Jonathankeefe08@gmail.com | 07835708248

[keefecodes.com](keefecodes.com) | [GitHub](GitHub) | [LinkedIn](LinkedIn)

## PERSONAL PROFILE:

Security-focused IT professional with 4+ years of hands-on experience across cybersecurity, infrastructure, and development. Proven track record in implementing SIEM, authoring cybersecurity policy, managing threat response, and leading compliance projects including Cyber Essentials and ISO 27001.

Currently leading IT operations at Health Academy while pursuing a Level 7 MSc in Cybersecurity. My interests are shifting into offensive security, with hands-on work in penetration testing, vulnerability research, and ethical hacking using Kali Linux, Wazuh, Burp Suite, and custom scripting. Currently studying toward OSEP and the Full-Stack Pentesting Lab.

Looking for roles in penetration testing, red teaming, or SOC environments where I can contribute technical insight, real-world experience, and ongoing offensive security development.

## SKILLS & ACHIEVEMENTS:

**Offensive Security & Tooling:** Kali Linux, Wazuh (SIEM), Nikto, WPScan, Burp Suite, Nmap, ClamAV, vulnerability scanning, web server hardening, real-world IR experience.
**Scripting & Automation:** Python (automation, scraping), Bash (backups, endpoint patching), Google Apps Script, PHP.
**Infrastructure & Admin:** Windows Server, Linux CLI, Google Workspace Admin, firewall configuration, SSH lockdown, DNS and backups, DR planning.
**Web & Dev Security:** WordPress lockdown, plugin security, LearnDash hardening, DevOps (CI/CD), git-based workflow.
**Development Stack:** React 18, Tailwind CSS, TypeScript, shadcn/ui, GitHub, Vite, Three.js.
**Learning Focus:** OSEP (in progress), Full-Stack Pentesting Lab, ISO 27001 Lead Auditor.

## WORK EXPERIENCE:

**IT Manager / Cybersecurity Lead**
*Health Academy* | Jan 2024 – Present

- Deployed Wazuh SIEM, ClamAV, and Fail2Ban across systems for real-time threat detection
- Created internal security policy, asset register, patch cycle, and DR documentation for ISO 27001
- Led incident response to a PHP redirect malware campaign on WordPress – handled forensic log review, plugin lockdown, and post-exploit cleanup
- Built CI/CD-ready infrastructure: dev–stage–live deployment, caching/CDN integration
- Automated internal backups, endpoint monitoring, and folder creation using Bash and Apps Script
- Provided L2–L3 IT support across hybrid team (Google Workspace, email, hosting, hardware)

**Software QA Tester**
*ParcVu* | Jul 2023 – Dec 2023

- Ran manual test cycles (Agile + Waterfall) across GDPR-sensitive platforms (Tempo, Plot)
- Used Postman and MySQL Workbench for API/database integrity testing
- Logged detailed bugs using internal system (The Beast); optimised regression fix cycles

**IT Technician & Developer**
*Aston Berkeley* | Jan 2023 – Jul 2023

- Provided full-stack WordPress dev + Linux server admin support
- Configured Draytek firewalls and VPNs, monitored infrastructure with ShadowControl
- Improved site speed, reduced downtime through proactive patching and scripting

**Junior Developer**
*Yoma* | Jul 2021 – Dec 2022

- Maintained Magento/WordPress sites and backend systems
- Built Python scripts for SKU automation; sped up catalog syncs significantly
- Optimised UX, site speed, and mobile responsiveness for e-commerce clients

(Additional roles in testing, customer-facing, and freelance work available on request.)

## Key Projects & Labs

**SafePort (In Progress)**
Cross-platform backup tool that only syncs photos/videos to local storage over trusted Wi-Fi—no cloud, no subscriptions. Prioritises privacy and offline resilience.

**Full-Stack Pentesting Lab (In Progress)**
Hands-on offensive security lab covering AD abuse, lateral movement, privilege escalation, and C2 techniques—built on OSEP learning structure.

**Malware Recovery (Live Incident)**
Investigated and remediated PHP-based redirection malware on production WordPress instances. Work included forensic log review, DNS cleanup, credential resets, and hardening of themes/plugins.

**WordPress Lockdown Suite**
Custom-coded plugin and NGINX-level lockdown for LearnDash-based LMS platform. Implemented auto-patching, login tracking, and brute force detection.

## Education

**MSc Digital & Technology Specialist – Cyber Security Pathway**
Northumbria University | Expected Apr 2027
Modules: Ethical Hacking, Secure Systems, ISO 27001, Risk & Governance

**Certifications / Progress**

- Offensive Security Experienced Penetration Tester (OSEP) – In Progress
- Full-Stack Pentesting Lab – In Progress
- ISO 27001 Lead Auditor – Studying

- Google Cybersecurity Certificate – Studying

**Apprenticeships & Level 3 Qualifications**

- Software Development Technician – Level 3 – Pass (2022)
- BSC L3 Programming (Python, JS) – Grade B
- BSC L3 Dev Methodologies – Grade B

## Portfolio & Profiles

- GitHub: https://github.com/Jon8897
- Website: https://keefecodes.com
- LinkedIn: https://linkedin.com/in/jonathan-keefe-39022b175/

*(References available on request)*