**Bradley William D. Mclaughlan**  
📍 London, UK | 📧 bradleymclaughlan@yahoo.com /bradleywilliam\_mclaughlan@yahoo.com  
📞 +44 7467 302975 | [🔗Bradley William Mclaughlan](https://www.linkedin.com/in/bradley-william-mc-laughlan-091777a9/) LinkedIn

**Professional Profile**

A highly motivated **Cyber Security Engineer** with extensive experience in **threat detection, vulnerability management, endpoint security, and compliance**. Proven ability to lead security initiatives, enhance risk management frameworks, and implement robust security measures. Adept at working collaboratively with cross-functional teams to ensure cybersecurity best practices. Passionate about continuous learning and staying ahead of evolving security threats.

**Key Skills**

**Threat Detection & Response** – SIEM, IDS/IPS, XDR Solutions  
**Vulnerability Management** – Qualys, Palo Alto XDR,Ivanti EPM,WSUS  
 **Cloud Security** – AWS, Azure Security, CyberArk  
 **Endpoint Security** – McAfee ePolicy Orchestrator, Mimecast  
 **Network Security** – Firewalls, Active Directory, SCCM  
**Compliance & Risk Management** – ISO 27001, GDPR, NIST  
**Incident Response & Forensics** – Reliaquest, Splunk  
**IT Service Management** – ServiceNow, IBM Remedy, Confluence

**Professional Experience**

**Cyber Security Analyst**

**Regent College London | Jan 2024 – Present**

* Led vulnerability management initiatives, reducing risk exposure by 30% through regular assessments.
* Developed and delivered security awareness training, resulting in reduced phishing incidents.
* Investigate cyber incidents, data breaches, and phishing attacks.
* Document incidents, conduct root cause analysis, and recommend preventive measures.
* Educate users on safe password practices, phishing awareness, and secure browsing habits.
* Ensured compliance with industry regulations (ISO 27001, GDPR) by collaborating with cross-functional teams.
* Managed third-party MSP providers for infrastructure upgrades and security enhancements.

**IT Support Engineer**

**Regent College London | Feb 2023 – Dec 2023**

system & Network Administration

* Manage and maintain Windows and Linux servers.
* Administer Active Directory (AD), DNS, DHCP, and Group Policies.
* Configure and troubleshoot LAN, WAN, Wi-Fi, and VPN networks.
* Support Microsoft 365, Google Workspace, and enterprise applications
* User Training & Documentation
* Educate employees on IT best practices and cybersecurity awareness.
* Maintain documentation for troubleshooting procedures and IT policies.
* Assist with onboarding and IT setup for new employees.
* Assist with IT infrastructure upgrades, migrations, and deployments.
* Work with IT teams to improve system performance and automation.
* Collaborate with vendors and service providers for technical solutions.

**ICT Engineer**

**Woodcote Senior High | Sep 2022 – 2023**

IT Infrastructure Management

* Design, install, and manage IT networks, servers, and storage systems.
* Configure and maintain routers, switches, firewalls, and wireless networks.
* Monitor and troubleshoot network performance, latency, and connectivity issues.

System Administration & Cloud Services

* Administer Windows and Linux servers, including Active Directory, DNS, DHCP, and Group Policies.

ICT Project Management

* Plan and implement new IT solutions, upgrades, and infrastructure improvements.
* Manage IT budgets, procurement, and vendor relationships.
* Manage Relationship with Managed Service Providers for Network stability
* Research and integrate emerging technologies to enhance IT operations.

**Security Engineer II**

**Reed Elsevier Shared Services (Philippines) | Jan 2021 – Sep 2022**

* Supervised and mentored a team of security engineers, managing daily security operations.
* Led incident response and vulnerability management, ensuring timely resolution of security threats.
* Developed and implemented incident response plans and compliance reports.
* Coordinate with SOC teams, and blue teams to improve overall security posture.
* Conduct security audits and ensure all systems adhere to regulatory requirements.
* Assist in internal and external cybersecurity audits and risk assessments
* Develop custom security scripts and automation workflows to improve vulnerability management.
* Provide detailed security reports and risk analysis to CISOs, IT directors, and stakeholders.
* Conduct security awareness training for employees to reduce human-related security risks.
* Work with developers and system admins to implement security fixes and hardening measures.

**Security Engineer I**

**Reed Elsevier Shared Services (Philippines) | Feb 2019 – Dec 2021**

**Vulnerability Assessment & Management**

Conduct regular vulnerability scans on networks, servers, applications, and cloud environments.

Use tools like Qualys to detect security weaknesses.

**Security Patch & Remediation Coordination**

Analyse scan results and prioritize critical vulnerabilities based on risk impact.

Work with IT teams to remediate vulnerabilities and verify fixes.

**Penetration Testing & Security Audits**

Identify misconfigurations, zero-day vulnerabilities, and security gaps.

Document findings and recommend security improvements.

**Threat Intelligence & Risk Analysis**

Monitor cybersecurity threats, malware trends, and emerging attack vectors.

Analyze security logs and alerts from SIEM solutions (Splunk, QRadar).

Conduct risk assessments to identify high-impact threats and prioritize security measures.

Work with system admins to apply security patches and updates.

Ensure timely patch management for OS, applications, databases, and firmware.

Verify that security configurations follow best practices

**Compliance & Security Frameworks**

Ensure adherence to industry security standards (ISO 27001, NIST, CIS, GDPR, PCI-DSS, HIPAA).

Assist in internal and external audits related to IT security.

Maintain documentation of security policies, procedures, and remediation reports.

**Security Awareness & Reporting**

Provide security guidance to IT teams and employees to reduce human errors and insider threats.

Generate detailed reports on vulnerability findings, risk levels, and remediation status.

Present security findings to management and stakeholders in a clear, actionable manner

**IT Server Engineer**

**Xerox Business Services (Philippines) | Mar 2015 – Feb 2019**

* Provided **Level 1 and Level 2 support** for Windows Server OS, DNS, DHCP, and storage solutions.
* Implemented **server security best practices**, enhancing infrastructure resilience.

**Field Engineer**

**Accent Micro Technologies Inc. (Philippines) | Jul 2014 – Feb 2015**

* Provided **on-site support** for desktop computers, network troubleshooting, and IT hardware.
* Assisted in system configurations and software installations.

**Education & Certifications**

**Bachelor of Science in Information Technology** – International Electronics & Technical Institute (2010 – 2014)

**Technical Proficiency**

* **Security Tools:** Qualys, Palo Alto XDR, McAfee, Reliaquest, Mimecast, CyberArk
* **Cloud Platforms:** AWS, Azure, Active Directory
* **ITSM Platforms:** ServiceNow, IBM Remedy, Confluence
* **Endpoint & Network Security:** SCCM, LANDesk EPM, Firewalls

**References**

Available upon request.