Product Security Domain Architect

Location	Veldhoven, Netherlands
Degree	Master
Experience	8+ years

Introduction

ASML is the largest supplier in the world of photolithography systems for the semiconductor industry and manufactures machines for the production of integrated circuits. It is a heavily R&D driven company, and as such, it is critical that we properly safeguard our intellectual property.
All R&D is performed to deliver products to our customers (whether in physical or software only form). Changing threat and risk horizons require us to further improve on product security focusing on cyber security and information security resilience in respectively products and product intellectual property.

Job Mission

The product security domain is responsible for assuring the business develops their products within ASML cyber and information security risk appetite by developing, maintaining, and improving cross-product reference architecture in alignment with ASML risk appetite, product security risk management framework, and business needs.

Job Description

The Product Security Domain Architect is responsible for:

- Development, maintenance, and improvement of the cross-product security reference architecture in close cooperation with the product security focus group lead/ enterprise product security architect;
- Development, maintenance, and improvement of product security design patterns and integration of these in business/ product development processes;
- Alignment of cross-product security reference architecture with product security risk management framework;
- Execute product security control and risk assessments and drive mitigation in product development processes;
- Register product security risks and exceptions in respective R&D registers;
- Execution and coordination in product security incident and exception management processes;
- Capable to design and to support in design of solution architecture -including technical and operational aspects- for product security services;
- Support business line programs, product architects, and engineers in solution architecture, design and implementation of security requirements in products and services;
- Provide and contribute to security awareness trainings for specialized topics such as secure software development.
- Contribute to the development of product security policies, standards, benchmarks, and guidelines;
- Contribute to the development of product security means and methods such as assessment tooling;

- Contribute to the maturity of the product security technical competence;
- Remain oversight, manage dependencies and integration aspects, and assure cross-product security architecture is consistent across product security services.

Education

Bachelor/ master degree or equivalent combination of education and experience.

Experience

- Minimum of 10 years of relevant experience in IT security, OT security, Cyber Security;
- Proven strong IT and software architecture knowledge and background;
- Proven experience with risk management frameworks such as ISO 27001;
- Vendor agnostic expertise of IT/ software architecture;
- Proven up-to-date experience with vulnerability scanning and/ or penetration testing;
- Knowledge of open source software;
- Experience in Linux (RHEL-based) environments;
- Proven experience in security software development and secure programming (Java, Python, Golang)
- Knowledge of Securing Cloud Solutions such as GCP, Azure;
- Knowledge of virtualization and containerization technologies such as Kubernetes, VMware, and Docker.
- Monitoring tools: Splunk ITSI, Enterprise Security, Observability Suite, Phantom, Cribl;
- HashiCorp: Vault, Boundary, Consul, Terraform, Waypoint;
- Pre: Experience with certificates and encryption techniques.
- Generic security certifications like CISSP, and CISM;
- Specialized security architecture certifications like TOGAF9, SABSA, CISSP-ISSAP, and GDSA.

Personal skills

- Skill to lead, influence, and negotiate without authority;
- An business enabling security attitude in opposite to a business disabling one;
- Strong analytical skills in combination with common sense;
- Ability to translate risks, threats, and vulnerabilities to business stakeholder level and to drive risk mitigation, dealing with resistance and risk appetite;
- Pro-active and self-motivated attitude;
- Political aware and sensitive;
- Fluent English (written and verbal);
- Team player;
- Strong communication and presentation skills;
- Drive to retrieve the root cause of the problem.

Other information

This position requires access to U.S. controlled technology, as defined in the United States Export Administration Regulations. Qualified candidates must be legally authorized to access such U.S. controlled technology prior to beginning work.