Job Description and Person Specification

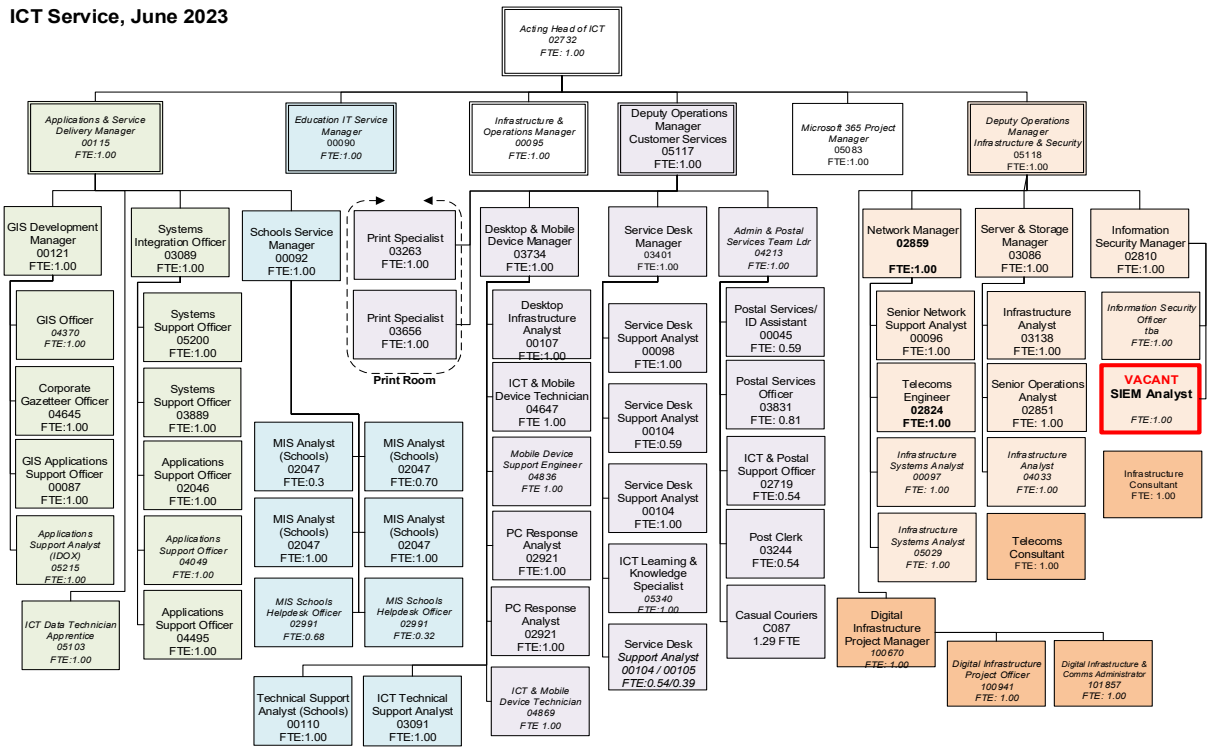
Job title:	IT Security Analyst - Securty Information Event Management (SIEM)
Directorate:	Resources
Service:	Customer Services and ICT
Team:	ICT Operations
Post number:	05396
Salary grade:	Grade H – fixed term contract
Work location:	Market Street Offices, Newbury
Reports to:	Information Security Manager
Supervises:	None

Job Purpose

This role will be part of the Information Security team at WBC, ensuring that the council maintains appropriate levels of security, privacy and resilience to protect our people, data, operations, and facilities from harm.

- To support, maintain, and develop the Council's System Information Event Management (SIEM) environment; including monitoring and response to various security alerting channels, including SIEM tools such as Security Onion.
- To provide additional capacity to support the Information Security Manager.
- To assist in related investigations as required by the Information Security Manager.
- To develop, document and adopt responsibility, as required, for operational processes relating to delivery of SIEM within the Information Security team.
- To undertake daily investigations based on cyber threat intelligence from open sources and local government partners.
- To assist in the development of incident response playbooks.
- To assist with remediation activities.
- To constantly improve the tuning of SIEM alerts and automation of regular tasks.
- To undertake basic research and produce feedback reports to improve knowledge of the WBC cyber threat landscape.
- To give input into regular security control dashboard reporting.

Structure Chart



Main Duties and Responsibilities

The Security Information Event Management (SIEM) Analyst plays a critical part in ensuring the security of West Berkshire Council and is involved in the monitoring and investigation of security events and incidents. You will identify, contain and assist in remediating incidents, identify potential process improvements, and maintaining organisational readiness through preparedness exercises, advising product and service owners of potential mitigations.

- You will collect, analyse and process security event data arising from activity across the organisation, tune and improve generating security alerts, and follow up by investigating indicators of potentially malicious activity, escalating incidents or initiating responses as required.

- Monitor, triage and investigate security alerts across various monitoring platforms to identify security incidents and perform analysis of event data to support the response, reporting and resolution of security incidents.

- Support implementation of the monitoring roadmap to enhance monitoring in line with requirements, policies and standards to govern all activities and outputs.

- Operate as a key member of the information security incident response team, providing log analysis and investigation as required.

Main Duties and Responsibilities

- Assist in the design, development and enablement of automated monitoring processes, recommending and implementing the latest SIEM (Security Information and Event Management) and network analysis tools, techniques and procedures to detect malicious activity.

- You will be responsible for the Corporate SIEM servers and application software environment, working with others within the Operations team where necessary to:
    - Install and configure SIEM applications.
    - Configure data collector and provider pairings from:
        - Server Infrastructure.
        - Storage infrastructure.
        - Network switch Infrastructure.
        - Network Security Infrastructure.
        - Endpoint Security software.
    - Develop and deploy event filtering, action and reporting solutions.

- Analyse the SIEM reporting and make recommendations to reduce the number of 'false positive' events that infrastructure equipment produce.

- Highlight the SIEM reporting events that are suspicious or otherwise unusual for further investigation by the system owner.

- Provide support as necessary to the Information Security Manager in the event of a significant or major security event or data breach which may or may not have been identified by the SIEM solution.

- Provide additional assistance for ICT Operations projects, ensuring that SIEM is considered in their design and deployment or by utilising core Infrastructure skills directly as a project resource.

- Provide documentation and ad-hoc training to support the SIEM solution and configuration on an ongoing basis.

- Comply with WBC health and safety policies, procedures and rules, taking reasonable care of yourself and others.

- Adhere to the standards set out in the WBC competency framework.

- Integrate this SIEM (Security Onion) system into

Scope (impact on / control of resources, people, money etc)

- The Security Information Event Management (SIEM) Analyst plays a critical part in ensuring the security of West Berkshire Council and is involved in the monitoring and investigation of security events and incidents.

- Although the individual will not manage any direct reports, the post requires an individual with highly specialized skills to understand SIEM methods, systems and processes, and will be required to engage and interact with the Information Security Manager, as well as other ICT colleagues and Digital, Data and Technology (DDaT) professionals to problem solve and implement solutions for improved security within the WBC ICT environment.

- During periods of cover and / or whilst performing delegated tasks, this post may assume a very high level of responsibility.

- Operational decisions are expected that can impact the security and operation of the entire ICT Infrastructure, impacting on all of Council activities.

- The work carried out by the SIEM Analyst impacts on all individuals across the entire council. This is not a result of direct interaction, but rather by maintaining appropriate levels of security, privacy and resilience of the SIEM system, to protect our people, data, operations, and facilities from harm.

- This individual does not have budgetary control within this post.

West Berkshire Council is proud to be an equal opportunity employer. We embrace diversity and are committed to creating an inclusive environment for all employees. All employment is decided based on open and fair competition, merit and business need.

Person Specification	
Qualifications	**Essential / Desirable**
Educated to A-Level standard or equivalent (a focus on IT and/or cyber security).	**E**
Recognised qualifications in one or more of the following disciplines: Unix/Linux Server; Windows Server (2016/2019); Active Directory; MS Exchange; Citrix and Application Packaging; Anti-Virus Systems; LAN/WAN Networking; vmWare; SCCM.	**D**
A basic understanding of networks, Transmission Control Protocol (TCP) and Internet Protocol (IP), and other standard protocols such as Domain Name Service. (DNS), (Hypertext Transfer Protocol (HTTP), etc.	**E**
Experience	
A minimum of 2 years ICT Infrastructure experience in a Unix/Linux/Windows environment.	**D**
Has worked with Cyber Security tools, and understands how to highlight SIEM reporting events, to assist with further investigation and proposed solutions.	**D**
Knowledge and understanding	
Must be able to demonstrate knowledge of ICT Operational and Support techniques.	**D**
Ability to identify and report error conditions on a wide range of hardware and software platforms.	**D**
Skills and abilities	
Proven problem solver.	**E**
Technical Skills in – Microsoft Windows Client & Server Operating Systems Unix/Linux – Ubuntu/CentOS Anti-Virus and Security IT Networks	 **D** **D** **D** **D**
High level of practical skill and experience relating to Cyber Security and/or SIEM	**E**
Self-Starter / ability to work with minimal supervision.	**E**
An effective communicator and able to operate as a key member of the information security incident team, engaging with colleagues within this specialist area, to influence the resolution, through analysing, requesting and transmitting information for clarification, to achieve the required end result.	**E**
Able to forward plan over a period of weeks and months to deliver the outputs of this Security Information Event Management (SIEM) post.	**E**
Work-related personal qualities	
Attention to detail & quality of work produced.	**E**
Creativity / problem solving.	**E**
Proven ability to learn new tasks, whilst doing and completing current tasks.	**E**
Plan and organise own time to complete the complex task of SIEM reporting analysis, and resolution.	**E**
Awareness & adherence to standards and mitigation of risks.	**E**
Other work-related requirements	
Must be prepared to work outside normal business hours as situations demand.	**E**
Ability and willingness to travel occasionally.	**D**
This role has been identified as public facing in accordance with Part 7 of the Immigration Act 2017; the requirement to fulfil all spoken aspects of the role with confidence in English applies	**E**

Enhanced DBS check with relevant barred list/s	No
Is this post politically restricted?	No