{B(W)} CYBER SERVICES

Senior Digital Forensics Incident Response Specialist

Overview

BW Cyber Services' Digital Forensics Incident Response (DFIR) team is seeking a subject matter expert with in-depth understanding of existing and emerging threat actors. It DFIR specialist should have extensive experience identifying rapidly changing tools, tactics, and procedures (TTPs) of attackers. Candidates must be able to see the big picture, understanding evolving attacker behavior and motivations, participate and manage large client-facing projects, and help to train/mentor other security consultants. The successful candidate will possess sound business acumen, strong consulting skills, current technical skills and be adept in leading multiple projects under tight deadlines.

Key Responsibilities

- Conduct digital forensics on hosts, networks, and cloud applications including log analysis and malware triage in support of incident response investigations
- Utilize common industry technologies to conduct investigations and examine endpoint, network, and cloud-based sources of evidence
- Recognize and codify attacker TTPs in indicators of compromise (IOCs) that can be applied to current and future investigations
- Build scripts, tools, or methodologies to enhance internal investigation processes
- Develop and present comprehensive and accurate reports, trainings, and presentations for both technical and executive audiences
- Work with clients' security and IT operations teams to implement remediation plans in response to incidents
- Create and/or update clients' Incident Response Plans ensuring appropriate phases of IR are considered for client's specific risk profile

Qualifications

- Bachelor's degree in a technical field with minimum of 4 years of comparable experience
- Possess at least one computer forensics/examination related certifications (e.g., CCE, EnCe, CFCE, GCFA/GCFE, or CSFA)
- Experience with
    - Windows disk and memory forensics
    - Network Security Monitoring (NSM), network traffic analysis, and log analysis
    - Unix or Linux disk and memory forensics
    - Static and dynamic malware analysis
- Thorough understanding of enterprise security controls in legacy Active Directory and cloud-based environments (i.e., Azure, AWS, GCP, etc.)
- Experience building scripts, tools, or methodologies to enhance investigation processes

Additional Qualifications

- Ability to travel up to 10%
- Effectively communicating investigative findings and strategies to technical staff, executive leadership, legal counsel, and internal and external clients
- Effectively develop documentation and explain technical details in a concise, understandable manner
- Strong time management skills to balance time among multiple tasks, and lead junior staff when required
- US-Citizens able to obtain clearance if needed for task requirements

Interested in joining our team? Please send your resume and cover letter to info@bwcyberservices.com