POSITION DESCRIPTION

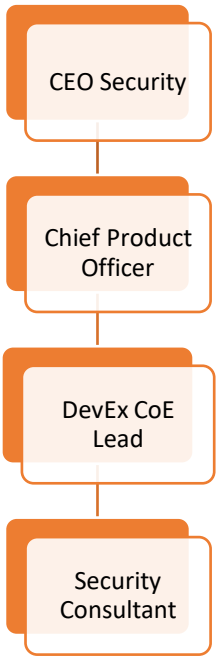
Position Title: Security Consultant	**Direct Manager: DevEx CoE Lead**	
Budget Responsibility: N/A	**Direct Reports: N/A**	**Indirect Reports: N/A**

WHAT YOU'RE HERE TO ACHIEVE

Key purpose: *Improving the security of Gallagher Security's development process and product security suites through enabling development teams to understand, manage and resolve risks in their areas.*

The Security Consultant role is responsible for implementing Gallagher Security's cyber security risk processes.

WHERE YOU'LL FIT IN #TEAMGALLAGHER



WHO YOU'LL BE WORKING WITH

INTERNAL RELATIONSHIPS	EXTERNAL RELATIONSHIPS

Created/ Edited: Dec 2023
By: Daniel McVeagh

Cyber Security Squad, All Security Squads and Value Streams, Group Information Security Team, Wider Gallagher Security Division	Third Party Penetration Testers

WHAT YOU'LL BE DOING

Key Accountability	Outcomes/ Expectations
Risk Management & Assurance: *Planning and implementing processes and procedures for the management of risk to the success or integrity of the enterprise.*	• Identifies risks and vulnerabilities, assesses their impact and probability, develops mitigation strategies, and reports to the business. • Performs technical assessments of complex or higher-risk information systems. • Identifies risk mitigation measures required in addition to the standard organisation or domain measures. • Enabling risk owners to best manage their risks • Establishes the requirement for accreditation evidence from delivery partners and communicates accreditation requirements to stakeholders. • Maintain external Hardening and other Cybersecurity documentation.
Vulnerability Research and Assessment: *ensure that the process of identifying, analysing, and mitigating vulnerabilities in a system is carried out effectively.*	• Applies standard techniques and tools for vulnerability research. • Uses available resources to update knowledge of relevant specialism. • Participates in research communities. • Analyses and reports on activities and results. • Collates and analyses catalogues of information and technology assets for vulnerability assessment. • Performs vulnerability assessments and business impact analysis for medium complexity information systems. • Contributes to selection and deployment of vulnerability assessment tools and techniques. • Assist in monitoring for vulnerabilities in third party components.
Security Expertise & Collaboration *Foster a culture of cyber security awareness through within the Security business unit*	• Help to educate members of the Security Division, Channel Partners, and Customers, on best practice for software security. • Participate in the Cybersecurity Advisory and Triage group helping to access and prioritise vulnerabilities as they are identified. • Manage relationships between squads and third-party Penetration Testing firms and coordinate their engagement when required. • Assist with consulting services to Channel Partners and Customers as required. • Provide support to the Tech Support team when addressing security concerns from customers. • Provides guidance on the application and operation of elementary physical, procedural, and technical security controls.

	• Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems. • Work in a manner and standard that upholds the Cyber Security Team Charter • Share knowledge and experience to help develop the team. • Work on improvements to security services, including continuous improvement of methodologies and supporting material.

Including any other duties not specified that may be required to complete the role, and as requested by the Reporting Manager.

HOW YOU'LL BE DOING IT

Qualifications& Experience:

- Tertiary qualification in computing or risk management related studies or equivalent experience.
- Experience working in a team environment alongside Developers, Testers and Product Owners using agile methodologies (particularly Scrum and Kanban).
- Demonstrated experience in Cybersecurity, preferably with exposure to application security testing, Windows, Linux and network topologies.
- Previous experience of using risk management platforms.

Required Skills & Competencies:

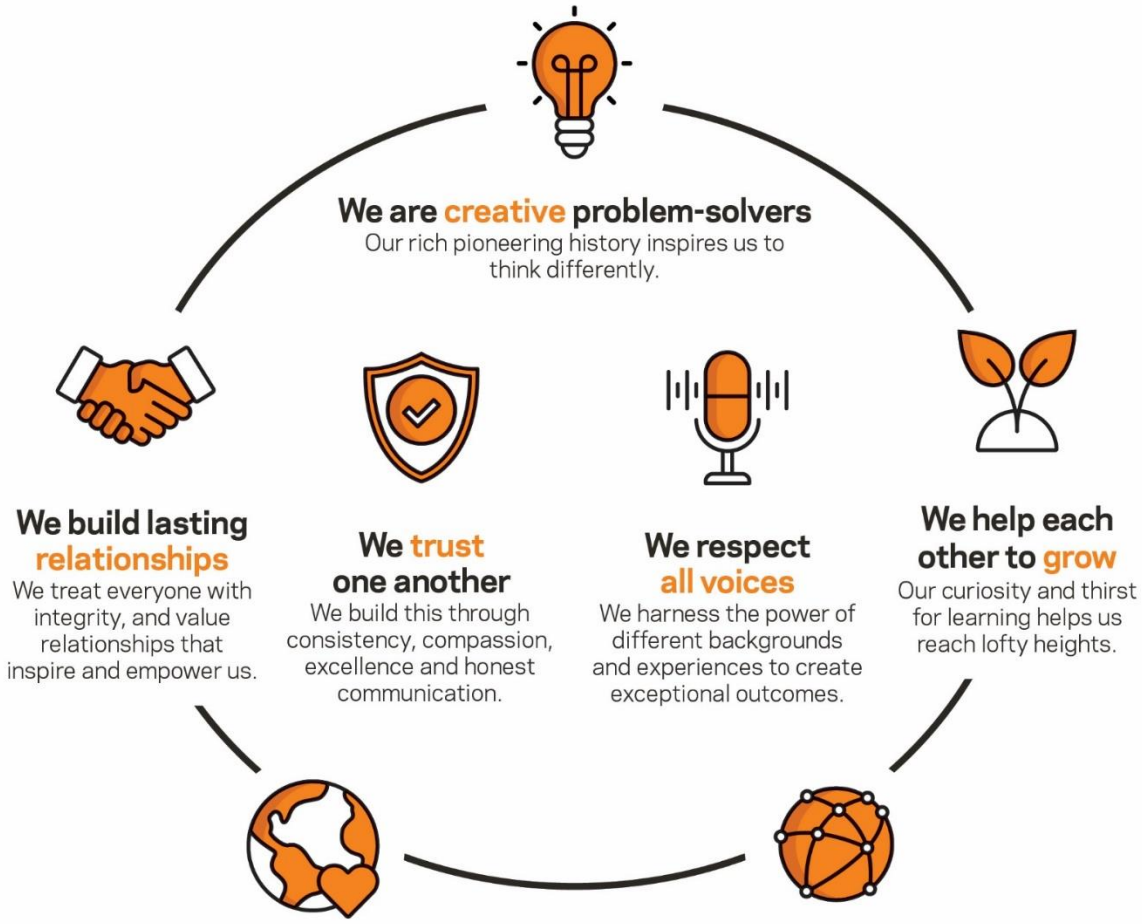
- Strong verbal and written communication and ability to write clear and concise documents describing process or problems.
- Strong time management and prioritisation skills.
- Strong relationship management skills in managing relationships between technical and non-technical stakeholders

Desired Skills & Competencies:

- Ability to evaluate the impact of product anomalies and set appropriate classifications.
- Strong technical understanding of PC's, Operating systems, networks and virtualisation.
- Good understanding of network protocols, design and operations.
- Vulnerability and threat management experience
- Understanding of cryptography principles

Protect what matters most.

Our purpose and our values apply to our extended Gallagher family including our employees, customers, partners and community.



We are creative problem-solvers
Our rich pioneering history inspires us to think differently.

We help each other to grow
Our curiosity and thirst for learning helps us reach lofty heights.

We respect all voices
We harness the power of different backgrounds and experiences to create exceptional outcomes.

We trust one another
We build this through consistency, compassion, excellence and honest communication.

We build lasting relationships
We treat everyone with integrity, and value relationships that inspire and empower us.

We share knowledge freely
We're a global community that sees collaborative information flow as a super power.

We're committed to a better tomorrow
Our practices, behaviours and processes are good for us all and for our planet.

Created/ Edited: Dec 2023
By: Daniel McVeagh