CLP Internship Programme 2024

Project Outline: Sandwich – Information Technology

Project Code	IT_SAND_01	
Project Details	**Internship Period**	June 2024 to May 2025
	Preferred Disciplines	**First Preference:** • Information Technology related • Computer Science related **Second Preference:** • Energy related • Engineering related
	Project Name	Customer Experience Transformation Program
	Business Objective(s)	• Provide personalised customer experience, offering convenience, choices and control to our customers • Deepen our understanding and relationships with 360 customer profile & capability • Develop personalized products & services based on customers' needs
	Project Description	This role aims to support the program in the below areas: • Software testing • Testing coordination • Test data preparation • Requirement collection • Documentations
	Required Skills	• Analytical and Critical Thinking • Problem solving • Software testing • Communication

CLP Internship Programme 2024

Project Outline: Sandwich – Information Technology

Project Code	IT_SAND_02	
Project Details	**Internship Period**	June 2024 to May 2025
	Preferred Disciplines	**First Preference:** • Cyber Security or Information Technology related **Second Preference:** • Computer Science related
	Project Name	Cyber Security Strengthening Project
	Business Objective(s)	At CLP, our business commitment is to ensure continuous supply of electricity to public. As such, it is critical for us to deploy the appropriate cyber security technologies and design proper security architecture to enhance overall cyber security protection for the enterprise.
	Project Description	Project to strengthen CLP cyber security protection portfolio by adopting leading edge security solution. Project involve researching latest technology trend & solution offering, understanding latest security architecture in enterprise environment, hands on experience in security project management.
	Required Skills	N/A

CLP Internship Programme 2024

Project Outline: Sandwich – Information Technology

<table>
<tr><td>Project Code</td><td colspan="2">IT_SAND_03</td></tr>
<tr><td rowspan="4">Project Details</td><td>Internship Period</td><td>June 2024 to May 2025</td></tr>
<tr><td>Preferred Disciplines</td><td>First Preference:
Cyber / Information Security
Second Preference:
Computer Science
Electrical Engineering
Mechanical Engineering</td></tr>
<tr><td>Project Name</td><td>Operational Technology / Industrial Control Systems - Security Strengthening</td></tr>
<tr><td>Business Objective(s)</td><td>At CLP, our business commitment is to ensure continuous supply of electricity to Hong Kong. As such, it is critical for us to protect our operational technology (OT) systems, which is control the operations for the generating, transmitting and distributing power. For recent years, many cases of power plants around the world had been attacked by different types of Cyber threats which had caused, not only money lost to the company but also affecting the normal life on many people.

As OT/ICS technology plays an important role for our plant's operation and control, it is important for CLP to protect our assets by strengthen our knowledge of Cyber Security in this field in order to enhance, prevent and avoid any potential risks from Cyber threats.</td></tr>
<tr><td>Project Description</td><td>OT/ICS Cyber Security is becoming one of the hottest topics in the industrial operations sector due to many recent Cyber-attack as utility companies are usually being targeted. Many companies are looking for ways / methodologies to enhance and prevent systems that are used to monitor and control industrial processes against different types of Cyber Threats which may cause substantial amount of damage lost to company.

3 key objectives of OT/ICS Cyber Security which includes:
Identify and Detect - Discover and eliminate vulnerabilities, mis-configurations, unsecured connections and unauthorized remote access by enforcing access policies and recording sessions.
Protect - System monitoring and detect malicious activity and high-risk changes and prevent any future attacks.
Respond - Able to resolve any new arises issues in fast pace to minimize any further damages and risks.
During this internship, the intern will have the opportunity to be inspired, explore and learn the following:
OT / ICS Framework - basic principles of OT/ICS frameworks, Learn on ways of cyber security threats attacks on OT/ICS systems, risk management, security assessment methodologies and many more.</td></tr>
</table>

		• Security Monitoring - Learn about data / system monitoring processes, data assessment and analysis. • Project Management - Activity planning and tracking, issue management process and cross team integration.
	Required Skills	Candidates with knowledge on Computer, Electrical or Mechanical Engineering background.

CLP Internship Programme 2024

Project Outline: Sandwich – Information Technology

Project Code	IT_SAND_04	
Project Details	**Internship Period**	June 2024 to May 2025
	Preferred Disciplines	**First Preference:** • Information Security/Computer Science **Second Preference:** • Engineering
	Project Name	ThreatBusters: Empowering CLP Digital Defense
	Business Objective(s)	Are you ready to join the elite ranks of cybersecurity professionals and become a Threat Buster? We are seeking passionate individuals to join our team, dedicated to protecting organizations from the relentless onslaught of digital adversaries. Just like the Ghostbusters movie, Cyber Operations team are always ready to hunt various adversaries and protect ourselves with the latest and exciting technology.
	Project Description	As an intern in Cyber Operations Team and being a part of an elite Cyber Threat Buster team, the intern will assist to: • Detect Threats - sense malicious activities with their specialized equipment. You will employ advanced threat intelligence platforms, security monitoring tools, and data analysis techniques to identify and analyse potential cyber threats. • Bust Threats - capture and contain the evil. You will develop and implement robust security controls, conduct vulnerability assessments, and respond to security incidents swiftly and decisively. • Involve in Continuous Learning - Stay at the forefront of the ever-evolving cybersecurity landscape by actively researching and keeping up with the latest threat vectors, attack techniques, and emerging technologies. You will continuously enhance our organizations knowledge while also growing as a cybersecurity professional through different in-house / external training. • Collaborate with fellow Threat Busters - Work closely with our team of cybersecurity professionals, sharing your expertise and findings to enhance our organization's overall security posture. Collaborate on incident response efforts, participate in threat intelligence sharing initiatives, and contribute to the development of cybersecurity policies and procedures.
	Required Skills	At CLP, our business commitment is to ensure continuous supply of required electricity to public. As such, it is critical to hold a strong cyber defence, and handle cyber incident professionally. Technology related: • Proficient in Microsoft Office

		• Basic understanding of cyber security Non-technology related: • Fast learner with ''can-do" attitude • Proficient in English. Chinese is optional but preferred • Ability to communicate and document technical details in a concise, understandable manner