SAGAR BIDARI

0420 310 550 | cybersecure@bidarisagar.com | Melbourne, VIC (Australian Citizen)
linkedin.com/in/sagarbidari | github.com/sagarbid | bidarisagar.com

PROFESSIONAL SUMMARY

Entry-level cybersecurity and IT professional with a CompTIA Security+ CE certification and a Monash University Cybersecurity Bootcamp credential. Hands-on experience across SIEM (Splunk, Wazuh), network scanning, vulnerability assessment, and digital forensics — built through structured bootcamp projects, homelab practice, and three industry simulations. Eligible for NV1/NV2 Defence Security Clearance. Seeking a Level 1 SOC Analyst, Security Analyst, or IT Service Desk role where I can apply my detection and troubleshooting skills and grow within a professional security team.

TECHNICAL SKILLS

- **SIEM & Monitoring:** Splunk Enterprise (SPL queries, dashboards, alerts) — Monash Bootcamp + homelab practice; Wazuh (agent deployment, custom rules, OpenSearch backend) — homelab SOC lab
- **Frameworks & Methodologies:** MITRE ATT&CK (tactical mapping, TTP identification, incident classification); NIST Cybersecurity Framework (awareness)
- **Network & Scanning:** Nmap (host discovery, port scanning, OS/service detection); Wireshark (packet capture and analysis); OpenVAS (lab); Nessus (scan interpretation — bootcamp)
- **Penetration Testing (Lab):** Metasploit Framework (vulnerable VM exploitation); Hashcat (brute-force and dictionary attacks — lab); Kali Linux toolset
- **Operating Systems:** Windows (Event Log analysis — Event IDs 4624, 4625, 4672, 4688); Linux/Ubuntu (CLI, auth.log, syslog, Bash scripting); Kali Linux
- **Digital Forensics:** Autopsy, SQLite Browser, iPhone Backup Extractor; chain-of-custody procedures; evidence timeline construction (bootcamp project)
- **Scripting:** Exposure to Python scripting — log parsing, Nmap automation, file I/O (bootcamp); Bash (homelab regular use)
- **Virtualisation & Homelab:** VMware Workstation, VirtualBox; multi-VM environments (Windows, Ubuntu, Kali); cloud VMs (AWS/TF/Azure free tier)
- **IT & Security Tools:** Active Directory (basic lab exposure — TryHackMe/homelab); DNS, firewall rules, SSL/TLS configuration (live Shopify production); ticketing systems (training environment)
- **Platforms & Practice:** TryHackMe (active); HackTheBox; Blue Team Labs Online; LetsDefend; bug bounty participation (no accepted findings)

CERTIFICATIONS

- CompTIA Security+ CE (SY0-701) — Certified January 2026, valid to January 2029 | Credential ID: COMP001022828912
- Monash University Cybersecurity Bootcamp — Jun–Dec 2024 (Splunk, Nessus, Incident Response, Python, Network Security)
- Introduction to Cyber Security — IAT NSW Government / Microsoft — January 2023 | Credential ID: HLIDqefbKI
- Diploma of Business — Zenith Business Academy — October 2016

PROJECTS & SIMULATIONS

Wazuh Homelab SOC — Personal Project April 2026

Tools: Wazuh 4.x, OpenSearch, Ubuntu Server 22.04, Kali Linux, VMwaregithub.com/sagarbid/wazuh-homelab-soc

- Deployed a full SOC simulation environment: Wazuh Manager + Indexer + Dashboard on Ubuntu Server, with a Kali Linux agent connected via VMware NAT network

- Configured real-time log ingestion, custom detection rules, and alert generation; visualised events on Wazuh Dashboard
- Executed simulated attack scenarios mapped to MITRE ATT&CK: T1046 (Nmap service discovery), T1110 (SSH brute-force), file integrity monitoring violations
- Authored automated test scripts (Shell/GitHub Actions) and documented agent lifecycle management, rule validation, and incident investigation patterns

Splunk SIEM Monitoring — Vandalay Industries Dec 2024

Tools: Splunk Enterprise, SPL, Nessus, Apache & Windows Event Logsgithub.com/sagarbid/Splunk-SIEM-Monitoring-Vandalay-Industries

- Ingested and parsed multi-source logs (Apache web server, Windows Event Logs) into Splunk; built three production-grade dashboards: Attack Overview, Authentication Monitor, Vulnerability Posture
- Wrote SPL queries to detect DDoS (>1,000 requests/min from single source) and brute-force attacks (>20 failed logins in 5 min); achieved sub-3-minute simulated mean time to detect
- Interpreted Nessus vulnerability scan output; cross-referenced critical/high findings against active traffic patterns to prioritise remediation
- Produced formal threat intelligence reports with remediation guidance — reusable dashboard templates documented for enterprise deployment

Virtual Space Industries SOC Project — Monash Bootcamp Nov 2024

Tools: Splunk Enterprise, SPL, MITRE ATT&CK Framework

- Wrote SPL searches to identify active attack patterns within a simulated enterprise log environment
- Created Splunk dashboards and threshold-based alerts; mapped attacker behaviour to MITRE ATT&CK tactics and techniques
- Authored a formal SOC incident report — findings, evidence, timeline, and remediation recommendations — mimicking real analyst deliverables

Automated Nmap Network Scanner Oct 2024

Tools: Python 3, Nmap, python-nmap, argparsegithub.com/sagarbid/Automated-Nmap-Network-Scanner

- Built a Python CLI tool that automates host discovery, port scanning, and OS/service fingerprinting using Nmap — simulating the enumeration phase of a penetration test
- Supports single IPs, CIDR ranges, and hostname lists; exports results in JSON and CSV formats for integration with downstream analysis tools
- Added audit logging and verbose output for security documentation purposes; feeds results into tools like Nessus and Metasploit

Mobile Device Forensics — iPhone Investigation Sep 2024

Tools: Autopsy, SQLite Browser, iPhone Backup Extractor, Cellebrite UFED (simulated)github.com/sagarbid/Mobile-Device-Forensics-iPhone-Investigation

- Conducted a simulated digital forensics investigation on an iOS device: forensic imaging, deleted data recovery (14 iMessages), geolocation extraction, and app database analysis
- Built an evidence timeline correlating artefacts across multiple sources; produced a formal forensic report with chain-of-custody documentation and legal admissibility considerations

VirtualBox Cybersecurity Homelab Ongoing — from 2024

Tools: VirtualBox, Kali Linux, Ubuntu, Windows, TryHackMe, HackTheBoxgithub.com/sagarbid/VirtualBox-Cybersecurity-Lab

- Maintains a multi-VM homelab (Windows, Ubuntu, Kali Linux) for continuous hands-on security practice: Metasploit exploitation, Hashcat password attacks, Wireshark packet analysis
- Actively practices on TryHackMe and Blue Team Labs Online; participates in bug bounty programs

Industry Simulations (Virtual Work Experience) Jan–Feb 2026
Clifford Chance | ANZ Australia | Datacom

- Clifford Chance Cyber Security Global Simulation (Feb 2026): GDPR compliance analysis, ICO Dawn Raid response, data breach escalation procedures
- ANZ Australia Cyber Security Management Simulation (Jan 2026): phishing email investigation, Wireshark packet capture analysis, incident containment recommendations
- Datacom Cybersecurity Simulation (Jan 2026): cyberattack investigation, risk assessment, security control recommendations for a simulated enterprise incident

WORK EXPERIENCE

Disability Support Worker — Agapi Care Inc. Feb 2024 – Jan 2026
Preston, VIC

- Documented 5+ critical incidents per month in structured written reports — applying consistent reporting frameworks and escalation procedures analogous to IT incident documentation workflows
- Handled sensitive and confidential client information with strict compliance to NDIS standards — demonstrating attention to data handling policies and regulatory requirements
- Delivered clear verbal shift handovers and written reports under time-sensitive conditions, building communication and documentation discipline

E-Commerce Business Owner (Shopify) Jul 2020 – Jan 2026
Self-Employed — Online

- Managed hosting infrastructure: configured DNS records, server-level firewall rules, and SSL/TLS settings for a live production e-commerce environment
- Monitored web traffic via Google Analytics; managed store security settings including access controls and secure checkout configuration

Head Chef / Sous Chef Apr 2019 – Mar 2023
Multiple Sydney Venues

- Led kitchen teams of up to 12 staff; enforced food safety compliance standards and conducted staff training on SOPs — developing strong process-driven leadership and compliance mindset
- Managed high-pressure environments with consistent attention to procedural accuracy and risk mitigation

IT Business Analyst Intern — E-Soft Technologies Oct 2019 – Jan 2020
Toongabbie, NSW (Unpaid university placement)

- Attended stakeholder meetings and captured business requirements; produced Business Requirement Documents (BRDs) and process flow diagrams
- Gained SDLC exposure through requirements gathering, documentation, and basic coding/testing tasks alongside the development team

EDUCATION

Bachelor of Business (Information Systems Management) Dec 2018
Victoria University, Melbourne VIC | Specialisations: Business Intelligence, Database Development, IT Project Management

Monash University Cybersecurity Bootcamp Jun – Dec 2024
Full-time intensive program — Splunk, Nessus, Incident Response, Python, Network Security, Penetration Testing