

# Carrefour社、Splunk Cloud Platformを導入して従来の3分の1の時間でセキュリティ脅威に対応

## 主な課題

レガシーインフラのメンテナンスやセキュリティイベントの検出に膨大なリソースを費やしていたにも関わらず、複雑さが原因で顧客が求めるマルチチャネルエクスペリエンスを提供できないことがあった。

## 主な成果

Splunk Cloud Platformによってシステムパフォーマンスに関する実用的なインサイトを取得できるようになり、セキュリティ脅威に短時間で対応できるようになった結果、ビジネスを強固に保護しながらカスタマーエクスペリエンスを向上させることができた。



業種：リテール(小売り)

ソリューション：  
プラットフォーム、セキュリティ

## 今日のスーパーマーケットへの来店客が求めているマルチチャネルエクスペリエンス

世界第8位の小売企業、Carrefour社は、ヨーロッパ、南米、アジアにスーパーマーケットを展開しています。モバイルアプリからの注文でも、オンライン注文品の受け取りでも、顧客がオンラインに求めているのは実店舗と変わらない利便性です。これを理解しているCarrefour社は、オンラインショッピングチャンネル全体のカスタマーエクスペリエンスを向上させるために、クラウドベースサービスの利点も備えたデジタル化戦略を採用しました。

Carrefour社は、Splunk Cloud Platformによって、新しい機能やサービスの開発に集中できる俊敏性を獲得しました。また、セキュリティ管理が簡素化された結果、顧客に安全なショッピングエクスペリエンスを提供できるようになりました。Splunkから得られるリアルタイムのインサイトを活用して、セキュリティ脅威に従来の3分の1の時間で対応できるようになり、インシデントの防止に関する意思決定も適切に行えるようになりました。

## 従来の3分の1の時間でセキュリティイベントに対応

レガシーデータセンターを基盤とする複雑なインフラを運用していたCarrefour社のSOC(セキュリティオペレーションセンター)チームは、これまでシステムの管理に膨大な時間と労力をとられ、マルウェアからビジネスを保護することに集中できていませんでした。Splunk Cloud Platformは、セキュリティ分析を一元化し、いくつかのデータソースを統合することによって、インシデントにリアルタイムで対応するSOCチームの能力を大幅に高めました。

「Splunk Cloud Platformは、当社が導入しているウイルス対策ソフトウェアであれ、エンドポイント検出/対応ツールであれ、あらゆるソースからのログを処理します」と、Carrefour社のSOCアナリストであるRomaric Ducloux氏は言います。「アラートを生成してチケットをオープンし、オンコールSOCアナリストに通知するSplunkは、私たちのセキュリティ運用の基盤です」と同氏は評価します。

クラウドモデルを採用したことで、セキュリティ運用とインフラの管理をSplunkに委ねられるようになったCarrefour社のSOCチームは、アプリケーション管理や脅威分析、セキュリティの調査に集中する時間を多く持てるようになりました。今ではインシデントが発生するとすぐに対応し、システムや顧客に損害や影響が及ぶのを未然に防ぐことができます。侵害の発生に至った場合も、問題箇所に関する情報を収集できるため、後でシステムを改善することができます。

最終的にチームは、インシデントに従来の3分の1の時間で対応できるようになりました。Ducloux氏は、「Splunk Cloud Platformによって、顧客がいつも安全にショッピングできるよう万全を期すという最も重要な業務に再び集中できるようになりました」と述べています。

## データ活用の成果

**3分の1**

従来の3分の1の時間で脅威に対応

**100億ユーロ**

2026年までの  
eコマース予想売上  
高は104.5億ドル

**時間の有効活用**

より価値の高い業務に  
取り組む時間を確保

## Splunkがもたらすイノベーションとレジリエンス

Carrefour社は、Splunk CloudがSOCチーム全体にとって、つまり技術エキスパートにも、ビジネスアナリストにもアクセスしやすい点を評価しています。セキュリティイベントの調査に使用する言語が習得しやすい上に、強力な分析も実行できるため、SOCチームはサイバー攻撃者の戦術や手法、使われているツールについての詳細なインテリジェンスを迅速にマイニングできます。このため、将来のインシデントに対しても強力な防御体制を築くことができます。

「Splunkは非常に大きな価値をもたらしています。ルールの作成や、複雑すぎて苦勞するツールに時間を浪費せずに、検出ユースケースの分析から得られたインサイトを最大限に活用できるようになりました」とDucloux氏は語ります。さらにビジネスユーザーも、セキュリティイベントが起きた際に、発生中の事象に関するシステムレベルと運用レベルの全情報にフルアクセスできるため、エキスパートに頼らずに調査を行って、組織全体に対しアラートを生成できるようになりました。

ログとデータを一段と深く掘り下げるため、SOCチームはSplunkbase Appも活用しています。Splunkbase Appを使用すればいくつものソースをシームレスに統合できるため、SaaSプロキシの適用といった業務を最小限の労力で行えます。今やCarrefour社は、レジリエンスと効率的なセキュリティ運用を維持しながら、顧客に革新的な新機能やサービスを提供できるという自信にあふれています。



Splunkは非常に大きな価値をもたらしています。ルールの作成や、複雑すぎて苦勞するツールに時間を浪費せずに、検出ユースケースの分析から得られたインサイトを最大限に活用できるようになりました”

Romarc Ducloux氏、Carrefour社  
SOCアナリスト



Splunk Cloud Platformは、私たちのセキュリティ運用の基盤です”

Romarc Ducloux氏、Carrefour社  
SOCアナリスト

## eコマースでの売り上げを100億ユーロにするための拡張

Carrefour社は、2026年までにeコマースによる売り上げを3倍の100億ユーロ(104.5億ドル)にまで伸ばし、世界的に拡大するという野心的な計画を持っています。

容易に拡張して、複数の国にまたがるグローバルなSOCの基盤とすることができ、新しい国や市場からの増え続けるデータやログを管理できるSplunk Cloud Platformは、革新に満ちた将来の土台となるセキュリティ基盤を維持するために必要なインサイトと俊敏性をCarrefour社にもたらし続けます。

Splunkの無料トライアルをダウンロードするか、Splunk Cloudの無料トライアルをお試しください。Splunkは、クラウドかオンプレミスか、また組織の規模の大小などにかかわらず、お客様のニーズに最適な展開モデルでご利用いただけます。



営業へのお問い合わせはこちら：[https://www.splunk.com/ja\\_jp/talk-to-sales.html](https://www.splunk.com/ja_jp/talk-to-sales.html)  
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階

[www.splunk.com/ja\\_jp](http://www.splunk.com/ja_jp)  
[splunkjp@splunk.com](mailto:splunkjp@splunk.com)