Darsh Kapadia

Chicago, IL | linkedin.com/in/darshkapadia

EDUCATION

Illinois Institute of Technology, Co-Terminal MAS in Cyber Forensics & Security — Jan 2025 – May 2027

Illinois Institute of Technology, BS in Applied Cyber Security & Information Technology — Aug 2023 – May 2027

- GPA: 3.96

CERTIFICATIONS

ISC2 CISSP — Expected May 2027

AWS Certified Cloud Practitioner — Expected May 2026

CompTIA Security+ — Apr 2023

EXPERIENCE

Identity Security Engineer Intern, GE HealthCare – Waukesha, WI — May 2025 – Aug 2025

- Automated CyberArk Privilege Cloud onboarding, safe provisioning, role assignments, and license management using REST APIs, Python, Bash, and PowerShell, improving operational efficiency by 25× and saving $200K+ annually in licensing costs.
- Integrated several thousand high-risk Ansible and SOX accounts into CyberArk, strengthening privileged access controls and aligning with compliance standards.
- Authored comprehensive technical documentation and standard operating procedures (SOPs) for identity security processes, facilitating knowledge transfer and operational consistency.
- Administered core IAM services, resolving ServiceNow tickets for access provisioning, identity lifecycle management, and security incidents.

Technology Officer Volunteer, Sanskriti – Illinois — Aug 2022 – Ongoing

- Administer Google Workspace (including provisioning, access control, and security) for a 50-member organization, enabling secure collaboration and resource delivery to external sponsors and donors.
- Develop and maintain website, e-commerce platform, and integrations, raising $50K+ in non-profit donations in two years.

Information Technology Intern, Valley View School District – Illinois — Aug 2022 – May 2023

- Streamlined device provisioning and access management for 3,600+ users using Google Admin Console, Okta LDAP, and custom automation to enforce access controls.

PROJECTS

Homelab — Apr 2017 – Ongoing

- Secured a full-stack home network with OPNsense (DHCP, DNS, Firewall, VPN, IDS/IPS) and Wazuh SIEM/XDR; enforced identity-aware access using Authentik IdP and Cloudflare Zero Trust.
- Managed Proxmox and Docker environments with reverse proxies, hosting containerized applications and smart devices via Home Assistant.
- Performed red/blue team exercises with Kali, Nmap, Metasploit, Burp Suite, and forensic analysis using Autopsy, Volatility, FTK Imager; hosted redundant services on AWS, Azure, and GCP.

Responsible Vulnerability Disclosure — Oct 2025

- Discovered a critical access control misconfiguration in Illinois Tech's Navigate360 portal exposing sensitive PII and entire student body academic records.
- Documented a high-impact (FERPA) vulnerability and followed responsible disclosure procedures by reporting findings directly to institutional leadership, leading to its remediation.

CBORD Reverse-Engineered API — Oct 2024

- Reverse-engineered CBORD CS Access app's private HTTPS API with Burp Suite to map authentication flows and endpoints.
- Built a Python microservice (Docker-deployed) exposing a simplified REST API for voice-activated door control via Siri.

Discord Bot — Sep 2023

- Developed a Python-based Discord bot integrating with the Proxmox REST API for VM lifecycle management and real-time server monitoring.
- Automated idle-shutdown logic to reduce resource usage and created a secure, permission-based self-service portal for users.

SKILLS

Operating Systems: Linux (Kali, Debian, Ubuntu, Arch, Alpine, Fedora), Windows, macOS, Android, iOS

Security & Identity: Authentik (IdP), Cloudflare Zero Trust (SASE), CyberArk Privilege Cloud (PAM), Suricata (IDS/IPS), Okta LDAP (IAM), OPNsense (Firewall), pfSense (Firewall), Saviynt (IGA), Wazuh (SIEM/XDR), WireGuard (VPN)

Cloud & Infrastructure: Ansible, AWS, Azure, DHCP, DNS, Docker, GCP, MDM, OAuth, Proxmox, QUIC, REST APIs, ServiceNow, VMware

Reconnaissance & Forensics: AnyRun, Autopsy, Burp Suite, FTK Imager, Gobuster, Maltego, Metasploit, Nessus, Nmap, Volatility, Wireshark

Programming & Scripting: Python, Bash, PowerShell, Java, JavaScript, SQL, HTML, CSS

Concepts & Frameworks: CISSP Domains, Containerization, Cryptography, Cyber Kill Chain, Digital Forensics, Least Privilege, OSI Model, OSINT, Virtualization, Vulnerability Analysis, Security+, SOX Compliance, TCP/IP, Zero Trust Architecture

Learning Platforms: HackTheBox, LetsDefend, PortSwigger Academy, TryHackMe

ACTIVITIES & SOCIETIES

Founder & Educator, Digital Literacy Program — Nov 2023 – Ongoing

Brother Mentor, Sigma Phi Epsilon – Illinois Beta — Nov 2023 – Ongoing

- Former President
- Former VP Recruitment
- Former VP Programming

Scholar & Volunteer, Camras Scholars Program — Aug 2023 – Ongoing