**IT Security Operations Dept**
Position: **Security Platform Management**

**Level:** Advanced – Senior level (Middle – Senior Level)
**Brief Description**:
In this role, you will be a key person for the overall CSOC architecture design and integration between the various platforms and components. You will be testing and building new, or updating existing, automation within CSOC technologies and integration between such technologies, including the larger set of systems and applications within KBank.

**Responsibilities**

- Identify, evaluate, design new systems and technologies and provide security engineering guidance and recommendations
- Work with the Threat Intelligence team to develop the technical design of the use case to be implemented in the SIEM
- Develop reporting dashboards and track key performance indicators
- Collaborate with the security monitoring team to improve the performance of the CSOC operations and assist in incident response and remediation efforts
- Evaluate and select appropriate technology solutions to meet SOC consumer needs
- Work with other SOC services to design automation and integration that meets their needs
- Work with the CSOC Architect to test and fine tune the technical design of the use case to be implemented in the SIEM
- Document SOC technology platform architecture and deployments
- Perform day-to-day CSOC log management platform administration tasks including configuration management, patch management, updates and testing, fine tuning, etc.
- Create searches, reports, dashboards and visualization
- Manage all security and other data collected and stored by the CSOC
- Implement, configure and onboard new data source

**Qualifications:**

- Bachelor's Degree in a related field such as Information Security, Management or Computer Engineering
- Platform-specific certifications is preferred
- Extensive experience with the design, development, implementation and management of security analytics, threat intelligence, security use case management and other CSOC and information security platforms
- Working knowledge and expertise in various security technology and product e.g. Splunk, ThreatQ, ThreatGrid and Cybercops
- At least 10 years of relevant experience in Cyber Security, Security Architecture, with minimum of four years in the design and implementation of a SIEM
- Experience working in a Security Operations Centre (SOC), Managed Security Service (MSS), or enterprise network environment
- Excellent written and oral communication skills
- Excellent organizational and time management skills

**Preferable capabilities:**
CSOC and Information Security Platforms
**Working Location:**
KBTG Building (Muang Thong Thani, Nonthaburi)