Application Security Engineer

Department: Security

Reports to: Head of Security

Direct reports: No direct reports

Competency level: Intermediate-Senior

Purpose of Role Summary

As an Application Security Engineer you will be responsible for supporting the security of Catalyst's software applications throughout the development lifecycle. You will work closely with development teams, the Head of Security, Senior Security Specialist and other stakeholders to integrate security into all stages of application design, development, and deployment.

Your role will involve open-source research and development of security applications, conducting security assessments, performing threat modelling, driving secure coding practices, and supporting compliance with the organisation's information security policies and industry standards. You will help reduce the organisation's application risk profile and foster a culture of security awareness across engineering teams.

Application Security Engineering

Jobholder is accountable for:

- Conducting security reviews, code audits, and vulnerability assessments of internal applications.
- Performing threat modelling to identify potential attack vectors and design appropriate mitigations.
- Integrating static application security testing (SAST), dynamic application security testing (DAST), and software composition analysis (SCA) tools into CI/CD pipelines.
- Collaborating with development teams to remediate identified vulnerabilities in a timely manner.
- Developing and maintaining secure coding guidelines, security playbooks, and standard operating procedures.
- Monitoring and providing statistics for application security posture and tracking the status of vulnerabilities through to resolution.
- Supporting security incidents and assisting with root cause analysis.
- Ensuring a preventive maintenance plan for application security tooling is in place and overseeing its implementation.
- Evaluating, recommending, and implementing new security tools and technologies, including documentation, to strengthen security.

Jobholder is successful when:

- Evaluating, recommending, and implementing new security tools and technologies, including documentation, to strengthen security.Security is embedded as a standard part of the software development lifecycle (SDLC).
- Vulnerability findings are reported on, responded to, and resolved in a timely and professional manner.

- The Head of Security and other stakeholders are fully informed on application risk posture on a regular and ongoing basis.
- Work is completed by agreed deadlines.
- Jobholder takes ownership of security outcomes and works effectively with development, operations, and other teams to meet stakeholder expectations.
- High-quality security documentation, including threat models and assessment reports, is produced, as required.

Communication and Stakeholder Engagement

Jobholder is accountable for:

- Maintaining professional communications with developers, project managers, clients, and other Catalyst employees.
- Supporting management and team members with security-related recommendations, associated document production, and incident support, as required.
- Providing security guidance and training to development teams on secure coding practices and common vulnerabilities (e.g., OWASP Top Ten).
- Engaging with stakeholders to communicate application security posture and advise on risk mitigation strategies.
- Attending and contributing to design reviews, project planning, and architecture discussions to represent the security perspective.

Jobholder is successful when:

- Confidentiality is maintained at all times.
- Both verbal and written communications are clear, concise, and accurate.
- Jobholder models appropriate behaviour that represents Catalyst and Catalyst's values in all external engagements.
- Both clients and Catalyst employees are communicated with in a fair, honest, and open way.

Continual Learning and Development

Jobholder is accountable for:

- Staying current with emerging application security threats, vulnerabilities, tools, and frameworks.
- Participating in relevant security training, conferences, and certification programmes.
- Exploring opportunities to add value through automation, tooling improvements, and process enhancements.
- Setting goals and targets for career development in application security.
- Taking on new and variable tasks as the role develops, as directed by the Head of Security.
- Entering timesheets in WRMS in a timely manner.

Jobholder is successful when:

- New and relevant knowledge or experience is gained via training or work experience, and is actively applied in day-to-day work.
- Goals and targets are met, both short and long term.

Skills and Requirements

- Proficiency in one or more programming languages commonly used in web development (e.g., Python, Java, JavaScript, C#, Ruby).
- Strong knowledge of application security testing tools such as Burp Suite, OWASP ZAP, SonarQube, Semgrep, or Snyk. Experience focused on opensource tools is highly-desirable.
- Experience with secure SDLC practices and integrating security into CI/CD pipelines (DevSecOps).
- Familiarity with security frameworks and standards such as OWASP Top Ten, NIST, CWE/SANS Top 25, and ISO 27001.
- Understanding of web application architecture, RESTful APIs, microservices, and cloud-native environments.
- Experience with threat modelling methodologies (e.g., STRIDE, DREAD, PASTA).
- Knowledge of common vulnerability classes including injection attacks, XSS, CSRF, authentication/authorisation flaws, and insecure deserialisation.
- Experience with incident response processes, particularly for application-layer security events. Specific experience with incident malware reverse engineering and digital forensics is highly-desirable.
- Relevant certifications are desirable (e.g., CSSLP, CEH, OSCP, GWAPT, or equivalent).

Competencies

Clear and effective communication style, with the ability to articulate complex security concepts to both technical and non-technical audiences.

Strong analytical and problem-solving skills.

The ability to build rapport with developers and stakeholders, fostering a relationship of mutual trust and collaboration.

Critical thinking and attention to detail when evaluating application security.

Calm and collected under pressure, particularly during security incidents.

A commitment to continuous learning and adaptability in a rapidly evolving threat landscape.