MAX THEOHARIS

0405 406 680 | maxtheoharis@gmail.com | Petersham, NSW

PROFESSIONAL SUMMARY

Recent cybersecurity graduate with hands-on experience in digital forensics, secure data handling and system analysis. Strong technical foundation across Python, Linux, and forensic tooling, combined with communication and problem-solving skills developed through tutoring and customer-facing roles.

TECHNICAL SKILLS

Governance & Frameworks: MITRE ATT&CK, Cyber Kill Chain, NIST Cybersecurity Framework (CSF) 2.0, NIST SP 800-61, ISO/IEC 27001, ACSC Essential Eight, BC/DR Planning, Risk Assessment, Chain of Custody

Defence & Security Operations: Splunk (SIEM), Wireshark, Autopsy, Windows Event Logs, DeepBlueCLI, Sysmon, Burp Suite, OWASP Top 10, IOC Analysis, Cisco Packet Tracer, CloudTrail, Forensic Timelines

Identity & Access Management: AWS IAM, Active Directory, Tailscale ACLs, Access Control Models (RBAC, DAC, MAC), MFA

Infrastructure: Proxmox VE, Docker, LXC, Linux, Tailscale Mesh VPN, 802.11 Capture & Analysis, RSSI Mapping, Cisco Packet Tracer

Programming & Automation: Python, PowerShell, Bash, SQL, Java, C++, Git/GitHub

EDUCATION & CERTIFICATIONS

Bachelor of Cybersecurity
University of Technology Sydney (UTS)
Dean's List Award Recipient, 2024 & 2025
Graduated 2026 – High Distinction Average

High School Certificate
Newtown High School of the Performing Arts, 2019

Blue Team Level One (BTL1) - Security Blue Team
Covers Phishing Analysis, Threat Intelligence, Digital Forensics, SIEM Management and Incident Response

Certified in Cybersecurity (CC) - ISC2
Covers Business Continuity & Disaster Recovery, Access Controls, Network Security and Security Operations

SELECTED CYBERSECURITY & TECHNICAL PROJECTS

Digital Forensics Investigation & Evidence Timeline *University Project*	Examined a disk image and Outlook PST evidence set, verified integrity with MD5 hashing and correlated EXIF, deleted file, email, web and keyword artifacts into a formal investigative timeline.
Threat Intelligence & Incident Response Report *University Group Project*	Produced a ransomware response plan for a healthcare organisation, covering triage, containment, evidence preservation, recovery, root cause analysis, stakeholder impact and remediation actions.
Proxmox Homelab & Self-Hosted Security Infrastructure *Self-Directed Project*	Built a Proxmox-based homelab for self-hosted services including Nextcloud, Jellyfin, Immich, Tailscale remote access and external storage mounts, as a secure service deployment exercise.
Secure AWS Cloud Architecture & Compliance Design *University Project*	Designed a secure AWS PaaS architecture for a financial application using segmented networking, least-privilege identity, encrypted services, centralised logging and detection controls.
Wireless Security Analytics Device (WiFinder) *Self-Driven Group Project*	Contributed to a Raspberry Pi-based wireless network auditing prototype for passive 802.11 metadata capture, GPS-synchronised RSSI mapping, Python heatmaps and automated reporting.

EXPERIENCE

Tutor - Perfect Practice Tutoring
Jul 2020 - Present

- Tutored Years 7–12 Mathematics and Physics, translating complex technical concepts into clear explanations for students with different skill levels.
- Developed strong communication, analytical reasoning and problem-solving skills through long-term client-facing work

Bartender - Public House Petersham
Oct 2023 - Present

- Worked in a high-pressure service environment requiring teamwork, attention to detail, task prioritisation and calm decision-making.
- Managed competing customer needs and operational tasks while maintaining reliable professional standards.