Senior Elastic Stack Content Engineer (m/w/d)

Kennziffer: 992026007BE | Standort: Berlin, Dresden, Frankfurt, Hamburg, Leinfelden-Echterdingen, München, Nürnberg, Senftenberg, Wolfsburg, Zwickau

operational services (OS) ist einer der führenden ICT Service Provider im deutschen Markt und gilt als Backbone der Digitalisierung für Branchen wie Public, Automotive, Logistic, Finance und Healthcare.

Als agile Einheit der Telekom Gruppe beschleunigt OS die digitale Transformation kritischer Infrastrukturen nachhaltig. Mit über 1.000 hochqualifizierten Mitarbeitenden entwickelt und betreibt OS modernste Informationssysteme, managt Private & Public Cloud-Plattformen und sichert den langfristigen 24/7-Systemsupport sowie die Verfügbarkeit kritischer Betriebsprozesse.

DER JOB

- Planung, Projektierung und Durchführung von Implementierungen, Inbetriebnahmen mit Schwerpunkt auf Security, SIEM und Observability
- Analyse und Behebung von Problemen sowie Fehlerdiagnose in von Detektionsszenarien in SIEM-Systemen (Content Engineering)

- Gestaltung, Einführung und Optimierung von Detektionsszenarien in Security-Analytics-Systemen (wie z.B. Elastic SIEM)
- Leitung komplexer Aufträge und Projekte, inklusive Ressourcenplanung, Steuerung und Koordination der Zusammenarbeit mit dem SOC-Provider , Steuerung eines Projektteams von Content Engineers, sowie Sicherstellung technischer und zeitlicher Zielerreichung
- Definition, Initiierung und Kontrolle von Maßnahmen zur Gewährleistung von Service Levels, Security-Standards und Kundenzufriedenheit
- Ausarbeitung strategischer Konzepte für die Spezifikation und Entwicklung umfangreicher Lösungen und Pflichtenhefte insbesondere im Bereich Detektionsszenarien und Schutzziele sowie ganzheitliche Erkennungskonzepte
- Technische Unterstützung oder Leitung bei Akquise-Prozessen, inklusive Machbarkeitsanalysen
- Aktive Mitwirkung bei der Weiterentwicklung des Service- und Lösungsportfolios sowie der beim Kunden implementierten Security-Lösung, insbesondere im Bereich Elastic Security, Observability, und Content Engineering

YOU

- Master- oder Diplomabschluss in Informatik, IT-Sicherheit oder vergleichbarer Qualifikation – alternativ entsprechende, nachweisbare Berufserfahrung
- Mindestens sieben Jahre Berufserfahrung, davon mindestens fünf Jahre in der IT-Security, in den Bereichen Threat Detection, Content Engineering, SOC o.Ä.
- Erfahrung mit SIEM- und/oder XDR-Systemen (Palo Alto, Elastic, SPLUNK, etc.)
- Sehr stark ausgeprägtes kundenorientiertes und unternehmerisches Denken, auch in der Zusammenarbeit mit Management- und C-Level-Ebenen
- Hohe analytische und konzeptionelle Kompetenz, insbesondere bei Angriffstechniken und Verteidigungsmaßnahmen im Cybersecurity-Umfeld
- Zertifizierungen im Bereich IT-Security oder Elastic von Vorteil
- Sehr gute Deutsch- und Englisch- Kenntnisse in Wort und Schrift

UNSERE BENEFITS

- Deutschlandweites mobiles Arbeiten
- Attraktives Gehaltspaket mit Erfolgsbeteiligung
- 37 Stunden/Woche mit Arbeitszeitkonten
- Arbeitgeberfinanzierte Weiterbildungen und Zertifizierungen

Ein weiteres Plus sind außerdem unser Fahrradleasing, 30 Tage Urlaub, subventioniertes Deutschlandticket, arbeitgeberfinanzierte Altersvorsorge, vermögenswirksame Leistungen, Gruppenunfallversicherung für Arbeit und Freizeit sowie Mitarbeiterkonditionen für viele Produkte des Konzerns Deutsche Telekom.

Jetzt Bewerben

Ihre Ansprechpersonen
OS HR-Team
FMB-Bewerbung@o-s.de