

Work Placement Position CSU Research -Insider Threat Detection

Charles Sturt University offers a unique work placement opportunity for students to participate in a cutting-edge research project on insider threat detection. This project aims to develop and implement advanced techniques for identifying and mitigating insider threats within organisational networks. Participants will gain hands-on experience with state-of-the-art tools and methodologies in cybersecurity and data science.

Subject:	Session 2 (60): ITC599 (140 Hours)
Specialisation:	Cyber Security, Data Science, Software Development, Networking and AI
Location:	Port Macquarie
Availability:	1 position

Further information:

Key Responsibilities:

- Assist in the development and deployment of insider threat detection models.
- Conduct data analysis and curate datasets relevant to insider threat scenarios.
- Collaborate with the research team to refine methodologies and improve detection accuracy.
- Participate in regular project meetings and contribute to preparing research reports and presentations.
- Implement and test security measures within simulated environments using on-premises systems and IoT devices.

Learning Opportunities:

- Gain practical experience in cybersecurity, data science and governance.
- Work with advanced security systems and IoT devices.
- Develop skills in data analysis, threat modelling, and security testing.
- Enhance understanding of the MITRE ATT&CK framework for threat analysis.
- Collaborate with experienced researchers and industry professionals.

Requirements:

- Enrolment in ITC599 at Charles Sturt University.
 - Strong interest in cybersecurity and data science.
 - Basic understanding of network security principles and data analysis techniques.
 - Ability to work both independently and as part of a team.
-



Position: Cybersecurity CSU Student Research Assistant

- Position: Cybersecurity CSU Student Research Assistant
- Project: Insider Threat
- Location: Port Macquarie Campus
Supervisor: Research Assistant

Role Overview: We seek a motivated Cybersecurity student to join our Insider Threat Project team. The successful candidate will assist in setting up and managing systems and network devices, monitoring network traffic, conducting security assessments, and collaborating with the data science team to enhance threat detection mechanisms.

Key Responsibilities:

- Assist in setting up and configuring network devices, including Cisco 1941 Series Wireless Router and Cisco 3560 Switch.
- Monitor network traffic and analyse logs for potential insider threats using EDR tools.
- Conduct vulnerability assessments with OpenVAS and implement DLP strategies to protect sensitive data.
- Collaborate with the data science team to implement threat detection models.
- Document and report on security findings, providing actionable recommendations.
- Stay updated on the latest cybersecurity trends and tools relevant to insider threats.
- Contribute to literature reviews and assist in paper writing using Overleaf.
- Report to the Research Assistant and support their tasks as needed.
- Participate in project administration using Notion and facilitate collaboration through Google Chat/Workspace.
- Manage and monitor servers configured for AD, DNS, DHCP, DLP, Microsoft Exchange, SIEM/SOAR, and Behavioural Analytics/UEBA.

Position:

Qualifications:

- Currently enrolled in a Cybersecurity program.
- Understanding of network protocols, firewall configurations, and intrusion detection systems.
- Experience with cybersecurity tools such as Wireshark, Metasploit, Splunk, EDR, DLP, and OpenVAS.
- Basic knowledge of scripting languages (e.g., Python, Bash) for automation tasks.
- Strong analytical and problem-solving skills.
- Ability to work independently and as part of a team.
- Good written and verbal communication skills.

Email cover letter, résumé and academic transcript to:

How to apply:

- Dr. Sabih Rehman (sarehman@csu.edu.au); and
- Supervisor: Louis Hourany, Lecturer, School of Computing, Mathematics and Engineering. Email: lhourany@csu.edu.au

Start and end date: 01/08/2024 – 25/10/2024
