splunk> a CISCO company

お客様事例

GMOインターネット、Splunk EnterpriseとSplunk Enterprise Securityによる SOC運用高度化。SplunkとAIを組み合わせた不正検知により、アナリストの業務負荷を軽減。

課題

複数の監視ツールを組み合わせた従来の運用では、障害原因の特定や対応が後手に回ることが多く、運用の効率化が急務だった。特に、エンドユーザーサービスの品質向上とインシデント未然防止の両立が求められており、そのためにはリアルタイムなログ検知と高い拡張性を備えた統合的な監視基盤の導入が必要だった。

導入効果

データ分析プラットフォームのSplunk Enterprise および市場をリードするSIEMであるSplunk Enterprise Securityの導入により、アラート検知から詳細分析、遮断対応までを一気通貫で実施可能に。特にWindowsログ分析においては判断が標準化され、セキュリティアナリストの業務負荷が大幅に軽減。さらに、AIとの連携による非構造化データの異常検知や外部ツールとの自動連携を実現し、運用効率と対応精度が向上した。

GMO INTERNET

業種・業界：オンラインサービス

ソリューション：セキュリティ、IT 運用

製品：Splunk Enterprise Security

GMOインターネットの高度なセキュリティ運用を支えるSplunk

GMOインターネットグループは、「すべての人にインターネット（Internet for Everyone）」という理念のもと、ドメイン、クラウドホスティング、インターネット接続、セキュリティといったインターネットインフラ事業をグローバルに展開しています。2025年1月には、グループの再編によりインフラ事業を承継した新会社として、GMOインターネット株式会社が発足しました。

中でも北九州拠点は、24時間365日体制でインターネットインフラサービスの運用保守を担う重要な拠点です。開発、インフラ、セキュリティ領域にまたがるエンジニアが数多く在籍し、2025年には新たにデータ・AI領域のチームも発足。技術的挑戦と高度なオペレーションの最前線として、グループ内外から注目を集めています。

GMOインターネットでは、「なくならない、なくてはならない」インターネットインフラを提供し続けるために、セキュリティには重点的に注力しています。グループ全体でパートナーとの協業体制のもと、日々進化する脅威に立ち向かう体制を築いています。2016年にログ収集基盤としてSplunk Enterpriseを導入、その後、2021年にSplunk Enterprise Securityの追加ライセンスも導入し、インシデントレスポンスを担うSIEM基盤として本格活用しています。

成果

- Splunk Enterprise Securityにより誤検知・過検知が軽減し、アナリストの業務負荷が軽減
- WAF・ブラックリスト連携によりIP遮断や通知などの対処をSplunk経由で自動連携
- LLMとSplunkを連携し不正兆候を早期に可視化

エンドユーザー向けサービスの品質向上が急務 ログ収集基盤からSplunkの活用を開始

GMOインターネットの主力事業であるインターネットサービスの運用について、同社 システム本部 CISO Office SOCチーム リーダーの濱本 直樹 氏は、「複数の監視ツールを組み合わせて運用していたため、障害の原因が『見えるもの』と『見えないもの』に分かれ、対応が後手に回るケースも少なくありませんでした」と話します。かねてよりパフォーマンス監視や障害対応に課題を抱えており、特に、障害対応は人海戦術に依存する場面が多く、運用の効率化が急務となっていました。

GMOインターネットが重視したのは、単なる機器やネットワークの監視にとどまらず、エンドユーザー向けサービスそのものの品質を向上させるためのパフォーマンス監視です。障害を未然に防ぐだけでなく、サービスの価値そのものを高めていく視点が求められていました。

こうした背景を受けて、セキュリティ上のインシデントが起きないようセキュリティを強化する目的で、2021年にSplunk Enterpriseの導入を開始。当初はログ収集基盤としての活用から始め、段階的に活用範囲を拡張していきました。「導入の決め手となったのは、Splunkの『リアルタイムでのログ検知』や『高い拡張性』でした」（濱本氏）。

そして、導入後には、より高度なセキュリティ運用を可能にするため、「Splunk Enterprise Security」の追加ライセンスも導入し、本格的なSIEM環境を構築しました。

「Splunkの拡張に際しては、他にも競合のデータ監視プラットフォームを比較検討しましたが、すでにツールを使い慣れていることによる将来的な学習コストや自社での運用性、相関分析ルールの整備状況といった観点から、Splunk EnterpriseおよびSplunk Enterprise Securityが最も適していると判断しました」と濱本氏は話す。特に、攻撃手法が日進月歩で進化する中で、Splunk Enterprise Securityの提供する検知ロジックの整備、アップデートの頻度の高さは、ルール作成・運用にかかる負荷を大幅に軽減してくれる要素として高く評価されました。

LLMを活用し非構造化データから特徴量を抽出
異常検知に活用

現在GMOインターネットでは、Splunkを中心に「SIEM」「不正検知・データマイニング」「IT運用管理」「SRE」など、複数のユースケースでデータ活用が進められています。中でも注力しているのが、SOC（Security Operation Center）チームによるSIEM運用と、SplunkとAIを組み合わせた先進的な不正検知・データマイニングの取り組みです。

SOCチームは現在8名体制で、そのうちSplunkのログ監視、分析を専門に担うメンバーは3名です。収集対象のログは、社内外の多数のシステムから構成されており、「WAF（Web Application Firewall）のログやOSレベルのサーバーログ、アプリケーションログ、IPアドレスの挙動まで幅広くカバーしています」と濱本氏は話します。そして、24時間365日体制での初動対応を担うメンバーがアラートを検知し、アナリストが詳細なログ分析を行うフローを構築しています。

分析では、Splunk Enterprise Securityの提供する相関ルールだけでなく、自社で独自作成したルールも併用しており、運用効率を高める鍵となっています。外部攻撃に対しては、GMOインターネットグループ内でセキュリティ事業を提供する「GMOサイバーセキュリティ by イエラエ」のSOCサービスとも連携しており、WAFで防ぎ切れなかった攻撃の痕跡などは、社内のSplunkログ分析で捕捉。遮断対象のIPアドレスはブラックリストに自動登録され、再発防止にもつながっています。

「外部からWAFをすり抜けて内部に侵入し、内部で横展開するような動きを早く検知するためには、社内のネットワーク環境に精通したメンバーが担当した方が効果的、効率的だとの考えからこのような体制を敷いています」（濱本氏）。

> アナリストは日々、多種多様なログを見ています。新たな脆弱性や攻撃が出現する中で、Splunkは、アナリストが足りないワークロード、リソースをカバーしてくれる製品だと思っています。
>
> GMOインターネット株式会社
システム本部 CISO Office
SOCチーム リーダー
濱本 直樹 氏

さらにユニークなのが、SplunkとGPU環境を備えたコンテナ基盤を連携させたAI活用の実践です。LLM（大規模言語モデル）を活用して非構造化データから特徴量を抽出し、それを用いた異常検知を行っています。「データ分析基盤としてDSDL（データ・サイエンス・ディープ・ラーニング）とSplunkを接続し、複雑なログパターンや入会・利用といったサービス行動の裏にある潜在的な不正兆候を可視化しています」と濱本氏は述べ、検知結果はレポート形式で事業部門に提供され、実際の対応に役立てられているということです。

こうした運用には、Splunkの強みである「オープン性」も活かされています。同社では、WAFやブラックリスト、その他の分析ツールとSplunkをAPI経由で連携。Splunk上のカスタムサーチ機能により、抽出されたIPアドレスなどの情報を即座に他ツールに連携し、遮断やアラート処理が自動化されています。濱本氏は、「Pythonによる連携も柔軟で、ツール間のシームレスな連携が高度な運用を支えています」と話しました。

Splunk Enterprise Securityがログ分析の判断を標準化
アナリストの業務負荷は大きく軽減

Splunk EnterpriseとSplunk Enterprise Securityをフル活用しているGMOインターネットですが、現在の運用に至るまでには多くの試行錯誤がありました。特にSplunk Enterprise Securityの活用では、「ESCU（Enterprise Security Content Update）」という相関分析ルール群の取捨選択に注力したということです。「すべてを有効化するのではなく、自社の環境に適したルールを見極めて適用する必要があり、毎週、毎月のように提供される新しいルールの中から、定期的なチューニング作業を行っています」（濱本氏）。

Splunk Enterprise Securityの導入により、セキュリティアナリストの業務負荷は大きく軽減されました。「特に、Windowsログの分析においては、ログ構造が複雑で、誤検知や過検知が発生しやすい傾向がありましたが、Splunk Enterprise Securityのルールセットがその判断を標準化してくれています」と濱本氏は話します。黒に近いグレーなログをいかに絞り込み、アナリストが「判断すべき対象」に集中できるかという観点で、大きな成果を挙げています。

また、濱本氏は「形式がバラバラなログを統一的な形式（CIM）に整えることで、Splunk Enterprise Securityによる相関分析の効果を最大限に引き出しています」と述べます。これは、Splunkの柔軟なデータ処理能力に支えられており、導入当初から丁寧に環境を整備してきた成果ということができるでしょう。

定量的な面では、アラート処理の効率化や、誤検知の減少、アナリスト1人あたりの対応件数の増加といった効果がみられます。社内でも「セキュリティ維持にSplunkはなくてはならないツール」と認識されるまでに定着しており、運用基盤としての信頼性は高く評価されています。

Splunkのさらなる活用に向けた
「ログ対象範囲拡張」「AI連携の精度向上」「自動化」の構想

今後、GMOインターネットではSplunkをさらに進化させる3つの方向性を描いています。「1つは、ログの対象範囲とデータ量を拡張し、より多くのシステムやサービスの挙動を包括的に可視化することです」と濱本氏は述べます。2つめは、AI連携の精度向上です。「より精緻な特徴量を用いた分析により、事前検知の精度を高めたいと考えています」（濱本氏）。そして3つめは、各種ソリューションとの連携強化を通じたセキュリティ対応の自動化と運用効率の追求です。

こうした構想に対し、同社はSplunkを「戦略的なセキュリティパートナー」として位置づけています。「営業担当者やSEとのやりとりの中で、アイデアベースの相談にも親身に応じてもらえる体制に信頼を寄せています。こうした関係性があってこそ、自社に適した高度な活用が実現できているのです」と濱本氏は話しました。

その上で、これからSplunk導入を検討する企業に対しては、「やりたいことを明確にし、自社のセキュリティで重視すべきことを明らかにした上で、スモールスタートで導入していくこと」が重要だということです。濱本氏は「多機能な製品だからこそ、目的を定めて段階的に活用を深めることが、真の価値を引き出す近道になります」と締めくくりました。

Splunk無料トライアルまたはCloudトライアルをダウンロードしてお試しください。Splunkは、クラウドとオンプレミスのオプションを備えており、ご利用容量の規模に応じて、ご要望に合うデプロイメントモデルをお選び頂けます。

splunk> a CISCO company

営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html

www.splunk.com/ja_jp
splunkjp@splunk.com

Splunk, Splunk>およびTurn Data Into Doingは、米国およびその他の国におけるSplunk Inc.の商標または登録商標です。
他のすべてのブランド名、製品名、もしくは商標は、それぞれの所有者に帰属します。© 2025 Splunk Inc. 無断複写・転載を禁じます。

25_CMP_customer-story_GMO_v1_1010