Nathan Millwater

Security Operations Engineer

nathan@millwater.io · LinkedIn · Hack The Box

Profile

I am a security operations engineer, with 12 years experience designing and operating technical security controls. I have worked primarily at businesses within the regulated financial services sector, as well as within MSSP organisations.

I currently build, operate, and automate security solutions at a UK clearing bank. I work across multiple domains from detection engineering, incident response, identity & access management, vulnerability management, and other cyber controls.

I combine hands-on engineering with line management and stakeholder communication, translating technical risk into practical recommendations all areas of the business can follow.

Outside work, I run a self-hosted homelab, take part in Capture the Flag challenges, and volunteer at a local cat rescue.

Experience

Security Operations Engineer, ClearBank — August 2022 – Present

- Delivered business-wide rollout of passwordless authentication; built enforcement with Terraform-managed Conditional Access Policies.
- Managed SIEM detection engineering; introduced test-driven rule validation and measurably improved detection rule fidelity.
- Designed the internal vulnerability-assessment and management programme; implemented custom-built AI Agent driven prioritisation automation workflows.
- Engineered automated control testing and reporting; supported internal/external audit attestations (including ISO 27001).

Senior Vulnerability Management Analyst, Bridewell — September 2021 – August 2022

- Delivered managed vulnerability management for CNI clients across aviation, finance, and energy, managing large-scale vulnerability assessments across IT & OT environments.
- Built reporting frameworks integrating different vulnerability assessment tooling into single-pane-of-glass views using Python and PowerBI.
- Assessed emergent CVEs and produced executive summaries of risk; guided clients through prioritizing remediation actions tailored for their environments.

Cyber Security Officer, Pepper Money — April 2019 – September 2021

- Designed and implemented end-to-end vulnerability-management procedures and automated remediation reporting across user endpoints and cloud estate.
- Developed and maintained Microsoft Sentinel SIEM detections, improving detection coverage and establishing incident response for the business.

- Performed cyber risk assessments, maintained security policies and standards, and presented cyber risk reports at monthly director-level information-security forums.
- Enabled secure digital transformation by championing automation workflows and helping teams build and use solutions securely.

Senior Web Security Analyst, Alert Logic — March 2015 – April 2019

- Operated customer WAF deployments in a managed security service, maintaining protection policies and controlled changes across a wide range of clients.
- Advised customers on emerging web application vulnerabilities and deployed rulesets to mitigate threats.
- Contributed bug fixes to a proprietary WAF product and built internal tooling, improving threat detection reliability for the managed service.

Technical Analyst, CGI — July 2014 – March 2015

- Delivered KPI-driven first-line technical support for a healthcare service, resolving tickets to meet strict SLAs.

Credentials

- **Blue Team Level 2 (BTL2)** — Centri — April 2026
- **Blue Team Level 1 (BTL1)** — Centri — February 2025

Education

University of South Wales — MComp in Computer Security (with Merit) — September 2010 – June 2014

Skills

Technologies - Azure Logic Apps - KQL - Microsoft Azure - Microsoft Defender - Microsoft Entra ID - Microsoft Sentinel - Power BI - Python - Tenable - Terraform

Security Operations - Detection engineering - Incident response - Infrastructure as code (Terraform) - Security automation

Identity and Access Management - Conditional Access - Passwordless / passkeys

Vulnerability Management - AI-assisted vulnerability prioritisation - IT / OT vulnerability assessment - Risk-based prioritisation - Vulnerability management - Web application security / WAF

Governance - Control testing - Cyber risk assessment - Cyber risk reporting - ISO 27001

Leadership - Director-level reporting - Line management / mentoring