Insert Partner Logo
Size to be visually equal to F5 Logo.
Align to left edge and center vertically.

データシート

監視と分析：インサイトサービス

F5 の専門家による継続的な分析により、セキュリティ対策を長期的に改善する

パブリッククラウド環境を保護するには、従来のインフラストラクチャ保護とは**根本的に異なるアプローチが必要不可欠です。**しかし、どこから手をつければよいのか、事後対応型リスク管理から、事前対応型スタンスに移行するにはどうすればよいのか、アプローチを理解することは簡単ではありません。

F5 製品の一員となった Threat Stack、現在の F5® Distributed Cloud App Infrastructure Protection（AIP）Insights サービスでは、実際のインフラストラクチャのリスクを基に Cloud SecOps 戦略を策定する上で大変有効です。Distributed Cloud AIP Insights は、実装するテクノロジのリストを提供するコンサルティングサービスやフレームワークとは異なり、Distributed Cloud AIP ソリューションから取得したデータと分析を基に、当社の専門セキュリティアナリストがお客様向けにキュレーションいたします。サービスの一環として、書面による推奨事項と戦略コーチングセッションをご提供いたしますので、お客様は、全体的なセキュリティ体制の改善に向けて優先順位を決定し、目標を設定することが可能となります。

提供内容

- トレンド、詳細な検出、脆弱性、および異常に関するレポート
- 高リスクの動作削減に向けた推奨事項
- Cloud SecOps 戦略セッションと継続的なコーチング

機能

1. 担当アナリストが毎月、お客様のクラウド環境からいくつかの KPI データを取得
2. 担当アナリストがデータをレビューし、お客様のインフラストラクチャの脆弱性を調査
3. 担当アナリストがレポートを作成し、お客様が積極的にリスクを軽減できるようにいたします

主な指標

Distributed Cloud AIP Insights のレポートは、お客様のインフラストラクチャのあらゆる側面を分析し、次のような SecOps の成熟度達成をご支援いたします。

- ネットワークアクティビティ
- AWS セキュリティ
- ファイルの動作とユーザアクティビティの管理
- 脆弱性評価

Distributed Cloud AIP Insights レポートの一部から抜粋した、受け取る可能のある種類のインサイトのサンプルを次に示します。

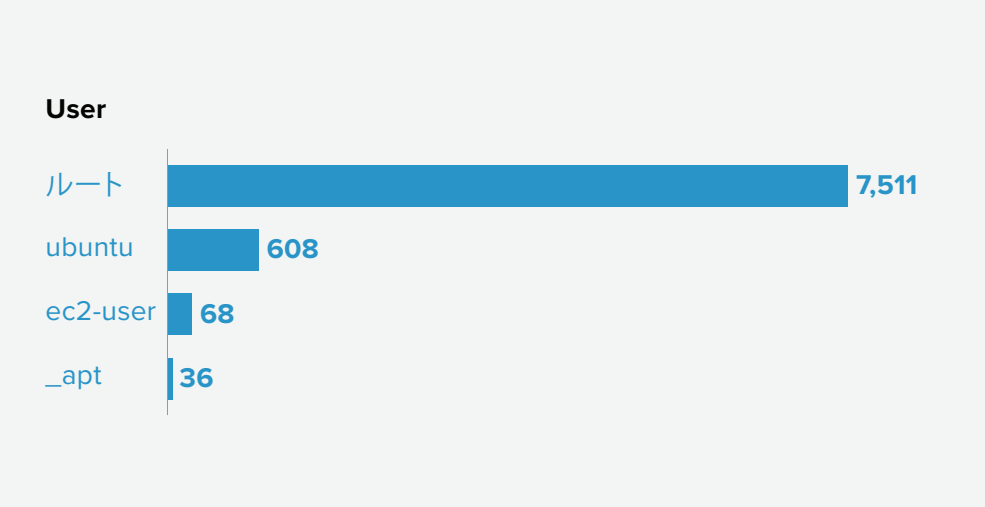

図 1：**ユーザ**：ルート - ユーザアクティビティ管理レポート - 上位 4 つのユーザアクティビティ

観察結果

ルートユーザが過剰に使用されています。

危険である理由

アクティビティのタイプと頻度によっては、この動作は自動化されたアクティビティに関連している可能性があります。

修復の手順

ユーザとサービスに適切な権限を付与し、ルート権限に依存しないように設定します。そうすることで、これらのタイプのアクティビティを実行するためにスコープ指定のユーザを作成できます。

AWS グループ	AWS サービス	t6MH	Uh20gn	josh@biz.com	ロールセッション	fN9h
ストレージ	s3.amazonaws.com	285	367	675	3,629	7,934
	elasticfilesystem.ama...				19	
セキュリティアイデンティコンプライアンス	sta.amazonaws.com		1,528			
	kms.amazonaws.com			36	395	16
	iam.amazonaws.com			12	54	
	signin.amazonaws.com	3		11		
データベース	rds.amazonaws.com				200	
	elasticache.amazona...				100	
	redshift.amazonaws.c...				100	
	dynamab.amazonaws...				50	

図 2: CloudTrail：ユーザ別 AWS アクティビティ

観察結果

RoleSession ユーザが RDS サービスにアクセスしており、それには顧客データが含まれている可能性があります。

危険の理由

特定の AWS サービスにアクセスしているユーザを可視化できないため、インフラストラクチャが脆弱になります。これは、過剰な権限設定である可能性を示します。

修正の手順

最小権限の原則に従います。ユーザに必要なアクセスのみを許可し、AWS で権限昇格のインスタンスをすべて追跡します。

Serverity	Image ID	CVE	CVSS Score
High	ami-6057e21a	CVE-2015-2806	10,000
		CVE-2017-16844	10,000
		CVE-2015-2328	7,500
		CVE-2016-3191	7,500
	ami-c58c1dd3	CVE-2015-2806	10,000
		CVE-2017-16844	10,000
		CVE-2015-2328	7,500
		CVE-2016-3191	7,500

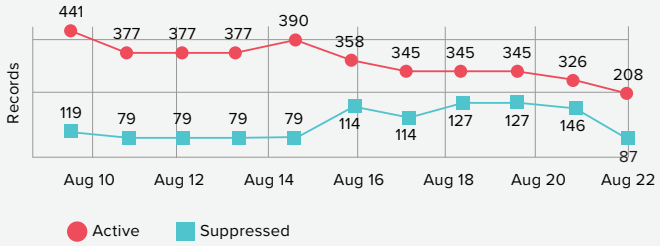

図 3：アクティブな脆弱性とトレンドの CVE

観察結果

パッチが適用されていないサーバーは、深刻度の高い脆弱性が生じています

危険の理由

特にインターネットに接続されているサーバーの場合、脆弱性が深刻であればあるほど、悪用される可能性が高くなります。

修復の手順

パッチ適用プロセスを標準化・自動化します。

Threat Stack：現在は F5 ソリューションの一部です

Threat Stack は、F5 Distributed Cloud App Infrastructure Protection（AIP）に製品名称変更いたしました。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ぜひお問い合わせください。

お客様のクラウドセキュリティに関する懸念が発生した場合、F5 の専門家がすぐに対応いたしますので、お客様は安心してご担当業務に専念いただけます。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 12.2022 | JOB-CODE-DS-950864156-AIP-Insights