**職　務　経　歴　書**

　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　20xx年xx月xx日現在

　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　氏名　○○ ○○

**■職務要約**

・20xxx年xx月～現在　　　　　株式会社△△△△　情報システム部門にてセキュリティ専任担当

　　　　　　　　　　　　　　　 20xx年xx月からセキュリティ部

・20xx年xx月～20xxx年xx月　株式会社◆◆◆◆にてセキュリティエンジニアとしてSOC業務を推進

・20xx年xx月～20xxx年xx月　○○○○株式会社にてネットワークエンジニア

**■職務経歴**

　□20xxx年xx月～現在　株式会社△△△△

|  |  |  |  |
| --- | --- | --- | --- |
| 期間 | プロジェクト内容 | 環境／ツール | 役割 |
| 現在  ～  20xx年x月 | セキュリティ部　全体統括  ■概要  CISO補佐として、セキュリティ施策全般の企画・運営  ■担当業務  セキュリティ企画・推進  SOC・CSIRT統括  経営会議資料作成  ユーザー部門折衝・調整 |  | 【役割】  課長  メンバー：6名  【担当】  CISO補佐  CSIRT運営  人員管理  予算管理 |
| 20xx年x月  ～  20xx年x月 | CSIRT部署の起ち上げ  ■概要  それまでは、インシデント発生時のみの組織としてCSIRTを推進していたが、インシデントの発生件数と事前対策の必要性から組織を起ち上げることになった。  ■担当業務  リーダーとして、SOC業務と並行してCSIRT部署の起ち上げを推進。  ※ユーザー部門の連携に合わせて各部門から人員を出してもらうことに苦慮。メリットを感じてももらえないとユーザー部門の協力を得られないと痛感。 |  | 【役割】  リーダー  メンバー：4名  CSIRT：15名  【担当】  関係者調整 |
| 20xx年x月  ～  20xx年x月 | セキュリティ部SOC担当  ■担当業務  外注からの引継ぎがほぼ完了したタイミングでセキュリティ部門をシステム部門から切り出し。サブリーダーとして、インシデント管理、ユーザー部門窓口を担当。  ※初めてサブリーダーで管理業務が増えましたが、メンバーとの対話を増加させて意思疎通を図る。 | 拠点数14  クライアント数1100社 | 【役割】  サブリーダー  メンバー：2名  【担当】  インシデント管理  ユーザー部門窓口 |
| 20xx年x月  ～  20xx年x月 | 情報システム部SOC担当  ■担当業務  新規に立ち上がったSOCのメンバーとして、365日24時間の監視業務に従事。外注していたベンダーから業務移管を受けながら推進。 | 拠点数10  クライアント数800社 | 【役割】  メンバー  要員数：○名 |

□20xx年xx月～20xx年xx月　株式会社◆◆◆◆

|  |  |  |  |
| --- | --- | --- | --- |
| 期間 | プロジェクト内容 | 環境／ツール | 役割 |
| 20xx年x月  ～  20xx年x月 | 金融機関向けSOC業務  ■担当業務  自社センターに常駐し、クライアント3社分の監視、運用を担当。  　・日々のSOC業務において、インシデント状況・影響調査  ・クライアント情報システム部門報告  ・月2回　クライアントCSIRT報告会参加 | 拠点数80  クライアント数1000社  【使用ツール】 **SIEM（**Splunk） SOAR（McAfee） | 【役割】  メンバー  要員数：○名 |

□20xx年xx月～20xx年xx月　○○○○株式会社

|  |  |  |  |
| --- | --- | --- | --- |
| 期間 | プロジェクト内容 | 環境／ツール | 役割 |
| 20xx年x月  ～  200x年x月 | 金融機関向け大規模ネットワークの運用・保守、追加構築  ■担当業務  データセンターに常駐し、金融機関2社分のネットワークを担当。  　・日々の実運用業務、1次切り分けだけではなくクライアントに応じて2次対応まで実施。  ・クライアントに対しての改善提案の実施（折衝経験）を行う。  ・追加構築案件では、詳細設計、構築も遂行。 | NW機器（50台）  【ルーター】  CiscoISR2800（15）  【スイッチ】 Catalyst4000（1）  【運用ツール】  JP1 | 【役割】  メンバー  要員数：○名 |

　※20xx年xx月～20xx年xx月　通信キャリア向け、金融機関向けネットワークを中心に複数の運用業務案件に参画しました。

**■活かせる経験・知識・技術**

サイバーセキュリティ領域について幅広い知識

自社システムに関連する領域を中心に、脆弱性情報、インシデント事例、攻撃形態について、IPAや各ベンダーからの発信や同業勉強会などの様々なソースから収集し、日々体系的に整理しています。

社内説明・折衝能力

　成果が見えにくいからこそ、自社状況、社会情勢、各施策のメリット・デメリットについて、経営陣およびユーザー部門責任者に継続して説明。「インシデントが発生していない」状態を続けるための必要コストとリターンについて数値化して折衝しています。

メンバーマネジメント

メンバーにも日々の知識拡充を求めています。ビジネスの遂行とのセキュリティのバランスを意識させるために、ユーザーの業務理解と関係性構築を優先させています。併せて部門全体のコスト・スコープ・スケジュール・人員管理まで行っております。

　技術的スキル

　・セキュリティ：CSIRT構築、SOC運用、脆弱性調査（WEB、NW）、マルウェア対策、デジタルフォレンジック

・OS：Linux（RedHat、CentOS）Windows2019・2016・2012・2008

・クラウド：AWS、Azure

・Webサーバー：Apache、WebLogic、WebSphere

・メールサーバー：sendmail、qmail

・NW機器：Cisco（CatalystXXXX、CiscoXXXX）、Juniper

・プロトコル：TCP/IP、OSPF、BGP

**■資格**

・安全確保支援士（20xx年xx月）

・CCNP（20xx年xx月）（更新切れ）

・LPIC　Level１（20xx年xx月）

・応用情報技術者（20xx年xx月）

・TOEIC 650点（20xx年xx月）

**■自己PR（スキル、社内、顧客）**

責任感と良識を持って取り組みます

セキュリティ業務はものづくりと違って成果が見えにくく、ビジネスサイドから見るとマイナスの要素が大きいため、経営陣、ユーザー部門との信頼がなければ進みません。そのために、責任感と良識を持って進めるよう心がけています。

エンジニア経験を活かしています

　これまでNWエンジニア、SOCエンジニアとして現場を経験してきたことから、机上では想定しえないインシデントにも冷静に対応できます。ベンダーとの調整においても、現実的な進め方が可能です。

ビジネス推進を常に意識しています

セキュリティ施策について、ビジネス推進においてのリスクとリターンを明確にし、メリット・デメリットをわかりやすく、経営陣やユーザー部門に提示ができます。

セキュリティ知識の習得を継続しています

日々変化するセキュリティ知識拡充のため、ベンダーHPや専門家ブログは毎日確認。同業界ISACにも参加し、情報連携を継続しております。5G、IoTの普及や自社ビジネスの進む方向を見据えた「先回りの知識習得」を行えます。

以上