POSITION DESCRIPTION

Position Title: Senior Information Security Analyst
Organisation Unit: Information Technology Services
Position Number: 3036458
Type of Employment: Fixed term, 12 months
Classification: Hew Level 6/7 + 15% industry loading

THE UNIVERSITY OF QUEENSLAND

The University of Queensland (UQ) contributes positively to society by engaging in the creation, preservation, transfer and application of knowledge. UQ helps shape the future by bringing together and developing leaders in their fields to inspire the next generation and to advance ideas that benefit the world. UQ strives for the personal and professional success of its students, staff and alumni. For more than a century, we have educated and worked with outstanding people to deliver knowledge leadership for a better world.

UQ ranks in the world’s top universities, as measured by several key independent ranking, including the CWTS Leiden Ranking (32), the Performance Ranking of Scientific Papers for World Universities (43), the US News Best Global Universities Rankings (42), QS World University Rankings (48), Academic Ranking of World Universities (55), and the Times Higher Education World University Rankings (69). Excluding the award component, UQ is now ranked 45th in the world in the ARWU, and is one of the only two Australian universities to be included in the global top 50.

UQ has an outstanding reputation for the quality of its teachers, its educational programs and employment outcomes for its students. Our students remain at the heart of what we do. The UQ experience – the UQ Advantage – is distinguished by a research enriched curriculum, international collaborations, industry engagement and opportunities that nurture and develop future leaders. UQ has a strong focus on teaching excellence, winning more national teaching excellence awards than any other in the country and attracting the majority of Queensland’s highest academic achievers, as well as top interstate and overseas students.

UQ is one of Australia’s Group of Eight, a charter member of edX and a founding member of Universitas 21, an international consortium of leading research-intensive universities.

Our 52,000-plus strong student community includes more than 16,400 postgraduate scholars and more than 15,400 international students from 135 countries, adding to its proud 250,000-plus alumni. The University has more than 6,600 academic and professional staff (full-time equivalent) and a $1.75 billion annual operating budget. Its major campuses are at St Lucia, Gatton and Herston, in addition to teaching and research sites around Queensland and Brisbane city. The University has six Faculties and four University-level Institutes. The Institutes, funded by government and industry grants, philanthropy and commercialisation activities, have built scale and focus in research areas in neuroscience, biomolecular and
biomedical sciences, sustainable minerals, bioengineering and nanotechnology, as well as social science research.

UQ has an outstanding track-record in commercialisation of our innovation with major technologies employed across the globe and integral to gross product sales of $11 billion+ (see http://uniquest.com.au/our-track-record).

UQ has a rapidly growing record of attracting philanthropic support for its activities and this will be a strategic focus going forward.

Organisational Environment

The Division of Information Technology Services (ITS) at The University of Queensland provides an information environment that supports the teaching, learning, research and engagement objectives of the University and contributes positively to the student experience and the University’s reputation, in line with our values of excellence, creativity, honesty, accountability, supportive, respect and diversity. It delivers network, systems and IT infrastructure support to the University, and application development. Also located within ITS is the internationally recognised network security group, AusCERT, which provides Internet security services throughout Australia and New Zealand. ITS manages core networks not only for the whole of The University of Queensland but also works with other Queensland universities to manage access to the national university network (AARNet). ITS also operates research computing infrastructure and hosts many of the University’s largest servers.

For further information visit our website www.its.uq.edu.au

Information for Prospective Staff

Information about life at UQ including staff benefits, relocation and UQ campuses is available at - http://www.uq.edu.au/current-staff/working-at-uq

DUTY STATEMENT

Primary Purpose of Position

This position is responsible for technical and operational support within the Security Operations Centre at ITS.

Duties

Duties and responsibilities include, but are not limited to:

<table>
<thead>
<tr>
<th>HEW level 6</th>
<th>HEW level 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Incident response and other related provision of services to members.</td>
<td>• Incident response and other related provision of services to members.</td>
</tr>
<tr>
<td>• Consult on the technical aspects of information technology to UQ staff.</td>
<td>• Consult on the technical aspects of information technology and provide high level support for services delivered to UQ staff.</td>
</tr>
<tr>
<td>• Vulnerability analysis.</td>
<td>• Vulnerability analysis.</td>
</tr>
<tr>
<td>• Development and evaluation of</td>
<td>• Provide advice regarding the</td>
</tr>
<tr>
<td>security tools and techniques.</td>
<td>security, design, implementation, installation and maintenance of the SOC’s information technology systems and infrastructure. Duties may include evaluation of open source security tools and techniques.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Carry out individual work or participate in group-based projects assignments as required, with some freedom to propose own topics of interest where relevant to the SOC’s goals.</td>
<td>• Undertake design, development and project management of information technology projects, including ICT service development, and evaluation.</td>
</tr>
<tr>
<td>• Maintain a current knowledge of networking, computer and security standards, state-of-the-art developments and products. Maintain links with authorities, vendors, and relevant personnel within international peer groups, the Internet and the global university and research community.</td>
<td>• Maintain a current knowledge of networking, computer and security standards, state-of-the-art developments and products. Maintain links with authorities, vendors, and relevant personnel within international peer groups, the Internet and the global university and research community.</td>
</tr>
<tr>
<td>• Contribute to the activities of other groups within ITS as directed, under the supervision of the relevant manager.</td>
<td>• Contribute to content development and delivery of services within ITS.</td>
</tr>
<tr>
<td>• Supply information and advice for the production of operational, budgeting and planning reports as required.</td>
<td>• Assist the team leader and unit manager in matters of budget preparation, management of the unit, planning and adherence to ICT procurement guidelines.</td>
</tr>
<tr>
<td>• Assist team members in developing their skill set through mentoring, providing senior support and expertise to other staff on information security and technology topics, as appropriate.</td>
<td>• Travel (intrastate, interstate and/or overseas) on ITS business as required.</td>
</tr>
<tr>
<td>• Travel (intrastate, interstate and/or overseas) on ITS business as required.</td>
<td>• Travel (intrastate, interstate and/or overseas) on ITS business as required.</td>
</tr>
</tbody>
</table>
Other
Ensure you are aware of and comply with legislation and University policy relevant to the duties undertaken, including but not exclusive to:

- the University’s Code of Conduct
- requirements of the Queensland occupational health and safety (OH&S) legislation and related OH&S responsibilities and procedures developed by the University or Institute/School
- the adoption of sustainable practices in all work activities and compliance with associated legislation and related University sustainability responsibilities and procedures
- requirements of the Education Services for Overseas Students Act 2000, the National Code 2007 and associated legislation, and related responsibilities and procedures developed by the University

Organisational Relationships
The position reports to the Security Operations Centre Team Leader. At HEW 7, the position may be required to direct other professional or technical staff on work relating to specific tasks or projects.

SELECTION CRITERIA

Please indicate in your selection criteria response for which HEW level you are applying:

HEW 6

Essential
- EITHER:
  - Bachelor’s Degree, or equivalent, ideally with significant information technology component; Industry certification in one or more of the following areas: computer security, training, systems administration, programming or networking
  - At least two years’ experience in the IT industry, with at least one year of experience relevant to IT security. Some variation may be considered for applicants with a strong match to the other selection criteria. A demonstrable interest in information security is expected.
- Knowledge of:

HEW 7

- EITHER:
  - Bachelor’s Degree, or equivalent, ideally with significant information technology component; Industry certification in one or more of the following areas: computer security, training, systems administration, programming or networking
  - Formal training in one or more of the following areas:
    - IT security related discipline
    - SANS certification in an IT security related area
    - CSSLP, CISSP, or CISM certification
  - At least four years’ experience in the IT industry, with at least two years of
• Shell scripting or equivalent system administration toolset.
• The architecture and services of the TCP/IP protocol suite;
• Linux operating systems (preferably RHEL and/or Debian).

Strong communication and interpersonal skills, with a demonstrable ability to work effectively with others to achieve positive outcomes.

Australian Citizen eligible for a national security clearance. (The successful applicant will be required to submit to background checks).

Desirable
• Formal training in one or more of the following areas:
  • An IT security related discipline.
  • CSSLP (https://www.isc2.org/csslp/default.aspx) or CISSP https://www.isc2.org/cissp/default.aspx
• Experience in one or more of the following:
  • Computer/ network forensics.
  • IT security incident resolution.
  • A CSIRT team, particularly a coordination centre area.
  • Consulting or customer service experience in information technology, preferably in information security.
  • Windows operating systems (including Active Directory and administration).
• Knowledge and/or experience in one or more of the following areas:
  • Networking/firewalls.
  • Programming and/or the ability to read/troubleshoot shell script, Python, object oriented Perl

Experience relevant to IT security including IT security incident resolution and/or a CSIRT team. Experience in computer/network forensics, or consulting in information security will be highly regarded. Some variation may be considered for applicants with a strong match to the other selection criteria. A demonstrable interest in information security is expected.

• Experience applying information security management standards in a workplace, as well as ability to produce comprehensive policy and procedure documents, business proposals, content for publication and other forms of written communications in a high quality and accurate manner.

• A willingness and ability to work with other staff including in a mentorship and support role.

• Knowledge and experience in at least four of the following:
  • Shell scripting or equivalent system administration toolset.
  • The architecture and services of the TCP/IP protocol suite;
  • Linux operating systems (preferably RHEL and/or Debian).
  • Networking/firewalls
  • Big data analysis systems such as ELK and/or Splunk
  • Programming and/or the ability to read/troubleshoot shell script, Python, object oriented Perl GTK, Java or PHP

Strong communication and interpersonal skills, with a demonstrable ability to work effectively with others to achieve positive outcomes.

Desirable
• Experience in the supervision of
GTK, Java or PHP.
- Big data analysis systems such as ELK and/or Splunk

staff.
- Experience in program management and/or project leadership for small projects

The University of Queensland values diversity and inclusion and actively encourages applications from those who bring diversity to the University. Please refer to the University’s Diversity and Inclusion webpage (http://www.uq.edu.au/equity) for further information and points of contact if you require additional support.

This role is a full-time position; however flexible working arrangements may be negotiated.

Accessibility requirements and/or adjustments can be directed to recruitment@uq.edu.au