Case Study

THALES
CYBERSECURITY

imperva

SDIS 62（仏・消防局）、Cloud WAFの導入で重要なデータの保護と公共安全業務のセキュリティ確保を実現

THALES

CYBERSECURITY

SDIS 62について

SDIS 62（Service Départemental d'Incendie et de Secours du Pas-de-Calais）は、フランスのパ・ド・カレー県の消防隊を統括する有名な公的機関です。その使命には、事故、技術的災害、自然災害など、あらゆる種類の市民安全リスクを評価して予防し、緊急事態への応急対策を準備することが含まれます。また、救助資源の編成、消火活動、個人への緊急支援の提供、人命・財産・環境の保護も担っています。本質的には、予防・予測・運用という3つの機能を中心に活動しています。

課題

旧式のWAFと露出した攻撃対象領域が、重要なデータと公共安全の脅威に

SDIS 62には、公共安全を担う組織として、迅速な緊急対応を支えるシステムの可用性とセキュリティの両立が求められます。SDIS 62のチームは中央集権型のIT環境で運用しており、サービスの中断は救助活動に重大な支障をきたす可能性があります。

SDIS 62はこれまで、ファイアウォールベースの内部WAFに依存していましたが、可視性と制御性に欠け、特定のサードパーティアプリケーションのアップデートに苦労していました。そのため、既知のCVE（共通脆弱性識別子）が未修正のままとなっていました。32個のパブリックIPアドレスでさまざまなアプリケーションをホストしているSDIS 62にとって、攻撃対象領域の保護は不可欠です。

「中央集権型のシステムで50の消防署すべてを管理しているため、もしシステムがダウンすれば、緊急サービスを調整できなくなります」と、情報システム、ネットワークおよび通信部門責任者のRomuald Delattre氏は語ります。

従来のWAFでは、不正なトラフィックのブロックや地理的条件による接続のフィルタリングを効果的に行うことができませんでした。チームはフランス国外のIPをブロックするよう設定しましたが、正当なユーザーまで誤ってブロックしてしまう事態が続いていました。

導入

Imperva Cloud WAF：機関自身によるシンプルな導入で外部公開インフラの保護を実現

SDIS 62は、いくつかの代替ソリューションを評価した結果、パブリックIPの露出を排除し、悪意あるトラフィックを内部システムに到達する前にフィルタリングできるタレスImperva Cloud WAFを採用しました。

「すべてのトラフィックをタレスImperva Cloud WAF経由に切り替えました。現在ではインフラ全体がエンドツーエンドで保護されており、トラフィックが内部システムに直接到達することはありません」と、Delattre氏は語ります。「DDoS攻撃、ボットネット、APIの悪用、SQLインジェクションの試みなどがありますが……このソリューションを導入して以来、正直なところ安心して眠れるようになりました」

Imperva Cloud WAFは、ほぼゼロに近い誤検知率で攻撃を阻止し、グローバルSOC（セキュリティオペレーションセンター）を活用して、最新の攻撃が発見されてから数分以内に組織の保護を強化します。Imperva Cloud WAFは、Advanced Bot Protection、Advanced API Protection、Advanced DDoS Protectionを統合した多層アプリケーションセキュリティソリューションの一部であり、すべてを統一された管理コンソールから操作できます。

タレスチームの支援のもと、導入は同機関自身で実施されました。タレスチームによる技術的な手順説明と継続的なサポートにより、移行プロセスに対する信頼感が高まりました。情報システム、ネットワークおよび通信部門の副責任者であるSofian Saïd氏は、タレス主導のデモを参考に各サービスに対してプロセスを再現し、32個のパブリックIPすべてをわずか15日間で段階的に保護しました。「これらすべての背後には重要なサービスがあるため不安もありましたが、Impervaではすべてが自動化されており、パブリックDNSの管理権を取得して、わずか2クリックでトラフィックをリダイレクトできました。本当に、驚くほどスムーズでした」と、氏は語っています。

業種
公共安全

所在地
フランス、サン・ローラン・ブランジー

ウェブサイト
www.sdis62.fr

成果

攻撃対象領域の削減と可視性の向上により、セキュリティが強化され、公共安全の支援にも貢献

SDIS 62では、攻撃対象領域が減り、可視性が向上し、安心感が高まりました。ジオフィルター機能だけでも、侵入する脅威の減少につながりました。直感的なダッシュボードにより、チームはセキュリティデータを可視化し、リアルタイムの統計情報を上層部に提示できるようになりました。

「以前は、データもグラフもカスタマイズもありませんでした。今では、数字や統計、グラフを持って経営会議に参加し、『私たちのセキュリティシステムが1日や1週間で何件の攻撃をブロックしていると思いますか?』と聞けるようになったのです。それから実際の数字を見せ、『えっ、そんなに? それって1か月分?』『いえいえ、1日分ですよ!』と皆を驚かせています」と、Saïd氏は語ります。

運用面でも、Imperva Cloud WAFはユーザーの負担を軽減しました。「セキュリティインシデントへの対応だけでなく、仕事量が本当に減りました」と、Saïd氏は言います。「以前のジオフィルターは設定が不十分でした。今ではImpervaが私たちの求めていることを正確に実行してくれます。データベースはリアルタイムで更新され、私たちにとって完全に透明で、管理が非常に楽になりました」

Imperva Cloud WAFの導入により、SDIS 62はコンプライアンスを維持しながら、安全なスケーラビリティを確保しています。「現代では、外部攻撃対象領域の削減や排除を実現したと言えることは、もはや贅沢ではなく必要なことです」と、Delattre氏は語ります。「外部からの攻撃はすべてThales Imperva Cloud WAFに吸収され、直接的な攻撃試行が組織内部に届かなくなったため、非常に安心できます。セキュリティと安心感の向上を考えると、Imperva Cloud WAFへの投資は間違いなく価値があります。その投資対効果は非常に高いものとなるでしょう」

> 「DDoS攻撃、ボットネット、APIの悪用、SQLインジェクションの試みなどがありますが……[Imperva Cloud WAF]を導入して以来、正直なところ安心して眠れるようになりました」
>
> **– Romuald Delattre氏、SDIS 62の情報システム、ネットワークおよび通信部門責任者**

タレスについて

タレスはデータセキュリティのグローバルリーダーとして、世界中で高い信頼を得ているさまざまな組織が、あらゆる場所で重要なアプリケーション、機密データ、およびIDを包括的に保護できるよう支援しています。タレスは、革新的なサービスと統合プラットフォームを通じて、リスクの可視化、サイバー攻撃の防御、そしてコンプライアンスギャップの解消を可能にし、毎日数十億人の消費者に安心で信頼性の高いデジタルエクスペリエンスを提供します。