Junior Cybersecurity Analyst – Fusion Center

Moody's

careers.moodys.com/

Lietuva

Projektas nebegalioja

Apie poziciją:

Vietovė

Vilnius, Lietuva

Atlyginimas (Į rankas)

€1300 - 2100/Mėn.

Trukmė

Pastovus Darbas

Pratęsimas (projektui)

Ne

Nuotoliniu būdu (galimybė)

Taip

Galioja iki

2022-02-28 *(Prieš 1 savaitę)*

Aprašymas:

Moody’s Cyber Security team is looking for a Junior Cybersecurity Analyst to join its growing organization. This position requires a technical background in IT, analytical mindset and communication skills. The successful candidate is very motivated and willing to take on challenges, and has the ability work independently and with minimal oversight.

Moody’s Cyber Security 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. Cyber Security team sets strategic direction for security within the organization and aligns with stakeholders throughout the company.

The Junior Cybersecurity Analyst will be responsible for investigating and escalating of alerts which require technical analysis, such as network intrusions and malware infections which have been identified by the Cyber Security team.

Functional Responsibilities

· Analyze, correlate and action on data from subscription and public cyber intelligence services, develop tactics to combat future threats, and invoke the Incident Response Plan if necessary.

· Provide timely review of security alerts originating from any source, including managed security services, internal tools, and internal or external reporting.

· Analyze and respond to security events in alignment with the Incident Response Plan and its procedures.

· Perform forensic review of systems in response to incidents or investigations, providing timely and complete reports to management.

· Keep abreast of current security threats, events, technologies, vendors, and other aspects of the cyber threat landscape. Propose changes or enhancements to our security posture where appropriate.

· Investigate security incidents and events, using SIEM and other tools; collect evidence and work with teams to isolate and/or remediate as necessary.

· Communicate and escalate incidents to management in accordance with the Incident Response Plan.

· Work with third party security monitoring firms to research and respond to incidents.

· Monitor security tools alerts for anomalous or suspicious activity; research alerts and make recommendations to remediate concerns.

Qualifications

Minimum education and work experience required for this position include:

· At least 1 year of IT industry experience, preferably in a financial services organization.

· BS or BA degree, preferably in technology.

· Relevant certifications such as Network+, Security+ or CEH are considered a plus.

Key Competencies

· Strong interest in cyber security incident investigation and response processes.

· Technical, analytical mindset.

· Ability to work in a time-sensitive environment; must be detail oriented.

· Written and oral communication skills.

· Fast-learning skills.

· Ability to work in shifts (24/7).

Reikalinga Patirtis

ADMIN & NETWORK
Network Security iki metų