## Specialism

Information management and security

## Experience Statement

### Breadth of Knowledge

After graduating from the University of Edinburgh with a degree in Computer Science and Artificial Intelligence I joined Logica PLC as a developer. As part of the Space Division I took the opportunity to work at the European Space Agency in Germany developing satellite control software and being part of the launch support team. Following my work at the ESA I began developing Websites using technologies including Perl/CGI, ColdFusion, MySQL, SQL, ASP “classic”, and ASP.net. By moving through several smaller consultancy companies I completed work as a full-stack developer for large clients such as McDonalds, Virgin Cars, Marks and Spencer’s, and Thomas Cook.

Since joining the Bank of England as a developer working on data collection and analysis systems I have held several roles including Technical Lead, Team Lead, Operations Lead, Software Security Trainer, and subject matter expert for ALM and CI/CD tooling. These skills aided in my work to create a team of Secure Code Champions as a centre of excellence for secure coding practices. I also helped to introduce Agile working practices to developer teams within the Bank and promoted the use to tooling for work management, version control, and release management. I implemented the infrastructure and tooling necessary to allow CI/CD to be adopted by teams to ensure secure and repeatable deployments.

I am now a Security Analyst working within the Cyber Security Division. My responsibilities include threat and vulnerability management, continuous monitoring of Bank assets and running CSIRTs for critical vulnerabilities. CSIRTs are required whenever a vulnerabilities has been identified within the Bank and remediation actions are required. As the CSIRT manager it is my responsibility to engage with the necessary teams, formulate an action plan, and oversee any remediation.

I have also been tasked with creating Cyber Data Analytics team within the division to create a Cyber data repository and reporting system. The system will gather data from disparate sources into a single source of truth using automation including APIs and ETL processes. The data will then be used to create reports and visualisations for stakeholders at all levels of management to help with data-driven decision making.

With the introduction of the Agile methodology across the Bank, I have become an Agile practices SME for Cyber Security, and administrator for our work management system, JIRA. I am responsible for the training of staff across the Bank to the new working practices and tooling, including providing guidance to teams who have never used the methodology.

Within the Bank I am a Technology Ambassador and help my engaging with students from state secondary schools across the UK to promote working in the Bank of England. Outside of the Bank I am a STEM ambassador for my county and school governor responsible for ICT.

### Autonomy

Most recently the CISO gave me his vision of a centralised source of Cyber data to be used to produce reports allowing for data-driven decision making. After working to develop a PoC I was given budget for additional resources and was responsible for the recruitment, on-boarding, and induction process. This has created a new Cyber Security Analytics team within the division for which I am responsible.

I have worked with a numerous teams to help with identification and classification of their data. To help with this I have created an on-boarding process to allow my team to develop the ETL and reporting procedures for the ingestion and visualisation of data.

With the introduction of Agile working practices I have taken the role of Product Owner and I am responsible for formalising the vision and objectives for the project as well as the roadmap for delivery. I am in charge of stakeholder management and the creation User Stories, and tasks for the SCRUM project. I manage the development team on a daily basis and report our progress to the Delivery Manager, Programme Manager, Cyber Security Leadership team, and the CISO.

The CyberMI system will have increased visibility due to the reports being generated providing data to all levels of management including the Bank’s executive board.

This work is in addition to my work on the Continuous Monitoring and report of the Bank’s assets for security vulnerabilities and running CSIRTs when required.

### Influence

My work to collect and report on data from numerous sources has required me to interact with teams throughout the Bank including the Cyber Security Division. The relationships I have built have allowed me access to resources normally kept within silos and in turn helped me influence how these resources are handled internally. My requirements have helped formalise how some teams collect data from their own systems and provide access to stakeholders.

As part of my Threat and Vulnerability Management (TVM) role I am responsible for triaging and collecting information on vulnerabilities. Following a review of information from numerous sources, recommendations are made on the need for remediation, patching, or improved processes. In extreme cases, such as the identification of a critical vulnerability, I am responsible for the formation and management of a CSIRT and overseeing of any actions of remediation. CSIRTs require working with teams including the Cyber Defence Centre, incident management team, and system owners to ensure that the Bank remains secure.

To aid in future CSIRTs I have created a TVM “playbook”. This is a process document to dictate the steps needed to run a CSIRT, who the main contacts are, and record the actions undertaken. This will act as a record of incidents and an instruction manual for other members of the team.

### Complexity

My role as Cyber Security Analyst have three responsibilities: Threat and Vulnerability Management (TVM), Continuous Monitoring (CM), and team leader of the Cyber Security Analytics (CSA) team.

My TVM responsibilities include providing advice and guidance to other teams within Cyber Security, and when necessary forming and managing a Cyber Security Incident Response Team.

CM requires me to be an SME for our information security and compliance system, Qualys, as well as support and maintain the service. I am tasked with the management and training of users to allow them to report on the systems for which they are responsible. This has included the move from an on premise solution to a cloud service and the introduction of new data zones within the Bank.

As the leader of the CSA team I am responsible for the delivery of the CyberMI Reporting system. This system performs automated ETL and reporting process to allow managers to make data-driven decisions. I am the Product Owner for the project and responsible for stakeholder management as well as the creation of User Stories for users across the Bank.

Beyond my Security Analyst role I am the Agile methodology and tooling SME for the Cyber Security Division. I am responsible for the training of staff and support of the JIRA system for my colleagues within Cyber as well as providing guidance on best practices for KANBAN and SCRUM.

### Business Skills

My experience as a manager and working within different areas of the Bank has allowed me to utilise relationships to support the work on cyber data analysis. I have created processes and controls for requirements capture and the on-boarding of new data feeds to ensure they add to our vision and enhance our capability. I have worked as an ambassador for Cyber Security to the business to ensure any data being added to the system adds value to our business stakeholders. The data enables the business to view the security posture of their system in simple terms and allows them to calculate risk and plan future work. This process has been communicated to all data owners to help them formalise any data feeds to be ingested by the system, and increases our velocity for on boarding.

As a developer I became interested in secure coding and insider threats, creating and running training courses for other developers. This interest lead me to increase my knowledge of cyber security by helping with Cyber Security events. Now, as part of the Cyber Security division, I regularly attend conferences and utilise my access to online learning resources such as LinkedIn learning. Though self-paced study I am also working towards my CISSP exam.