

Jack Tricker

email: me@jacktricker.com | web: jacktricker.com

RELEVANT EXPERIENCE

Dunnhumby

Security Operation Engineer

London, UK

Jan 2025 - Current

Security Engineering:

- Own, Manage and Deploy **WDAC (App Control for Business)** Policies across servers and endpoints
- Monitor audit logs and access impact of changes to policies across the organization
- Investigate and Control application usage and security events
- Write and Maintain **Powershell** and **CI/CD** to manage policies
- Work with **Intune** to scope, update and maintain security controls
- Application Security tasks involving **Code Review** and Architecture Review
- Maintain and Update **IAC (Infrastructure as Code)** repositories
- Create metrics and visibility using **Qualys / KQL / Defender** for Security Issues
- Conduct training for Associate members of the team in Scripting and Tooling

EndeavourX

Cyber Security Engineer

Sydney, Australia

Sep 2021 - Dec 2023

Security Infrastructure:

- Managed **CrowdStrike** (EDR), including automation for threat mitigation.
- Administered **Cloudflare** (WAF, zone/user management) via Terraform.
- Integrated **Zero Trust** network principles for secure access.
- Led the transition from **Microsoft Sentinel** to **Hive** for incident response, integrating MISP and Cortex.
- Developed an **email sandboxing solution** using Google Mail, Joe Sandbox, and Azure Functions.

Incident Response:

- Investigated and mitigated security incidents using various security tools.
- Created **custom remediation scripts** for CrowdStrike & Cloudflare APIs.

Reporting & Documentation:

- Built **automated security dashboards** for leadership insights.
- Centralized logging via **Microsoft Sentinel** for real-time threat detection.

KEY SKILLS

Code: Python, JavaScript, Rust, Go, Terraform, Powershell, Bash, KQL, SQL

Services: Cloudflare, CrowdStrike, Azure, AWS, GCP, Docker, Kubernetes, Sentinel, Splunk

EDUCATION

University of Liverpool: Bachelor of Science with Honors in Mathematics

2011-2015

Microsoft AZ-900: Microsoft Azure Fundamentals

2021

Self-Directed study for OSCP: via HackTheBox/TryHackMe

2020-2021