Dhyey Sanghvi

+1 623-206-9860 | dhyeysanghvi15@gmail.com | Linkedin | Github | Portfolio

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst Intern, **Projacs International** | **Doha, Qatar** **May 2024 - Jul 2024**

- Engineered an Airflow-based ETL pipeline in Python and PostgreSQL processing 1TB+ telemetry, improving data fidelity and cutting latency from 2s to 300ms.
- Designed a zero-trust data lake using AWS S3, IAM, and KMS, ensuring encryption-at-rest, access logging, and compliance for 100+ enterprise users.
- Integrated CloudTrail logs with Elasticsearch to automate anomaly detection, enhancing visibility across 12 construction regions and reducing detection time by 40%.
- Automated log normalization in Python to standardize JSON formats for SIEM ingestion, improving alert accuracy and cutting triage time by 35%.

Office Data Aide, **Human Resources Office - ASU** | **Tempe, AZ** **Aug 2023 - Jan 2024**

- Automated HR record validation using Python and Excel macros, reducing manual data entry time by 75% and ensuring consistent data accuracy across 350+ faculty profiles.
- Designed and maintained SQL-based relational databases for onboarding and payroll workflows, cutting query response times by 4× and improving retrieval efficiency for 20+ daily HR requests.
- Implemented access control reviews with IT using role-based permissions to safeguard sensitive employee information, ensuring compliance with FERPA and ASU data privacy policies.
- Created Python audit scripts to identify data anomalies and duplicate entries, enhancing reporting integrity and supporting quarterly compliance audits with zero record discrepancies.

Cybersecurity and IT Intern, **Keepet Containers** | **Gujarat, India** **May 2023 - Aug 2023**

- Deployed Suricata IDS in Docker containers to monitor 50GB+ network logs daily, reducing false-positive alerts by 26% through optimized rule configuration.
- Conducted vulnerability assessments using Metasploit and Burp Suite, identifying 12 critical exploits in internal VLANs and strengthening container security posture.
- Configured Elasticsearch pipelines to correlate multi-source logs from firewalls, DHCP, and app servers, improving incident traceability and achieving 99.2% SLA adherence.
- Delivered CIS-aligned vulnerability reports preventing $25K potential data loss, elevating vendor compliance and executive awareness of infrastructure risk.

EDUCATION

Arizona State University - *Bachelor of Science Computer Science (Cybersecurity),* **May 2026**
Minor: Mathematics | *Certified in Business Data Analytics*

PROJECTS

ThreatOps (Incident Investigation Simulator)

- Created end-to-end incident investigation casefiles that guide analysts from alert triage to containment and final reporting.
- Mapped scenarios to MITRE ATT&CK to strengthen threat-informed defense and coverage-driven analysis.
- Designed repeatable investigation steps (timelines, evidence queries, false-positive notes) to improve analyst consistency and decision quality.

CloudSentinel (AWS Cloud Security Lab)

- Built an AWS security posture + CloudTrail detection lab with attack simulation and guided remediation workflows to improve real-world incident readiness.
- Implemented IAM least-privilege analysis and policy linting patterns to identify risky permissions and tighten access control.
- Automated validation workflows in Python to make detections repeatable and auditable (security testing mindset and reproducible lab design).

AutoTriage (SOAR Pipeline and Dashboard)

- Built a SOAR-style workflow that enriches, deduplicates, correlates, scores, and routes security alerts end-to-end.
- Implemented prioritization logic that improves analyst throughput and consistency (automation-first triage design).
- Delivered an analyst-friendly dashboard and a reproducible demo environment, ensuring clear data flows and operational usability.

SKILLS

Security & Monitoring : Suricata IDS, Metasploit, Burp Suite, Elasticsearch, IBM QRadar, Wireshark, IAM, CIS/NIST Controls, Zero-Trust Architecture, Log Normalization, SIEM Pipelines, CloudTrail, Access Control Management

Programming & Databases : Python, Java, C/C++, SQL, PostgreSQL, MySQL, SQLite, R, VBA, JavaFX, JDBC, Excel Macros

Cloud & Infrastructure : AWS S3, IAM, KMS, CloudTrail, GCP, Docker, Apache Airflow, CI/CD Pipelines, Cloud-based Data Lakes, Role-Based Access Control

AI, ML & Data Frameworks : TensorFlow, scikit-learn, OpenCV, CNNs, Apache Spark, Predictive Modeling, Data Analytics, Feature Engineering

Visualization & Analytics : Tableau, Power BI, Matplotlib, seaborn, Interactive Dashboards, KPI Reporting, SQL-based Analytics