Payments Network Malaysia Sdn Bhd (836743-D)

Job Description	
Position	Head of Systems Access Control
Department	IT Security
Division	Information Services

Summary of responsibilities

- Key member of the Senior Technical Committee for IT Security and represents Access Management, Application and Cloud Security within ISD Division and PayNet
- Leads major improvement initiatives in the overall access management
- Drives security within DevSecOps culture, develops framework and governs secure code development
- Leads security of applications in the cloud
- Plans, directs and organizes work program for team members within corresponding functional area on solutioning & dimensioning, including development, deployment, support and operation.

Key Areas of Responsibilities

- Responsible in leading and managing the delivery and solution of PayNet's Access Management, which includes the areas of Identity & Access Management (IAM), Privilege Access Management and Identity Governance
- Leads security in DevSecOps, driving down risk of exposure in code development for business applications, track and ensure potential threats are mitigated by the respective owners/developers
- Accountable for production issues and serves as a Subject Matter Expert (SME) within an area of specialty, extending advice and consultancy to cross functional teams.
- Acts as first level approval for user & systems access, vpn access and certificate renewals requests
- Improves the efficiency and effectiveness of the provisioning and fulfilment cycle by way of automation of repeatable tasks and fact gathering for post configuration validation
- Coaching and mentoring professional and junior team members – talent management, performance management and people management.
- Ensures relevant team members responsible for the provisioning of access are able to support and troubleshoot with the banks (and internal users, where applicable)
- Acts as the 3rd or 4th level technical point of escalation supporting the team during troubleshooting / support to the banks
- Manages and improves the support quality to the banks for new and existing access issues

Other areas of responsibilities include:

- To plan out work assignments for access management and project execution for team members within the department / Information Services division
- To correlate organization's / division's prioritization for the work plan and manage resources towards execution accordingly
- To keep abreast with industry security practices
- To be well aware of emerging risk, interpret and prioritize within organizational context, assess and propose improvement of relevant controls
- To be aware of and uphold security responsibilities as stated in the company's Information Security Policy;
- Heads cross collaboration within and between functional units
- Supports and promotes cyber exercises such as tabletop & cyber drill
- Acts as the liaison regarding the work of information security consultants, contractors, temporaries, and outsourcing firms
- Initiates and manages special projects related to information security which may be needed to appropriately respond to ad-hoc (or as dictated by current business and technological developments) or unexpected

information security events
- Brings pressing information security vulnerabilities to top management's attention so that immediate remedial action can be taken
- Stays informed about the latest developments in the information security field, including new products and services, through on-line news services, technical magazines, professional association memberships, industry conferences, special training seminars, and other information sources
- Constantly reviews measures & KPIs where it make sense, consistently achieving / exceeding measures set
- Communicate clear and specific performance expectations and measures of success to subordinates inclusive of explaining business unit goals and results, and how their contributions made a difference
- Provide candid performance feedback to subordinates and peers (as applicable)

Qualifications

Minimum Qualifications

- Degree in Computer Science with a minimum of at least 10 years of relevant work experience.
- Experience in the IT banking and Telecommunications sector would be an added advantage.

Technical Qualifications

- Expert level knowledge with Identity Architecture, designing & implementing federation with OAuth 2, OpenID Connect, SAML
- Expert level knowledge with Cloud and DevSecOps, designing highly available, resilient and scalable cloud native services and microservices architectures
- Extremely experienced architecting and designing from ground zero a resilient, highly available and low latency native Cloud service using AWS components.
- Extremely experienced with building on end-to-end Cloud >80% automated pipeline covering the phases of Development, Staging, UAT and Production.
- Must be adept at programming in at least one language: C, .NET, Go, Python, Rust, Java, Node.js, Angular, Ruby, Perl or advanced shell scripting.
- Experienced with jig-saw puzzling SaaS or tool set offerings to provide a holistic Cloud managed service:- Sumologic or Datadog for logging; PagerDuty for escalations; Runscope for synthetic monitoring; SonarQube for code hygiene; Veracode for secure coding etc.
- Cryptographic key management including PKI and digital certificates
- Technical documentation
- Understanding of ISMS and PCI DSS

Additional Requirements:
- Effective communication skills.
- Extremely diligent, fine eye for details, supreme problem solving capabilities and a team player.