Wer wir sind

Stark wie ein Konzern – agil wie ein Startup!

Mit 1.000 Mitarbeitern an 26 Standorten in 8 Ländern unterstützen wir unsere Kunden 24/7 in den Bereichen Business Solutions, digitale Plattformlösungen und den Betrieb kompletter IT-Infrastrukturen.

We are seeking an experienced and versatile Technical Security Consultant to join our growing cybersecurity team.
In this role, you will act as a technical expert and trusted advisor across a broad range of security technologies and frameworks.
You will leverage your experience in SOC operations, threat detection, network security, and compliance frameworks to protect and enhance our security posture.

Technical Security Consultant (Allrounder) (m/w/x) - Full Remote

Key Responsibilities

- Operate, monitor, and optimize XDR (SentinelOne), SIEM platforms, and Privileged Identity Management (PIM) solutions

- Analyze security alerts, identify threats, and coordinate incident response activities
  Support the design, implementation, and management of network security controls (DNS security, firewall configurations, VPNs, segmentation)
- Conduct technical assessments and provide recommendations to improve security infrastructure
- Assist in the development and maintenance of security policies and procedures aligned with standards such as ISO 27001, SOC 2, and NIST
  Collaborate with IT and business teams to identify security gaps and drive remediation efforts
- Participate in security audits, assessments, and compliance initiatives
  Provide knowledge transfer, training, and support to internal stakeholders regarding security technologies and best practices

Qualifications

- 4–6 years of hands-on experience working in a Security Operations Center (SOC) environment
- Strong technical expertise with:
  SentinelOne (XDR) or similar EDR/XDR solutions
  SIEM tools (e.g., Microsoft Sentinel, Splunk, LogSign etc.)
  Privileged Identity Management (PIM) platforms
- Solid understanding of network protocols and technologies (TCP/IP, DNS, DHCP, VPNs, firewalls)
  Basic to intermediate knowledge of security standards and frameworks (e.g., ISO/IEC 27001, SOC 2, NIST Cybersecurity Framework)
- Experience with security monitoring, threat hunting, and incident response processes
  Familiarity with endpoint protection, vulnerability management, and data protection strategies
- Excellent analytical, troubleshooting, and communication skills

Nice-to-Have:

- Certifications such as CompTIA Security+, Certified Ethical Hacker (CEH), GIAC certifications (e.g., GCIH, GCIA), or Microsoft Certified: Security Operations Analyst
- Hands-on experience with cloud security (Azure, AWS) is a plus
- Knowledge of scripting (PowerShell, Python) for automation is an advantage
- Experience working in regulated industries or environments with strict compliance requirements

Darauf kannst du dich freuen

- A dynamic, supportive, and innovative team environment
- Opportunities for continuous learning and professional development
- Flexible working arrangements (remote/hybrid)
- Competitive salary and benefits package
- The chance to work with the latest security technologies and frameworks

in German:

- Moderne Büroräumlichkeiten in den Metropolregionen und technisches Equipment auf dem aktuellsten Stand
- Ein unbefristetes Arbeitsverhältnis mit einem attraktiven Gehaltspaket
- Flexible Arbeitszeiten und die Möglichkeit Full Remote zu arbeiten bei einer Reisetätigkeit von maximal 20%
- Jährliche Weiterbildungen und Zertifizierungen sowie Mitarbeiterentwicklung im Top Talent Program
- Je nach Standort und Position Mobilitätszuschüsse, z.b. Jobticket oder Geschäftswagen
- Betriebliche Altersvorsorge (BAV) und Zuschüsse für deine Gesundheit
- Team- und Firmenevents und die Möglichkeit deinen Hund mit ins Büro zu bringen

Jetzt bewerben

Kontakt

Aylin Vogt
Talent Acquisition, CONVOTIS Group

karriere@convotis.com