Job|| Sr Manager- Cyber Security - Business and practice development- Mauritius (7 yrs+)-

for MNC Consulting
Job Location :
Salary : 30 - 0 Lakh Per Annum
Experience: 0,40 Posted on: 01 Feb

Industry: Consulting
Job Type : Permanent

Job Description

Employer	: MNC Consulting
Job Location	:Mauritius
Profile	: Sr Manager- Cyber Security - Business and practice development
Exp	: Min 7 yrs+
Salary	: USD 4,500-5,000 per month(Basic, HRA and Car Allowance) + Insurance+ Travel Benefits+ Variable Pay

Roles and Responsibilities :

Business and practice development

- Building client relationships and establishing credibility by demonstrating knowledge of various aspects of cyber security, and identify opportunities where firm can assist.
- Supporting senior members of the team in developing client proposals and solution offerings.
- Managing project financials in line with agreed-upon budgets
- Driving the development of toolkits, methodologies and accelerators.
- Providing thought leadership and direction for the cyber security practice.
- Creating a positive working environment by monitoring and managing workloads of the team â balancing client expectations with the work-life quality of team members;
- Providing candid, meaningful feedback in a timely manner to team members;

- Keeping leadership and engagement management informed of progress and issues.

Client service

- Managing and delivering cyber security and cyber risk assignments, including producing documentation and reports, and quality assuring the work produced by junior team members.
- Working as a subject matter expert in your particular field to support a team, and/or managing a larger team in delivering engagements at scale.
- Maintaining awareness of key business and industry trends, and understanding how they impact responses to cyber risk.
- Design and development of IT Risk and Cyber security programs using industry frameworks and methodologies.
- Implementation and maintenance of enterprise-wide cyber risk governance frameworks.
- Assessment of enterprise-wide business risks and cyber threats, design and implementation of cyber risk management controls
- Championing the delivery of the highest quality services to firm's clients, and actively managing and mentoring junior team members to do the same, while managing the risks to the firm.
- - Conduct penetration tests on both business critical infrastructure and applications to support the organizations risk management program.
- Scope and deliver security testing engagements on time and within budget according to stakeholder requirements and organization needs.
- Provide quality assurance and technical reviews of deliverables, results and internal documentation (peer review)
- Evaluate remediation suggestions and provide consultative support with implementation of remediation steps, standards, and best practices where needed.
- Understand and consider industry trends, customer needs, business risk tolerance, and business environments relating to information security.
- Understand and clearly communicate potential threats, vulnerabilities, and control techniques.
- Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, anti-forensics, and detailed system usage
- Hunt and respond to advanced adversaries such as nation-state actors, organized crime, and hacktivists
- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis, or definitive data loss determinations
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation.
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connections

- Target advanced adversary anti-forensics techniques like hidden and time-stomped malware, along with utility-ware used to move in the network and maintain an attacker's presence
- Use memory analysis, incident response, and threat hunting tools to detect hidden processes, malware, attacker command lines, rootkits, network connections etc
- Track user and attacker activity second-by-second on the system via in-depth timeline and super-timeline analysis
- Identify lateral movement and pivots within client enterprises, showing how attackers transition from system to system without detection.
- Apply incident handling processes-including preparation, identification, containment, eradication, and recovery-to protect enterprise environments
-

Please send your CV with below details if this suits your requirement:

1. Current Salary
2. Expected Salary
3. Current Employer
4. Current Location

5, Current Location

6. Ok for Mauritius-Yes/ no

Regards,

Saket

Phenom Placement

saket@phenomplacement.com

Keywords: cyber security jobs, Mauritius Jobs, Cyber risk jobs

Desired Candidate Profile

Education: Any Graduate - Any Specialization,Any Post Graduate
Experience: 0,40