

JOB DESCRIPTION

Job Title	Product Security Engineer
Reports To	Product Security Lead
Responsible For	N/A

Purpose

As a Product Security Engineer you will work within a small AppSec team to help Blackford's Product Development division deliver secure products and solutions and continually champion the importance of cybersecurity.

Responsibilities

- Help ensure software products created, distributed and deployed by Blackford Analysis are meeting security requirements
- Maintain, refine and continually improve Blackford's processes for incorporating security into all aspects of the software development lifecycle
- Help with management of security vulnerabilities: triage, risk assessment and patching
- Work with the product and development teams to define security requirements
- Work with product development, IT and Devops teams to introduce, maintain and improve the use of automated security scanning / testing tools
- Help preparing for manual penetration tests of Blackford products by external security contractors
- Help the development teams to design and implement security features
- Facilitate threat modelling sessions with the development teams
- Raise security awareness in the product development team
- Assist Sales and Operations teams in communicating security aspects of Blackford products to customers
- Assist Operations team in deploying Blackford products securely
- Assist in determining adequate response to security incidents
- Act as deputy for Product Security Lead
- Comply with information security requirements as detailed in the Information Security manual

Competencies

Specialist job related knowledge and/or qualifications

Essential

- Strong cybersecurity knowledge, especially around secure coding practises, web applications, authentication and networking
- Understanding of software development practises

Desirable

- Software development experience
- DevSecOps: experience with security tooling and automation

	<ul style="list-style-type: none">• Technologies: .NET, Javascript, SQL, Docker, Google Cloud Platform, CI/CD (Jenkins), Kubernetes, OAuth2, OIDC• Medical IT (PACS / RIS / DICOM / HL7) domain knowledge• Knowledge of relevant security and privacy standards and regulations: ISO 27001, HIPAA, GDPR, SOC2, HITRUST• Experience with Threat Modelling
Job related skills / behaviour	<ul style="list-style-type: none">• Strong desire to help protect health systems and their patients by delivering secure products• Willingness to continually learn and stay informed about the latest security news and trends• Strong communication skills• Ability to work alone and in a team• Excellent problem solving skills• Strong interpersonal and relationship-building skills with external stakeholders and internal team.