

アンラボ・セキュリティレター

Press **Ahn**

2025.3 Vol.131

「AhnLab XDR」を導入した Golfzon、セキュリティリスク 56%減少！

「AhnLab XDR」を導入した Golfzon、 セキュリティリスク 56%減少！



概要

Golfzon(ゴルフゾン)は、ゴルフと自社の核心情報技術(IT)を組み合わせたゴルフシミュレーター(Golf Simulator、GS)専門企業である。このシステムを中心に、革新で没入感のある様々な統合ゴルフサービスを提供している。

Golfzon は、アンラボのセキュリティソリューションを導入し、組織のセキュリティを強化するとともに、顧客に安全で信頼できるサービスを提供するために努力している。アンラボのエンドポイントおよび統合セキュリティソリューションを導入することで脅威リスクを減らし、サービスの安定性を確保した。

2023年にランサムウェア攻撃を受けた後、Golfzon は自社のインターネット網と IDC、AWS、電子金融網などに「AhnLab EDR」と「AhnLab EPP」を導入した。さらに、管理型検知および対応サービスである「AhnLab MDR」も導入してアンラボの脅威専門家を通じて検知された脅威を能動的に分析し、対応策を提示するサービスも受けている。また、「AhnLab EDR」と共により効率的なセキュリティリスク管理のため「AhnLab XDR」を追加で導入した。「AhnLab V3」を始め、「AhnLab EDR」、「AhnLab EPP」がすでに導入されていたため、「AhnLab XDR」を容易に導入することができた。Golfzon は、これらのソリューションを通じてリアルタイムの脅威検知と対応、ランサムウェア攻撃の復旧とサービス再開のサポートを受けている。

Golfzon は、セキュリティが強化されたゴルフ商品とサービスを持続的に発売し運営することで、顧客に最高のゴルフ体験を提供する予定である。

“Golfzon はアンラボのサポートを受け、ランサムウェアの被害を迅速に復旧し、内部に潜在している攻撃者を識別して処理することができました。また、既存のセキュリティモニタリングサービスを受ける過程で、アンラボと共に構築した技術的・運営的ネットワークを積極的に活用できたことも大きな助けになりました。今後もアンラボとの密接に協力を通じて安全性が保証された様々なゴルフサービスと商品を開発していくつもりです。”

- Golfzon の情報セキュリティチーム キム・ジョンフン プロ-

課題

2023年11月23日、Golfzon はランサムウェア組織「ブラックスーツ(BlackSuit)」の攻撃を受けてサービス障害が発生した。窃取された情報はダークウェブ(DarkWeb)に公開された。

Golfzon は、この侵害事故を分析する過程で、許可されたユーザーの権限を不正に使用して様々な不正行為が行われていることを確認した。さらに、攻撃者はランサムウェア攻撃後でも、Golfzon の内部情報を利用して持続的に攻撃を試みていたことが分かった。Golfzon は、事態の深刻性を認知し、エンドポイント領域のすべての行為を分析し、攻撃活動を遮断しようと「AhnLab EDR」を導入した。また、アンラボのサポートを受け、Golfzon 内のサーバーとエンドポイントに、エンドポイント保護プラットフォームである「AhnLab EPP」を導入した。

今まで Golfzon は、20種類以上のセキュリティソリューションを運営していたため、様々なセキュリティソリューションで発生する単一のイベントを一つ一つ対応・処理するのに困難を抱えていた。それぞれのアラート(Alert)が単純なミスなのか、ハッカーの攻撃なのか、重要なのか無意味なのかが分かりにくかった。このイベントを慎重に検討できるリソースと人員、ツールなどの体制が不足していたのがその原因である。

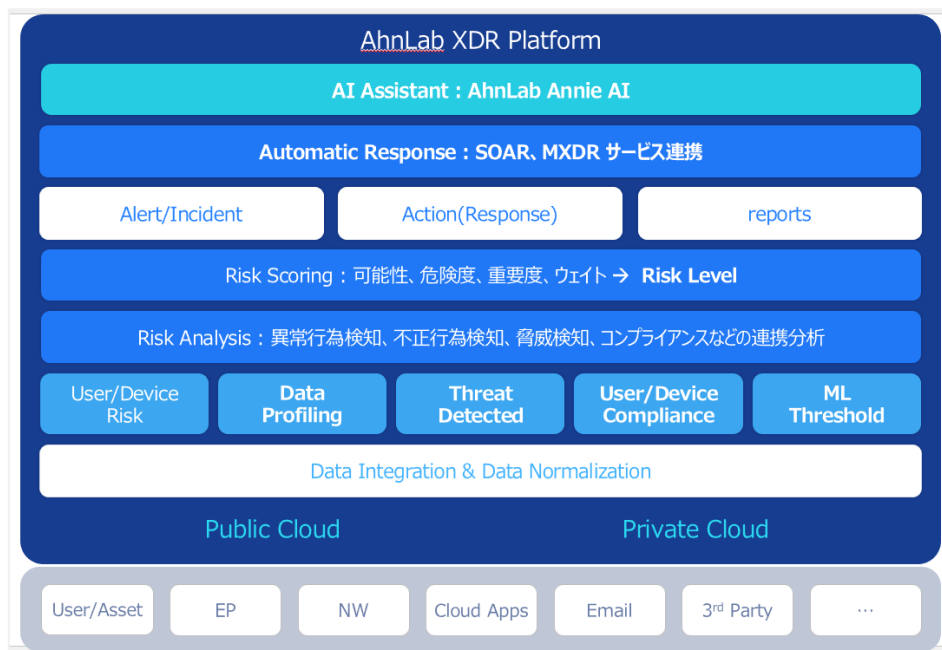
そのため、1日に数百万件も発生するアラートの中から、有意味な脅威を見つけ出して、事前に対応できるアプローチを導入し、既存の「AhnLab EDR」をより効率的に運営するためアンラボと協力して「AhnLab XDR」を導入した。

ソリューション

Golfzon は、「AhnLab EDR」と「AhnLab EPP」がすでに構築されており、「AhnLab MDR」サービスを同時に受けて、エンドポイントで発生する様々な脅威を効果的に管理している。ランサムウェア攻撃発生後、アンラボの脅威情報分析専門チームである「A-FIRST」が Golfzon の侵害事故を精密に分析し、問題点を診断して解決策を提供した。

Golfzon は、各セキュリティソリューションで発生する単一のイベントに一つ一つ対応するのが困難だった問題を解決するため、「AhnLab XDR」を導入した。「AhnLab XDR」は、SaaS 方式で構築され、データによるハードウェア拡張や性能問題などの悩みを解決し、迅速に構築することができる。また、サーバーやエンドポイントの可用性を損なわない範囲でスムーズな運営も可能である。

Golfzon は 1,500台以上の PC 資産と 700台以上のサーバーの資産情報を「AhnLab XDR」と連携させ、セキュリティシステムと主要な運用ソリューションのログを結合して検知シナリオに従って電子メール、Telegram などで脅威通知を送信するように設定した。これにより、セキュリティソリューションの個別管理を超え、全社的なリスク管理および対応領域へ「AhnLab XDR」の機能を拡張しようとした。



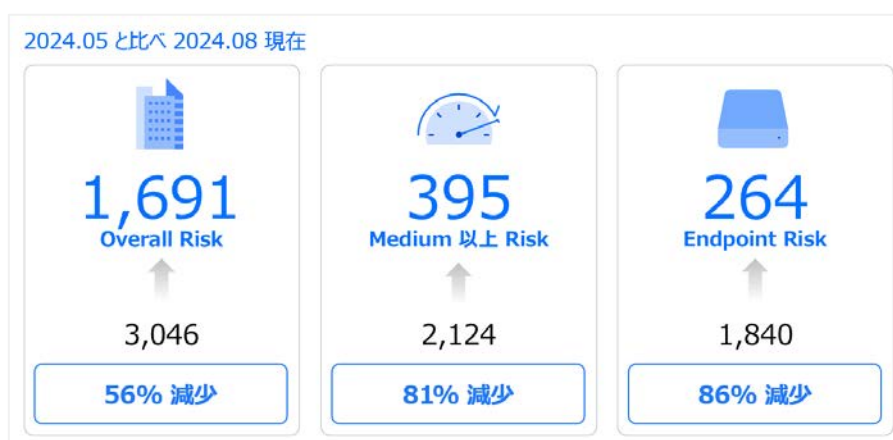
【図1】「AhnLab XDR」プラットフォーム構造図

導入効果

アンラボの EDR/MDR、EPP に続き「AhnLab XDR」を導入した後、Golfzon のセキュリティレベルは全体的に向上した。Golfzon は「AhnLab XDR」を中心に、様々なセキュリティソリューションログの相関関係分析を通じて、直感的で有意義な分析と処理を行っている。

Golfzon は、セキュリティシステムで発生する膨大な量のイベントに対する誤検知、重要度の低い脅威に対するリソースの無駄を減らし、担当者が検知や対応できなかった履歴を探し出す効果的なセキュリティシステムを構築した。これにより、不正な IP のアクセス、VPN 異常ログイン、ブルートフォース攻撃(Brute Force)、管理されていないファイアウォールポリシーの高度化などを実現して全体のセキュリティイベント数が大幅に減少した。

実際に、2024年5月の時点で3,046件だったセキュリティリスクが2024年8月には1,691件に減少し、3ヶ月で56%減少した。このうち、エンドポイント領域で確認されたリスクは1,840件から264件に、総計86%減少した。



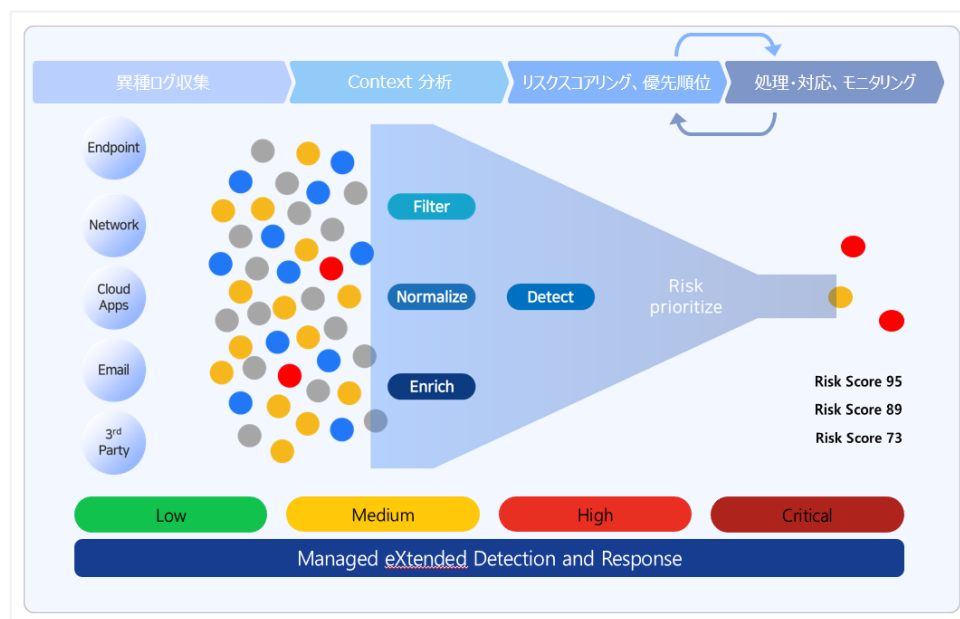
【図2】「AhnLab XDR」導入後、Golfzon 社内リスク減少状況

他にも、誤検知率が改善され、セキュリティ担当者の生産性が向上した。また、データハブ(Data Hub)を通じてセキュリティ強化とデータ収集および連携効率化を達成した。

今後の計画

Golfzon はセキュリティ強化のための持続的な投資と努力の一環として、アンラボのセキュリティソリューションを積極的に活用する計画である。特に、「AhnLab XDR」をベースに、ますます複雑化する脅威環境に、先制的に対応するため、より強固なセキュリティシステムを構築する予定である。「AhnLab XDR」を活用し、多様なセキュリティソリューションで発生するイベント間の相関関係を精巧に分析し、これをもとに全社的なリスク管理と対応機能を強化し、リアルタイムで脅威モニタリングおよび検知、分析能力を向上させる予定である。

最近では、アンラボの「MXDR サービス」の導入を検討している。「AhnLab MXDR」はリモートセキュリティモニタリングとは別のサービスで、アンラボのセキュリティ専門家が内部の脅威要素を識別し、詳細分析後に脅威要素を除去し、リアルタイムで警告を送信する XDR 専用管理サービスである。現在も、アンラボは自社「MDR サービス」を通じて Golfzon のリスク検知履歴や注意事項、マルウェア検知に関する推奨事項を電子メールで送信するなど、リアルタイムで Golfzon のセキュリティ強化に努力している。



[図3] 「AhnLab MXDR」脅威検知/対応プロセス

今後もアンラボとの協力を通じてエンドポイントのみならず、クラウド環境や外部システムに対するセキュリティチェックおよびモニタリングを強化し、攻撃者が Golfzon のインフラをターゲットにしないように対策を徹底的に備える予定である。これにより、顧客に安定したサービスを提供し、業界のリーダーとしての地位を固めることができるだろう。

「AhnLab XDR」に関する詳しい情報はアンラボのホームページで確認できる。

▶ [AhnLab XDR さらに詳しくはこちら](#)



<http://jp.ahnlab.com/site/main.do>

<http://global.ahnlab.com/site/main.do>

<http://www.ahnlab.com/kr/site/main.do>



アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。

1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。

アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)

© 2025 AhnLab, Inc. All rights reserved.