



SENIOR CYBER SECURITY ANALYST

80–100 % Pensum

Hybrides Arbeiten • Per sofort oder nach Absprache

Cyber Security ist unsere Leidenschaft – deine auch?

Wir suchen laufend neue Mitarbeitende, die uns auf unserer Mission und Vision, die Welt Tag für Tag digital sicherer zu machen, begleiten.

Deine Aufgaben

- Selbstständige Analyse und Bearbeitung komplexer sowie eskalierter Security Offenses
- Kontinuierliche Optimierung der Detections aus der Fallarbeit: Bewertung der auslösenden Regel, Umsetzung bzw. Nachverfolgung der Anpassung bis zur Wirksamkeit - Ursachenorientiertes Tuning statt Symptomunterdrückung.
- Baselining bei Neukunden und Nachjustierung bei Umgebungs- und Log-Quellen-Änderungen
- Threat Hunting auf Basis von CTI und Kundenkontext
- Unterstützung in der Qualitätssicherung: Fallreviews inkl. der als unkritisch geschlossenen Alerts, Vier-Augen-Prinzip bei kritischen Eskalationen, Kalibrierung der Bewertungsmassstäbe
- Überführung wiederkehrender manueller Schritte in Playbooks, Anreicherung und Automatisierung
- Ausbildung und Mentoring von Young Professionals auch im Optimierungs- und Qualitätsdenken
- Mitwirkung in Service-Entwicklung, internen Projekten und Service-Management-Meetings
- Support bei Eskalationen und Pikett (ca. 3–6x jährlich, mit Zusatzvergütung)

Das bringst du fachlich mit

- Abgeschlossenes Studium im Bereich Informatik (FH/Uni) oder Informatikausbildung EFZ mit mind. 5 Jahren relevanter Praxiserfahrung, davon 3 Jahre im SOC-/ oder Incident-Response-Umfeld
- Tiefes Verständnis von Angriffstechniken und Detektionslogik entlang MITRE ATT&CK
- Tiefgehende Kenntnisse in Windows, Unix/Linux, Netzwerk-/Firewall- und Loganalyse
- Erfahrung mit modernen XDR/SIEM-Plattformen (z. B. Microsoft Defender, Cortex XDR, CrowdStrike, Sentinel, Harfang, Vectra)
- Tiefgehende Kenntnisse im Bereich Incident-Management und Grundlagen digitaler Forensik

- Berufsbezogene Zertifizierungen (z. B. SC-200, GCDA, GCIA, GCFA, OSCP)

Das bringst du persönlich mit

- Verhandlungssicher in Wort und Schrift Deutsch
- Gute Englischkenntnisse (mündlich und schriftlich)
- Zuverlässigkeit und gewissenhaftes Arbeiten
- Schreibkompetenz: komplexe Sachverhalte darstellen
- Proaktives Einbringen: Bereitschaft, eigene Routinearbeit zu automatisieren
- Coaching-Haltung und konstruktives Verhalten im Peer-Review
- Fähig, in stressigen Situationen einen kühlen Kopf zu bewahren und unter Unsicherheit zu entscheiden

Du hast Lust, diese Herausforderung anzupacken?

Dann freuen wir uns auf deine Online-Bewerbung! Bei Fragen gibt dir Marius Maier gerne Auskunft (job@infoguard.ch).

Hinweis für Personalvermittlungen: Mit dem Upload von Kandidatendossiers akzeptieren Sie unsere [Allgemeinen Geschäftsbedingungen](#).

Jetzt bewerben

Zugang Personalvermittlung

InfoGuard ist ein führendes Unternehmen im Bereich Cyber Security mit umfassender Expertise in Cyber Defence Services, Incident Response Services, Managed Security & Network Solutions für IT-, OT- und Cloud-Infrastrukturen sowie Services in den Bereichen Architektur, Engineering, Penetration Testing & Red Teaming und Security Consulting. Über 230 Expert*innen sorgen tagtäglich für die Sicherheit bei über 400 Kunden in der Schweiz, Deutschland und Österreich. InfoGuard hat den Hauptsitz in Baar/Zug sowie Niederlassungen in Bern, München und Wien.

InfoGuard AG | Lindenstrasse 10 | 6340 Baar | Tel +41 41 749 19 00 | job@infoguard.ch