

## Role Profile: Cyber Security Graduate (2025)

### A bit about us...

Amiosec is a rapidly growing UK-based technology company, driven by innovation, agility, and state-of-the-art technology. We collaborate with UK government customers and commercial providers to deliver cutting-edge research, technology, products, solutions, and services in the communications security sector.

We offer a stimulating work environment where engineers have the opportunity to contribute to various projects, from early-stage proof-of-concepts to product development. Our self-managing agile teams utilise a blend of Scrum and Kanban techniques, providing engineers with a sense of ownership and the ability to see how their contributions impact the broader goals of the company.

Fostering collaboration and nurturing talent are fundamental pillars of our culture. We actively cultivate an environment where sharing knowledge and ideas is not only encouraged but celebrated. Our monthly Engineering Forum serves as an invaluable platform for exchanging tips, tricks, and techniques among our diverse teams and projects, facilitating continuous learning and growth.

Moreover, we recognise the importance of fostering a strong social bond within our team. That's why we organise regular social activities and gatherings, including coffee and cake mornings and engaging activity days. These events not only foster camaraderie but enhances collaboration resulting in an effective hybrid working scheme, while also ensuring a comfortable and inclusive social atmosphere for all team members.

We understand the importance of work-life balance and offer several options to support our engineers. Our optional 9-day fortnight scheme allows for flexible scheduling, enabling every other Friday off, promoting a healthy work-life balance. Additionally, our hybrid working policy strikes a balance between on-site collaboration and remote work flexibility, subject to individual project needs. This approach empowers our team to perform at their best while maintaining a fulfilling work-life balance.

**NOTE:** - Due to the nature of our work, all candidates will be required to obtain and maintain an appropriate UK security clearance.

### Our Graduate Scheme

We are passionate about nurturing new talent and have been running a successful Graduate Scheme since 2021. With a dedicated Head of Early Careers, we support our graduates in learning, growing and exploring new opportunities.

Our Graduate Scheme offers structure and support, allowing you to refine the skills you already have and take advantage of tailored opportunities and training over a 12-month period. Our graduates will rotate through different projects putting new skills into practice. These are designed



not only to help graduates grow and learn but also to deliver valuable contributions to the business.

As a cybersecurity graduate at Amiosec, you will play a key role in protecting systems, networks, and data from cyber threats. This is a varied position where you could be developing a new service for a customer one moment and then monitoring security alerts, analysing vulnerabilities, conducting risk assessments, and implementing measures to defend against malware, phishing, and unauthorised access the next. Keeping up with emerging threats and evolving technologies will be a continuous and essential part of your responsibilities.

We are looking for talented engineering graduates to join our growing team in September 2025. You will be an essential part of small, multi-disciplinary teams working on secure communication products and services that benefit both us and our customers. You will also have the chance to work within Product Engineering, helping to keep Amiosec ahead of the curve.

## Typical Activities

Subject Area	Activities
<b>Development</b>	<ul style="list-style-type: none"> <li>Design, develop and implement new functionality into existing systems</li> <li>Identify areas of improvement, and design and implement enhancements</li> </ul>
<b>Documentation</b>	<ul style="list-style-type: none"> <li>Documentation of design specifications and implementation decisions, with guidance</li> <li>Handover documentation for transitioning functionality into live service</li> </ul>
<b>Lifecycle</b>	<ul style="list-style-type: none"> <li>Obtain an appreciation and some experience in all areas of the system lifecycle, from requirements through to testing and commissioning</li> </ul>
<b>Technology Evaluation and Research</b>	<ul style="list-style-type: none"> <li>Investigate new tools and technologies, and how they can be incorporated into the systems</li> </ul>
<b>Team Activities</b>	<ul style="list-style-type: none"> <li>Using Agile methodologies and getting involved with sprints</li> <li>Working within teams to contribute to technical solutions</li> </ul>
<b>STEM outreach</b>	<ul style="list-style-type: none"> <li>STEM outreach is very important to Amiosec, and all early careers staff will be encouraged to get involved with the creation of new activities and attending events</li> </ul>

## Technical Competencies

Subject Area	Competency
<b>Qualifications</b>	<ul style="list-style-type: none"> <li>Minimum of 2:1 degree in a relevant subject such as Computer Science or Cyber Security</li> </ul>
<b>Knowledge</b>	<ul style="list-style-type: none"> <li>Required to have a good understanding of Linux (RHEL derivatives preferred)</li> <li>Knowledge of containerisation tools (e.g. Docker, Podman)</li> <li>Familiarity with automation and scripting tools such as Bash, Ansible, Python and Git CI/CD</li> <li>Understanding of core networking concepts (including IP addressing, common network protocols, OSI 7-layer model)</li> <li>Experience with hypervisors (e.g. VMware, Proxmox etc)</li> </ul>



Subject Area	Competency
Security	<ul style="list-style-type: none"> <li>Knowledge of how to configure OS and deploy applications securely (firewalls, OS hardening)</li> <li>Knowledge of tooling that helps bolster security (e.g. VPN, WAF, Proxy)</li> </ul>

## Potential Responsibilities & Desirable Competencies

Subject Area	Activities
SOC analysis	<ul style="list-style-type: none"> <li>Respond to alerts and carry out root cause analysis of security events</li> <li>Tune alerting to ensure coverage across the environment, minimising false positives</li> <li>Document findings of RCA, and create reports of events</li> <li>Read documentation to get an understanding of how new tools / technologies work, to understand what could cause an alert to be triggered</li> </ul>
Knowledge	<ul style="list-style-type: none"> <li>Desirable to have familiarity of IDS / IPS systems, and the ability to write rules to capture specific events</li> <li>Desirable to have knowledge of SIEM systems, ability to query the data and write custom dashboards (Splunk, ELK)</li> <li>Desirable to understand cryptography / encryption methods.</li> <li>Desirable to be familiar with security frameworks and standards (ISO 27001)</li> </ul>

## Core Competencies

Subject Area	Competency
Approach	<ul style="list-style-type: none"> <li>Enthusiasm for technology and desire to understand and utilise it to develop innovative solutions</li> <li>Ability to quickly learn innovative technologies.</li> <li>Ability to apply a systematic and methodical approach to debugging/resolving technical issues</li> </ul>
Working Style	<ul style="list-style-type: none"> <li>Ability to work individually or as a member of a multi-disciplined team</li> <li>Self-motivated</li> <li>Willingness to embrace new technologies/techniques.</li> <li>Good time management and ownership of own deliverables</li> <li>Good troubleshooting and problem-solving</li> </ul>
Innovation	<ul style="list-style-type: none"> <li>Ability to foster and develop innovative ideas</li> <li>Willingness to contribute to improvements in products and ways of working</li> </ul>

Amiosec is committed to providing equality of opportunity for all. We aim to ensure our workplaces are free from discrimination and that our current and future colleagues, are treated fairly and with dignity and respect. Please inform us of any reasonable adjustments that we may need to make to the application or interview process.