Forensic Lab Manager & DFIR Analyst: Key Duties and Responsibilities

Lab Manager's roles and responsibilities include, but are not limited to:

- Hardware/Software management/repair for entire lab (all servers, devices and network)
  - System administration for all lab servers (VMware vSphere) and devices
  - Creation/cloning of Virtual Machines (MS Windows OS in VMware vSphere)
  - Network Administration (Cisco and Fortinet)
  - Timely vulnerability patching on all systems/firewall
  - Workstation administration (Windows)
  - Data backups for all relevant lab systems
- Technical field assistance for matters (internal team, clients and partners)
- Manage offsite backup responsibilities and ensure all aspects of archiving process are documented (e.g., document engagement numbers on each external hard drive, etc.)
- Labeling of evidence and enforcement of chain of custody rules
- Preservation and duplication of original media
- Shipping and receipt of evidence for matters
- Sanitization of drives, encryption of drives/data for sending to client during and post engagement
- Experience with accessing password-protected, secured, and deleted data.
- Knowledge of the techniques for examining electronic devices and data storage media using physical disassembly, forensic hardware, and software tools.
- Basic experience with forensic acquisition/preservation of data from desktops, laptops, mobile devices/tablets, servers (cloud and on-premises), email systems, social media, etc. and understand basic forensic concepts
- Provide advice and guidance regarding seizure and handling of digital evidence to clients
- Organize and participate in annual Management Review assessments with relevant personnel and prepare a report of findings in accordance with ISO standards

Overflow as a **digital forensics and incident response (DFIR) Analyst**, including:

- Candidates should have problem solving skills, analytical skills, be highly motivated with 2+ years of experience in areas of cybersecurity (digital forensics, information security, incident response or SOC experience)

- Experience with conducting digital forensic analysis using commercial and open-source forensic tools including file system forensics, memory analysis and network analysis preferred
- Strong understanding of computer operating systems, software and hardware
- Ability to conduct cloud cyber incident response/analysis and mobile forensic analysis helpful
- Provide data collection and triage support for Senior Analysts in all types of matters (RW, BEC, UA, DF matters)
- Actively share knowledge with team members cultivating a culture of continuous learning, and stay up to date on industry trends, emerging threats, and best practices
- Provide after-hours (on-call/weekend rotational) support as required to address critical incidents and maintain continuous coverage