PRIYA PATEL

Contact: (+91) 9691187858 | Email: patelpriya0800@gmail.com | LinkedIn: linkedin.com/in/priya-patel-820b74177/

SUMMARY

Security professional with roughly **2 years** of experience in **Security Operations**, and incident response. Proficient in **SIEM, EDR** and **SOAR** platforms to investigate and remediate security incidents. Proved ability to optimise defense mechanisms through continuous fine-tuning and automated playbook development.

Seeking to associate with an innovative and vibrant organization, allowing to leverage expertise in **threat detection and incident response** to add value to the organization and contribute to my overall growth as an individual.

WORK EXPERIENCE

Ernst & Young (EY) | Global Delivery Services 04/2025 – Present
Security Analyst Bengaluru

- Investigated **30+ security incidents** monthly across network and endpoints, identifying root causes and mitigating threats to reduce potential breaches.
- Performed initial containment strategies under supervision, including endpoint isolation and **Indicator of Compromise** blocking.
- Investigated and triaged security incidents using **SIEM alerts**, escalating suspicious activity promptly.
- Validated **EDR alerts** involving malicious activity, suspicious command execution, and lateral movement behaviour.
- Analyzed **malicious documents**, extracted and cataloged IoCs for continuous monitoring.
- **Fine-tuned** 11+ CrowdStrike detection rules by refining correlation logic, exclusion conditions, and behavioural tuning.
- Mentored interns and guide SOC operations, threat analysis, and incident response procedures.
- Maintained incident reports, response procedure and SOC documentation.

Indian Telecom Industries Limited (ITI Ltd.) 03/2023 – 09/2023
Graduate Trainee – Security Engineer Bengaluru

- Supported security automation and SOC-based engineering activities.
- Assisted in developing and testing **XSOAR playbooks** to automate repetitive investigation steps (IoC enrichment, log pulls, timeline correlation).
- **Integrated** 3rd parties' security tools with XSOAR using **APIs** and **connectors** to streamline alert handling and data flow.
- Collaborated with senior analyst to analyse **phishing/spam emails** and **automate enrichment** in SOAR playbooks, **saving 20% of triaging time.**

SKILLS

SIEM & Monitoring: **Splunk**, CrowdStrike **NG-SIEM**

Endpoint & threat management: CrowdStrike **Falcon**

Automation & Orchestration: **Cortex XSOAR**

Email Security: **Proofpoint**

Network security: Nmap, Virustotal, **Wireshark**

Processes: **SOC operations, Fine-tuning & Playbook expert, Incident Response**

EDUCATION

Master of Technology, Cyber Security Engineering 09/2023 – 05/2025
Kerala University of Digital Sciences, Innovation & Technology (Formerly IIITM, Thiruvananthapuram

Bachelor of Technology, Electrical Engineering 08/2018 – 07/2022
Government Engineering College, Jabalpur

CERTIFICATIONS

- **SIEM 100: Next-Gen SIEM Fundamentals**, CrowdStrike University
- **Falcon Administrator**, CrowdStrike University
- **Certified Network Security Practitioner** (CNSP), The SecOps Group
- **Certified Cyber Security Practitioner**, NPTEL

PROJECT

Cybersecurity Risk Assessment & Threat Modelling 02/2024 – 07/2024
Research Intern | Indian Institute of Information Technology and Management Thiruvananthapuram

- Performed end-to-end risk analysis for an e-commerce system by decomposing business processes, system components, and data flows to identify critical assets and trust boundaries.
- Conducted **threat** and **abuse-case analysis** using attacker profiling, attack surface evaluation, and vulnerability correlation (**CVSS/CWE**), mapping realistic attack paths and loss events.
- Applied the **FAIR** risk framework to quantify likelihood and business impact of cyber events, producing prioritized risk statements to support security decision-making.

*Tech Stack: OpenVAS, OWASP Threat Dragon, **CVE**, CVSS, **OSINT**, **MITRE ATT&CK**, **FAIR***

ACHIEVEMENTS

- Recognised with **Achiever Extraordinaire** appreciation | EY GDS
- SIH'23 (Smart India Hackathon) - **Semi-Finalist** | Ministry of Education, India
- Ranked in **top 8%** out of ~170,000 candidates in GATE 2025 (CSE stream)
- **Lance Corporal** rank & **C** Certificate holder | 4 MP CTR - NCC, Jabalpur.
- Secured **MMVY** Scholarship | Madhya Pradesh state government (Merit)

LEADERSHIP & ACTIVITIES

- Volunteered for Information Security Awareness program | Delivered **phishing awareness** & **PII protection** sessions in rural areas.
- M.Tech **Placement Representative** | Coordinated recruitment drives and student–placement cell engagement.
- Extracurriculars: Regional Science Congress representative | NSS volunteer.