

# Rakesh Kathiresan

Cybersecurity Analyst | Southampton, United Kingdom | rakeshofficial.cse@gmail.com | +44 7393153168 | LinkedIn

## PROFILE

Cybersecurity Analyst experienced in implementing security tools, frameworks, and vulnerability management programs. Proven track record in coordinating patch schedules, producing clear reporting, and supporting global infrastructure assessments. Known for delivering measurable improvements through teamwork, continuous improvement, and precise execution in both applications and network security environments.

## WORK EXPERIENCE

**Security Operations Centre Analyst** - Renderways Technology Pvt Ltd, India

May 2023 – Jan 2025

- Monitored and triaged 1,000+ weekly alerts using Splunk SIEM, escalating 150+ critical threats to engineering teams for containment and remediation.
- Developed Python and PowerShell scripts to automate log parsing and alert enrichment, reducing manual triage effort by 35%.
- Performed vulnerability assessments and supported patch implementation aligned with ISO 27001 and NIST CSF guidelines, reducing critical risks by 40% in six months.
- Designed MITRE ATT&CK-aligned detection use cases and tuned alert logic, improving signal-to-noise ratio by 25%.
- Automated repetitive security tasks using scripting and SOAR tools, improving efficiency and reducing manual workload by 40%.
- Produced clear weekly incident and compliance reports to assist internal audits and maintain operational transparency.

**Freelance Front-End and E-Learning Developer** – MF Media Pvt Ltd, India

June 2022 - Apr 2023

- Delivered adaptable and secure coding for SNCF Virtual Train Simulator and social media-based e-learning modules.
- Collaborated with cross-functional teams to monitor security and performance, ensuring 25% higher platform responsiveness.
- Communicated project progress clearly and implemented improvements based on analytical insights and IT best practices.

**Cyber Security Intern** – Necurity Solutions Pvt Ltd, India

Feb 2022 - May 2022

- Analyzed logs and identified 30+ suspicious events, supporting early-stage breach investigation and incident documentation.
- Contributed to vulnerability testing and remediation simulations in Linux lab environments, based on OWASP Top 10 and NIST 800-53 frameworks.
- Performed basic static and dynamic malware analysis to assist engineering teams with early threat validation.
- Built Python scripts to automate threat indicator extraction and IOC correlation from SIEM logs.
- Helped configure and maintain open-source security tools across Linux and Windows systems for technical skill-building and lab testing.

## SKILLS

- **Security & Monitoring:** SIEM (Splunk, CrowdStrike), IDS/IPS, Incident Response, Threat Hunting, MITRE ATT&CK
- **Penetration Testing:** Nmap, Metasploit, Burp Suite, Wireshark
- **Systems & Platforms:** Linux (Kali, Ubuntu), Windows, GCP, Docker, Git
- **Languages & Scripting:** Python, PowerShell, Bash, SQL, C/C++, HTML, CSS, JavaScript, ReactJS
- **Compliance:** ISO 27001, NIST, GDPR, OWASP Top 10, PCI DSS
- Written & Verbal Communication, Team Collaboration, Time Management, Client Focused Problem Solving

## EDUCATION

**University of Southampton, Southampton, UK**

**MSc in Cyber Security** - GPA: 7.4/10.0

- Modules: Cryptography, Digital Forensics, Incident Response, Network and Web Security, Malware and Penetration testing.

**Saveetha Engineering College, Chennai, India**

**B.E. in Computer Science and Engineering** - GPA: 8.8/10.0

- Modules: Operating Systems, Cloud Security, Information Security, Software Engineering, Database Management System.

## ACADEMIC PROJECTS

Comparative Analysis of Steganography Techniques in Real and AI-Generated Images: Embedding Efficacy and Detection Resistance

Image recognition-based attendance system with spoof detection using python

Surveillance of species at risk by unarmed aerial vehicles using python

E-Forms Service- Generating secure electronic forms with validation and digital signature integration using XAMPP

## CERTIFICATIONS

(2025)CompTIA Security+, **CompTIA**

(2025)Google Cyber Security Professional, **Google**

(2025)Junior Penetration tester(eJPT), **INE**

(2022)Complete Ethical Hacking Bootcamp, **Udemy**

## ACHIEVEMENTS

(2024 – Present)Hack The Box- Successfully captured **30+ flags** on Hack The Box, showcasing penetration testing expertise.

(2024)University of Southampton MSc Cyber Security Ambassador.

(2022)Google Cloud Program - Reached **Google Cloud Ultimate Milestone**, mastering key **cloud security** concepts.