**Job Title** Cyber Security Operations Analyst

**Reports to** Technical Network Manager

**Job Purpose**

The IT Department provides, manages, and supports all aspects of IT life at the College. The Cyber Security Operations Analyst at Eton College is tasked with the active monitoring and support the defence of Eton’s network and fostering a culture of security awareness among pupils and staff. In addition, this role would assist in analysing and providing reports to the safeguarding team on safeguarding and pastoral matters, supporting their work with relevant insights and data.

**Key Tasks and Responsibilities**

* Work with the Technical Network Manager and network support provider to ensure cyber resilience across the network;
* Work alongside the IT Technical Network Manager in all projects, and support ownership of the security aspects of any such project;
* Manage monitoring tools and provide regular reports relating to safeguarding and other pastoral requirements as directed by the Technical Network Manager;
* In co-operation with other senior member of the IT Department, develop and implement policies and procedures for IT network security matters;
* Complete network monitoring, packet analysis, protocol analysis and data visualisation in conjunction with the Technical Network Manager;
* Monitor and provide regular reports on the security of Eton’s network environment;
* Manage and maintain all network security appliances and software systems deployed on the College network in conjunction with the Technical Network Manager;
* Create and provide regular reports on the security of the College’s network systems and safeguarding and pastoral data, any threats to which the College is vulnerable or has been subjected, and any actions taken;
* Specify, deploy, manage and maintain any security system or process aimed at protecting Eton’s systems, data, interests or reputation in conjunction with the Technical Network Manager;
* Make recommendations to the Technical Network Manager of any changes or additions to Eton’s IT environment that would improve the security of the network topology;
* Ensure all aspects of the College’s IT network security are accurately documented, and that this documentation is regularly updated and available to other members of the IT department;
* Provide regular training to the College’s user base on cyber security, advising staff and pupils on best practices and explaining systems and processes in place for their protection;
* Keep up to date with current and emerging threats, trends and industry best practices;
* Work as directed by the Technical Network Manager or Director of IT;
* Be a highly motivated team player with the skills and ability to manage changing priorities;
* Be willing to attend internal and external training as necessary to keep up to date with the latest technology and internal system processes;
* Work within industry standard legislation, policies and procedures;
* Undertake other duties not specifically stated which from time to time are necessary without altering the nature or level of responsibility;

**General & College Responsibilities**

* Participate in training and team development activities, to update knowledge and skills:
* Be aware of and comply with the health and safety legislation and other College requirements that are relevant to his/her post.
  + All employees have a general duty in law to take reasonable care for the health and safety of themselves and of other persons who may be affected by their acts or omissions.
  + Understand and be committed to the College’s Health and Safety Policy statement and the College’s safety priorities and be aware of his/her contribution to such priorities
* Demonstrate commitment and enthusiasm to promote the principle of equality and diversity in employment and service delivery:
  + Be familiar with and promote the Equality and Diversity Policy.
* Be familiar with Safeguarding requirements as outlined in the Safeguarding Policy and comply with its requirements to safeguard and protect the welfare of children, young people and vulnerable adults.
* Undertake such additional duties or projects as the Head of IT Systems may determine from time to time, after consultation with the post holder.

**Skills and Competencies Required**

To be successful in this role, the incumbent should have:

* Excellent knowledge of Microsoft Windows Server Operating Systems and Linux;
* Scripting experience using Python and bash (essential)
* Experience using and ingesting data from Splunk and other monitoring tools (essential)
* Knowledge of networking protocols and investigation (capture, Wireshark)
* Competence with computer, server, and peripheral hardware;
* Excellent knowledge of networking topologies, standards, terminologies, and operation;
* A thorough understanding of the cyber security threat landscape;
* A good standard of written and oral communication;
* Ability and willingness to provide user training on security topics, whether in an individual, group or forum setting;
* Ability to work effectively within a team environment, both taking direction from and supporting other colleagues;

You may also enjoy this role if you have:

* Excellent technical skills and a friendly and helpful manner;
* A demonstrable aptitude and enthusiasm for information and communications technology;
* Confidence and willingness to build on knowledge acquired to date;
* Effective communication skills and ability to work well in a team environment;
* Ability to organise and prioritise workloads;

**Hours of work**

This role is for 35 hours per week, worked over 52 weeks per annum with 21 days paid holiday entitlement, plus bank holidays. The hours of work are not fixed but would usually be between 9.00am and 5.00pm on weekdays. Some flexibility is required as a response to peaks in workload.

**Disclosure Checks**

**Eton College is committed to safeguarding and promoting the welfare of children, and applicants must be willing to undergo child protection screening appropriate to the post, including, but not limited to, reference checks with past employers, an Enhanced Disclosure from the Disclosure and Barring Service (including Barred List information), an online search and, where applicable, Prohibition checks. If you are successful in your application, you will be required to complete a DBS Disclosure Application Form.  Any information disclosed will be handled in accordance with any guidance and/or Code of Practice published by the DBS. The College is exempt from the Rehabilitation of Offenders Act 1974 and therefore all convictions, cautions, reprimands and final warnings (including those which would normally be considered as “spent” under the Act) must be declared, subject to the DBS filtering rules. It is a criminal offence for any person who is barred from working with children to attempt to apply for a position at the College.**