Cisco Secure Endpointからの古いWindows除外の削除

内容

概要

このドキュメントでは、Windows Secure Endpointの顧客環境から一般的な不正形式の除外を削除するための計画プロセスについて説明します。

問題の説明

パフォーマンスへの影響を最小限に抑え、Cisco Secure Endpointの機能を最大限に活用するための継続的な取り組みの一環として、当社のエンジニアは、お客様の環境で最も一般的な古い除外項目を特定しました。この除外項目は、2022年10月に削除される予定です。Secure Endpoint（6.x以前）の以前の反復は、マルチドライブ除外を利用するためにワイルドカード機能(*)に依存していました。その後、除外定義と入力に対する変更と改善により、このような広範な形式の必要性がなくなり、ワイルドカードによって生じたパフォーマンスの影響に対処するためにCisco Maintained Exclusionsが調整されました。Windows Secure Endpoint 7.5.3のリリースに伴い、ワイルドカード(*)プロセスの除外に使用できる新しい機能が追加されました。この機能により、アスタリスクを使用する除外の処理が変更され、環境内に次の除外が依然として存在するお客様のCPU消費が増加しました。

```
*\Windows\Security\database\*.sdb
*\Windows\Security\database\*.edb
*\Windows\Security\database\*.chk
*\Windows\SoftwareDistribution\Datastore\Logs\*.log
*\Windows\Security\database\*.jrs
*\Windows\Security\database\*.log
*\Windows\Temp\content.zip.tmp\*.diff
*\Windows\Temp\content.zip.tmp\cur.scr
*\Windows\Temp\TMP*.tmp
*\Windows\Temp\musdmys_*
*\Windows\Temp\content.zip.tmp\SymDeltaDecompressOptions.xml
*.sas*
*\Windows\SoftwareDistribution\Datastore\Logs\edb*.log
*\System Volume Information\tracking.log
*\Program Files (x86)\SysTrack\LsiAgent\Condense\*\*\*.tmp
*\Program Files (x86)\SysTrack\LsiAgent\Condense\*\*.hld
*\Windows\Temp\AltirisScript*.cmd
*\Windows\System32\drivers\*-*.tmp
*\Users\*\AppData\Local\Temp\*-*.tmp
*\Users\*\AppData\Local\Temp\warsaw_*
```

```
*\Windows\Temp\warsaw_*
*Windows\SoftwareDistribution\Datastore\Logs\*.log
*\Windows\System32\Dns\*.dns
*\Windows\System32\DNS\*.scc
*\Windows\ntds\EDB*.log
*\Windows\ntds\Edbres*.jrs
*\Windows\ntds\*.pat
*\Windows\SoftwareDistribution\Datastore\Logs\edb.log
*Windows\Temp\mus*
*Windows\Temp\content.zip.tmp*
```

その他の手順

これらの除外を削除しても、環境に悪影響を及ぼすことはなく、Windows Secure Endpoint 7.5.3以降を使用しているホストのパフォーマンスが向上する可能性があります。アスタリスク(*)で始まる除外について現在のカスタム除外リストを確認し、複数のドライブが必要な場合はワイルドカードで使用できる「すべてのドライブ文字に適用」機能を使用するように、また必要でない場合はパスにドライブ文字を入力するように変更してください。次のソフトウェアのいずれかを使用する場合は、Cisco Maintained Listをポリシーに追加してください。これは、正しい除外がすでに適用されているためです。

- Microsoft Windowsのデフォルト
- SymantecのAltiris
- ドメイン コントローラ
- ダイボルトワルシャワ
- Lakesideソフトウェア – Systrack
- SASアプリケーション
- Symantec

注：組織内でChange Freezeに関する問題がある場合は、TACケースをオープンし、**2022年10月7日までにこの記事を参照してください。**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。