Senior Cybersecurity Analyst – Fusion Center

Moody's

careers.moodys.com/

Lietuva

This assignment expired :when

About the assignment:

Atrašanās vieta

Vilnius, Lietuva

Rate (after tax)

€2200 - 3500/mēnesī

Ilgums

Pilna laika darbs

Extension (project)

No

Remotely (optionally)

Yes

Expire On

2022-08-20 *(1 week ago)*

Description

Moody’s Cyber Security team is looking for a Senior Cybersecurity Analyst to join its growing organization. This position requires a strong technical background in Information Security practice, deep knowledge of IT Security and Investigations, SIEM, SOAR, and solid communication and organizational skills. The successful candidate is very motivated and willing to take on challenges, and has the ability work independently and with minimal oversight.

The 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 Senior Cybersecurity Analyst will be responsible for investigating and escalating of alerts which require highly technical analysis, such as network intrusions and advanced malware infections which have been

identified by the Cyber Security team.

Functional Responsibilities

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

· Investigate security alerts, using SIEM, SOAR and other technologies; collect evidence and work with teams to isolate and/or remediate as necessary.

· Communicate and escalate potential incidents to Incident Response team.

· Provide detection tuning ideas to help optimizing TP/FP rate.

· Perform detection engineering activities for continuous coverage increase.

· Work with engineering team on ideas and implementation of manual analyst task automation via SOAR.

· Analyze, correlate and action on data from subscription and public cyber intelligence services, develop tactics to combat future threats.

· 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.

· Perform daily audit of closed investigations with guidance and mentorship to more junior colleagues.

· Help developing standard operating procedures (SOP).

Qualifications

Minimum education and work experience required for this position include:

· At least 5 years of IT industry experience, preferably in a financial services organization.

· At least 3 years experience in security alerts investigation and handling.

· Extensive knowledge and hands-on experience

with SIEM technologies and other forensics, evidence collection, and incident remediation tools.

· Knowledge of regular expressions and at least one common scripting language (e.g. Python, PowerShell).

· BS or BA degree, preferably in technology.

· Relevant certifications such as BTL1, GCIA, GCIH, GCFE, GCFA, or CISSP are considered a plus.

Key Competencies

· Ability to think with a security mindset. The successful candidate has a strong IT background with knowledge of multiple relevant security practice areas (anti-malware solutions, network security; monitoring; endpoint, etc.) in addition to forensics and incident management.

· Extensive knowledge of security tools which perform functions such as intrusion detection and prevention (IDS/IPS), SOAR, and log archiving.

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

· Experience in large, geographically diverse enterprise networks.

· Strong written and oral communication skills including the ability to interact directly with customers that do not have an IT background.

· Ability to work in shifts (24/7).

· Endpoint forensics experience is considered a plus.

Ability to work in shifts (24/7).

Required Skills

ADMIN & NETWORK
Network Security 3-4 years