Karan Soni

SOC Analyst | Security Operations | Vulnerability Management
Oshawa, ON, Canada | +1 438-773-0899 | sonikaran8899@gmail.com
linkedin.com/in/karan-soni-4b56a11b4 | github.com/karansoni8 | karansoni8.github.io/Karan-s-Portfolio

PROFESSIONAL SUMMARY

Security operations analyst with hands-on Security Information and Event Management (SIEM) experience across Elastic Stack, Splunk, and Security Onion, built through a seven-host detection lab and enterprise IT support. Writes and tunes detection rules mapped to MITRE ATT&CK, triages alerts end to end, and documents investigations, runbooks, and escalation paths. Available immediately.

TECHNICAL SKILLS

Security Operations and Incident Response: Alert triage, detection engineering, threat hunting, incident investigation and documentation, escalation workflows, playbooks and runbooks, Indicators of Compromise (IOC), MITRE ATT&CK mapping, vulnerability management

SIEM and Monitoring: Elastic Stack (Elasticsearch, Logstash, Kibana), Kibana Query Language (KQL), Splunk and Universal Forwarder, Security Onion, Sysmon, Zeek, Snort, Syslog, Zabbix, log correlation, alert tuning, dashboarding

Networking: TCP/IP, LAN/WAN, VLAN, DNS, DHCP, VPN, routing and switching, OSPF, Cisco IOS, Cisco ASA, pfSense, Wireshark, Nmap, packet analysis

Systems and Identity: Windows Server 2019/2022, Active Directory (AD), Group Policy (GPO), Azure AD (Entra ID), Microsoft 365, Exchange Online, Public Key Infrastructure (PKI), AD Certificate Services, Ubuntu, RHEL, Kerberos, SSSD

Scripting and Automation: Python, Netmiko, PowerShell, Bash, VMware, Hyper-V, Docker, Microsoft Azure, AWS, Kali Linux, Metasploit

Governance and Service Management: NIST Cybersecurity Framework, ISO 27001, CIS Benchmarks, COBIT, ITIL, GDPR, ServiceNow, Jira, SLA tracking

PROFESSIONAL EXPERIENCE

Independent Security Consultant | *Security Health Check*, Ajax, ON — Sep 2025 – Present

- Deliver security assessments for small businesses without internal IT, covering identity hygiene, patch posture, endpoint configuration, backup validation, and network exposure, with prioritised remediation steps.
- Maintain a threat intelligence knowledge base of adversary techniques and control mappings, and validate every recommendation against live attack traffic in a self-built lab before it reaches a client report.

IT Support Technician | *Logic Play Web Solutions*, Oakville, ON — Jan 2025 – Aug 2025

- Resolved 60+ incidents per month through ServiceNow and Jira with 90% first-contact resolution, documenting symptoms, investigation steps, priority, business impact, and escalation actions.
- Administered Active Directory accounts, Group Policy, and access controls, applying least-privilege review during onboarding and offboarding.
- Supported LAN and WAN infrastructure using Wireshark and Nmap for traffic and anomaly analysis while sustaining 99% uptime; authored runbooks, standard operating procedures, and knowledge base articles that cut mean response time by 20%.

SECURITY PROJECTS

SOC Detection Lab, seven hosts | *Elastic SIEM, Sysmon, Fleet, Zeek, pfSense, Kali Linux, Metasploitable 2*

- Built a segmented blue-team environment with Elastic Agent and Fleet enrolment, Sysmon endpoint telemetry, and Zeek network monitoring feeding a central SIEM.
- Wrote and tuned nine KQL detection rules mapped to MITRE ATT&CK, covering credential dumping via LSASS handle access (T1003.001), encoded PowerShell (T1059.001), and low-jitter command-and-control beaconing (T1071.001).
- Ran attacks from Kali against lab targets to verify each rule fired, documenting eighteen mapped techniques with coverage status and three named detection gaps.
- Built Kibana threat-hunting dashboards with 12+ queries for credential abuse, failed-logon spikes, and lateral movement, and configured alert thresholds, retention, and log-source health checks with documented triage and escalation criteria.

Active Directory, PKI, and Monitoring Labs | *Windows Server, AD Certificate Services, SSSD, Kerberos, Zabbix*

- Deployed a Public Key Infrastructure with AD Certificate Services and a custom Encrypting File System certificate template, joined Ubuntu hosts to the domain using realm, SSSD, and Kerberos, and built Zabbix SNMP monitoring across network devices, diagnosing failures caused by DHCP-driven IP address drift.

Network Simulation, Linux Hardening, and Automation | *Cisco Packet Tracer, pfSense, OSPF, VPN, Ubuntu, RHEL, Python, Netmiko, PowerShell*

- Designed a multi-site topology with inter-VLAN routing, OSPF, DHCP, DNS, and site-to-site VPN, documenting addressing, firewall rules, and troubleshooting procedures.
- Hardened Linux servers with SSH key authentication, host firewall rules, privilege separation, and patch-alerting scripts; automated Cisco configuration deployment with Python and Netmiko.

EDUCATION

Cybersecurity Graduate Certificate | *Durham College*, Oshawa, ON
Diploma, Network Management with Cisco and Microsoft | *LaSalle College*, Montréal, QC
Bachelor of Computer Applications | *Parul University*, Vadodara, India

CERTIFICATIONS

Cisco Networking Academy Course Certificate – CCNA: Enterprise Networking, Security and Automation, Jan 2025 *(course certificate, not the 200-301 exam)*

In progress: CompTIA CySA+ (CS0-004), exam scheduled | Cisco CCNA 200-301 | CompTIA A+ | CompTIA Network+ | Microsoft SC-900