Australian Government
Bureau of Meteorology

A NEW OUTLOOK
FOR YOUR CAREER

Senior Cyber Security Threat Hunter

APS Level 6

JOB REFERENCE NUMBER	16198
CLASSIFICATION	APS Level 6 (ITO2)
GROUP	Data and Digital
PROGRAM	Cyber Security Centre
LOCATION	Melbourne
STATUS	Ongoing
WORKING HOURS	Full time
SALARY RANGE	$80,665 to $91,713, plus an additional 15.4% superannuation
CLOSING DATE	11:30pm AEST/AEDT Thursday, 5 November 2020
APPLICANTS	Australian Citizenship – see Eligibility Requirements
CONDITIONS	The successful applicant will be required to obtain and maintain a Negative Vetting 1 security clearance
CONTACT OFFICER	*Janette Nozzolillo* P: *03 9616 8325* E: *janette.nozzolillo@bom.gov.au*

Australian Government
Bureau of Meteorology

ABOUT US

The Bureau of Meteorology is one of the few organisations that touches the lives of all Australians and all Australia, every day. The Bureau works across Australia and remote islands, providing services from the Antarctic to beyond the equator, and from the Indian Ocean to the Pacific.

We are Australia's national weather, climate and water agency, in the Agriculture, Water and Environment portfolio of the Australian Government, operating under the authority of the Meteorology Act 1955 and the Water Act 2007. We provide data, information, knowledge, insight and wisdom to help Australians prepare and respond to the realities of their natural environment, including droughts, floods, fires, storms, tsunami and tropical cyclones.

Our products and services include observations, forecasts, analysis and advice covering Australia's atmosphere, water, oceans and space environments. We undertake focussed scientific research in support of our operations and services. Through regular forecasts, warnings, monitoring and advice, we provide one of Australia's most fundamental and widely used public services.

We have strong relationships with our customers, partners and stakeholders in Australia, including the Australian Community and the emergency services sectors, all-levels of Government, and focus sectors including aviation, agriculture, energy and resources, national security and water.

Our vision is…

To be an organisation of global standing, that is highly valued by the community for our pivotal role in enabling a safe, prosperous, secure and healthy Australia.

to achieve our mission…

To provide trusted, reliable and responsive weather, water, climate and ocean services for Australia – all day, every day.

by focussing on…

- Impact and Value
- Operational Excellence
- Insight and Innovation
- The Bureau Way

To contribute to a future with zero lives lost through natural hazards

Contribute to $2 billion of added social and economic value to the Australian community by 2022.

Australian Government
Bureau of Meteorology

WORKING AT THE BUREAU

The Bureau represents a dynamic and exciting opportunity. A role with the Bureau involves:

OUR WORK	OUR PEOPLE	OUR ENVIROMENT	OUR EXPIERENCE
Purpose-driven impactful work that brings real benefit to the Australian Community, businesses and industry.	A deeply passionate and highly skilled workforce that continuously challenges the status quo to achieve greater impact and experiences for our colleagues and customers.	A world class organisation with excellent workplaces in great locations, access to cutting-edge technology and a safe and inclusive environment for everyone.	A commitment to professional development and growth, backed by clear career pathways and training opportunities, and complimented by a competitive remuneration package.

POSITION OVERVIEW

The role of the Senior Cyber Security Threat Hunter is to detect, protect, contain, collaborate and to out-think cyber actor threats. The Senior Cyber Security Threat Hunter is to focus on solving challenging cyber security problems.

The Senior Cyber Security Threat Hunter plays an active role in detecting in advance threats to the Bureau network. They will hunt for malicious activity utilising indicators from sources both internal and external.

The Senior Cyber Threat Hunter may have computer network defence and network defence operational skills, is able to think like a cyber actor and use analytical skills to sift through false positives to find patterns and Indicators of Compromise (IoCs).

ROLE RESPONSIBILITIES

The responsibilities of the role include but are not limited to:

1. Search network flow, PCAP, logs and sensors for evidence of cyber-attack patterns and hunt for Advanced Persistent Threat (ATP) activity.
2. Actively hunt for IoC's and APT Tactics, Techniques and Procedures (ATTPs) in the network and host as necessary
3. Recognise and research attacks and attack patterns and tactics, techniques and procedures (TTPs), deep analysis of threat across the enterprise by combining security rules, content, policy and relevant data sets.
4. Create detailed incident reports and contribute to lessons learned in collaboration with the appropriate teams.
5. Collaborate with the Cyber Security Defence Centre and CSOC and threat analysts to contain and investigate major incidents.
6. Provide simple and reusable hunt tactics and techniques to a team of security engineers, specialists and CSOC analysts (when the augmented CSOC functions are established) and contribute to the development of cyber incident playbooks.
7. Work with the CSDC and other members of the CSC program team to improve and expand available toolsets and capability.

8. Analyse network perimeter data, flow, packet filtering, proxy firewalls and IPS/IDA to create concrete plan of action to harden defensive posture.
9. Monitor open source and commercial threat intelligence for IOC's new vulnerabilities, software weaknesses and other attacked TTP's.
10. Undertake other duties as directed.
11. Complying with all Bureau work, health and safety policies and procedures, and taking reasonable care for your own health and safety and that of employees, contractors and visitors who may be affected by your conduct.

SELECTION CRITERIA

The Bureau encourages applications from all suitably qualified candidates. Applications will be considered based on alignment with selection criteria, which have been matched to the APSC Work Level Standard and Integrated Leaderships Systems for APS6 positions.

1. Demonstrated experience in securing and hardening IT infrastructure.
2. Experience with scripting, vulnerability testing tools, network hunting, SIEM or other relevant tools or methods.
3. Knowledge or networking, applications and operating system concepts across a variety of platforms and environments including cloud environments.
4. Knowledge of vulnerability identification and exploitation.
5. Ability to work on multiple projects with changing priorities.
6. Ability to write procedures and present reports and recommendations, root cause analysis, incident response security vulnerability analysis and penetration testing findings.
7. Strong analytical and problem-solving skills, persistence, ability to undertake research, write and communicate and brief varying audiences (technical and non-technical).
8. Understanding of the Bureau's diversity and inclusion statement of commitment and APS Values and Code of Conduct

Mandatory qualifications (if applicable):

A degree or diploma of an Australian educational institution, or a comparable overseas qualification, which is appropriate to the duties; OR other comparable qualifications, which are appropriate to the duties.

MERIT POOL

The selection process will establish a merit pool that may be used to fill similar positions within 12 months

HOW TO APPLY

Applications can be lodged through BOMCareers.

Your application will consist of resume, contact details for two referees and a '800-word pitch' that considers:

- position overview
- job responsibilities
- selection criteria
- relevant sections of the Integrated Leadership System (ILS) and APS work level standards.

The Bureau is an equal opportunities employer. We will support applicants with disability through our RecruitAbility Program and will provide reasonable adjustments such as access, equipment and other practical support at relevant stages of the recruitment process.

We recognise the need for our workforce to reflect the community we serve and provide an inclusive environment that respects and values diversity and is described in our Diversity and Inclusion Statement of Commitment. We strongly encourage qualified applicants from diverse backgrounds to apply.

The Bureau offers flexible working options, reasonable workplace adjustments and an Employee Assistance Program (EAP). Should you have any questions or experience any difficulties with applying online, please contact the Recruitment Team on jobs@bom.gov.au or phone 03 9669 4401.

COVID-19 RESTRICTIONS

We understand there are unique and evolving challenges due to the current COVID-19 pandemic. The Bureau is responsive and making changes to ensure the safety of all candidates and our team.

Under the relevant legislation and guidance of the National Chief Medical Officer:

- Currently all interviews will be held via audio/video conference (across a range of platforms to accommodate personal requirements) unless otherwise advised.
- The successful candidate may be required to carry out the duties remotely for either a period or until otherwise advised.

ADDITIONAL INFORMATION

To find out more about the employment conditions at the Bureau, please refer to the Bureau of Meteorology Enterprise Agreement 2018.