Hemraj Patel

Hemraj@osiris.cyber.nyu.edu | +1 (718) 513-8585 | LinkedIn | Personal Webpage | GitHub | New York 11228, US

Aspiring Cybersecurity practitioner, studying at New York University with hands-on experience in SOC operations, incident response, vulnerability management and remediation, and application security. Strong background in security automation, SIEM/SOAR, threat intelligence, and compliance frameworks (NIST CSF 2.0, ISO 27001, MITRE ATT&CK), with growing focus on AI and cloud security.

EDUCATION

Master of Science | Cybersecurity | ***GPA: 3.57*** **|** ***New York University*** | New York, United States **Sep 2024 – May 2026**

Courses: Application Security, Information Security & Privacy, AI Governance, Cyber Resiliency Management, Network Security, Vulnerability Assessment & Penetration Testing (VAPT), Cloud Security, Cryptography, Ethical Hacking, Digital Forensics

SKILLS

Core — Incident Response & SIRT Operations, SOC Monitoring, Cyber Threat Intelligence (TTPs, IOC Analysis), Threat Hunting, Risk Assessment & Management, Firewall & Network Security, Endpoint Detection & Response, IAM & Access Control, Web Application Security (SAST, DAST, OWASP Top 10), Information Security, Cloud Security, Application Security, Data & AI Security

Tools — Burp Suite, Wireshark, Metasploit, OWASP ZAP, Autopsy, Encase, FTK, Splunk, Elastic Stack (ELK), SIEM/SOAR (Phantom), Snort, Nessus, OpenVAS, Nmap, Tcpdump, Jira, Microsoft TMT, SIEM, Tenable, OpenSSL, Cloudfox, Cobalt Strike, Shodan, Censys, EC2, S3

Framework/Compliance — NIST CSF, ISO 27001, CIS Controls, MITRE ATT&CK, PCI DSS, GDPR, CCPA, HIPAA, SOC 2, NIST AI RMF

Programming Languages — Python (Security Automation, Scripting), Bash, JavaScript, SQL, C++, REST APIs, Git, CI/CD, HTML, React

Certifications — CISSP (In Progress), CCSK (In Progress), CompTIA Security+, Google Cybersecurity, Data Science

PROFESSIONAL EXPERIENCE

Research Assistant | ***New York University*** **|** New York, United States **Sep 2024 – May 2026**

- Researched AI-driven cyber threats and adversarial ML models impacting data integrity and system security, proposed risk-based mitigation techniques integrated with NIST AI RMF and ISO 42001 frameworks for GRC course material.
- Designed and delivered security awareness sessions and interactive workshops on data protection, incident response, regulatory compliance, and cyber hygiene, using Microsoft Office 365, improving student phishing detection by 30%.
- Supported GRC and compliance initiatives (ISO 27001, NIST CSF 2, GDPR), improving compliance posture by 20%.

Security Engineer | ***Span Inspection System Pvt. Ltd.*** | Gandhinagar, India **May 2023 – July 2024**

- Conducted vulnerability research and attack surface analysis using Nessus and OpenVAS, incorporating anomaly detection techniques to enhance cloud and on-prem threat visibility, remediating 100+ vulnerabilities and reducing high-severity risks by 40%.
- Orchestrated patch management workflows by integrating CVE and CVSS vulnerability data into Splunk dashboards and MITRE ATT&CK–aligned playbooks, increasing endpoint compliance to 95% and improving CIA triage efficiency by 35%.
- Performed forensic network and packet-level analysis using Wireshark and Zeek to detect data exfiltration attempts, anomalous traffic, and misconfigurations, strengthening network defenses and improving detection accuracy by 25%.

Security Analyst | ***TechDefenceLabs Solution Pvt. Ltd.*** | Ahmedabad, India **May 2022 – May 2023**

- Performed comprehensive vulnerability assessments and penetration tests (VA/PT) using Burp Suite, Metasploit, and OWASP ZAP, identifying and remediating 150+ application flaws and improving the organization's security posture by 15%.
- Monitored and analyzed security events in Splunk and ELK SIEMs, automating alert correlation and integrating findings with forensic tools (EnCase, FTK, Autopsy) to support rapid incident investigations and reduce false positives by 28%.
- Supported SOC operations and compliance audits, performing control mapping, gap analysis, and continuous monitoring.

PROJECTS

LLM Package Hallucination – Software Supply Chain Security Tool (OSIRIS Lab, NYU)

Developed LLM PackageGuard, a Python-based scanner that detects and catalogs hallucinated or malicious dependencies in AI-generated code, validating imports against PyPI, OSV, and GitHub APIs, and analyzing hallucination patterns across multiple LLMs (GPT-3.5, GPT-4, Gemini, and Cohere) to improve software supply chain security and model reliability.

Swiper No Swiping – PII Detection Chrome Extention

Developed Swiper-No-Swiping, a Chrome extension that identifies and flags Personally Identifiable Information (PII) in sensitive documents before web uploads, implementing an intuitive UI-based real-time scanning workflow to prevent accidental exposure of confidential data and enhance organizational data privacy and compliance.

EXTRACURRICULAR

Osiris Labs (NYU Center for Cybersecurity) — Core Member; represented NYU in national CTFs (Top 10 nationwide), organized and coordinated CSAW (largest student-run event), applied strategic problem-solving, and conducted security research and projects.

School Athlete — Silver medalist at the National Swimming Tournament (2019, 2023), with 18 years of competitive training, demonstrating discipline, teamwork, endurance, and long-term commitment.