BILL BENSON

Merseyside, UK | +44 7824 328914 | billbenson886@gmail.com | LinkedIn | GitHub | Portfolio | Right to work in the UK, no sponsorship required | Open to relocation anywhere in the UK

PROFESSIONAL SUMMARY

Cybersecurity professional with Microsoft Sentinel and KQL detection work, production endpoint and email security work, and Sophos and FortiGate firewall experience. Built a Sentinel detection lab ingesting 5,000+ WAF events, with KQL rules tuned to remove the false positives observed in the test dataset, following an MSc dissertation on ModSecurity WAF detection. In a client-facing security role covering a 40+ account portfolio, worked on selected client engagements including a Sophos Intercept X rollout via Intune, supported Sophos Email Protection configuration for 136 mailboxes, an unauthorised VPN access investigation and Sophos XG to XGS firewall migrations. Backed by a year of first and second-line IT support, a web application security testing lab record (43 PortSwigger labs), an MSc in Cybersecurity (Distinction), CompTIA Security+, ISC2 CC and two Sophos engineer certifications.

KEY SKILLS

Security Monitoring and Detection: Microsoft Sentinel, KQL detection rules, Azure Monitor Logs Ingestion API, Data Collection Rules, Log Analytics, false-positive tuning

Endpoint and Email Security: Sophos Intercept X Advanced, Sophos Central, Microsoft Intune deployment, tamper protection, Sophos Email Protection (phishing, malware, DLP, encryption, MFA), endpoint alert resolution

Incident and Vulnerability Handling: unauthorised access investigation, VAPT remediation support, first-level IT service support under a P1 to P4 SLA, security health checks, vulnerability scanning with Nessus and Nmap

Network Security: Sophos XG/XGS firewalls (SFOS v20/v21), FortiGate (VDOMs, IKEv2/IPsec VPN, web filtering), firewall rule audits, VLANs, IPsec and GRE VPN configuration, DNS protection

Offensive Security: OWASP Top 10, Burp Suite, OWASP ZAP, sqlmap, Metasploit, Hydra, Kali Linux, OSINT

Platforms and Scripting: Active Directory, Azure AD, Microsoft 365, Windows, Linux, Docker, Python

Frameworks: knowledge of PCI DSS, GDPR, ISO 27001 and NIST CSF

PROJECTS

Microsoft Sentinel WAF Bypass Detection (KQL, Azure Monitor Logs Ingestion API)

- Ingested 5,000+ WAF traffic events, attack and benign, from the dissertation testbed into a Microsoft Sentinel lab using custom tables, a Data Collection Rule and app-registration auth with scoped RBAC.
- Wrote KQL detections using anti-join correlation between NGINX access logs and ModSecurity audit logs to surface SQL injection that bypassed the WAF; tuned the logic to attack grammar rather than keywords, removing the false positives seen in the test data. Code: GitHub.

MSc Dissertation: WAF Evaluation of ModSecurity and OWASP CRS (Docker, NGINX)

- Evaluated ModSecurity CRS 3.3.8 at Paranoia Levels 1 and 2 against 200 malicious SQLi and XSS payloads and 500 benign requests in a Docker-based NGINX testbed; graded Distinction (88%).
- Measured a 97% true positive rate and 1.0% false positive rate at PL1, identified six bypass techniques including MySQL comment terminators and double URL encoding, and traced PL2's doubled false positives to anomaly-score threshold arithmetic.

Malware Detection with Machine Learning (Python, LightGBM, EMBER)

- Built static PE malware classifiers (SVM, LightGBM, MLP) on the EMBER 2018 dataset; LightGBM reached F1 0.9474 and ROC AUC 0.9892, with stable rankings across two stratified subsets.

EXPERIENCE

Casper Technologies Ltd | Network Security Engineer | Lagos, Nigeria | Jul 2024 - Jan 2025

- Deployed Sophos Intercept X Advanced for a client: Sophos Central setup, pilot then full rollout via Microsoft Intune, policy configuration, migration from TrendMicro and tamper protection.

- Supported configuration of Sophos Email Protection for a 17-company group covering 136 mailboxes: spam, malware and phishing URL protection, encryption, DLP, MFA, user sync, testing and client documentation.
- Investigated unauthorised VPN access for a client; when their firewall became unreachable with very high memory use, delivered a stopgap XGS and restored their backup onto it to keep them online.
- Supported a client through a VAPT remediation cycle: walked them through the results, implemented SMB signing, audited firewall rules and configuration, and scheduled AD hardening and network segmentation.
- Ran Sophos Central and Sophos Firewall health checks covering admin exposure, ARP-poisoning logging, ATP, certificates, backups and resource usage, across 8 customer engagements in one quarter.
- Carried out Sophos XG to XGS firewall migrations for three clients: backed up appliances, upgraded to SFOS v21, registered in Sophos Central, migrated configuration, tested policies, VPNs and VLANs, and planned rollback.
- Installed, configured and managed FortiGate firewalls for customers as part of Casper's Fortinet partnership; on one client, worked with the team on an IKEv2 site-to-site IPsec VPN to an IoT partner's cloud gateway, troubleshooting repeated IKE Phase 1 failures that traced to the partner's gateway, and reported the findings to the MD.
- Provided first-level support for a client's ITSM platform under a formal SLA with P1 to P4 priorities, liaising with the vendor on open tickets.
- Delivered cybersecurity awareness training to 200+ client staff and presented Sophos Firewall and Sophos Central to every internal department.

Self-directed Penetration Testing Labs | Burp Suite, Kali Linux | Sep 2023 - Jun 2024

- Tested deliberately vulnerable lab targets against the OWASP Top 10, including SQL injection, XSS, IDOR, CSRF, SSRF and XXE, using self-built Kali, Metasploitable, Windows and Ubuntu VMs.
- Solved 43 PortSwigger Web Security Academy labs, including 23 at Practitioner/Expert level, and studied for CompTIA Security+, since passed.

Horty Benade Company | IT Support Engineer | Lagos, Nigeria | Aug 2022 - Jul 2023

- Resolved endpoint security alerts and managed Active Directory user accounts, enforcing password policies and supporting system patching.
- Handled password and MFA resets for end users as part of Active Directory account administration.
- Provided first and second-line support across Windows environments, resolving hardware, network connectivity, software and Active Directory issues.
- Documented each case and recurring issues to improve resolution times, and escalated issues to third-party suppliers where needed.

CERTIFICATIONS

CompTIA Security+ (SY0-701) | ISC2 Certified in Cybersecurity (CC) | Google Cybersecurity Professional Certificate | Sophos Firewall Certified Engineer v20.0 | Sophos Central Endpoint Protection Certified Engineer v5.0

EDUCATION

Wrexham University | MSc Cybersecurity (Distinction) | Wrexham, UK | Jan 2025 - Apr 2026

- Modules included Secure Computing (risk, IAM, security operations), Offensive Security and Incident Response, and Networking and Defensive Security.

University of Ibadan | BSc (Hons) Computer Science | Ibadan, Nigeria | 2018 - 2022