



Teilzeit & viel remote: Palo Alto Cortex XSOAR Experte (w/m/d)

Für unseren Kunden suchen wir einen Palo Alto Cortex XSOAR Experten (w/m/d)

Rahmendaten:

Start: asap

Laufzeit: 31.12.2026++

Auslastung: 1-2 Tage/Woche (zu Beginn eher mehr und im Laufe des Projektes reduziert es sich vsl. auf 1 Tag/Woche)

Einsatzort: Berlin, überwiegend remote

Aufgaben & Skills:

- Grundlegendes Verständnis von SOC Prozessen (Incident Response, Vulnerability Management, IOC Enrichment)

Kenntnisse in der:

- Administration von Cortex XSOAR als SaaS
- Anbindung von Systemen an Cortex XSOAR über Standardintegrationen und Rest-API
- Erfahrungen im Umgang mit OAuth2, JSON, HTTP, Pagination, Rate Limits, Fehlerbehandlung
- Erstellung von Custom Integration
- Entwicklung bzw. in der Automatisierung mit Python
- Entwicklung von Playbooks

Best Practices zur Abbildung von SOC-Prozessen, insbesondere:

- Aufbau und Kombination von Sub-Playbooks (Modulare Playbooks)
- Berechnung von KPIs und Aufbau von Playbooks
- Automatisierten Zuweisung von Playbooks

Nice-to-have:

- Anwendung von Splunk-SPL und Microsoft KQL
 - Kenntnisse von AWS, Kubernetes und Terraform
-