Cyber Threat Detection SIEM Specialist

Description

Cyber Threat Detection (CTD) Security Information and Event Management (SIEM) Specialist is required to perform a leadership role while exercising a considerable degree of technical skill and independence pertaining to the monitoring and response function of Services Australia Cyber Security.

The primary focus of the CTD SIEM Spec8ialist is to lead a multi-disciplinary team to develop and implement detection methods to identify, monitor, respond, protect against malicious cyber events targeting Services Australia and shared service agency networks.

This role requires in-depth knowledge of cyber security fundamentals to accurately determine impact and relevance of emerging and existing threats to operating environments. The CTD SIEM Specialist will draw upon their knowledge of detection methodologies and technologies, attack vectors, vulnerability management principles, network security, security engineering principles, information systems control design and control monitoring.

Key duties may include, but are not limited to:

- Threat Detection development inclusive of reviewing and approving detection use cases, response playbook development and implementation of detection use cases.
- Provide technical or strategic advice on complex issues related to detection technologies. Coordinate the accurate and appropriate referral and subsequent tuning of detection use cases.
- Review and contribute to process documentation including providing input into the development of processes and ensuring documentation created by the shift aligns with outcomes and goals of the process.
- Provide timely, relevant and accurate information to the Director Cyber Threat Detection where business impacts of events and decisions are sensitive, including but not limited to:
- Wide ranging impacts. Events affecting senior executives or other agencies.
- Confidentiality, integrity and availability are impacted.
- Provide technical guidance and support to Cyber Security Operations staff while overseeing Cyber Threat Detection roles.
- Prioritise tasks and duties in accordance with direction from Cyber Security Divisional teams considering risk, urgency and impact using independent judgement.
- Provide expert advice and assistance to team members performing technical work.

Primary Technologies required for role include:
IBM QRadar, Splunk, Elastic, Sentinel.

Qualifications

You must have a Negative Vetting Level 1 Security Clearance.

Experience

Mandatory Criteria

- Proficiency in managing SIEM platforms – QRadar, Splunk and Elastic.
- Knowledge of network architecture concepts including topology, protocols, components, and principles.

Weighted Criteria

- Experience in developing SIEM use cases and/or rules.
- Experience in SIEM administration.
- Understanding of the requirements of network security monitoring.

Hiring organization

Services Australia

Employment Type

Contractor

Beginning of employment

01 August 2024

Duration of employment

Initial contract of 12 months with possible two extnsions of 12 months each.

Job Location

ACT, VIC, QLD

Date posted

July 8, 2024

Valid through

15.07.2024

- Must possess strong verbal and written communication skills.

- Strong stakeholder engagement skills.
- Understanding of Windows and Unix/Linux logging.
- Familiarity with the MITRE ATT&CK Framework.