



Senior Incident Manager IT-Security Operations (w/m/d)

Für diese verantwortungsvolle Position suchen wir eine durchsetzungsstarke Persönlichkeit, die für die ganzheitliche Abwehr, Analyse sowie Bewältigung von Cyberbedrohungen unsere IT-Security-Prozesse rund um Threat Monitoring, Threat Response und Security Incident Response verantwortet. Du überzeugst mit ausgeprägten analytischen sowie konzeptionellen Fähigkeiten, bist strukturiert und verstehst dich auf aktives Netzwerken im Umfeld von IT-Security? Dazu arbeitest du gerne eigenständig sowie im Team und zeichnest dich durch pragmatisches, lösungsorientiertes Handeln aus, bei dem du stets Kosten, Nutzen und Risiken abwägst? Dann sagen wir: Herzlich willkommen bei der Aareal Bank Group.

Darauf kannst du dich freuen:

- ✓ Unter Berücksichtigung von Industriestandards sowie regulatorischen Anforderungen (u. a. DORA) konzipierst, dokumentierst und verbesserst du prüfungssichere Prozesse, Verfahren sowie Richtlinien.
- ✓ Neben der laufenden Überwachung stellst du ihre Operationalisierung sicher, begleitest Prüfungen und beweist deine Fachkompetenz beim Bewerten, Nachverfolgen sowie Bearbeiten von Ergebnissen.
- ✓ Du übernimmst die Optimierung, Steuerung sowie Qualitätssicherung von Threat-Monitoring-Use-Cases (SIEM / EDR / XDR) und bewertest auf Basis präziser Analysen kritische Security Alerts aus dem SOC.
- ✓ Auch bei der ganzheitlichen Bearbeitung von Security Incidents ist auf dich Verlass – ob Risikoanalyse, Koordination von Gegenmaßnahmen, Kommunikation, Dokumentation oder Eskalation.
- ✓ Neben Incident-Response-Runbooks für Angriffsszenarien erarbeitest du Incident-Kategorien im Security-Modul von ServiceNow, pflegst sie und unterstützt uns bei weiteren Bedrohungsanalysen durch die Auswertung von Security-Datenquellen wie SIEM oder EDR.
- ✓ Auf Basis eigener fundierter Analysen und fachlicher Prüfungen von Threat-Hunting-Ergebnissen externer

Dienstleister leitest du Verbesserungen für Detektionsmechanismen sowie Use Cases ab.

- ✓ Als Ansprechperson rund um Threat Prevention, Detection und Response begleitest du den Betrieb der vom SOC genutzten Systeme und führst mit der IT bzw. Entwicklung neue Technologien / Prozesse ein.
- ✓ Ob Service-Management, KPI-Monitoring oder Qualitätskontrolle – du steuerst den SOC-Dienstleister, treibst fachliche Projekte voran und steigerst durch Workshops bzw. Schulungen die Security Awareness innerhalb unserer Bank.

Darauf können wir uns freuen:

- ✓ Erfolgreich abgeschlossenes Studium der Informatik, Informationstechnologie oder eine vergleichbare Qualifikation
- ✓ Idealerweise mind. eine der folgenden Zertifizierungen: SANS / GIAC (z. B. GCIA, GCED, GCDA, GMON, GDAT) oder CISSP, CEH, CompTIA Security+ oder vergleichbar
- ✓ Mehrjährige Berufspraxis im Kontext von SOC-Blue-Team oder Incident Response – bevorzugt in einer Bank oder einem regulierten Umfeld
- ✓ Erfahrung in der Leitung und Steuerung von IT- und Security-Projekten unter Einbindung interner Fachbereiche sowie externer Dienstleister
- ✓ Bestens vertraut mit SIEM- und EDR-Lösungen, Threat Monitoring sowie Use-Case-Management, dazu fundiertes Know-how in Netzwerktechnologien, -architekturen und -sicherheit (Firewalls, IDS / IPS etc.)
- ✓ Expertise in aktuellen Bedrohungslagen, Angriffstechniken und Taktiken (MITRE ATT&CK) mit Kenntnissen im COS-Umfeld (z. B. Windows, macOS, iOS) und Endpoint-Security-Architekturen
- ✓ Sicherer Umgang mit Windows- sowie Linux-Infrastrukturen für Analysen und Gegenmaßnahmen
- ✓ Verhandlungssicheres Englisch in Wort und Schrift

Das machen wir anders:

- ✓ **A**abwechslungsreiche Aufgaben: Bei uns kannst du deine Expertise einbringen, Themen voranbringen und Neues gestalten. Wir haben eine Kultur, in der sich alle aktiv einbringen und Einfluss nehmen können.
- ✓ **A**ußergewöhnliche Weiterentwicklung: Wir fördern jede Person gleichermaßen, deshalb unterstützen wir dich mit individuellen Entwicklungsmöglichkeiten und Lernwegen. Damit du bestehende Kompetenzen ausbauen und neue zukunftsweisende Fähigkeiten aufbauen kannst.
- ✓ **A**usgeglichene Worklife-Balance: Mit mobilem Arbeiten und flexiblen Arbeitszeitmodellen hast du die Möglichkeit, deine Arbeit individuell zu gestalten. So lassen sich Arbeit, Familie und die persönliche Lebenssituation bestmöglich unter einen Hut bringen.
- ✓ **A**usgezeichnete Benefits: Unsere Services und Benefits bieten dir einen echten Mehrwert, die uns so zu einem Top-Arbeitgeber machen. Bei uns erhältst du beispielsweise Vergünstigungen bei Kooperationspartnern oder Zuschüsse zum Nahverkehr. Ebenso sorgen wir mit einer betrieblichen

Altersversorgung oder vermögenswirksamen Leistungen für deine Zukunft vor.

- 🕒 **A**ktives Gesundheitsmanagement: Ärztliche Check-ups, Beratungsangebote, gemeinsame Sportevents, unsere beliebte Kantine oder Kaffeebar – Bei uns kannst du das nutzen, was deine Gesundheit fördert und dir guttut.

[Jetzt bewerben](#)

Das sind wir:

Willkommen in der Welt der Aareal Bank!

Wir sind Mittelständler und Global Player. Als internationaler Immobilienspezialist arbeiten wir alle auf ein gemeinsames Ziel hin: den Erfolg unserer Kunden. Bei uns arbeiten über 1.000 Menschen aus 44 Nationen auf drei Kontinenten daran, dass wir **als Bank ganz schön anders sind!** Wir sind verantwortungsvoller und erstklassiger Ausbildungsbetrieb und eine Organisation mit viel Expertise und kurzen Wegen, viel Gestaltungsspielraum und dem Anspruch, für unsere Kunden immer besser zu werden. **Das macht uns stark und vor allem: anders!**

Aareal Bank AG
Human Resources
Paulinenstraße 15 · 65189 Wiesbaden
Leon Buderus
Telefon: +49 611 348 2880
E-Mail: leon.buderus@aareal-bank.com

Aareal

AAREAL BANK – GANZ SCHÖN AANDERS.