

Requisition Number:

Job Description. Cybersecurity Specialist

MIRA is a world-class, independent engineering consultancy, operating in multiple locations around the world, to support vehicle manufacturers and their supply chain with cutting-edge engineering and testing expertise. We offer full-system design, test and integration expertise to automotive, defence, rail and transport industries and also specialise in developing low carbon and autonomous and co-operative driving technologies.

At our headquarters in the Midlands, we have access to one of the most comprehensive vehicle proving grounds which boasts 93km of test tracks and over 35 world-class test facilities and laboratories. Our facilities, combined with the engineering expertise of our 600 strong team makes MIRA Technology Park Europe's number one location for transport sector R&D.

Title of Job:	Cybersecurity Specialist		
Department:	Vehicle Resilience		
Grade:	Senior Engineer or above depending on background		
Date Required:	ASAP		
Salary Range:	Competitive		
Number Required:	1		
Location:	HORIBA MIRA, Nuneaton		
Reason for Vacancy:	Technology Team Expansion		
Contract Type:	Permanent:	Y	Contractor: N
Responsible To:	Head of Vehicle Resilience		
Subordinates:	None		

Main Purpose of Job
<p>MIRA is looking for a dynamic and proactive Cybersecurity Specialist to join a new team in Nuneaton. Based within the Vehicle Resilience department they will form part of the growth strategy within HORIBA MIRA. This roles will include, but not be limited to, increasing MIRA's trusted automotive cybersecurity service offerings with specific focus on:</p> <ul style="list-style-type: none"> • Complete automotive cybersecurity engineering and test service development/delivery with emphasis on a systems engineering approach: <ul style="list-style-type: none"> ○ Threat and risk analysis ○ Development of cybersecurity concepts and requirements ○ Cybersecurity verification planning and management ○ Cybersecurity vulnerability assessments and penetration testing ○ Design, development and problem solving to ensure client product security <p>Secondary focus will include supporting MIRA's Functional and Safety specialists to:</p> <ul style="list-style-type: none"> • Further develop our advanced Verification and Safety services • Perform any associated new technology research and horizon scanning <p>This technical role requires a highly motivated individual with experience in creative but structured problem resolution, advanced data manipulation / analysis, and new technology cybersecurity test</p>

and engineering methods.

Key Functions

The role offers a wide range of diverse activities and opportunities for the selected individual to make a real difference to the new and existing teams. The following activities cover the typical requirements of the roles:

- Service Development
 - Research cybersecurity aspects of new technology standards including potential vulnerabilities and secure design principles
 - Develop and validate new cybersecurity engineering capabilities
 - Optimise new technology services through structured continuous improvement
 - Write procedures for the delivery of cybersecurity engineering services
 - Assist in the optimisation of current test and engineering processes and policies
- Consultancy
 - Lead / assist consultancy, and large / complex, customer programmes
 - Provide technical support in own area of expertise to cross-discipline team
 - Provide internal support to product development areas of HORIBA MIRA
 - Lead / assist research and development projects
 - Problem resolution
- Project Management
 - Support cross-discipline delivery across core programmes / projects

A large part of this role will involve new service strategy, development, implementation and delivery tasks. As such, strong technical knowledge and experience of cybersecurity, computer science and electrical and electronic principles are essential. A working knowledge of test and measurement equipment, antennas, EM theory, systems engineering, and problem resolution will be a significant advantage.

Entrants will have a hands-on expert knowledge of cybersecurity test and engineering standards and methods, and an understanding of new vehicle technologies, architectures, diagnostics and applicable test and engineering methods to assess and resolve their associated cybersecurity vulnerabilities. **It is essential that applicants understand the challenges of cybersecurity within the automotive industry.**

Successful candidates will work as part of a collaborative team to deliver customer and development programmes across multiple disciplines including EMC, Connectivity, Cybersecurity and Functional Safety for the automotive, off-highway, agricultural and military sectors. Excellent communication skills (both written and verbal) are essential as liaison with both internal project managers and external customers occurs on a daily basis. Excellent time management and flexibility in working hours are essential.

Attention to detail and an ability to plan and deliver complex work programmes, along with an understanding of the importance of data validation are key.

The successful candidate will have the ability to:

- Make effective decisions
- Communicate effectively (written and verbal)
- Deliver a high standard of technical writing
- Work under pressure, individually and as part of a team
- Take responsibility and ownership
- Remain calm in all situations
- Plan and prioritise delivery of both short and long duration projects
- Deliver customer expectations in a timely fashion, to aid contractual / financial goals

--

Essential Qualifications	Preferred Qualifications
<ul style="list-style-type: none"> Bachelors degree (minimum 2:1) or equivalent qualification in electrical / electronic engineering, computer science, cybersecurity or other relevant discipline 	<ul style="list-style-type: none"> Relevant Masters Degree or PhD Professional membership of a relevant engineering or computing institution for example Chartered Engineer

Essential Experience	Preferred Experience
<p>Minimum 10+ years of experience in a relevant field covering many of the key functions detailed previously</p> <p>Experience in some combination of the following:</p> <ul style="list-style-type: none"> Wireless technologies (e.g. Wi-Fi, Bluetooth, NFC) Wired networking technologies (e.g. CAN, Ethernet) Embedded operating systems (e.g. QNX, Linux, Android) Threat modelling and vulnerability analysis Security risk assessment Systems engineering Fuzz testing Penetration testing 	<p>Minimum 15+ years of experience in a relevant field covering many of the key functions detailed previously</p> <p>Knowledge or experience in any of the following:</p> <ul style="list-style-type: none"> Security engineering for cyber-physical systems Working knowledge of SAE J3061 or other appropriate cybersecurity standards Knowledge of in-vehicle network protocols (CAN, FlexRay, automotive Ethernet) AUTOSAR framework Cryptography principles, applications and implementation considerations

What are the candidates likely to be doing now?
<p>Hands-on cybersecurity engineer or specialist in a high technology industry or within the automotive industry</p> <p>Cybersecurity research specialist</p>

Other information
<p>Must hold a full driving licence</p>