CYBER INCIDENT RESPONDER - BUCHAREST

CyBourn is a Managed Detection and Response (MDR) organization with a unique approach towards servicing clients. Our CREST accredited Security Operations Center (SOC) combines advanced monitoring services and threat detection capabilities with best-in-class business risk assessment to provide the optimal incident response approach for every client. We integrate threat intelligence, event monitoring, security analytics and incident response, while catalyzing machine learning and automation orchestration to detect targeted cyberattacks. CyBourn was established in 2018 in Europe, with its SOC in Bucharest, Romania, R&D Lab in Naples, Italy and established a sales hub in the UK market in 2020.

Application Process:

Please send cover letter and CV to talent@CyBourn.com

Role Overview:

The Cyber Incident Responder will be reporting to the Director of Cybersecurity Operations and will coordinate activities with the rest of the SOC team. The Cyber Incident Responder will lead security investigations and provide technical expertise for all types of cyber security incidents. The Cyber Incident Responder will guide and mentor juniors according to Cybourn's career path and professional excellency. In partnership with Cybourn's Dream Lab team, the Cyber Incident Responder will help build requirements, transition improvements, and ensure a successful introduction into operations.

Key Responsibilities

- Identify, triage, conduct forensic analysis and respond to security incidents
- Own the full lifecycle of a security incident from discovery to completion to include root cause analysis and guidance in recovery efforts.
- Work closely with both technical and non-technical customers to guide them through the incident response process and provide guidance on best practices and remediation when needed.
- Conduct analysis on output from host and network-based security tools to provide context for both ongoing and historical security events.
- Analyse threats for unique indicators of compromise; work with fellow SOC team members to create countermeasures to aid in future prevention and detection of cyber threat activity.
- Maintain knowledge of current and emerging cyber threats; grow relationships with other incident response professionals, industry partners and vendors.
- Monitor and enforce guidelines for security and compliance.
- Train, mentor and guide junior analysts within the SOC.

Requirements

- Strong understanding of both Windows and Linux server environments including commonly configured roles and related technologies, such as web, database, domain services, etc.
- Able to perform live triage of hosts to include examining running processes, network

connections, system logs, file system activity, and more for signs of anomalous behaviour.
- Strong understanding of attacker tools, techniques, and methodologies. Ability to gather and act on cyber threat intelligence.
- Familiar with industry standard forensic tools such as X-Ways Forensics, EnCase, Volatility
- Experience with HIDS/NIDS, Web Application Firewalls (WAF), IDS/IPS and SIEM systems
- Able to read and understand the following languages: PHP, Python, Bash, Powershell, SQL