

Intern Requirement

No. of students required	1 or 2
Preferred Discipline	<ul style="list-style-type: none">IT Security
Prerequisites/ Skills Required	<ul style="list-style-type: none">Strong interest in IT securityBasic knowledge on system loggingStrong analytical skills

Project Details

Title	Security Log Analysis
Overview/Background	To enhance the security monitoring capability of Enterprise Security Information and Event Management (SIEM solution) to detect each phase of inside and outside attacks. This includes reconnaissance, scanning, exploitation and password attacks
Objectives/Scope/ Deliverables	<p>The intern would be required to generate and analyse event logs of each phase of inside and outside attacks from Windows and Linux-based servers within the SIEM Solution. He/she would also need to configure/write rules to detect each phase of inside and outside attacks.</p> <p>For the insider attack, the intern would be further required to create a dashboard to monitor all events of the administrator's activities (e.g. tracking of login and logout sessions).</p> <p>User guides/training materials on SIEM solution will be provided for guidance.</p>
Project Duration	2-4 months