RAGHAV MAHAJAN

SOC Analyst · Cybersecurity Analyst · Blue Team · IT Security

(825) 343-1168 · raaghvv0508@gmail.com · raghv.dev · github.com/HomeLab-Raghav · Edmonton, AB

PROFESSIONAL SUMMARY

Cybersecurity professional holding the ISC2 CC, CompTIA Security+ (SY0-701), and Google Cybersecurity Certificate — with deep hands-on experience built through a self-designed enterprise SOC lab running Wazuh SIEM, Splunk, Windows Server 2022 AD, and Kali Linux. Triaged 50+ real attack simulations, built threat-detection dashboards from scratch, and documented every lab to audit-ready standard. Brings a background in physical security operations — access control, anomaly escalation, and incident reporting — that translates directly into SOC monitoring and triage. Calm under pressure, documentation-obsessed, and ready to contribute on day one.

CERTIFICATIONS

▸ **ISC2 Certified in Cybersecurity (CC)**	2026	*ISC2*
▸ **CompTIA Security+ (SY0-701)**	2026	*CompTIA*
▸ **Google Cybersecurity Professional Certificate**	2025	*Google / Coursera*
▸ **TryHackMe — SOC Level 1 Path**	50+ Labs	*Try Hack Me*
▸ **Alberta Security Guard License**	Valid	*Province of Alberta*

TECHNICAL SKILLS

SIEM & Monitoring	Wazuh (agent deploy, rule tuning, log ingestion, alert customization) · Splunk (SPL, dashboards, brute-force & port-scan detection) · ELK / Kibana
Threat Detection	Alert triage · IOC identification · Event correlation · Anomaly detection · MITRE ATT&CK · OWASP Top 10 · Vulnerability scanning
Network Analysis	Wireshark (packet capture, display filters, protocol dissection, SYN/ARP/DNS analysis) · tcpdump · Nmap · Network traffic forensics
Security Tools	Kali Linux · Burp Suite · Nikto · Hydra (lab) · SQLMap · Gobuster · Netcat · Metasploit (foundational)
OS & Infrastructure	Windows Server 2022 (AD DS, DNS, DHCP, GPO, PowerShell) · Ubuntu Server · Kali Linux · Windows 10/11
Active Directory	Domain build, OU structure, user/group management, GPO hardening, PowerShell automation, Kerberos/LDAP auth
Compliance & GRC	NIST CSF · CIS Controls · ISO 27001 (awareness) · MITRE ATT&CK · OWASP · Risk register documentation
Incident Response	Triage → Escalation → Containment → Evidence collection → 5-W reporting → IOC documentation → Post-incident write-up
Documentation	Audit-ready reports · Incident logs · Runbooks · SOPs · GitHub-maintained lab documentation
Cloud & Dev	Azure (fundamentals) · AWS (fundamentals) · Git/GitHub · Docker (basic) · PowerShell scripting · VS Code

CORE COMPETENCIES

- Security Event Monitoring
- SIEM Log Analysis & Triage
- Threat & Vulnerability Detection
- Incident Response & Escalation
- Network Traffic Analysis
- Active Directory & IAM
- Endpoint Security Monitoring
- Vulnerability Assessment
- NIST CSF / CIS Controls
- Audit-Ready Documentation
- Compliance & GRC Support
- Security Awareness

CYBERSECURITY HOME LAB — HOMELAB CORP

Enterprise SOC Simulation Lab · HomeLab Corp — homecorp.local 2024 – Present / *Edmonton, AB*

Stack: Windows Server 2022 · Ubuntu Server · Kali Linux · Wazuh · Splunk · Wireshark · Active Directory · VirtualBox

- **Deployed Wazuh SIEM** across DC01/WEB01/KALI01 — ingested logs from 3 nodes, wrote custom detection rules, tuned alert thresholds; triaged 50+ simulated attack events end-to-end
- **Built Splunk threat dashboards** using SPL — detected brute-force login chains, Nmap scan patterns, and lateral movement indicators across correlated log sources
- **Performed Wireshark packet forensics** on live captures — isolated SYN scans, ARP poisoning, DNS exfiltration, and TLS anomalies to reconstruct attack timelines
- **Built Windows Server 2022 AD domain from zero** — homecorp.local, 7 accounts, 3 security groups, OU hierarchy, GPO hardening, DNS/DHCP, Kerberos/LDAP; fully scripted in PowerShell
- **Ran adversarial simulations** (Nmap, Hydra, ARP spoof, Gobuster, Nikto) from KALI01 against DC01/WEB01 — correlated every alert in Wazuh and Splunk, documented containment steps
- **Completed 50+ TryHackMe SOC Level 1 labs** — AD attacks, Kerberoasting, BloodHound, SIEM triage, Wireshark/tcpdump, John the Ripper, and IR workflows

Edmonton Cybersecurity Community · Discord — Founder & Moderator 2025 – Present / *Edmonton, AB*

- Founded and lead an Edmonton-area security community — sharing Wireshark walkthroughs, SIEM lab breakdowns, and threat analysis write-ups with fellow learners

PROFESSIONAL EXPERIENCE

Screening Officer / Security Analyst · Impact Security · ADESA / Covenant Health Apr 2023 – Present / *Edmonton, AB*

- Monitored access control for 100+ daily entrants — enforced credentials, policies, and access logs; directly mirrors IAM and identity-verification workflows in IT security
- Monitored CCTV feeds and restricted areas for anomalies — identified, flagged, and escalated incidents following structured protocols that map 1:1 to SOC alert triage
- Authored evidence-based incident reports under operational pressure — consistent with chain-of-custody standards and security audit documentation requirements

Line Cook · Earls Kitchen + Bar & St. Louis Bar & Grill Jul – Oct 2025 / *Edmonton, AB*

- Maintained concurrent employment at two establishments simultaneously — demonstrated time management, reliability, and ability to perform under competing operational demands

Assistant Kitchen Manager · Leopold's Tavern Feb – Jul 2025 / *Edmonton, AB*

- Supervised 10+ staff in a high-volume, time-critical environment — enforced compliance standards, led shift handoffs, and produced structured operational reports under pressure

Freelance Web & Software Developer · Self-Employed — Aug 2022 – Present / *Edmonton, AB*

- Delivered full-stack applications with built-in security controls: encrypted auth, CSRF/XSS validation, RBAC, and secure API design aligned to OWASP Top 10
- Managed patching, dependency updates, and vulnerability remediation across client environments — practical ongoing security maintenance experience

Line Cook → Kitchen Supervisor · Boston Pizza — Sep 2022 – Dec 2023 / *Edmonton, AB*

- Promoted from Line Cook to Kitchen Supervisor — led station coordination, enforced HACCP compliance, and delivered structured shift handover documentation
- Trained new hires and maintained process documentation — skills transferable to SOC runbook maintenance and analyst onboarding

EDUCATION

Diploma — Digital Media & IT, Software Development · NAIT — Completed / *Edmonton, AB*

- Networking fundamentals · Systems administration · Software development · Database management · IT project management

References available upon request · raghv.dev · github.com/HomeLab-Raghav