

SYGNIA

インシデント 対応



以下を受賞しています

Gartner FORRESTER

侵害と対峙する際は、最良のチームをお客様の側で編成する必要があります。Sygniaのグローバルインシデント対応チームには、サイバー攻撃の迅速な封じ込めと撃退についての折り紙付きの実績があり、事業の混乱を最小限に抑え、危機を利用して組織への指導を行います。

脅威アクターが犯罪者集団、国家関与型の脅威またはインサイダー脅威であるかに関わらず、Sygniaはクライアントが迅速に調査を行い、攻撃者を封じ込めて根絶できるようにします。Sygniaは、エリート部隊からデジタル戦闘経験があり、脅威アクターの戦術を深く理解しているトップ人材を配備しています。

実績のある利益

サイバー攻撃を迅速に封じ込めて撃退する

事業中断を最短にし、ダメージを最小に抑える

効果的な危機管理

より強力な危機を切り抜ける

SYGNIAの優位性



攻撃者の全体像

Sygniaでは、広範な国家レベルのサイバー戦争の経歴、攻撃と防御の能力と、十年來のインシデント対応経験を持つ熟練のA-チームのみを採用しています。当社のチームは、裏をかき、謀略を使って攻撃者に勝ることができます。



戦闘で実証された方法論と迅速対応

Sygniaのやり方は、軍隊での広範なサイバー戦闘経験の成果です。Sygniaのインシデント対応の方法論には、攻撃に対処するために必要とされる各種の活動、調査とフォレンジック分析、封じ込め、戦術的交渉、修復と復旧、幹部層向けの危機管理、訴訟支援と侵害後のモニタリングの並列実行が含まれます。



技術的優位性

当社の俊敏なチームは、あらゆるITまたはセキュリティスタックを備えたいかなる環境下でもインシデントに効果的に対応します。当社の経験としては、クラウド、アプリケーション、CI/CD、OT、モバイル、IoTなどがあります。また、Sygniaは、専有の高度なプラットフォーム間共通のXDRを導入しており、必要な場合にクライアントの既存のセキュリティツールを強化するために使用されます。



SYGNIAの高度な脅威研究チーム

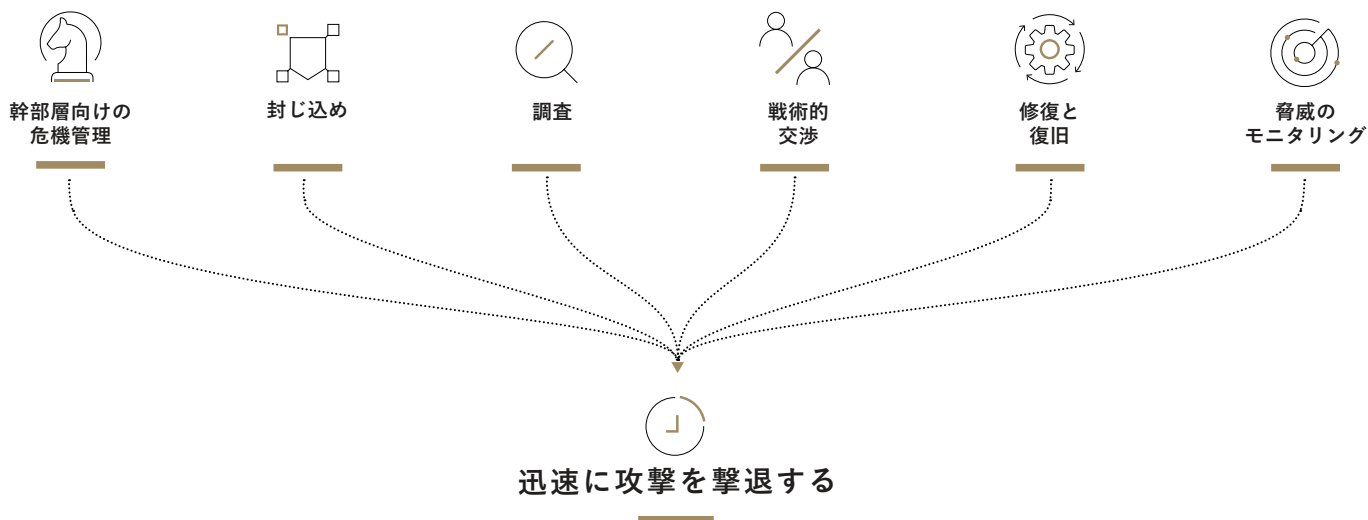
脅威研究とグローバルな脅威の見通しの継続的なモニタリングは、Sygniaのインシデント対応活動に組み込まれており、効果的なフォレンジック調査を可能にし、グローバルなセキュリティコミュニティへの新しい脅威アクターを明らかにします。

“ Forbes

しばしば、サイバーセキュリティデルタフォースと説明される…(Sygnia)は、攻撃への対応速度と決断力で名声を築き、フォーチュン誌「働きがいのある会社」ランキングにランクインした企業が自社のサイバーレジリエンスを構築するのを支援しています。

素早い、多方面からの対応

組織が攻撃下にあるときは一刻を争います。Sygniaは複数の領域で活動を開始し、インシデントの早期解決を目指します。Sygniaは、非常に堅牢で俊敏な対応を可能にするため、すべての領域での活動を並行して進め、それらを調整し、隔々まで管理できます。



幹部向けの危機管理

Sygniaは幹部層とチームを組み、危機を乗り越え、関係者、従業員、及び一般公衆に正確な回答をいたします。Sygniaは、技術的なインシデント解決の流れと並行して、法的および規制上の取り組み、PRと社内管理活動など幹部層向けの危機管理をサポートします。

封じ込め

攻撃によりまだ影響を受けていない環境領域が侵害されないように迅速に対策を講じることが重要です。これは、攻撃を分離や隔離することで実現できます。調査結果を活用して、脅威を迅速に封じ込め、事業へのさらなるダメージを防ぎます。

調査

Sygniaは、トリアージを行い調査をした上で、初期の侵入地点、侵害の範囲、攻撃の環境を通じてどのように伝搬したかと、攻撃者が使用したツールと現在の脅威レベルを特定します。Sygniaは、迅速かつ正確に攻撃ベクトル、タイムラインおよび除去が必要な攻撃者の能力を特定します。

戦術的交渉

Sygniaは、専門家である交渉者を活用して、重要な時間を確保し、攻撃者から得た情報を技術調査チームにフィードバックします。このアプローチは、身代金要求を大幅に減額できるだけでなく、技術調査と復旧活動を大幅に加速します。

修復と復旧

復旧活動は、初期調査と並行して直ちに開始されます。組織は、侵害方法が解明される前に主要なサービスを再構築する「セキュアアイランド」を活用して、組織が完全な事業運営を回復するのにかかる時間を短縮できます。修復活動は、セキュリティを特定して閉鎖し、環境内の攻撃者の存在を抹殺します。

脅威のモニタリング

攻撃者は随時悪意のある行動をさらに試みる恐れがあります。このリスクを最小限に抑えるため、Sygniaのインシデント対応チームは、インシデント全体を通じて、さらにその後も状況に合わせたモニタリングを行い、追加の悪意のある活動と再侵入の試みが、直ちに検出されブロックされるようにします。

Sygniaのインシデント 対応

Sygniaのインシデント対応リテナー（IRR）は、サイバーインシデントの解決時間を短縮する所定の重大事象パラメータを提供します。これらのパラメータが提供されることで、インシデント発生時にSygniaのチームは直ちに全力で取り組み、インシデント対応活動を開始できます。

SygniaのIRR（ティア2以上）には、すべての新規クライアントのオンボーディングセッションが含まれます。このセッションは、クライアントのネットワークとITアーキテクチャー、重大システム、セキュアデータ共有とアクセスプロセスの大まかなレビューが含まれます。対応ガイドラインは、クライアント固有のIRRアクティベーションハンドブック内にSygniaにより定義および保存され、これにより、インシデント対応を加速できます。

サービスティア

Sygniaは、4つの異なるリテナーサービスティアを用意しており、クライアントは、そのビジネス上のニーズに最もよく合ったティアを選択できます。

	ティア 1	ティア 2	ティア 3	ティア 4
署名済み契約書と利用規約	●	●	●	●
年中無休24時間のIR通知ホットライン	●	●	●	●
専有テクノロジーの導入	●	●	●	●
IRR オンボーディングセッション	○	●	●	●
リモート対応時間SLA	ベストエフォート	6時間	4時間	2時間
エンルート対応時間SLA	ベストエフォート	48時間	24時間	24時間
前払いIRサポート時間	○	100時間	200時間	300時間
IRサービスの割引率	標準料金	10%割引	15%割引	20%割引
リテナー期間	1年	1年	1年	1年

未利用時間は、Sygniaの他のサービスに充当できます。

SYGNIA IRRの優位性

複数のティア

組織のニーズへの整合を可能に

迅速対応

SLA

専用アカウント

マネージャー

オンボーディングプロセス

シームレスな対応を保证するように設計

利用率100%

リテナー時間の利用率：任意のSygniaのサービスに再利用可能

補完サービス

IRRクライアント向け

リテナー時間の柔軟な利用

未利用のIRR時間は、任意のSygniaのサービスに再利用可能です。また、Sygniaは特にIRRクライアント向けにデザインされたサービスのセットも提供しており、これには幹部向けの上演習、技術的な机上上演習、トリアージとエスカレーションの合同演習と敵対的なシミュレーションが含まれます。

リテナーがもたらす利益

安心を保証

対応時間を短縮

対応にかかるコストを削減

対応の有効性を改善

継続的改善を可能に

Sygnia® はサイバーコンサルティングとインシデント対応を行う会社で、世界中の組織にインパクトの大きいサービスを提供しています。Sygniaは、自社のクライアントと協力して、脅威に迅速に対応し、レジリエンスを積極的に強化します。当社の折り紙付きの実績、コミットメントと思慮分別により、Sygniaはセキュリティチーム、上級幹部、およびフォーチュン誌「働きがいのある会社」ランキングにランクインした企業を含め世界中の大手企業の取締役会の信頼を勝ち得ています。

TEMASEK ISTARI Temasek社およびISTARI Collectiveメンバー

24時間365日のインシデント対応

インシデントの疑いですか？今すぐお電話を +1-877-686-8680 | 詳細はwww.sygnia.coにアクセスしてください

SYGNIA