

SCHWARZ



› Cyber Security Engineer ^{m/w/d}

Die Schwarz IT KG ist als zentraler IT-Dienstleister für Auswahl, Bereitstellung und Betrieb sowie Weiterentwicklung von IT-Infrastrukturen, IT-Plattformen und Business-Anwendungen zuständig. Damit erbringt die Schwarz IT sowohl für Kaufland und Lidl als auch für die Schwarz Dienstleistung KG IT-Dienstleistungen. Um die Fachbereiche durch IT-Lösungen optimal bei deren Geschäftsprozessen zu unterstützen, nimmt die Schwarz IT Anforderungen der Fachbereiche in Beratungsgesprächen auf und erarbeitet gemeinsam mit diesen professionelle und leistungsfähige IT-Lösungen.

Einsatzbereich: IT - Infrastruktur // Ort: Neckarsulm (hybrid) // Arbeitsmodell: Vollzeit

Deine Aufgaben

- Du bist mitverantwortlich für die Weiterentwicklung und Dokumentation unserer Detection Use Cases
- Du hilfst die Sicht des Cyber Defense Centers auf IT Prozesse im Unternehmen mit sinnvollen Logging Policies und SIEM Suchen zu erweitern
- Du erkennst aktiv Lücken in unserer Detection Coverage und hilfst diese zu schließen
- Du überprüfst bestehende Use Cases auf deren Sinnhaftigkeit und Aktualität
- Du hältst die allgemeine Bedrohungslage im Blick und ermittelst Handlungsempfehlungen
- Du entwickelst zusammen mit unseren Incident Respondern Handlungsschritte zur Bearbeitung von Alarmen
- Du berätst ggf. interne Projekte im Hinblick auf sicherheitstechnische Fragestellungen

Dein Profil

- Du hast eine Berufsausbildung im IT-Bereich (bevorzugt mit Fokus auf Security) mit entsprechender Weiterbildung oder ein Studium der Fachrichtung Informatik erfolgreich abgeschlossen
- Du verfügst über Kenntnisse relevanter Standards und Frameworks im Bereich des Detection Engineering wie z.B. das MITRE ATT&CK Framework, SIGMA, YARA und Snort
- Du hast Erfahrungen in der Entwicklung von Alarmen für SIEM Systeme und Security Software wie EDR, IDS, usw.
- Du verstehst wie Incident Response Prozesse funktionieren und kannst auf Basis dessen Handlungsschritte für die Bearbeitung von Alarmen definieren
- Du zeichnest dich durch hohe analytische und kommunikative Fähigkeiten aus, arbeitest eigenverantwortlich und bist teamfähig
- Du trittst überzeugend auf und kommunizierst dabei sicher in Deutsch und Englisch

Unser Angebot

Team: Werde Teil der wachsenden "Research, Automation und Development" Sparte des Cyber Defense Centers und bewege in einem motivierten Team gemeinsam großes

Weiterbildung: Dich erwarten individuelle Angebote zur persönlichen und fachlichen Weiterentwicklung

Einarbeitung: Wir arbeiten dich intensiv in deine Themen ein

Vielfalt: Bei uns hast du die Chance neue Themen zu besetzen sowie eigene Ideen und Kompetenzen einzubringen

Sicherheit: Du profitierst von einem sicheren Arbeitsplatz in einem dynamischen Handelsunternehmen

Wir freuen uns auf deine Bewerbung!

Schwarz Dienstleistung KG | Maraike Schnura | Referenz-Nr. 38995
Stiftsbergstraße 1 · 74172 Neckarsulm
www.it.schwarz

› JOBS.SCHWARZ