ЛОКАЦІЯ: м. Бухарест, Румунія

Глобальний аналітик з кібербезпеки та комплаєнсу /

Global Cyber Security & Compliance Analyst

Глобальний аналітик з кібербезпеки та комплаєнсу відповідає за підтримку та впровадження необхідних заходів з безпеки і забезпечує, щоб усі ключові бізнес-додатки дотримувалися встановлених правил щодо кібербезпеки та внутрішніх і зовнішніх вимог аудиту GITC (загального IT контролю)

Обов'язки:

•Надавати постійну підтримку та забезпечувати роботу існуючих платформ кібербезпеки та інструментів звітності на основі визначених політик безпеки, включаючи:

○ Платформа обізнаності про кібербезпеку
○ Управління щодо здійснених порушенн у відповідності до комплаєнсу
○ Надання дозволів доступу для користувачів і конроль за тими, хто приєднався, перейшов до інших підрозділів або покинув компанію
○ Надання спеціальних доступів користувачам (доступ з привілеями)
○ Політика щодо паролів
○ Дотримання політик комплаєнсу (операційні системи, бази даних, сторонні програми)
○ Управління змінами

•Підтримувати існуючі та впроваджувати нові заходи щодо контролю кібербезпеки на основі зовнішніх рекомендацій з аудиту GITC, нових і існуючих політик і процедур
•Надавати допомогу у виправленні усіх виявлених недосконалостей
•Формувати звіти з конкретних випадків щодо розслідування порушень з інформаційної безпеки
•Співпрацювати з командою SAP Basis Security & Authorization для виявлення порушень і проведення розслідувань
•Формувати і надавати необхідні показники, а також щомісячну, квартальну та річну звітність з дотримання вимог кібер безпеки
•Брати участь в операціях з ліквідації наслідків стихійних лих, у разі необхідності
•Проводити резервне копіювання застосунків аудиту та виконує аварійно-відновлювальні дії
•Співпрацювати щодо проведення зовнішнього аудиту GITC

•Підтримувати глобальну структуру політики кібербезпеки та інформаційної безпеки, обізнаний щодо найкращих світових практик та технологічних тенденцій у цій галузі

•Брати участь у процесі закупівлі

Базові вимоги (освіта, необхідний досвід роботи, знання мов):

•Відповідна освіта у коледжі або університеті в галузі кібербезпеки, інформатики, інформаційних технологій, суміжних чи еквівалентних галузях

•Мінімум 5 років досвіду в управління бізнес-додатками та в підрозділах з IT-підтримки

•Загальне розуміння галузі інформаційної безпеки, включаючи знання щодо політик і стандартів, оцінки ризиків і контролю, нормативних вимог і управління доступами користувачів, а також знання щодо вимог комплаєнсу, надійності технологій, управління ризиками і контролю за показниками і захистом даних.

•Вільне володіння англійською (письма та усна)

Необхідні знання (технічні знання, які необхідні для посади):

•IT Audit Control & ITGC

•Професійні знання щодо доменів з інформаційної безпеки

•Обізнаність щодо безпеки

Необхідні навички:

•Розвинута здатність вирішувати проблеми та знаходити їх першопричини

•Ефективна письмова і усна комунікація

•Start-up мислення

•Досвід роботи з SAP ERP

•Відповідні сертифікати безпеки, такі як CISSP, SANS, CISM, CISA будуть перевагою

Про компанію: Carmeuse – це світовий лідер у виробництві вапна, висококальцієвого вапняку та доломітового каменю. Продукція Carmeuse необхідна для виробників енергії, екологічних послуг, будівництва та виробництва. Компанія веде бізнес у 22 країнах світу, має понад 90 виробничих потужностей, розташованих майже на кожному континенті, в компанії понад 4500 співробітників. Головною цінністю компанії є люди.

Сайт компанії: www.carmeuse.com

Якщо вас зацікавала дана позиція: надсилайте CV на адресу**:** **jobsforukraine@carmeuse.com**