Cyber Security Operations Analyst

Join a leading Canberra security specialist firm as Cyber Security Operations Analyst and demonstrate your existing expertise in the security space. In this full time role you will be pivotal in monitoring networks, systems and responding to cyber attacks.

Responsibilities

- Analyze potential application and infrastructure security incidents to determine if incident qualifies as a legitimate security breach
- Perform host and network incident investigations, determining the cause of the security incident and preserving evidence for potential legal action
- Initiate escalation procedures to counteract potential threats/vulnerabilities
- Appropriately inform and advise management on incidents and incident prevention
- Develop technical solutions to help mitigate security vulnerabilities and automate repeatable tasks
- Write comprehensive reports including assessment-based findings, outcomes and propositions for further system security enhancement

Requirements

- Proven working experience in maintaining and monitoring security systems
- Hands on experience in security systems, including firewalls, intrusion detection systems, anti-virus software, authentication systems, log management, content filtering, etc
- Experience with network technologies and with system, security, and network monitoring tools
- Experience with Security Information and Event Management (SIEM) tools like ArcSight, QRadar, Splunk, etc.
- Experience with Vulnerability scanners like Nessus, MVM, Qualys, etc.
- Programming and scripting skills
- Problem solving skills and ability to work under pressure
- Bachelor degree in Engineering, Computer Science or related field
- Australian citizen able to receive government security clearance

Self Improvement

The cyber security field is highly dynamic and requires committed professionals who seek to continually learn and improve. Ionize recognise the importance of self-improvement and invests heavily in its people so they can be the best in their respective disciplines. As such, the successful candidate is expected to complete the (ISC)^2 CISSP exam within six months after commencement. Study materials will be provided and reasonable study leave will be approved while the successful candidate is pursuing certification. Future education requirements will be guided by the successful candidate's domain specialisation.

Workplace Culture

Ionize is an equal opportunity employer seeking representation from all areas of the community. We believe a diverse set of people with varied perspectives give us a significant advantage and a great place to work!

Application Process

We are seeking to hire ASAP! If you think you fit the role and want to join a local success story that can offer you a challenging and rewarding environment whilst supporting your career development apply now! Email your CV and an introduction of yourself to careers@ionize.com.au quoting reference CSOA0516. Salary is negotiable based on skill and expertise.

Please note, due to the nature of this work, eligibility to obtain an Australian security clearance is mandatory.

Disclaimer: Ionize does not accept unsolicited agency resumes. Ionize is not responsible for any fees related to unsolicited resumes.