Deloitte.
デロイト トーマツ

セキュリティ脅威分析サービス

Threat and Security Monitoring（TSM）

クライアントに関連する情報を能動的に広範囲から収集・更新したインテリジェンスをもとに、クライアント固有のビジネスリスクとサイバーリスクとの関連性を踏まえた高度な分析サービスを提供します。ベンダーニュートラルなスタンスからクライアントに最適なセキュリティソリューションを活用します。3種のメニューから選択いただけます。

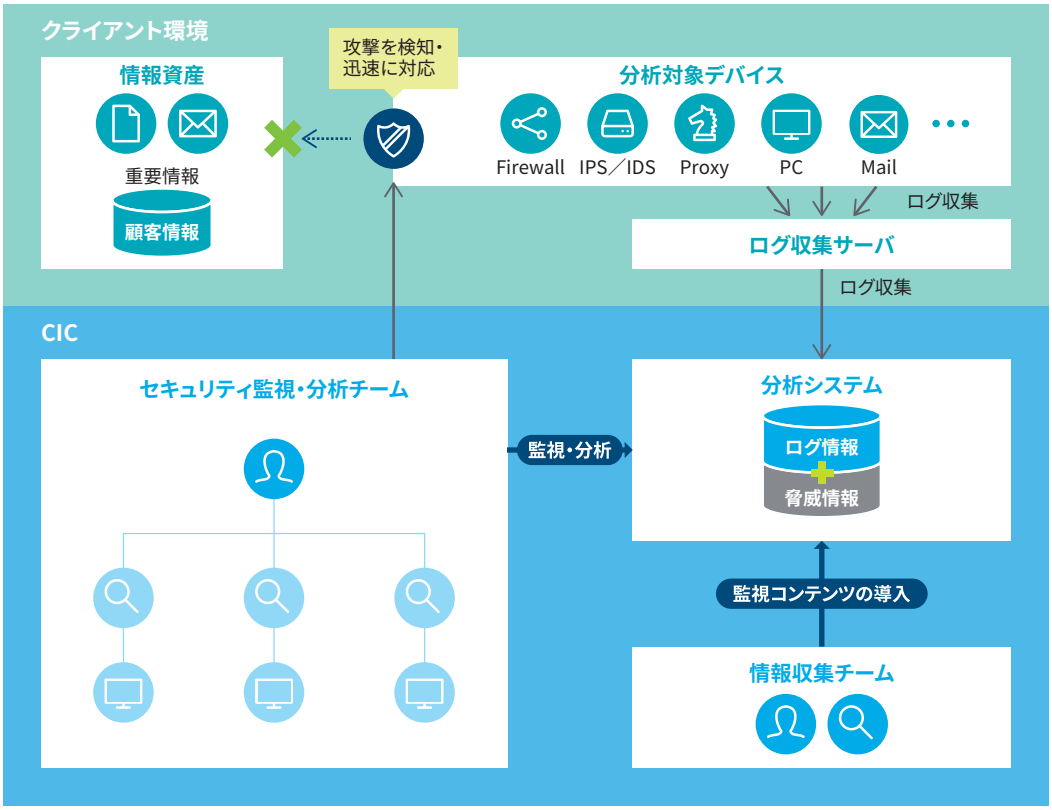
3種の提供メニュー

- **スタンダード**
  アセットレスで手軽にスタート
- **プレミアム**
  クライアント環境のSIEMのログをリモートで監視・分析
- **プレミアムハイブリッド**
  時間帯や想定リスクなどクライアント要件に合わせたSIEMによる監視・分析を、クライアントとCICが分担して実施

共通サービス

- 24時間365日体制でサービス提供
- クライアント専任のインシデントコーディネーターをアサイン

TSM：スタンダード



アセットレス

クライアント環境に「ログ収集サーバ」を設置し、監視対象システム／デバイスのログをCICのSIEMに転送。CICアナリストが分析します。アセットレスにてサービスを享受いただけます。

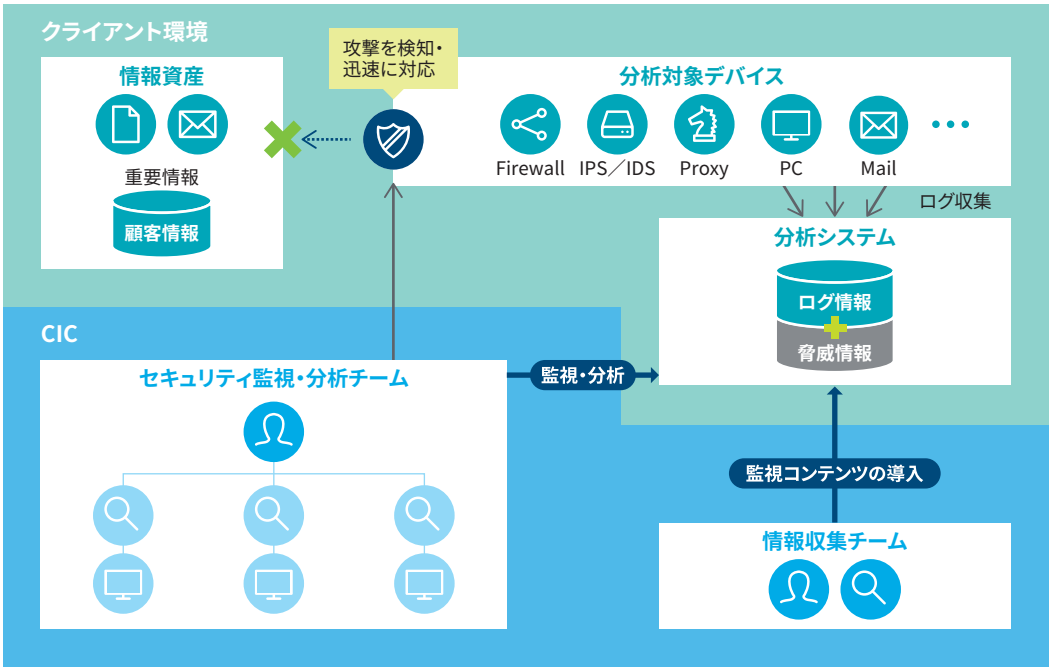
マシンラーニング活用

監視対象システム／デバイスのログデータから、あるパターンやルールをマシンラーニングで学習し、平時のそれとは異なる徴候（＝アノーマリ）を検知・分析します。

V-SIEMオプション

CICが分析に使用するプラットフォームをクライアントにご提供します。クライアントご自身による詳細なログ分析が可能です。

TSM：プレミアム



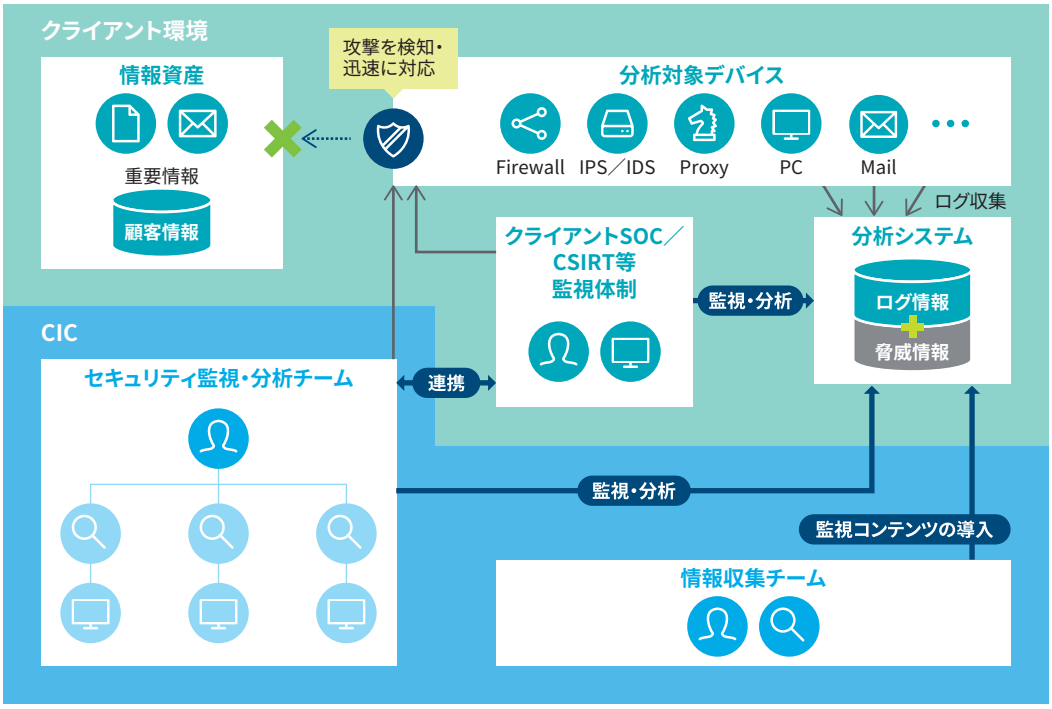
リモートで監視・分析

クライアント保有のSIEMに収集された監視対象システム／デバイスのログを、CICがリモートで分析します。ログはCIC環境には保存されませんので、社外に持ち出せないデータを運用されているクライアントにも最適です。

内部不正にも対応

監視対象システム／デバイスには社員が使うデバイスも含みます。そのログを解析することで、セキュリティポリシーに反するデバイスの使い方をしている社員の特定などを通じ、内部不正への迅速な対応が可能です。

TSM：プレミアムハイブリッド



クライアントのSIEM運用を支援

TSMプレミアムの充実したサービスに加え、時間帯や想定リスクなどクライアントの要件に合わせてSIEMの監視・分析内容を柔軟に設計し、クライアントリソースの最適化をCICがサポートします。

支援スタイルの例

- **時間帯**：夜間休日のSIEM監視・分析をCICがサポート
  クライアントのセキュリティ担当部門が稼働する平日日中以外の、夜間や休日のSIEM監視・分析を実施します。セキュリティ担当部門の業務負荷軽減や人的リソース最適化に貢献します。
- **ロール**：Tier3に該当するリスク検知時にCICがサポート
  深刻なリスクの発生を検知した時から、CICが分析をスイッチします。迅速なインシデント対応により、被害を最小限に抑制します。
- **リスク別**：サイバー脅威はCICが分析を実施
  外部からのセキュリティ脅威はCICが、内部不正に類するものはクライアントのセキュリティ担当部門が分析します。

インテリジェンス提供サービス

Threat Intelligence and Analytics（TIA）

インテリジェンス提供サービスは文字どおり、クライアントのIT資産や情報資産、ひいては企業価値・ブランド価値の防衛に貢献できるインテリジェンスを提供するサービスです。単なる情報提供にとどまらず、リスクの最適化と対処の効率化に必要な、評価・分析・整理された情報（＝インテリジェンス）をお届けします。

お届けするインテリジェンス

戦略的インテリジェンス セキュリティ施策の前提となるリスク評価に影響する情報	● 新しいタイプの脅威の出現 ● 攻撃技術の急速な進展など	〈貢献層〉経営層 〈活用例〉 ・セキュリティポリシーの見直し ・ITシステム・設備の更新
作戦的インテリジェンス 攻撃の可能性を予見し、被害防止に役立つ情報	● ITシステムやビジネスに影響するマルウェアや攻撃手法の動向 ● 同業他社に対する攻撃の手口や、自社を標的とする攻撃グループの動向 ● 自社の内部情報の流出状況	〈貢献層〉マネージャー層 〈活用例〉 ・ITシステムの設定見直し ・アップデート適用 ・従業員教育
戦術的インテリジェンス 自組織で使用しているITシステムの脆弱性情報	● マルウェアの通信先や不正なWebサイトのURL、IPアドレス ● 攻撃メールの件名、本文、添付ファイル名	〈貢献層〉社内対応部署従業員 〈活用例〉 ・セキュリティ製品への取り込み ・従業員への注意喚起

TIA（Threat Intelligence and Analytics）では「戦略的インテリジェンス」、「作戦的インテリジェンス」を重視したサービスデザインを実施し、EWS（Early Warning Service）、および開発中のTIF（Tactical Intelligence Feed）はより即効性が高い「戦術的インテリジェンス」領域に対応するサービスとして設計しています。

インテリジェンスの活動サイクル

プロジェクトキックオフ
- インテリジェンス要件、スコープの確認
- コミュニケーションプラン策定

1. 情報収集計画の立案・継続的見直し
2. 当社アナリストによる情報の分析、評価・インテリジェンスレポートの作成
3. 月次報告会で調査結果の確認、議論、次回アクションの決定
4. 報告会で得られたフィードバックを反映

リサーチの範囲

誰にでもアクセスできるサーフェースWebはもちろん、一般に非公開になっているダークWeb（ディープWeb／ダークネット）、さらにSNSのアクティビティなど、通常の手法ではアクセスが困難なサイバー空間もリサーチ対象とし、情報を収集します。

リサーチの手法

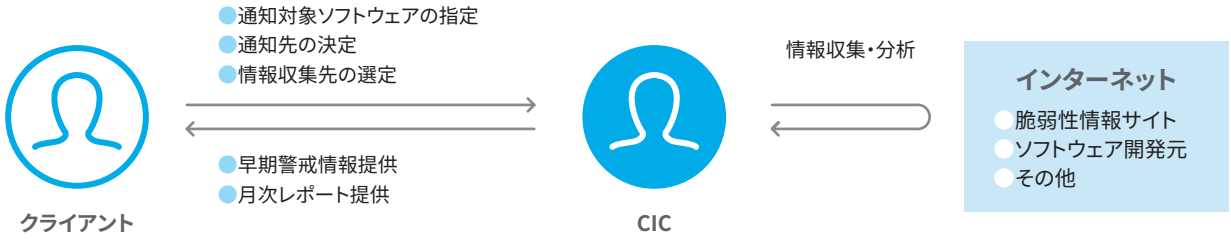
専任リサーチチームが能動的に情報収集を実施。仮想人格を用いたヒューミントによる活動や、ダークWebを自動巡回するツールなどを併用し、クライアントのブランド価値に悪影響を及ぼす可能性のある情報を収集・監視します。

情報提供フロー

重要度や緊急度に応じ、複数の手段でインテリジェンスを提供します。毎月、対面でリサーチャーが月次レポートの内容報告を行うほか、緊急性の高い脅威についてはメールまたは電話により通知します。

早期警戒情報提供サービス
Early Warning Service

CICが国内外から収集した情報の中から、クライアントのシステムやビジネス継続に影響を及ぼす可能性のある、ソフトウェアのリスクに関する情報を早期に通知することで、脆弱性に対する早期対策を実現します。戦略的・作戦的インテリジェンスを提供するTIAを補完する戦術的インテリジェンスとしてご活用いただけます。



通知する情報の種類

脆弱性情報	対象ソフトウェアに関する脆弱性の公表や修正版の公表などに関する情報
開発動向情報	対象ソフトウェア開発元における脆弱性に関する議論やテスト版のリリースなど、新たな脆弱性の内容を類推できる情報
攻撃コード情報	対象ソフトウェア開発に関連するフォーラムなどへの攻撃コードのアップロードなど、攻撃の増加につながる情報
注意喚起情報	対象ソフトウェアを標的とした攻撃発生に関する注意喚起などの情報

IOC配信サービス Coming soon!
Tactical Intelligence Feed

戦術的インテリジェンスの新サービスとして、IOC配信サービスの提供を予定しています。IOCとはIndicator Of Compromise（セキュリティ侵害の痕跡や証拠）。デロイト各国のCICで収集されたIOCに対して、独自の分析を加えたより精度の高いインテリジェンスを提供いたします。脅威の傾向分析やその対策にお役立ていただけます。

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、
本サービス内容がご提供できない可能性があります。詳細はお問合せください。

デロイト トーマツ サイバー合同会社
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡

2019.09_0179