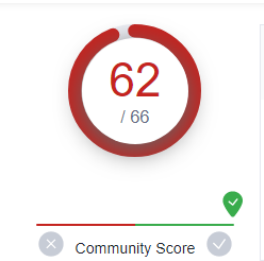
誤検知修正リクエスト

誤検知とは

エンドポイントセキュリティ製品において安全と思われるファイル/URL に対し過剰検知が発生する場合がございます。これはファイルに含まれるコードの一部がウイルスコードに類似した事が原因となり回避困難な現象として発生します。その場合 WithSecure ウイルス研究ラボへ誤検知修正をリクエストいただけます。誤検知修正は弊社製品の性能向上を目的とし「ユーザが安全と判断する」ファイルのみ承っており検知されたファイルのすべてをご提出いただく事はできません。緊急性の高い誤検知を除き解析完了までにはお時間をいただいております。なおウイルス検知基準は各アンチウイルスソフト毎に異なり危険性評価があいまいなファイルについては検知状況が分かれる事がございます。その場合 VirusTotal で各社対応状態をご利用いただく事で危険性度合いをユーザ側でご判断いただけます。また後述の”ファイル解析リクエスト”で検体ファイルの再検査をリクエストできますが危険性評価があいまいなファイルは検知対象データベースへの追加を行わない事もございます。その理由等の解析結果/詳細情報提供は行っておりませんのでご了承ください。

VirusTotal　https://www.virustotal.com/gui/home/upload

「VirusTotal（ウイルストータル）はファイルやウェブサイトのマルウェア検査を行うウェブサイトである。ファイルを VirusTotal にアップロードしたりウェブサイトの URL を指定すれば、そのファイルやウェブサイトが「マルウェアを含むかどうか」検査できる。」

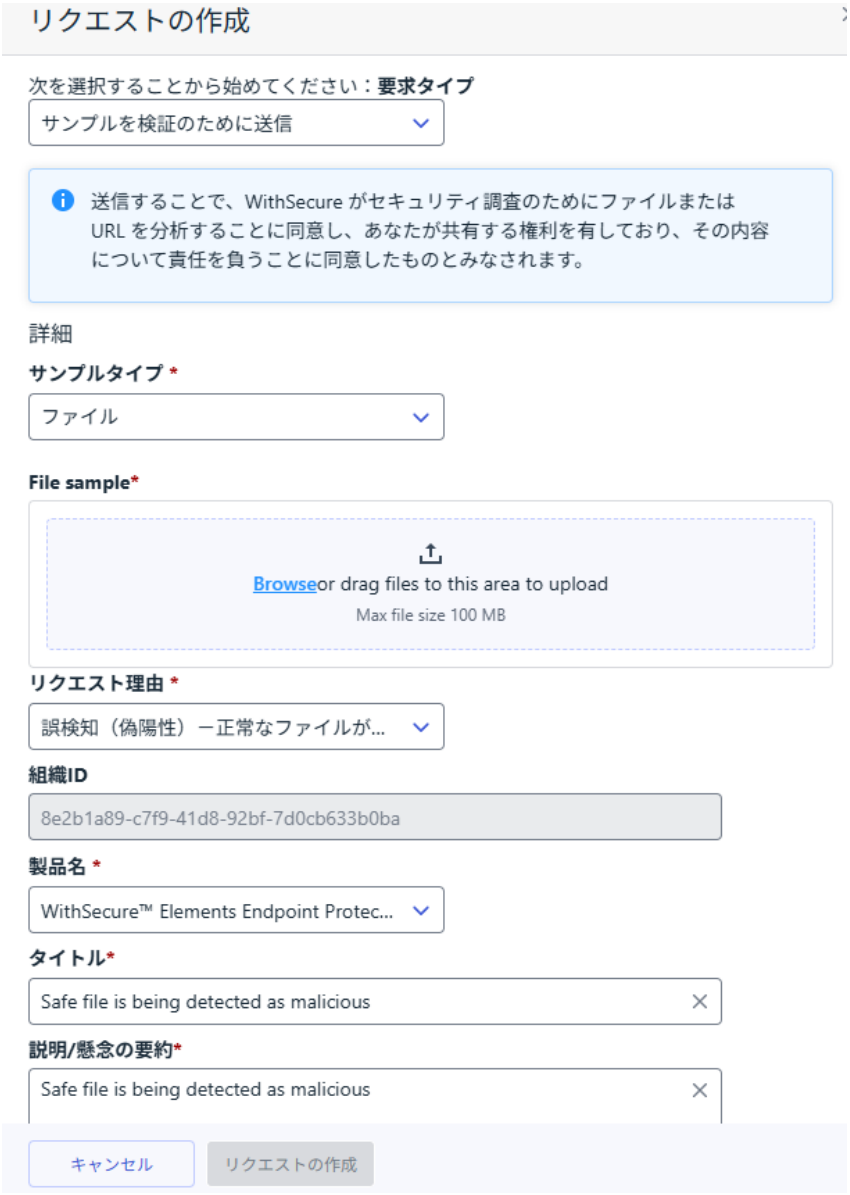


例）Withsecure 製品で検知したファイルを VirusTotal でチェック、66 社中 62 社が危険として判断。この場合、検知は正常と判断できます。

誤検知修正リクエストの提出手順

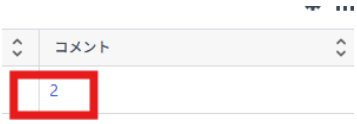
1. 誤検知発生端末で検体ファイルを採取します。(後述)
2. Elements Security Center にログインします。
   ※一般向け検体解析システム (SAS)は廃止されました。
   ~~https://www.withsecure.com/jp-ja/support/contact-support/submit-a-sample~~
3. 「リクエスト」→「リクエストの作成」をクリックします。

4. リクエスト詳細を記入します。(英語対応のみ)



5. リクエストが一覧に作成されます。

6. 「コメント」に Withsecure からの回答が記載されます。



※投稿者からの追加コメントもこちらに記載いただけます。

■必要情報

A. 検体ファイル(“infected”でパスワード付き暗号化 ZIP 圧縮)

B. 検知名(Backdoor:W32/Pushbot.gen!A 等)

※EPP の場合”マルウェア保護”→”隔離保存したファイルを表示する”で表示されます。

C. 診断情報 (採取方法は製品により異なります。こちらをご参照ください)

D. 検知したデバイスのインターネット接続有無

英文依頼

ラボとのメール対応は英文のみとなります。(ユーザーが)安全と判断しているファイルが検知された場合「Possible safe file is being detected as Virus by WithSecure products. 」と記載してください。 (ユーザが)危険と判断しているファイルが検知されない場合「Possible malicious file is not detected by WithSecure products」と記載してください。オフライン環境の場合オフライン用パターンファイルでの修正が必要な為「Please fix this in offline pattern file.」と追記してください。

スキャン除外

ユーザが社内で作成したスクリプト等を検知し、明らかに誤検知であると確信されている場合はスキャン除外機能での一時的対処を行ってください。

日本語対応

検体提出日本語対応窓口は廃止となりました。前述の SAS をご利用ください。

検体ファイル復元手順

- **安全と思われるファイルの場合**

  →Windows EPP 製品

  リアルタイムキャンを無効化し、検知されたファイルを復元→採取してください。操作には十分なご注意をお願い致します。暗号化 ZIP 圧縮後リアルタイムスキャンを有効化してください。

  ※ElementsEPP 「隔離保存したアイテムを復元する」手順

  https://www.withsecure.com/userguides/product.html#business/computer-protection-windows/latest/ja/release_a_program_from_quarantine-latest-ja

  ※BS Client Security/Server Security 「隔離保存したアイテムを復元する」手順

  https://www.withsecure.com/userguides/product.html#business/client-security/16.00/ja/release_a_program_from_quarantine-16.00-ja

  →Linux EPP 製品

  リネーム処理(Linux Security/EPP for Linux)からの復元

  検知時処理がリネームの場合、該当ファイルを元のファイル名に変更する事でファイル復元が可能です。リネームされたファイルには“.malware”が付加され元の場所に存在し続けます。

- **安全性の確証がないファイルの場合**

  下記 KB 記載の WithSecure Quarantine Dumper を利用して離されたファイルを収集する。

  https://community.withsecure.com/ja/kb/articles/29662

  1. このリンクをクリックして、任意の場所 (例: c:¥temp) にダウンロードします。
     32 ビット版: https://download.withsecure.com/support/tools/wsdumpqrt/wsdumpqrt.exe
     64 ビット版: https://download.withsecure.com/support/tools/wsdumpqrt/wsdumpqrt64.exe
  2. コマンドプロンプト (CMD) を起動します。
  3. 手順 1 で選択した場所にディレクトリを移動します。たとえば、 cd c:¥temp¥と入力し、キーボードの **Enter キーを**押して c:¥temp¥ フォルダーに移動します。

4. ツールを実行するには、 w sdumpqrt.exe -dc:¥temp¥と入力します。
5. プロンプトが表示されたら管理者の資格情報を入力してください。WithSecure のライセンス条項が表示されます。
6. ライセンス条項に同意する前に、最後までスクロールしてください。
7. ライセンス条項に同意するには、キーボードの **E** を押します。
8. 実行を完了するには、任意のキーを押してください。隔離されたファイルは、手順 1 で指定した場所に、デフォルトのパスワード（infected）が付いた「**malware_samples.zip**」というファイルに収集されます。

ジェネリック検知について

検知サンプル: Generic.malware.[variant], Generic.[variant], gen:win32.malware.[variant], Gen:variant.

ジェネリック検知とはファイルのデータパターン等が類似している場合に発生します。特定パターンファイルに登録されているウイルスの情報にファイルが一致したわけではない為、自動解凍形式ファイルや自動ダウンロードといった自動処理がファイルに組み込まれている場合、このジェネリック検知が頻繁に発生する可能性があります。この問題はパターンファイル精度の問題ではなく「疑わしい振る舞いは検知する」セキュリティー・ポリシーによるものです。ファイルの作成者側でデジタル証明書を埋め込み、弊社側でデジタル証明書のリスク判断を下げる事で誤検知発生頻度を低減する事が可能です。ご希望の場合、弊社サポートへデジタル証明書をご提出ください。リアルタイムスキャンの除外フォルダを作成し、そのフォルダ内での該当ファイル操作を行う等でも対処可能です。その場合、該当フォルダ内のセキュリティーは下がりますのでご注意ください。