Job Description Form – Cyber Security Analyst

|  |  |  |  |
| --- | --- | --- | --- |
| **Position number:** | Generic | **Classification:** | Level 5 |
| **Division:** | Corporate Services | **Branch/section:** | Digital and Technology Services |
| **Reports to:** | 16347 – Manager Cyber Security – L7 | **Direct reports:** | Nil |

About the Department

|  |  |  |
| --- | --- | --- |
| Mission | Vision | Values |
| To lead the public sector in community – focused delivery with a high performing organisation and thriving workforce. | Western Australia is celebrated as the best place to live in Australia. | Respectful AccountableResponsiveOpen-mindedIntegrity |

Context

The Corporate Services team includes human resources, payroll, business operations and digital and technology services. It helps the Department of Local Government, Sport and Cultural Industries to reach its mission to enable dynamic and inclusive communities and support the WA economy through effective regulation and the facilitation of outstanding sporting and cultural experiences and opportunities.

Position purpose

Responsible for the detection, analysis, and response to security events to protect DLGSC information assets. This role involves continuous monitoring, investigation, and response to security incidents, addressing threats as they arise. Undertakes network security analysis, threat hunting, and incident response. The role provides expert advice on current, evolving, and emerging information security issues.

Responsibilities

1. Monitors and reviews system events, threat notifications and other security alerts to prevent and detect cyber security threats.
2. Discovers and analyses security incidents and vulnerabilities.
3. Triages, contains and assists in responding to cyber security incidents in alignment with procedures, by gathering information to support the analysis, containment and recovery
4. Assists in the configuration of security tools, controls, monitoring and alerting.
5. Oversees vulnerability management program, including triaging of vulnerability scanning reports and coordination of remediation activities.
6. Liaises with internal and external stakeholders in the coordination of investigation into security incidents, exposures and potential breaches and works closely with internal stakeholders on effective threat detection activities aimed at protecting DLGSC from cyber security threats and incidents.
7. Engages stakeholders to raise awareness of cyber security protection requirements and foster a ‘security first’ culture.
8. Undertakes threat management, threat modelling, the identification of threat vectors and develops use cases for security monitoring.
9. Assists to undertakes cyber security risk assessments.
10. Provides technical advice and expertise to stakeholders regarding security matters and provides advice regarding information technology options or solutions that will uplift cyber security posture.
11. Contributes to the development and implementation of procedures and standards for ICT systems to safeguard sensitive and confidential data and associated information.
12. Contributes to the creation and generation of security reports, dashboards and metrics to evaluate the efficacy of security policies, tools and controls.
13. Adheres to Work Health and Safety, Equal Opportunity and other legislative requirements in accordance with the parameters of the position.
14. Perform any other duties as assigned or necessary to support the objectives of DLGSC.

Work related requirements

This section outlines the necessary minimum requirements, in relation to the knowledge, skills, experience and qualifications required to perform the duties of the position.

Essential

1. Demonstrated experience in the identification and management of information technology risks and security vulnerabilities in a complex and varied ICT environment, including methods to strengthen cyber security posture.
2. Demonstrated experience and knowledge of modern cyber security threats, tools and techniques with an ability to detect and analyse threats, respond to security incidents and identify root causes.
3. Sound written communication skills including the ability to prepare presentations, reports, technical documentation and other materials tailored to the target audience.
4. Sound verbal and interpersonal skills with the ability to build productive relationships and capability of communicating technical concepts to diverse stakeholders at all levels.
5. Demonstrated capability to achieve deadlines, self-manage workload and manage competing demands simultaneously with attention to detail and quality.

Desirable

1. Possession of or progression towards a relevant tertiary qualification.
2. Possession of relevant industry certifications for security (e.g. Security+, CC, SC-200, CSX-P, GSOC, CISSP).
3. Proficiency in scripting languages (eg. PowerShell, Python).
4. Knowledge and experience in providing information security services within a government or large corporate environment aligned to recognised frameworks (eg ASD Essential 8, NIST Cyber Security Framework or ISO/IEC 27000-series)

Special conditions

Nil

Pre-employment requirements

All department positions require a current Criminal History Check (National Police Certificate or equivalent) and 100-point Identification Check prior to commencement.

|  |  |
| --- | --- |
| Registration date | 7 October 2024 |