CYBER360
TRUSTED SECURITY ADVISOR

SERVICE BROCHURE

CYBER360 / SPECIALIST SERVICES

Defensive Security

Know your exposure. Strengthen your controls. Build a practical defence.

Connect risk, architecture and operational readiness. Understand where your defences need attention and turn the findings into a prioritised plan your teams can act on.

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.

Connect risk, architecture and operational readiness. Understand where your defences need attention and turn the findings into a prioritised plan your teams can act on.

Risk & asset assessment

Selected business services, information assets, systems, access arrangements and dependencies.

A scoped risk view and priorities for investigation or treatment.

Cyber readiness review

Agreed preventive controls, monitoring arrangements, response responsibilities and recovery dependencies.

A readiness assessment separating observed evidence, assumptions and improvement needs.

Security architecture & requirements

A defined solution, integration or architecture change, including relevant trust boundaries.

Documented recommendations and security requirements for design or procurement teams.

Configuration & hardening

Named systems or services, agreed baselines and the configuration evidence available for review.

A prioritised hardening backlog. Implementation and production changes require a separately agreed scope.

Policy, process & procurement support

Selected policies, operating procedures, security requirements or RFP documentation.

Recommendations or agreed document updates grounded in your operating model.

Improvement planning & validation

Findings from the agreed review and the dependencies needed to address them.

A phased roadmap and proposed validation steps; active testing is separately scoped.

02 / APPROACH & DELIVERABLES

From agreed scope to practical action.

Set the objective

Agree the business question, target services, stakeholders and boundaries.

Collect the evidence

Review agreed documents, architecture, configurations and operational information through approved access.

Assess the gaps

Compare the evidence with agreed requirements and relevant practices, recording assumptions and limitations.

Prioritise the response

Discuss impact, existing safeguards, feasibility and dependencies with accountable owners.

Build the roadmap

Set out recommended actions and the evidence needed to demonstrate progress.

Review improvement

Agree any implementation support, follow-up review or technical validation as a separate work package.

WHAT YOU RECEIVE

For leadership & risk owners

- A summary of the assessed risks and control themes.
- Priorities linked to relevant business services and dependencies.
- Scope, evidence gaps and limits on the conclusions.
- A phased improvement roadmap for discussion with accountable owners.

For technical & delivery teams

- Evidence-backed observations for the systems and processes reviewed.
- Configuration, architecture or process recommendations in the agreed scope.
- Suggested sequencing, dependencies and validation criteria.
- A findings debrief and agreed supporting documentation.

03 / PREPARATION & NEXT STEPS

Start with the right context.

Services & priorities

• Identify critical services, information and the security question driving the review.
• Share relevant changes, known concerns and existing risk assessments.

Evidence & access

• Agree documents, diagrams, configuration exports and interviews needed.
• Use approved access and secure handling for sensitive information.

Owners & decisions

• Nominate technical, operational and business risk owners.
• Confirm who can approve requirements, exceptions and subsequent changes.

Change & follow-up

• Identify maintenance constraints and delivery dependencies.
• Agree what advisory work includes and scope implementation or testing separately.

PRACTICAL QUESTIONS

Is this a penetration test?

No. This review focuses on risk, control design, configuration evidence and readiness. Active exploitation or attack simulation is only undertaken through a separately scoped and authorised engagement.

Will you change our production systems?

A review does not automatically authorise changes. Any implementation support needs an agreed scope, approvals, testing and change-control arrangements.

LET’S DISCUSS YOUR PRIORITIES

info@cyber360.co | cyber360.co

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