**Job Profile**

**Job Title: Senior Cyber Security Engineer**
**Job Grade: Level 4, Zone 2**
**Salary Range: £47,671 - £49,515 (depending on experience)**

## 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 Senior Cyber Security Engineer, you will support the Security Operations team by being responsible for the ongoing content development for the various security systems such as Security Information & Event Management (SIEM), Data Loss Prevention (DLP), Endpoint Detection & Response (EDR), Intrusion Detection & Prevention (IDPS), Firewalls / Servers / Workstations / Laptops and IOT devices, Vulnerability Assessment, and internal training awareness programme. Furthermore, you will have experience working within a large-scale enterprise IT environment. Excellent communication skills is a must, you will be dealing with Stakeholders, 3rd Party Vendors and partners while ensuring adherence to expected SLAs. You will be a self-starter, comfortable taking a lead role within the team and on high profile projects.

Some of these tasks include but not limited to:

- Proactively support security engineers and security analysts in concluding the investigation of security system logs
- Must have broad knowledge and experience of Information Security, understanding applications, data, threats and mitigation, and security trends
- Must have practical experience of SIEM / EDR / Cloud-based platforms to enhance detection and visibility
- Must be able to deploy, implement and test leading Microsoft cloud-based platforms
- Must be able to contribute towards CTI function to build additional detections for new threats

- Analyse advanced anomalous behaviour, risks, and threats, and perform complete mitigation appropriately when necessary
- Expertise in taking policy statements and translating them into implementable, security controls that can be monitored, audited, and constantly improved. Ability to judge their effectiveness and recommend improvements
- Good understanding and demonstrable hands-on experience with operating systems and tools (Linux/Unix preferred) and fundamental Internet and security technologies (routing/switching, DNS, packet analysis, etc), in an enterprise or service provider environment
- Must take lead on 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)
    - Advanced Threat Analytics / Threat Modelling
    - Vulnerability Assessment
- Scripting and automation: good ability to read and understand logs and alerts, to use specialist tools and programming / scripting languages (Python, Shell, PowerShell, etc), to automate tasks
- Experience of open-source security tools and how they could be used in an enterprise
- Conducting regular reviews of application requests from Camden colleagues to ensure our data remains secure
- Coaching and assisting in training of Security Operations engineers / analysts in the team
- Lead investigations into alerts generated by various security systems as well as by other reporting means in Camden
- Performing risk assessments using multiple methods including IS1, ISO27001, NIST, Mitre, STRIDE.
- Working to maintain regulatory requirements through audit remediation / support, vulnerability scans, and remediation where appropriate
- Develop cutting-edge playbooks and detection use-cases, using industry best-practice, threat intelligence and detections frameworks
- Extensive experience and knowledge in securing web applications, mobile applications, infrastructure and supporting frameworks
- Provide subject matter expertise on architecture, authentication, and system security
- Ability to work under pressure and handle multiple projects with tight deadlines related to security tools and technologies
- Excellent organisational and time management skills, and the ability to work on multiple projects at the same time

**About you**

Camden is on a journey to transform our digital experiences using cloud technology. To be a successful Senior 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. This role is a front line, hands-on, operationally focused position, responsible for implementing security controls, for monitoring and responding to security events and incidents.

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 such as CISSP, and experience to demonstrate your capabilities and fit for the role.

Core skills include:

- Subject matter expert in multiple Cloud Technology areas such as O365, Azure (Identity, Security and Compliance, Microsoft Endpoint Management, PIM), Defender, Azure AD, Azure Sentinel / SIEM and Tenable
- Knowledge and experience in dynamic or static digital forensic skills and malware analysis
- Demonstrable experience and application of IT Security principles including regulatory, legislative and industry practices gained through practical experience and /or professional certifications
- Solve technical problems of the highest scope, complexity, and ambiguity
- Experience of running Threat Modelling for teams and products with reference to secure engineering principles, and standards (e.g., OWASP\NIST)
- Good knowledge of Business Continuity Planning (ISO 22301) and Disaster Recovery plans
- Understand security requirements in the Cloud and be able to drive technical implementation requirements
- Understand the implications of standards and regulations such as GDPR, ISO27001, NCSC Cloud Security Principles, SOAR, CIS, to inform decision making

- Solid demonstrable comprehension of Cyber Security including malware, emerging threats, attacks, and vulnerability management
- Strong working security knowledge and experience gained working with standard accreditation frameworks
- Develop security training and socialise the material to internal teams
- Demonstrate the ability to think and act quickly in emergencies or under pressure
- Able to demonstrate an ability to work as part of a team. Able to deal calmly and confidently with all demands from the public

Desirable Skills Include:

- Experience of using agile collaboration tooling, such as Jira and Confluence
- Experience working in PCI and ISO27001 environment
- Relevant certifications including Microsoft Azure, 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 for emergency support and routine maintenance

**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 Operations Manager 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