Daniel Murphy

Nottingham, United Kingdom 07895 999209 danhatesnumbers@gmail.com

Personal Statement

With a wide range of skills developed through roles in Application Security, Security Consultancy, Quality Engineering and Software Engineering, I'm a fast learner who thrives on interesting problems.

As security practitoners I believe we have a responsibility to the teams we support to provide secure defaults and good guardrails for when they need to deviate from those defaults. I'm looking for a role that encourages experimentation, embraces learning from failure and where my work has real meaning.

Professional Experience

Staff Application Security Engineer (Remote) at Simply Business *May 2019 - present*

At Simply Business, I have had a range of responsibilities including:

- Working with our Cloud and Platform Engineering team to threat model the architecture of a new CI/CD system built on Github Actions and AWS CodeBuild
- Mapping out possible privilege escalation routes in the IAM policies and role trust relationships used by our CI/CD system, looking at options to remove, control or audit the use of risky IAM actions and apply the principle of least privilege to the actions available to build pipelines
- Supporting an engineering team with the design and implementation of a non-standard OpenID Connect integration with a large bank and a mechanism to exchange data between two internal systems that must take place in the user's browser while maintaining confidentiality, integrity and authenticity
- Building a service to validate the integrity of AWS CloudTrail log files across more than a dozen accounts aggregated to central S3 buckets as a trusted source of data for our SIEM
- Leading a project to design and build a system to collect data from open source security tooling to enable data-driven decision making and provide centralised visibility into the security of our application portfolio, which was opensourced as Kiln
- Mentoring less experienced team members through pairing sessions, providing technical and professional guidance and serving as a point of escalation for removing impediments
- Participating in incident response in support of our SOC
- Supporting our assurance team to write and review security policies and prepare for an audit

Information Security Consultant at Capital One *August 2018 - May 2019*

In this role I supported feature teams with advice on secure development practises, participated in Threat Modelling sessions, reviewed infrastructure designs for systems in both AWS and on-premises environments, and produced self-service guidance and advice. The teams I consulted for were responsible for a range of different products and used a wide variety of technologies, which required me to effectively juggle competing priorities and cope with frequent context switching. I initiated a piece of work with the AppSec team and the development owner of the online account servicing platform to triage security findings, advise on options for remediation and prioritise open findings.

Quality Engineer at Capital One *November 2016 - August 2018*

As a Quality Engineer at Capital One, I helped to deliver a project bringing the online account servicing platform in-house. As part of this project I participated in story refinement, defined the testing approach used by my team, developed automated functional tests, and conducted knowledge sharing sessions to help the team become more cross-functional. While in this role, Capital One launched it's first iteration of a Security Champions program, which allowed me to start introducing Security aspects to my role. I presented a walkthrough of a Boot2Root VM I had recently completed to this forum, which inspired another member of the community to investigate Java Deserialisation vulnerabilities and present on the topic.

Graduate Software Engineer at Gala Coral Group *May 2014 - November 2016*

My role at Gala provided me with an excellent opportunity to tackle a variety of engineering challenges including: building functionality for a suite of internal iOS applications built on the Xamarin C# mobile app platform, resolving technical debt in business critical codebases, building a virtualised OS X build environment for iOS apps using VMWare ESXi and implementing Continuous Integration for a number of existing mobile apps, web apps and a large desktop app using TeamCity.

Software Engineer Industrial Placement at ARM *June 2012 - August 2013*
While working at ARM, I was part of a team of engineers embedded in the Marketing Communications department. My focus was on building prototypes that showcased ARM technologies with specific marketing goals. I also represented ARM at industry events explaining technical demonstrations to partners and members of the public.

Skills & Knowledge

Security

- Facilitating Threat Modelling sessions and teaching this skill to fellow security engineers
- Understanding of cryptographic primatives, protocols and how they can be applied to meet security objectives
- The OAuth 2, OpenID Connect and SAML standards, and their uses for single sign on and delegated authorisation
- AWS IAM policy authoring and security review
- AWS security controls, e.g. SCPs, CloudTrail, VPC flow logs, Security Groups & NACLs
- Working familiarity of PCI-DSS

Engineering

- Strong Rust and Python knowledge and proficiency in Bash scripting, Ruby and Javascript
- Linux Containers and orchestrating them with AWS ECS
- Building distributed systems on AWS
- Ansible, Terraform, Packer, Vagrant
- Unit, functional and integration testing
- Git
- CI/CD with Jenkins and Github Actions
- Kafka & Event Sourcing Architecture

Core Competencies

- Resolving ambiguity and clarifying value to stakeholders with varying levels of technical expertise
- Communicating the likelihood and impact of security risks as well as mitigation options to technical stakeholders without a background in security
- Researching unfamiliar problem spaces and technologies and producing digestable presentations for my team
- Scrum practices
- Technical writing and diagramming

Presentations

Building a Data Driven AppSec Programme with Kiln at BSides Leeds 2020
This talk showcased an open source project I lead at Simply Business which integrates security tooling into CI/CD pipelines, collects that data and enables teams to make data-driven security decisions. In preparation for this talk, I built a test environment in a Kubernetes cluster using Kops to host the services that power Kiln. Data collected by running Kiln over the commit history of a selection of open source projects was analysed using Python in JupyterLab to demonstrate to attendees how the collected data can be utilised.

Recording: https://www.youtube.com/watch?v=pygDNLc7HE8
Demo environment: https://github.com/simplybusiness/Kiln/blob/main/docs/quickstart/README.md
Data analysis: https://github.com/simplybusiness/Kiln/blob/main/docs/data-analysis/README.md

Education

Nottingham Trent University September 2010 - May 2014
BSc Computer Science 1st Class (Hons)