

Suman Sedhai, CISSP

TORONTO, ONTARIO

Summary

Cyber Security Engineer (CISSP) with 6+ years of experience designing and securing enterprise networks and endpoints across cloud and on prem environments. Expertise in zero-trust architecture, EDR/XDR, vulnerability management, and incident response. Proven success in leading threat detection, automation, and compliance initiatives aligned with frameworks such as NIST CSF and MITRE ATT&CK. Skilled in Python scripting, SIEM integration, and cross-functional collaboration to strengthen enterprise security posture.

Core Competencies

Network Security: Penetration Testing, Vulnerability Analysis, Antivirus software, disaster management/recovery, Security Architecture, Zero-Trust Frameworks, EDR/XDR, Network Security, SIEM (Arctic Wolf), Vulnerability Management, Threat Intelligence, and Incident Response

Identity & Access Management: IAM (O365, Entra, ADDS), Privileged Access Management, Authentication and Authorization

Compliance & Frameworks: MITRE ATT&CK, NIST CSF, ISO 27001, SOC 2 Compliance, Risk and Gap Assessment, Tabletop Exercises

Computer Networks: Windows/Linux Server Administration, CISCO, DHCP, DNS, TCP/IP, Firewall

Automation & Programming: Security Automation (Python), Metrics and Dashboard Development

Operating Systems: Windows, MacOS, Linux

Management: Team and conflict management, leadership skills

People: Decision-making, Dependability, Active Listening, Empathy, Friendliness

Experience

Concierge Security Engineer 3 Engineer 2

Sep 2023 – Current Concierge Security
June 2022 to Sep 2023

Arctic Wolf

Waterloo, Canada

- Partner closely with enterprise clients' CISO teams to design and implement zero-trust-aligned security architectures and drive the adoption of modern endpoint and network defense strategies.
- Act as subject-matter expert for EDR/XDR tooling (CrowdStrike, Sentinel One, Defender for Endpoint, Arctic Wolf Platform), guiding clients on configuration, detection tuning, and response strategies.
- Develop and maintain incident response playbooks, threat detection dashboards, and automated alerting rules to strengthen visibility and shorten mean time to response (MTTR) by 45%.
- Lead vulnerability management and endpoint compliance initiatives, reducing critical vulnerabilities by 70% across multiple enterprise environments.
- Collaborate cross-functionally with SOC, Compliance, and Customer Success teams to ensure security controls meet NIST CSF, ISO 27001, and SOC 2 standards.
- Analyze threat intelligence feeds and security telemetry to identify emerging attack vectors, create detection use cases, and recommend proactive countermeasures.
- Drive security automation using Python and Bash, improving the efficiency of alert triage and threat correlation processes by 35%.
- Mentor junior analysts in incident response, scripting, and stakeholder communication; supported onboarding and training programs for new team members.
- Participate in on-call rotation, triaging escalated L2/L3 incidents, and coordinating remediation efforts with SOC teams.

Technical Support Specialist (IT Security)

July. 2019 – May 2022

MacDon Industries Ltd.

Winnipeg, Manitoba

- Managed daily information security operations, monitoring and remediating vulnerabilities, and performing in-depth log and forensic analysis during incident investigations.
- Deployed and managed firewalls, IDS/IPS, endpoint security, and network monitoring tools, ensuring 99.9% uptime for critical systems.
- Participated in security audits and risk assessments, documenting controls and recommending policy updates aligned with ISO 27001 and SOC 2 standards.

- Researched and implemented new security solutions (data loss prevention, intrusion detection, vulnerability scanning) to proactively mitigate risks.
- Developed and maintained technical documentation, remediation plans, and user awareness materials to improve overall security posture.

ELECTRONICS AND COMPUTER ENGINEER

May. 2016 - Apr. 2017

Habre Technology Private Limited

Pulchowk, Nepal

- Designed and implemented secure client network infrastructures with strong authentication and access controls.
- Developed scripts and tools in Python and C++ for system optimization and automation of network monitoring tasks
- Conducted system analyses, database queries, and LAN design to improve operational security and efficiency.

COMPUTER NETWORK TECHNICIAN INTERN

Jan. 2016 - Jul. 2017

Softech Foundation Private Limited

Kathmandu, Nepal

- Designed and maintained LAN and Wireless networks and configured the firewall for internal office usage
- Maintained, troubleshoot, and administered the use of local area networks (LANs), wide area networks (WANs), mainframe networks, computer workstations, connections to the Internet, and peripheral equipment
- Solved problems related to network services, printers, and connections by adopting a procedural method that saved time and resources
- Conducted tests and performed security and quality controls by regularly assessing vulnerabilities and loopholes according to office standards

TELECOM TECHNICIAN

Sep. 2009 - Nov. 2011

United Telecom Limited (UTL)

Kathmandu, Nepal

- Supervised test operation of different telecommunication equipment, such as central server unit, cables, gateway devices, UPS, and battery bank to support 99.99% runtime
- Performed electrical wiring, design, and routine tasks such as testing and fault identification in different base transceiver station(BTS) locations and successfully operated 200 BTS all over Nepal for UTL
- Performed optical fiber splicing and new fiber connections in different sites as a backup connection to avoid downtime
- Diagnosed and located faults and replaced or repaired telecommunications equipment as per the instructions of senior engineers
- Completed tests and prepared reports related to battery bank status, generator, and air conditioners for the smooth operation of the central office and base transceiver station (BTS), and kept service records for future usage
- Performed inventory management and store management, including day-to-day updates of the status of tools and machines required by using real-time online software tools

Other Experience

CUSTOMER EXPERIENCE SALESFLOOR ASSOCIATE [PART TIME]

June 2018 – Nov. 2019

Walmart Winnipeg North Supercenter

McPhillips, Winnipeg

- Answering customer queries and addressing the problem quickly, satisfying the customers in person and via phone
- Helping customers select the best product that fits their needs and maintaining a visually appealing and clean aisle
- Interacting with customers with the latest designs and trends, maintaining shelves full and always replenished, and promoting customer satisfaction
- Mentoring newly joined associates regarding daily operations within the store

Education

POST DEGREE DIPLOMA, NETWORK SECURITY

The University of Winnipeg

Aug. 2017 - Oct. 2018

Winnipeg, Manitoba

BACHELORS IN ELECTRONICS AND COMMUNICATION ENGINEERING

Institute of Engineering, Pulchowk Campus

Nov. 2011 - Jan. 2016

Pulchowk, Nepal

Extracurricular Activity

APPLICATION DEVELOPER

Institute of Engineering

Nov. 2011 - Jan. 2016

Kathmandu, *Nepal*

- Actively participated in different programming language competitions
- Developed applications using C, C++, and Python as academic projects and non-academic projects
- Developed a machine learning application using MATLAB that can recognize Devanagari characters as an OCR application as the final academic project in Bachelors

CORE MEMBER

Robocon 2013

Oct. 2012 - Aug. 2013 ABU

Danang, Vietnam

- Gained expertise in the design, modification, and testing of hardware and software components of automatic and manual robots
 - Designed a hand controller for maneuvering robots' movement
- Participated in different training and seminars to obtain up-to-date technical knowledge in robotics for better robotics development
- Designed, implemented, and practiced various safety regulations to protect peers and the workplace from hazards

MEMBER AND MENTOR

Robocon 2014

Oct. 2013 - Aug. 2014 ABU

Pune, India

- Provided ideas and suggestions related to the design and application of electromechanical components for manual and automatic robots
- Mentored six core team members for different project-related activities to achieve goals within the time

FOUNDER & TECHNICAL WRITER

Graphene Magazine

Mar. 2012- Mar. 2013

Pulchowk, Nepal

- Drafted and wrote articles for a yearly magazine about IT technologies, robotics, and technical innovations to keep students up to date about recent trends and technology

Certifications

(ISC)² Certified Information Systems Security Professional (CISSP) - Active