https://itorizon.com/job/security-operations-analyst/

Security Operations Analyst

Hiring organization
ITOrizon

Employment Type
Full-time

Experience
0–3 Years

Role
Analyst

Job Location
Bengaluru / Trichy (or as applicable), India, India

Working Hours
Shift: Rotational / 24×7 Support (including night shifts)

Date posted
April 17, 2026

Description

About Us

ITOrizon is a global consulting and technology company that helps enterprises design, implement, and optimize complex supply chain and digital transformation initiatives. Headquartered in Atlanta, USA, with offices in India (Bengaluru) and the UAE (Sharjah), we partner with global clients across retail, manufacturing, logistics, and distribution sectors.

We combine deep domain expertise with modern technology to deliver practical, scalable
solutions. Our teams work across strategy, implementation, and managed services — helping
organizations adopt leading platforms such as Oracle, Manhattan, Blue Yonder, and our next-generation composable enterprise platform, Karolium.

Role Overview:

ITOrizon is looking for motivated and security-focused graduates to join the Security Operations team. This role is responsible for supporting continuous security monitoring, incident triage, and vulnerability management activities under defined processes and supervision.

The position is ideal for candidates with strong foundational knowledge in cybersecurity who are looking to build hands-on expertise in real-time threat detection, response, and enterprise security operations.

Key Responsibilities

Security Monitoring & Incident Management

- Monitor and analyze security alerts from SIEM, EDR, and other security tools
- Perform initial triage and classification of security incidents based on severity and impact
- Escalate incidents to L2/L3 teams as per defined runbooks and SLAs

Incident Response Support

- Assist in incident containment, investigation, and resolution activities
- Collect and preserve evidence for analysis and reporting
- Maintain detailed incident logs and documentation

Vulnerability & Risk Management

- Support vulnerability scanning activities and track remediation status
- Perform basic vulnerability analysis and risk prioritization
- Coordinate with internal teams to ensure timely closure of findings

Log Analysis & Threat Intelligence

- Review logs from servers, firewalls, endpoints, and cloud platforms
- Assist in identifying suspicious patterns and potential threats
- Support threat intelligence research and awareness

Compliance & Documentation

- Participate in security audits, compliance checks, and internal reviews
- Maintain SOPs, incident reports, and knowledge base documentation
- Ensure adherence to organizational security policies and regulatory requirements

Collaboration

- Work closely with Infrastructure, Cloud, Application, and IT teams
- Support cross-functional issue resolution and incident handling

Required Skills & Expertise

- Strong understanding of cybersecurity fundamentals (CIA triad, threat lifecycle, attack vectors)
- Basic knowledge of network security concepts (TCP/IP, DNS, firewalls, VPNs)
- Familiarity with Windows and Linux operating systems
- Awareness of common threats (OWASP Top 10, phishing, malware, ransomware)
- Understanding of logging, monitoring, and alerting concepts
- Analytical thinking and problem-solving skills
- Good communication and documentation skills
- Basic programming/scripting knowledge (Python / Go preferred)

Certifications

- CompTIA Security+ – Mandatory
- Certified Ethical Hacker (CEH) – Preferred
- ISC2 Certifications (SSCP / CC or equivalent) – Preferred

Ideal Candidate Profile

- Bachelor’s degree in computer science, Information Technology, Cybersecurity, or related field

Nice to Have

- Exposure to SIEM tools (Splunk, Microsoft Sentinel, IBM QRadar, ArcSight, etc.)
- Basic understanding of cloud security (AWS / Azure fundamentals)
- Hands-on labs, internships, or academic projects in cybersecurity
- Awareness of ITSM / incident management frameworks (e.g., ITIL)

Shift & Work Requirements

- Willingness to work in rotational shifts, including night shifts
- Ability to operate in a 24×7 Security Operation environment
- High learning agility and ability to work under defined SLAs

Performance Expectations (First 6 Months)

- Complete onboarding and SOC tool training (SIEM, EDR, ticketing systems)
- Independently handle L1 alert triage and incident logging

- Demonstrate adherence to SOPs and escalation protocols
- Achieve defined SLA compliance for alert response and documentation

Career Progression

This role provides a structured pathway into advanced cybersecurity roles:

- SOC Analyst – L2
- Incident Responder
- Threat Intelligence Analyst
- Vulnerability Management Specialist
- Cloud Security Engineer

Why Join Us?

- Exposure to enterprise-grade security operations and global clients
- Structured learning and certification support
- Hands-on experience with modern security tools and cloud environments
- Clear growth path aligned to performance and capability development

How to Apply:

Email your Resume to engage@itorizon.com