Verifica analisi Windows Secure Endpoint (CSE)

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Premesse

Scansione completa

Scansione Flash

Analisi pianificate

Analisi completa pianificata

Altre analisi

Risoluzione dei problemi

Introduzione

In questo documento vengono descritti i diversi tipi di digitalizzazione di un connettore Windows.

Prerequisiti

I prerequisiti per questo documento sono:

- Endpoint Windows
- Secure Endpoint (CSE) versione v.8.0.1.21164 o successiva
- Accesso a Secure Endpoint Console

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Endpoint Console
- Endpoint Windows 10
- Secure Endpoint versione v.8.0.1.21164

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Le analisi sono state testate in un ambiente lab con il criterio impostato per il debug.
La scansione flash durante l'installazione è stata abilitata tramite il download del connettore.
Le scansioni sono state eseguite dall'interfaccia grafica Secure Client e dallo scheduler.

Scansione completa

Questo log mostra quando viene richiesta un'analisi completa dall'interfaccia grafica (GUI) CSE.

```
(1407343, +0 ms) Aug 23 18:06:01 [9568]: Processing AMP_UI_SCAN action: 1, type 2
```

Scansione dall'interfaccia utente

In questo caso, il processo ScanInitiator avvia il processo Scan.

```
(1407343, +0 ms) Aug 23 18:06:01 [9568]: ScanInitiator::RequestScan: Attempting to start scan: dConnect
```

Come mostrato nell'immagine, è possibile notare che viene attivata la funzione di scansione completa sulla GUI.

A questo punto, si dispone del SID (ID di sicurezza), che è un valore di lunghezza variabile assegnato a questo particolare evento. Questo ID di sicurezza consente di tenere traccia dell'analisi nei log.

```
(1407343, +0 ms) Aug 23 18:06:01 [17268]: imn::CEventManager::PublishEvent: publishing type=554696714,
json={"iclsa":"0","sce":108,"scx":"Full Scan","sid":1407343,"sit":2,"sop":0,"stp":5},
ui64EventId=7135211821471891460
```

Evento Publish

È possibile far corrispondere questo valore con l'evento dalla console CSE.

Evento console

Nei log è quindi possibile visualizzare quanto segue:

```
(1407343, +0 ms) Aug 23 18:06:01 [17268]: PublishScanStartEvent publishing event succeeded for 1407343, (null)
```

Pubblicazione completata

Questo significa che l'evento è stato pubblicato correttamente nel cloud CSE.

L'azione successiva consiste nell'eseguire la scansione:

```
(1407343, +0 ms) Aug 23 18:06:01 [17268]: Scan::ScanThreadProcess: published event. Starting Scan: 1407343, [type:
5]
```

Inizio analisi

Come si può notare, il SID è lo stesso, quindi si è sotto il flusso di SID 1407343.

Di seguito sono riportati i passaggi eseguiti dal connettore quando viene rilevata una minaccia durante l'analisi.

Passaggio 1. Il connettore indica il file che ha causato il rilevamento. In questo esempio, è causato da Hacksantana Trainer GLS.

```
(2443984, +0 ms) Aug 23 18:23:18 [11964]: Scan_OnObjectScanComplete: threat types: 63
(2443984, +0 ms) Aug 23 18:23:18 [17664]: imn::CEventManager::FileRoot \\?\C:\Users\[redacted]
[redacted]\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Files\S0\4\Attachments\HackSantana Trainer GLS And GIS By
PollinxD 27-12[1829].rar, , , ,
(2443984, +0 ms) Aug 23 18:23:18 [11964]: Scan_OnObjectScanComplete action: 1 [5, 5]
```

Rilevato file

Passaggio 2. L'evento viene pubblicato nella console CSE con il nome Threat Detection e il percorso in cui si trova.

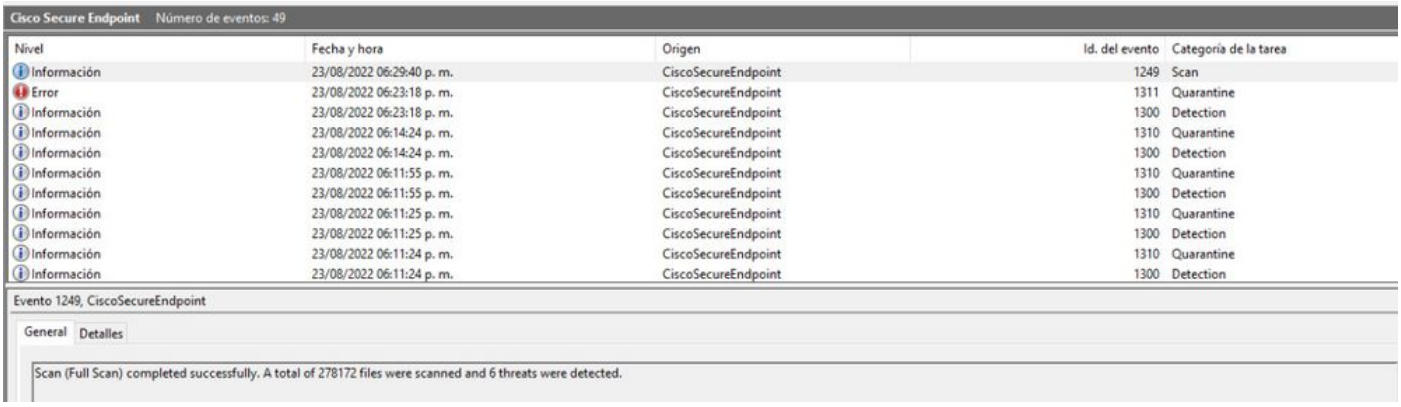
```
(2443984, +0 ms) Aug 23 18:23:18 [17664]: ERROR: imn::GetProcessInfo ProcessId is zero
(2443984, +0 ms) Aug 23 18:23:18 [17268]: IsFileSizeWithinScanLimit: dwMinFileSize = 0, dwMaxFileSize = 52428800
(2443984, +0 ms) Aug 23 18:23:18 [17664]: imn::CEventManager::PublishEvent: publishing type=1090519054, json={"am":0,"dete":64,"dfc":"13305770598","dfs":"0"
"dfsl":"","did":"7135216275352977414","dnm":"Gen:Variant.Graftor.596528","fcr":"","fcx":2148204800,"ffv":"","fnd":"HackSantana Trainer GLS And GIS By
PollinxD 27-12[1829].rar","fnp":"","fpd":"\\\\?\\C:\\Users\[redacted]
[redacted]\\AppData\\Local\\Packages\\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\\LocalState\\Files\\S0\\4\\Attachments\\HackSantana Trainer GLS And GIS
By PollinxD 27-12[1829].rar","fpn":"","fpv":"","ft":"0x0000000000000000000000000000001","ftd":"0x0000000000000000000000000000001","ftnd":0,"is":1,"md5d":"
388949798249ad7c53f8e30725a0361","pbd":0,"pcx":0,"pfc":"0","pfs":"0","sha1d":"69d456e8aeec4c4c99b932d1911feef0328a47
```


Nome rilevamento


```
(2443984, +0 ms) Aug 23 18:23:18 [8744]: Successfully configured endpoints: https://mgmt.amp.cisco.com/agent/v1/ https://intake.amp.cisco.com/event/
(2443984, +0 ms) Aug 23 18:23:18 [17664]: UIPipe::SendDisposition file: HackSantana Trainer GLS And GIS By PollinxD 27-12[1829].rar(3), detect:
Gen:Variant.Graftor.596528
```


Pubblicazione evento minaccia

Al termine dell'analisi, è possibile esaminare il Visualizzatore eventi per un riepilogo dell'analisi.



Visualizzatore eventi

Scansione Flash

Le scansioni Flash sono veloci e richiedono da secondi a minuti per essere completate.
In questo esempio, è possibile vedere quando viene avviata l'analisi e, come in precedenza, viene fornito un SID, questa volta, con un valore di 2458015.


```
(2458015, +0 ms) Aug 24 19:21:19 [17500]: Scan::ScanThreadProcess: beginning scan id: 2458015, [type: 1, options: 3, 3, pid: 0, initiator: 2]
```


Inizio analisi flash

L'azione successiva consiste nel pubblicare l'evento nel cloud CSE.

```
(2458015, +0 ms) Aug 24 19:21:19 [17500]: imn::CEventManager::PublishEvent: publishing type=554696714, json={"iclsa":"0","sce":108,"scx":"Flash
Scan","sid":2458015,"sit":2,"sop":3,"stp":1}, ui64EventId=7135602311308509188
```

Al termine dell'analisi, l'evento viene pubblicato nel cloud.


```
(2458015, +0 ms) Aug 24 19:21:19 [17500]: imn::CEventManager::PublishEvent: publishing type=554696714, json={"iclsa":"0","sce":108,"scx":"Flash
Scan","sid":2458015,"sit":2,"sop":3,"stp":1}, ui64EventId=7135602311308509188
```


Fine scansione - Pubblica

L'evento può essere visualizzato nel Visualizzatore eventi di Windows. Come si può notare, le informazioni sono identiche a quelle presentate nei log.

```
- <EventData>
    <Data Name="JsonEvent">{"dios":0,"ds":0,"hi":0,"scx":"Flash Scan","sdds":0,"sdfs":10951,"sdps":215,"sid":2458015,"sios":0,"sit":2,"sop":3,"sspc":0,"stp":1}
      </Data>
    <Data Name="EventTypeId">554696715</Data>
    <Data Name="TimeStamp">133058605022030000</Data>
    <Data Name="EventId">7135602410092756997</Data>
    <Data Name="Description">EVENT_SCAN_COMPLETED_CLEAN</Data>
  </EventData>
</Event>
```

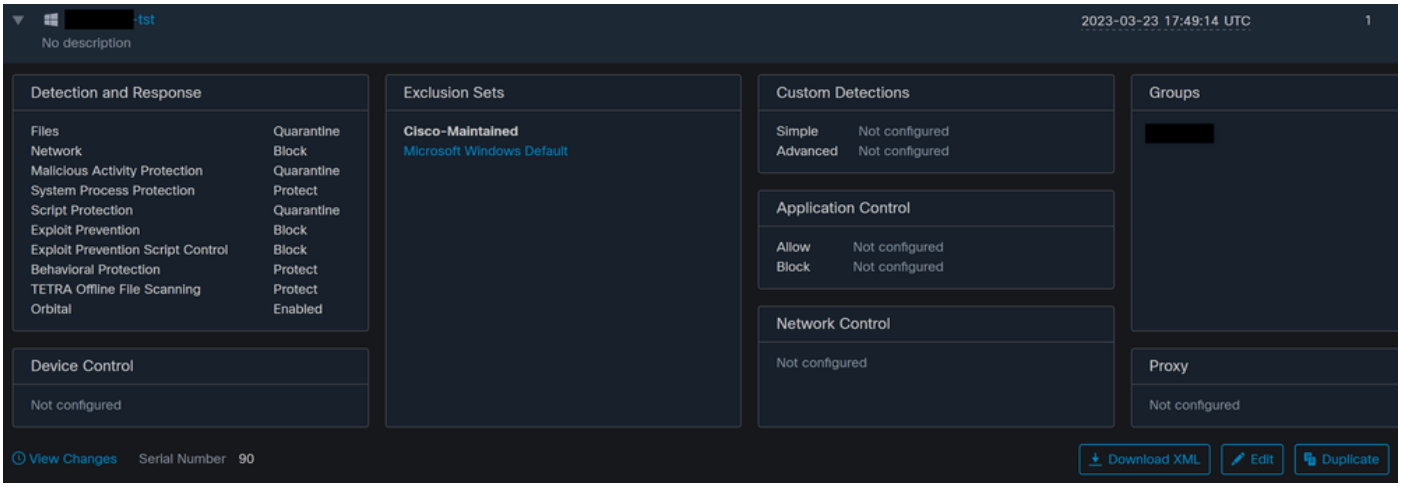
Evento JSON

Analisi pianificate

Quando si tratta di analisi pianificate, è necessario essere a conoscenza di una serie di aspetti.

Una volta pianificata l'analisi, il numero di serie viene modificato.

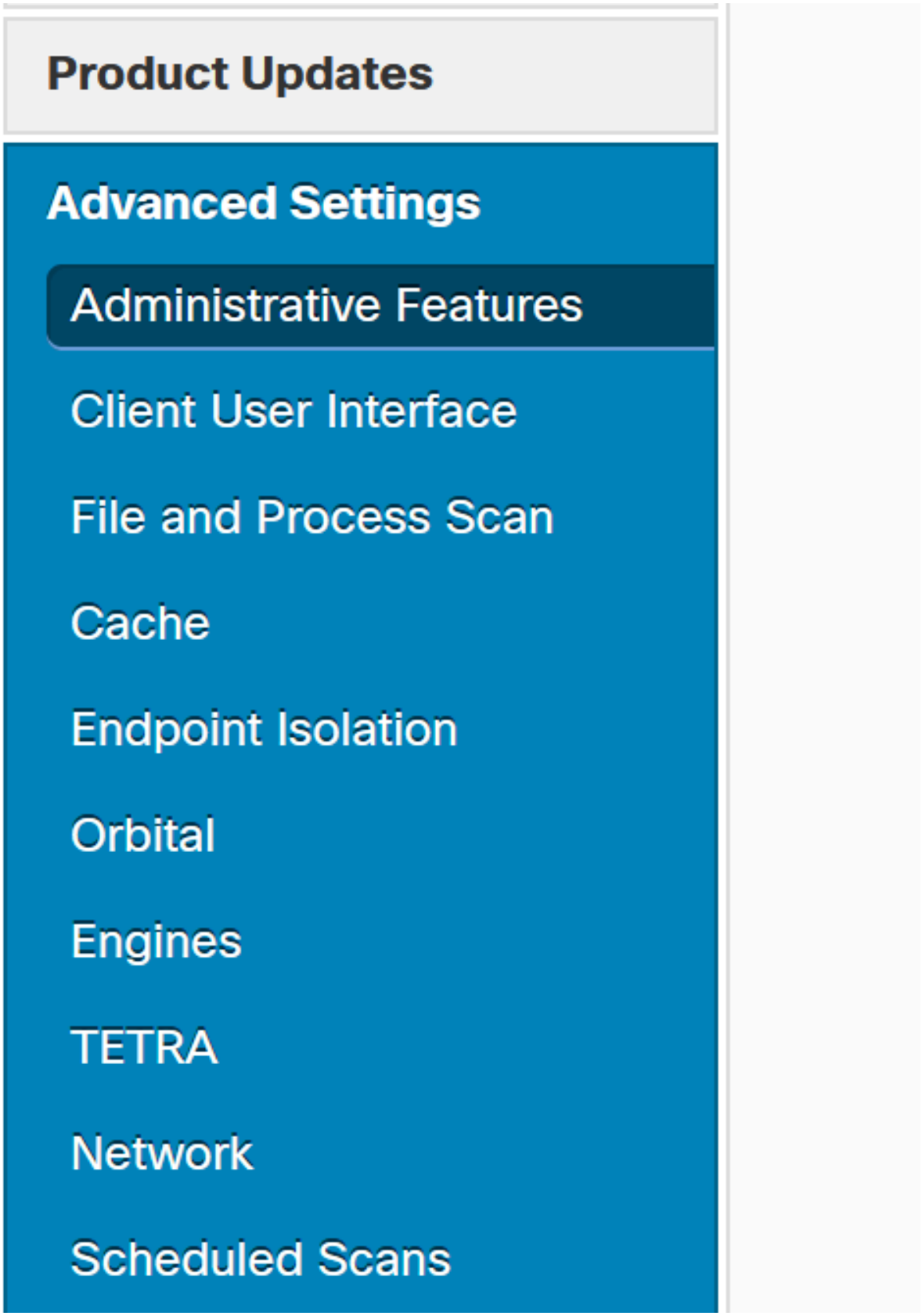
In questo caso, il criterio di test non dispone di analisi pianificate.



Numero di serie del criterio

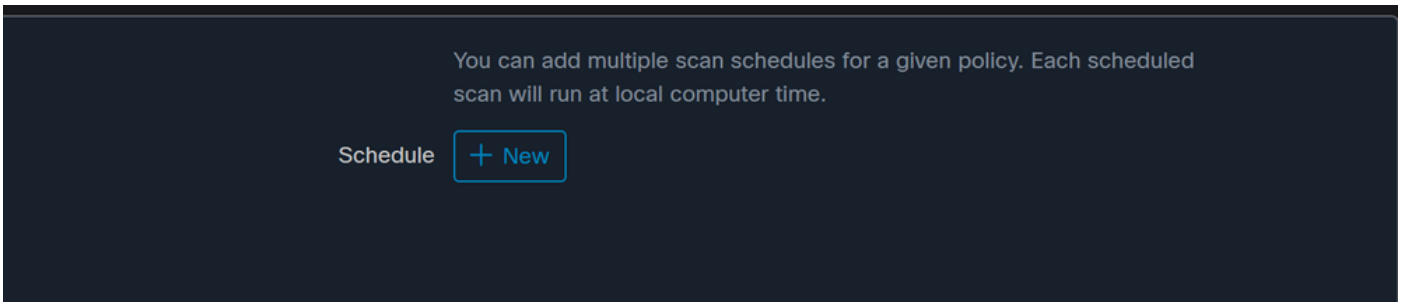
Se si desidera pianificare un'analisi, fare clic su Modifica.

Passa a Advanced Settings > Scheduled Scans.



Impostazioni avanzate

Fare clic su New.

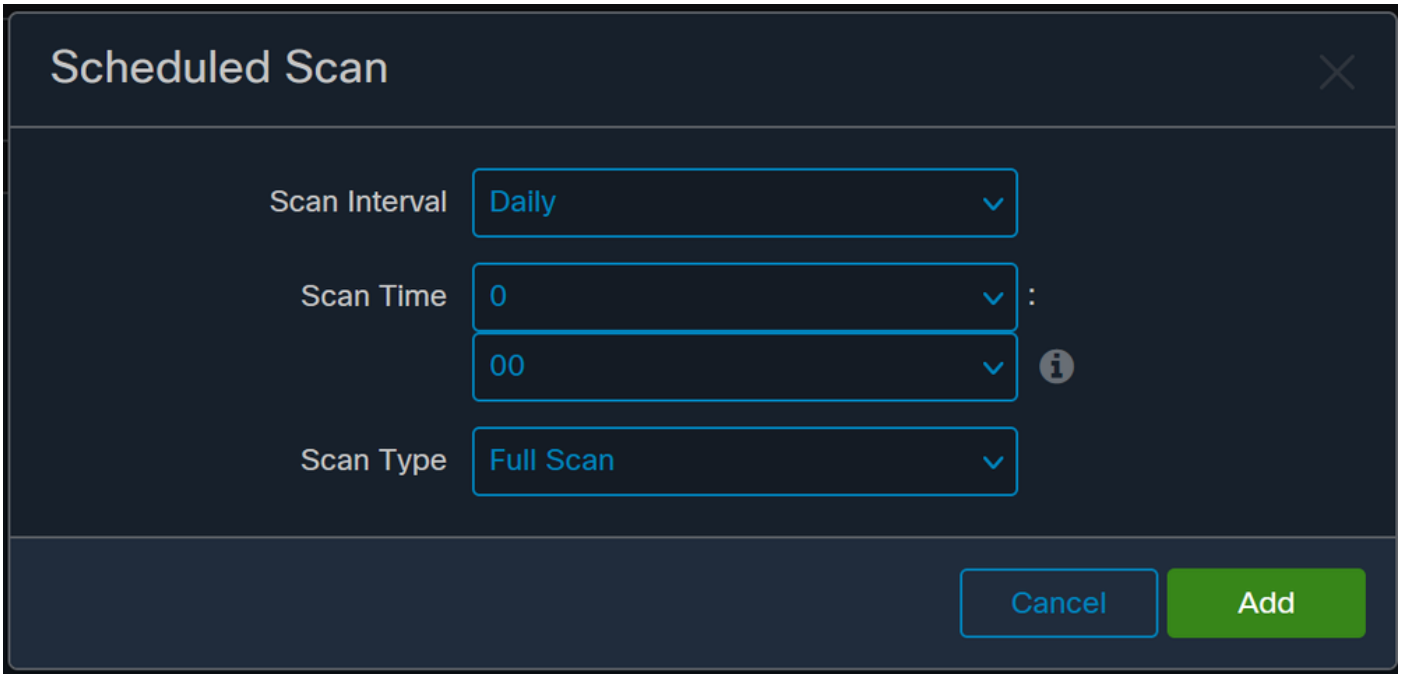


Nuova configurazione di digitalizzazione

Le opzioni sono:

- Intervallo di scansione
- Tempo di scansione
- Tipo di analisi

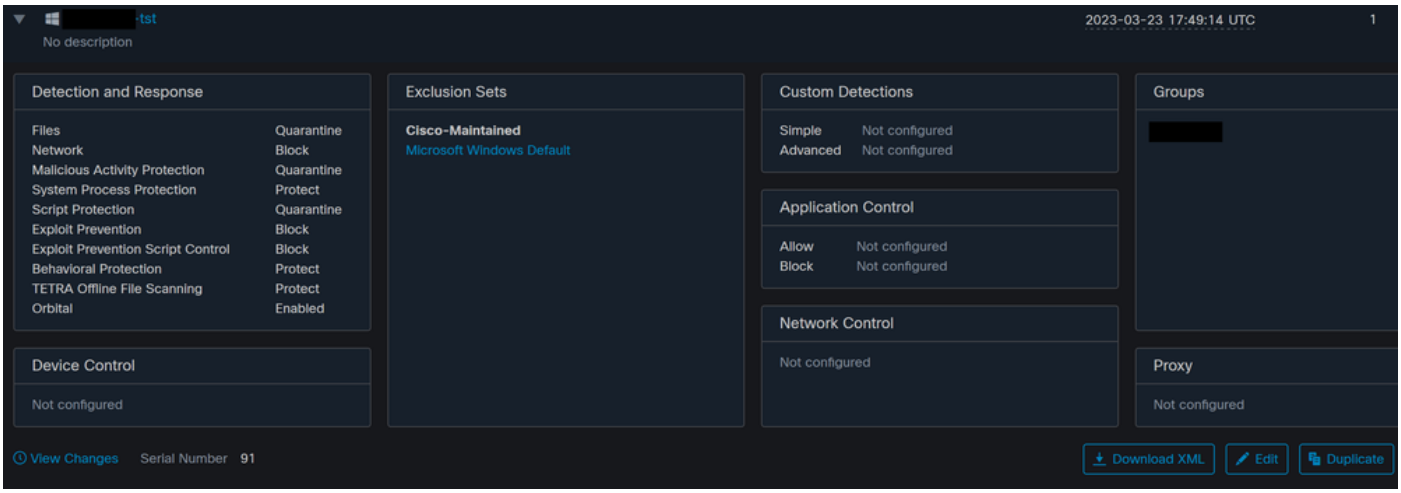
Dopo aver configurato l'analisi, fare clic su Aggiungi.



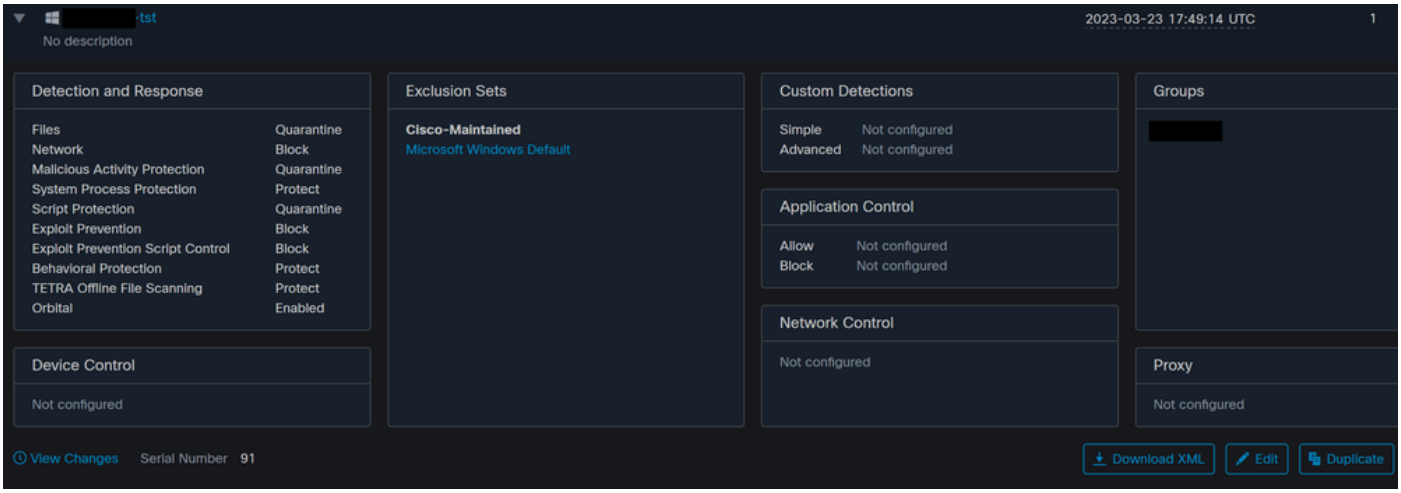
Configurazione analisi pianificata

Salvare le modifiche apportate ai criteri. Verrà visualizzato un popup che conferma le modifiche.

Popup



Modifica numero di serie



Modifica numero di serie

L'analisi è configurata nel criterio, in questo esempio, sono configurate due analisi, una Flash e una Full Scan.

```
<sched_userlogon>0</sched_userlogon>
<scheduled>20|1661470488|Daily Flash Scan (18:40)|1|3|-|48|0|2022|8|24|2122|8|24|18|40|0|0|1|1|1|0|0|0|0</scheduled>
<scheduled>20|1661470489|Daily Full Scan (18:50)|5|0|-|48|0|2022|8|24|2122|8|24|18|50|0|0|1|1|1|0|0|0|0</scheduled>
<maxarchivefilesize>52428800</maxarchivefilesize>
<maxfilesize>52428800</maxfilesize>
```

XML criteri

Vengono aggiunti a uno scheduler in HistoryDB. I caratteri accanto al tag <pianificato> sono l'ID processo (PID) che identifica l'analisi.

```
(86616093, +0 ms) Aug 25 18:43:59 [12408]: AddScheduledScanExecStatusToHistoryDB Queued 1661470488 scan. last run status: 0x0 with status: 0x0
```

ID processo

Come mostrato nell'immagine, viene inserito in coda.

```
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScheduledScanMgr::CheckAndTriggerScheduledScans scan_id: 1661470488 queued execution status: 0x0
```

Scansione in coda

È possibile eseguire una ricerca nei log per l'analisi e verificare se l'analisi può essere eseguita ora o meno. In caso affermativo, la scansione viene eseguita.

```
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScheduledScanMgr::CanTriggerNow: [TASK_TIME_TRIGGER_DAILY] executing 1661470488 scheduled scan,
bShouldTrigger: true, timeDiff: 0, days_interval: 1
(86616093, +0 ms) Aug 25 18:43:59 [8472]: ClEngineInterface::ReadOptions 1, 1, 0, 0, 120000
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScanInitiator::RequestScan loading scheduled scan ID 1661470488
```

Esecuzione scansione

È possibile notare che le opzioni per l'analisi sono caricate e il processo ScanInitiator richiede l'avvio dell'analisi.

```
(86616093, +0 ms) Aug 25 18:43:59 [8472]: ClEngineInterface::SetOptions setting scanner options
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScanInitiator::RequestScan: successfully loaded scheduled scan:
(86616093, +0 ms) Aug 25 18:43:59 [8472]: ClEngineInterface::SetOptions 1, 1, 0, 0, 120000
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScanInitiator::RequestScan: Name: Daily Flash Scan (18:40), Type: 1, Options: 3, ScanPath: -
```

Quindi, Process Scan::ScanThreadProcess avvia Scan.

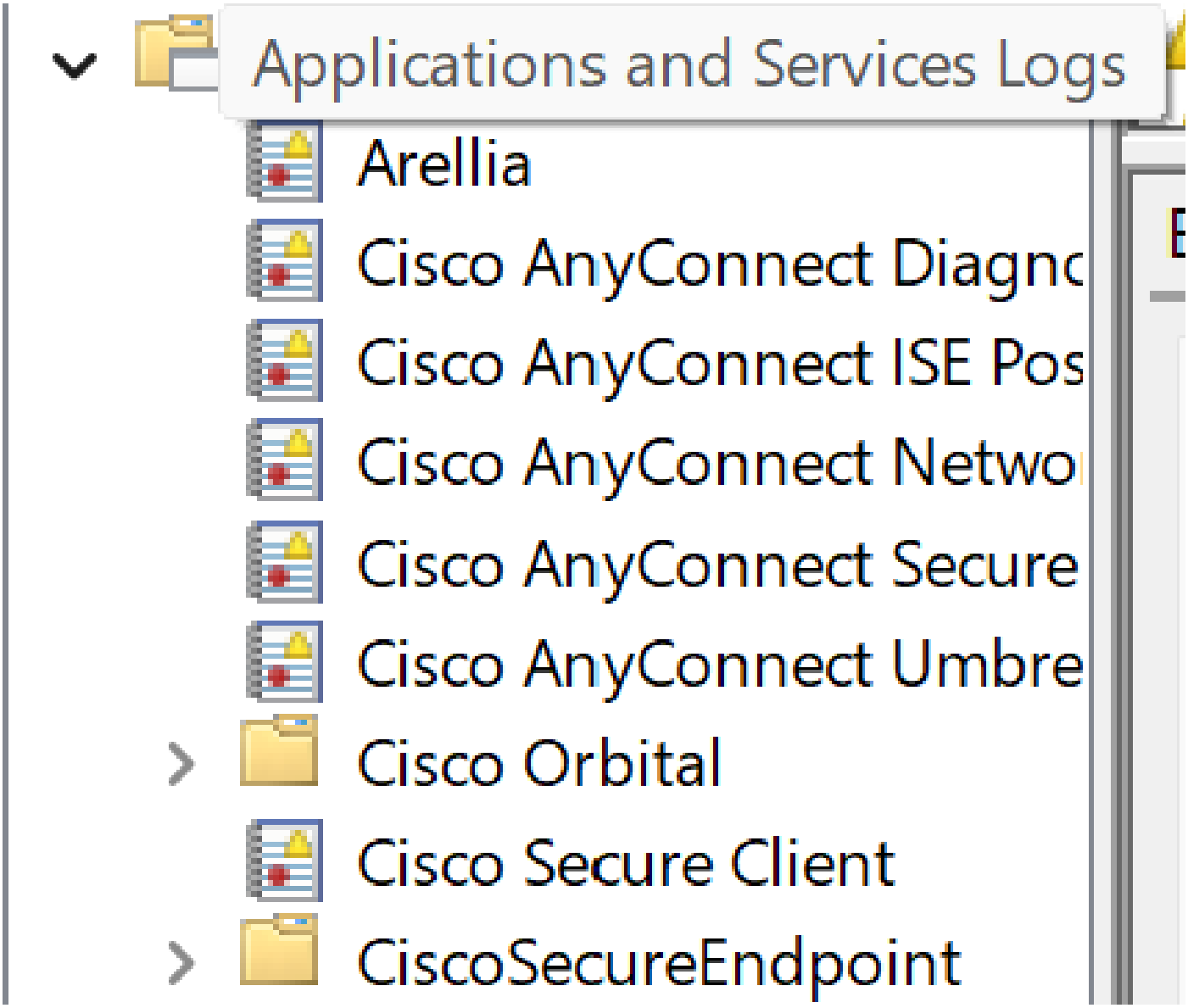
```
(86616093, +0 ms) Aug 25 18:43:59 [15372]: Scan::ScanThreadProcess: beginning scan id: 86616093, [type: 1, options: 3, 3, pid: 1661470488, initiator:
4]
```

Analogamente agli eventi precedenti, deve essere pubblicato nel cloud CSE. I log possono indicare il tipo di scansione, che in questo caso è Flash.

```
(86616093, +0 ms) Aug 25 18:43:59 [15372]: imn::CEventManager::PublishEvent: publishing type=554696714, json={"iclsa":"0","sce":108,"scx":"Flash
Scan","sid":86616093,"sit":4,"sop":3,"stp":1}, ui64EventId=7135963775756140548
```

Evento di pubblicazione dell'analisi pianificata

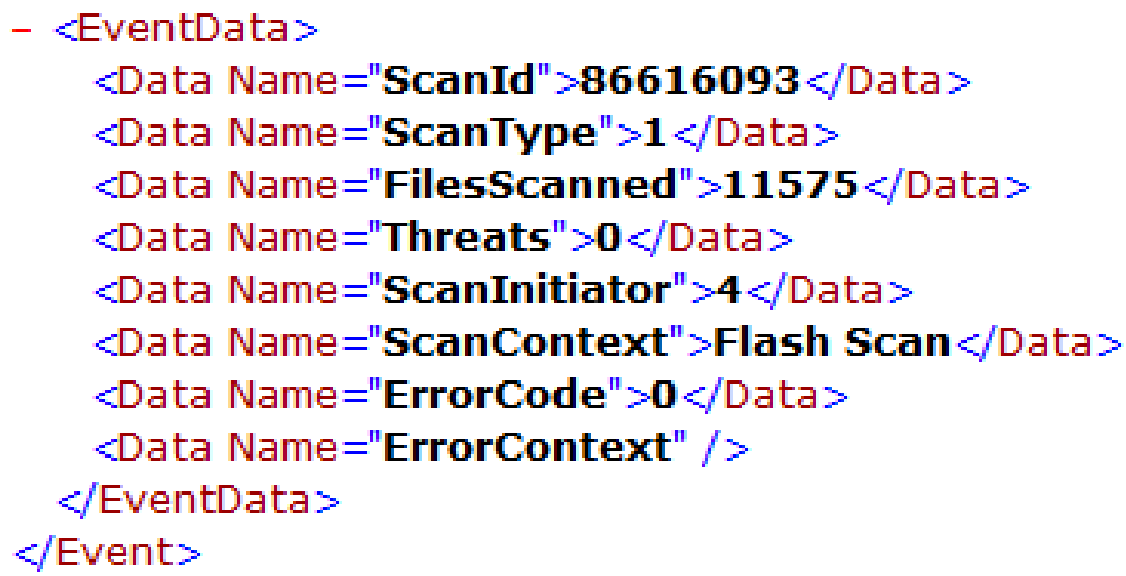
È possibile passare a Event Viewer > App and Services Registries.



Registri applicazioni e servizi

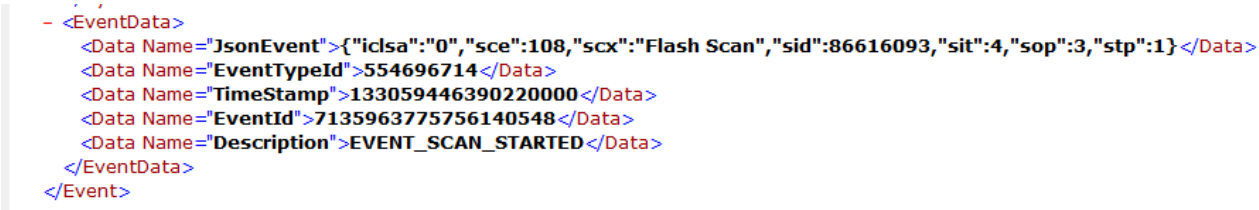
Cercare Cisco Secure Endpoint e aprire Cloud ed eventi. Ogni scheda offre una visualizzazione diversa.

Eventi:



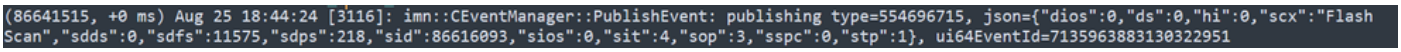
Visualizzazione eventi

Cloud:



Visualizzazione tramite cloud

Al termine dell'analisi, sarà possibile visualizzare l'evento pubblicato nel cloud.



Fine scansione - Pubblica

Analisi completa pianificata

Nel Visualizzatore eventi di Windows viene visualizzato Event Scan Started, come illustrato nell'immagine.

```
- <EventData>
    <Data Name="JsonEvent">{"iclsa":"0","sce":108,"scx":"Full Scan","sid":87216125,"sit":4,"sop":0,"stp":5}</Data>
    <Data Name="EventTypeId">554696714</Data>
    <Data Name="TimeStamp">133059452390500000</Data>
    <Data Name="EventId">7135966352736518152</Data>
    <Data Name="Description">EVENT_SCAN_STARTED</Data>
  </EventData>
</Event>
```


Al termine, sarà possibile confrontare l'evento pubblicato.


```
(88165093, +0 ms) Aug 25 19:09:48 [18536]: imn::CEventManager::PublishEvent: publishing type=1091567628, json={"dios":0,"ds":2,"hi":0,"scx":"Full Scan","sdds":46012,"sdfs":280196,"sdps":224,"sid":87216125,"sios":0,"sit":4,"sop":0,"sspc":0,"stp":5}, ui64EventId=7135970428660482061
```


È possibile visualizzarlo nel visualizzatore eventi di Windows.


```
- <EventData>
    <Data Name="JsonEvent">{"dios":0,"ds":2,"hi":0,"scx":"Full
      Scan","sdds":46012,"sdfs":280196,"sdps":224,"sid":87216125,"sios":0,"sit":4,"sop":0,"sspc":0,"stp":5}</Data>
    <Data Name="EventTypeId">1091567628</Data>
    <Data Name="TimeStamp">133059461880170000</Data>
    <Data Name="EventId">7135970428660482061</Data>
    <Data Name="Description">EVENT_SCAN_COMPLETED_DIRTY</Data>
  </EventData>
</Event>
```


Visualizzatore eventi

Altre analisi

Quando si tratta di scansioni personalizzate o rootkit, la differenza principale che avete notato è il Tipo di scansione nel Visualizzatore eventi o nei log.

Risoluzione dei problemi

Se non viene eseguita un'analisi pianificata:

- Verificare che l'endpoint sia disponibile nel momento in cui si desidera che venga eseguita l'analisi.
- Verificare che l'analisi sia pianificata nel criterio. Se non è visibile, attivare una sincronizzazione dei criteri.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).