



CROWDSTRIKE

CrowdStrike

Falcon Insight

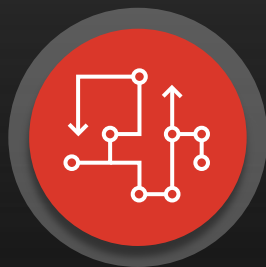
製品概要

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



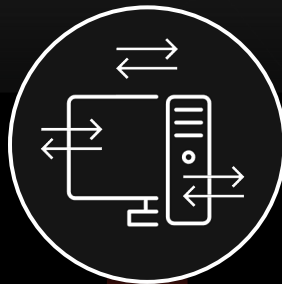
今日のセキュリティの維持が困難

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

保護技術

難易度

シグネチャ
IOC/ブラックリスト
機械学習

レピュテーションサンドボックス
機械学習
ホワイトリスト

エクスプロイトブロッキング
ホスト IPS

SIEM関連
振る舞い分析
脅威ハンティング

プロアクティブな
脅威ハンティング

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

時代遅れの防御

マルウェア
32%



マルウェア
脅威の
高度化



HIGH
—
LOW
—
LOW
—
HIGH

予防と検知が困難

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%

マルウェア
脅威の
高度化

マルウェア以外の攻撃

テロリスト

ハクティビスト/
自警団

サイバー犯罪者

組織的犯罪集団

国家

HIGH
—
LOW
—
LOW
—
HIGH

予防と検知が困難

攻撃者は素早い

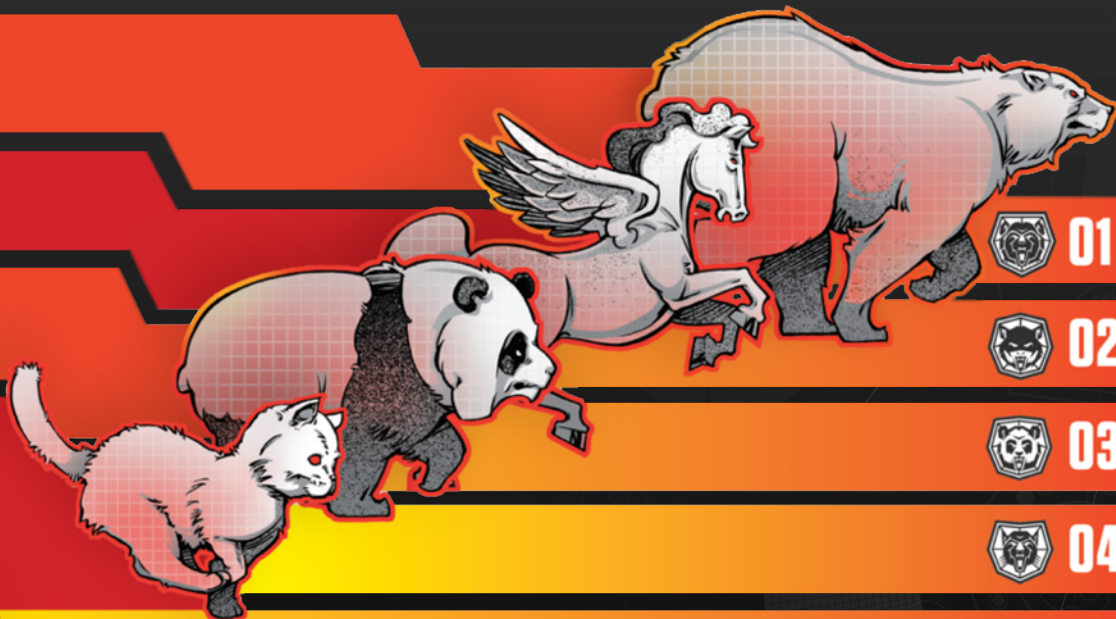
BEAR 00:18:49

GHOLLIMA 02:20:14

PANDA 04:00:26

KITTEN 05:09:04

SPIDER 09:42:23



01



02



03



04



05



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

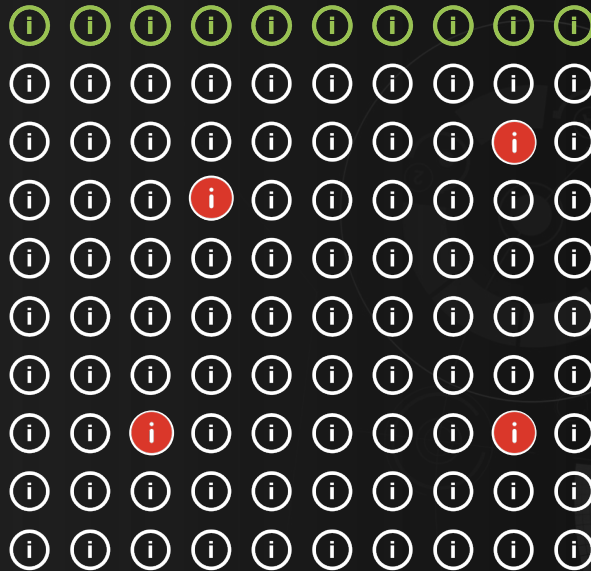
アラートの疲労

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、
重要なアラートを見逃している
と考えている



Falcon Insight



検知時間を短縮



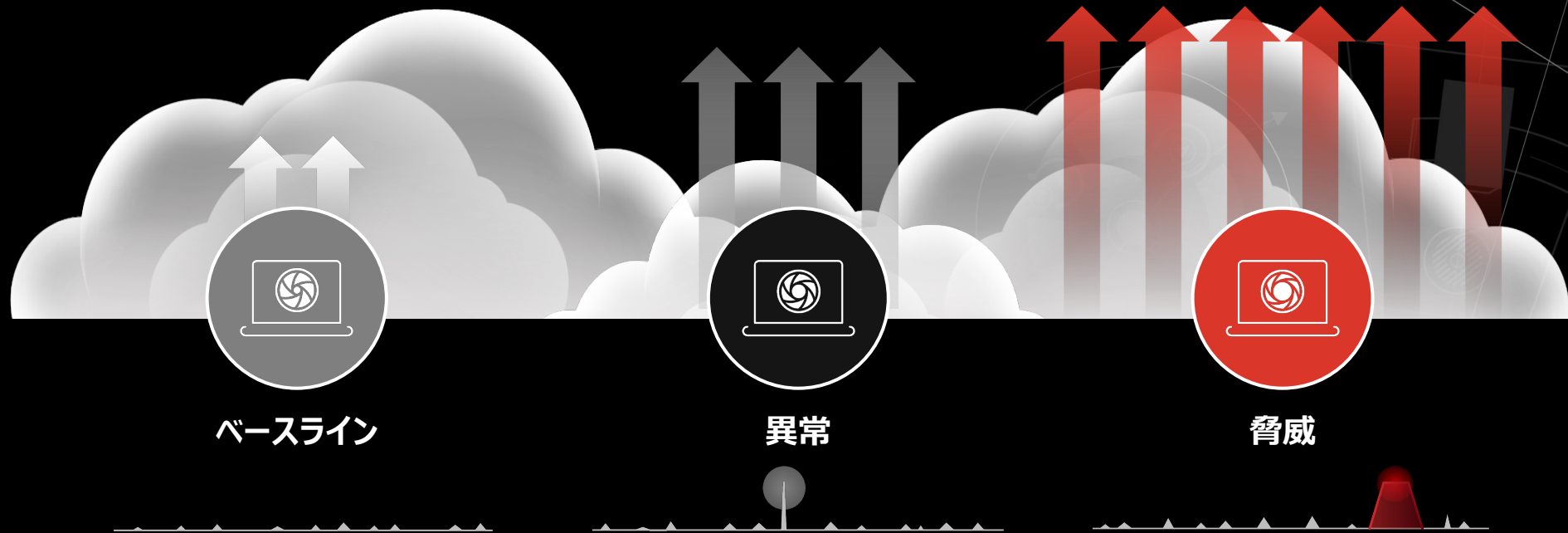
サイレント障害を
防ぐ



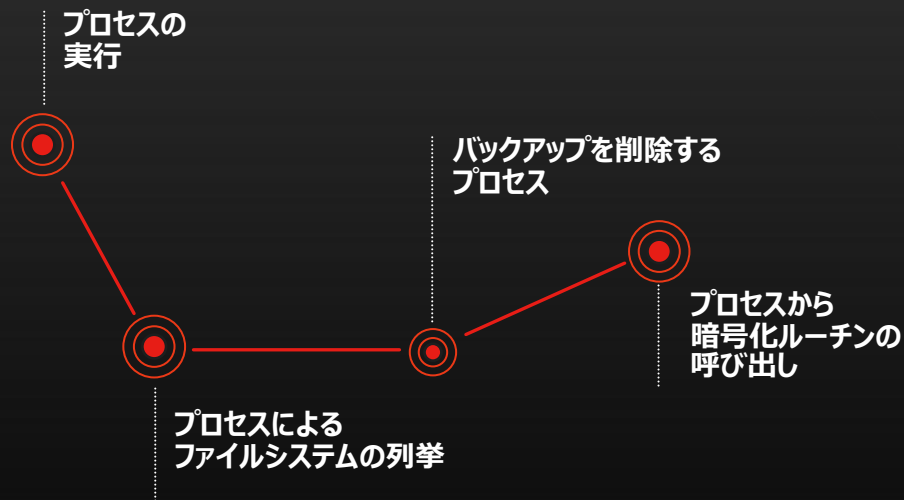
修復時間の短縮



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

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

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

分析データ





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

脅威を防ぐ

積極的な
ハンティング

より早く調査する

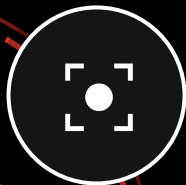


Endpoint Detection And Response Falcon Insight

リアルタイムおよび
履歴検索



すべてを記録



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

リアルタイムレスポンス
と隔離



脅威ハンティング



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

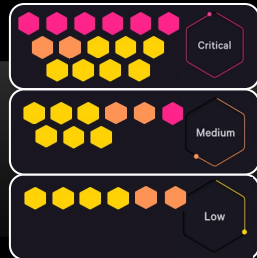
10倍のデータ削除



即時に トライアージ

インシデント

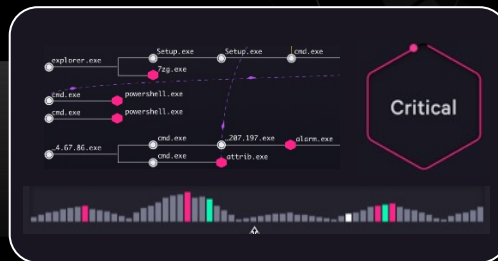
優先順位付けと
追加されたコンテキスト



スピード 調査

ワークベンチ

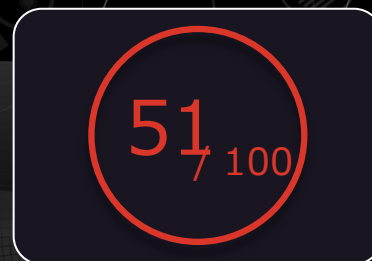
調査を
数分単位で合理化



全体像の 把握

CrowdScore

明確な脅威レベル
リアルタイムで更新



レスポンスと修復を強力にサポート

情報収集



プロセス



ファイルシステム



レジストリ



ネットワーク
アクティビティ



メモリ



OSイベント



プロセスの
停止



ファイルの削除
ブラックリストファイル



レジストリの変更



ネットワーク隔離



カスタムスクリプト

アクションを起こす





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

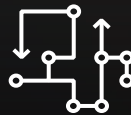
インシデント
レスポンスと
修復の高速化



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



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



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

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き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

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。



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。”



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

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and the GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights' Choice constitutes the subjective opinions of individual end-user reviewers, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. Gartner Peer Insights' Voice of the Customer: Endpoint Detection and Response Solutions, 31 March 2020 and Gartner Peer Insights' Voice of the Customer: Endpoint Protection Platforms, Peer Contributors, 13 October 2021. <https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/crowdstrike/product/falcon/review/view/1039090>



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



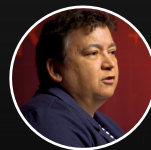
TOP10の5

最大の医療提供者



TOP10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。バームビーチ州立
大学セキュリティオフィサー

