

remote – Infrastructure Engineer Splunk SCCC (m/w/d)

Für unseren Kunden suchen wir einen „Infrastructure Engineer“ (m/w/d) mit Splunk SCCC Zertifizierung.
Ohne diese Zertifizierung kann die Bewerbung nicht in Betracht gezogen werden.

Rahmenparameter
Start: 01.01.2027
Laufzeit: 3 Jahre, bis 31.12.2029
Auslastung: insgesamt 660 PT
Einsatzort: remote
Projektsprache: Deutsch
Besonderheit: Splunk SCCC Zertifizierung ist verpflichtend

Projektbeschreibung
Für einen Auftraggeber mit KRITIS-relevanter IT-Infrastruktur suchen wir einen erfahrenen Infrastructure Engineer zur Unterstützung ein bestehenden Splunk-Lösung für Logging und Angriffserkennung.
Im Projekt wurden Werkzeuge für Systeme zur Angriffserkennung (SzA) umgesetzt, die eine frühzeitige Erkennung und Abwehr potenziell Bedrohungen unterstützen. Im Mittelpunkt stehen die Automatisierung des Onboardings neuer Kunden, die Optimierung des Entwicklung sowie die Weiterentwicklung der Architektur und des GitLab-basierten Entwicklungs-Lifecycles.
Ein weiteres Projektziel ist, doppelte Aufwände beim Einlesen von Daten zu vermeiden.
Als Senior Infrastructure Engineer übernehmen Sie die technische Umsetzung und Weiterentwicklung von Komponenten der Splunk-Infra Sie achten dabei auf die Compliance- und Security-Vorgaben im KRITIS-Umfeld und arbeiten eigenständig sowie selbstorganisiert.

Aufgaben
- Splunk Enterprise im SIEM-, SOC- oder KRITIS-Umfeld betreiben und weiterentwickeln.
- Splunk ITSI konfigurieren und betreiben sowie Splunk-Multisite-Cluster unterstützen.
- GitLab-Pipelines im Zusammenspiel mit Splunk-Konfigurationen und Splunk-Apps entwickeln und pflegen.
- Technische Komponenten in Applikationen programmieren, implementieren und anpassen, einschließlich zugehöriger Schnittstellen, M Datenbanken; dabei die Standards, Entwicklungsumgebungen und Programmierrichtlinien des Auftraggebers einhalten.
- Lösungsarchitekturen nach etablierten Architekturpraktiken, Mustern und Frameworks dokumentieren und kommunizieren.
- Den Development Lifecycle mit GitLab und Versionsverwaltung unterstützen.
- Das automatisierte Onboarding neuer Kunden und die Optimierung des Entwicklungsprozesses vorantreiben.
- Compliance- und Sicherheitsvorgaben für die Splunk-Infrastruktur sowie geltende IT-Richtlinien und -Verfahren berücksichtigen.

Erfahrungen & Kenntnisse
Zwingend erforderlich
- Mehr als 5 Jahre Erfahrung im Betrieb von Splunk Enterprise in einem SIEM-, SOC- oder KRITIS-Umfeld.
- Mehr als 5 Jahre Erfahrung in Konfiguration und Betrieb von Splunk ITSI.
- Mehr als 5 Jahre Erfahrung mit GitLab-Pipelines im Zusammenspiel mit Splunk-Konfigurationen und Splunk-Apps.
- Mehr als 5 Jahre Erfahrung im Betrieb von Splunk-Multisite-Clustern.
- Gültiges Zertifikat **Splunk Core Certified Consultant**.
- Deutschkenntnisse auf annähernd muttersprachlichem Niveau (C2).

Wünschenswert

- Mehr als 5 Jahre Erfahrung in der Administration von Linux-Systemen.
- Mehr als 3 Jahre Erfahrung mit dem Splunk AI Toolkit.
- Drei Referenzen zur Steuerung von Projekten und zur Sicherstellung ihrer Projektziele.