securonix

データシート

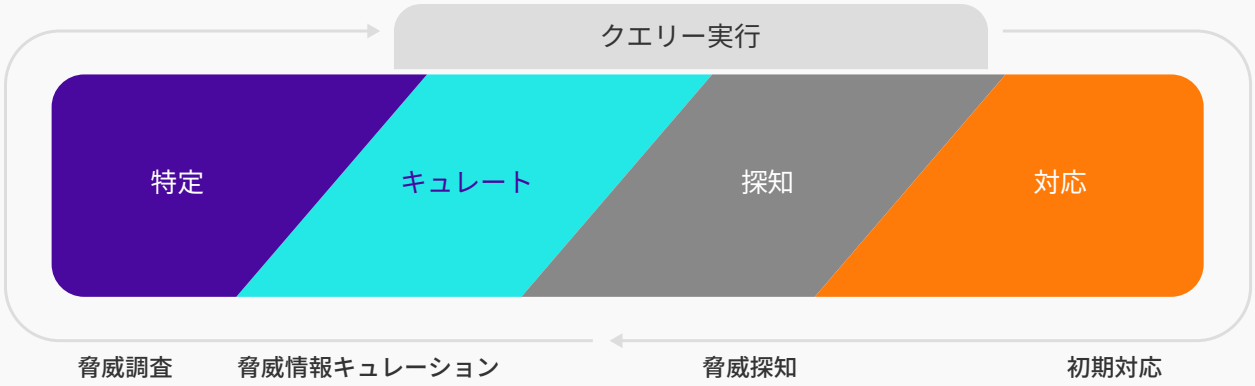
Autonomous Threat Sweeper

サイバー脅威に迅速に対応する自動化した脅威勧告と事後探知

お客様の SOC 運用を強力に支援

セキュリティチームは、日々、新たに出現する脅威の対応に追われ、多大なプレッシャーにさらされています。サイバー攻撃が対象範囲や規模を拡大しているため、組織は、継続的に出現する脅威に関し、セキュリティ侵害の有無を評価する自動化ソリューションが必要になっています。

Securonix Threat Labs の最新リサーチと脅威コンテンツを活用した、Autonomous Threat Sweeper (ATS) は、手作業で行われていた調査の多くを体系化しています。セキュリティ侵害の調査プロセスとインシデント対応の着手を自動化し、セキュリティ運用を強力に支援します。



ATS は、キュレートされた脅威インテリジェンス、自動化された探知技術と調査により、お客様環境に潜む未知の脅威を見つけ出します。

ATS の真価

新たな脅威や進化する脅威の先を行く

継続的にキュレーションされた脅威インテリジェンスにより、セキュリティチームは、高リスクの脅威を優先的に対処できるようになります。ATS は、大量の過去ログデータに対する遡及的な探知を行う、SOC の拡張機能を提供します。

セキュリティ侵害をすばやく知る

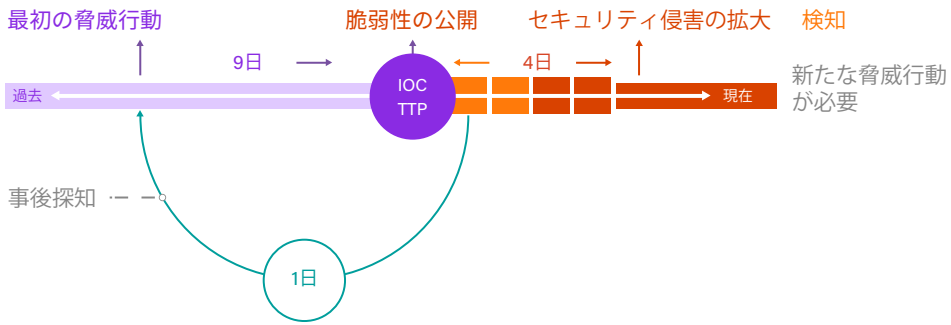
攻撃を主体とした IOC（セキュリティ侵害の痕跡）と TTP（攻撃者の戦術、技術、手順）に基づく探知により、新たな脅威にさらされていることを迅速に把握できます。ATS は、Securonix Threat Labs によって選定および体系化された、IOC と TTP の両方を使用した事後的探知を行い、「ロー・アンド・スロー」アタックの検知を実現します。

サイバー脅威の緊急対応を加速する

自動化されたレポート作成、アラート通知、インシデント登録により、サイバー脅威の緊急対応を加速します。ATS は、お客様環境を断続的に監視し、新たな脅威に関するインテリジェンスをキュレーションすることで、セキュリティチームが平均対応時間（MTTR）を短縮し、重大な脅威を優先的に対応できるよう支援します。

ATS で SOC を効率化

セキュリティチームは、ATS の強力な機能により、多くの日々の調査タスクの負荷を軽減でき、最も重大な脅威に集中することができます。



キュレーションされた脅威情報の通知

最新の脅威コンテンツとレポートが提供され、脅威の存在を把握します。

脅威インテリジェンス : Securonix Threat Labs（脅威ラボチーム）の専門家がキュレーションした最新の脅威コンテンツを入手できます。

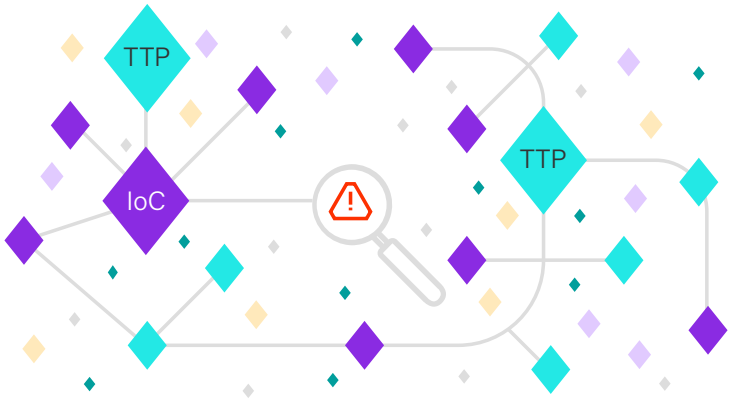
脅威探知レポート : お客様環境内で重大な脅威を探知すると、すぐに通知を受け取ります。

マルチベクトル探知モード

複合的な探知手法を活用し、セキュリティ侵害の known-known 指標と、TTP に由来する known-unknown 指標の両方を探知します。

IOC 探知モード : 脅威インテリジェンスからセキュリティ侵害の指標を選定し、お客様環境の長期保存の過去データに潜む新たな脅威を探知します。

TTP 探知モード : 脅威ハンターが IOC に関する事前の知識がない場合、戦術、技術、手順の分析を行ない、セキュリティ侵害の指標を特定するための支援をします。



詳細なレポートとアラート通知

ATS は、包括的なレポート作成とインシデントを自動登録の後、セキュリティチームにアラートを通知し、対応ガイダンスを提供します。

自動化 : ATS は、現在および過去のログデータにセキュリティ侵害の痕跡がないか、検索クエリーを実行してお客様環境を自動的に探知することで、検知と対応の迅速化を図ります。

対応ガイダンス : IOC と TTP がお客様環境で探知された場合、詳細な調査結果と対応ガイダンスを入手することができます。

Securonix ATSの詳細については、
www.securonix.com/request-a-demo でお申し込みの上、デモをご覧下さい。