INCIDENT RESPONDER - FORENSICS ANALYST | BAHRAIN | FULL-TIME | AVAILABLE INSTANTLY

About us:

ZENDATA is a leading player in the cybersecurity industry, offering services such as complete, fully managed cyber protection, vulnerability assessment, pen testing, and red teaming. With locations in Geneva, Dubai, and Bahrain, ZENDATA provides services to clients globally and collaborates with law enforcement authorities and threat intelligence companies. As an official cybersecurity expert of the Swiss federal government, ZENDATA's expertise is recognized by institutions, businesses, and the media.

Role Description:

This is a full-time on-site role as Incident Responder - Forensics Analyst in our Security Operations Center (SOC) Team. The role will be part of a team of SOC analysts of our ZEN360 Detection & Response environment to detect, respond to, mitigate, and report on cybersecurity incidents. The role will also be responsible for cyber forensics and performing threat-hunting activities.

Primary Responsibilities:

- Acts as Incident Commander for high-impact cyber breaches and advanced attack methods, using the Cyber Kill Chain methodology.
- Provide project support-related tasks to integrate the security platform's ongoing tuning support for existing technology.
- Apply technical acumen and analytical capabilities to improve the efficiency and effectiveness of the response.
- Develop and enhance capabilities of digital and computer forensics
- Knowledge sharing of threat intelligence/ management during weekly meetings
- Conduct security event analysis and validation, triage validated incidents, perform initial containment where feasible, research incidents and enrich incident case documentation, and escalate incidents for further analysis, containment, and eradication.
- Review and analyze threat intelligence information and proactively search applications, systems, and network logs to hunt for and thwart relevant threats identified threats.
- Contribute to the development and maintenance of playbooks to establish and continuously improve the team's operating knowledge base.
- Participate in post-incident activities and contribute to lessons learned to improve security operations.
- Provide sound technical recommendations that enable remediation of security issues.
- Utilize advanced threat models, SIEM use cases, and incident response playbooks.
- Provide guidance and mentorship to improve analyst skill sets guiding threat management and modeling, identify threat vectors, and develop use cases for security monitoring.

Skills and Qualifications:

- Bachelor's Degree in an IT-related field and 4+ years' experience in an information technology field with a minimum of 3 years of experience in the areas of incident detection and response, malware analysis, or computer forensics.
- Relevant certifications in Blue Teaming and Forensics.
- Excellent knowledge of cybersecurity protocols and procedures.
- Proven previous experience as a SOC Analyst, on triage of alerts.
- Proven 2 years of experience with forensic analysis, performing static and dynamic analyses of suspect malware-Knowledge of Windows, Linux, and Mac OS environments.
- Excellent communication and interpersonal skills, including the ability to effectively communicate security concepts and protections to technical and non-technical audiences.

We also place a strong emphasis on a candidate's willingness to learn, adapt, and take on new challenges.

Extra points for the position:

- The position will require work on non-regular working hours shifts and on-call schedules.
- The candidate must possess a passport that is easy to travel (last-minute trips to perform incident response on clients)

Benefits:

- Dynamic and innovative work environment.
- Opportunities for professional development and continuous training.
- Competitive salary package with comprehensive social benefits.