# (Chosen for application) Job 1 – Security SOC (Security operations centre) analyst @ Government Digital Service

Salary: £34,550 - £38,580 (negotiable depending on experience.)

Locations: London, Bristol, Manchester

Type: Permanent

Hours: Full time (37 hours a week)

My role:

* Improving the detection capabilities of cyber threats and incident response times.
* Identifying, analysing and investigating security alerts and managing security incidents.
* Working in technical teams to improve the security of their services.
* Research into new and evolving threats, threat actors and vulnerabilities.
* Promote good practices across the organisation.

What they’re looking for:

* An interest in cyber security.
* Naturally inquisitive minds, showing proactive approaches to investigation in a work or educational environment.
* Analytical and interpretational skills towards data.
* Knowledgeable of current vulnerabilities and how to remediate them.
* Confident in Linux, mac and windows platforms, along with python and bash.
* Excellent communication skills.

Benefits:

* Activities to improve your mental and physical wellbeing, including yoga and meditation.
* A personal training budget you can use for training courses, books or conferences.
* 25 days annual leave. Plus, an extra day off for the Queen's birthday.
* In-year bonus scheme.
* Civil service pension. Average employer contribution of 27%.
* 12 weeks of full pay for maternity, paternity or adoption leave.

Further Research:

I picked job 1 (Security SOC analyst @ Government Digital Service) to apply for as I believe working in the public sector for my first job out of my degree will provide me with good experience for moving into the private sector later in life. While I might not have access to benefits such as the civil service pension if I chose to leave the job after a period of time, I believe the increased salary I would be able to negotiate with the experience I’ve gained will make up for this.

Through research into the GDS it’s become apparent that it is a pleasant place to work, with policies in place to make new recruits feel welcome such as the “Its okay” posters on the office walls (It’s ok to say what’s ok - Government Digital Service, n.d.).

# Job 2 – Cyber Security Analyst @ Microsoft Security Response Centre

Salary: Not stated

Locations: Cheltenham

Type: Permanent

Hours: Not stated

My role:

* To perform forensic investigations on suspected compromised assets, to determine what occurred.
* Collaborate with the team to create adversary eviction and incident remediation plans.
* Build and develop the forensic program through expertise, collaboration, and influence.
* Automate response and forensic functions through coding and scripting.
* Evaluate security risks and their impact to the Microsoft Cloud platform and its online services.
* Create technical documentation for other analysts and other teams to follow.

What they’re looking for:

* Experience in performing forensic analysis of digital files and physical media from a wide array of operating systems and application software.
* Experience in responding to, investigating and recovering from compromise and data breach events.
* One or more of the following qualifications: CFCE, GCFA, GNFA, GCIH, GCFE, OSCP, CISSP.
* Experience in developing services or scripts for automation of analysis, response or forensics.

Benefits:

(These benefits are very vague with no easily accessible information about them online, this would be a key point I would raise in interview if I were to apply.)

* Industry leading healthcare
* Savings and investments
* Giving programs
* Educational resources
* Maternity and paternity leave
* Opportunities to network and connect
* Discounts on products and services
* Generous time away

# Job 3 – Cyber Security Engineer @ Thames Water Utilities

Salary: £45,000 - £50,000

Locations: Reading

Type: Permanent

Hours: Does not State

My role:

* Working as part of a team to ensure that corporate data is safeguarded.
* Maintaining tools to ensure availability.
* Maintain vulnerability scanning infrastructure.
* Assess potential risks and opportunities of vulns in the network.
* Developing methods to ensure teams comply with security policies.
* Actively look for enhancements to SOC security processes.
* Maintaining internal KPI dashboard for highlighting system capabilities.
* Creating and maintaining knowledge base and end user documentation.

What they’re looking for:

* Previous experience being a sysadmin on both windows and linux estates.
* In-depth knowledge of networking and DNS.
* Understanding of both physical and virtual checkpoint firewalls. How to monitor, tune and update them.
* Knowledge of Cyberark.
* Keen interest in technology, with an ability to understand the basics and application of automation scripts and security tools.
* Be able to produce quality documentation.
* Keep up to date with the latest vulnerabilities and threats.

Benefits:

* Competitive salary.
* 26 days of holiday.
* Annual pay review.
* Loyalty reward scheme.

# References:

It’s ok to say what’s ok - Government Digital Service. (n.d.). Gds.Blog.Gov.Uk. Retrieved November 20, 2020, from https://gds.blog.gov.uk/2016/05/25/its-ok-to-say-whats-ok/