

Senior Cyber Security Operations Analyst (042863)

Status
Open

Recruiter
Wyatt, Steve

Status Details
Sourcing

Hiring Manager
Perez, Yelibeth

Primary Location
London

Requisition Type
Professional

Hired Candidates
0 out of 1

Job description

Internal description

Description - Internal

Location: Pier Walk, North Greenwich / remote working

Job Purpose:

You will be responsible and accountable for defined aspects of the implementation and improvement of TfL's cyber security posture. This includes the identification and capture of requirements, engagement with stakeholders, the selection and delivery of solutions, and ensuring that solutions maintain their effectiveness in an ever-changing threat environment.

This means you will work with colleagues in the Cyber Security and Incident Response Team (CSIRT), delivering TfL's cyber security strategy, as they continuously improve cyber security techniques that reduce the risk posed by cyber attack to TfL's information, systems and operations.

Key Accountabilities:

- Responsible for proactively monitoring TfL systems for malicious activity and intrusions using real time data and alerting from various data sources measured against agreed SLAs.
- Responsible for ensuring processes and operational documentation is maintained, fit for purpose and updated regularly to reflect changing business needs.
- Responsible for implementing the TfL Incident Response process for Cyber Security Incidents, in collaboration with key stakeholder across the organisation
- Responsible for the triaging and investigation of notable events before elevating them to an incident and executing the incident response process.
- Responsible for investigating and handling escalated events and incidents in collaboration with key stakeholders and seeing them through to closure
- Responsible for tuning detection and monitoring tooling to provide high fidelity alerting worthy of further investigation and mitigating false positives.
- Responsible for keeping up to date with current cyber developments and trends, and maintaining your skills through continuous personal development and working collaboratively with colleagues, both internal and external to the team.

Knowledge:

- Broad knowledge of cyber security and information security controls best practice with supporting qualifications where possible - such as Security+, Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), CPNI 10 and SANS 20.
- Broad knowledge of relevant legislation and government standards - including Security Policy Framework, Information Assurance Maturity Model, Security Essentials, CPNI 10, Data Protection Act, Freedom of Information Act, EU Procurement Directives.
- A broad understanding of network and computer system architecture, operations and protocols.
- Understanding of information security management concepts to support solutions and processes.
- The post holder requires a good understanding of information security, common data network protocols and IT infrastructure and the requirements of confidentiality, integrity and availability.

Skills:

- Selecting security controls with meaningful measures to monitor their effectiveness and identify improvements.
- Ability to communicate effectively and influence at equivalent role levels of a complex organisation, such as in meetings with business partners and other stakeholders.
- Able to swiftly build an understanding of a security problem presented by a senior security analyst.
- Ability to plan and prioritise multiple workstreams in response to rapidly developing and changing workloads.

Experience:

- Experience of delivering IT/cyber security in a large organisation.
- Familiar with enterprise-level cyber security technologies for use in complex environments.
- Successfully engaged with internal stakeholders and third parties to achieve business objectives.
- Experience of creating and presenting cyber security reports and recommending solutions.

Closing date for applications: Sunday 9th July 2023 @ 23:59

Application Process

Please apply supplying both your CV and a covering letter preferably in “ .docx ” format. Both documents should be A4, in Arial 12 font, and a maximum of 2 pages per document.

Please think carefully about the skills, knowledge and experience outlined in the job description and ensure your submission reflects the requirements of the role you are applying for.

Probation:

In line with our Resourcing Policy (Feb 2014), internal employees are required to complete their probationary period before applying for internal TfL positions. Please ensure you have successfully completed your probation before submitting an application for this role, otherwise your application may be withdrawn.

Formal warnings:

Internal employees with any current formal warnings are not eligible to apply for internal TfL vacancies until expiry of the warning. Ineligible applications may be withdrawn. Details of what is defined as a current formal warning can be found on Platform: <https://transportforlondon.sharepoint.com/sites/Instructions-and-guidance-people-performance-and-rewards/SitePages/Applying-for-a-vacancy-with-a-formal-warning.aspx>

NPL Applications

Applications to internally advertised roles can only be accepted from temporary workers who are on PAYE terms via agency, or PAYE via Umbrella Companies. Temporary workers who are paid through their own limited companies are not covered by the Agency Worker Regulations and are ineligible to apply.

On this recruitment campaign, as part of TfL 's continuing commitment to be an inclusive and equal opportunity employer we will be removing personal identifiable information from CVs and covering letters that could cause discrimination.

Many of our staff work flexibly in many different ways. Please talk to us at interview about the flexibility you need. We'll see what we can do.

We understand a confidence gap can get in the way of meeting spectacular candidates. So please don ' t hesitate to apply if you think you have what it takes even if you feel you don ' t meet all the criteria. We ' d love to hear from you.

External description

Description - External

External Job Description