ISHANT JASWAL

CONTACT

- Shimla, India 171004
- 6230995532
- ishantjaswal03@gmail.com

SKILLS

- Securonix SIEM and Qualys VMDR
- CrowdStrike and Netskope CASB
- Incident response and management
- SOC operations and threat analysis
- UEBA and threat hunting
- CVE analysis and documentation
- Python, HTML, CSS, JavaScript, and React
- Analytical thinking and problem solving
- Collaboration and team engagement
- Technical documentation
- Team collaboration

WEBSITE

- https://ishantjaswal03.github.io/portfolio/

SUMMARY

Cybersecurity Analyst with a track record of optimizing security operations at Evalueserve. Achieved a 25% reduction in false positives by refining Securonix SIEM correlation rules. Expertise in incident response and threat hunting, enhancing SOC efficiency and security posture through analytical skills and teamwork.

EXPERIENCE

SOC Analyst, 06/2025 - Current
Evalueserve - Gurugram

- Monitored and analyzed security events with Securonix SIEM, reducing false positives by 25% through fine-tuned correlation rules.
- Administered vulnerability management via Qualys VMDR and Cloud Agent, ensuring continuous monitoring and timely remediation.
- Utilized CrowdStrike EDR for endpoint threat hunting, investigation, and dark web credential monitoring.
- Enhanced cloud visibility with Netskope CASB, applying DLP and access control policies to protect data.

Cybersecurity Analyst Intern, 01/2024 - 09/2024
Nomad Labs

- Assisted in triaging security alerts, researching threats, and documenting incidents.
- Participated in vulnerability assessment and endpoint protection initiatives.
- Drafted SOC process documents and developed reports for security posture improvement.

CERTIFICATIONS

- VMDR specialist
- Qualys Cybersecurity Asset Management Specialist
- Qualys Cloud Agent Specialist
- Cisco junior cybersecurity analyst
- Linux Cybersecurity Essentials LFC108
- Deloitte Cyber Job Simulation
- Udemy Cybersecurity Essentials
- Udemy Python Bootcamp

EDUCATION

B.Tech: Computer Science & Engineering, 05/2025
University Institute of Technology - Shimla, HP

PROJECTS

Threat Detection Lab: Created a mini SOC environment simulating phishing and ransomware attacks for incident response practice. Qualys Vulnerability Scanning: Implemented network-wide scanning and CVE validation to track vulnerabilities. Portfolio Website: Developed a responsive personal website using HTML, CSS, and React for cybersecurity portfolio display.