

Job Profile

Job Title: Cyber Security Engineer

Job Grade: Level 4, Zone 1

Salary Range: £51,087.60

About Camden

Camden is building somewhere everyone can thrive, by making our borough the best place to live, work, study and visit. Because we're not just home to UK's fast-growing economy. We're home to the most important conversations happening today. And we're making radical social change a reality, so that nobody gets left behind. Here's where you can help decide a better future for us all.

A key part of our Digital and Data Services (DDS) department, our Technology Service provides secure, innovative, efficient, and scalable technology solutions that empower our Staff and our Citizens. We are a team of collaborators and knowledge sharers working in an agile, fast-paced environment.

About the role

As a Cyber Security Engineer, you will support the Security Operations team by being responsible for the ongoing monitoring, analysis, escalation, and response to alerts generated by the various security systems such as Security Information & Event Management (SIEM), Data Loss Prevention (DLP), Endpoint Detection & Response (EDR) and Intrusion Detection & Prevention (IDP).

You will be responsible for the ongoing maintenance and improvements to the security controls of the organisation and carry out administrative changes to Camden's security systems, responding to requests from Camden colleagues and partners while ensuring adherence to expected SLAs.

Some of these tasks include but not limited to:

- Actively monitoring and reviewing security system logs
- Analysing and responding to anomalous behaviour, escalating appropriately when needed
- Ensuring security coverage and efficiency
- Act as a security evangelist by providing advice to the organisation and ensuring that security standards are understood and complied with
- Ensure a strong and efficient security coverage with continuous maintenance and troubleshooting of security systems
- Performing administration tasks and changes on Camden systems related to:

- Firewall policies
 - Cloud access policies
 - Anti-malware policies
 - Vulnerability scanning
 - Email Protection policies (anti-spam, anti-phishing)
- Conducting regular reviews of application requests from Camden colleagues to ensure our data remains secure
- Researching and evaluating emerging cyber security threats
- Coaching and assisting in training of junior members of the team
- Lead investigations into alerts generated by various security systems as well as by other reporting means in Camden
- Maintaining and improving on existing documentation
- Working to maintain regulatory requirements through audit remediation / support, Vulnerability scans, penetration testing and remediation where appropriate
- Develop cutting-edge playbooks and detection use-cases, using industry best-practice, threat intelligence and detections frameworks
- Ability to work under pressure and handle multiple projects with tight deadlines related to security tools and technologies

About you

Camden is on a journey to transform our digital experiences using cloud technology. To be a successful Cyber Security Engineer, you will need to adapt to a fast-paced, ever-changing environment, as well as maintaining a professional, security-focused approach to all tasks. You will ensure that you keep up to date with current threat trends and use that to the benefit of our organisation and its goals.

You will be a good problem solver who can work on your initiative and with others to identify creative and innovative solutions. You will also be adaptable and flexible in your approach to work and have excellent organisational skills to manage a varied workload.

You will have relevant professional certifications and experience to demonstrate your capabilities and fit for the role.

Core skills include:

- An appreciation for Cyber Security with fundamental computer forensic skills

- Demonstrable experience and application of IT Security principles including regulatory, legislative and industry practices gained through practical experience and /or professional certifications.
- Good understanding of network ports and protocols
- Experience working in a modern agile delivery environment (scrum, Kanban etc)
- Proficient in understanding the principles and application of cloud/virtualisation (including ownership, responsibilities, and security implications)
- A working knowledge of Microsoft operating systems including a Windows 10 and Windows Server 2012/2016/2019
- A working knowledge of Microsoft Active Directory, Azure and Office 365
- Good understanding of DLP, EDR, IDS/IPS and firewall technologies (Palo Alto experience preferred)
- Good understanding of attack vectors, exploits and vulnerabilities
- You will naturally collaborate with and learn from the people around you, always looking to seek improvements on a continuous basis.

Desirable Skills Include:

- Experience of using agile collaboration tooling, such as Jira and Confluence
- Experience working in an ISO27001 environment
- Relevant certifications including CompTIA Sec+, GSEC, SSCP, CCSP, CISSP
- Experience working with SIEM technologies as well as the development, implementation, and maintenance of custom playbooks
- Working experience with the Microsoft Threat Protection stack and Azure Security.
- Availability for After-Hours Support

Work Environment:

In line with Camden's Agile Working approach, there is an expectation that the post holder will split their time between working in the office and working at home as appropriate for their role. You are expected to work core hours between Monday – Friday.

Relationships:

- This post reports to the Security Architect and additionally works closely with the Information Security Manager.

- Internal at all levels.
- Local government, membership bodies and professional bodies including the NCSC, external auditors and accreditation bodies as required

Over to you

We're ready to welcome your ideas, your views, and your rebellious spirit. Help us redefine how we're supporting people, and we'll redefine what a career can be. If that sounds good to you, we'd love to talk

Is this role Politically Restricted?

Some posts at Camden are politically restricted, which means individuals holding these posts cannot have active political role. For a list of all politically restricted roles at Camden [click here](#).

Diversity & Inclusion

At Camden, we value and celebrate difference and encourage diversity in all respects. Our diverse workforce ensures we represent our communities to the best of our ability and enables us to make better decisions. Because of this, we particularly welcome applications from Black, Asian and other ethnic groups, those who identify as LGBT+, neurodiverse and disabled people. Click [Diversity and Inclusion](#) for more information on our commitment.

Agile working

At Camden we view work as an activity, not a place. We focus on performance, not presenteeism. We create trusting relationships; we embrace innovation rather than bureaucracy and we value people. Collaboration is the Camden way, silo working isn't.

At Camden we are proud to be one of Hire Me My Way's inaugural campaign supporters. Hire Me My Way is a national campaign led by Timewise, designed to increase the volume of good quality jobs that can be worked flexibly in the UK (www.HireMeMyWay.org.uk). Hire Me My Way aims to treble the number of available good quality flexible jobs to 1 million by 2020.

Asking for Adjustments

Camden is committed to making our recruitment practices barrier-free and as accessible as possible for everyone. This includes making adjustments or changes for disabled people, neurodiverse people or people with long-term health conditions. If you would like us to do anything differently during the application, interview or assessment process, including providing information in an alternative format, please contact us on 020 7974 6655, at resourcing@camden.gov.uk or post to 5 Pancras Square, London, N1C 4AG