公開資料

日本セキュリティオペレーション事業者協議会 ISOG-J

セキュリティ対応組織（SOC/CSIRT）の教科書 ハンドブック 別紙

セキュリティ対応のサービス一覧

A　CDC/CSCの戦略マネジメント

何をどう守っていくのかセキュリティチームの活動内容を決め、具体的な取り組みを仕切っていくお仕事

A-1	リスクマネジメント	セキュリティ対応全体の活動についての方針を管理し、推進する
A-2	リスクアセスメント	組織の資産や脅威、セキュリティ対策の観点から、組織のリスクレベル把握をする
A-3	ポリシーの企画立案	具体的なセキュリティポリシーの定義や、ガイドラインの作成などの活動を支援する
A-4	ポリシーの管理	ポリシーや組織の規定を定期的に見直したり新しいものに準拠をする
A-5	事業継続性	事業継続計画の実現や実行を支援する
A-6	事業影響度分析	被害がどの程度になるか金額だけでなく信頼損失や風評被害も分析する
A-7	リソース管理	セキュリティ対応に必要な予算、人員、システムを計画し、配分する
A-8	セキュリティアーキテクチャ設計	ビジネスにセキュリティをどう組み込むかを設計する
A-9	トリアージ基準管理	セキュリティ事故が起こってしまったときの対応優先度を決める
A-10	対応策選定	セキュリティ事故が起こってしまったときの対処方針を決める
A-11	品質管理	運用や対応において問題がなかったか把握し、改善する
A-12	セキュリティ監査	定期的な監査や効果測定を行う
A-13	認証	組織が必要な規格や認証に向けた支援をする

B　即時分析

セキュリティ製品のログを常時監視して、ウイルスの感染がないかなどを分析し、インシデントを発見するお仕事

B-1	リアルタイム基本分析	ネットワークやサーバーのログを分析する
B-2	イベントデータ保管	各種収集したログやデータを一元的に保管する
B-3	通知・警告	見つけた情報を各種関係するところへ通知をする
B-4	レポート問い合わせ対応	報告した内容について問い合わせ対応する

C　深掘分析

発見されたインシデントにおいて、どんな攻撃手法で何の情報が盗まれたのかなど、より深い分析をするお仕事

C-1	フォレンジック分析	被害に遭った端末で何が起こったのか、必要なら詳細な分析を行う
C-2	検体解析	ウイルスがどのような動きをするものだったか解析する
C-3	追及・追跡	これまでの分析結果全てをふまえ、攻撃の目的や手法を明らかにする
C-4	証拠収集	裁判など法的な対応に必要な証拠を保存しておく

D　インシデント対応

起きてしまったインシデントに対し、被害が広がらないようにしたり、原因となったシステムを安全に復旧したりするお仕事

D-1	インシデント報告受付	即時分析で見つかったり、外部からの指摘されたインシデントを受け付ける
D-2	インシデントハンドリング	受け付けたインシデントの対応進捗管理を行う
D-3	インシデント分類	受け付けたインシデントをどのように対処していくべきか判断する
D-4	インシデント対応・封じ込め	被害や影響が拡大する前の封じ込めをする
D-5	インシデント復旧	通常の状態に回復をする支援を行う
D-6	インシデント通知	インシデント対応チームやその他関連するグループにインシデントの発生を伝える
D-7	インシデント対応報告	インシデントの影響や原因、対処内容についてとりまとめる

E　診断と評価

脆弱性診断や標的型メール訓練などによりセキュリティがきちんと守られているか評価するお仕事

E-1	ネットワーク情報収集	守るべきネットワークの構成を把握する
E-2	資産棚卸	守るべき端末やサーバーの情報に加えてアプリケーションの情報も収集する
E-3	脆弱性診断	脆弱性を特定し、リスクをどう軽減できるか提案する
E-4	パッチ管理	ネットワークやアセット情報と脆弱性情報を突合し弱いシステムを把握、対処する
E-5	ペネトレーションテスト	攻撃に悪用される可能性のある脆弱性から侵害方法を見つけてテストする
E-6	高度サイバー攻撃態勢評価	標的型メール訓練などにより高度な攻撃へに耐えられるか確かめる
E-7	サイバー攻撃対応力評価	サイバー攻撃対応訓練を行い、きちんと対処できるか確かめる
E-8	ポリシー遵守	定義したポリシーに適合しているか、遵守しているかを検証する
E-9	堅牢化	セキュリティの設定の評価や見極めによりITコンポーネントの構成最適化を行う

F　脅威情報の収集および分析と評価

ネット上のセキュリティニュースやこれまでチームで見つけたインシデントを取りまとめ、次に生かすお仕事

F-1	事後分析	社内で発生したインシデントに関する情報を集め中長期的な改善案を整理する
F-2	内部脅威情報の整理・分析	リアルタイムの分析やインシデントから見つかった情報を集めて整理する
F-3	外部脅威情報の収集・評価	公開されたセキュリティ情報を収集し、未対策の脅威がないか確認する
F-4	脅威情報報告	内部外部の脅威情報を定期的に取りまとめ報告する
F-5	脅威情報の活用	脅威情報を関係者へ展開し、みんなに活用してもらう

G　CDC/CSCシステム開発・保守

セキュリティ対応に必要なシステムを設置したり、管理したりするお仕事

G-1	セキュリティアーキテクチャ実装	セキュリティアーキテクチャの実装を実現する
G-2	ネットワークセキュリティ製品基本運用	ネットワークセキュリティ製品の設置や設定、その運用を行う
G-3	ネットワークセキュリティ製品高度運用	ネットワークセキュリティ製品のオプション機能などをより効果的に活用する
G-4	エンドポイントセキュリティ製品基本運用	エンドポイントセキュリティ製品の導入や設定、その運用を行う
G-5	エンドポイントセキュリティ製品高度運用	エンドポイントセキュリティ製品のオプション機能などをより効果的に活用する
G-6	クラウドセキュリティ製品基本運用	クラウドセキュリティ製品の導入や設定、その運用を行う
G-7	クラウドセキュリティ製品高度運用	クラウドセキュリティ製品のオプション機能などをより効果的に活用する
G-8	深掘分析ツール運用	フォレンジックやウイルス解析のためのツールを管理、運用する
G-9	分析基盤基本運用	SIEMなどに代表される分析用システムを導入、運用する
G-10	分析基盤高度運用	SIEMのカスタマイズや独自開発により、より高い性能を引き出す
G-11	CDC/CSCシステム運用	レポート生成や問合せ受付などの業務上必要なをシステム運用する
G-12	既設セキュリティ対応ツール検証	すでにあるセキュリティ製品のバージョンアップ検証などを行う
G-13	新規セキュリティ対応ツール検証	今後導入予定の新たなセキュリティ製品の目利きやトライアルなどを実施する

H　内部不正対応支援

社内の内部統制や内部不正に関して、ネットワークやパソコン操作のログを提供、分析して、総務や法務を支援するお仕事

H-1	内部不正対応・分析支援	内部不正が発覚した際のログ情報の提供などを通し支援する
H-2	内部不正検知・再発防止支援	内部不正が繰り返されないよう、検知や防止ができないか検討する

I　外部組織との積極的連携

社内社外問わず勉強会などへ参加したり、会を催したり、セキュリティ仲間を増やすお仕事

I-1	意識啓発	実際のインシデント事例などをもとに社員へ意識啓発する
I-2	教育・トレーニング	自分たちが得た知見を他の社員に対して広めていく
I-3	セキュリティコンサルティング	開発部門などに対して、セキュリティの観点での助言や支援などを行う
I-4	セキュリティベンダーとの連携	製品やサービスを提供するベンダーと良好な関係を築く
I-5	セキュリティ関連団体との連携	セキュリティ関連団体へ加盟し、情報共有、活用の輪を広げる
I-6	技術報告	監視運用の結果の報告をする
I-7	幹部向けセキュリティ報告	幹部向けの定期的な報告や統計的な分析を行う