*Permanent Placement & Consulting Services in Information Technology*

# Security Management

Available Candidates

## Senior Cyber Security Manager – Flower Mound, TX

**Candidate Ref: 20182004**

Senior Cyber Security Manager with extensive focus on managing a Security Operations Center (SOC)

### Candidate Profile:

Provide oversight and day-to-day leadership for global security operations including SOC/incident response, user behavior analytics, threat and vulnerability management, red team, security engineering and architecture and cyber assurance including awareness training, vendor risk management, compliance (regulatory, customer, internal), business pursuit support, disaster recovery program management, policy and standards management, and IT risk management.
Notable Accomplishments:

- Set strategy and guided teams through evaluation and selection of next-gen firewalls consolidating stand-alone web filtering, intrusion protection, and sandboxing systems.
- Oversaw evaluation and implementation of volumetric DDOS protection for 6 data centers globally.
- Procured and developed simulated phishing campaigns with with PhishMe.
- Selected and Procured Skyhigh for Shadow IT monitoring and used to reduce the number of high risk cloud applications in use. Conducted a POC of UBA for sanctioned cloud services.
- Ran RFP for selection and implementation of managed SOC. Defined deliverables and ensure they are met.
- Selected and oversaw deployment of multi-factor authentication on our VPN system.
- Selected and procured Varonis for file server activity monitoring.
- Designed and authored a monthly executive level threat report which included an executive level summary of incidents, threats, and explanation of notable changes in metrics, a few key metrics, and summary of monthly security news including impact to CBRE or how CBRE is addressing.
- Conducted various assessments and/or gap analysis based on SANS top 20, DSD top 35, and ISO27K. Used 3rd party vendors when needed. Engaged Microsoft to conduct a proactive adversary detection assessment. Normalized results across assessments and created remediation plans including resourcing and costs.
- Selected and procured Tanium for better end-point visibility and incident response support.
- Built IT Disaster recovery program from the ground up including application tiering standards, various templates for testing reports and recovery plans. Initiated a project to create a global application inventory, consistently tier applications and built an annual risk-based testing plan.

- Selected and procured McAfee full disk encryption product and built a deployment strategy addressing high risk systems first then moving to a more organic approach to encrypting remaining systems.
- Globalized various technologies such as SIEM, Anti-malware, vulnerability scanning, pen testing, Intrusion protection, and Tanium which provided a common toolset for asset protection and incident response.
- Deployed global security awareness training via third party CBT modules.
- In 2012 became the interim global infrastructure leader while searching for a suitable replacement. This included managing a staff of several hundred and annual planning for $100M plus budget. During this time, I had the opportunity to lead the teams in recovery efforts from a significant technology failure resulting in activation of Disaster Recovery plans.

***Submit your request for this candidate by contacting us today!***

Contact Us