Technical Lead for Digital Forensics and Incident Response/Rescue Team

Job Title: Technical Lead-Digital Forensic and Incident Response (DFIR)
Location: Remote, USA
Role: Full time

Job Description

CyXcel is actively seeking a Technical Lead for our Digital Forensic and Incident Response team. This opportunity is a full-time, remote opportunity.

As a Technical Lead, you will be responsible for leading complex digital forensic/incident response engagements, interacting with clients, cyber insurers, and legal counsel. Your expertise will guide scoping calls, and you will collaborate closely with other Technical Leads, guide less experienced DFIR Consultants on our team and foster an environment of continuous learning, and consistent, high quality work. This role will require advanced forensic analysis and problem solving skills and 3+ years of experience.

Key Responsibilities

- Lead active client-facing forensic and incident response engagements, working closely with other team members to guide clients and partners through the entire incident response lifecycle.
- Conduct scoping calls with clients to distinguish the incident scope, objectives, and expectations of each engagement as well as communicate clear and concise next steps for each client.
- Provide guidance and realistic solutions that go beyond immediate client challenges to greatly improve client security posture.
- Work closely with other Technical Leads and DFIR Consultants to ensure effective coordination of resources, partners and expertise on client matters.
- Build rapport and cultivate strong client relationships based on transparency, open communication, and collaborative problem-solving.
- Actively knowledge share with team members cultivating a philosophy of continuous learning, and stay up to date on cyber trends, emerging threats, and best practices.
- Communicate advanced cybersecurity concepts both internally and externally and produce clear and concise verbal and written reports detailing incident findings, and analysis.

- Provide after-hours (on-call/weekend rotational) support as required to address critical incidents and maintain continuous coverage, as expected by all DFIR team members.

Basic Requirements

- Previous career experience in leading and managing complex digital forensic and incident response investigations, interaction with clients, legal counsel, and cyber insurers.
- Experience with security investigations in Linux/ Mac and Windows environments.
- Basic understanding of cloud platforms and security considerations within AWS, Azure, and GCP.
- Knowledge of Open-Source tools and tools such as Axiom, XWF, FTK, Volatility.
- Experience identifying specific artifacts to determine attack vector, lateral movement and data exfiltration in incidents.
- Expertise in conducting forensic analysis, threat assessments, and post incident reviews.
- Experience analyzing logs such as firewall, IIS, network traffic, AV and DNS as well as the ability to corroborate these sources to find crucial artifacts during investigations.
- Enthusiasm to learn from your team, grow your own knowledge, and teach your colleagues.
- Ability to provide after-hours (on-call/weekend rotational) support as required to address critical incidents and maintain continuous coverage as expected by all DFIR team members.

Helpful Requirements

- Deep expertise with cloud data investigations such as AWS, Azure and GCP
- Experience analyzing mobile device platforms such as smart phone and tablets
- Bachelor’s degree in Cybersecurity/Digital Forensics, Computer Science, Information Technology, related degree, or relevant professional work experience in these disciplines.