Elliot Buckland-Weir

Nottingham, UK | 07496 145641 | Elliot.buckland-weir@outlook.com | elliotweir.co.uk

Professional Profile

Junior Security Analyst with hands-on experience across Microsoft 365 security, endpoint management, identity governance, email security, vulnerability remediation, and security operations. I focus on reducing manual work, tightening controls, and building tools that help with investigation and reporting.

Experienced in Microsoft Intune, Entra ID, PAM/PIM, SOC/SIEM alert handling, and enterprise security tooling. Recognised for being proactive, reliable, and technically curious, with a strong focus on improving security processes, reducing risk, and supporting secure service delivery.

Major Achievements

- Created policies and SOPs governing hardware compliance and external sharing across SharePoint Online, Microsoft Teams, and Entra B2B, improving governance and reducing data leakage risk.
- Designed and implemented Jira workflow automations to streamline security support processes and reduce manual workload.
- Produced the organisation's IT Security Executive Report, providing leadership with clear metrics, trends, and risk insights.
- Played a key role in taking the Microsoft Intune project from initial setup to live service within three months.
- Supported the implementation of BeyondTrust PAM and Microsoft PIM, strengthening privileged access control and just-in-time access governance.
- Acted as the internal lead for a third-party SOC/SIEM service, reviewing, actioning, and escalating security events.
- Became the team's email security platform SME, providing daily administration, troubleshooting, and B2B integration support.

Key Skills

Microsoft Security & Endpoint Management Microsoft Intune, Autopilot, Apple Business Manager MobileIron to Intune migration Configuration profiles and compliance policies	**Identity & Access Management** Entra ID and Conditional Access Privileged Identity Management (PIM) Privileged Access Management (PAM) External collaboration governance
Security Operations SOC/SIEM alert review and escalation Incident response support Vulnerability management Phishing simulation and user awareness	**Email Security** Email security platform administration Targeted Threat Protection Secure Messaging and Large File Send B2B integration support
Governance & Compliance SOP and policy creation External sharing controls Hardware compliance processes	**Automation & Reporting** Jira workflow automation Executive-level security reporting Remediation script deployment

Professional Experience

SOCOTEC - Junior Security Analyst

Sep 2024 - Present

- Acted as email security platform SME, owning configuration, optimisation, and troubleshooting.
- Designed and implemented Gateway Policies, Targeted Threat Protection, and misaddressed email protection.
- Investigated and resolved complex email security incidents with vendor support where required.
- Implemented CIS benchmark hardening across servers and endpoints.
- Supported Cyber Essentials and CE+ certification through vulnerability remediation.
- Managed vulnerability and patching cycles across endpoints.
- Monitored and investigated alerts using Microsoft Sentinel, Darktrace, and Varonis.
- Conducted incident analysis and improved response processes.
- Deployed and maintained WAF rules to protect against OWASP Top 10 threats.
- Implemented PAM controls and supported rollout of PIM.
- Designed and delivered phishing simulation campaigns.
- Developed and enforced security policies and SOPs.
- Authored the IT Security Executive Report for senior leadership.
- Designed SMTP relay solutions and improved mail flow security.
- Refined SPF, sharing controls, and other configurations to reduce attack surface.

SOCOTEC - Senior Desktop Technician

2023 - Sep 2024

- Managed escalations across infrastructure and application support.
- Conducted root cause analysis to reduce recurring incidents.
- Administered user access across on-prem and cloud systems.
- Delivered security-focused initiatives including phishing campaigns and VPN rollout.
- Supported endpoint security, MDM, and secure software deployment.
- Provided technical leadership and acted as an escalation point for complex issues.

Nottingham City Council - Managed Technician

2021 - 2023

- Delivered 1st and 2nd line support across multiple sites.
- Managed mobile devices using MDM solutions and enforced secure configurations.
- Ensured GDPR and organisational security compliance.
- Collaborated with stakeholders and suppliers to maintain service delivery.

Home Bargains - Sales Assistant (Part-time)

2018 - 2021

Certifications and Current Study

Cyber Security 101 (SEC1) TryHackMe - Verified Issued 15 August 2026 - expires 15 August 2029 Covers networking, operating systems, security principles, and core technical assessment.	**Certified Pre Security (SEC0)** TryHackMe - Verified Issued June 2026 - expires June 2029 Covers computer systems, operating systems, networking, web technologies, and cyber security fundamentals.
Security Analyst Level 1 (SAL1) TryHackMe - In progress Current study focus across SOC fundamentals, alert triage, threat detection, investigation, and report writing.	**Microsoft SC-300** Microsoft - Planned next focus Identity-focused study covering Entra ID, Conditional Access, identity governance, privileged access, and Zero Trust controls.

Education and Qualifications

Nottingham College (2017 - 2020)

- Level 4 System Support & Peripherals - Merit
- Level 3 System Support - Distinction

- Level 2 System Support - Distinction

George Spencer Academy (2012 - 2017)

- GCSEs including ICT, Maths, Science

Portfolio Evidence

Microsoft Defender for Office 365 write-up Technical write-up covering investigation, licensing context, Safe Links, Safe Attachments, and practical rollout considerations.	**SharePoint B2B external sharing research** Research and documentation around external sharing controls, Entra B2B governance, and reducing collaboration risk.
Browser-based security tools Built practical tools including IP intelligence, domain lookup, and guest-risk calculation utilities.	**Portfolio site** Maintained personal portfolio with research, certifications, practical tools, and security learning evidence.

Additional Information

Active home lab focused on Active Directory, security tooling, network configuration, and improving day-to-day security skills.
References available on request.