Bedrijfsgegevens

ASML Netherlands
B.V.

De recruiter

MelvinToemin
Myler

Telefoon: +31629011288

E-mail: Melvin.toemin@headfirst.nl

Storage Security Specialist

Functie	**Storage Security Specialist**
Locatie	**Veldhoven**
Uren per week	**40 uren per week**
Looptijd	**20.11.2022 - 21.11.2024**
Opdrachtnummer	**105522**
Sluitingstijd	**21.11.2024**

Rolomschrijving en taakafspraken

Role and responsibilities

Undertaking of storage vulnerability assessments

Performing detailed security assessments on storage services

Assessing IT security exception requests on validity and provide advice to the team lead application security and business stakeholder for acceptance
or rejection including advice on additional security controls

Ensuring the audit ability of storage

Conducting, on a regular basis, security reviews of new and existing systems

Reviewing and monitoring security designs

Monitoring of existing security controls in the storage domain

Develop and maintain policies, standards and procedures to provide governance for storage security

Providing secure baselines

Utilizing in-depth knowledge of storage security to create implementation plans, ensuring successful completion of those plans in a timeliness manner that maintains current, recommended levels of protection

Owning and promoting the security strategy for protecting storage and integrating it with the wider security strategy

Researching latest best practices, make recommendations and assist in implementation of security measures to ensure the highest level of security available

Candidates will ideally have experience on risk assessment, security architecture and data sanitization techniques and tools. Also desired are skills in scripting languages (Perl, bash, ruby, python), safe backup and recovery technologies, data replication techniques, SQL, PL/SQL, and UNIX shell scripting and good OS administration skills (ideally Linux & MS SQL). Experience with and knowledge of NetApp SolidFire and NetApp EF-Series storage systems. Experience with and knowledge of the NFS, CIFS and SMB protocols.

Education and experience

Min 5+ years professional experience with a focus on storage security, risk and compliance.

Experience in executing Threat and Vulnerability analysis (TVA) or IT Security risk assessments

Experience with a wide range of SAP applications is a plus (no authorization management)

Experience with Cloud security and 3rd party management

Experience in collecting information through research and interviews

Good working knowledge of Office suite applications (must) like Excel and SharePoint

Skills

Working at the cutting edge of tech, you'll always have new challenges and new problems to solve – and working together is the only way to do that. You won't work in a silo. Instead, you'll be part of a creative, dynamic work environment where you'll collaborate with supportive colleagues. There is always space for creative and unique points of view. You'll have the flexibility and trust to choose how best to tackle tasks and solve problems.

To thrive in this job, you'll need the following skills:

Excellent English communication and presentation skills. Command of the Dutch language is a plus

Able to operate independently/with minimal supervision, self-starter

Ability to interact with all levels including users, engineers, executives and senior managers

Analytical, precise, tenacious, autonomous

Knowledge of IT-security, Information Security and Architecture methodology

Ability to overcome organizational resistance

Excellent organizational skills and the ability to prioritize multiple tasks and assignments

Able to digest large amounts of new information quickly

Able to grasp the deep technical characteristics of new environments quickly

Able to draft clear and concise visualizations of complex processes and environments

Able to stand your ground in a flexible / changing environment

Requirements

Academic qualifications are an advantage, but not a substitute for professional experience.

CISSP/CISM/ CISA or CompTIA Security+ certification is required.

CCSP or equivalent is a plus

Security/Technical/IT/informatics background bachelor's degree (or equivalent experience)

Deep Knowledge of current security technologies and governance processes

IT audit experience is a plus

Risk management experience is a plus

In-depth working knowledge of IT Risk / security frameworks and best practices, e.g.:

NIST Cyber Security Framework

ISF Standard of Good Practice for Information Security

NIST SP 800 30 framework

ISO 27001/2 framework

Bekijk opdracht online