ANÜ: Incident Response Manager (m/w/d) Hamburg, English speaking

We are currently seeking an Incident Response Manager (m/f/d) for a client in the logistics industry on a temporary staffing assignment Arbeitnehmerüberlassung (ANÜ).

Start: ASAP
End: December 31, 2026 +
Workload: Full-time (80 Days)
Location: 60% Hamburg, 40% remote
Language: English

Tasks:
• Manage threat detection and response strategies, plans, capabilities, activities, and improvements.
• Oversee the daily operations of the TDR team, ensuring timely, accurate, and effective security incident response and proactive threa activities.
• Be the primary liaison between technical teams, business units, and Managed Security Service Providers (MSSP) to reduce the impact incidents and maintain business operations.
• Develop and maintain TDR playbooks, defining procedures, best practices, and escalation protocols to enhance response capabilities
• Review incident response cases, offering guidance on anomaly-based detection, and facilitating improvements in detection and analy
• Provide timely and detailed post-incident reports, summarizing root cause analyses, and making recommendations to stakeholders ar sponsors.• Drive the continuous improvement of processes and procedures.
• Monitor levels of service within the TDR team and interpret threats using intrusion detection systems, SIEM platforms, and other securi management products.
• Drive the development and implementation of TDR processes, leveraging insights from lessons learned to improve response efficiency reduce response times.
• Continuously assess and adapt TDR processes and toolsets to stay aligned with emerging cybersecurity trends and threats.
• Convey the proper security severity by explaining the risk exposure and its consequences to non-technical stakeholders.
• Ensuring the effectiveness and efficiency of the security incident response services and processes (e.g., by designing and executing ta exercises to ensure all relevant stakeholders understand their roles and can execute their responsibilities during an incident).

Skills:
• Experience in incident response, security monitoring, digital forensics and/or advanced malware analysis.
• Ability to maintain strategic overview while managing operational detail in complex environments.
• Clear and concise communication, including translating technical risks into business impact for senior stakeholders.
• Stakeholder management and influence across IT, security, cloud, and development teams.
• Accountability, especially in high-pressure or incident-driven situations.
• Problem-solving mindset with a focus on practical, scalable solutions.
• Collaboration and team orientation, with the ability to drive cross-functional alignment.
• Adaptability and resilience in fast-changing threat and technology landscapes.
• Process discipline and attention to detail, ensuring consistency and audit readiness.
• Continuous improvement mindset, with a focus on automation and efficiency.