

|                 |   |
|-----------------|---|
| No.             | SS201802  |
| 募集ポスト           | インシデントレスポンス技術者  |
| 採用部署            | ソリューションサービス部  |
| 業務内容            | <p>セキュリティインシデントの発生が疑われるお客様に対し、インシデントレスポンスを実施します。ネットワークフォレンジックやWindows端末ログ分析、マルウェア解析を実施し、すみやかに感染経路/被害範囲/漏えい情報の特定を行います。</p> <p>高度なスキルを身につけるため、日々下記の様なりサーチ業務を行います。</p> <ul style="list-style-type: none"> <li>マルウェア種別特定、被害範囲特定を行う能力を身につけるための最新のマルウェア挙動についての情報収集</li> <li>ネット上で公開されている各種悪性ツールについての情報収集および検証</li> <li>独自の調査ツールや調査を効率化するためのツール等の作成</li> <li>新しいエンドポイント製品やベンダの脅威情報提供サービスの検証</li> </ul> <p>■求める人物像</p> <ul style="list-style-type: none"> <li>情報セキュリティやハッキング技術に強い興味がある方</li> <li>新しい技術に興味を持ち、それを積極的に調査、活用しようとする意欲のある方</li> <li>問題や課題を論理的に分析し、解決策を考えられる思考力を有する方</li> </ul> |
| 必要な経験・能力・資格     | <ul style="list-style-type: none"> <li>TCP/IP、Linux、Windowsに関する知識</li> <li>サーバーの構築経験3年以上、または運用経験5年以上</li> <li>基礎的なプログラミング経験</li> <li>情報セキュリティに関する強い興味</li> </ul>  |
| あると望ましい経験・能力・資格 | <ul style="list-style-type: none"> <li>情報セキュリティに関する業務経験</li> <li>コンピュータフォレンジックスに関する基礎的な知識</li> <li>コンピュータフォレンジックスに関する業務経験</li> <li>プロジェクトマネジメントの経験</li> </ul>   |
| 応募資格            | 当該職務、及びそれに準じる職務の実務経験を有する方   |
| 勤務地             | 東京23区内  |
| 募集人数            | 若干名   |
| 雇用形態            | 正社員<br>※試用期間 4か月  |
| 勤務時間            | 9:00~17:30  |
| 休日、休暇           | 週休2日制(土、日) 祝日、年次有給休暇、夏季休暇、年末年始休暇 他  |
| 給与・手当           | 役割給(職務内容に応じて決定します)及び業績給(成果達成度合いに応じて支給します)<br>その他:通勤費(全額支給)、時間外手当、休日手当、深夜手当、食事手当 他   |
| 福利厚生            | 健康保険、厚生年金、雇用保険、労災保険、企業年金基金 他  |
| 退職金             | 無し  |