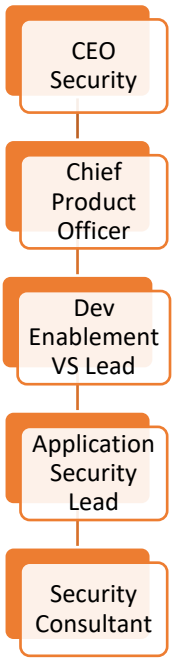
POSITION DESCRIPTION

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

WHAT YOU'RE HERE TO ACHIEVE

To improve the security of Gallagher Security products by enabling the success our application security lifecycle, performing security and penetration testing, staying aware of current and emerging threats, assisting with strategic relationships within security communities, and providing technical expertise for cyber security.

WHERE YOU'LL FIT IN #TEAMGALLAGHER



WHO YOU'LL BE WORKING WITH

INTERNAL RELATIONSHIPS	EXTERNAL RELATIONSHIPS
Cybersecurity Services squad, all Security squads and Value Streams, IS Cybersecurity team, wider Gallagher Security team	Third-party penetration testers, security researchers, hacker communities, key customers and channel partners

Created/ Edited: Sep 2024
By: Jeremy Utting

WHAT YOU'LL BE DOING

Key Accountability	Outcomes/ Expectations
Security Expertise	• Participate in our Security Reviews process for new features, including threat models as required. • Assist Solution Delivery teams to follow best practices for product security. • Assist with Cybersecurity Advisory and Triage (CAT) activities, helping the group to assess and prioritise vulnerabilities. • Contribute to evaluation of the security of infrastructure and applications, under direction of a senior team member. • Assist with support and guidance to internal teams (e.g., Tech Support, Engineering), when addressing security concerns from customers.
Collaboration & Outreach	• Participate in efforts to enable Gallagher Security to be seen as a thought leader in the cybersecurity of our products, represented through a variety of channels (e.g., white papers, blog posts, conference presentations, interviews). • Assist with consulting services to key Channel Partners and Customers as required. • Contribute to external Hardening and other Cybersecurity documentation, under direction of a senior team member.
Security and Penetration Testing	• Perform penetration testing activities on Security products and systems, under direction of a senior team member. • Contribute to implementation of automated vulnerability tests where appropriate. • Perform vulnerability research and identification tasks, using established procedures. • Contribute to analysis and reporting on testing activities and results. • Assist with vulnerability assessments for information systems. • Assist with evaluation of vulnerability assessment and discovery tools and techniques.
Risk Management & Assurance	• Contribute to identification of risks and vulnerabilities, assessment of their impact and probability, development of mitigation strategies, and reporting to the business. • Assist with technical assessments of information systems. • Assist with Identification of risk mitigation measures required.
Self-Development & Awareness	• Keep up to date with techniques, tools, and threats relevant to software security, cyber-physical systems, and penetration testing. • Maintain awareness of general cyber security trends, and vulnerability discoveries.

Created/ Edited: Sep 2024
By: Jeremy Utting

	• Participate in cybersecurity and vulnerability research communities for relevant tech domains, to maintain awareness of trends.

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.

Required Skills & Competencies:

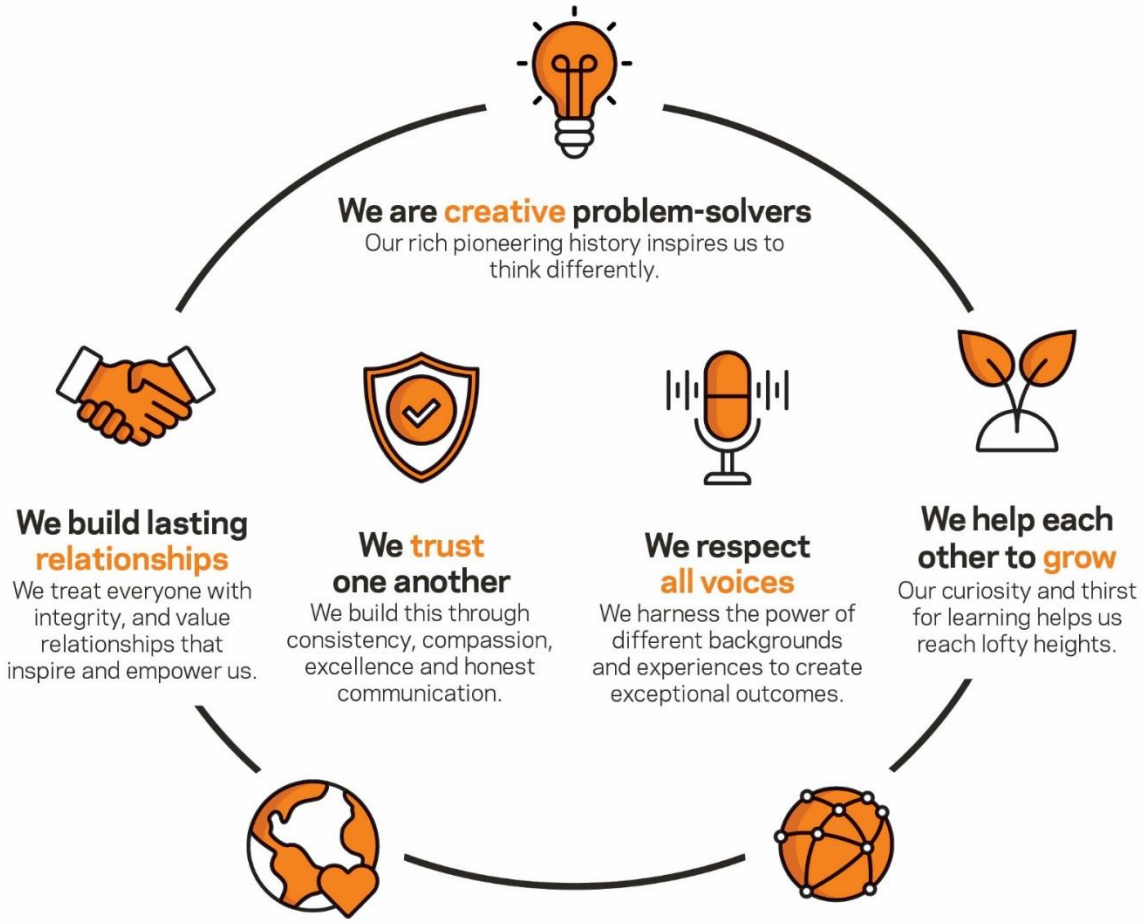
- Strong verbal and written communication and ability to write clear and concise documents describing process or problems.
- Time management and prioritisation skills.
- Relationship management skills in managing relationships between technical and non-technical stakeholders

Desired Skills & Competencies:

- Experience working in a team environment alongside Developers, Testers and Product Owners using agile methodologies (particularly Scrum and Kanban).
- Previous professional and/or academic experience in Cybersecurity, preferably with exposure to application security testing, Windows, Linux and network topologies.
- Previous experience of using risk management platforms.
- Technical understanding of PCs, Operating systems, networks and virtualisation.
- Good understanding of network protocols, design and operations.
- Vulnerability and threat management experience
- Understanding of cryptography principles
- One or more security-related certifications (e.g., CC, CEH, CompTIA Security+, AWS Solution Architect-Associate, Azure Security Engineer-Associate)

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: Sep 2024
By: Jeremy Utting