Security Operations Analyst Role Description

Duties of Role

- Ensure log coverage across environments, SIEM configuration improvements, alert triage and initial response
- Implement/ensure AV coverage across all environments, alert triage and initial response
- UI administration of security tools such as MDM, Removable device management, vulnerability and configuration management, web proxy, password store
- Report generation from security tools
- Conducting user access reviews
- Assisting in security investigations/incident response/disaster recovery as required
- Security control automation and monitoring
- Provide support to business stakeholders with security-related issues/inquiries
- Maintain security monitoring tools
- Investigate suspicious activities
- Create and maintain security reports as required by management
- Assist in ISO27001 and ASAE3402 compliance audits
- Keep on top of latest security trends and alerts
- Best practice security recommendations for current and new technologies
- Evaluate and determine required remediation after penetration tests
- Action vulnerability reports
- Action patching reports
- Action anti-virus alerts and reports
- Monitor usage of unlicensed and pirated software
- End to end risk assessment of all solutions bot in BAU and core Class production services
- Integration of security logging from internal and cloud sources
- Eyes on glass (ongoing security monitoring)
- Documentation of security related procedures and system configurations

Required Knowledge

- Familiarity with general information security concepts and practices
- Familiarity with general IT environment concepts such as change and patch management
- Knowledge of common security tool implementation, concepts, configuration and administration
- Knowledge of common attack vectors, threat tactics and attacker techniques
- Understanding of Windows and Linux operating systems
- Understanding of Infrastructure as Code concepts
- Familiarity with DLP
- Familiarity with IAM & RBAC
- Understating of SSO concepts such as integrated windows authentication, SAML

Desirable Experience

- 3+ Years working in an IT Security Operations role or similar
- Experience with cloud (AWS, Azure) solutions

Desirable Qualifications

- Relevant industry certifications such as CCNA Security, CISSP, CEH
- Tertiary Education in related field

Required Qualities

- Ability to work independently without direction on day to day activities
- Ability to work in a team
- Ability to analyse and understand technical information
- This position will interact with stakeholders across various groups of Class' business; the ability to build strong working relationships is critical for success
- Capable of learning new concepts and processes quickly, and adapting to a constantly changing environment
- Strong communication skills