George Gilligan

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

Security Engineer/Detection & Response for Kubernetes, the Cloud, and on-prem. Python dev, boulderer, ballroom dancer.

Experience

Marshall Wace Asset Management, ***Security Engineer*** London, *May 2024 - Present*

- Provided framework for SIEM config to be written in Terraform.
- Tagging exercise to migrate 1000 detections from one EDR vendor to another without loss of coverage.
- Wrote framework to manage all detections as code. Cronjobs to merge rules from upstream, CI workflow to validate and push rules to SIEM after PR, and CLI tooling to import rules from SIEM to code.
- PoC'd MCP-style (not MCP) Agent for the SOC with tools (no resources) using weird internal framework.
- Wrote Falco pre-commit hook to validate rules before deployment.
- Security operations and response responsibilities for heterogeneous Windows/Linux on-prem/cloud organisation.
- Managed 2 graduate engineers and supervised their projects.

Thought Machine, ***Security Engineer*** London, *March 2022 - April 2024*

- Deployed brand new GCP Organisation with secure root user management and organisation policies.
- Worked with clients to ensure that the product we shipped would comply with their Azure Policy requirements.
- Safely executed multiple upgrades of AWS EKS cluster, as well as upgrades to Elasticsearch cluster, and ECK Operator.
- 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.
- Wrote Go microservices for Detection Testing, 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 3 meetups of the OWASP London chapter, giving a talk on E2E Detection Testing at the most recent one.

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 6th iteration.
- Travelled with fellow committee to conferences and competitions nationwide and overseas.

Metaswitch (now part of Microsoft), ***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 in October 2023.

Technologies

- **Proficient**: Python, Kubernetes, Git, Terraform, VS Code, AWS (various services), GCP (various services), Falco, ELK
- **Intermediate**: Go, Bash, C#, Powershell, Docker, Helm, OPA, Semgrep, Grafana, Kapitan, Kustomize

Education

University of Oxford 2023 - 2025 (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 ~2 years.
- **Topics**: Forensics, Malware, Incident Management, Network Security, Secure Programming, Trusted Computing

University of Edinburgh 2016 - 2020

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

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