Secureworks

脅威検知能力の強化を目指し Taegis XDR / Taegis ManagedXDRを導入 安心・安全なサービス提供に貢献

sansan

お客様名：Sansan株式会社

資本金： 66億33百万円
(2023年8月31日時点)

従業員数： 1,421 名
(2023年8月31日時点)

設 立：2007年6月11日

所在地：東京都渋谷区神宮前5-52-2

URL：jp.sansan.com

ソリューション

Taegis XDR

Taegis ManagedXDR

プロジェクトのゴール

1. 防御システムの脅威検知能力をより強化すること

2. セキュリティ運用管理に要する負荷を軽減すること

システム導入時期

2023年6月

セキュリティと利便性を両立させ 顧客企業のイノベーションを加速

「出会いからイノベーションを生み出す」をミッションとし、「ビジネスインフラになる」というビジョンを掲げるSansan。同社では、このミッション・ ビジョンの下、顧客企業のビジネス革新を支援する事業を展開。100万件以上の顧客情報を営業活動に活用できる営業DXサービス「Sansan」をはじめ、企業全体の請求書業務を加速するインボイス管理サービス「Bill One」、あらゆる契約書を正確にデータ化し全社で活用できるようにする契約DXサービス「Contract One」、名刺管理やキャリア形成に活用できる名刺アプリ「Eight」 など、多彩なサービスを提供している。

個人情報などの顧客の重要な情報を預かるだけに、セキュリティ対策にも抜かりはない。Sansan技術本部 情報セキュリティ部CSIRTグループ兼 情報セキュリティマネジメントグループ 佐藤 健太 氏は「一般にCSIRTはインシデント対応が主な役割とされますが、当社CSIRTでは各プロダクトを担当する事業部門とも密接に連携し、サービスの安全性を高めるための支援も行っています。また、情報セキュリティマネジメントグループでも、情報管理の指針やルール作り、教育・啓蒙活動などの取り組みを通して、ガバナンスの強化に努めています」と説明する。

こうした活動を展開する一方で、従業員の働きやすさや生産性などにも十分配慮しているとのこと。佐藤氏は「当社では『セキュリティと利便性を両立させる』をPremiseとして掲げています。安心・安全はもちろん大前提ですが、それがイノベーションの妨げになってしまったのでは好ましくない。この両者を高度にバランスさせることが、我々の使命だと考えています」と語る。

脅威検知能力の強化を目指し Taegis XDR/Taegis ManagedXDR を導入

多種多様なソースのログを相関分析して脅威を検知するXDR製品に着目。

同社では、年々悪質化・巧妙化するサイバー攻撃に対処するために、セキュリティ対策の継続的な見直しも行っている。その一環として、今回実施されたのが、XDR(Extended Detection &Response)製品の導入プロジェクトだ。佐藤氏はその背景を「当社では毎年ペネトレーションテストを実施していますが、その中で課題として浮かび上がってきたのが、脅威検知能力のさらなる強化です。近年では新たな攻撃手法も次々と生まれていますので、こうしたものも的確に検知できるようにしておかなくてはなりません」と語る。

もちろん同社では、EDR(Endpoint Detection & Response)やSIEM(Security Information and Event Management)などの製品も導入済みだ。しかし、エンドポイントやネットワーク、クラウドなどの各領域に特化した製品だけでは、巧妙なサイバー攻撃の検知は困難であるため、各領域の横断連携も必要となる。そこで、多種多様なソースのログを相関分析して脅威を検知するXDR製品に着目したのである。

製品選定にあたっては、脅威検知能力の高さに加えて、対応サービス／ソリューションの幅広さ、使い勝手、リーズナブルなコストで利用できることなどが要件となったとのこと。これらを満たす製品として選ばれたのが、セキュアワークスの「Taegis XDR」、並びにマネージドサービス「Taegis ManagedXDR」だ。

佐藤氏はTaegis XDRを選んだ理由を「既存のEDR製品にもXDR機能が用意されていますが、それだと単一ベンダーの視点でしか脅威を検知できません。その点、当社では従来から提供されていたセキュアワークスのマネージド・セキュリティ・サービスを利用した経験があり、その能力も高く評価しています。そこで、今回はTaegis XDRを採用し、複数ベンダーのエンジンでより網羅的に脅威を検知できるようにしたいと考えました」と説明する。

約3,000台のエンドポイントや IaaS/SaaSのログを網羅的に監視

インシデントへの初動対応もスピーディかつ効率的で、マネージドサービスの導入に関しては悩んだ部分もあったのですが、結果的には入れておいて正解でした。

現行環境への導入もスムーズに進んだとのこと。「この手の製品では、ログの取り込みに苦労することが多いのですが、Taegis XDRは非常にインテグレーションしやすかったですね。ログの取り込みだけなら一週間程度、評価や検証まで含めても一ヶ月程度で導入を終えられました。中には評価だけで数ヶ月掛かるような製品もありますので、かなり導入しやすい製品だと思います」と佐藤氏は振り返る。

具体的な監視対象としては、本社や拠点に配置された約3,000台のエンドポイントのほか、AWSやOkta、AzureAD などのIaaS/SaaSサービスが挙げられる。EDR/XDR導入企業の中には、過検知や誤検知への対応に苦慮するところも少なくないが、同社ではTaegis ManagedXDRも併せて導入しているため、こうした問題とも無縁である。

「検知内容に特に問題がない場合は、セキュアワークスのアナリストがそのままクローズしてくれますので、我々の運用管理工数が増える心配はありません。また、Taegis ManagedXDRでは、発生した侵害の詳しい内容を調査した上で報告してもらえますので、インシデントへの初動対応もスピーディかつ効率的に行えます。マネージドサービスの導入に関しては悩んだ部分もあったのですが、結果的には入れておいて正解でした」と佐藤氏は満足げに語る。

強固な監視体制を確立し 新たな脅威にも確実に対処

IDの不正利用など対処すべきリスクも増えていきますが、Taegis XDRを導入してからは検知できるようになりました。

現在同社では、Taegis XDRと既存のSIEM基盤を組み合わせたハイブリッド運用を実施している。普段の監視についてはTaegis XDRで行い、特別な調査を行う場合のみSIEMでの分析を行うことで、拡張性を保ちつつ費用対効果の高い監視体制を築いているのだ。監視対象は以前より増えているが、それによってアラート対応の負荷が増えるようなこともないとのことだ。

「SIEMにはいろいろなところからログが入ってきますが、その情報をいざ活用しようと思っても、手間が掛かってなかなか難しいというケースも多い。その点、Taegis XDRを使えば、様々

な情報を相関分析して、『面』として捉えることができます。アラートー一つを取っても、どのセンサーとどのセンサーで検知して、こういう時系列で侵害が起きていると、事象を分かりすく把握できます。これは非常に大きなメリットですね」と佐藤氏は語る。

懸案であった脅威検知能力の強化についても、十分な成果が上がっているとのこと。「クラウド利用の広がりに伴って、IDの不正利用など対処すべきリスクも増えていきます。こうしたものは事業者側の防御機能でも対処できないことがあるのですが、Taegis XDRを導入してからは検知できるようになりました」と佐藤氏は語る。

また、もう一つのメリットが、セキュアワークスのグローバルな知見を活用できる点だ。Taegisのプラットフォームには、最新の脅威インテリジェンスや検知ルールが自動的に反映されるため、常に安心・安全な環境を保つことができる。佐藤氏は「ユーザー企業が自前で情報収集などを行うのは非常に大変ですから、世界中の専門家の知見を使わせてもらえるのは、かなりありがたい」とにこやかに語る。

今後監視対象のサービスが増えたとしても、Taegis XDRのオープンさを活かすことで十分対応することが可能だ。
「当社ではこれまで相当高いレベルのセキュリティを作り上げてきました。しかし、現在の状況を鑑みると、より検知の難しい脅威にも確実に対処していく必要があります。それだけにTaegis XDRの今後のエンハンスにも、大いに期待しています」と佐藤氏は述べた。

Sansan株式会社
技術本部 情報セキュリティ部 CSIRTグループ
兼 情報セキュリティマネジメントグループ
佐藤 健太 氏

取材 2023年9月
- 記載内容は、2023年9月15日時点のものです。
- 本文書に記載されている仕様は2023年9月時点のものであり、予告なく変更する場合があります。最新の仕様については、弊社ホームページにてご確認ください。

詳細は当社のセキュリティ専門家までご相談ください。

03-4400-9373
secureworks.jp