




# NIRAKARA MISHRA

Cybersecurity Graduate | SOC & Cybersecurity Analyst

 Bhubaneswar |  nirakaramishra.cse@gmail.com |  +91-958-390-9109 |  [Linkedin](#) |  [Portfolio](#)

## PROFILE SUMMARY

Cybersecurity graduate with professional certifications from Google and IBM, possessing hands-on experience in security monitoring, vulnerability assessment, incident response, and risk management. Built real-world security systems including an AI-powered Intrusion Detection and Prevention System and a Web Application Security Scanner aligned with OWASP Top 10. Strong foundation in networking, Linux, SIEM concepts, and security frameworks such as NIST, ISO 27001, and MITRE ATT&CK. Actively developing skills through labs and projects to contribute effectively to both SOC and cybersecurity analyst roles.

## TECHNICAL SKILLS

### Cybersecurity & SOC Skills

Security Monitoring & Alert Analysis • Incident Response Lifecycle • SIEM (Splunk – Basics), Log Analysis • Vulnerability Assessment & Penetration Testing • Risk Management & Threat Modeling • Cyber Threat Intelligence • Security Auditing & Reporting

### Tools & Frameworks

Splunk, Wireshark • Nmap, Nessus, Burp Suite, Metasploit • OWASP Top 10, MITRE ATT&CK • NIST CSF, NIST RMF, NIST 800-53 • ISO 27001, GDPR, PCI DSS, COBIT

### Networking & Operating Systems

TCP/IP, Firewalls, VPNs, Routing, Wireless Security • Linux (Kali, Ubuntu), Windows Security • Active Directory (Basics) • Virtualization: VirtualBox, Docker

### Programming & Scripting

Python (Security Automation, Data Analysis, ML Basics) • Bash, SQL • HTML/CSS (Web Security Context)

### Soft Skills

Analytical Thinking • Incident communication • Documentation • Teamwork • Attention to detail

## PROJECTS

### Advanced Intrusion Detection and Prevention System (IDPS) using AI/ML

- Designed and developed a Flask-based IDPS using a machine learning model trained on the NSL-KDD dataset to classify network traffic as normal or malicious.
- Implemented centralized logging with IP address and timestamp to simulate SOC-style incident records and improve traceability.
- Added filtering, Excel export, and real-time dashboards to support forensic analysis and incident investigation.
- Analyzed attack patterns to support threat detection and risk evaluation.

**Tech:** Python, Flask, Pandas, Scikit-learn, Matplotlib

### Advanced Web Application Security Scanner

- Built a vulnerability scanner to detect OWASP Top 10 issues including SQL Injection and Cross-Site Scripting (XSS).
- Automated vulnerability detection and reporting to reduce manual security testing effort.
- Implemented scan history, dashboard analytics, and Excel report generation for professional security audits.

**Tech:** Python, Flask, Nmap, BeautifulSoup

### Driver Drowsiness Detection System

- Developed a real-time monitoring system using facial landmark detection and EAR technique.
- Implemented event logging, GUI dashboard, head pose estimation, and voice alerts, demonstrating security-style event tracking and alerting concepts.

**Tech:** Python, OpenCV, Dlib, Tkinter

## EDUCATION

### ➤ Bachelor of Technology (B.Tech) in Computer Science & Engineering

- Biju Patnaik University of Technology (BPUT), Odisha — 2025

## CERTIFICATIONS

- Google Cybersecurity Professional Certificate – **Google**
- IBM Cybersecurity Analyst Professional Certificate – **IBM**
- Cyber Threat Management – **Cisco Networking Academy**
- Network Defense – Cisco Networking Academy
- Applied ChatGPT for Cybersecurity – Infosys
- Getting Started with Git and GitHub – IBM

## ADDITIONAL INFORMATION

- Hands-on practice with TryHackMe and Hack The Box labs
- Familiar with incident ticketing, documentation practices, and security reporting
- Strong interest in SOC operations, vulnerability management, and AI-driven security systems
- Comfortable working in Linux-based environments and scripting for automation