Anil Budthapa

hypemsltech@gmail.com | +61 421 688 186 | Open to relocate anywhere in Australia; currently based in Melbourne, VIC, Australia.
linkedin.com/in/anilbudthapa | github.com/anilbudthapa1

Cybersecurity Analyst
SOC (Level 1)
GRC (Governance, Risk Compliance) Analyst
IAM (Identity Access Management) Analyst

Professional Summary

Entry-level cybersecurity and SOC candidate based in Melbourne with hands-on lab and project experience in alert triage, incident handling, SIEM investigations, log analysis, Windows security events, Active Directory and IAM fundamentals, vulnerability assessment, and OWASP-aligned web testing. Comfortable mapping activity to MITRE ATT&CK and producing clear investigation notes, findings, and security documentation. Seeking junior SOC, cybersecurity analyst, vulnerability management, or security operations roles in Australia.

Technical Skills

*

[SOC & Incident Response] Alert triage, incident handling and escalation, SIEM investigations, log analysis, threat detection, investigation playbooks, security reporting
*

[Detection & Analysis] MITRE ATT&CK mapping, Windows security events, phishing analysis, authentication analysis, endpoint analysis, network traffic analysis, threat hunting fundamentals
*

[Vulnerability & Web Testing] Vulnerability assessment, OWASP Top 10, reconnaissance, access control testing, authentication testing, findings documentation
*

[Identity & Endpoint] Active Directory fundamentals, IAM concepts, user and group management, access reviews, EDR/XDR fundamentals
*

[Platforms & Tools] Windows, Linux, networking fundamentals, AWS and Azure fundamentals, Splunk, Burp Suite, Nmap, Wireshark, Git, GitHub
*

[Scripting] Python, Bash, SQL (basic), Go (basic)

Certifications

*

[Completed] **Google Cybersecurity Professional Certificate**
Provider: Google
Certificate: coursera.org/account/accomplishments/...
*

[Completed] **SOC Level 1 Certificate**
Provider: TryHackMe
Certificate: tryhackme.com/certificate/THM-6K5TBUSQXE
*

[Completed] **Cloud Computing Fundamentals**
Provider: Simplilearn SkillUp

Projects and Practical Experience

*

[2025–Present] **insoSIEM** github.com/anilbudthapa1/insoSIEM
SIEM-focused project exploring log collection, normalization, detection use cases, and investigation workflows.

- Built repeatable workflows for log review and triage-style investigation notes.

- Practised turning raw events into security-relevant context by identifying what happened, why it mattered, and next investigation steps.
- Documented detections and mapped relevant activity to MITRE ATT&CK where applicable.

*

[2025–Present] **Pentesting Framework** github.com/anilbudthapa1/Pentesting_Framework
Modular web security testing framework aligned to OWASP Top 10, with evidence capture and reporting structure.

- Implemented reconnaissance and testing modules to support consistent, repeatable assessments.
- Added evidence handling and output export to keep findings reproducible.
- Practised validating common issues including access control weaknesses, injection risks, and security misconfiguration.

*

[2025–Present] **Care Portal** github.com/anilbudthapa1/care_portal
Role-based application project emphasizing permissions, authentication and authorization flows, and secure design thinking.

- Designed role-based access requirements and translated them into workflow rules.
- Implemented backend logic with a focus on least privilege and clear separation of roles.

*

[Ongoing] **SOC / Analyst Practice (Labs)**
Hands-on practice with SOC-style investigations and web testing using Burp Suite, Linux, and scripting.

- Investigated HTTP traffic, sessions, and authentication behavior, and tested for common weaknesses.
- Analysed Windows security events and authentication activity to identify suspicious patterns.
- Practised triage, escalation decisions, and writing clear, structured findings.

*

[Ongoing] **Active Directory Security Lab** github.com/anilbudthapa1/My_Portfolio/tree/main/My_project/Active_Directory
Lab-based practice covering Active Directory fundamentals and identity-security concepts.

- Worked with users, groups, privileges, and access review concepts.
- Connected identity-related events to SOC monitoring and investigation use cases.

Education

*

[2026] **Bachelor of Information Technology**
Major: Cybersecurity
Kent Institute Australia, Melbourne
Expected Completion: 2026

*

[Certificates] **Google Cybersecurity Professional Certificate**
Provider: Google

*

[Completed] **SOC Level 1 Certificate**
Provider: TryHackMe
Certificate: tryhackme.com/certificate/THM-6K5TBUSQXE

Memberships and Additional Information

*

[ISACA] ISACA ID: 2244571
Name: Mr. Anil Budthapa
Level: Member
Member Since: 21 October 2025
Paid Thru: 31 December 2026
Status: Active

*

[ACS] Australian Computer Society (ACS) Member
Membership ID: 4476790
Level: Member
Status: Active

*

[Availability] Based in Springvale, Melbourne, VIC, Australia
Open to graduate, junior, and entry-level cybersecurity opportunities
Available for on-site, hybrid, and remote roles