrics, develops SIEM use cases and alerts, and continuously monitors network, system and application vulnerabilities and threats;
- Monitors and continually fine-tunes advanced threat detection technology policies and practices in accordance with current threats and best practices;
- Builds, executes and maintains a Threat and Vulnerability Management System, including vulnerability and patch scanning, web application scanning, penetration and application testing, compromise and configuration assessment;
- Builds Minimum Security Baselines (MSB) and performs System Hardening and Configuration Management for Endpoints (PCs, mobile devices, kiosk, etc.), servers (Windows, database, DNS, DHCP, etc.), network (switches, routers), other systems (copiers, fax VoIP, SCADA, IOT, Cloud etc.); and
- Provides input and makes enhancements around securing new and existing IT systems as well as third party connectivity.

Security Operations \ System Hardening and Configuration Management

- Monitors for attacks, intrusions, anomalies, unauthorized or illegal activities;
- Internal threat monitoring and contributing through intelligence services/platforms;
- External threat monitoring from various threat feeds and ISAC platforms and incorporating these feeds to security tools to ensure that known threats are blocked;
- Investigates, documents, and reports on information security incidents, issues and emerging trends;
- Assists and performs system updates, IPS/IDS signature updates, antivirus updates and roll out software patches; and
- Tracks, reports on and remediates vulnerabilities and system weaknesses by working collaboratively with IT Infrastructure and other technical staff.

Security Audit

- Ensures that critical systems and processes are in compliance with the organization's minimum-security baselines and/or industry practices;
- Coordinates with other system owners to assess and improve their cyber security risk postures;
- Develops security metrics templates and prepares monthly and annual security metrics reports;
- Maintains cyber forensic toolsets and makes enhancement acquisition recommendations;
- Assists with ISMS compliance, security programs, projects and other initiatives as required;
- Manages the organization's Data Governance Lifecycle (discover, remediation, asset registry, data flow mapping);
- Performs Privacy Impact Assessments (PIA) for new and existing projects/systems; and
- Supports the organization's vendor management processes by performing Vendor/3rd Party Risk Assessments.

The successful candidate must have strong analytical skills in security analysis in order to identify appropriate solutions. He/she must be able to analyze security breaches to determine their root cause. The successful candidate must be able to anticipate cyber-attacks, always thinking one-step ahead of a cyber-threat. He/she must be detail-oriented, self-motivated and demonstrate initiative when performing tasks. The successful candidate must be able to discover, identify, capture and document relevant information into a cohesive report. He/she must have superior research and report writing skills and must be able to conduct security and compliance audits. The successful candidate must have strong customer service orientation with the ability to deal effectively with end users. These abilities, as well as a professional, positive attitude will ensure success in building positive working relationships in a team environment.

Qualifications for this position include:

- Completion of a three-year diploma/degree in a relevant field of study that may include, but is not limited to Information Technology, Information Systems, or Engineering;
- Five years of experience in a similar position where duties included participating in threat and risk assessment;
- Experience in deploying and operating vulnerability scanners, such as Tenable, Rapid7 products or any other SCAP scanner;
- Experience in configuring and operating software whitelisting functionality in Windows environment, such as AppLocker, Faronics and similar tools;
- Experience in deploying and managing patch management systems, including SCCM, ManageEngine and similar tools;
- Experience in using network access control solutions such as NAC, Cisco ISE, Aruba Clear Pass;
- Experience with log management systems and SIEM systems;
- Demonstrated experience with endpoint protection methods and malware defenses.
- Strong knowledge of Python, PowerShell scripting languages;
- Excellent understanding of and experience with networking principles, standards and technology, and common protocols;
- Must demonstrate a deep understanding of Microsoft Windows account permission controls;
- Familiarity with security tools and software. Must demonstrate ability to use nMAP, Metasploit, OpenVAS, Netcat, Wireshark, Kali Linux suite;
- Familiar with IDS/IPS systems. Must demonstrate ability to customize IPS signatures;
- Must demonstrate the ability to write custom SQL query, RegEX queries to filter for security events; and
- Excellent communication and written skills in English.

The following will be considered as assets:

- Experience with NIST, HIPAA, and CIS standards;
- GIAC Certifications, IT Security Certifications;
- Knowledge of PCI-DSS, ISO 27001:2013 and ITIL Standards and procedures; and
- Bilingualism (English and French).

Candidates must be in possession of a Class G drivers' licence (province of Ontario or Québec equivalent) along with a driver's abstract (issued within the last month) and must be in possession of or be able to obtain a security clearance for an Airport Restricted Area Identification Card (RAIC).

Interested candidates should forward their résumé by June 26, 2019, to work4us@yow.ca.

We thank all applicants; however only those selected for an interview will be contacted.

The Ottawa Airport Authority is committed to the principles of Employment Equity and to achieving a workforce that is representative of the diversity of the Canadian population. We strongly encourage candidates to self-identify if they are a person with a disability, an Aboriginal person or a member of a visible minority group.

International Airport Authority Ottawa Administration de l'aéroport international