IT Security Engineering Lead

|  |  |
| --- | --- |
| **Job Description** | **Job Purpose**The job purpose is to continually improve the confidentiality, integrity and availability of Secure Trust Bank systems and data by automating and integrating processes and applications into the existing environment, as well as introducing new platforms and improvements to increase STB’s cyber resilience and EDR/XDR posture. You will also make STB’s network more secure by implementing secure configurations and automated testing, in order to protect customer and employee data and maintain high levels of customer service. **Key Responsibilities*** Proactively develop tools to improve detection and response of security related events and incidents across the business
* Identify, improve and automate IT related processes
* Identity and define system security requirements
* Work with SOC and Threat Intelligence analysts to analyse, review and remediate security related incidents/logs, as well as automating the process as much as possible
* Contribute towards building maintainable SIEM, SOAR and SOC solutions
* Introduce and architect new technologies and platforms to improve Secure Trust Banks security posture and resilience
* Define, document, maintain and issue IT security related build and configuration documentation
* Configure, maintain IT security related infrastructure devices
* Work with the Infrastructure team to design secure configurations for network and system architecture
* Prepare and document standard operating procedures and protocols
* Complete comprehensive reports including assessment-based findings, outcomes and propositions for further system security enhancement
* Be an escalation point for the Service Desk in respect to IT security-related matters
* Undertake threat monitoring using defined sources of intelligence from across the industry and keep abreast with the latest and emerging threats and security trends.
* Test adherence to security policies and operational procedures utilising various testing methods (e.g. vulnerability scanning, liaising with external Pen Test providers, configuration reviews etc.)
* Conduct IT risk assessments for solutions, processes and applications.
* Support with the development and testing of desktop, laptop, server and mobile builds.
 |
| **Job Specification** | **Knowledge/Experience*** Hands on experience in the maintenance and administration of security systems, including firewalls, intrusion detection systems, anti-virus software, authentication systems, log management, content filtering, etc
* Experience with Windows and \*nix operating systems, including public and private hosting.
* Experience architecting, implementing and maintaining security systems
* In-depth knowledge with various web related technologies and network/web related protocols
* Experience in creating in-house tools or security related applications/controls
* Good practical knowledge of IT security monitoring tools/SIEM solutions.
* Experience of IT testing tools, including but not limited to vulnerability scanners, data discovery and network auditing.
* Knowledge of scripting and programming languages (PowerShell, Python, C#, bash etc)
* Hands on experience with code repository maintenance, CI/CD pipelines
* Ability to identify and implement areas for improvement following Change Control and IT governance practices.
* Credible and able to communicate with employees at all levels.
* Good understanding and use of of IT/Cyber/Information Security control frameworks, such as ISO27001, ITIL and/or Cobit.
* People facilitation skills.
* Ability to apply general/commercial awareness, specifically in the areas of security and IT services.
* Ability to communicate technical data to a non-technical audience.
 |