GALAH CYBER

Foundations of Application Security with Cole Cornford

Practical training for secure-by-design software development

From $1,800 per person (ex. GST)

Student pricing available – see terms below

Overview

Build resilient, secure-by-design software with confidence. This two-day, in-person course equips software and security engineers with the foundational skills to interrogate source code, identify vulnerabilities, and embed DevSecOps practices that scale. Delivered by Cole Cornford, one of Australia's most recognised leaders in application security, this program blends hands-on exercises, case studies, and group discussions that elevate your technical capability and operational security maturity.

Course Overview

This course integrates technical exercises with program management skills to help you:

- Build security from the ground up.
- Confidently assess and remediate vulnerabilities in real-world codebases.
- Deploy DevSecOps tools and workflows that align with your technology stack.
- Communicate security ROI and embed secure practices in engineering culture.

Graduates become part of The Flock, an alumni network of leading product security professionals across the Asia Pacific region, providing ongoing connections, shared learnings, and a community that continues to support your growth long after the course.

Target Audience

This is an advanced technical course designed for:

- **Mid-level software engineers and security engineers.**
- Technical staff in **DevOps, Cloud, Infrastructure, Data, or IT roles.**
- **Technical managers** seeking to introduce or uplift application security capabilities.
- **Startup and scale-up teams** embedding security without dedicated AppSec hires.

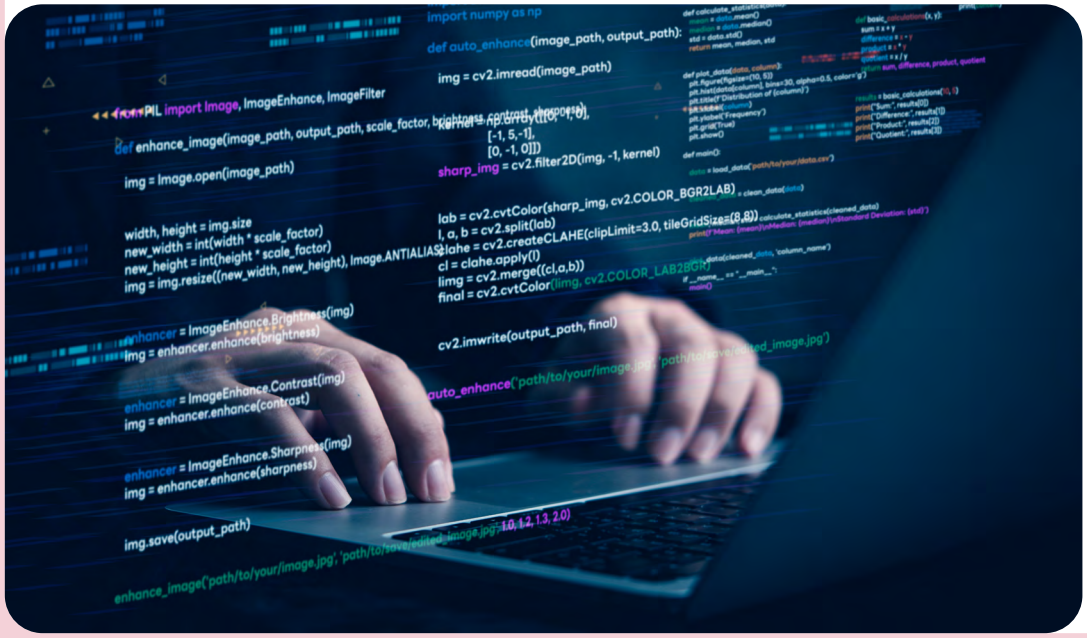
Not recommended for non-technical or executive-only staff.

Prerequisites

Participants are expected to have:

- Practical experience in software development and strong computer science fundamentals.
- Ability to read and run unfamiliar codebases, use package managers and containers, and apply git flow.
- Capability to run DevSecOps tools (Checkov, Snyk, SemGrep) locally.
- A **personal computer** (not a work device) with **Docker** or **Python3** installed and reliable network connectivity.

Students without a strong engineering background may struggle to follow advanced concepts and exercises.



Learning Objectives

- Explain the business case and objectives of an application security program.
- Apply secure coding techniques to improve code quality and reliability.
- Interrogate source code repositories for vulnerabilities.
- Design cost-appropriate security controls.
- Evaluate and implement DevSecOps capabilities in workflows.
- Architect applications with inherent security mechanisms.
- Perform threat modelling using frameworks such as **4Q's** and **STRIDE**.
- Build vulnerability management processes and developer training programs.

Course Outline

Introduction

- About the course and trainer
- Professional and personal drivers
- About Galah Cyber and Birdhouse teaching aid
- Course schedule, resources, feedback

Foundations of Application Security

- What Application Security is and why it's critical
- Evolution: Dev → DevOps → DevSecOps
- Reducing workload pressure and friction
- Delivering at speed and scale
- Current industry trends and future challenges
- Successful case studies

Secure Coding – Theory

- Injection vulnerabilities and vectors
- Safe file handling
- Authentication and authorisation vulnerabilities
- OAuth, OIDC, SSO, IDPs, MFA
- Misconfigurations and secrets management
- Cryptographic configuration, security headers, and frameworks

Secure Coding – Practical

- Identifying and remediating injection, misconfiguration, and authentication/authorisation vulnerabilities in Birdhouse

Course Outline

Application Security Testing – Theory

- SAST, SCA, SBOM
- Secrets scanning
- DAST, IAST, and IaC testing
- Penetration testing and bug bounty programs
- AI-enhanced AST

Application Security Testing – Practical

- SAST, SCA, and secrets scanning in pipelines
- Performing assurance with AST tooling

Secure by Design

- Least privilege, attack surface reduction, blast radius reduction
- Zero Trust, trust boundaries, environment parity
- Redundancy, fault tolerance, reproducibility
- Supply chain management, observability, monitoring

Threat Modelling

- Four Questions, STRIDE, Attack Trees frameworks
- Scaling and repeatability, common anti-patterns
- AI for adoption and contextualisation
- Practical threat modelling exercises

Developer Security Training Programs

- Running Security Champions programs
- Incentives, collaboration between InfoSec and engineering
- Metrics to demonstrate value

Vulnerability Management

- Risk matrices, CVSS, EPSS, KEV, VEX
- Mapping ratings to internal risk, triage approaches
- AI-enhanced triage and remediation

Application Security Program Design

- Case studies: Telco, Government, SaaS, Financial Services, Startups

Upcoming Locations

Newcastle Oct 2–3 Rydges, Newcastle

Melbourne Oct 6–7 Cliftons Melbourne, Collins Street

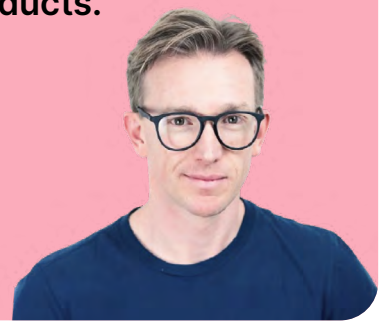
Sydney Nov 10–11 Novotel Sydney, Darling Square

Canberra Nov 17–18 Crowne Plaza, Canberra

> **Galah's application security workshop was both practical and engaging. It gave our engineers a clear understanding of secure coding principles and how to apply them in their day-to-day work. The session helped lift our overall security maturity and improve the way we build and maintain our products.**

★★★★★

Jonathan Milgate
Chief Technology Officer
Camplify



Your Investment

$1,800 per person (ex. GST)

$900 for students. To qualify for the student discount, you'll need to provide proof of current student status and a short video testimonial after completing the course.

All prices are in AUD.

Instructor

Cole Cornford – Founder, Galah Cyber

Cole is a recognised leader in Australia's application security scene. As Founder of Galah Cyber, he has led major security programs across global teams, is an active OWASP contributor, and hosts the Secured podcast.

GALAH CYBER

galahcyber.com.au

hello@galahcyber.com.au

Enrol Now