iSECのセキュリティサービス（i-Cybertech）

「i-Cybertech」は、iSECが提供するセキュリティソリューションの総称です。
IT・OTいずれの環境においても、異常の検知から調査・対応・報告までをワンストップで対応します。
課題をヒアリングした上で、ご要望に応じて柔軟にサービスをカスタマイズし、最適なサービスをご提供いたします。

ネットワークアセスメント

セキュリティ検知システムを用いて、ネットワーク上に存在する情報資産（デバイス等）の把握を行います。未知の脅威をもたらすマルウェアへの対策も強化することができます。

コンサルティング

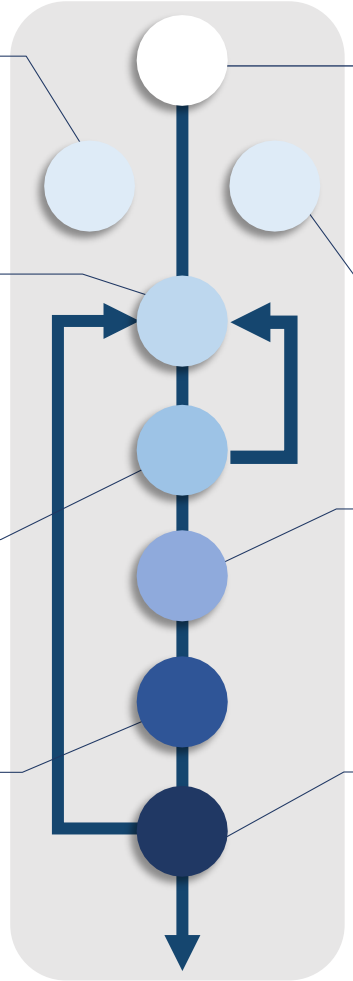
予算に応じたロードマップを作成し、その完遂を目標とした提案を行います。
環境全体を俯瞰し、最適なソリューションの組み合わせの検討、不要なシステムの洗い出し、中長期的な視点でのセキュリティ強化プランの立案等を行います。

セキュリティ対策の製品導入

国内では他に取り扱いのない、海外の最新鋭のセキュリティツールを多数取り扱っています。最適なツールの選定から、導入および運用、組織内で運用される場合のサポートまで対応しています。

インシデント対応（初期対応）

インシデント発生時のCSIRTへのエスカレーションを始め、インシデント調査やCSIRT支援（原則リモートでの対応）を行います。
海外拠点への対応も可能です。



ヒアリング

ヒアリング結果をもとに、有効と考えられる解決方法をお伝えします。
過去の弊社実績、同業種における先行事例、世界的な動向や情報、日々の運用経験で得た知見などを加味して判断します。

リスクアセスメント

ヒアリングと目視ベースのリスク分析、セキュリティポリシーの策定を行います。
要望に応じて、分析結果を踏まえたポリシー策定・教育もお引き受けします。

SOC運用（MSS）

制御システムのセキュリティ運用に対応しています。ネットワークに影響のない方法で監視ツールを導入し、24時間365日の体制で、異常の検知、調査、対応、報告を行います。

インシデントレスポンス（現地駆けつけ調査）

有事の際の、現地駆け付け・サポートに対応しています。インシデント発生時、弊社の技術者が、現場に駆け付けて対処します。
※SOCサービスのオプションメニューとして提供しています。

主な取扱製品

セキュリティ監視サービスあり

※掲載のない製品についてはお問合せください

Guardian／NOZOMI NETWORKS

OT/IoT環境に適した脅威検知・ネットワーク可視化ソリューションです。製造業・電気・ガス・水道・化学・石油・工場などの産業制御システム（ICS）の資産管理、リアルタイムモニタリング、異常検知、脆弱性診断に対応しています。

NDR for OT

MENDEL／GREYCORTEX MENDEL

AI を活用したネットワークふるまい分析エンジンが、ネットワークの定常状態を学習して異常なふるまいを検知、未知の脅威やパフォーマンスの問題に対応します。ネットワークの遅延把握や、EDRを導入できないカメラやプリンタなどのセキュリティ対策にも有効です。

NDR for IT

Cybereason／cybereason

リアルタイムでサイバー攻撃を検知できる、次世代エンドポイントセキュリティソリューションです。検知後は速やかに担当者に伝達、迅速に対処できるプラットフォームを提供します。特にテレワークのセキュリティ対策に有効です。

※2022年12月リリース予定

EDR

Safetica／safetica

「Auditor」「DLP」「Supervisor」の機能を有した情報漏えい対策ソリューションです。エンドポイントに導入し、該当ユーザのふるまいを監視します。クラウド対応により導入が容易で、ポリシー違反やヒューマンエラーを保護します。

DLP

FortiGate／FORTINET

分析機能と自動化機能を備えた統合型セキュリティアーキテクチャです。セキュリティファブリックというプラットフォーム全体の分析と自動化を実現し、優れた検知とレスポンスを提供します。

UTM

FortiSIEM／FORTINET

端末から出力されたログを集約・解析し、検出されたセキュリティ情報とイベントを統合管理できる製品です。

SIEM

Cybellum／Cybellum

ソフトウェアの脆弱性検出から対応、監視まで統合的に脆弱性管理を行うプラットフォームです。SBOM抽出によりバイナリファイルから脆弱性管理が可能です。

脆弱性管理 for CSIRT

i-Auditor／iSEC information security inc.（自社開発製品）

ファイルサーバ、アクティブディレクトリ、DHCP サーバのアクセス管理ツール。ネットワーク野パケットを解析することにより、既存の環境に影響を与えずに導入が可能です。

監査ログ

iNetSecFC／PFU a Fujitsu company

OT環境内の機器やネットワークを簡単に可視化し、インシデントを未然に防ぐ装置です。

資産管理 for OT

IEC-G102-BPシリーズ／MOXA

ホワイトリストの作成等を行い、脅威から資産を保護する次世代IPS機器です。サポート切れのOS（Windowsサーバ等）の保護に有効です。

NWセキュリティ for OT

Elastic stack／elastic

さまざまなデータソースから情報を取得し、検索・分析・可視化をリアルタイムで行うことで、セキュリティの脅威からDXをサポートします。

※2022年12月リリース予定

SIEM

EkranSystem®／EKRAN

ユーザの端末操作をリモートで監視・記録し、内部不正を検知する証跡管理ソリューション。PCI DSS の要件の「アクセスの追跡・監視」に対応しています。

操作ログ取得