Organisation for Joint Armament Co-operation
Executive Administration

VACANCY NOTICE	
Post	B040 – CYBER SECURITY IDENTITY & CLOUD SPECIALIST
Nationality	Vacancy is only open to nationals of an OCCAR Member State: Belgium, France, Germany, Italy, Spain and the United Kingdom.
Grade, Step, Salary	Grade B6, Step 1 We offer an excellent compensation package. Find out more on our remuneration webpage
Division	Information Division
Section	Information and Communication Technology Section
Management of Staff	0
Location	Bonn, DE
Initial Contract Duration	3 years
Closing Date for Applications	12/01/2026
Start Date	01/05/2026
Interview Date	Week commencing on 16/02/2026

1. Background

The Information Division (ID) is responsible for providing services related to Information and Communication Technology (ICT) and Information Management (Info Mgmt) to support and enable the Programme Divisions and the Central Office to carry out the core activities of OCCAR-EA efficiently and effectively.

This includes all matters relating to ICT and Info Mgmt, including the management of IT infrastructure, cybersecurity, data protection, digital communication systems, collaboration tools, software applications, knowledge management, data governance, and ensuring the secure and compliant handling of all information across OCCAR-EA.

In this vacancy, OCCAR is seeking a Cyber Security Specialist to maintain and strengthen the security of its Cloud services, the hybrid identity infrastructure and its classified on-premises environments.

2. Duties and Responsibilities

The Cyber Security Identity & Cloud Specialist will report to the ICT Section Leader. The post holder supports the ICT Security Manager (ICTSM) and works in close collaboration with the ICT Security Support Engineer (ISSE), ICT administrators, and the Information Management Section. Together, they contribute to the continuous development, implementation, and review of OCCAR-EA's IT and cyber security measures, following the established ICT Security policies and procedures. The role plays an active part in identifying, mitigating, and managing cyber security risks, vulnerabilities, and incidents.

The overall objective of the position is to help ensure that effective cyber security and protection measures are applied consistently across OCCAR-EA's hybrid IT infrastructure and support. Particular emphasis is placed on Microsoft Cloud services and identity management environments.

In particular, they will:

- Support the implementation and monitoring of cyber security controls across OCCAR's Microsoft cloud and on-premise environments;
- Provide support for the planning, implementation, and secure execution of projects related to Identity Management, including identity-related controls, measures, and associated technologies.
- Help maintain security across Microsoft Sentinel, including rule configuration, data connector management, playbook integration, and incident response;
- Participate in the response to cyber incidents, brute-force attempts, phishing campaigns, or DLP violations across M365 and on-premise systems;
- Support the integration, configuration, and daily operation of cybersecurity tools used for monitoring, threat detection, data protection, and network security across both cloud and on-premise environments;
- Collaborate on projects related to forensic investigations, vulnerability management, integration and compliance with security policies and classifications;
- Assist in the preparation and maintenance of cybersecurity documentation, including support for audits, accreditation processes, and continuous improvement activities, with a primary focus on Microsoft cloud and identity services, and additional contributions related to on-premise systems where applicable;
- Contribute to awareness campaigns and internal training initiatives;
- Support every procurement process related to their expertise and projects related;
- Provide advice and support in all related contracts, contractors and Service Level Agreements;
- Additional tasks as defined by ICT Section Leader and Head of Division

3. Key competences and skills required for the grade

(You must provide evidence of meeting these key competences and skills in your Application, Section 12).

CS 1 Excellent interpersonal skills with the ability to interact and communicate at all levels within OCCAR as well as with Nations;

CS 2 The ability to work in a changing, developing and demanding environment;

CS 3 The ability to work independently based on objectives set by the line manager;

CS 4 The ability to use Computer and Information Technology (ICT) facilities, and able to demonstrate a good working knowledge of MS Office software;

CS 5 Good team-working skills with ability to establish good working relations at all levels in a multicultural context and with respect for diversity.

4. Specialist knowledge and experience required for the post

(You must provide evidence of meeting these specialist requirements in your Application, Sections 10 and 11).

4.1 Essential:

ES 1 Proven understanding and practical application of core cybersecurity principles and best practices in hybrid environments (preferred Microsoft), including risk assessment, mitigation strategies, and protection of information assets across both cloud-based and on-premise infrastructures; familiarity with confidentiality, integrity, and availability models, and their implementation in operational security frameworks;

ES 2 Proven experience in supporting identity and access management (IAM, preferred Entra Id) processes, including user provisioning, role-based access control, account lifecycle management, and secure authentication mechanisms; sound knowledge of credential protection practices and practical involvement in the implementation and maintenance of IAM solutions, preferably in cloud or hybrid environments;

ES 3 Sound knowledge of cloud-based environments and their associated security challenges, including secure configuration, access control, and data protection; experience supporting or administering cloud platforms, preferably Microsoft 365, and familiarity with cloud identity models, security baselines, and compliance requirements in hybrid infrastructures based on Microsoft;

ES 4 Proven experience working with security monitoring and detection tools, including Security Information and Event Management (SIEM, Sentinel and Splunk preferred) platforms; practical involvement in configuring alerts, analysing events, or supporting incident response activities in operational environments, with a focus on threat visibility and early detection;

ES 5 Proven experience collaborating within technical teams in the context of cybersecurity operations; familiarity with incident handling workflows, coordination of response actions, and documentation of technical procedures across both cloud-based and on-premise environments, including the ability to support structured investigations and cyber security improvements.

4.2 Desirable:

DS 1 Proven experience in hybrid identity scenarios involving the integration of on-premises and cloud authentication systems; familiarity with Microsoft Entra ID, including its synchronization with Active Directory, as well as technologies such as ADFS and Single Sign-On (SSO), covering both implementation and operational aspects;

DS 2 Sound knowledge and experience in interpreting cybersecurity policies, procedures, and technical documentation, and translating them into operational workflows and playbooks; experience supporting the development or implementation of automated response actions, particularly within cloud or hybrid security platforms;

DS 3 Good knowledge of data protection and classification tools, including the use of labelling, encryption, and access controls to safeguard sensitive information; understanding of how Data Loss Prevention (DLP, Microsoft Purview, and Trellix for on-premise) policies support compliance, mitigate risks, and enforce governance requirements across cloud and on-premise environments;

DS 4 Good knowledge or demonstrated interest in digital forensics and open-source intelligence (OSINT); prior involvement in forensic investigations, evidence preservation, or threat intelligence analysis using open data sources will be considered a strong asset for this role;

DS 5 Experience with Microsoft cloud security tools, such as Entra ID, Microsoft Defender for Cloud, Microsoft Purview, and Sentinel, will be considered a significant advantage; familiarity with log aggregation and analysis platforms such as Splunk, as well as exposure to alerting workflows and automated incident response processes, is also highly relevant to the role.

5. Language Requirements

- ADVANCED level[1] of ENGLISH both oral and written.
- Additional knowledge of another OCCAR Member or Participating State's language will be considered as an asset.

[1] *The language levels can be found on the OCCAR website, www.occar.int Careers / Applying.*

6. Qualifications

A relevant vocational qualification or technical education equivalent to EQF level 4 is required. A higher EQF level is not mandatory but will be positively considered. Candidates should have a minimum of five years of professional experience in cybersecurity roles in areas directly related to the responsibilities of the position, including at least two to three years specifically focused on cloud identity and security.

Certifications in cybersecurity and cloud security will be considered an asset. These may include:

- Basic cybersecurity certifications, such as CompTIA Security+, CompTIA CySA+, or equivalent;
- Microsoft certifications, particularly those focused on security and identity, such as SC-900 (Microsoft Security, Compliance, and Identity Fundamentals), SC-200 (Security Operations Analyst), SC-300 (Identity and Access Administrator), and AZ-500 (Azure Security Engineer);
- Other relevant certifications in the field of cybersecurity and cloud security will also be positively considered.

7. Security Clearance

Security clearance at OCCAR SECRET level is required for this post - or needs to be obtained within the first 6 months of employment.

8. Applications and Points of Contact

Applicants wishing to apply for this Post should email the completed application and supporting documentation to: application@occar.int

For further information regarding this post please send your inquiry to the same email address.

OCCAR Privacy Statement:

When applying for an OCCAR vacancy, it is necessary for OCCAR to collect and process personal data about you in order to assess and evaluate your suitability for the vacancy, and (if successful) to coordinate with relevant service providers in preparation of your appointment. For further information please visit our web-site: OCCAR Privacy Statement - http://www.occar.int/privacy-data-protection.