

User & Entity Behavior Analysis (UEBA) Consultant for project in IT Security team. Danske Contract

HITCONTRACT

www.hitcontract.lt/en

Vilnius, Lithuania

About the assignment:

Location

Vilnius, Lithuania

Rate (after tax)

from €3000/Month

Duration

Mid-term project (>6 months)

Extension (project)

No

Remotely (optionally)

Yes

Expire On

2021-03-10 (1 day ago)

This assignment expired :when

Description:

We are a part of an organization, which delivers world-class digital financial solutions to customers. We have an understanding that the current change is Technology-driven, and we prioritize IT as a key component for success in our journey to drive digital disruption in the bank. Our teams work with complex tech challenges and develop Danske Bank's global competitive edge on innovative digital solutions. Teams are driven by job content, share ownership of strategic services, own service strategy and lead improvement.

Job description:

Consultant will become a part of a Group Information Security department, which is currently focused on a big scale security Programme, covering multiple cyber security related improvements in the organization. The overall purpose of the UEBA initiative is to strengthen protection against risks that go otherwise undetected. Current project is in R&D phase and is seeking a contractor to help in properly shaping delivery requirements, assessing current environment situation

and driving the implementation process with assistance from internal resources.

Consultant will report and adhere to tasks of dedicated Project manager.

Responsibilities:

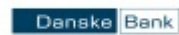
- Contractor will be part of Cyber Design & Build team in Vilnius, Lithuania.
- Identify prerequisites for UEBA tooling in the bank (existing possibilities, identifying missing parts, etc.)
- Analysis for UEBA Use cases, following industry standard and relevance for the bank
- Detailed roadmap/ implementation plan for defined Use cases
- Prepare recommendation based on Danske Bank environment assessment (which use cases to prioritize and provide detailed plan for implementation)
- Driving RFI process (information from potential vendors on the Market)
- Collaboration with internal Security Architect and engineers during R&D, POC and final implementation phases.
- Participate in Project meetings and report to assigned Project manager.

Requirements:

- Combined 5+ years' technical subject matter experience as a Security Architect and one of the following: Detection Engineering, Threat Hunting, Threat Intelligence, or Incident Response.
- Has experience with industry process and technologies (SIEM, Endpoint, Network, Security logs, etc.)
- Knowledge of industry recognized security and analysis frameworks (Mitre ATT&CK, Kill Chain, NIST Incident Response, etc.)
- Excellent technical capabilities, including an understanding of enterprise security network architecture, user and entity behavior analytics (UEBA) and other risk-based security operations with the ability to integrate state-of-the-art solutions into security operations.
- People skills and the ability to communicate effectively with various distributed Engineering teams

with the ability to explain and elaborate on technical details.

- Holds at least one of security certifications (e.g. CISSP)
- Active participation in leading and designing a successful UEBA solution and working experience in Financial Sector is considered as an advantage



Required Skills

IMPLEMENTATION

IT Security 5-6 years