Disha Phatta

New Jersey, USA | +1 (646)457-1164 | dphatta@stevens.edu | Portfolio | LinkedIn

Education

Stevens Institute Of Technology - Present — Hoboken, NJ
Master of Science in Cybersecurity — *Sep 2024 – May 2026*

A.P Shah Institute Of Technology - CGPA 8.64 — Mumbai, India
Bachelor of Engineering in Information Technology with Honors in Cybersecurity — *Sep 2020 – May 2024*

Projects

SentinelX – Self-Aware Threat Detection Tool | *Python, AbuseIPDB, SOAR-like automation* — May 2025
- Developed a Python-based threat detection system integrating abuse databases, automated alerting, and GUI for SOC analysts.
- Simulated SOAR capabilities with custom workflows for automated response and indicator enrichment.
- Enabled analyst response through real-time monitoring, observable triage, and threat classification.

Visual Packet Tracer | *Python, Wireshark, KML* — Apr 2025
- Analyzed network packet data captured via Wireshark and mapped it to global geolocations using Python.
- Enabled real-time anomaly detection by visualizing live traffic patterns and network flow deviations.
- Supported threat hunting and network forensics with custom KML generation for packet visualization.

Custom Keylogger Project | *Python, pynput* — Jan 2025
- Developed a background keylogging tool using Python and pynput for educational red-team simulation.
- Captured keystrokes and logged data to file with exception handling for special character inputs.
- Explored endpoint monitoring, ethical implications, and detection countermeasures.

SOC Analyst Lab – Blue Team Series | *Sysmon, Sysinternals, Wireshark, VirtualBox* — Dec 2024
- Built a SOC lab using VirtualBox and Sysmon to analyze Windows event logs and detect IOCs.
- Practiced log aggregation, event correlation, and SIEM-based threat detection.
- Generated incident response reports with mitigation steps for simulated attack scenarios.

Security Incident Response Platform | *TheHive, Cortex, MITRE ATT&CK* — Oct 2024
- Configured TheHive for incident case management and Cortex for automated IOC enrichment.
- Simulated real-world incident response workflows through observable triage and task assignments.
- Mapped threats using the MITRE ATT&CK framework to identify tactics and techniques.

Vulnerability Management Lab | *VirtualBox, Nessus Essentials* — Sep 2024
- Deployed a virtual IT infrastructure and conducted vulnerability scans using Nessus Essentials.
- Applied patches and configuration updates to remediate high-risk vulnerabilities.
- Maintained vulnerability management reports with remediation metrics and audit records.

AWS IAM Security Implementation | *AWS Console, IAM Policies, MFA* — Aug 2024
- Designed a secure IAM architecture with role-based access and least-privilege policies.
- Configured users, groups, and enforced MFA for access control across AWS services.
- Documented access boundaries, policy logic, and compliance workflows for audits.

AI-Powered Network Traffic Classifier | *Python, Scikit-learn, CICIDS2018* — Jun 2024
- Developed a machine learning model to classify malicious traffic using CICIDS2018 and NSL-KDD datasets.
- Applied feature engineering, SMOTE, and ROC curve analysis to improve detection accuracy.
- Achieved 92% classification accuracy in intrusion detection and supported real-time monitoring use cases.

Technical Skills

Python, Scikit-learn, SMOTE, Wireshark, Sysmon, Sysinternals Suite, VirtualBox, TheHive, Cortex, Nessus Essentials, Arduino Pro Micro, AWS IAM, JSON IAM Policies, MFA, RBAC, SIEM Operations, Log Analysis, Threat Detection, Incident Response, Vulnerability Management, IAM Policy Design, Red Team Tactics, USB Threat Simulation, Network Traffic Analysis, MITRE ATT&CK, Confusion Matrix, ROC Curve Visualization

Soft Skills

Analytical Thinking, Attention to Detail, Critical Thinking, Incident Documentation, Time Management, Team Collaboration, Communication & Reporting, Problem-Solving, Adaptability, Conflict Resolution, Self-Learning, Decision-Making under Pressure, Strong Communication, Public Speaking, Leadership, Mentoring, Student Engagement, Multitasking, Organizational Skills

Certifications & Publications

Publications: Co-authored *Web Sculptor - Generative AI-Based Comprehensive Web Development Framework*, published by IEEE, showcasing advancements in AI-driven web development.
Certifications: Cisco Linux Essentials Certification, Cisco PCAP - Programming Essentials in Python Certificate, AICTE Data Analytics Virtual Internship, Cisco Certified Cybersecurity Essentials, Google Cybersecurity Certificate