



Security Engineer – Managed Detection & Response

Are you ready to join the highly motivated cyber counterintelligence team at SpearTip?

Do you enjoy a good challenge? Are you the kind of person who accepts a challenge and finds a way to overcome, or are you the person who hides in your cubicle hoping your boss doesn't even know you're in the room? If you're up to the challenge and want to work with a motivated team of like-minded people who put hard work, commitment to excellence, and the client first – we have a place for you!

SpearTip puts comprehensive cyber counterintelligence capabilities at the disposal of directors, key executives, and chief legal and compliance officers to confront growing threats to technology development, protection of intellectual property, and other essential competitive information.

Our ideal candidate will have previously worked in a network security role and have a track record of continued professional growth, responsibility, and have the following experience:

- Triage and validate alerts from Enterprise Detection and Response tools including CrowdStrike, LogRhythm, Fidelis, Imperva, and others
- Conduct threat intelligence research based on metadata from alerts to associate a threat with known campaigns or threat actors
- Write technical reports explaining security incidents, technical analysis, and findings
- Communicate with SpearTip clients regarding suspicious/malicious activity detected within the environment
- Maintain security event triage documentation through the SpearPortal
- Assist in SpearTip's Incident Response Practice as requested by supervisor
- Certifications such as: Encase Certified Examiner (EnCE); EC-Council Certified Incident Handler (CHFI); GIAC Certified Incident Handler (GCIH); CompTIA Security+; CompTIA CSA+
- Previous experience with AWS is desirable but not required
- Problem solve; independently and in a team environment

More important than any of your skills and prior experience is the attribute that you have an extraordinary level of personal initiative and proactivity.

MUST be eligible to apply for a US Government Clearance

When Applying - provide your most recent résumé and contact information. Send résumé to careers@speartip.com