Australian Government
Australian Financial Security Authority

afsa.gov.au

Selection documentation

Position title/ No: IT Security Operations Analyst / 30875

Classification: APS Level 6

Location: Brisbane/Sydney/Canberra/Melbourne/Hobart/Adelaide/Perth

Division/Section: Internal Client Services/ICT Service Delivery & Support

Reports to: Assistant Director Technology Security

Employment status: Ongoing / Non-ongoing (temporary) *

Hours: Full time - 37.5 hours per week

Security clearance: Negative Vetting 1

Salary: $86,090 - $96,494 p.a. (plus 15.4% super)

Closing date: Wednesday, 3 November 2021

Contact for questions: Paul Quirk: (02) 6198 3581

AFSA actively promotes flexibility with working options in this role to support your family commitments and personal interests

*This recruitment process is being used to fill a current **ongoing** position in either our Adelaide, Brisbane, Canberra, Melbourne, Sydney, Hobart or Perth office. A merit pool of suitable candidates may be established as a result of this process to assist AFSA to fill similar ongoing and non-ongoing positions that may become available over the next 12 months. Non-ongoing positions may be offered for a period of up to 18 months with the possibility of extension (up to a total period of 3 years). Should a non-ongoing position become ongoing or should an ongoing position become available, the merit pool established by this process may be used to determine a suitable candidate(s).

Eligibility

Please note that this opportunity is open only to Australian Citizens. The successful applicant must have, or be willing to undergo a security clearance to the level of Negative Vetting 1 as a condition of employment.

To satisfy character requirements all AFSA employees must undergo a police records check. Where a person has received a redundancy benefit from APS agency employment and their corresponding redundancy benefit period has not expired, they may be ineligible for employment.

About the area

The Internal Client Services Division is responsible for delivering a range of business and enabling services that support the Australian Financial Security Authority purpose through partnering with business divisions that regulate Australia's personal insolvency and personal property securities programs. The division provides professional services and leadership that promotes the efficient and effective operations of the agency whilst ensuring compliance with commonwealth legislation, polices and guidelines and promoting integrity, accountability and transparency.

Purpose of the position

The AFSA IT Security Operations Analyst will support the organisation through the monitoring and coordination of wide-ranging IT security solutions. The IT Security Operations analyst will provide generalist IT Security support and advice to the ICT Technology Security team and other stakeholders within AFSA. The primary purpose of the role is to take ownership of the practical security logging, investigation and reporting within AFSA.

Key Accountabilities

- Assist with the web and email policy and Whitelisting and respond to IDS alerts, monitor and report upon AFSA's specialist ICT Security systems and alerts.
- Assist with the management of incoming enquiries and correspondence through the Technology Security Operations mailbox and provide ad hoc advice to the Assistant Director Technology Security.
- Assist with the management AFSA's Security Incident and Event Management (SIEM) solution.
- Produce reports on the status of the security of AFSA's ICT environment, utilising AFSA's IT security systems and tools.
- Monitor vendor security notifications, assess potential impacts on AFSA's systems and engage internal teams to undertake remediation activities.
- Assist with the security maturity AFSA's ICT systems in accordance with the Australian Government's Information Security Manual (ISM).
- In collaboration with other members of the Security Operations team conduct vulnerability assessments, report assessment findings, and assist with remediation of identified threats and vulnerabilities.
- Maintain currency and expertise in information security related technologies, threats and trends.

- Display, uphold and adhere to the APS Values, Code of Conduct and AFSA's Workplace Diversity Program
- Comply with WHS obligations and take responsibility for own health and safety and that of others
- Understand and comply with the agency risk management framework and relevant legislation. Contribute to identification, reporting and mitigation of risks in your area.

Skills and Capabilities

Technical Capabilities

- Conduct security research and intelligence gathering on emerging threats and exploits
- Maintain the technical architecture of the cyber security systems, enabling all the components meeting established service-level objectives for system uptime.
- Maintain IT Security tools, develop and deploy content for the cyber security infrastructure, including use cases for dashboards, active channels, reports, rules, filters and trends.
- Coordinate and conduct event collection, log management, event management, compliance automation, and identity monitoring activities. Conduct vulnerability scans and review vulnerability assessment reports.
- Conduct system reviews for emerging Business needs and identify possible cyber threats/risks.
- Detects threats, investigates those threats, and respond to them in a timely fashion. Perform initial investigation and triage of potential incidents and escalate or close events as applicable.

Operates Efficiently

- Prioritises workload to achieve outcomes.
- Takes a flexible approach to planning in order to meet changing circumstances and considers the impact on others.

Examines and evaluates information and data from a wide range of sources to make evidence-based decisions

- Draws on information from diverse sources and uses experience and organisational/environmental awareness to analyse what information is important and how it should be used in the decision-making process.

Builds productive relationships

- Acts with honesty, integrity and respect in dealings with others
- Has the ability to understand others' perspectives, respectfully deal with conflict, manage boundaries and appreciate others' strengths and skills.
- Works effectively with stakeholders to achieve positive outcomes.

Qualifications, accreditations and experience

Mandatory Experience:

- Demonstrated experience in an IT security operations position
- Demonstrated experience with the administration, management, and investigation of alerts for a SIEM product both on-prem and cloud systems.

Desirable Experience:

- Awareness of the Australian Signals Directorate's Essential 8

Mandatory Qualifications:

The following skills and qualifications are mandatory for the position:

- Undergraduate degree in an IT Security related qualification
- Prior experience in one or more of the following disciplines:
    - Platforms administration eg: Windows,Linux etc
    - Network Administration
    - Storage Administration
    - Cloud Platforms eg: Azure, AWS, etc

Desirable Qualifications:

The following skills and qualifications are not mandatory but will be useful for the position:

- Studying for or completed the Certified Information Systems Security Professional (CISSP)
- Demonstrated experience within a cyber security operations environment
- Cloud Security Engineer qualifications (Azure, AWS)
- SIEM maintenance / Firewall / IDS/IPS rule management
- CISSP / CCSP / Linux skills
- Other cyber security qualifications or accreditation

Application details

The application is the tool that the selection committee will use to shortlist applicants.

Your application must include:

1. A completed Position Application Form (available on the AFSA website)
2. A current Resume/ CV including contact details for at least two recent referees
3. A one-page pitch, that considers the key responsibilities and essential capabilities of the position and states the following:
    - Why you are interested in the position
    - How your skills and experience make you the best person for the position
    - What value you can add to AFSA and the Internal Client Services Division.
4. State the position title and location in the subject line and email: recruitment@afsa.gov.au

Applications must be submitted no later than Wednesday, 3 November 2021.

A selection decision may be made on the basis of your application only. A telephone interview may be conducted in the first instance. Candidates may also be required to undergo psychometric and/or work sample testing as part of this selection process.

All pre-employment checks will be conducted via an external party (Equifax). For further information on Equifax's privacy policy please refer to: https://www.equifax.com.au/privacy

We encourage applications from Indigenous Australians, peoples from culturally diverse backgrounds and people with disabilities. We are committed to providing a working environment that values diversity and supports staff to reach their full potential.

If you are an applicant with a disability or other special needs, please contact the Disability Access Coordinator on (02) 8233 6999 to discuss any requirements that may assist you in your application.

Thank you for your interest in this position.