CYBER SECURITY ENGINEER – Bologna area, Torino area (IT)

In this role, you will be part of a team, responsible for achieving excellence in computer science, electrical & electronic engineering. You will use your knowledge of both hardware and software to develop and support production of a variety of new chassis, powertrain, hybrid and body components together with a dynamic team, finding solutions to interesting challenges.

We are looking for a full time Cyber Security Engineer with passion for the Automotive sector and willing to become a subject matter expert, who will act within internal company and customer projects.

What You'll Do

- Participate in engineering projects to identify threats and vulnerabilities in infrastructure, software and embedded system architectures of the vehicles
- Carry out threat modeling and security analyses
- Work with engineering teams from concept through implementation, ensuring that the security activities are timely executed according to the design process
- Define security architecture requirements adopting security-by-design approach
- Define cybersecurity requirements for and work with engineering teams to successfully integrate security mechanisms in software and hardware components
- Support the definition of the cyber security and software update management system
- Interpret and apply cyber security and software update standards and regulations
- Support security related customer milestones and assessments
- Specify and support the execution of system and vehicle level validation testing (e.g. pentest)
- Support the definition of company-wide cybersecurity and software update management systems

What We're Looking For

- Degree in Computer Engineering, Computer Science, Electronic Engineering, Telecommunicaton, or a related field
- Enthusiast in automotive cyber security and vehicle embedded systems
- Willing to learn and apply existing security practices such as the Cyber Security and Software Update standards (ISO 21434, SAE J3061, ISO 24089) and regulations (UNECE R155, R156)
- Ability to analyze threat and vulnerability information to prioritize for current and future vehicle architectures
- Familiarity with security design patterns for systems and software
- Ability to develop and implement novel and advanced security analysis techniques
- Ability to develop and explain technical decisions and recommendations effectively with technical and non-technical audiences through verbal and written communications that lead to actionable and measurable improvements
- Ability to perform meticulous work with careful attention to detail but performed in a very fast-paced and exciting environment to identify threats, defects and weaknesses in complex systems, and to identify process improvement opportunities
- Enthusiast in understanding and applying existing security practices such as the Cyber Threat Intel Standards (enisa, SANS, STIX), vulnerability management standards
- Availability to travel for work