Mohamad Taufiq Bin Mohammad Fuad

Puncak Jalil, Puchong, Selangor · 018-310 9139 · tadlin217@gmail.com · linkedin.com/in/mohamad-taufiq-mohammad-fuad-22561a24a · github.com/taufiqbo



PROFESSIONAL SUMMARY

Final-year Computer Science (Cyber Security) student at MMU and Technical Solutions Cybersecurity Intern at Bintara Solutions. Hands-on with SIEM monitoring, detection engineering and alert investigation through a self-built SOC home lab (Wazuh, Sysmon, MITRE ATT&CK), and built a PQC Migration Scanner for post-quantum readiness. At Bintara, hardened Microsoft Defender email protection and built an automated external security assessment platform and a threat-briefing agent.

EDUCATION

Bachelor of Computer Science (Cyber Security) — Multimedia University (MMU), Cyberjaya · Expected Dec 2026 · CGPA 2.99

Foundation in Information Technology — MMU · CGPA 2.99 | SPM — SMK Bukit Jalil · 2021 · 6A

Relevant coursework: Network Security, Digital Forensics, Database Security, Cryptography

CORE SKILLS

SIEM and monitoring: Wazuh, Sysmon, Windows Event Logs, alert triage, log analysis, incident response
Detection engineering: Wazuh rules, Sigma, MITRE ATT&CK mapping
Email and endpoint security: Microsoft Defender for Office 365 (anti-spam, Strict preset), SPF, DKIM, DMARC, Entra ID
Network security: Wireshark, PCAP forensics, Nmap, DNS and TLS analysis, FortiGate firewall, VLANs, IPSec VPN (StrongSwan)
Cryptography and PQC: NIST PQC (ML-KEM, ML-DSA, SLH-DSA), X.509 certificates, TLS cipher suites, cryptographic inventory
Threat emulation and forensics: Atomic Red Team, Mimikatz, Kali Linux, FTK Imager, Autopsy, Steghide
Automation and programming: Python (pytest), GitHub Actions, Power Automate, Copilot agents, Java, PHP, JavaScript, HTML/CSS
Infrastructure and data: Docker, Proxmox VE, VirtualBox, Ubuntu Linux, Microsoft SQL Server (RLS, TDE), MySQL

EXPERIENCE

Technical Solutions Cybersecurity Intern — Bintara Solutions, Malaysia · Jul 2026 – Jan 2027

- Tightened the Microsoft Defender for Office 365 anti-spam policy (Strict preset, block list) to cut spam and phishing
- Built CyberHealth Runner, a Dockerised Python web app that runs automated external security checks on a client domain (DNS, TLS, SPF/DKIM/DMARC, web headers, exposed services) and produces a scored report
- Built Threat Radar, a Microsoft 365 Copilot agent that writes a weekly threat briefing from trusted sources (NACSA, NVD, vendor advisories) for the company's tech stack and the Managing Director
- Planned and led a FortiGate 60F install for about 70 users: VLANs, policies, guest web filtering, dual-WAN failover
- Supported client requests on Active Directory and device security; automated daily task reporting with Power Automate

Other experience: Cashier at Hero Market; Event Operations Coordinator for a large-scale marathon (logistics, crowd control)

PROJECTS

PQC Migration Scanner — Post-Quantum Cryptography · github.com/taufiqbo/Post_Quantum_Computing-Migration_tool

- Built a Python static scanner that inventories quantum-vulnerable cryptography (RSA, ECC, DH, DSA, SHA-1, MD5, 3DES) in source code (regex and Python AST), server configs (nginx, Apache, OpenSSH, OpenSSL) and X.509 certificates
- Maps findings to NIST replacements (ML-KEM, ML-DSA, SLH-DSA); outputs a quantum-readiness score and HTML/JSON/CSV reports
- Packaged as a CLI (pqc-scan) with 44 pytest tests run by GitHub Actions on Windows and Linux

SOC Home Lab — Detection & Response · github.com/taufiqbo/SOC_LAB

- Built a virtualised SOC on Proxmox VE: Wazuh SIEM, Windows 10 with Sysmon, Kali attacker, isolated lab network
- Simulated brute force (T1110) and Mimikatz credential dumping (T1003.001); tuned the ATT&CK-mapped detections
- Reconstructed a full infection chain from PCAP in Wireshark, including DNS-over-HTTPS evasion
- Ran Atomic Red Team tests for persistence (T1547.001, T1053.005) and log clearing (T1070.003); documented detection gaps and a mismapped false-positive rule

Other projects

- Sigma detection rules converted for Wazuh, with test cases and false-positive tuning
- Final Year Project: AI-driven adaptive authentication that uses machine learning to score login risk
- Coursework: StrongSwan IPSec VPN verified in Wireshark; forensic investigation with FTK Imager, Autopsy and StegSeek; SQL Server hardening (RLS, DDM, TDE)

CERTIFICATIONS AND TRAINING

- Google Cybersecurity Certificate (in progress) · Fortinet NSE 1 (Oct 2026), NSE 2 in progress · Huawei HCIA-AI V4.0 · SentinelOne Securing AI
- Vendor training (2026): Fortinet Security Operations (FortiSIEM, FortiSOAR), Fortra Offensive Red Teaming, Fortinet SASE
- Platforms: TryHackMe, LetsDefend, Cisco Networking Academy

ACTIVITIES

- Amateur boxer (2 sanctioned fights) · Events 2026: RawSec MiniCon, CyberDSA, Tenable One CTF