

Join a young company active in Luxembourg and neighboring countries.
We help our customers put security at the heart of their digital transformation.
Although our field is profoundly digital, we put people at the heart of our business.

Your profile

With a degree in computer science or information security, **you have 3 to 5 years' experience in securing Microsoft environments and IT infrastructures.**

You are familiar with the principles of identity and access security and Microsoft workloads, with expertise in Microsoft Entra ID (ex-Azure AD), Microsoft 365 Security and Azure Security. You also have a good grounding in system administration and automation.

If you already have experience with Microsoft Security solutions (Defender, Sentinel, Entra ID, Conditional Access, PIM, etc.) and a good understanding of modern IT threats, this is the job for you.

We're looking for someone who is autonomous, rigorous, curious and able to work on complex projects with technical and business teams.

Core Competencies

Infrastructure Security & Microsoft Security

- Securing Windows Server, Active Directory, Microsoft Entra ID (ex-Azure AD)
- Implementation of Microsoft Defender solutions (Endpoint, Identity, Office, Cloud Apps, etc.)
- Access and identity management: MFA, Conditional Access, Privileged Identity Management (PIM), Entra Permissions Management
- Deployment and management of SIEM tools (Microsoft Sentinel), Log Analytics, Defender for Cloud.

Your profile**Microsoft 365 & Azure security**

- Microsoft 365 access and data protection (DLP, Information Protection, Safe Links, Safe Attachments)
- Securing Azure workloads: Network Security Groups (NSG), Identity Protection, Defender for Cloud Apps
- Role and permission management in Entra ID and cloud applications
- Threat monitoring and attack investigation on Microsoft 365 & Azure

System Administration & Automation

- Proficiency in Windows & Linux environments
- Automation with PowerShell, Bash, Python
- Management of security updates and patches (WSUS, SCCM, Intune)
- Log analysis and response to security incidents

Technical Audits & Remediation

- Vulnerability analysis and patching (Nessus, Qualys, OpenVAS)
- Security incident investigation and response
- Log monitoring and analysis of critical events
- Participation in compliance audits and technical recommendations

Certifications (a plus, but not mandatory)

- Microsoft Certified: Fundamentals of Security, Compliance and Identity (SC-900)
- Microsoft Certified: Azure Security Engineer Associate (AZ-500)
- Microsoft 365 Certified: Associate Security Administrator (MS-500)
- CompTIA Security+, Certified Ethical Hacker (CEH)



A socially committed company that values its employees and their well-being

Highly professional and experienced colleagues

Interesting and challenging projects

A unique opportunity to progress in the IT security field

A competitive salary and corresponding package

Send your application to

carriere@adronh.com