

DAVINDERNAIN SINGH SEHGAL

Cybersecurity | Security Operations | Incident Response & Threat Detection | Cyber Resilience

Boston, USA – Relocating to Thane, Maharashtra, India | +91 9653282499 | Davindernain.sehgal@icloud.com
[linkedin.com/in/Davindernain](https://www.linkedin.com/in/Davindernain) | [Complete CV](#)

PROFESSIONAL SUMMARY

Cybersecurity professional with an MS in Cybersecurity (Northeastern University) and hands-on U.S. experience running security operations for the City of Boston's Boston Public Library, covering 25+ locations and a multi-institution network. Directs day-to-day incident triage and response, vulnerability management, penetration testing, WAF and identity security as the sole security owner, reporting to the CTO. Results include 100% MFA coverage with passwordless rollout, a 70% cut in malicious bot traffic, a 90% lift in phishing reporting, 100+ end-of-life systems retired and a \$250,000 (~₹2.4 Cr) FCC security grant. Seeking a senior security operations / incident response role in Mumbai.

KEY ACHIEVEMENTS

- **\$250,000 (~₹2.4 Cr)** FCC Cybersecurity Pilot Program grant won by leading research, documentation and a multi-department application.
- **100% MFA coverage** across the organization, with a passwordless (passkey) rollout, delivered through enforced controls, guides and training.
- **70% reduction** in malicious bot traffic and automated attacks through WAF deployment and tuning.
- **90% increase** in phishing detection and reporting over 8 months via recurring simulations and role-based training.
- **100+ end-of-life systems** retired or upgraded in a multi-year program, materially shrinking the attack surface.
- **End-to-end ownership** of security for 25+ locations and a multi-institution network, reporting directly to the CTO.

CORE COMPETENCIES

Incident Response & Triage • Threat Detection (SIEM/EDR) • Vulnerability Management & Pen Testing • WAF, IDS/IPS & Firewalls • Identity & Access (MFA, Passwordless) • Digital Forensics & OSINT • Security Awareness & Phishing Simulation • Risk & Vendor Assessment

PROFESSIONAL EXPERIENCE

City of Boston – Boston Public Library (BPL), Boston, MA, USA

Nov 2023 – Present

IT Cybersecurity Analyst & BPL Cybersecurity Officer

Sole security owner for the Central Library, 25 branches and the Metro Boston Library Network (MBLN), a multi-institution consortium; bridge between the City of Boston Cybersecurity Operations team and BPL leadership.

- **Ownership:** Sole security resource reporting to the CTO for 25+ locations and the MBLN consortium, accountable for incident response, risk, auditing and security metrics.
- **Incident response:** Triage alerts daily and lead investigation, containment and remediation of a high monthly volume of incidents across Network, Server, Application, Help Desk and A/V teams; liaise with law enforcement and City counterparts.
- **Playbooks:** Built scenario-specific IR strategies and playbooks, plus playbooks for security operations, access management and endpoint security.
- **Perimeter defense:** Deployed and tuned a Web Application Firewall protecting public-facing systems, cutting malicious bot traffic and automated attacks by 70%; manage IDS/IPS, anti-malware, firewalls and encryption.
- **Vulnerability management:** Led internal vulnerability assessments and penetration tests (Metasploit, Nmap, Burp Suite) and drove remediation; led a multi-year program retiring or upgrading 100+ end-of-life systems.
- **Identity security:** Led MFA and passwordless (Microsoft Authenticator, passkeys) rollout to 100% organizational coverage.
- **Endpoint & asset control:** Maintained asset and license inventories; designed separate risk-based configurations for public-access and staff computers across dozens of locations.
- **Awareness:** Phishing simulation and security training program raised detection and reporting by 90% over 8 months.
- **Threat intelligence & stakeholders:** Track the threat landscape through threat intelligence, listservs and security organizations, and brief IT leadership on emerging vulnerabilities and countermeasures; coordinate with the City of Boston Cybersecurity Operations team on city-level security practices.
- **Resilience & vendors:** Directed business continuity and disaster recovery planning with Server and Network teams; point of contact for external vendors; advised IT leadership on emerging threats before systems reached production.
- **Governance & funding:** Secured a \$250,000 (~₹2.4 Cr) FCC Cybersecurity Pilot Program grant; led third-party risk assessments against NIST and CISA and wrote security standards and BCP/DR procedures.

Village Book Builders (Non-Profit), Boston, MA, USA**Apr 2023 – Nov 2023***Cybersecurity Associate (Volunteer)*

- Developed security policies and SOPs on the ISO 27001/27002 framework; ran cross-functional risk assessments that cut projected impact costs by over \$130,000 (~₹1.25 Cr).
- Built ransomware-specific incident response plans and delivered company-wide IT risk training for full-time and part-time staff.

Commonwealth Financial Network, Waltham, MA, USA**Jan 2023 – Apr 2023***Information Security Capstone*

- Built an operational risk register and monitoring system (Trello, Jira, Power BI) across 7+ departments on Agile 3-week sprints; authored training material and technical documentation.

YourDigitalBro Pvt Ltd, Mumbai, India**Sep 2020 – Jun 2021***IT Security Intern*

- Deployed firewalls, IDS/IPS and event monitoring, raising proactive detection and response capability by 35% and cutting unauthorized access attempts by 50%.
- Administered infosec policies protecting PII for 550+ clients monthly; security awareness training cut phishing and malware incidents by 25%.

Freelance, Mumbai, India**Aug 2018 – May 2021***IT Consultant*

- Secured 87 clients with anti-malware and encryption controls, trained 50+ on phishing and MFA, and resolved 95% of issues within 24 hours.

EDUCATION**MS Cybersecurity** – Northeastern University, Boston, MA, USA**May 2023***Coursework: Security Risk Assessment & Audits, Security Governance Risk & Compliance (Cyberlaw), Network Security, Software Vulnerabilities, Digital Forensics, Critical Infrastructure***BSc Computer Science** – University of Mumbai, Mumbai, India**Jun 2021****TECHNICAL SKILLS****Detection & Tools:** Microsoft Defender, SentinelOne, Splunk, QRadar, Wireshark, Snort IDS, pfSense, WAF, Bitdefender, IBM X-Force**Offensive & Forensics:** Nmap, Metasploit, Burp Suite, Nikto, Kali Linux, FTK Imager, Autopsy, Spiderfoot, Maltego, Shodan**Frameworks:** NIST 800-30/800-53, CISA, ISO 27001, MITRE ATT&CK, OWASP, GDPR, HIPAA, PCI DSS, SOC 1, SOX**Cloud & Languages:** AWS, Microsoft Entra ID; SQL, Python, Java, Bash**SELECTED PROJECTS (NORTHEASTERN UNIVERSITY)**

- **IDS/IPS Implementation:** pfSense firewall and Snort IDS with zero-trust, default-deny policies on two networks; used Nmap and packet inspection to find and close gaps.
- **Digital Forensics:** FTK Imager and Autopsy investigations of insider-threat, harassment and malware scenarios across four systems with chain-of-custody discipline.
- **Passive Reconnaissance:** OSINT assessments of two e-commerce platforms with 8+ tools (Spiderfoot, Maltego, Shodan) identifying exposed ports, DNS records and CVEs.
- **Incident Response Playbook:** Team guidelines across all NIST IR phases for unauthorized access, SQL injection and data leaks.

PROFESSIONAL DEVELOPMENT & AFFILIATIONS

- **In progress:** CISSP – self-study completed across all 8 domains.
- **Hands-on programs:** TryHackMe Jr. SOC Analyst (Level 1); AIG Shields Up (incident response); Mastercard (phishing campaign analysis). Member of (ISC)², SANS and MS-ISAC.

Languages: English, Hindi, Marathi, Punjabi | **Notice period:** 30–45 days (negotiable) | **Preferred location:** Mumbai / Thane**Interests:** Music (ukulele, music production), emerging technology, competitive and RPG gaming, travel, film/TV and anime.