STAFF VACANCY CODE CA070921

Description: Cybersecurity Analyst, **CA090721**

Department: Information Systems

Type of position: Full-Time Permanent

Location: 5160 Yonge Street, Toronto, Ontario

Reporting to: Director, Technology

Since 1976, Tarion has provided new home warranty protection to more than 2 million Ontario homes. We serve new home buyers and new homeowners by ensuring that one of their life's biggest investments is protected. Almost every new home in the province is covered by a new home warranty. This warranty protection is provided by Ontario's builders and lasts up to seven years. It is backstopped by Tarion. More than 375,000 homes are currently enrolled in the warranty program. Every year about 55,000 new homes are enrolled.

With more than 265 employees, Tarion works hard every day to serve the public interest by, first and foremost, protecting consumers and their new home purchases. We investigate homeowner warranty claims; resolve warranty disputes between homeowners and builders; and provide deposit and delayed closing protection for new home buyers. We also manage the Guarantee Fund, an important financial reserve designed to help shield Ontario consumers from possible catastrophic building events. All of this enhances fairness and confidence in Ontario's new home building industry.

The Cyber Security Analyst protects company hardware, software, users, network, and the organization from cybercriminals. The analyst's primary role is to understand company IT infrastructure and the organization's technology landscape in detail, always monitor it, and evaluate threats that could potentially breach the company defences. The cybersecurity analyst continuously looks for ways to enhance company's security posture and protect its sensitive information.

Responsibilities:

Identify

- Identify, evaluate and report on current threats to environment based on known vulnerabilities, exploits and the IT controls and technologies deployed in the organization.
- Assess security requirements and controls during the application development and acquisition process as defined in the company's security policies and standards.
- Coordinate and perform vulnerability testing on a cross section of IT systems, and identify gaps in security, recommend courses of action to mitigate any apparent risks and strengthening operational security.

Monitor

- Monitor vulnerability business metrics and produce regular security reporting and security dashboards. Execute, manage and maintain activities within the Enterprise Information Security Awareness program

Report

- Maintain key business metrics for Security Awareness throughout the organization and produce regular security reporting.
- Report to management concerning residual risk, vulnerabilities and other security exposures, including misuse of information assets and noncompliance.
- Response and produce regular security reporting.
- Provide support to ongoing external and internal audits and audit remediation on information technology, including generating technical recommendations.
- Assist in the design of information security controls and development of standard security configurations, around new and existing information systems and processes
- Assist in the review, analysis and documentation of system, network and application security vulnerabilities. Recommend remedial actions, and work with system owners, custodians and business partners to develop plans and timelines to address risks.
- Develop, manage and deliver on effective implementation of the Cyber Security Program
- Perform vulnerability assessments and tests to uncover flaws and help technical teams to remediate identified vulnerabilities to maintain high security standards.
- Provide risk analysis in configurations and procedures for existing and newly introduced systems, third party providers and processes.
- Develop and maintain the organization's Information Security Incident Response capability, procedures and processes

- Develop and review Information Security related standards, procedures and documented controls, to identify gaps and recommend process improvements. Coordinate activities to mitigate and respond to any identified risks.
- In partnership with internal business units and staff across the organization ensure that corporate information security policy; standards and practices are embedded in projects/initiatives, new implementations and operational tasks.
- Creation of security playbooks.

Vendor Management

- Perform and monitor security risk of third-party vendors and assist with the escalation of any issues that may impact business objectives and priorities involving vendor selection.
- Assist and execute information security risk and control identification, evaluation, documentation, analysis and reporting using analytical tools to support the process.
- Partner with cross functional stakeholders (Finance, Legal, CIO, Business Unit Security teams, etc.
- Research New Technologies.
- Conduct security research in keeping abreast of latest security threat landscape and stay abreast with the current information technology trends.

Qualifications:

- Minimum 3-5 years of experience working in an IT security function, specifically related to industry best practice compliance frameworks.
- Security and privacy first mindset
- Strong analytical skills to analyze security requirements and relate them to appropriate security controls.
- Experience in ITI, NIST or a comparable set of best practices for Information Technology Service Management
- Working knowledge of the incident response lifecycle and MITRE ATT&CK Framework
- Relevant accreditations/certifications and experience with ERM/GRC platforms an asset.
- Bachelor's degree in information systems or equivalent experience
- Experience with Enterprise Network & Systems cloud Architectures
- Experience with Information Security & Risk Management Security Frameworks
- Relevant accreditations/certifications and experience with ERM/GRC platforms an asset.
- Vulnerability Management and Security Awareness

If you are a person with a disability and have questions or would like help with your application, please email careers@tarion.com

Application Submissions & Deadline:

Please submit a covering letter and resume with vacancy code **CA070921**, no later than **September 21, 2021** to careers@tarion.com.