SPEARTIP®
CYBER COUNTERINTELLIGENCE
Outmaneuver Your Adversary™

SpearTip, LLC 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.

SpearTip, LLC is seeking a driven consultant within our Incident Response / Malware Analysis team that is looking for a rewarding, yet extremely challenging environment that is combating nation-state threat actors and international crime syndicates within the corporate sector.

Incident Response / Malware Analysis Consultant

We are seeking an Incident Response and Malware Analysis Consultant with strong technical and consulting skills that would allow this individual to converse with deep technical knowledge, to include the ability to present the analysis to chief executives. Consultant will be involved with collection, analysis, and dissemination of Actionable Threat Intelligence and provide ongoing breach detection, incident response, forensic examination, and malware analysis.

Specific job duties include (but not limited to):

- Perform incident response & malware analysis – host & network
- Opportunities to assist in internal, external, web application, malware, and social engineering security assessments
- Collect and analyze Threat Intelligence in a Fusion Cell methodology and produce analytical products, as appropriate
- Write investigatory, assessment, and analytical reports for clients.

Specific job requirements include (but not limited to):

- US Citizen
- Possession of current security certifications: such as GREM, CEH, GCIH, GCFA, EnCE or similar certifications
- Mastery of commercial and open source security tools (e.g. Splunk, FireEye, Fidelis, CarbonBlack, CrowdStrike, Nessus, Nexpose, SAINT, Burp, Nmap, Kali, Metasploit, Meterpreter, Wireshark, Kismet, Aircrack-ng, Volatility, Responder Pro, etc.)
- Understanding / knowledge of various languages – such as Java, Python, Perl, PHP, C# or C++
- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security and risk-related concepts
- Must be a critical thinker with strong problem-solving skills
- Firm understanding of advance networking terminology and concepts
- Experience in malware analysis and reverse engineering of malicious code & static code analysis
- Ability to convey complex technical security concepts to technical and non-technical audiences including executives
- Ability to lead and mentor others; willingness to collaborate and share knowledge with team members.
- Willingness to work after hours and/or weekends during and incident