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

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役割一覧

A　セキュリティ対応組織運営

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	全体方針管理	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	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-3	アクション方針管理	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-4	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-5	セキュリティ対応効果測定	全体としてのセキュリティ対策がうまくいっているか指標をまとめ、効果を確認する
A-6	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

B　リアルタイムアナリシス（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	リアルタイム高度分析	基本分析で足りない場合、より多くのログやデータを含め分析する
B-3	トリアージ情報収集	対応優先度を決めるため、分析結果以外の関連情報を集める
B-4	リアルタイム分析報告	リアルタイム分析で分かったことを取りまとめて報告する
B-5	分析結果問合受付	報告した内容について問い合わせ対応する

C　ディープアナリシス（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	ネットワークフォレンジック	リアルタイムで行いきれなかった詳細な分析を行う
C-2	デジタルフォレンジック	被害に遭った端末で何が起こったのか明らかにする
C-3	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-4	攻撃全容解析	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-5	証拠保全	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	インシデント管理	受け付けたインシデントの対応進捗管理を行う
D-3	インシデント分析	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	リモート対処	監視センターなどからリモートで対処、復旧する
D-5	オンサイト対処	現場に駆けつけて対処、復旧する
D-6	インシデント対応内部連携	社内の関係者（経営者、関係部門）などへ報告、協力依頼する
D-7	インシデント対応外部連携	社外の関係者（顧客、取引企業）などへの説明、調整をする
D-8	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　セキュリティ対応状況の診断と評価

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	アセット情報収集	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	脆弱性管理・対応	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-4	自動脆弱性診断	簡易な診断として、機械的な脆弱性診断を行う
E-5	手動脆弱性診断	より正確な診断として、手動による脆弱性診断を行う
E-6	標的型攻撃耐性評価	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

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	内部脅威情報の整理・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	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-3	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-4	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　セキュリティ対応システム運用・開発

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	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-2	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-3	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-4	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のオプション機能などをより効果的に活用する
G-5	ディープアナリシス(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-6	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-7	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-8	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-9	新規セキュリティ対応ツール調査、開発	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
G-10	業務基盤運用	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

H　内部統制・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	内部統制監査データの収集と管理	内部監査などに必要なデータを集められるようにし、定期的にレポートする
H-2	内部不正対応の調査・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-3	内部不正検知・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	社員のセキュリティ対する意識啓発	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	社内研修・勉強会の実施や支援	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	社内セキュリティアドバイザーとしての活動	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	セキュリティ人材の確保	人事と連携して人材の登用積極化、流出防止施策などを打つ
I-5	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-6	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