United Kingdom Jobs Expertini®

Tier 2 SOC Analyst

Apply Now

Company: NCC Group

Location: United Kingdom

Category: computer-and-mathematical

The Opportunity

The R2 Analyst plays a vital role in the Security Operations Centre (SOC), contributing to the organization's overall cybersecurity posture by actively participating in the monitoring, analysis, and response to security incidents and events. With a focus on continuous learning and collaboration, the R2 Analyst supports the SOC team in identifying, assessing, and mitigating potential security threats and vulnerabilities. Through the application of foundational technical skills and a strong dedication to detail-oriented analysis, the R2 Analyst assists in safeguarding the organization's critical systems, data, and assets from cyber risks.

By working closely with senior analysts and leveraging emerging technologies, the R2 Analyst helps maintain a vigilant and proactive defence against evolving cyber threats, enabling the organization to operate securely and with confidence.

Key Accountabilities:

Threat Detection and Monitoring:

Monitor the SOAR platform for EDR Logs, SIEM Logs, IDS Logs and Managed Intelligence sources.

Identify potential threats, vulnerabilities, and indicators of compromise.

Initiate escalation procedures to counteract potential threats and vulnerabilities.

Ability to analyze and interpret threat intelligence feeds and implement protective measures accordingly.

Incident Remediation and Documentation:

Provide incident remediation and prevention recommendations to customers using established procedures and analyst experience.

Document and adhere to security monitoring processes.

Apply preventative measures by implementing domain blocking, host isolation and file hash blacklisting.

Customer Service and Escalation:

Exceed customer expectations by always delivering exceptional customer service.

Serve as an escalation point for junior and R1 team members, offering assistance and mentorship as needed.

Contribute to the creation and maintenance of security documentation, including incident response playbooks, standard operating procedures, and knowledge base articles.

Reporting and Continuous Improvement:

Compile and review service-focused reports for effective communication.

Contribute to the creation and maintenance of security documentation, including incident response playbooks, standard operating procedures, and knowledge base articles.

Threat Analysis and Collaboration:

Contribute practical insights to the analysis of common security incidents.

Maintain working relationships with the Analytic Development and Security Engineering teams.

Collaborate with shift partners to provide a high quality of service.

General Duties:

Perform additional assigned duties as required.

Flexibility to quickly learn and adapt to new security tools, technologies, and processes.

Strong analytical and problem-solving skills.

Good communication skills, both written and verbal.

Ability to work collaboratively as part of a team.

Keep up to date with latest emerging threats and APT groups.

Minimum Requirements

Network and OS Knowledge:

Understanding of common network protocols and tools.

Analysis of PCAP files and network traffic

Proficient knowledge of Windows, Linux & MacOS operating systems.

Customer interaction:

Experience with documenting both high level and technical customer facing information.

Confidence providing critical/sensitive information accurately.

Contacting key stakeholders during major incidents

Incident Analysis and Response:

Awareness of the MITRE ATT&CK framework

Pedigree in performing in-depth analysis of security alerts.

Assess customer impact through investigation and work with senior analysts for resolution.

Liaise with CIRT for active compromises.

Initiate escalation procedure for potential threats

Ability to interpret threat priority against the cyber kill chain.

Provide appropriate mitigation and remediation steps.

Desirable Requirements

Tooling

Hands-on experience with Security Information and Event Management (SIEM) platforms (e.g., Splunk, Sentinel, Swimlane) and their use in aggregating and analyzing security event data.

Knowledge of EDR solutions such as Defender for Endpoint and Carbon Black

Proficiency with network analysis tools (Wireshark) to perform PCAP analysis.

Desirable Certifications

CompTIA Network+

CompTIA Security+

CompTIA CySA+

Cisco CCNA

Microsoft SC-200

Behaviours

Client-Focused: Prioritizes client needs and expectations, ensuring that all actions and decisions lead to client satisfaction and success.

Collaborates as 'One NCC': Works in unison with all departments and teams, fostering a united front and shared objectives across the entire organisation.

Adds Value: Goes beyond the minimum requirements to provide solutions and contributions that enhance the customer's success and growth.

Enables and Empowers: Provides tools, resources, and support to team members, fostering an environment where they can thrive and excel.

Personal Responsibility: Takes ownership of actions, decisions, and outcomes, acknowledging successes as well as areas for improvement.

Communicates Openly and Respectfully: Shares information transparently while maintaining respect and consideration for all stakeholders.

Open Mindset: Embraces new ideas, diverse perspectives, and is willing to adapt in response to evolving situations or feedback.

Growth and Development: Actively seeks opportunities for personal and professional growth, championing learning and evolution for oneself and the organisation.

Analytical Thinking: Demonstrates a systematic approach to resolving issues and identifying improvements.

Collaboration: Works effectively across various teams and fosters a collaborative environment.

Proactive Nature: Anticipates potential service issues or user needs and acts on them before they escalate.

Continuous Learning: Shows a commitment to personal and professional growth and keeps up with the latest trends and practices.

Customer-Centric: Always considers the end-user's experience and strives to enhance the quality of IT services delivered.

Problem-Solving: Demonstrates resilience in finding solutions to complex challenges.

Adaptability: Remains flexible and positive in a constantly evolving environment and handles change constructively.

Apply Now

Cross References and Citations:

1. **Tier 2 SOC Analyst Jobs United Kingdom ↗**
2. **Tier 2 SOC Analyst Jobs United Kingdom ↗**
3. **Tier 2 SOC Analyst Jobs United Kingdom ↗**
4. **Tier 2 SOC Analyst Jobs United Kingdom ↗**
5. **Tier 2 SOC Analyst Jobs United Kingdom ↗**
6. **Tier 2 SOC Analyst search United Kingdom ↗**
7. **Tier 2 SOC Analyst job finder United Kingdom ↗**

1. **Tier 2 SOC Analyst jobs↗**
2. **Tier 2 SOC Analyst jobs↗**
3. **Tier 2 SOC Analyst jobs↗**