Chinmay Deore

Fort Lauderdale, FL | chinmaydb@outlook.com |+1 (734) 612-9351

linkedin.com/in/chinmay-deore-547531297/ | github.com/ChinmayDeore | ChinmayDeore.github.io/chinmayd

Education

Wayne State University Detroit, MI

*Bachelor of Engineering in Computer Science – **GPA: 3.32*** *May 2025*

Certifications: Google Cybersecurity Certificate, CITI Health Information Privacy and Security (HIPS), CompTia Network+ (In-Progress)

Experience

Center for Urban Studies July 2024 – April 2025

IT/IS Technician (Student Assistant) *Detroit, MI*

- Provided Tier 1→Tier 2 support for **100+** hybrid staff. Owned ticket lifecycle in **Jira Service Management**, delivering fixes via **Quick Assist**, **RDC**, and **Teams** screen-share/live events while documenting knowledge bases to cut repeat incidents.
- Remediated endpoint issues across **Windows 10/11** and **macOS** through performing driver/firmware updates, **UEFI**/boot repairs, **BitLocker** unlocks, and disk imaging/cloning. Rebuilt machines after **SFC**/**DISM** integrity checks and **Event Viewer** triage.
- Managed identity and access in **Active Directory** (AD) incorporating **OU-aware** user provisioning, group design, **GPO** baselines, browser policy lockdown, and **PoLP** audits. Cleaned orphaned objects and standardized drive mappings.
- Stabilized floor-wide printing **MFP** fleets with static **IP/DHCP** reservations, Mac print workflows, jam/spooler/queue fixes, validated **LAN** switch ports, and enabled secure **HTTPS** admin with **DigiCert** trust to stop cert-warning lockouts.
- Restored **MySQL** dumps locally from Rackspace. Validated data integrity (**DDL**/**DML**) and reconciled copies with server copies.
- Centralized license lifecycle for o365, Adobe CC, and research tools. Mapped invoices to devices/users cutting dormant licenses.
- Consolidated multi-sheet Excel asset inventories and added formulas for reconciliation. Tracked loaners with **FWA**s, enforcing **HIPAA**/**NIST** style handling for SPII across research datasets.
- Ran **AV** staging for leadership presentations by integrating projectors/TVs and Meeting Owl 3 with Zoom hybrid setups.
- Supported **VoIP** softphones (Mitel Clearspan, Line2) for CATI lab that surveyed **60,000+** recipients seasonally. Contributed to **~85%** reduced call failures by validating call dispositions flows and scheduled windows tasks for daily database exports.
- Maintained endpoint fleet readiness for Windows 11 through scripted **TPM 2.0** inventory checks in **PS**. Flagged incompatible hardware and delivered a deprecation roadmap. Followed **enterprise green disposal** practices for obsolete equipment.
- Secured users against scareware pop-ups upon killing rouge **JS** sessions, cleaning browsers, and **verifying DNS/hosts**.
- Automated survey ops with **300+** batch-printed weekly label sets via **Remark OMR** collapsing manual steps to minutes.
- Tuned **SMB** performance via **IRPStackSize** via registry policy and throughput tests. Reduced timeouts for high-vol share moves.
- Troubleshot **BI** tools (**IBM SPSS/Cognos Analytics**) by correcting form-view errors and verifying org code availability.

Wayne State Cyber Defense Club September 2021– May 2025

Detroit, MI

- Blue-teamed across **Collegiate Cyber Defense Competition** (CCDC) seasons, placing 2nd in MI 2025. Triaged **SIEM** alerts, hunted anomalies, and filed time-boxed **Incident Reports** with clear timeline, **IoCs**, scope, containment, and lessons learned.
- Deployed **Splunk forwarders** for **Sysmon**, **journald**, **auditd**, and **NGFW** logs. Built saved searches to surface auth anomalies, suspicious **RDP**, service restarts, and webshell beacons across **10+** endpoints.
- Hardened **Windows/Unix** hosts through lockout policies, **RDS** lockdown, rotated **svc credentials**, disabled legacy protocols (Telnet), enabled **PowerShell** loggings, **LAPS**, and rebuilt **Docker** baselines to evict persistence.
- Tuned **Palo Alto NGFW**/**pfSense** policies comprised of **App-ID** style rules, **URL filtering**, **east-west** segmentation.
- Captured and analyzed traffic with **tcpdump/Wireshark**, carving **PCAPs** for **C2** patterns, **lateral movement**, and data **egress** attempts. Escalated with artifacts and **ATT&CK** mappings.
- Ran a **Proxmox** range reachable over **OpenVPN** for multi-session drills. Snapshot-reverted hosts to maintain reproducibility.

MAGMA – Stock Analysis Platform (Lead) | *Flask, PostgreSQL, Render, Syncfusion, Flutter, NeuralForecast* January - May 2025

- Owned end-to-end operability of a **Flask monolith** behind **HTTPS** (**TLS 1.2+**), designing a layered API with exception-safe **JSON** errors, health checks, and **graceful fallbacks** to prevent outages from paging the team.
- Productionized data flow with **Alembic migrations** and **SQLAlchemy** guardrails. Documented roll-forward/rollback steps and validated interface contracts in **Postman** before merges.
- Cut repeat latency from seconds to near-instant by implementing **cache-first retrieval** logic reducing 3rd-party API calls by **~80%**.
- Managed environment-scoped secrets applied **Bcrypt** for passwords, **AES-256** at-rest for sensitive fields, **OAuth2/JWT** session model, and **one-time passcode** (OTC) email verification via **SMTP**.
- Shielded app with **WAF** to damp **DDoS** credential-stuffing bursts, tuning rules from **ELK** and **4xx/5xx** patterns to reduce alerts.
- Codified **CI gates** with **Selenium** smoke suite for validating alignment with acceptance criteria.
- Deployed on **Render** with managed **PostgreSQL** and **L7 load balancer**. Parametrized queries only with **ORM-level** constraints.
- Handled stakeholder-facing reporting by keeping **RTM/SRS/Design/Test Plan** and **UAT** signoffs in sync.

Technical Skills

Development: Python, JS, HTML, PHP, JSON, XML Bash, PS, VSC, Vim, IIS, Flask, Flutter, Apache, nginx, Git, Selenium, .NET
Data Management: MySQL, PostgreSQL, MongoDB, DynamoDB, Redis, Microsoft Access/SMSS
Networking: PAN-NGFW, pfSense, ufw, iptables, OpenVPN, GlobalProtect, Postfix, Dovecot, Thunderbird, MobaXterm, PuTTy
Security Operations: Splunk, Suricata, Snort, fail2ban, MS Defender, Ansible, OpenVAS, Wireshark, tcpdump, netcat, Nessus
Cloud/Hosting: Azure, Entra ID, Intune MDM/MAM, o365, Heroku, Render, Google GCE/GCS, AWS EC2/S3/Lambda
Deployment/Management: Jira, AD, WDS, MDT, WAIK/ADK, SCCM, LAPS, Server Manager, AWS IAM, Docker, VirtualBox
Governance/SRE: PCI-DSS, HIPAA, GDPR, NIST 800-53, IEC, ISO 27002, ITIL, SOAR, CIA triad, ISSP, DRP/BCP, KPI/SLA/OLA, MTTR/MTBF