Security Engineer SIEM – Via Resource

**Job Title:** Security Engineer SIEM

**Location:** UK

**Terms:** Permanent/Contract

**Salary:** £

**About Us**

Via Resource specialise in Information and Cyber Security talent in UK, Europe and USA. We have developed a unique methodology over the past twelve years that delivers proven results for both candidates and clients.

Our consultants have a minimum of four years of Information & Cyber Security recruitment experience, and work with candidates and clients acting as true consultants.

If you’re seeking to attract the best talent or find the ideal career opportunity, Via Resource’s experienced industry experts can help.

**The Role**

You will focus on improving the telemetry, processes and tools for Tesco’s SIEM system. This role requires proven experience with security telemetry, security intelligence, anomaly hunting and incident response.

The Engineer must leverage intuition, security knowledge and a broad of array of tools and advanced security techniques to help us uncover and stay alert to malicious activity. Bilaterally, we’re building a threat hunting capability to feed back into our telemetry and processes.

**Key Responsibilities**

* Experience performing technical analysis involving security event data and evaluating malicious activity.
* Knowledge of TCP/IP and related network protocols: knowledge of standard network protocols like TCP, ARP, ICMP, DHCP, DNS, HTTP, SNMP etc., and accompanying protocol/packet analysis/manipulation tools.
* Knowledge of information security protection/detection and authentication systems (firewalls, IDS, IPS, anti-virus, etc).
* Knowledge of commonly-accepted information security principles and practices, as well as techniques attackers would use to identify vulnerabilities, gain unauthorized access, escalate privileges and access restricted information.
* Knowledge of current operating environments (Microsoft, Linux, & OS X).
* Understanding and application of the following security tools: Development / Configuration experience with any industry leading SIEM platform.
* Experience of development using a programming language in a DevOps environment using agile techniques.
* Exceptional analytical and critical thinking, willingness to challenge status quo.
* Excellent interpersonal skills.
* Advanced written and oral communications, self-motivator.
* Team player and independent worker, highly adaptive

**Desired Skills**

* Splunk (including Enterprise Security, UBA and CIM)
* AWS
* Devops toolsets – Github, Jenkins, Jira etc.
* Python, Java
* Academia: College degree or equivalent work experience.
* Desirable Certifications: SSCP, GSEC, GCIH, GCIA or other industry relevant certifications

**What We Offer**

We offer excellent benefits that help make our organisation a great place to work. These include but aren’t limited to:

* An annual bonus scheme
* Holiday starting at 25 days plus a personal day
* A retirement savings plan
* Life Assurance
* Buy As You Earn Scheme
* Save As You Earn Scheme
* Deals & Discounts platform