Cyber Security Vulnerability Management Platform Engineer

Hiring organization
Services Australia

Employment Type
Contractor

Beginning of employment
January 2025

Duration of employment
12 months with 2 extensions of 12 months each.

Job Location
ACT, VIC, QLD, SA

Valid through
24.10.2024

Base Salary
$ 1200 - $ 1360

Description

- The Cyber Vulnerability Management team are seeking cyber security professionals with extensive experience in developing and maturing Cyber Vulnerability Management capability. The successful candidate(s) will lead the development of required processes and supporting technologies to mature Services Australia's Cyber Vulnerability Management capability.
- Vulnerability Management Platform Engineers use their in-depth knowledge of specific ICT Platforms to provide expert advice on the management and maintenance of those platforms. They work closely with key third party suppliers to ensure the provision of a robust infrastructure capability to the business and liaise with architecture and shared services areas to ensure the security of the day-to-day technical operations.
- Vulnerability Management Platform Engineers exercise a considerable degree of independence, with decision making substantially dependent on their high-level judgement and consideration of wider agency implications, with work being performed under the general guidance of senior staff.

Vulnerability scanning tools

Rapid7, Tenable, Sentinel, Windows Defender, Forescout and any additional tools

Responsibilities

Key duties may include, but are not limited to:
• Develop and document relevant processes to mature Vulnerability Management capability.
• Align the Vulnerability management process with the relevant policies.
• Undertake actions to discover, assess, report, act and evaluate cyber vulnerabilities.
• Prepare detailed reports and presentations for management on vulnerability status.
• Analyse vulnerability findings and prioritize remediation actions.
• Collaborate with IT and development teams to implement security measures. key to delivery of an optimal vulnerability management solution manage the design, installation and operation of the ICT system for vulnerability management and end to end process mapping.
• Provide broad technical support for project build, test and solution deployment activities.
• Configure and manage all non-functional platform capabilities including job scheduling, output management, email, archiving, technical security, technical connectivity between software components.
• Liaise with the infrastructure team in the design, procurement and deployment of hardware and related assets.
• Manage the regular maintenance of patches and support packages for all technical layers.
• Manage the operation of backup, high availability and disaster recovery solutions for IT systems.
• Develop staff capability through coaching, mentoring and succession planning collaborate with a broad range of internal and external stakeholders to achieve project outcomes prepare and review a range of technical documentation and reports

Qualifications
You must hold a Negative Vetting Level 1 Security Clearance

Experience
Mandatory Criteria
• Demonstrated experience in vulnerability management platform deployment/management/design for ICT projects within Federal Government.
• Proven experience in developing cyber vulnerabilities management processes and supporting technologies to effectively discover, assess, report, act and evaluate cyber vulnerabilities.
Weighted Criteria
• Experience in various vulnerability management platforms within large scale ICT projects for Federal Government.
• Experience in aligning the Vulnerability management process with the relevant policies.
• Demonstrated experience in preparing detailed reports and presentations for management on vulnerability status.
• Ability to analyse vulnerability findings and prioritize remediation actions.
• Collaborate with IT and development teams to implement security measures.

Skills
Key skills and experience requirements:

1. Proven experience in developing cyber vulnerabilities management processes and supporting technologies to effectively discover, assess, report, act and evaluate cyber vulnerabilities.
2. Good understanding of tools and technologies used to perform regular vulnerability identifications.
3. Develop and maintain vulnerability management policies and procedures.
4. Excellent analytical and problem-solving abilities.