JOB DESCRIPTION – SECURITY ANALYST (OPS)

About HackIT

HackIT Technology and Advisory Services is an IT/Cyber Security company, operating since 2009. HackIT is an Indian Computer Emergency Response Team, CERT-IN (www.cert-in.org.in) empaneled provider for IT Security Audit Services. HackIT provides a broad range of security consulting and advisory services to a diverse group of clients, including government organizations, corporations, Military establishments, financial institutions and start-up, to name few. Our work spans multiple sectors and industries, including Telecommunications, Defense and Military, ITeS, Financial Services, Aviation, Hospitality, Healthcare and Research. We work end-to-end—from diagnosis to delivery of lasting impact — together generating tangible results that are improving the security posture of organizations worldwide.

We are looking for passionate Information Security Professionals to help us keep growing. If you're excited to be part of a winning team, HackIT Technology & Advisory Services is a perfect place to get ahead.

Job Title
- Security Analyst (OPS)

Location
- Delhi

Job Overview

We are looking for a detail-oriented Security Analyst (OPS) to join our Security Testing team. In this role, you will collect, analyze, and interpret open-source intelligence to support risk assessments and ongoing security operations. You will work closely with internal experts and clients, ensuring accurate insights, timely threat monitoring, and high-quality reporting. This position requires strong analytical skills, hands-on OSINT experience, and the ability to manage sensitive information with complete confidentiality.

Job Responsibilities

- Data Collection: Conduct comprehensive information gathering from diverse open-source platforms, including social media, news websites, forums, and other publicly accessible resources, using advanced OSINT tools and methodologies.
- Data Analysis: Analyze and interpret large volumes of data to identify trends, patterns, anomalies, and actionable insights. Assess the credibility, relevance, and reliability of sources using strong critical-thinking and analytical skills.
- Reporting: Develop clear, concise, and well-structured intelligence reports summarizing key findings. Present insights to stakeholders, highlighting potential risks, opportunities, and strategic recommendations.

- Threat Monitoring: Continuously monitor online platforms and open sources for emerging threats, risks, or impactful developments. Maintain awareness of global events, geopolitical changes, and industry-specific trends.
- Cross-functional Collaboration: Collaborate with internal teams, including intelligence analysts, cybersecurity professionals, and external partners such as law enforcement agencies, to share findings and enhance collective situational awareness.
- Tool & Methodology Enhancement: Support the development, refinement, and automation of OSINT tools, processes, and methodologies to improve efficiency and effectiveness of intelligence operations.
- Compliance & Ethics: Ensure all OSINT activities comply with applicable laws, regulations, and organizational policies, including data privacy, ethical guidelines, and information security standards.

Technical Skillsets (Mandatory)

- Hands on experience in OSINT and Social Engineering.
- Basic Knowledge in Penetration Testing. Strong analytical and problem-solving skills and the ability to explain complex technical concepts in a clear and concise manner and to provide remediation recommendations.
- Knowledge of / or experience with both Enterprise and open-source offensive security tools for reconnaissance, scanning, exploitation.

Technical Skillsets (Preferred)

- Proficiency in a programming language(s) (e.g. Python).
- Hands-on experience in Threat Hunting, OSINT, and Threat Modelling.

Experience

1 to 3 years' experience

Education and Certifications

- Bachelor's degree in IT or equivalent.
- Industry recognized certifications preferred.

Send your updated profiles to **careers@hackit.co.**