CROWDSTRIKE

2023年版 クラウドリスクレポート：

クラウドを標的にする攻撃者とその戦術を知る

95%

クラウドエクスプロイトが増加

3倍

クラウドを意識した脅威アクターが関与するケースが増加

攻撃者はクラウド TTP を先鋭化

COZY BEAR（ロシア由来）、SCATTERED SPIDER（サイバー犯罪：eCrime）、LABYRINTH CHOLLIMA（北朝鮮由来）、COSMIC WOLF（トルコ由来）などをはじめとする多くの攻撃者グループはより巧妙になっており、クラウドを標的にすることに注力しています。

COZY BEAR

- **発信国：**ロシア連邦
- **戦術：**悪意のあるツールを使用してクラウドサービスを改ざん

この攻撃者についての詳細およびグローバルなクラウド環境に与える影響についてご確認ください。

詳細情報

SCATTERED SPIDER

- **発信国：**不明
- **戦術：**クラウドステージング環境からのランサムウェアを展開

このサイバー犯罪（eCrime）攻撃者とクラウド環境を標的にする手法を知る。

詳細情報

LABYRINTH CHOLLIMA

- **発信国：**北朝鮮
- **戦術：**クラウドリソースを使用して悪意のあるマクロを含む文書を配信

この危険な攻撃者がとのようにクラウド環境全体に損害を与えているのかをご覧ください。

詳細情報

COSMIC WOLF

- **発信国：**トルコ
- **戦術：**クラウド環境に保存されている被害者データを狙う

この標的型攻撃者がクラウドを攻撃する方法をご確認ください。

詳細情報

アイデンティティは重要なクラウドアクセスポイント

脅威アクターはクラウドでアイデンティティを活用する新たな方法を模索

43%

攻撃者は有効なアカウントの使用を増やしています。観察されたクラウド侵入の**43%**で初期アクセスを獲得する際に使用されたのは、正規のアカウントでした。*

67%

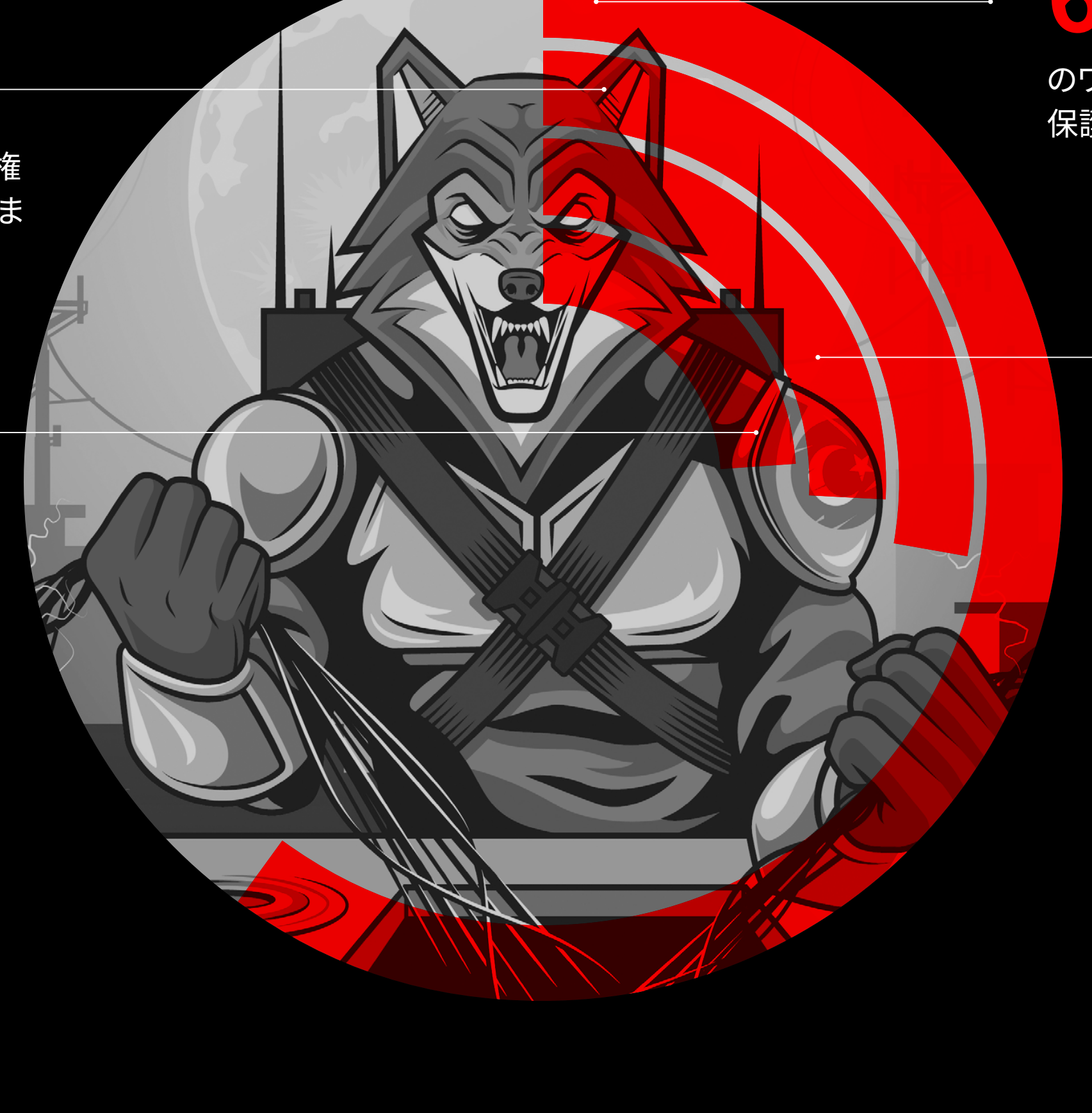
クラウドセキュリティインシデントの67%で、クラウドストライクはアイデンティティ/アクセス管理（IAM）ロールが必要以上に権限昇格されていたことを発見しました。これは、攻撃者がロールを破壊して環境を侵害し、ラテラルムーブメントした可能性を示しています。*

47%

重大な設定ミスの半数近く（47%）は、アイデンティティと権限のハイジーンの悪さに関連。*

ヒューマンエラーによりクラウドリスクが増大

クラウドの設定ミスは、クラウド環境をリスクにさらすギャップ、エラー、脆弱性の原因になります。これはセキュリティ設定が不適切に選択されたり、またはセキュリティ設定がまったく選択されていない場合に発生します。マルチクラウド環境は複雑になる場合もあるため、アカウントに付与された権限が過剰であるか、パブリックアクセスの不適切な構成がされているか、あるいは他の間違いがないかどうかを判断するのが困難なことがあります。



28% のワークロードはルート権限として実行されるか、またはルートに昇格可能*

24% のワークロードはルート権限に類似した機能を所有*

60% のワークロードで、セキュリティ保護が適切に行われていない*

26% のワークロードで Kubernetes Service Account Token を自動化*

貴社のクラウド環境への脅威の詳細をご確認ください。

クラウドストライクの2023年版クラウドリスクレポートをダウンロードする

詳細情報：https://www.crowdstrike.jp/
ソーシャルメディア：Blog | Twitter | LinkedIn | Facebook | Instagram
今すぐ無料トライアルを開始する：https://www.crowdstrike.com/free-trial-guide/

CROWDSTRIKE
Protection that powers you

CrowdStrikeについて

CrowdStrike (Nasdaq: CRWD)、は、サイバーセキュリティのグローバルリーダーであり、エンドポイント、クラウドワークロード、アイデンティティ、データを含む企業におけるリスクを考える上で重要な領域を保護する世界最先端のクラウドネイティブのプラットフォームにより、現代のセキュリティを再定義しています。

CrowdStrike Falcon® プラットフォームは、CrowdStrike Security Cloud およびワールドクラスの AI を搭載し、リアルタイムの攻撃指標、脅威インテリジェンス、進化する攻撃者の戦術、企業全体からの充実したテレメトリを活用して、超高精度の検知、自動化された保護と修復、精鋭による脅威ハンティング、優先付けられた脆弱性の可観測性を提供します。

Falcon プラットフォームは、軽量なシングルエージェント・アーキテクチャを備え、クラウド上に構築されており、迅速かつスケーラブルな展開、優れた保護とパフォーマンスを提供し、複雑さを低減し即座に価値を実現します。

クラウドストライク：包括的な保護でお客様にパワーを

* 出典：Observed cloud security data over a 24-hour evaluation period（24時間評価期間でのクラウドセキュリティデータの観察）