Dip Nalawade

+91-8432008707 | dipnalawade24@gmail.com | linkedin.com/in/dip-nalawade | github.com/bot0024

Professional Summary

Cybersecurity student with hands-on experience in SIEM alert triage, threat analysis, and network security. Proven ability to deploy cloud-based honeypots capturing 266,000+ live attacks and analyze threat intelligence using ELK Stack. Certified in cybersecurity fundamentals with practical expertise in log analysis, system hardening, and incident response. Seeking to leverage technical skills and analytical mindset to contribute to a dynamic security operations team.

Education

Suryadatta International Institute of Cyber Security — Pune, Maharashtra
Bachelor of Science in Cybersecurity and Digital Science — *June 2023 – May 2026 (Expected)*

Maharashtra State Board of Secondary and Higher Secondary Education — Pune, Maharashtra
XII (HSC) - Science — *Completed May 2023*

Professional Experience

Cyber Security Intern — may 2025 - June 2025
Elevate Labs — *Remote*

- Conducted network reconnaissance using Nmap to identify open ports and vulnerabilities, analyzing security impact of exposed services across environments
- Configured Windows Firewall rules for inbound and outbound traffic, implementing security policies that restricted unauthorized access
- Analyzed phishing campaigns to identify social engineering tactics and malicious payloads, documenting indicators of compromise (IOCs) and creating threat intelligence reports
- Performed threat analysis on email headers and attachments, identifying malware signatures and contributing to security awareness initiatives

Technical Projects

Global Threat Intelligence Analysis using Cloud-Based Honeypots — December 2025
Microsoft Azure — T-Pot — ELK Stack — Suricata

- Deployed and managed T-Pot honeypot infrastructure on Microsoft Azure, successfully capturing and analyzing 266,000+ live cyberattacks from global threat actors
- Utilized ELK Stack (Elasticsearch, Logstash, Kibana) and Suricata IDS for real-time threat pattern analysis, identifying attack vectors, malicious IP addresses, and exploit attempts
- Conducted malware analysis on captured payloads, identifying Redtail crypto miner and critical CVEs through forensic log examination and network traffic analysis
- Resolved Docker memory bottlenecks on resource-constrained infrastructure by implementing custom Linux swap configurations, improving system stability by 40%
- Generated comprehensive threat intelligence reports documenting attack trends, geographic distribution, and recommended mitigation strategies

Technical Skills

Security Operations: SIEM Alert Triage, Splunk Log Analysis, Threat Hunting, Incident Response, OSINT
Network Security: Firewall Configuration, Network Traffic Analysis, Vulnerability Assessment, Suricata IDS,
Cloud & Infrastructure: Microsoft Azure, Linux System Administration,
Tools & Technologies: Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), T-Pot, Burpsuite, Wireshark, etc..
Operating Systems: Windows (CLI/PowerShell), Linux (Bash/Command Line)
Analysis: Malware Analysis(basic), Phishing Detection, Forensic Log Analysis, Threat Intelligence

Certifications & Training

Google Cybersecurity Certificate: Connect and Protect: Networks and Network Security — Tools of the Trade: Linux and SQL — Foundations of Cybersecurity
Oracle Cloud Infrastructure: 2025 Certified Foundations Associate
Tata Consultancy Services (TCS): Cybersecurity Analyst Job Simulation (Forage)
TryHackMe: Cyber Security 101 — Pre Security Certificate — CTF Participant