Ishant Jaswal

6230995532 | ishantjaswal03@gmail.com
Portfolio | LinkedIn

Professional Summary

Cybersecurity Analyst with hands-on experience in Security Operations Center (SOC) environments, specializing in SIEM tuning, vulnerability management, and endpoint threat detection. Proven ability to monitor and triage security alerts at scale, reduce critical CVEs, and support rapid incident response. Certified in Qualys VMDR and CrowdStrike EDR. Eager to apply technical expertise and continuous learning mindset to secure enterprise systems and proactively defend against cyber threats.

Education

B.Tech – Computer Science & Engineering
University Institute of Technology, Summer Hill, Shimla, HP
2021 – 2025

Work Experience

Cybersecurity Analyst

Evalueserve – *June 2025 – Present*

- Fine-tuned Securnix SIEM rules while analyzing 500+ daily alerts, increasing threat detection accuracy by 15%.
- Led vulnerability lifecycle management for 7,500+ assets via Qualys VMDR & Cloud Agent, reducing critical CVEs by 25%.
- Monitored endpoints using CrowdStrike EDR and conducted dark web sweeps, proactively preventing credential compromise incidents.
- Investigated 30+ incidents monthly and escalated critical cases, helping reduce SOC response time by 20%.
- Coordinated patching and remediation efforts across departments, cutting false positives in SIEM alerts by 20%.

Cybersecurity Analyst Intern

Nomad Labs – *Jan 2024 – Sep 2024*

- Gained hands-on exposure to SOC workflows including incident triage, escalation protocols, and structured reporting procedures.
- Contributed to vulnerability research projects and explored endpoint protection strategies under guidance of senior analysts.
- Developed security documentation templates and internal reports, solidifying knowledge of threat analysis and the full incident response lifecycle.

Certifications

- Qualys VMDR Specialist
- Qualys Cloud Agent Specialist
- Qualys CSAM (CyberSecurity Asset Management)
- Cisco Junior Cybersecurity Analyst

Skills

Cybersecurity

SIEM (Securnix), EDR (CrowdStrike), Vulnerability Management (Qualys VMDR & Cloud Agent), Incident Response, Threat Hunting

Web Development

HTML, CSS, JavaScript, React