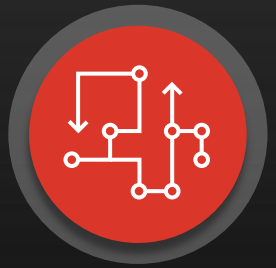
CrowdStrike
Falcon Insight
製品概要

クラウドストライク株式会社

サイバーセキュリティの主な課題

攻撃の高度化



ソリューションの
複雑さ

知識不足

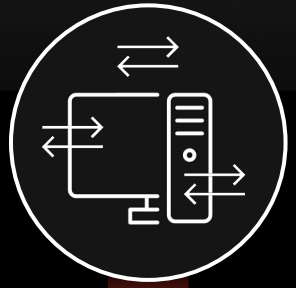
CROWDSTRIKE

今日のセキュリティの維持が困難

オンプレミスでは
進化するニーズに
対応できない

コスト

エージェントの
肥大化

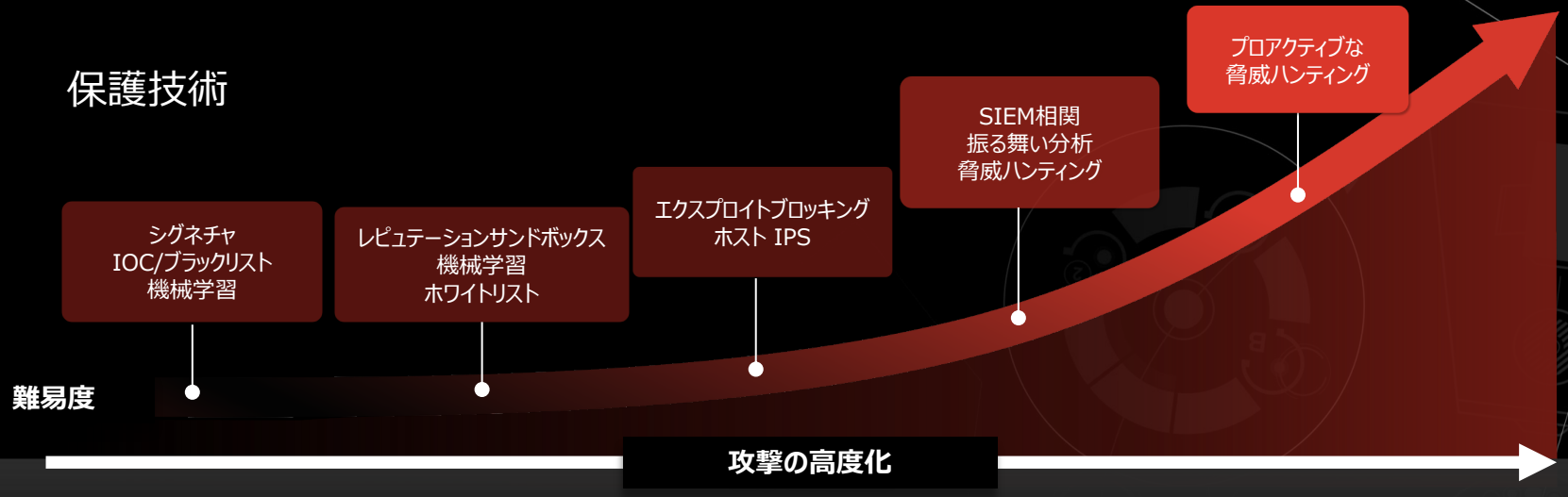


複雑さ

シグネチャが機能しない
–
新しいタイプの攻撃を見逃す

結果なし

攻撃の高度化



ファイルベースのマルウェア

マルウェア　ゼロデイ マルウェア

ファイルレスとエクスプロイト

脆弱性の悪用　ゼロデイ マルウェア　資格情報の盗難

LIVE ATTACKER/INSIDER

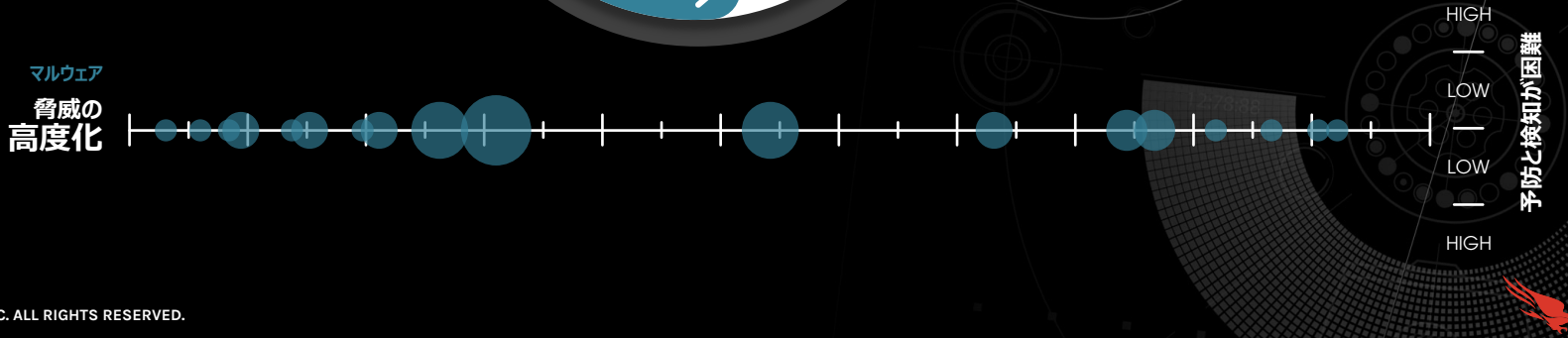
Living off the land　Hands-on keyboard

CROWDSTRIKE

時代遅れの防御

マルウェア

32%



CROWDSTRIKE

時代遅れの防御

マルウェア

32%

完全な
侵害防止が必要

マルウェアフリー

68%

CROWDSTRIKE

攻撃者は素早い

CROWDSTRIKE

最速のサバイバル

先を行くには:

1分 で検知

10分 で調査

60分 で対応

MITRE ATT&CK フェーズ

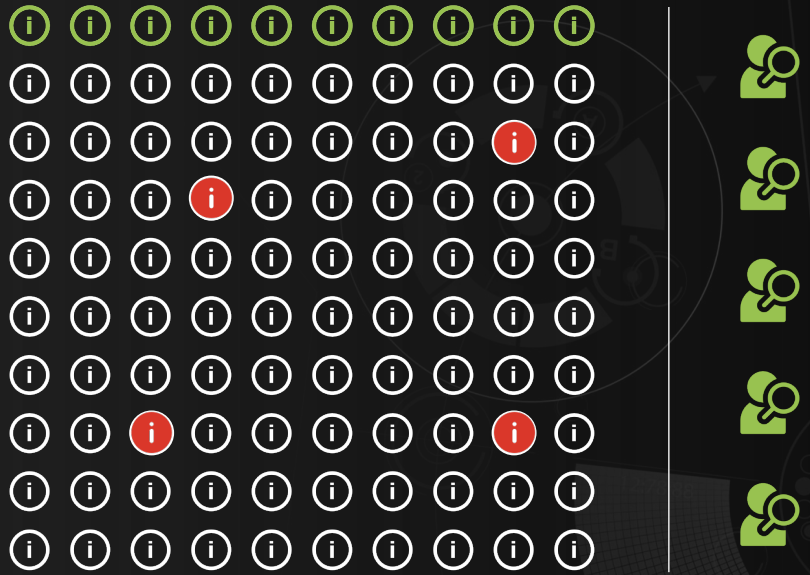
アラートの疲労

セキュリティアナリストは、データと非効率を改善

多くの組織（94%）は、1日あたり500を超えるアラートを受け取ります

アナリスト（人）が処理できるのは10件程度

多くの組織（54%）は、重要なアラートを無視していると考えている



Falcon Insight

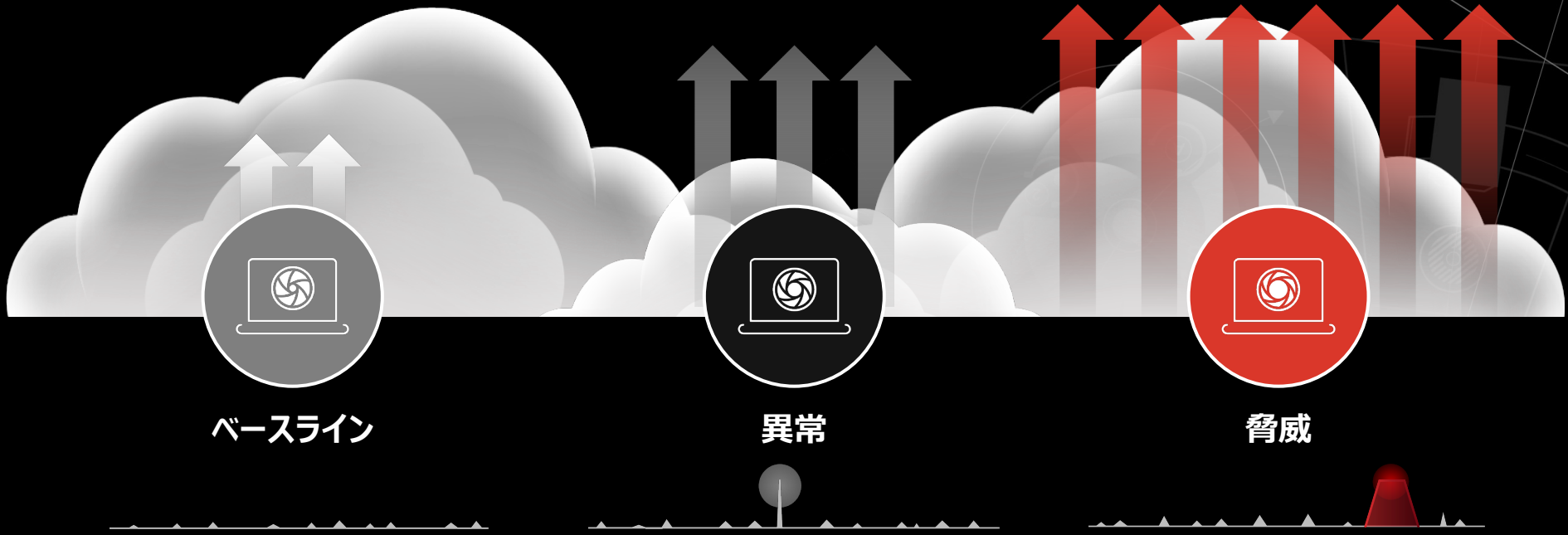
検知時間を短縮

サイレント障害を
防ぐ

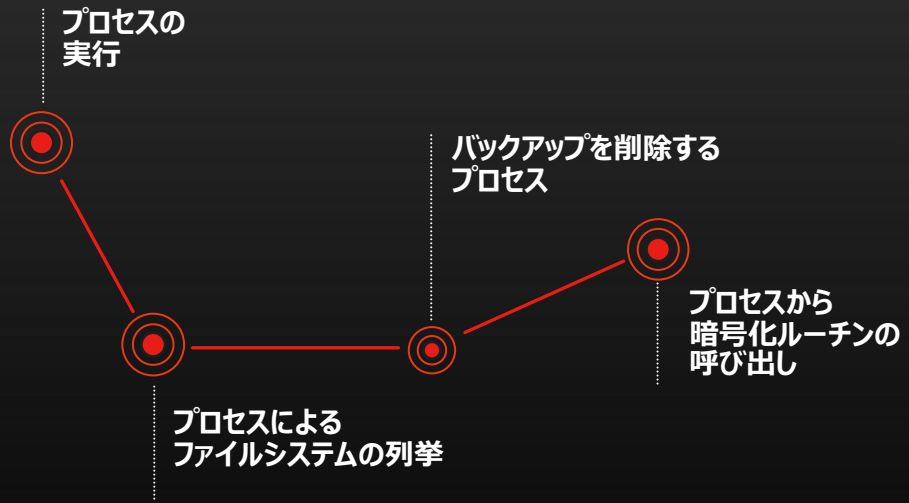
修復時間の短縮

CROWDSTRIKE

未加工のイベントの継続的な取得
SMART FILTERING AGENT と忠実度の高いデータ



インテリジェント EDR – 自動検知
INDICATORS OF ATTACK（IOA）



INDICATORS OF ATTACK

コードの実行、永続性、ステルス、
コマンド制御 横方向の移動

プロアクティブな
INDICATORS OF ATTACK
VS
リアクティブな
INDICATORS OF COMPROMISE

IOCs

マルウェア、シグネチャ、エクスプロイト、
脆弱性、IPアドレス

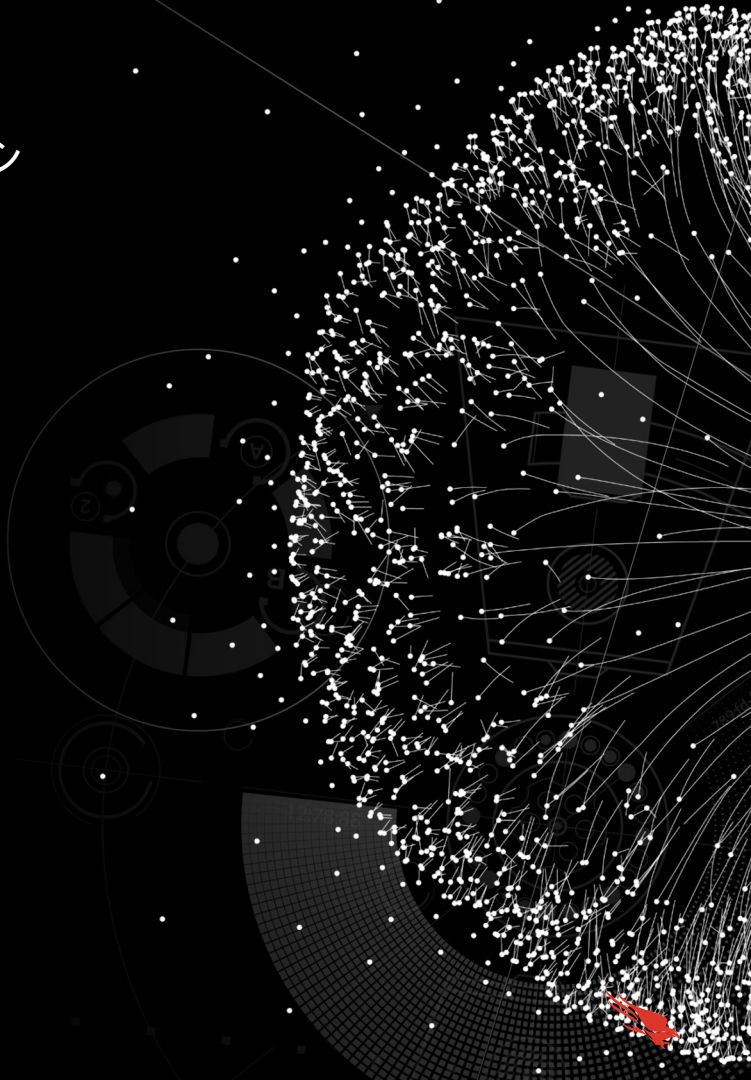
CROWDSTRIKE

自動ハンティングエンジン
Threat Graph

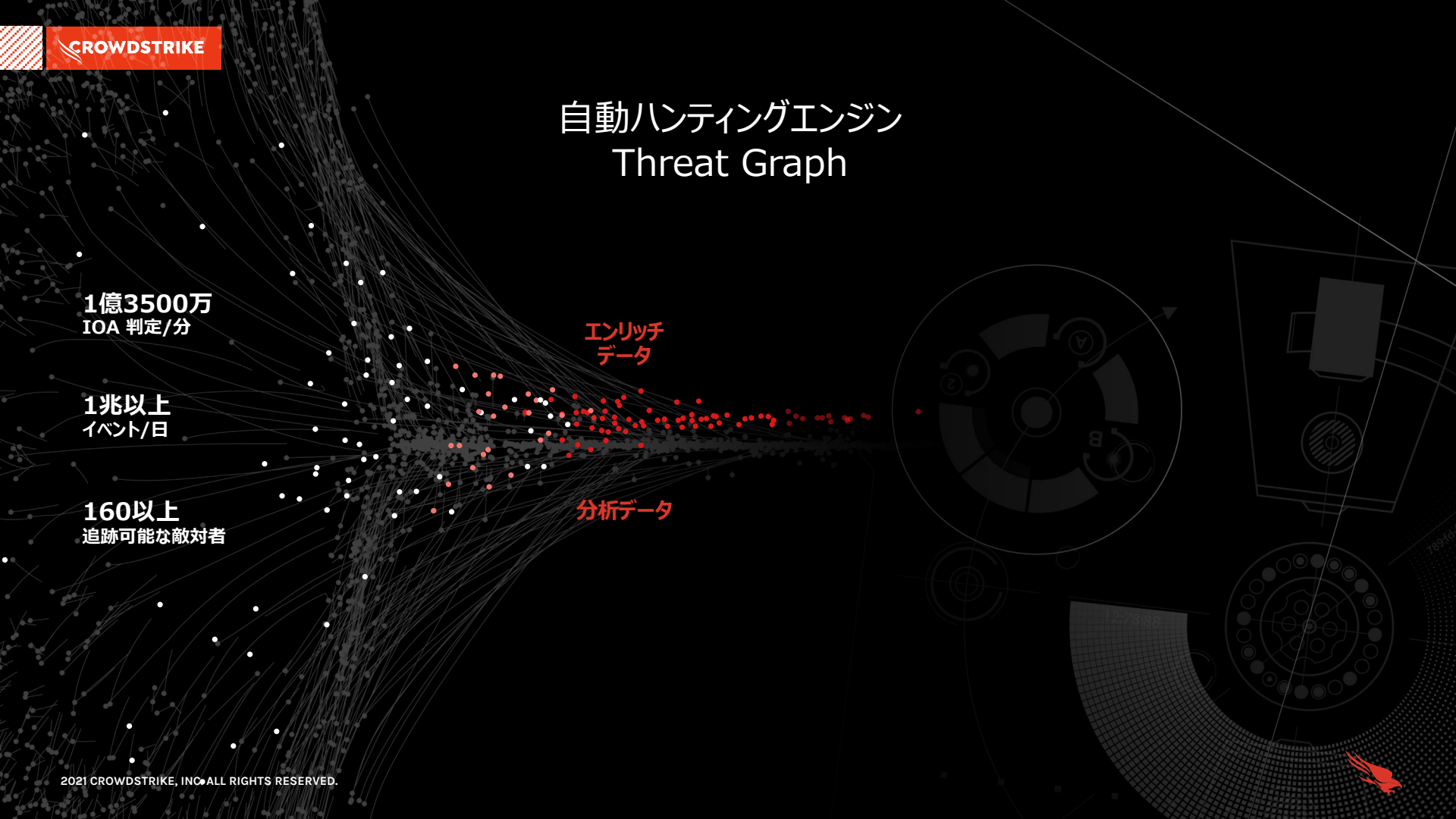
1億3500万
IOA 判定/分

1 兆以上
イベント/日

160以上
追跡可能な敵対者



自動ハンティングエンジン
Threat Graph



CROWDSTRIKE

自動ハンティングエンジン
Threat Graph

1億3500万
IOA 判定/分

1兆以上
イベント/日

160以上
追跡可能な敵対者

エンリッチ
データ

実用的な洞察

分析データ

65,000
潜在的な侵入を阻止

Endpoint Detection And Response
Falcon Insight

ビジネスバリュー

- レスポンスまでの時間を短縮
- SOCの生産性の向上
- 修復までの時間の短縮
- スキルと専門知識の
強化
- リスクの削減
- セキュリティの効率と
効果の向上

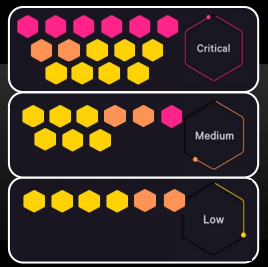
CrowdScore
最も重要なことに素早く焦点を合わせる

データの過不足を排除する

検知
10倍のデータ削除

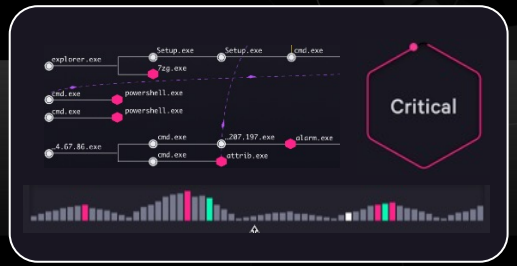
即時にトリアージ

インシデント
優先順位付けと
追加されたコンテキスト



スピード調査

ワークベンチ
調査を
数分単位で合理化



全体像の把握

CrowdScore
明確な脅威レベル
リアルタイムで更新

CROWDSTRIKE

レスポンスと修復を強力にサポート

Falcon Fusion

複雑なワークフローを自動化するための**統合**された拡張可能な

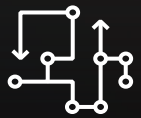
contextual insightsを活用したセキュリティクラウド

複雑なフローの自動化と拡張

インシデントレスポンスと修復の高速化

拡張可能なトリガー

コンテキストに富んだ複雑なフロー



アクティブレスポンス

プラグインフレームワーク

CROWDSTRIKE

ユニークな点

検出、レスポンス、フォレンジックにまたがる継続的で包括的なエンドポイントの可視性を提供する唯一のEDRソリューションにより、見逃しがなく、潜在的な侵害が阻止されます

Falcon Insight

- 未加工のイベントの継続的な取得
- インテリジェント EDR
- CrowdScore
- 属性
- 管理された脅威ハンティング
- 統合された脅威インテリジェンス
- 単一の軽量エージェント

CROWDSTRIKE

Falcon Insightの可視性を展開

Falcon OverWatch
マネージド脅威ハンティング

Falcon Discover
ITハイジーンの可視性を拡張

Falcon Spotlight
脆弱性に対する可視性の拡大

Falcon for Mobile
Mobile EDR

Falcon Device Control
追加のUSBデバイスの可視性

Falcon Discover Cloud and Containers
ハイブリッドクラウドと
プライベートクラウドにおける
可視性の獲得

CROWDSTRIKE

なぜ、
Falcon Insightなのか？

圧倒的な可視性の提供

継続的な未加工のイベントの監視と記録。

エンドポイントで何が起こっているかをリアルタイムまたは遡及的に把握します

サイレント障害からの保護

見逃しがなく、ステルスな悪意のあるアクティビティをすばやく見つけるために必要な可視性と分析機能を提供します

セキュリティ効率の向上

セキュリティ運用を加速します。

検出を自動化します。

アラートの処理に費やす労力を最小限に抑えます。

調査をスピードアップします。

インシデントへの対応と修正にかかる時間を短縮します。

1-10-60 チャレンジの有効化E

1分で検出、10分で調査、60分で修復を可能にするために必要な可視性、自動化、およびワークフローを提供します。

CROWDSTRIKE

エンドポイントプロテクションの実績あるリーダー

リーダー

Gartner

FORRESTER®

IDC

お客様の選択

“CrowdStrike Falcon は、組織のセキュリティツールボックスで最も重要なルールの１つです。”

Gartner peerinsights customers' choice

EDRで4.9/5、エンドポイントプロテクションプラットフォームで4.8/5の最高評価

検証済み

MITRE

AV comparatives

SE Labs

信頼できるお客様

44 / 100
FORTUNE 100社

37 / 100
トップグローバル企業

9 / 20
主要銀行

TOP 10の5
最大の医療提供者

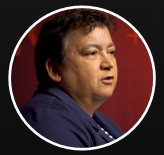
TOP 10の7
最大のエネルギー機関

NIK PATEL
テクノロジーセキュリティサービスの責任者、クレディ・スイス

JOHN VISNESKI
情報セキュリティおよびデータ保護担当ディレクター、Pokémon Company International

ROBERT THOMAS
最高経営責任者、メルセデス-AMGペトロナスモータースポーツ

ROLAND CLOUTIER
シニアVP、チーフセキュリティオフィサー、ADP



DAWN ARMSTRONG
ITディレクター、Virgin Hyperloop One

GUY ALBERTINI
情報。パームビーチ州立大学セキュリティオフィサー