**JOB DESCRIPTION**

# Security Operations Engineer

# **ABOUT UNITING**

**Our purpose:** To inspire people, enliven communities and confront injustice.

**Our values:** As an organisation we are **Imaginative, Respectful, Compassionate** and **Bold**.

At Uniting, we believe in taking real steps to make the world a better place. We work to inspire people, enliven communities and confront injustice. Our focus is always on the people we serve, no matter where they are at in their life.

Our services are in the areas of aged care, disability, child and family, community services, and chaplaincy and we get involved in social justice and advocacy issues that impact the people we serve. As an organisation we celebrate diversity and welcome all people regardless of disability, lifestyle choices, ethnicity, faith, sexual orientation or gender identity. We commit to respecting children and take action to keep them safe.

Uniting is the services and advocacy arm of the Uniting Church NSW & ACT and as such Uniting leaders understand, support and can express the mission and purpose of the Uniting Church.

# **ABOUT THE ROLE**

**Role Purpose**

This role is responsible for monitoring, analyzing, and responding to security incidents, as well as implementing measures to prevent future incidents. This role requires a strong understanding of cybersecurity principles, as well as experience with security tools and technologies.

# ROLE KEY ACCOUNTABILITIES

You will be an integral member of the Security Operations team in the Finance, Property and IT di directorate through the following:

* Providing analysis of relevant research and operational information and assisting managers to evaluate and integrate the information they receive.
* Coordinating and maintaining team management systems and ensuring relevant information is input on a consistent and regular basis.
* Providing a collection of relevant data to assist with budgeting, the operation of the team and production of regular reports.
* Conducting specialised studies as required, providing insights into the operation of the team and the organisation.
* Actively promoting safe work practices in the workplace during all activities consistent with Uniting’s policies and comply with all WH&S legislation, policies and procedures.
* Actively contributes to a safe and supportive working environment that is inclusive of all staff through celebrating their nationality, cultural background, LGBTI status, abilities, gender and age.

As the security operations engineer, your role specifically will:

* Monitor security alerts and events to identify potential threats and vulnerabilities.
* Analyze security incidents to determine the root cause and develop effective response strategies.
* Implement and manage security tools and technologies to detect and prevent cyber threats.
* Conduct regular security assessments and vulnerability analyses to identify weaknesses in systems and networks.
* Collaborate with cross-functional teams to implement security controls and best practices.
* Develop and maintain security documentation, including incident response plans and security policies.
* Stay up-to-date with the latest cybersecurity threats, trends, and technologies.
* Provide guidance and support to other IT teams on security-related matters.
* Participate in incident response activities, including containment, eradication, and recovery.

# ABOUT YOU IN THE ROLE

As a staff member of Uniting you will celebrate diversity and welcome all people regardless of lifestyle choices, ethnicity, faith, sexual orientation or gender identity.

**Your directorate:**  Finance, IT and Property

**You’ll report to:** Security operations manager

# YOUR KEY CAPABILITIES

**Individual leadership**

* **Improving performance -** Works with others and offers suggestions to find ways of doing the job more effectively.
* **Owning the job -** Takes ownership for all responsibilities and honours commitments within their own role and strives to achieve goals with a "can-do" attitude to levels of excellence.
* **Perseverance** - Remains committed to completing the job in the face of obstacles and barriers.
* **Timeliness of work -** Sets achievable timeframes and works to complete projects, tasks and duties on time.

**Business Acumen**

* **Organisational Operation -** Displays awareness of Uniting’s business objectives and understands how personal objectives relate to those objectives.
* **Organisational Objectives -** Has broad awareness of Uniting’s vision and values and how they apply to issues in the team.
* **Develops and Grows the Business –** Understands team and organisational goals and works collaboratively with Team Members to achieve organisational goals**.**
* **Makes Sound Decisions –** Analyses problems, seeks input from relevant people and then takes appropriate action to implement the most effective solution in a timely manner.

# QUALIFICATIONS & EXPERIENCE

**Qualifications:**

Bachelor qualification in a relevant field or equivalent experience.

**Experience:**

Typically this role will require 10 or more years’ experience in your field of expertise. You will have excellent written and verbal communication skills, be organized, systematic, thorough, accurate and disciplined. You will be continuing to develop in your area of expertise and be expected to provide innovative ideas to solve problems in your discipline. It is expected that you will be developing good skills at navigating a complex organisation, forging relationships, and managing through influence rather than direct authority as required.

* Proven experience working in a cybersecurity operations role.
* Strong understanding of cybersecurity principles and best practices.
* Experience with security tools such as SIEM, IDS/IPS, vulnerability management, and endpoint detection and response (EDR) solutions.
* Strong understanding of Microsoft products, both on premise (Windows, SCCM, AD and WSUS), and cloud (Office 365, Defender suite and Azure)
* Knowledge of network protocols, architecture, and security technologies.
* Familiarity with industry standards and regulations (e.g., NIST and ISO27001).
* Excellent problem-solving and analytical skills.
* Strong communication and collaboration skills.

**Even better:**

* Relevant certifications such as CISSP, CISM, or CompTIA Security+ are a plus.
* Experience with Secure Service Edge(SSE) products and services.

|  |  |  |  |
| --- | --- | --- | --- |
| **Employee Name:** | Insert employee name | **Manager’s Name:**  **Title** | Insert manager’s name  Insert manager’s title |
| **Date:** | Insert date | **Date:** | Insert date |
| **Signature:** |  | **Signature:** |  |