Cybersecurity Engineer

Founded in 2015 to address the unmet financing needs of SMEs, **Validus is today the largest online lending marketplace in Singapore** with a growing presence in Indonesia, Vietnam and Thailand.

An award-winning Fintech, Validus uses data analytics and AI to provide growth financing to SMEs via funds from HNWIs and institutional investors. Backed by global VCs, our mission is to drive financial inclusion for SMEs through technology, data and industry collaboration.

As with the SMEs we serve, we may be small but together we are a mighty force! Our success is dependent on what each of us does, how we do it, and our belief that we can always do better. We're building a strong team of passionate, capable individuals who are committed to making Validus the best online lending marketplace in the region.

Background

We are looking for Cyber Security Engineer for a leading Fintech based in Singapore. Our ideal candidate is a professional with experience in providing IT Security and Ops services in the areas:

- Enterprise security across all the platforms (Web, App), Infrastructure, Cloud Ops
- Enterprise service ops and monitoring

Job Responsibilities

- Review and development of Technology Risk Management policies covering security framework, information security policies, processes / procedures and guidelines on an ongoing basis
- Work with vendor to conduct security assessments and penetration tests across regional platforms
- Identify security gaps, perform threat risk assessments in current setup and propose mitigating measures
- Standardize and refine security incident response and escalation processes
- Mitigate and contain threats when detected, and escalate security incidents and non-compliances on a timely basis
- Work with IT infrastructure / DevOps team to evaluate, implement and enhance the Cloud security, Network perimeter security and endpoint security,
- Monitor information security alerts triage mitigate, and escalate issues as needed
- Conduct information security awareness training.
- IT Security Management of various aspect, e.g. network security, server security, application security, end point security, email security, physical access security, logical access security

Qualifications

- At least 3 years of related work experience in cybersecurity management and security governance
- Good working knowledge of security risk management, security governance framework and compliance (IT Security Audit / log review), technical vulnerability management (vulnerability assessment, penetration testing), application security, security technologies, security incident response and security assessment
- Hands-on experience in managing AWS Security and Web / App security
- Have understanding of Technology Risk Management, Disaster Recovery, Business Continuity and IT Regulatory Compliance
- Possess at least CISSP, CISM or equivalent IT security certifications.

- Very good inter-personal and collaboration skills