

George Gilligan

Email: ggilligan12@gmail.com | Personal Site: gilly.tech | GitHub: github.com/ggilligan12

Security Engineer, Golang, C# and Python developer, Ballroom Dancer and Competitive Hacker.

EXPERIENCE

Thought Machine, Security Engineer

London, March 2022 - Present

- Deployed and maintained Falco (container runtime monitoring agent) for >2000 compute instances.
- PoC'd CloudQuery for asset inventory with K8s source and Elasticsearch sink.
- Worked as detection engineer, SOC Analyst and incident responder with TheHive, ELK stack and Elastalert detections.
- Wrote Semgrep and OPA static analysis tests and autofixes to improve container security contexts.
- Designed and implemented root user management policy for GCP estate.
- Wrote Go microservices for AWS AMI scanning, and blocking release pipelines with serious vulnerabilities.
- Delivered presentations to colleagues on intrusion detection, binary exploitation, K8s security contexts, and static analysis.
- Organised hosting of 2 meetups of the OWASP London chapter.

Trading Hub, Software Engineer

London, June 2020 - March 2022

- Wrote interactive dashboards in .NET web app to delegate granular control of EC2's to non-infrastructure instance owners.
- Wrote Powershell running tool in .NET web app, allowing developers to save down clearly documented, parameterised scripts for intuitive use via GUI by less technical users.
- Helped design and develop a WORM compliant backup storage pipeline using C# and S3 Glacier.
- Maintained and supported custom C# automatic deployment and cloning pipelines for client EC2's.

SIGINT Edinburgh (University Cybersecurity Society), Secretary

Edinburgh, June 2019 - June 2020

- Wrote, organised, promoted, and secured sponsorship for Capture the Flag (CTF) competitions and other technical events, including the first edition of *pwnEd*, Scotlands largest CTF, now past its 4th iteration.
- Travelled with fellow committee to conferences and competitions nationwide and overseas.

Metaswitch Networks, Software Engineer (Intern)

Edinburgh/London, May 2019 - August 2019

- Added *Liquid Templating* to Ruby on Rails based diagnostics tool. Deleted thousands of lines of code with no functionality lost.

CERTIFICATIONS

Offensive Security Certified Professional (OSCP): 24 hour practical penetration testing exam and report. Passed at first attempt in October 2023 after 3 months of intensive evening study. Course assessed abilities in enumeration, gaining footholds, privilege escalation, post exploitation and pivoting. Abilities tested in Linux and Windows standalone machines, and Active Directory networks.

SKILLS

Programming Languages:

- **Proficient:** Go, Python
- **Intermediate:** Bash, C#, Powershell

Technologies & Libraries:

- **Proficient:** Kubernetes, Git, Terraform, VS Code, AWS (various services), GCP (various services), Falco
- **Intermediate:** Docker, ELK, Vector, Filebeat, Helm, OPA, Semgrep, CloudQuery, Grafana, SVN

TEAM EVENTS

Deloitte CTF Qualifier 2019: Took 3rd place in the 2019 Deloitte CTF Qualifying round with the SIGINT 2nd team, beating 40 other university teams nationwide. Unfortunately could not qualify for the final as only one team per university was admitted.

Scottish Universities Cybersecurity Challenge 2018: Took part in competition run by BAE, National Grid & BT. My team won the CTF and came 2nd overall when factoring in the Social Engineering & Incident Response challenges.

Hack Harvard 2018: Worked with team to build "*HexLedger*", a hacker profiling app built on a multichain blockchain with a front end made with WixCode. We won "Most Useless Hack" out of over 200 teams. By far my teams proudest achievement.

Oxford Hack 2017: Created "*IOTea*", a tea brewing robot controlled via web app. We won Netcraft's "*Best Hardware Hack*", MLH's "*Most Ergonomic Hack*", Facebook's prize for "*Aligning with their vision*", and were overall competition finalists out of 100 teams.

EDUCATION

University of Oxford

2023 - 2026 (Expected)

Postgraduate: Software & Systems Security MSc (Part-time)

- **Structure:** Part-time study alongside full-time employment consisting of 10 1-week in-person intensive courses over ~3 years.
- **Topics:** Forensics, Malware, Incident Management, Network Security, Secure Programming

University of Edinburgh

2016 - 2020

Undergraduate: Computer Science & Mathematics BSc (2:1)

- **Topics Studied:** Algebra, Calculus, Statistics, Algorithms, Security, AI, ML, NLP, Quantum Informatics