Cybersecurity Analyst – Digital Forensics & Incident Response (DFIR)

Moody's

careers.moodys.com/

Lithuania

This assignment expired :when

About the assignment:

Location

Vilnius, Lithuania

Rate (after tax)

€2300 - 3600/Month

Duration

Full time position

Extension (project)

No

Remotely (optionally)

Yes

Expire On

2022-07-31 *(3 weeks ago)*

Description

The Moody's Cybersecurity team is looking for a Cybersecurity Analyst or Senior Cybersecurity Analyst to join its growing organization. This position requires a thorough understanding of Cybersecurity concepts, terminology and practise, with specialisation in Digital Forensics and Incident Response. The successful candidate possesses a curious mindset and is highly driven to learn and solve challenges. Solid written and verbal communication, organizational and relationship management skills are also key.

The Moody's Cybersecurity team is responsible for helping the organization balance risk by aligning policies and procedures with Moody's business requirements. The team is responsible for the development, enforcement and monitoring of security controls, policies and procedures, and for the delivery of security services. The Cybersecurity team sets strategic direction for security within the organization and aligns with stakeholders throughout the company.

The Cybersecurity Analyst or Senior Cybersecurity

Analyst will be responsible for handling escalated cyber incidents and internal investigations which require a high level of technical analysis and coordination, such as network intrusions, invoice fraud and advanced malware infections. In addition, they may assist with the identification, implementation and support of technologies and procedures used to aid in the detection and prevention of new threats.

Functional Responsibilities:

- Provide timely review and response of security events raised by the SOC or reported by internal or external sources; resolve if the event should invoke the Incident Response Plan.
- Provide on-call support for emergency or high severity issues.
- Perform forensic review of systems in response to incidents or investigations, providing timely and complete reports to management.
- Keep tabs on current security threats, events, technologies, vendors and other aspects of the cyber threat landscape. Propose changes or improvements to our security posture where appropriate.
- Analyse, correlate and action on data from subscription and public cyber threat intelligence services, develop tactics to combat future threats, and invoke the Incident Response Plan if vital.
- Communicate and raise incidents to management in accordance with the Incident Response Plan.
- Work with third party threat intelligence firms and platforms to research and respond to incidents.
- Respond to Human Resources, Legal and Compliance investigation requests in a timely, cordial, and accurate manner.
- Write and test playbooks for common incident response scenarios.
- Participate in Cyber tabletop exercises to build muscle memory and practice for real-world incidents.

Qualifications

- BSc or MSc degree preferred, ideally in technology, computer science or cybersecurity.
- Certifications such as GCIH, GCFE, GCTI, GISF, SEC, Security+, Network+, CySA+, SSCP, BTL1, BTL2 are considered a plus.
- Minimum 1-2 years (Analyst) or 3-5 years (Senior

Analyst) experience working in a similar Cybersecurity role.
- Excellent analytical and problem-solving skills.

Key Competencies

- A solid grasp of fundamental cybersecurity and networking concepts and terminology; e.g. protocols, ports, processes, OWASP Top 10, common attack vectors, etc.
- A high-level understanding of the MITRE ATTACK Framework, CIS Controls, and NIST Cybersecurity Framework.
- Experience in digital forensics technology, procedures, and processes, as well as a solid grasp of the NIST Incident Handling Guidelines (800-61r2). Ability to talk confidently about each stage of the Cyber Incident Response Lifecycle.
- Hands-on experience with digital forensics tools and techniques, such as file carving, disk imaging and write blockers.
- Ability to remain calm under pressure; maintain composure to follow process and be detail oriented.
- Strong written and oral communication skills, including the ability to directly contact stakeholders at various levels that do not necessarily have a technical background.
- A passion for Cybersecurity with a strong desire to learn and develop your skills.
- A can-do attitude; being comfortable ‘wearing many hats’ and demonstrating focus and pro-activeness to get the job done.

Required Skills

ADMIN & NETWORK
Network Security 1-2 years
Network Protocols 1-2 years