Senior Cyber Defence Consultant

Stellenbeschreibung

Unser Motto ist "Cyber Security from Germany for the World". Seit 2021 sind wir auf die Erkennung, Analyse und Abwehr von Cyberangriffen spezialisiert. Wir suchen immer hochmotivierte Kollegen zur Verstärkung unseres Teams! Als **Senior Cyber Defence Consultant** begleitest du unsere Kunden bei der Konzeption, dem Design, der Implementierung und dem Betrieb von Security Operation Centern (SOC), Cyber Defense Centern bzw. Security Information & Event Management (SIEM) Lösungen sowie vielen weiteren interessanten Themen im Bereich der Cybersicherheit. Dein Verantwortungsbereich umfasst unter anderem:

- Konzeption, Design und Implementierung von SIEM-Lösungen.
- Entwicklung, Implementierung und Optimierung von SIEM Use-Cases.
- Erkennung, Analyse, Bewertung und Handling von Security Incidents.
- Schwachstellen Management bei unseren Kunden.
- EDR Management, Implementierung und Analyse.
- Threat Intelligence Informationen sammeln, bewerten und bereitstellen.
- Aufnahme und Analyse der Ziele und Rahmenbedingungen beim Aufbau eines SOC/CDC bzw. einer SIEM-Lösung.
- Entwicklung von Betriebs-, Rollen-/ Rechte-Konzepten sowie SOC-/CDC-Prozessen.
- Incident Response Tätigkeiten bei Kunden.
- Unterstützung und Durchführung von IT-Forensik aufgaben.
- Mentor von Junior Cyber Defense Consultants (SIEM) und Cyber Defense Consultants (SIEM).
- Projekt- und Teamleitung bei größeren Kundenprojekten.

Anforderungsprofil

Das solltest du mitbringen:

- Mindestens 3 Jahre Berufserfahrung im Aufbau und Betrieb von Security Operation Centern (SOC bzw. im Bereich Security Information & Event Management (SIEM).
- Tiefgreifende Kenntnisse in den Bereichen IT Security, IT Operations, IP Networks und gängigen Betriebssystemen (Windows, Unix, Linux).
- Verständnis von gängigen Security Standards (PCI DSS, IT Grundschutz, ISO 2700x…).
- Fähigkeit, Kunden bei der Konzeptionierung, dem Design, der Implementierung und dem Betrieb von Security Operation Centern (SOC), Cyber Defense Centern bzw. Security Information & Event Management (SIEM) Lösungen zu führen.
- Analytische Denkweise.
- Hohe Kunden- und Serviceorientierung.
- Unternehmerisches Denken und Handeln.
- Bereitschaft, im Team Verantwortung zu übernehmen.
- Reisebereitschaft.
- Sehr gute Deutsch- und Englischkenntnisse in Wort und Schrift.

Tiefgreifende Erfahrung mit mindestens einem der folgenden Produkten:

- Splunk.
- Elasticsearch.
- ArcSight.
- QRadar.
- Microsoft Sentinel.

- Google Chronicle.

Gern gesehene Zertifizierungen:

- CISSP.
- CISM/CISA.
- GIAC (GSEC, GCIA, GCIH, GCIM, GCFA).

Das bieten wir dir:

- 30 Tage Erholungsurlaub pro Jahr.
- Digitale Arbeitsausstattung inkl. Laptop und Smartphone.
- Teilnahme an Firmen-Events.
- Mindestens 10 Tage Weiterbildung pro Jahr.
- Standortunabhängiges Arbeiten Europa/Weltweit*.
- Flexible Arbeitszeiten*.
- Individuelle Firmenwagenregelung.
- Research Days.
- Ein auf dich zugeschnittenes On-Boarding und Mentoring.

*in Absprache mit Kollegen und Kunden