Government of **Western Australia**
Department of the **Premier and Cabinet**

Job Description Form

Threat Hunting and Critical Incident Response Manager - Level 7(DPC21060)

Date 9 March 2022

Division/Directorate
Office of Digital Government

Branch/Section
Cyber Security/Technical

Reports to
Director Cyber Security - Technical

Supervises
3

Operational Context:
The Office of Digital Government (DGov) is an Office within the Department of the Premier and Cabinet. DGov leads, supports, and coordinates the digital transformation of the WA public sector.

The Cyber Security Unit leads, coordinates and supports whole-of-government cyber security efforts to protect the WA Government's information, assets, and service delivery from cyber threats.

Role Overview:
Leads the Threat Hunting and Critical Incident Response team in the ongoing development, implementation and maintenance of information systems risk and security controls to protect the information assets of Western Australian Public Sector Agencies. Provides support for cyber security threat hunting and critical incident response to Public Sector Agencies.

Role Responsibilities:
Leadership and Management

- Leads and motivates staff within the Team in the provision of threat hunting and critical incident response services to Western Australian Public Sector Agencies.
- Promotes a culture supportive of innovation and continuous business process improvement.
- Provides information security policy, technical and operational advice to Public Sector Agencies on their cyber security incident response capabilities and processes.
- Works collaboratively with other members of the Cyber Security Unit to process threat hunting and cyber incident response workflows effectively and efficiently.
- Develops and maintains information security policies, standards, procedures, and frameworks.

Threat Hunting and Critical Incident Response.

- Establish and execute the Threat Hunting and Critical Incident Response program's strategic objectives and operational processes.
- Develop hunting hypotheses and use cases using insight gathered by the Security Operations Centre, Incident Response Coordination and Threat Intelligence teams
- Execute hunts, validate findings, and clearly communicate identified control gaps and detected adversary activity to the appropriate teams
- Maintain a current working knowledge of the forensic artefacts relevant in attack scenarios and how to obtain that evidence from the available technologies.
- Develop performance metrics to track, and drive continuous improvement of existing hunts, and make recommendations to close gaps identified in monitoring systems (such as SIEM use case and correlation rules, coverage, network/asset models)
- Provides principal support to the Director Cyber Security – Technical in the management and coordinated response to significant cyber security incidents affecting WA Public Sector Agencies.
- Provides principal support to the Director Cyber Security – Technical in the management and coordinated response to cyber security incidents that fall under the Cyber Incident Management Arrangements for Australian Governments (CIMA).

- Responsible for the analysis and reporting of cyber security incidents affecting WA Public Sector Agencies.

Corporate Responsibilities:

- Contributes to the achievement of corporate objectives by ensuring that stakeholders are dealt with in a professional and timely manner.
- Works within corporate policies and procedures, acts with integrity and demonstrates ethical behaviours aligned with the Department Code of Conduct.
- Performs other duties as directed.
- Takes reasonable care to protect your own safety and health at work, and that of others by co-operating with the safety and health policies and procedures of the Department and complying with all provisions of the Occupational Safety and Health Act 1984.

Role Specific Requirements and Capabilities

(The experience, qualifications and behaviours required to fulfil the role)

Leadership and Management

- Experience in a supervisory or management capacity.
- Well-developed conceptual and analytical skills, and the ability to resolve complex problems.
- Demonstrated written communication and interpersonal skills, and the ability to consult with internal and external clients, stakeholders, and business partners.

Threat Hunting and Critical Incident Response

- Demonstrable technical, hands-on experience investigating and responding to real world information security breaches, against appropriate security frameworks, principals, policies, and standards in various environments.
- Skilled in all aspects of the attacker/incident lifecycle process
- Knowledge of host forensic, network forensic, offensive security, malware analysis, and security monitoring.
- Experience in the development of automated detection logic.
- Extensive knowledge of threat actors, their tactics, techniques and processes, and mechanisms to detect them.
- Experience in analysing large data sets at scale.

Pre-Employment Requirements

To be eligible for permanent appointment to the Department, employees must be eligible to live and work in Australia indefinitely. Employees engaged on fixed term appointments require a valid work visa for the duration of the entire employment contract.

Appointment is subject to:

- 100-point identification check; and
- National Criminal Record Screening Clearance
- Baseline Clearance

Certification

DDG Signature:	**People Services:**
Date:	**Date:**