

Nishit Surti

Surat, Gujarat, India | nishitsurti312@gmail.com | +91 8200780368 | [Github](#) | linkedin.com/in/nishitsurti

tryhackme.com/nishitsurti | hackerrank.com/nishitsurti

Education

C. K. Pithawala College of Engineering and Technology, Surat

Nov 2020 – June 2024

• Bachelor of Engineering - Computer Engineering

CGPA: 9.2/10.0

Experience

SOC Analyst L1, Techowl Infosec Private Ltd. – Surat, India

Jan 2024 – Jan 2025

- Conduct security **incident monitoring** and **Root cause analysis** using **FortiSIEM** ensuring rapid identification and response to threats
- Security Tools Experienced in threat detection and log analysis using **ElasticSearch**, **Wazuh**, **Splunk**, enabling proactive identification of security incidents. Skilled in malware analysis and endpoint protection with **SentinelOne**.
- Proficient in using Manage Engine **End-Point Central** for endpoint management tasks, including **Patch Deployment**, **Data Loss Prevention**, **Browser Security**, **Software Deployment** and **Software Inventory**
- Conducted **Atomic Red Teaming**, exercises to simulate real-world attack techniques, enhancing detection capabilities and incident response strategies.

Cyber Security Intern, Zeronsec India Private Ltd. – Vadodara, India

Jul 2023 – Aug 2023

- Conducted periodic **Vulnerability Assessments** that identified potential threats and Analyzed traffic on Network with using Vulnerability assessment tool like, Nmap, Wireshark, Open-Vas, Metasploit.

NodeJs Intern, UniQual iTech – Surat, India

May 2023 – Jun 2023

- Developed a **Restful API** that allowed the app to integrate with backend services, resulting in enhanced user experience.

Projects

Stock Price Prediction

- Predict stock prices based on previous 10 year data-sets by Kaggle
- Achieved **92-95%** accuracy using **Support Vector Machine (SVM)**.
- Technologies: Python, Scikit-Learn, Machine Learning, HTML, CSS, JavaScript.

Fitness Website

- Directed a team of 2 to develop Full stack infrastructure to solve daily health issue using **PHP** and **MySQL-1**
- Technologies: HTML, CSS, JavaScript, MySQL - 1, PHP.

Skills

SOC Analyst Skills: Threat Monitoring, Incident Response, Log Management, Vulnerability Assessment, Patch Management

Tools & Platforms: Wazuh, Splunk, ManageEngine Log360 and End-Point Central, Fortinet, CrowdStrike, Docker, VMware, Dark Web Monitoring, FortiSIEM.

Programming & Scripting: Python, Bash, NodeJs, SQL, C, JavaScript, HTML, CSS

Soft Skills: Presentation, Group Discussion, Team Work, Time Management, Leadership.

Core Competencies

Security Information and Event Management (SIEM): Extensive experience with FortiSIEM, including event parsing, log analysis, and real-time monitoring.


Incident Response and Analysis: Proficient in identifying, investigating, and mitigating security incidents, including forensic analysis.

Client-Focused Solutions: Expertise in server installation, technical support, and client communication for issue resolution.

Technical Troubleshooting: Skilled in network connectivity issues, SSL inspection, and firewall log forwarding.

Certificates

Certified Cyber Security Internship Professional by IBMSkillBuild | 

Fortinet Certified Associate in Cybersecurity by Fortinet | 

Certified Ethical Hacking Bootcamp 2021 Zero to Mastery - Udemy

Certified Google Cyber Security Study Jams - Coursera

Achievements

- Secured **5 star** in Accomplishment - C by HackerRank
- Ranked **77,302th** globally in TryHackMe, placing in the top 6% of users, showcasing strong skills in cybersecurity challenges and threat analysis.