FFRI yarai バージョン 3.4 新機能のご紹介

検知精度の向上

検出精度の向上 1

Static分析
エンジン

Static機械学習機能を搭載

FFRIセキュリティが独自に収集したマルウェア及び正常系ソフトウェアのデータから学習した特徴をもとに静的にファイル構造を解析

Static分析
エンジン

Static機械学習機能 New!

機械学習から得た統計的な特徴データによるファイル構造の解析

機械学習
エンジン

機械学習から得た統計的な特徴データによる挙動の監視

マルウェア及び正常系ソフトウェアのデータを解析システムに投入

ファイル構造特性や振る舞いの特性を抽出

独自の機械学習を静的解析・動的監視 両方に反映

検出精度の向上 2

Static分析
エンジン

HIPS
エンジン

ATT&CK Matrix 対応

MITRE社が提唱するセキュリティフレームワークATT&CK Matrixのカバレッジを強化

ATT&CK Matrix for Enterprise の「Tactics」12カテゴリー

Initial Access(初期アクセス)

Execution(実行)

Persistence(永続化)

Privilege Escalation(権限昇格)

Defense Evasion(防衛回避)

Credential Access(認証情報アクセス)

Discovery(探索)

Lateral Movement(横展開)

Collection(収集)

Exfiltration(持ち出し)

Command and Control(指令 & 制御)

Impact(影響)

※ 出典 : <https://attack.mitre.org/> <https://www.socyeti.jp/posts/4873582/>

ATT&CK Matrix 「Tactics」の12カテゴリー全てをカバー

※各カテゴリーにおいて、「Technique」のいずれかをカバー

Microsoft Defender 連携機能強化

一般的なウイルス対策ソフトとの組み合わせ運用

今までの常識

これからの常識

Microsoft Defender AVではなく市販のウイルス対策ソフトに置き換えても防御範囲は同じなため未知の脅威は防げず、更新料も必要

市販のウイルス対策ソフトと検知力の変わらない Microsoft Defender AVとFFRI yaraiを導入することで既知・未知の脅威を防御

既存対策と組み合わせることで未知の脅威への防御力が大幅に向上します！

Microsoft Defender 連携強化

FFRI AMCより Microsoft Defender の動作状況の確認、スキャンや例外リストの配布、シグネチャ更新を実施

Microsoft Defender 運用にかかる 負荷やコストを軽減

Microsoft Defender配布イメージ

* Windows Defender コマンド *

種別	☒ シグネチャアップデート後にスキャン ☐ シグネチャアッ ☐ スキャン
スキャン種類	スキャンの種類を指定し ☐ クイックスキャン ☐ フルスキャン ☐ カスタムスキャン
カスタムスキャンパス	

戻る

FFRI Yara!
For unknown malware and 0-day attacks

エンジンステータス

- マルウェア検出
 - スタティック分析
 - サンドボックス
 - HIPS
 - 機械学習

脆弱性攻撃防御

- ZDP
- Windows (R) Defender

アップデート

バージョン : 3.4.0

Windows Defender

PCの状態: 保護

ホーム 更新 履歴

PCをスキャンしています

選択したスキャンの種類によっては、しばらく時間がかかることがあります。

スキャンの種類: クイック スキャン

開始時刻: 12:40

経過時間: 00:00:01

スキャンした項目数: 1098

スキャンを取り消す(C)

FFRI AMCからシグネチャアップデートやスキャンの配布が可能

Microsoft Defender除外リスト連携

設定 > その他例外リスト設定

Windows Defender除外リスト詳細: Defender例外[Total: 1]

☒	ファイルパス	パス除外	拡張子除外	プロセス除外
☒	C:%Users%admin%hoge%kanshigai	☒	☐	☐

ページ番号: 1 1ページあたりの表示件数: 20

CSV 参照... 追加 差し替え インポート エクスポート ファイルパス追加 ファイルパス削除

← 設定

⚙️ 除外を追加する

ファイルおよびフォルダー

+ ファイルを除外する

+ フォルダを除外する

C:%Users%admin%hoge%kanshigai

ファイルの種類

+ ファイル拡張子を除外する

プロセス

プロセスを除外すると、関連付けられているすべてのファイルも除外されます。

FFRI AMCからMicrosoft Defender除外リストの配布も可能

Microsoft Defender イベント監視

イベントタイプ	プロセス名	検出機構	詳細
スキャン完了	クイックスキャン	Windows Defender	詳細情報
スキャン完了	クイックスキャン	Windows Defender	詳細情報
スキャン完了	クイックスキャン	Windows Defender	詳細情報
駆除成功	C:\Users\%user%\AppData\Local\Microsoft\Windows Defender\Signature\Detections\feicar.exe	Windows Defender	詳細情報
シグネチャアップデート	1.327.592.0	Windows Defender	詳細情報
シグネチャアップデート	1.327.592.0	Windows Defender	詳細情報
保護操作完了	C:\Users\admin\AppData\Local\Microsoft\Windows Defender\Signature\Detections\Test.exe	Windows Defender	不審なファイルが検疫されました。(Trojan:Win32/Dynamer!ac)
マルウェアを検出しました	C:\Users\admin\AppData\Local\Microsoft\Windows Defender\Signature\Detections\Test.exe	Windows Defender	不審なファイルが検出されました。(Trojan:Win32/Dynamer!ac)
マルウェアを検出しました	C:\Users\admin\AppData\Local\Microsoft\Windows Defender\Signature\Detections\Test.exe	Windows Defender	不審なファイルが検出されました。(Trojan:Win32/Dynamer!ac)

Microsoft Defenderのイベント監視も可能

Microsoft Defenderクライアント管理画面

検索条件

すべての条件に一致
 いずれかの条件に一致

Windows Defender リアルタイム保護状態	▼	が次と等しい	▼	有効	▼	+	-
Windows Defender シグネチャーバージョン	▼	が次と等しい	▼	1.327.592.0		+	-
Windows Defender エンジンバージョン	▼	が次と等しくない	▼	1.1.17600.1		+	-

Windows Defender リアルタイム保護状態	Windows Defender シグネチャーバージョン	Windows Defender シグネチャーの最終更新日時	Windows Defender エンジンバージョン	Windows Defender スキャン最終終了日時	Windows Defender スキャン最終種類	Windows Defender 除外リスト	Windows Defender オンデマンドスキャン実施結果	Windows Defende オンデマンドスキャン実施結果
有効	1.327.592.0	2020-11-09 12:29:49	1.1.17600.5	2020-11-13 12:40:32	クイックスキャン	あり	正常	2020-11-09 14:30:

Microsoft Defenderの管理状況の確認や複数条件による検索も可能

EDR機能追加 (STIX/TAXII対応)

EDR機能の機能追加（STIX/TAXII対応）

脅威情報インポート/自動検索機能追加

STIX/TAXIIにて取り込んだ脅威を自動検索する機能を追加

FFRI yarai 3.4 EDR機能拡張内容

TAXII (Ver.1.1) と、それに準拠したバージョンのSTIX形式の脅威情報の取り込み機能 (STIXはVer.1.0系/1.1系を検証済み)

取り込んだ脅威情報の自動検索機能

検出した端末の自動ネットワーク隔離機能 (※)

検出アラートのSyslog (CEF形式に対応) 出力機能

※EDR機能以外で検出した場合は自動隔離対象外

脅威情報のインポート自動検索機能を追加し脅威検索の自動化を実現

STIX/TAXII連携運用イメージ

- ・ 配信する脅威情報 (STIX) の生成
- ・ 作成した脅威情報に関する問い合わせ窓口

※図は当社の想定イメージです

脅威情報インポート / 自動検索機能 画面イメージ

自動取得設定画面

ポリシー管理

設定 > EDR自動化基本設定

EDR自動化基本設定: 新規作成

基本設定名

TAXII設定	URL	<input type="text" value="http://example.org/xxxx"/>
	コレクション名	<input type="text"/>
	ユーザー名	<input type="text"/>
	パスワード	<input type="password"/>
	取得間隔	<input type="text" value="24"/> 時間
IOCグループ設定	IOCグループ名	<input type="text" value="Group1"/>
	有効期間	<input type="text" value="720"/> 時間

レポート

FFRI yarai EDR レポート

サマリー

結果	脅威の発見あり (ジョブ実行中)
ジョブ名	IOC_Task - 00299
ヒットしたハッシュ数 / 検索したハッシュ数	300 / 300
脅威が発見されたクライアント数 / 対象クライアント数	300 / 300
レポート出力日時	2018-10-03 11:00:07
備考	Comment - 00299

脅威状況詳細

脅威が発見されたクライアントの細離状況

隔離済クライアント数	54
脅威が発見されたクライアント数	300

発見された脅威の駆除状況

駆除を行った脅威の数	0
発見された脅威の数	300

検索対象詳細

IOCグループ名

IOC - 91117522 / IOC - 20629453 / IOC - 16876494 / IOC - 40343234 / IOC - 45030891

対象クライアント 統計

配布対象のクライアント	駆除全体	
対象クライアント数	300	
検索未完了クライアント数	153	
検索正常終了クライアント数	42	
検索正常停止クライアント数	25	
検索異常停止クライアント数	35	
検索不能クライアント数	yaraiが駆除された	41
	結果取得が成功	0
	ハッシュ計算が成功	0
	ハッシュ計算が未実行	0

対象クライアント 統計グラフ

駆除済 (51%)
正常完了 (14%)
正常停止 (10%)
異常停止 (12%)
yaraiが駆除 (14%)
検索が失敗 (0%)
計算が未完了 (0%)
検索が失敗 & 計算が未完了 (0%)