Position Description

SOC MANAGER

BUSINESS UNIT:	Security Operations Centre (SOC)
REPORTS TO:	Deputy Director Operations
MANAGEMENT:	Direct reports: Minimum 4
LOCATION/S:	Melbourne, VIC
POSITION TYPE	Permanent full-time

About AARNet

Australia's Academic and Research Network (AARNet) was established in 1989 and is widely regarded as the founder of the Internet in Australia and renowned as the architect, builder and operator of world-class network infrastructure for research and education.

We are Australia's National Research and Education Network (NREN). We connect over one million users—researchers, faculty, staff and students—at institutions across Australia, supporting education and research across a diverse range disciplines including high energy physics, climate science, genomics, radio astronomy and the arts.

Nationally, AARNet interconnects Australian universities, the CSIRO, and other organisations who have a research and education mission, or with whom the education and research sector interacts. These include hospitals, vocational training providers, schools and museums. Internationally, AARNet interconnects the Australian Research and Education (R & E) community to the world – and continuously develops new capabilities and partnerships to facilitate seamless data access and transfer.

AARNet also offers a suite of supporting applications to our customers. These include network and collaboration services such as CloudStor and Zoom, that enable innovation in the delivery of research and education.

We are an organisation of innovators, doers, and courageous thinkers. We are not constrained by traditional products and solutions and we constantly strive to build the solutions that our customers will need tomorrow – today. If you have the imagination, foresight and drive to build the future why not come and join us?

The Role

The Security Operations Centre (SOC) Manager has fully responsibility for the operations and management of the SOC.

The SOC Manager will ensure SOC excellence by guiding and coordinating the implementation of processes, practices, policies and procedures to support the strategic and operational objectives of the SOC. The SOC Manager will also measure and analyse the performance of the SOC and ensure that Service Level Agreements are met.

Leading the activity of the SOC team, the SOC Manager will be responsible for team performance and development. They will also oversee the escalation of incidents, and act as a conduit between the technical operational activities of the SOC and the wider business. The SOC Manager will also take a leading role in communicating the value of cyber security operations both internally and to customers and external stakeholders.

Responsibilities

Responsibilities for the role include:

- Leading the day-to-day operations of the SOC;
- Ensuring events and/or incidents are detected and responded to in accordance with established processes and SLAs;
- Oversee and review daily SOC analyst tasks;
- Coordinate the SOC team scheduling, including shift rosters, annual leave etc;
- Ensure effective incident management in accordance with established processes and SLAs;
- Identify and remediate operational disruptions and challenges;
- Effectively negotiate and escalate when required, roadblocks that may jeopardise security monitoring operations, infrastructure, SLAs, functioning of the SOC or any other SOC or Security related matter;
- Provide leadership guidance and mentoring to SOC staff;
- Interface and collaborate with external stakeholders and industry experts and thought leaders;
- Establish reportable data collection, analysis, monitoring and resolution metrics for SOC activities;
- Identify and action SOC Analyst training requirements;
- Ensure SOC staff follow agreed processes and procedures;
- Ensure all SOC processes and procedures are documented and published per AARNet requirements;
- Work with SOC staff to continually improve the operation and effectiveness of the SOC; and
- Serve as an incident manager for the SOC, along with other responsibilities as outlined above.

Expertise, experience & qualifications

- Bachelor's degree or equivalent;
- Post graduate studies will be highly regarded;
- 10-15 years experience in security operations, incident response, threat hunting roles and/or information security forensic roles;
- Significant team leadership experience;
- Demonstrated knowledge of all SOC related activities;
- Recognised as expert or leader in the domain of Security;
- Experience in a managed security services provider (MSSP) preferred;
- Broad Information Security technical knowledge; and
- Solid understanding of network services and other services as provided by AARNet.

Important skills

- Customer-oriented focus;
- Highly developed communication and influencing skills;
- Ability to succeed in a dynamic environment with competing priorities;
- Curiosity and a strong desire to learn;
- Ability to work with clear leadership but minimal day to day supervision;
- Strong analytical and problem-solving skills; and
- Experience guiding and/or mentoring staff.

Conditions of employment

AARNet is committed to diversity and providing equal opportunity to all. We're a great place to work if you want to make a difference. Remuneration will be based on skills and experience and will include an above market superannuation package.

How to apply

Applications, including a resume/CV and cover letter addressing the requirements of this role, should be sent by e-mail to employment@aarnet.edu.au. Closing date for applications: 26th July, 2019.