BERENBERG
PARTNERSHIP SINCE 1590

Für unsere **Abteilung Investment Banking Technology** in **Hamburg oder Frankfurt** suchen wir **zum nächstmöglichen Zeitpunkt** dich als

(Senior) SOC Analyst Engineer

Global Technology @ Berenberg

In einer Ära, in der Digitalisierung und moderne IT-Infrastrukturen das Banking revolutionieren, gestalten wir eine technologiegestützte Bank, in der du als IT-Profi eng mit unseren Geschäftsbereichen zusammenarbeitest. Unsere Technology-Teams bieten dir ein Umfeld, das dich vor spannende Herausforderungen stellt – sei es durch den Support und die Weiterentwicklung von Legacy-Systemen oder die Einführung moderner Technologien wie KI, Machine Learning und hochgradig automatisierte Handelsapplikationen.

Deine Rolle im Team

Die Abteilung Investment Banking Technology ist auf den Geschäftsbereich Investment Banking ausgerichtet, der in den letzten Jahren strategisch ausgebaut wurde und sich vor allem an internationale institutionelle Kunden richtet. Die Bank operiert global auf den internationalen Kapitalmärkten und auf höchstem Niveau. Die von Investment Banking Technology selbst entwickelte Software und die betreuten Systeme müssen den höchsten Performance- und Qualitätsansprüchen genügen.

Als erfahrener Senior SOC Analyst übernimmst du eine Schlüsselrolle in unserem Security Operations Centre (SOC) und bist verantwortlich für die Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen. Du führst tiefgehende forensische Untersuchungen durch, entwickelst präzise Incident-Response-Strategien und erstellst detaillierte Reports für das Management und relevante Stakeholder. Deine Expertise trägt maßgeblich zur Optimierung der Überwachungs- und Erkennungsmechanismen bei, um eine proaktive und resiliente Security Architecture zu gewährleisten. Darüber hinaus agierst du als Mentor für das SOC-Team, vermittelst Best Practices und förderst eine kontinuierliche Verbesserung der Incident-Response-Prozesse. Wir suchen eine hochmotivierte, analytische und lösungsorientierte Persönlichkeit, die über tiefgehende Erfahrung in Threat Intelligence, Incident Handling und der technischen Analyse von Cyberbedrohungen – insbesondere im Finanzsektor – verfügt.

Welche Aufgaben erwarten Dich?

- Leiten und koordinieren von Incident-Response-Maßnahmen, um Sicherheitsvorfälle effektiv einzudämmen und Risiken zu minimieren
- Erkennen und analysieren von Bedrohungen mit SIEM-Tools (z. B. Splunk), IDS/IPS und weiteren Sicherheitstechnologien zur frühzeitigen Identifikation von Angriffsmustern
- Untersuchen von Logs und Netzwerkverkehr, um Ursachen von Sicherheitsvorfällen zu ermitteln und Schwachstellen aufzudecken
- Eindämmen und beseitigen von Sicherheitsbedrohungen durch gezielte Gegenmaßnahmen und Absicherung betroffener Systeme
- Unterstützen der Wiederherstellung von Systemen und Diensten, um eine sichere Betriebsaufnahme nach einem Vorfall zu gewährleisten
- Durchführen von kontinuierlichem Threat Hunting und Analyse aktueller Bedrohungsvektoren zur proaktiven Stärkung der Sicherheitsarchitektur
- Erstellen detaillierter Vorfallsberichte, bewerten der Auswirkungen und definieren von Optimierungsmaßnahmen zur Stärkung der Sicherheitsstrategie
- Zusammenarbeiten mit Legal und Risk Management Teams, um Sicherheitsvorfälle effizient zu bearbeiten und regulatorische Anforderungen zu erfüllen
- Unterstützen und schulen des Teams, teilen von Wissen und weiterentwickeln der Security-Operations-Prozesse

- Pflegen und optimieren der Incident-Response-Prozesse, einschließlich Aktualisierung von Playbooks und Sicherheitsrichtlinien

Wen suchen wir?

- Mindestens 2 Jahre Berufserfahrung in einer SOC-Rolle mit Schwerpunkt auf Incident Response und Incident Reporting im Finanzdienstleistungssektor
- Abgeschlossenes Studium in Information Security, Informatik oder einem verwandten Bereich, alternativ eine vergleichbare Qualifikation (Zertifizierungen wie CISSP, CISM, CEH sind von Vorteil)
- Kenntnisse in der Nutzung von SIEM-Tools (insbesondere Splunk), IDS/IPS, Firewalls und weiteren Sicherheitstechnologien
- Erfahrung mit Cloud-Technologien, idealerweise in Azure, Google Cloud oder AWS
- Ausgeprägte Kommunikationsfähigkeiten, um komplexe technische Sachverhalte verständlich und präzise zu vermitteln – sowohl mündlich als auch schriftlich
- Starke analytische Fähigkeiten, um große Datenmengen zu untersuchen, Muster zu erkennen und sicherheitskritische Probleme zu lösen
- Teamfähigkeit und Erfahrung in der Zusammenarbeit mit Security- und Netzwerkoperationsteams zur effektiven Abwehr und Bewältigung von Bedrohungen
- Branchenkenntnisse, idealerweise Erfahrung in Finanzinstituten oder vergleichbaren Organisationen

Was wir Dir bieten:

- Flexible Arbeitszeiten innerhalb einer 39-Stunden-Woche
- 30 Tage Jahresurlaub
- Vielseitiges und spannendes Aufgabengebiet in einem modernen und dynamischen Umfeld sowie ein wertschätzendes Betriebsklima
- Gezielte Förderung durch interne und externe Schulungs- und Entwicklungsprogramme
- Berenberg-Patensystem für ein strukturiertes und reibungsloses Onboarding
- Vielfältige Zuschüsse (z.B. Deutschlandticket, JobRad, vermögenswirksame Leistungen, betrieblich mitfinanzierte Altersvorsorge, Pluxee-Checks)
- Zusätzliche Leistungen wie Familienservice, Arbeitszeitkonto (z. B. für Sabbaticals), betriebliche Sozialleistungen, Gesundheits- und Sportprogramme

Bewirb‘ Dich jetzt online und werde Teil des Teams – **wir freuen uns auf Deine Bewerbung!**