徹底解説！
まだ知られていないFalcon便利機能！

2018/12/11

マクニカネットワークス株式会社
技術統括部 第6技術部 第2課
大高　壮平

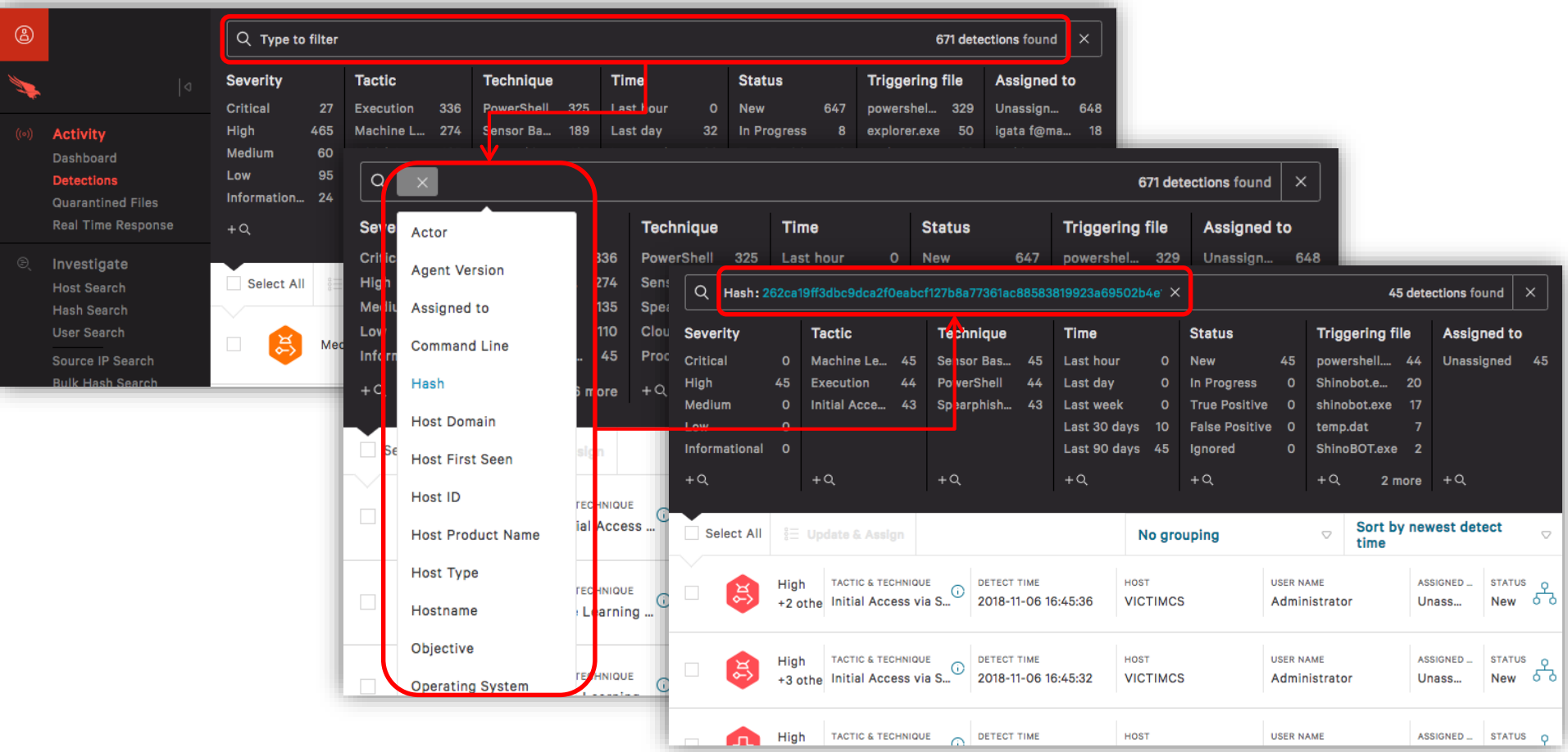
ご紹介内容

- 運用に活用できる小ネタ集
  - アラートのフィルタリング・グルーピング表示切替
  - アラートステータス・担当者一括変更方法
  - Whitelist登録方法
  - アラート一覧の取得
- MITRE社 ATT&CKフレームワーク
- Real Time Response機能
- 各APIの紹介

運用に活用できる小ネタ集

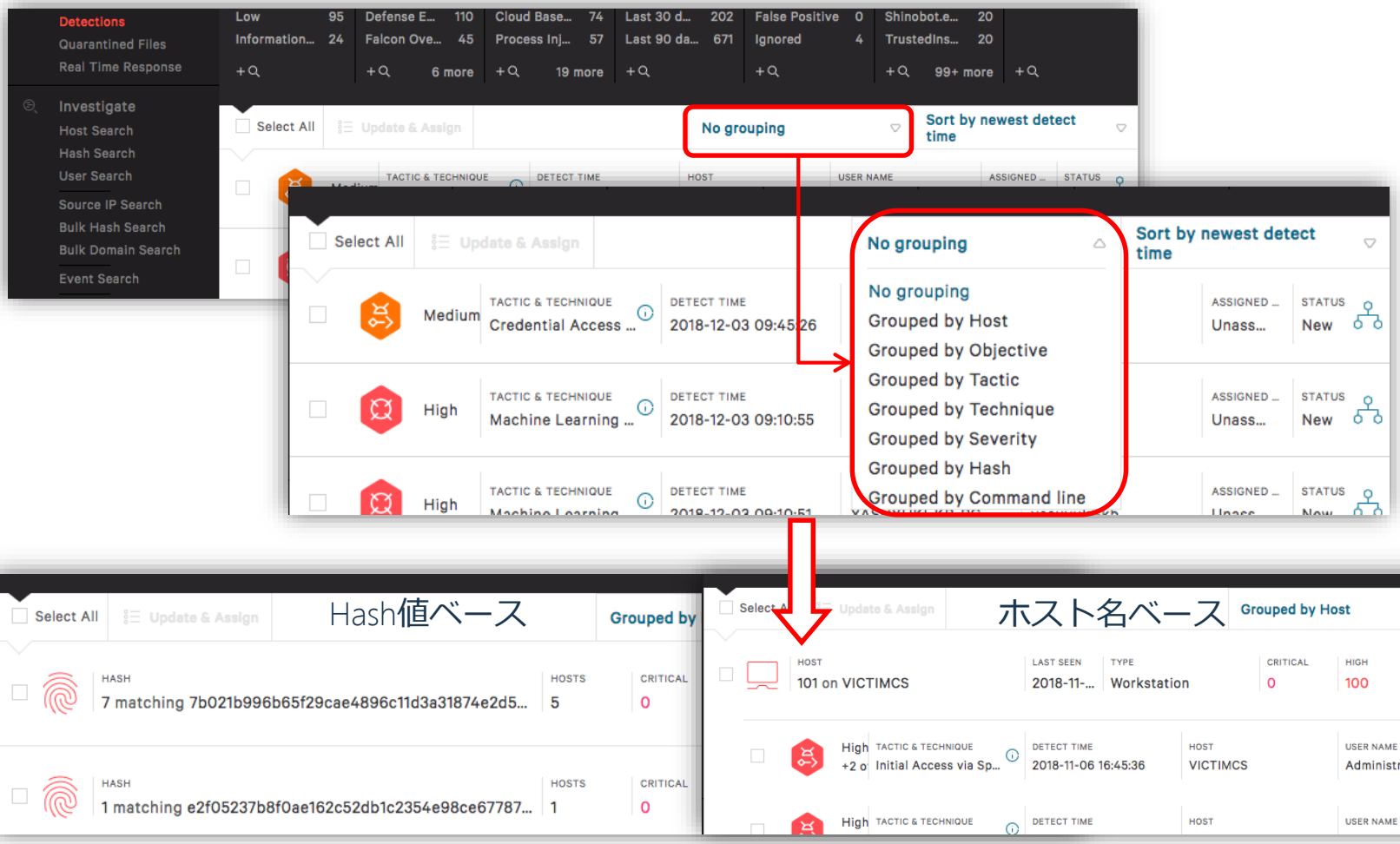
アラートのフィルタリング

ページ	「Activity」 > 「Detections」の画面上部
概要	「Type to filter」をクリックする事により、既に表示されている７項目以外の要素でもフィルタリングする事が可能です。AND条件で検索されます。



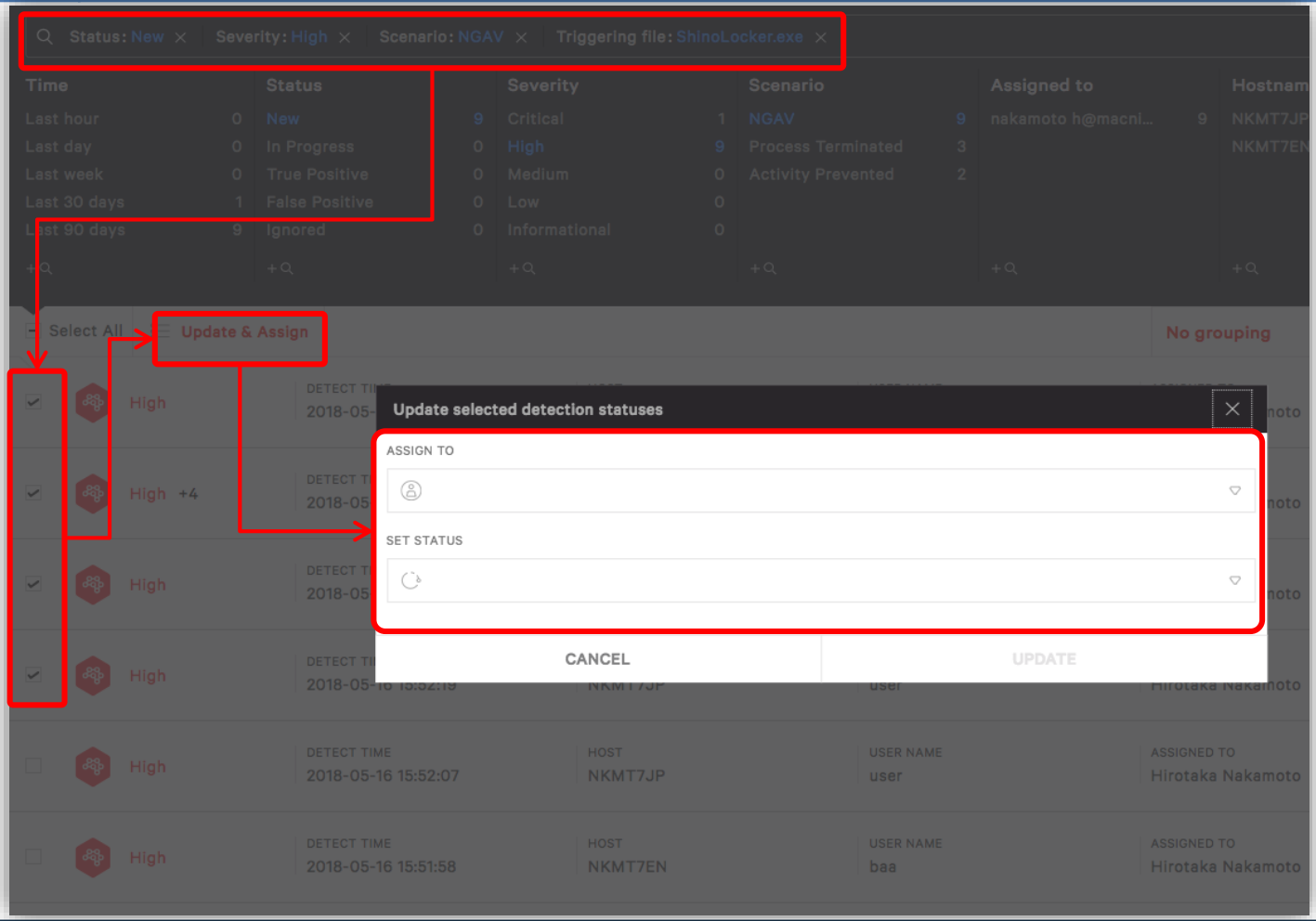
アラートのグルーピング

ページ	「Activity」 > 「Detections」の画面中部
概要	「No grouping」のタブをクリックすると、ホスト毎・ファイルHash値・ファイル名毎等のアラートにグルーピング出来ます。



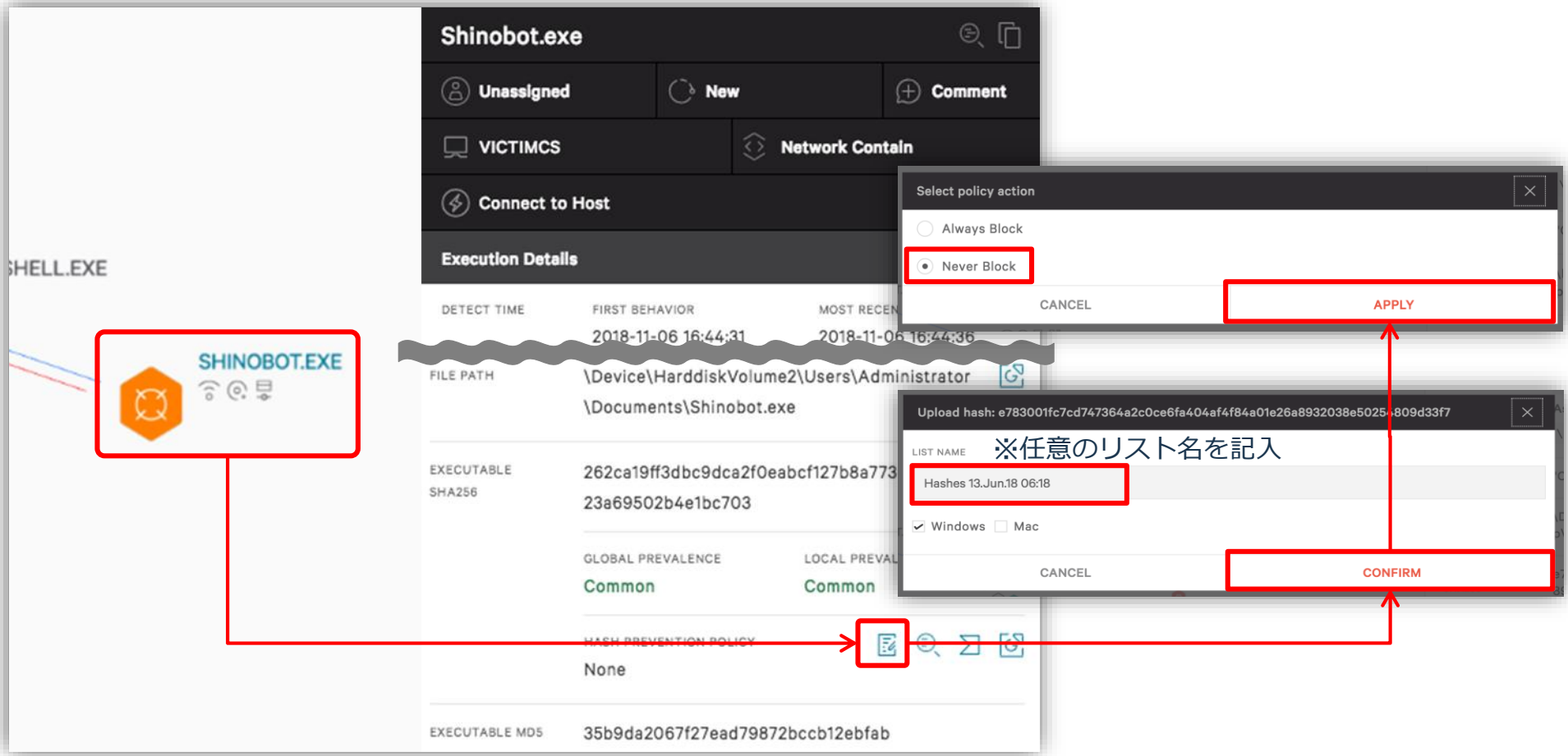
アラートステータス・担当者一括変更方法

ページ	「Activity」 > 「Detections」の画面中部
概要	個別にステータス・担当者変更も可能ですが、アラートフィルタリングやグルーピングを用いて、一括で複数アラートの変更も可能です。



Whitelist登録方法

ページ	「Activity」 > 「Detections」> 「EXECUTABLE SHA256」
概要	Detectionsページからの Whitelist登録の場合、数クリックで登録可能です。一括で複数のHash値を登録されたい場合は「Prevention Hashes」ページからのご登録がお奨めです。



【補足】Whitelist概要

Whitelistが適用される検知シナリオ

適用対象アラート（OR条件）

- 「Tactic」項目が”Machine Learning”となっているアラート
- 「Technique」項目が”Adware”または”PUP”となっているアラート

※上記シナリオ以外に対するWhitelist登録は弊社までお問い合わせ下さい。

適用対象ファイル

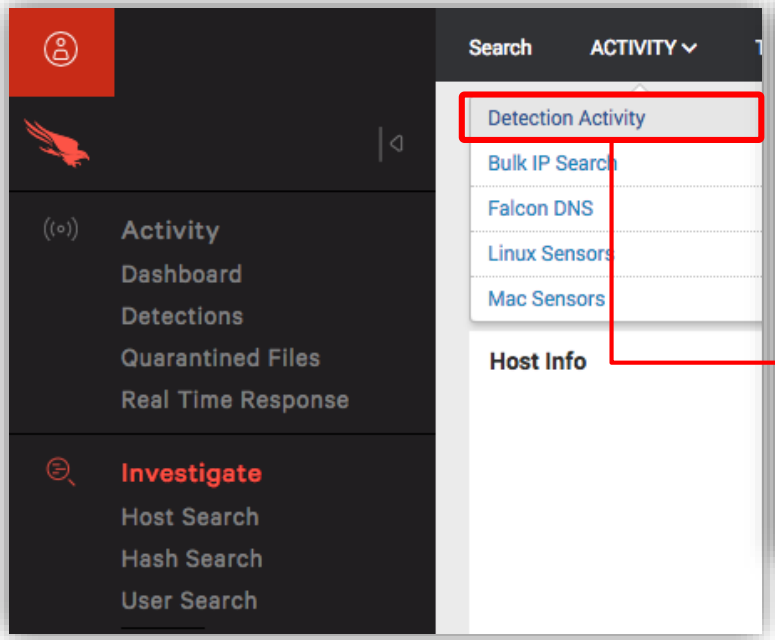
- 実行ファイル（exe/dll等）のみ。Microsoft Officeのファイル（.xlsx/.doc等）は登録頂けません。

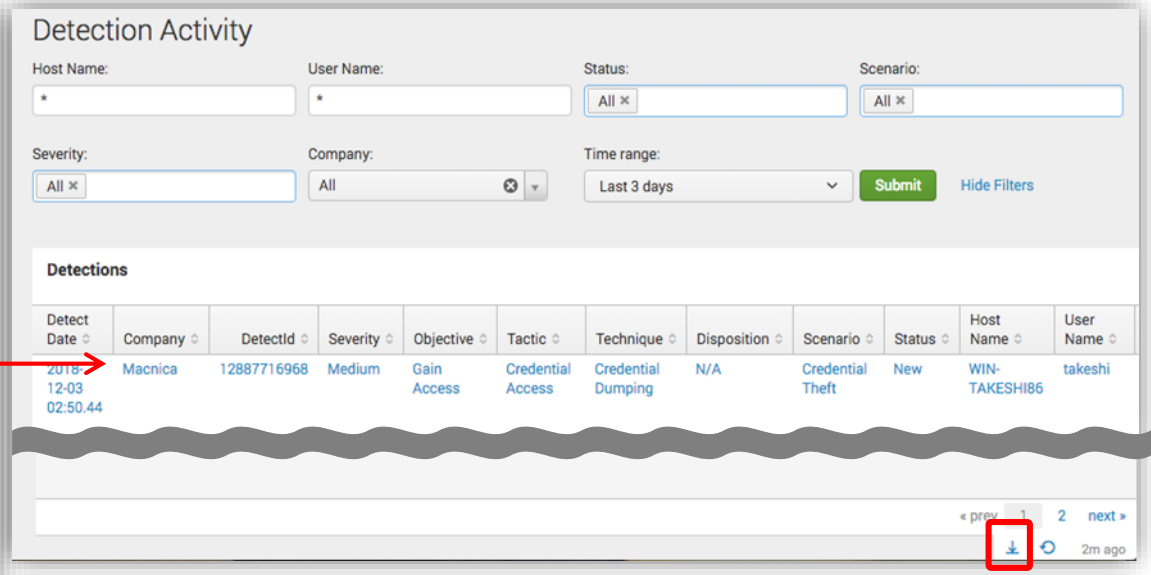
Whitelist化可能要素と登録場所

項目	登録場所
ファイルハッシュ	①Detections > EXECUTABLE SHA256 ②Configuration > Prevention Hashes
ファイル名	③Configuration > File Exclusions
ファイルパス	
ファイル拡張子	

アラート一覧の取得

ページ	「Investigate」 > 「Host Search」 > 「Activity」> 「Detection Activity」
概要	アラートの一覧を閲覧・取得できます。また、期間を指定してCSVで出力することも出来ますので、社内用のレポートの基データとしてもご利用頂けます。 「Dashboards」 > 「Detection Activity」からは統計情報を取得頂けますので、併せてご活用下さい。





※画面下部までスクロールしますと
エクスポートボタンが表示されます。

MITRE社 ATT&CKフレームワーク

MITRE社 ATT&CKフレームワーク

- MITRE（マイター）社について
  - 脆弱性管理番号（CVE）を発行している米国の非営利研究機関になります。
- ATT&CK（アタック）について
  - ATT&CK = Adversarial Tactics, Techniques, and Common Knowledge
  - 大まかな攻撃フェーズを表現した“Cyber Kill Chain”に、具体的な攻撃手法を追加したフレームワークになります。このフレームワークにより、CrowdStrike Falconからの各アラートに対して、攻撃者の目的・攻撃戦術・攻撃手法を理解することができます。

Cyber Kill Chain（攻撃のステップ）

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Custom Command and Control Protocol
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Cryptographic Protocol

攻撃手法

参考：https://attack.mitre.org/matrices/enterprise/windows/

CrowdStrikeのATT&CKへのアプローチ

CrowdStrikeでのマッピングについて

- ATT&CKの「Tactic (戦術)」「 Technique (手法)」に加え、CrowdStrikeは「Objective（目的）」を定義・追加しています。
- 「攻撃者は＜目的＞を達成するために、＜手法＞を使い、＜戦術＞を行いました。」という理解ができます。

※どの「Objective（目的）」にも該当しない攻撃に関しては、「Falcon Detection Methods 」というObjectiveに分類しています。

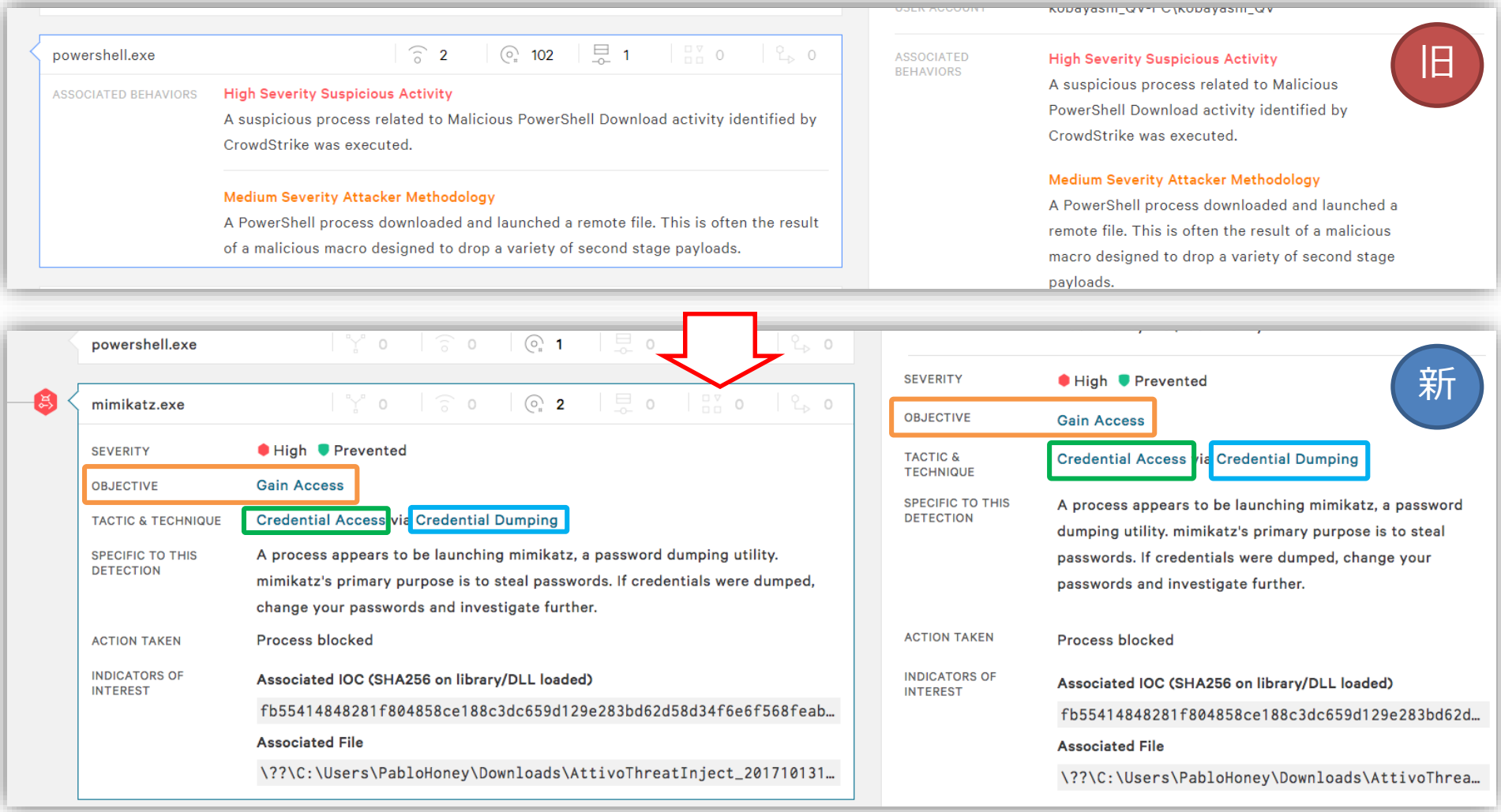
Objective	Tactic	Technique	ストーリー解釈
Gain Access	Initial Access	Spearphishing Attachment	攻撃者は**侵入**するために、**スピアフィッシングメール**を使い、**初期侵入**を行いました。
Gain Access	Credential Access	Credential Dumping	攻撃者は**侵入**するために、**認証情報ダンプツール**を使い、**認証へのアクセス**を行いました。
Keep Access	Persistence	Create Account	攻撃者は**継続侵入**するために、**アカウントを作成し**、**永続性の確保**を行いました。
Keep Access	Defense Evasion	Obfuscated Files or Information	攻撃者は**継続侵入**するために、**ファイルや情報を難読化し**、**防御システムの回避**を行いました。

ATT&CKの導入による変更点

- 検知画面
- 検知アイコンの変更
- アラート通知メールの変更
- API

検知画面

これまでの検知シナリオを廃止し、Objective/Tactic/Techniqueへ表記変更し、説明部分の情報量が増えました。



アイコンの変更

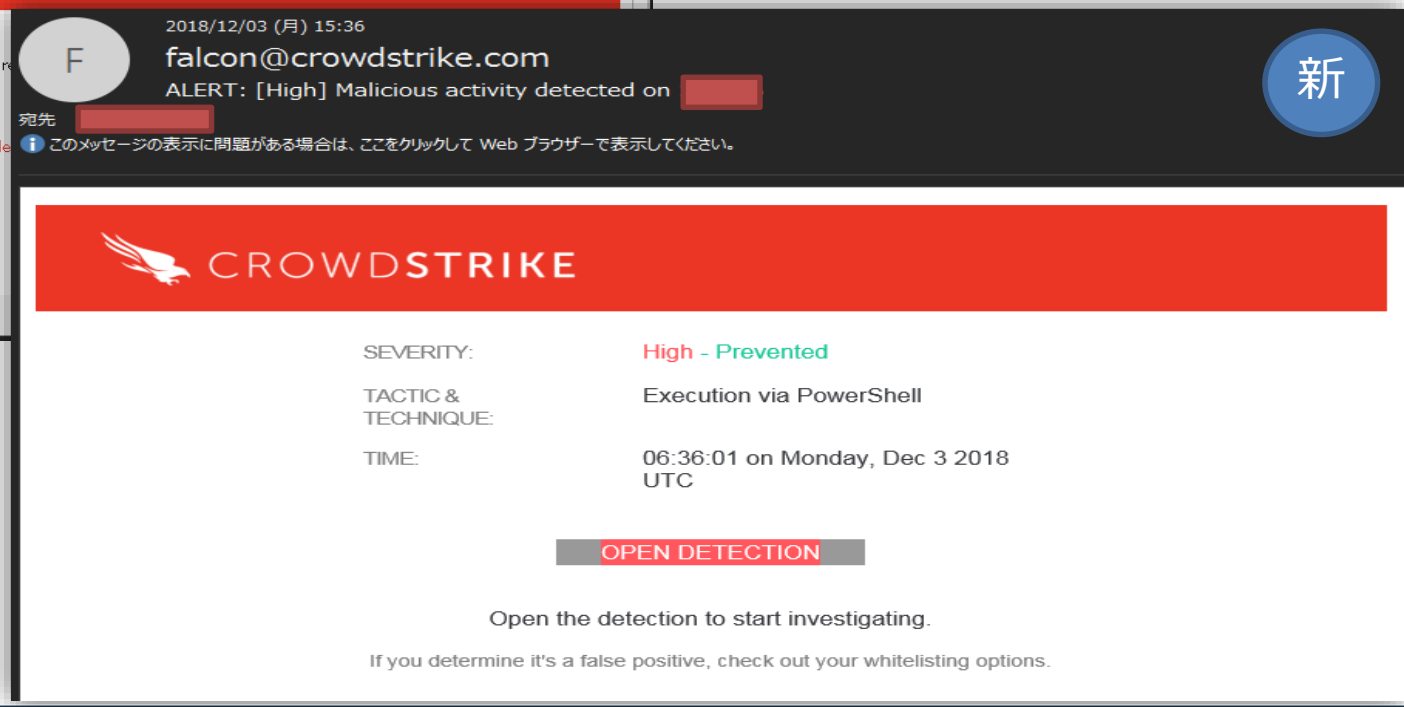
- これまで検知シナリオ毎にアイコンが用意されていましたが、変更後はObjective毎に用意されています。
- さらにブロック時やOverWatch検知時は、アイコンにバッジが付加されるようになりました。

Objective	アイコン
Gain Access	
Keep Access	
Explore	
Contact Controlled Systems	
Follow Through	
Falcon Detection Methods	

イベント	アイコン
ブロックイベント	
OverWatchイベント	

アラート通知メールの変更

- メール本文に検知シナリオが記載されていましたが、「Tactic & Technique」に表記がかわりました。また、ブロックされている場合は「Severity」項目に”Prevented”と表記されます。



APIの変更（予告）

2019年1月16日にQuery APIとStreaming APIの一部項目が変更されます。

Query API

変更前の項目名	変更後の項目名
scenario	objective
	tactic
	technique
	pattern_disposition

Streaming API

変更前の項目名	変更後の項目名
DetectName	Objective
	Tactic
	Technique
	PatternDispositionValue
	PatternDispositionDescription

Real Time Response機能

Real Time Response機能について

Real Time Response(RTR)について

オンラインの Falcon がインストールされた端末に対して、リモー トで用意されたコマンド（ファイルの取得・削除やプロセスのキル等）を実行できるようになります。これまで、対処機能としては端末のネットワーク隔離のみでしたが、本機能の追加により様々な端末追加調査および復旧作業を実行できるため、より洗練されたインシデント対応が可能になります。また、ネットワーク隔離中でも本機能は動作致します。

システム要件

- Powershell : Version 2.0以上
- .NET Framework : Version 3.5以上
- Falcon Sensor : Version 4.5.6806

必要Falcon UIアカウントロール

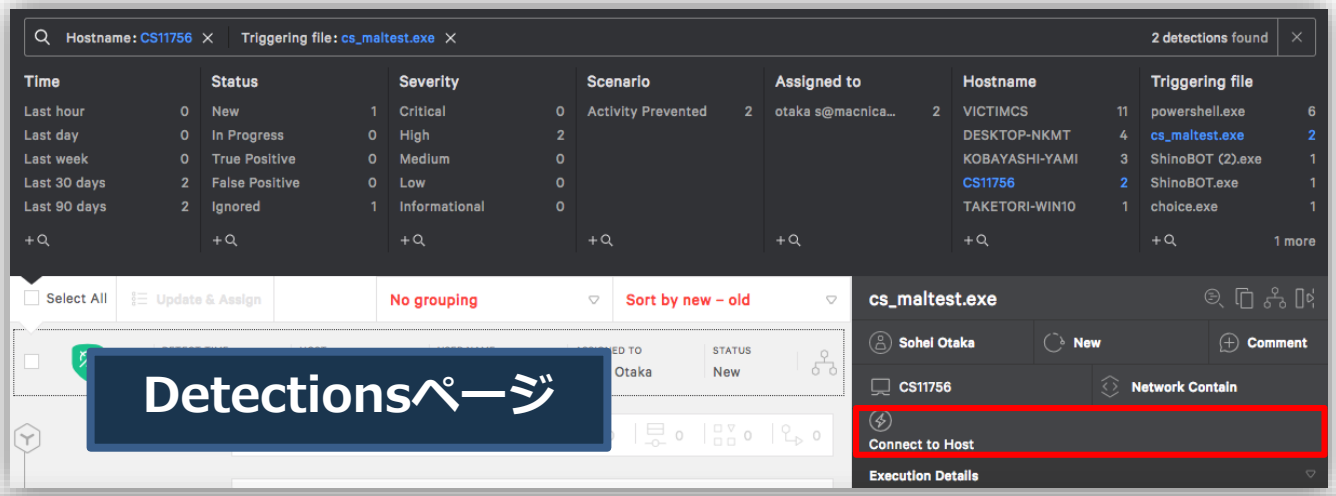
- Real Time Responder

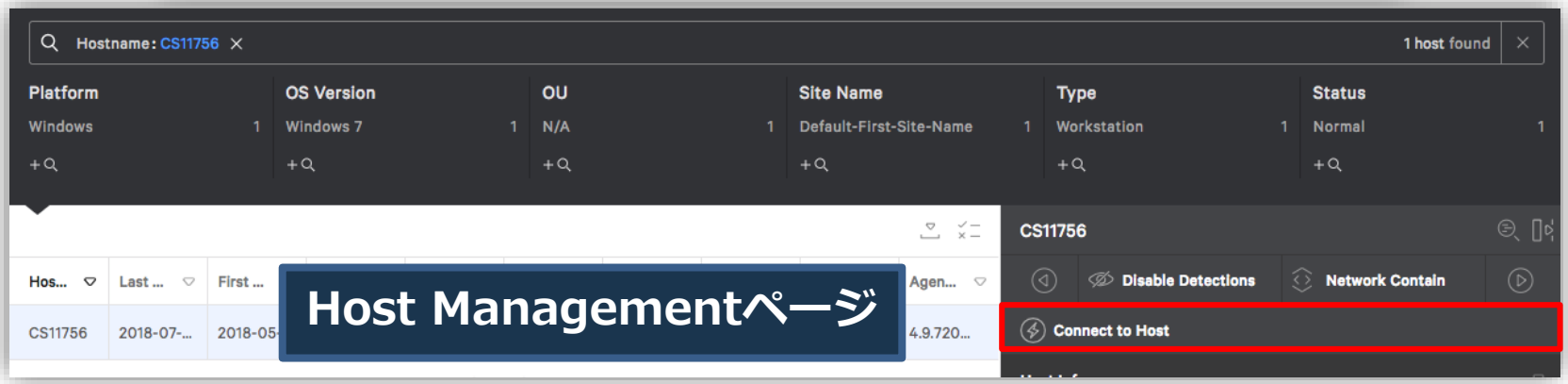
※「Falcon Administrator」に上記ロールは含まれていません。

Real Time Responseの起動

■ 起動方法

1. 「Detections」ページから修復を行う端末で発生したアラートを表示、または「Host Management」から当該端末を検索します。
2. 「Connect to Host」をクリックします。

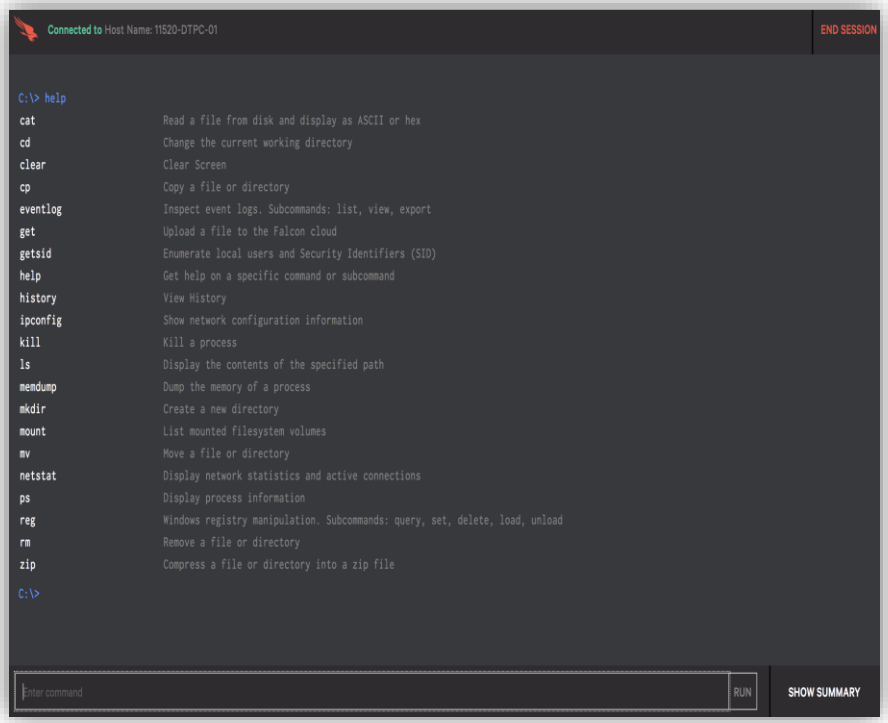




実行可能内容

macnica networks

- 画面下部のテキストボックスに実施したいコマンドを入力し、“RUN”をクリックします。取得コマンド(get等)はダウンロードリンクが画面上部に表示されます。



主要コマンド	概要
cat	ファイルの内容を表示
cd	フォルダの移動
cp	ファイル・フォルダのコピー
get	ファイルの取得
kill	プロセスの停止
ls	ファイル一覧表示
mv	ファイル・フォルダの移動
ps	プロセス一覧表示
reg	レジストリの検索・登録・削除
rm	ファイル・フォルダの削除
eventlog	Windowsイベントログ取得
xmemdump	フルメモリダンプ取得

各APIの紹介

Falcon APIの種類

Falcon APIとして、以下の4つが提供されています。ご利用にあたり、APIクレデンシャル情報やAPI有効化が必要となりますので、弊社サポート窓口までお問い合わせ下さい。

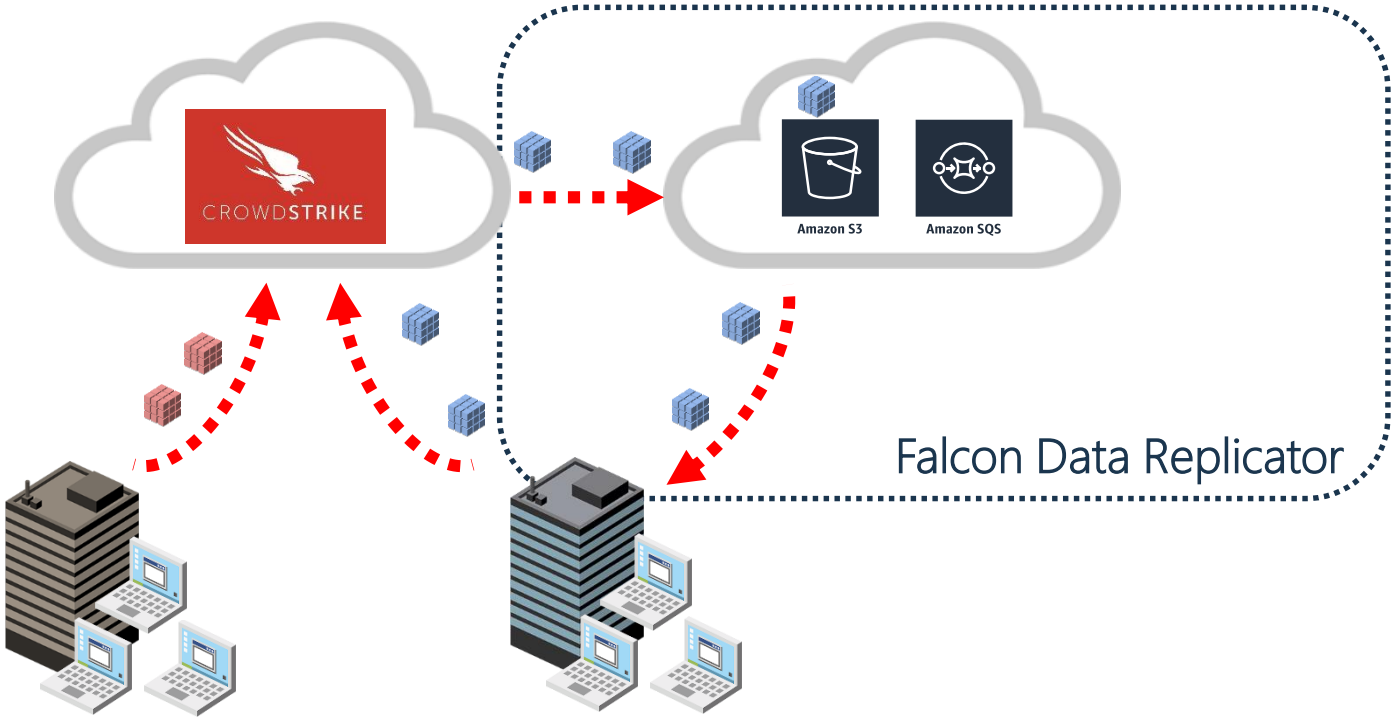
API名	取得可能情報
Streaming API	• 検知イベント • Falcon UIの操作イベント
Query API	• カスタムIoC登録 • ホスト検索 • インディケーターによる検索 • 検知ステータス設定、変更
Threat Graph API	• プロセス実行などのグラフ可視化
Data Replicator API	• 端末からアップロードした端末イベントログ

Falcon Data Replicator APIについて

システム概要

Falcon Data Replicatorを有効化しますと、各ユーザー毎にAmazon S3/SQSのアカウントが用意されます。発行されたアカウント情報とAPIを使い、端末からアップロードされたログを自社システムにダウンロードすることができます。

※ダウンロードしたログをCrowdStrike Falconへリストアする事はできません。



ご清聴ありがとうございました。

Thank you for your attention.