



Job Description

Job Title: Cyber Security Consultant

Revision Date: April 2025

Location: Home-based, with 2-3 days travelling per month to the client sites or other locations as needed in the performance of the role.

About Longwall Security

We are a leading cyber security specialist, delivering innovative & preventative strategies to protect organisations, their communities & data. We go beyond the conventional service provider – to our clients, we are an organic extension of their team.

Together, we are expert & extraordinary people sharing a passion for delivering outstanding service. We make a positive impact in every client engagement, focusing on addressing needs & pain points to drive essential business outcomes.

We believe in one team, succeeding together. For all our clients, partners & people, we'll be:



Exceptional

We strive to make an **impact** in everything we do.



Trusted

We deliver through close **partnership & collaboration**.



Determined

We **love** what we do & will go the extra mile.



Human

We **respect & support** each other to be our best.

Our purpose? Securing organisations so they can confidently do what they do best.

Role description

As a Cyber Security Consultant at Longwall, you will become a strategic advisor and a hands-on partner for our clients. Acting as a virtual CISO (vCISO), you'll help organisations understand their cyber risks, define their security strategy, and mature their security capabilities over time.

You'll become a key member of each client's security team—building strong relationships across both technical and executive stakeholders. Working within our Security Consulting Practice, you'll collaborate with our SOC to receive real-world insights into client environments—such as indicators of poor practice, recurring issues, and emerging threats.

Your role is to take these insights and translate them into actionable outcomes through a Security Improvement Roadmap, hosted and reviewed regularly with each client. From security governance and risk management to architecture reviews and incident readiness, you will be responsible for helping our clients become more resilient, more secure, and gain control of their risk.

Role responsibilities

- Act as a trusted security advisor and virtual CISO (vCISO), supporting clients in developing and maturing their cyber security strategy.
- Build strong, long-term relationships and embed yourself as a key member of each client's security team.
- Own and deliver a client-specific Security Improvement Roadmap, focused on reducing risk and increasing resilience.
- Lead security governance activities including risk reviews, board reporting, and mentoring of our clients teams.
- Identify security weaknesses through architecture reviews, audits, and threat exposure analysis across cloud, hybrid, and on-prem environments.
- Receive and interpret threat hunting results from our SOC, and drive remediation of poor practices with our clients.
- Guide our clients on compliance frameworks such as ISO 27001, CAF & Cyber Essentials supporting policy, process, and control improvements.
- Join our Cyber Security Incident Response Team (CSIRT) to support clients with incident planning, readiness exercises, and response when needed.
- Be an active contributor to the Longwall team, making constructive suggestions for improvement or new opportunities; asking for support when needed and giving it when asked.
- Adhere to Longwall Security internal policies as defined and updated from time to time.
- Other reasonable duties as required in support of Longwall Security goals.

Benefits

- 28 days annual leave + bank holidays
- Ongoing fully funded training & certifications
- Regular company social events
- Life cover
- Sickness cover*
- Private medical cover*
- Home working allowance*
- 5% employer pension contribution

*on completion of probation

Applicant profile

	Essential	Desirable
Experience	<ul style="list-style-type: none"> • Extensive experience designing and implementing secure technical solutions • Strong consulting background with a deep understanding of cyber security • Leading clients on a cyber journey, building and hosting security improvement roadmaps • Conducting security assessments & gap analysis reviews • Working with clients within Continuous Threat Exposure Management frameworks 	<ul style="list-style-type: none"> • ISO27001, ISO9001, Cyber Essentials, or similar security auditing experience • 12 months or more proven experience in cyber managed services • Ability to build trusting relationships with clients and colleagues
Knowledge & Skills	<ul style="list-style-type: none"> • Good understanding of security concepts, principles, and how emerging threats impact organisations • Able to assess business and technical requirements and recommend appropriate security solutions • Solid understanding of governance, risk, and compliance frameworks • Skilled at executive reporting, developing risk registers, and writing security policies • Comfortable presenting cyber risk to senior leadership and board members • Ability to think independently, work through complex challenges, and make clear recommendations 	<ul style="list-style-type: none"> • Architectural understanding of cloud and enterprise technologies like Azure, AWS, Microsoft 365 • Knowledge of incident response frameworks and how to run response efforts effectively
Behaviours	<ul style="list-style-type: none"> • Focused on delivering excellent service to clients • Committed to continuous learning and developing new skills • Takes pride in high quality work and getting things right first time 	<ul style="list-style-type: none"> • Highly organised, process driven, and good at documenting work clearly
Qualifications	<ul style="list-style-type: none"> • Entitlement to work in the UK • Full UK driving licence 	<ul style="list-style-type: none"> • ISC2 SSCP, CCSP, CISSP • ISACA CISM • ITIL Foundation or equivalent certification • Vendor-specific cyber security certifications (e.g. Microsoft, AWS, Rapid7)