Harsimar Singh Sudan

CYBERSECURITY ANALYST - SIEM, Identity & Access Management, and EDR Tools

harsimarsingh553@gmail.com (+1) 647-553-9025 Toronto LinkedIn

SKILLS

- **Programming & Web Tools**: Python, Java, JavaScript, C#, SQL, Kali Linux, HTML5, CSS, Azure, AWS.
- **Security Platforms**: Burp Suite, Metasploit, SIEM, OpenEDR, Kape, Kibana, Volatility, Autopsy, Wireshark.
- **Network & Threat Analysis**: Traffic monitoring, NGFW, IDS/IPS, packet capture, SQL injection mitigation.
- **Cloud & Compliance**: Microsoft Compliance Manager, Defender, Sentinel, HIPAA, GDPR, and IAM Setup.
- **Incident Response**: SOAR integration, device baseline configuration, phishing detection, and access control.

WORK EXPERIENCE

Inventory Associate **January 2024 – Present**
WIS International *Greater Toronto Area*

- Increased inventory accuracy by 28% using systematic barcode scanning, cross-referencing SKU data, and reconciling discrepancies for luxury, retail, and grocery clients including Holt Renfrew, Balenciaga, and Loblaws.
- Decreased stock shortages by 22% through standardized counting procedures, variance reconciliation, and validation against POS system records at multi-location client sites with high-volume merchandise turnover.
- Enhanced report generation speed by 35% through automated & optimized inventory data processing workflows, enabling faster turnover of analytical insights for clients such as Shoppers Drug Mart, Sephora, & Home Depot.
- Coordinated large-scale stock audits for national retailers, aligning physical counts with client-specific inventory management policies, and achieving a quantifiable drop in shrinkage rates across different product categories.
- Revamped team audit workflows to improve counting speed by 15% without compromising accuracy, utilizing optimized scanning sequences and zone-based allocation to support rapid completion of high-priority counts.

Cybersecurity Analyst **July 2021 – December 2023**
Alpha Arise Pvt. Ltd *India*

- Elevated security compliance posture by 35% through configuration of Microsoft Compliance Manager dashboards, mapping controls, and validating adherence to regulatory frameworks across enterprise-level systems.
- Executed and advanced database security strategies, managing targeted vulnerability assessments, reconfiguring permissions, and applying parameterized queries to eliminate SQL injection incidents by 25% within two months.
- Enforced network traffic control and firewall policies to detect anomalies, filtering suspicious packets across 40+ endpoints, resulting in a measurable reduction in potential intrusion attempts and enhancing network integrity.
- Coordinated the use of Microsoft Azure Defender and Sentinel SIEM for threat detection, developing automated rule sets and response workflows to enhance safeguard effectiveness by 30% against live cyber intrusion vectors.
- Designed and executed phishing awareness and secure login campaign, integrating MFA and password hygiene protocols, boosting employee cybersecurity compliance by 42% and mitigating credential-based security risks.

PROJECT EXPERIENCE

NIST CSF 1.1 Cybersecurity Policy
Team Lead

- Designed a cybersecurity policy framework aligned with NIST CSF 1.1, reducing security control gaps by 35% and enhancing resilience of critical infrastructure in a multinational MSSP hybrid deployment environment.
- Engineered network segmentation, NGFW, IDS/IPS, and Zero Trust framework, improving perimeter and internal defense effectiveness by 40% while reducing lateral movement risks across interconnected enterprise networks.
- Deployed cybersecurity incident response and disaster recovery frameworks with defined RTO/RPO, SOAR automation, and tabletop exercises, reducing incident containment time by 32% and recovery duration by 28%.

EDUCATION

Postgraduate Diploma in Cybersecurity and Computer Forensics January 2024 – September 2025
Lambton College, Mississauga
Bachelor of Computer Application July 2019 – June 2022
Bharati Vidyapeeth University, India

CERTIFICATIONS

- **CompTIA Security+** (In Progress) – CompTIA, • **ISC2 Certified in Cybersecurity** – ISC2
- **Microsoft Cybersecurity Analyst** – Coursera, • **Google Cybersecurity Certificate** – Coursera
- **Fortinet Certified Associate Cybersecurity** – Fortinet, • **Introduction to Cybersecurity** – Cisco
- **Fortinet Certified Fundamentals Cybersecurity** – Fortinet, • **ANZ Australia (Simulation)** – Forage
- **IBM PY0101EN: Python Basics for Data Science** – EDX, • **Tata Group (Simulation)** – Forage
- **Introduction to EASY Framework for Threat Intelligence** – AttackIQ, • **Splunk Power User** – Udemy
- **AIG Shields Up (Simulation)** – Forage, • **Deloitte Australia (Simulation)** – Forage