

## JOB DESCRIPTION

<b>Job title:</b>	DevSecOps Engineer.
<b>Department:</b>	IT Infrastructure.
<b>Location:</b>	Beaconsfield.
<b>Working hours:</b>	9.30am to 6pm Monday to Friday.
<b>Reporting to:</b>	Head of IT.
<b>Direct reports:</b>	N/A.
<b>Main purpose(s) of job:</b>	<p>The DevSecOps Engineer will play a key leadership role in our team as we automate our multiple development pipelines that flow into Docker and Kubernetes on-premise infrastructure.</p> <p>This position will be responsible for helping to implement a Secure Software Development Lifecycle and will need to understand software development (Dev), but enjoy all the things necessary for improving deploying, monitoring, and operating production services (Ops) whilst ensuring that secure development practices are followed (Sec).</p> <p>This position will take on challenging and exciting projects as well as learn and teach others in the team.</p>
<b>Main tasks and duties:</b>	<p><b>Essential:</b></p> <ul style="list-style-type: none"> <li>• Provide thought and subject matter leadership in DevSecOps.</li> <li>• Infrastructure, advising development managers in structuring and sizing their plans, and raise red flags on faulty models or assumptions to prevent misguided implementation.</li> <li>• Ability to automate release deployments across all stacks.</li> <li>• Strong experience with release pipelines, including blue/green deployments.</li> <li>• Develop effective tooling to accelerate deploy and release management.</li> <li>• Optimize deployments for scalability, efficiency and security.</li> <li>• Develop infrastructure standards and best practices with a proclivity towards automation.</li> <li>• Work closely with the Head of IT, C.I.S.O. and Directors to develop, implement and coordinate systems and procedures.</li> <li>• Maintain the configuration, identifying dependencies, potential conflicts, document the process and track a schedule of the deployments for each environment.</li> <li>• Manage the configuration and up-time of all environments and micro-services.</li> <li>• Hands on experience using the Kubernetes platform.</li> <li>• Design, implement, and maintain highly available and secure infrastructures.</li> <li>• Build and implement monitoring and logging services.</li> <li>• Carry out threat modelling and implement secure coding practices and ensure security standards are met using automated testing on build pipelines.</li> <li>• Design and implement a DR / remote service strategy.</li> <li>• Work with the Infrastructure team for the implementation of ITIL concepts and tools.</li> <li>• Remain current on broad technology infrastructure changes in the industry and how</li> </ul>

	<p>they may assist with driving down costs or increasing competitive advantage.</p> <p><b>Desirable:</b></p> <ul style="list-style-type: none"> <li>• Continually manage all cloud assets to ensure right-sized and minimize sprawl.</li> <li>• Experience of Gitlab</li> <li>• Experience of AWS Cloud</li> <li>• Relevant technical certifications</li> </ul> <p>This list is not exhaustive, and other duties may be required commensurate with this position as roles evolve.</p>
<p><b>Person Specification:</b></p>	<ul style="list-style-type: none"> <li>• Proven working experience or relevant experience</li> <li>• Excellent knowledge of technical management, information analysis and of computer hardware/software systems.</li> <li>• Experience with the systems detailed above.</li> <li>• Hands-on experience with computer networks, network administration and network installation</li> <li>• Ability to support/manage personnel – experience of managing teams / supervisory responsibilities.</li> <li>• Relevant professional qualifications</li> <li>• ITIL experience.</li> <li>• Team focused; motivated; innovative; diligent.</li> <li>• Enjoys working in a fast-paced and time pressured environment.</li> <li>• Exceptional organisational skills.</li> <li>• Pays strong attention to detail.</li> <li>• Excellent time management and communication skills.</li> </ul>