About Webjet Limited

We are a digital travel business spanning both global consumer markets (through B2C) and wholesale markets (through B2B). Our B2C travel business operates the leading OTA consumer brand of Webjet as well as various market-leading brands in complementary travel products within the Online Republic business. Established in 1998, Webjet is the leading online travel agency (OTA) in Australia and New Zealand, leading the way in online travel tools and technology. Our focus has always been to offer the greatest convenience and choice by enabling customers to compare, combine and book the best domestic and international travel flight deals, hotel accommodation, holiday package deals, travel insurance, and car hire worldwide. We have a truly global footprint and a diverse technology stack, so there is a range of security risks to manage to ensure the group is protected from an ever-changing threat landscape.

Role: Security Specialist

Reporting to: Senior Security Specialist

Team: IT - Security

Location: Open

Level: Entry/Mid-level

Job Description:

We are looking for a Security Specialist to join our growing Group Security team here at Webjet Limited. This is a wide-ranging role that covers a set of key responsibilities but may also require you to be involved in other tasks - from ensuring our security tools and technologies are appropriately configured to assisting in investigating and resolving security alerts, to running pilot tests for our security initiatives, and other assigned duties. If you have prior security experience and are excited by the idea of taking on new challenges in different areas of our business, then we want to talk to you.

Key responsibilities:

- Champion our monitoring and measurement program through regular audits and reporting.
- Monitor and review security incidents to discover trends for each of our business units.
- Support with audit checks against policies and standards.
- Contribute to the development and maintenance of our security awareness program.
- Support our regular security updates for the business.
- Monitor and escalate incidents and investigations to appropriate teams and ensure completion.
- Support the review of new security initiatives and the implementation of proof of concepts.
- Work with security engineers and other key stakeholders to ensure the successful implementation of security projects.
- Domain monitoring for typosquatting.

To be successful in the role, you will:

- Be familiar with cloud environments such as Azure, M365, AWS.
- Be familiar with or have knowledge of security tools and technologies (e.g. SIEM, EDR, Anti-malware, email security)

- Have the ability to talk to Stakeholders in a non “techie” way to articulate the risk.
- Research and recommend new security technologies for new or existing problems and be able to justify and communicate design decisions.
- Be aware of the Threat Landscape, current trends of Threat Actors and current attacks.
- Be familiar with Incident response planning and contribute to the Incident response plan and team.
- Have strong communication skills and be comfortable providing feedback and updates to key stakeholders within the business.
- Enjoy finding solutions to problems and working effectively with others to reach an agreement.
- Have a professional approach to work, integrity, and respect for policies.
- Be driven and eager to continuously learn and improve.