Snr Endpoint Cybersecurity Engineer

Moody's

careers.moodys.com/

Lithuania

This assignment expired :when

About the assignment:

Location

Vilnius, Lithuania

Rate (after tax)

€4100 - 6600/Month

Duration

Full time position

Extension (project)

No

Remotely (optionally)

No

Expire On

2025-01-31 *(13 hours ago)*

Description

Skills and Competencies

- Strong background implementing and supporting endpoint security technologies such as EDR, AV, local firewalls, encryption, mobile device management, VPN and proxy
- Experience with Microsoft 365 offerings - Endpoint Manager, Intune, and Device Management
- Workstation and Server Security:

oProficiency in securing Windows operating systems, incl. Windows 10 & 11, MacOS and Windows Server.

oKnowledge of security features, such as BitLocker, Windows Defender, and Group Policy.

oUnderstanding of vulnerability management, patch management, and security hardening techniques for endpoints.

oExperience with log analysis, event monitoring, and incident response on workstations and servers.

oCloud Server Security: familiarity with cloud computing platforms (e.g., AWS, Azure, Google Cloud) and their security controls.

- Endpoint Security Solutions:

oExpertise in implementing and managing endpoint security solutions, such as antivirus/anti-malware software and endpoint detection and response (EDR) tools.

oUnderstanding of advanced threat protection techniques, including behavior-based analysis and sandboxing.

oKnowledge of endpoint security management platforms for centralized monitoring and policy enforcement.

- Security Standards and Compliance:

oUnderstanding of relevant security standards and frameworks, such as PCI DSS, HIPAA, NIST, and ISO 27001.

oKnowledge of endpoint security controls required for compliance and ability to implement and maintain them.

- Working experience with cloud technologies such as AWS, Azure, Google Cloud
- Automation or scripting experience
- Broad technical background including understanding of networking, firewalls, servers, workstations, and Active Directory
- Strong working knowledge of Windows Server and Workstation
- Linux, MacOS, AWS \ Azure experience is a big plus
- Experience with identity and access management (IAM) is a plus
- Ability to run projects at the technical and organizational level
- Accountable, responsible, collaborative and takes ownership for supported technologies
- Strong organizational skills, presentation skills

Education

- Minimum 5 years of experience in IT industry, preferably in a financial service or consulting organization
- IT engineering experience with endpoint security tools and technologies
- BS or BA degree, preferably in engineering, science, or technology; or equivalent work experience

Responsibilities

- Assist and become subject matter expert on endpoint security products – with a focus on centralized host-based firewall, EDR and privilege management
- Help research, testing and roll-out of new features for existing endpoint security tools
- Enhance automation in areas such as compliance, installation, and reporting
- Assist with creating and updating documentation including standard operating procedures and guides for different audiences – internal team, the Cyber organization, and other IT teams
- Develop, collect, and mature security metrics for IT Risk programs
- Security tool deployment in cloud and on-premise environments
- Provide escalation support for endpoint security tools
- Work with IT teams to develop or enhance processes, provide cross-training, assistance and build relationships
- Assist with compliance, ensuring endpoint tools are properly installed, reporting and fully functional across the organization
- Plan and assist with implementation of security tools for new acquisitions
- Plan and rollout upgrades, perform true-ups and remediation

About the team

The Cybersecurity team is globally responsible for helping the organization balance risk by

aligning policies and procedures with Moody’s business and regulatory requirements. The

team is responsible for the development, enforcement, and monitoring of security controls,

policies and procedures, disaster recovery programs, GRC (Governance, Risk and Compliance)

reporting and the delivery of security services including the company’s Cyber Security program.

Some scheduled weekend work and on-call rotation is expected.

Required Skills

ADMIN & NETWORK

Firewalls 0-1 year Windows Servers 0-1 year