

Arya Deshpande

+919021340943
aryadeshpande2510@gmail.com
https://www.linkedin.com/in/arya-deshpande2510/
Portfolio

Skills

Tools

Wazuh, AleinVault, Elk Stack, Zabbix, DLP

Programming Language

Python, Java, C, ReactJS, SQL

Certifications

Trellix - DLP Network Essentials

Trellix - DLP Endpoint Essentials

Fundamentals of Microsoft 365
Generative AI

Forcepoint -Data Security - Level 1

Summary

Cybersecurity Analyst & Enthusiast

Cybersecurity professional with experience in penetration testing, SOC monitoring, and incident response. Skilled in vulnerability assessment and secure backend development with Python, Django, and MongoDB. Proficient in using ELK Stack, Wazuh, Zabbix, and AlienVault for log analysis, threat detection, and defense operations.

Achievements

AmbujaTech CTF

Participated in cybersecurity challenge organized by Ambuja Tech.

Experience

Imperative Business Ventures Pvt ltd August 2025 - Present
Security Analyst – Red Team & Blue Team Operations Pune

- Gained foundational knowledge of **Qubes OS** for secure and anonymous Red Team environments
- Contributed to **Blue Team operations** including SOC/NOC monitoring and incident response
- Worked with security tools such as **ELK Stack, Wazuh, Zabbix, and AlienVault** for log analysis, threat detection, and vulnerability assessment
- Assisted in **penetration testing** exercises and **vulnerability scanning** to support network defense strategies

Erfiedien Technologies Pvt. Ltd June 2025 - August 2025
Software Developer Intern Pune

- Learned and applied frontend development using React, HTML, CSS, and JavaScript for building responsive UI.
- Worked on database design and integration using Supabase. Contributed to connecting frontend, backend, and database for a working full-stack project.
- Gained hands-on experience in end-to-end web development within an Agribusiness domain project.

Amazure Technologies Pvt. Ltd June 2024 - Aug 2024
Cybersecurity Analyst Intern Pune

- A technology company focused on innovative software solutions.
- Installed, configured, and optimized **Trellix and Forcepoint DLP solutions**, ensuring data protection across endpoints and networks.
 - Collaborated on the development of a **Tenant Management System** with a strong focus on secure backend architecture
 - Performed **API testing and server management** to validate system resilience and security compliance.
 - Utilized the **ELK Stack for basic log monitoring and analysis**, enhancing visibility into system events.

Nexgensis technologies Private Limited June 2023 - Aug 2023
Software Developer Intern Pune

- A software development company specializing in innovative technology solutions.
- Designed and implemented interactive dashboards with React.js for data visualization.
 - Developed and tested backend APIs using Django and MongoDB for secure data handling.
 - Contributed to Agile development cycles, meeting project milestones efficiently.

Education

Symbiosis Skills and Professional University August 2022 - June 2026
B.Tech CSIT (Cyber Security)
8.3

Projects

Red and Blue Team Simulation Platform

- A comprehensive simulation platform for cybersecurity training, integrating real-world tools and technologies.
- Led the design of a cybersecurity simulation platform using React.js (frontend) and Django (backend).
 - Implemented a robust backend utilizing MongoDB for data storage and Django REST Framework (DRF) for API development.
 - Integrated tools like Wazuh for intrusion detection and the ELK Stack for log analysis and monitoring.
 - Automated scenario deployment with Ansible, reducing setup time by 30%.
 - Enhanced detection rates and user engagement through intuitive interfaces and real-time feedback mechanisms.
 - Leveraged Proxmox for virtualization and environment simulation.
 - Employed Python scripting for backend automation and task orchestration.

AI-Powered Skin Cancer Detection

- Developed a deep learning application for skin cancer classification using CNNs (TensorFlow/Keras).
- Designed secure Django + React-based web interface for uploading medical images.
- Deployed cloud-hosted model for real-time predictions with accuracy optimization.

Laptop Security Scanner

- Developed a SOC-focused utility to scan laptops for security posture and collect system/security logs.
- Implemented correlation and parsing of events inspired by Logstash pipelines for efficient analysis.
- Detected anomalies such as failed logins, suspicious processes, and unusual system activity.
- Generated structured reports for SOC/NOC analysts to support threat investigation.
- Designed with Python for lightweight integration into SIEM workflows (ELK/Logstash).

Chronic Disease Management

- Built a healthcare-focused web application to assist in monitoring and managing chronic illnesses.
- Developed backend using **Django** with secure patient record handling and REST APIs.
- Implemented **React.js** frontend for user-friendly dashboards, reports, and appointment tracking.
- Integrated **Supabase** for database connectivity and authentication workflows.
- Applied strong focus on **data security**, HIPAA-inspired access controls, and multi-user scalability.

SentinelMesh – Real-Time Cybersecurity Dashboard

- Built a full-stack SOC dashboard to visualize live security alerts and threat intelligence.
- Implemented React.js frontend with interactive charts and tables for log monitoring.
- Integrated ELK Stack and Wazuh for real-time log ingestion, anomaly detection, and alerting.
- Enabled role-based access and reporting features for SOC analysts.