# マネージドセキュリティサービスで正確さを高め、工数を減らす

## セキュリティログを深く掘り下げるのではなく、ビジネスへの付加価値を高めることに集中する

アプリケーションとクラウドネイティブインフラストラクチャを攻撃者や内部の脅威から確実に保護することは、非常に困難です。その上、継続的にそれらすべてを監視できる人材を発掘し雇用することも憂慮すべき問題です。

Threat Stack は現在、F5 ソリューションとなり、F5® Distributed Cloud App Infrastructure Protection（AIP）Managed Security Services に製品名称変更いたしました。Distributed Cloud App Infrastructure Protection（AIP）Managed Security Services はセキュリティインシデントやリスクの高い動作を特定して対応するために必要な時間とリソースを削減します。

F5 のセキュリティオペレーションセンター（SOC）は 365 日 24 時間体制でお客様のクラウドを継続的に監視し、お客様固有の環境のコンテキスト内での疑わしいアクティビティを詳細に分析・検証し、それ基づいたアラートに優先順位を付けます。脅威の検出時にできるだけ迅速に対応できるよう、SOC アナリストは 24 時間体制で深刻度 1 のアラートをレビューします。SOC アナリストは、お客様に代わって調査を行い、修復に向けた実用的な推奨事項を提供します。

## 提供内容

- アクティブなアラート監視とエスカレーション
- インシデントの調査
- 修復に向けた推奨事項とガイダンス
- 深刻度 1 のアラートの継続的レビュー
- 365 日 24 時間体制の対応

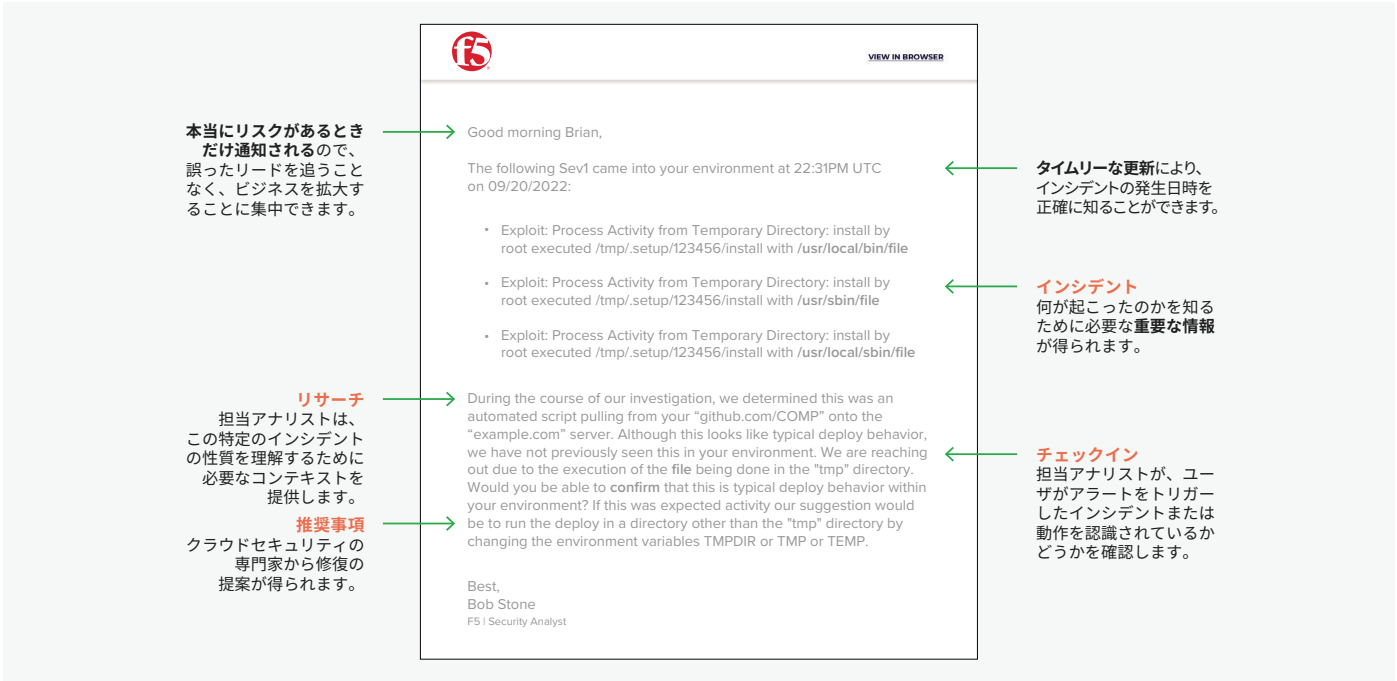
# SOC の事例

Distributed Cloud AIP Managed Security Services の SOC は、実際に発生している脅威を定期的にキャッチし、そのいくつかをブログを通して世界に発信しています。ブログでは、発見した新種のマルウェア、クラウド管理コンソールとホストにまたがる侵入、Docker クリプトジャッキングのエクスプロイトについて説明しています。

### 機能


# 脅威に関する通知の内容

脅威が検出・検証されると、Distributed Cloud AIP Managed Security Services の SOC チームメンバーは、すぐに修復の必要があることを示す検出結果、コンテキスト、そして、脅威への推奨事項をメールで通知します。メールレポートの例を次に示します。



## Threat Stack は、F5 ソリューションとなりました

Threat Stack は、現在、F5 ソリューションの一部となり、F5 Distributed Cloud App Infrastructure Protection（AIP）と製品名称を変更いたしました。このソリューション、当社のセキュリティオペレーションセンター（Distributed Cloud AIP Managed Security Services と Distributed Cloud AIP Insights を含む）などの詳細については、クラウドセキュリティやコンプライアンスの専門家にお問い合わせください。

**当社の専門家がクラウドセキュリティに関する懸念を払拭しますので、お客様は安心して業務に専念できます。詳細またはデモのご予約については、今すぐ当社の Web サイトでご確認ください。**


DC 10.2022 | JOB-CODE-DS-950846235-AIP-Managed-Security-Services