PwCコンサルティング合同会社

セキュリティエンジニア【TRC-CRS】・福岡

セキュリティエンジニア【TRC-CRS】/福岡:

Open/Closed Open

セクションを非表示 - DetailsDetails

Specific Information (External):

【職務内容】

PwCではグローバルで専門のチームを設け、脅威アクターやTTPsなどの脅威情報を含む、サイバーインテリジェンス情報を生成しています。 セキュリティエンジニアには、「サイバーインテリジェンスの作成」と「サイバーインテリジェンスを活用したサービスの提供」を担っていただきます。

セキュリティエンジニアが担当する主なプロジェクトは下記職務内容のとおりです。 PwCは、コンサルタントとエンジニアのコラボレーションが強みの１つであり、プロジェクトにおいても混成チームで互いの専門スキルを連動させ、社会課題の解決に取り組んでいます。

セキュリティエンジニアには、高い技術力と新しい技術に積極的に取り組んでいくチャレンジ精神を期待しています。

【主な職務内容】

■クライアントのシステムに対するプラットフォーム脆弱性診断

■ウェブアプリケーションの脆弱性診断

■クライアントの環境に対する内部及び外部のペネトレーションテスト ■サイバーインテリジェンスをベースとしたセキュリティアセスメント ■最新のセキュリティ脅威やマルウェア、対策技術に関する調査 ■サイバーインテリジェンスを活用したSIEMサービスの開発、ルール作成、導入およびクライアントシステムの監視・分析 ■クライアントのセキュリティインシデント発生時の技術的なサポート

■デジタルフォレンジック技術を用いたインシデントレスポンス

■ホワイトハッカー/手動またはツールを用いてお客様のシステムへ侵入し、セキュリティ対策やセキュリティ業務の妥当性を評価するレッドチーム演習や脅威ベースのペネトレーションテスト（TLPT）等の業務を実施

#LI-DNI:

Work Location(External) 福岡

セクションを非表示 - Application conditionApplication condition

Core Requirements(External):

■クライアントのシステムに対するプラットフォーム脆弱性診断/ウェブアプリケーションの脆弱性診断/クライアントの環境に対する内部及び外部のペネトレーションテスト

【必要スキル】

・Webアプリケーション診断、ネットワーク診断、スマートフォンアプリ診断の実務経験

・プログラミング経験（言語問わず）

・OS、ネットワークに関する知識

・ビジネスライティング、ビジネスコミュニケーションスキル

・自分自身の専門性を常に高める姿勢

・OffSec Certified Professional(OSCP)（Manager以上）

【歓迎するスキル】

・新しい脆弱性の発見／検証経験

・英語力（TOEIC700点以上相当）

・Offensiveに関する認定・認証資格

例）

OffSec Experienced Pentester (OSEP) HTB Certified Penetration Testing Specialist (HTB CPTS) Certified Red Team Professional (CRTP)

OffSec Web Expert (OSWE)

Certified Red Team Operator (CRTO) Offensive Security Exploitation Expert (OSEE) Burp Suite Certified Practitioner (BSCP) Certified Azure Red Team Professional (CARTP)

■サイバーインテリジェンスをベースとしたセキュリティアセスメント

【必要スキル】

・各種フレームワークを利用したセキュリティアセスメント経験

・MITER ATT&CKに関する知識

・ビジネスライティング、ビジネスコミュニケーションスキル

・自分自身の専門性を常に高める姿勢

【歓迎するスキル】

・脅威インテリジェンス分析、パープルチーミングの経験

・英語力（TOEIC700点以上相当）

■最新のセキュリティ脅威やマルウェア、対策技術に関する調査

【必要スキル】

・官公庁等の調査研究案件の実務経験

・プログラミング経験（言語問わず）

・TCP/IPネットワーク関連のスキルや構築・運用経験

・OS、アプリケーション、デバイスに関する知識

・各種OSに関する低レイヤの知識

・各種プログラミングに関する知識

・ビジネスライティング、ビジネスコミュニケーションスキル

・自分自身の専門性を常に高める姿勢

【歓迎するスキル】

・書籍、オンラインメディア等での執筆経験

・セミナー、研究会、学会等での発表、講演経験

・マルウェア解析業務経験

・ドライバ、組込機器開発経験

・英語力（TOEIC700点以上相当）

■サイバーインテリジェンスを活用したSIEMサービスの開発、ルール作成、導入およびクライアントシステムの監視・分析 クライアントのセキュリティインシデント発生時の技術的なサポート

【必要スキル】

・a,b,cのいずれかの経験　　a.セキュリティ運用監視またはネットワーク運用監視の導入、運用設計、運用、運用改善経験　　b.EDR あるいはファストフォレンジックツールを利用したインシデント調査の経験

c.スレッドハンティングの実務経験

・日本語でのビジネスライティング、ビジネスコミュニケーションスキル

・自分自身の専門性を常に高める姿勢

【歓迎するスキル】

・SIEM/SOAR の導入、利用あるいは運用経験（ルール開発含む）

・サイバー攻撃手法や対策技術に関する知識、国内外のセキュリティに関する全般的な情報収集能力

・Cloud IAM、SSO、OAuth、2段階認証等のクラウドセキュリティーに携わった経験

・各種サーバ（Web, Mail, DNS, Proxy等）、セキュリティ機器（FW, IDS, IPS, UTM等）に関する知識

・IDS/IPSのカスタマムシグネチャの作成経験

・マルウェア解析業務経験

・ドライバ、組込機器開発経験

・英語力（TOEIC700点以上相当）

■デジタルフォレンジック技術を用いたインシデントレスポンス/クライアントのセキュリティインシデント発生時の技術的なサポート

【必要スキル】

・サイバー攻撃に関する技術的なインシデント対応

・自分自身の専門性を常に高める姿勢

・ビジネスライティング、ビジネスコミュニケーションスキル

【歓迎するスキル】

・EnCase Certified Examiner (EnCE) 認定

・AccessData Certified Examiner (ACE) 認定

・英語力（TOEIC700点以上相当）

Treatment:

セクションを非表示 - RemarksRemarks

bloom