CYBER360
TRUSTED SECURITY ADVISOR

SERVICE BROCHURE

CYBER360 / SPECIALIST SERVICES

Secure Development

Design with security. Build with confidence. Deliver with evidence.

Bring security into the decisions that shape your software. Support design, code and delivery teams with focused reviews, practical requirements and a clear route from findings to fixes.

01 Clear scope

02 Practical evidence

03 Priorities for improvement

TRUSTED SECURITY ADVISORY

Advice that leads to action.

cyber360.co | info@cyber360.co | UK & Middle East

01 / SCOPE & FOCUS

The right question. A useful assessment.

Bring security into the decisions that shape your software. Support design, code and delivery teams with focused reviews, practical requirements and a clear route from findings to fixes.

Security requirements & design

A defined product, feature or architecture, with relevant user roles and data flows.

Security requirements, design recommendations and documented assumptions.

Focused code review

Agreed repositories, languages, components and security-sensitive functions.

Evidence linked to reviewed components, potential impact and remediation guidance. Coverage limitations remain explicit.

Secure development lifecycle

Selected development stages, responsibilities, existing checks and exception handling.

A practical improvement backlog with suggested decision points and ownership.

Dependencies & software supply chain

Agreed dependency inventories, package-management practices and build inputs.

Priorities for dependency governance and follow-up; a package scan alone does not establish exploitability.

Build, pipeline & release practices

Named repositories, CI/CD workflows, build permissions and release arrangements.

Recommendations for protecting delivery workflows and improving release assurance. Pipeline changes are separately authorised.

Developer support & testing

Agreed learning themes, remediation discussions and targeted application-security checks.

Practical guidance and agreed training or testing outputs. Penetration testing is separately scoped.

02 / APPROACH & DELIVERABLES

From agreed scope to practical action.

Understand the product

Agree its purpose, sensitive information, users, architecture and the decisions you need to support.

Define the review scope

Confirm repositories, versions, technologies, access, environments and coverage priorities.

Examine design & implementation

Review the agreed material using specialist analysis and appropriate supporting tools.

Discuss & prioritise findings

Work through evidence, prerequisites, impact and remediation options with the team.

Support the delivery plan

Translate findings into a practical backlog and agreed development or assurance actions.

Recheck & learn

Scope follow-up validation and regression guidance where needed, then address recurring causes.

WHAT YOU RECEIVE

For engineering & product leaders

- An overview of the assessed software risks and delivery implications.
- Prioritised recommendations and dependencies for planning.
- Review coverage, source versions, assumptions and limitations.
- Suggested lifecycle improvements and decision ownership.

For developers & security teams

- Findings tied to reviewed components and supporting evidence.
- Remediation recommendations and relevant validation criteria.
- Agreed design notes, requirements or process-review outputs.
- A technical debrief and proposed follow-up checks.

03 / PREPARATION & NEXT STEPS

Start with the right context.

Product & architecture

• Share product context, data flows, user roles and security-sensitive workflows.
• Identify integrations, critical dependencies and known concerns.

Code & environments

• Agree source versions, repositories, languages and access arrangements.
• Provide approved test environments and synthetic data where needed.

People & priorities

• Nominate engineering, product and security contacts.
• Agree review priorities around release plans and available team capacity.

Handling & follow-up

• Agree source-code confidentiality, evidence handling and retention.
• Confirm remediation ownership and whether re-review or testing is included.

PRACTICAL QUESTIONS

Does secure code review replace penetration testing?

No. Reviewing source and design can reveal issues that are difficult to see externally, while testing running software examines its behaviour in a deployed environment. The appropriate combination depends on the objective.

Can you review every language and technology?

Required expertise, tool support and delivery capability are confirmed during scoping. We do not assume that every technology can be covered by the same review.

LET’S DISCUSS YOUR PRIORITIES

info@cyber360.co | cyber360.co

UK +44 20 3286 1927 | UAE +971 55 768 7199