

CSE(Secure Endpoint) Windows 스캔 검토

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[전체 스캔](#)

[플래시 스캔](#)

[예약된 스캔](#)

[예약된 전체 스캔](#)

[기타 스캔](#)

[문제 해결](#)

소개

이 문서에서는 Windows 커넥터의 다양한 스캔 유형에 대해 설명합니다.

사전 요구 사항

이 문서의 전제 조건은 다음과 같습니다.

- Windows 엔드포인트
- CSE(Secure Endpoint) 버전 v.8.0.1.21164 이상
- Secure Endpoint Console 액세스

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 보안 엔드포인트 콘솔
- Windows 10 엔드포인트
- Secure Endpoint 버전 v.8.0.1.21164

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

스캔은 Policy가 debug로 설정된 랩 환경에서 테스트되었습니다.
Connector 다운로드를 통해 설치 시 플래시 스캔을 활성화했습니다.
스캔은 Secure Client GUI 및 Scheduler에서 실행되었습니다.

전체 스캔

이 로그는 CSE GUI(Graphic User Interface)에서 전체 스캔이 요청되는 경우를 보여줍니다.

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

사용자 인터페이스에서 스캔

여기서 ScanInitiator 프로세스는 Scan 프로세스를 시작합니다.

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

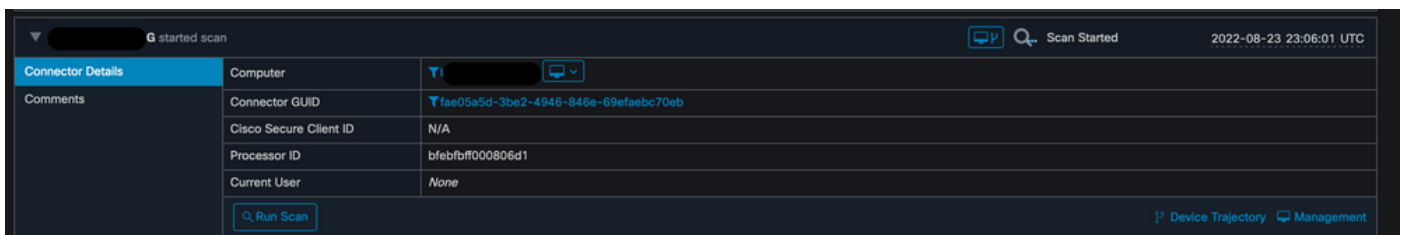
이미지에 표시된 대로 Full Scan(전체 스캔)이 GUI에서 트리거된 스캔 유형임을 확인할 수 있습니다.

다음으로 SID(Security Identifier)가 있습니다. 이는 이 특정 이벤트에 할당된 변수 길이의 값입니다.
이 보안 식별자는 로그에서 스캔을 추적하는 데 도움이 됩니다.

```
(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
```

이벤트 게시

이를 CSE 콘솔의 이벤트와 일치시킬 수 있습니다.



콘솔 이벤트

다음으로, 로그에서 다음을 확인할 수 있습니다.

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

게시 성공

이는 이벤트가 CSE 클라우드에 성공적으로 게시되었음을 의미합니다.

그런 다음 실제로 스캔을 수행합니다.

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

스캔 시작

알 수 있듯이 SID는 동일하므로 SID 1407343 스트림 아래에 있습니다.

다음은 스캔 중에 위협이 탐지될 때 커넥터가 수행하는 단계입니다.

1단계. 커넥터는 탐지를 일으킨 파일을 알려줍니다. 이 예에서는 Hacksantana Trainer GLS로 인해 탐지됩니다.

```
(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\...  
\\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]
```

파일이 탐지됨

2단계. 이벤트는 위협 탐지 이름 및 발견된 경로를 사용하여 CSE 콘솔에 게시됩니다.

```
(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\\...  
\\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":"0x00000000000000000000000000000001","ftd":"0x00000000000000000000000000000001","ftnd":0,"is":1,"md5d":"  
888949798249ad7c53f8e30725a0361","pbd":0,"pcx":0,"pfc":"0","pfs":"0","sha1d":"69d456e8aeec4c4c99b932d1911feef0328a47
```

탐지 이름

```
(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
```

위협 이벤트 게시

스캔이 완료되면 이벤트 뷰어에서 스캔의 요약을 확인할 수 있습니다.

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	23/08/2022 06:29:40 p. m.	CiscoSecureEndpoint	1249	Scan
Error	23/08/2022 06:23:18 p. m.	CiscoSecureEndpoint	1311	Quarantine
Información	23/08/2022 06:23:18 p. m.	CiscoSecureEndpoint	1300	Detection
Información	23/08/2022 06:14:24 p. m.	CiscoSecureEndpoint	1310	Quarantine
Información	23/08/2022 06:14:24 p. m.	CiscoSecureEndpoint	1300	Detection
Información	23/08/2022 06:11:55 p. m.	CiscoSecureEndpoint	1310	Quarantine
Información	23/08/2022 06:11:55 p. m.	CiscoSecureEndpoint	1300	Detection
Información	23/08/2022 06:11:25 p. m.	CiscoSecureEndpoint	1310	Quarantine
Información	23/08/2022 06:11:25 p. m.	CiscoSecureEndpoint	1300	Detection
Información	23/08/2022 06:11:24 p. m.	CiscoSecureEndpoint	1310	Quarantine
Información	23/08/2022 06:11:24 p. m.	CiscoSecureEndpoint	1300	Detection

Evento 1249, CiscoSecureEndpoint

General Detalles

Scan (Full Scan) completed successfully. A total of 278172 files were scanned and 6 threats were detected.

이벤트 뷰어

플래시 스캔

플래시 스캔은 빠르고, 몇 초에서 몇 분 만에 끝납니다.

이 예에서는 스캔이 언제 시작되는지 볼 수 있으며, 이전과 마찬가지로 이번에는 값이 2458015인 SID가 제공됩니다.

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

플래시 스캔 시작

다음 작업은 CSE 클라우드에 이벤트를 게시하는 것입니다.

```
(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
```

스캔이 완료되면 이벤트가 클라우드에 게시됩니다.

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

스캔 완료 게시

Windows 이벤트 뷰어에서 이벤트를 볼 수 있습니다. 알 수 있듯이, 정보는 로그에 표시되는 정보와 동일합니다.

```
- <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>
```

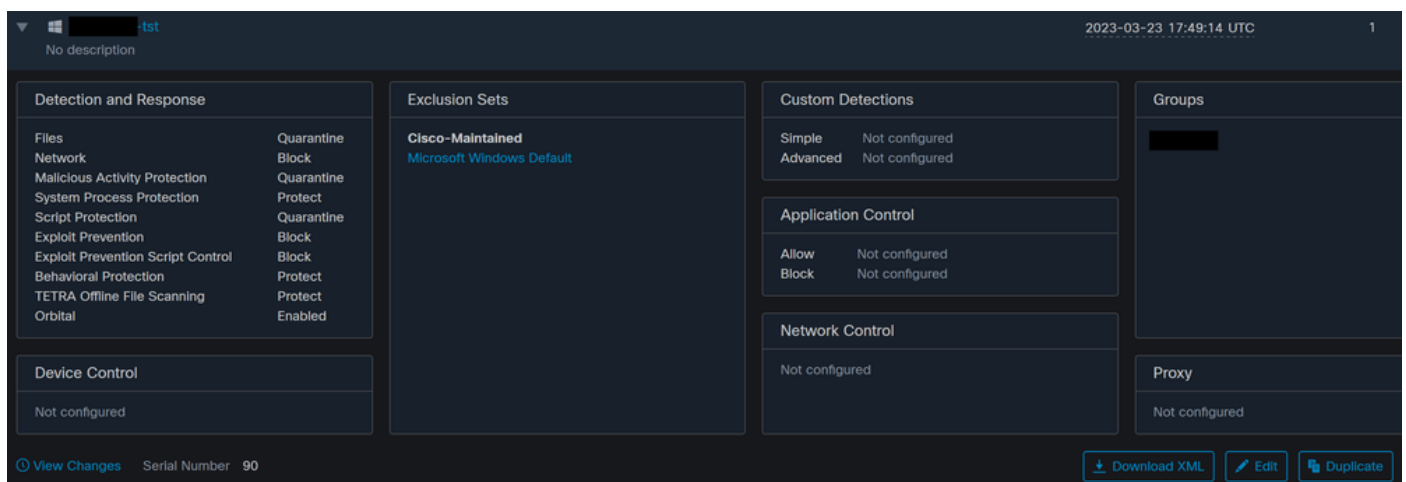
JSON 이벤트

예약된 스캔

예약 스캔에 대해서는 일련의 측면을 알고 있어야 합니다.

스캔이 예약되면 일련 번호가 변경됩니다.

여기서 테스트 정책에는 예약된 스캔이 없습니다.



정책 일련 번호

스캔을 예약하려면 Edit를 클릭합니다.

탐색 Advanced Settings > Scheduled Scans.

Product Updates

Advanced Settings

Administrative Features

Client User Interface

File and Process Scan

Cache

Endpoint Isolation

Orbital

Engines

TETRA

Network

Scheduled Scans

고급 설정

새로 만들기를 클릭합니다.

You can add multiple scan schedules for a given policy. Each scheduled scan will run at local computer time.

Schedule [+ New](#)

새 스캔 컨피그레이션

옵션은 다음과 같습니다.

- 스캔 간격
- 스캔 시간
- 스캔 유형

Scan을 구성한 후 Add를 클릭합니다.

Scheduled Scan


Scan Interval

Scan Time :

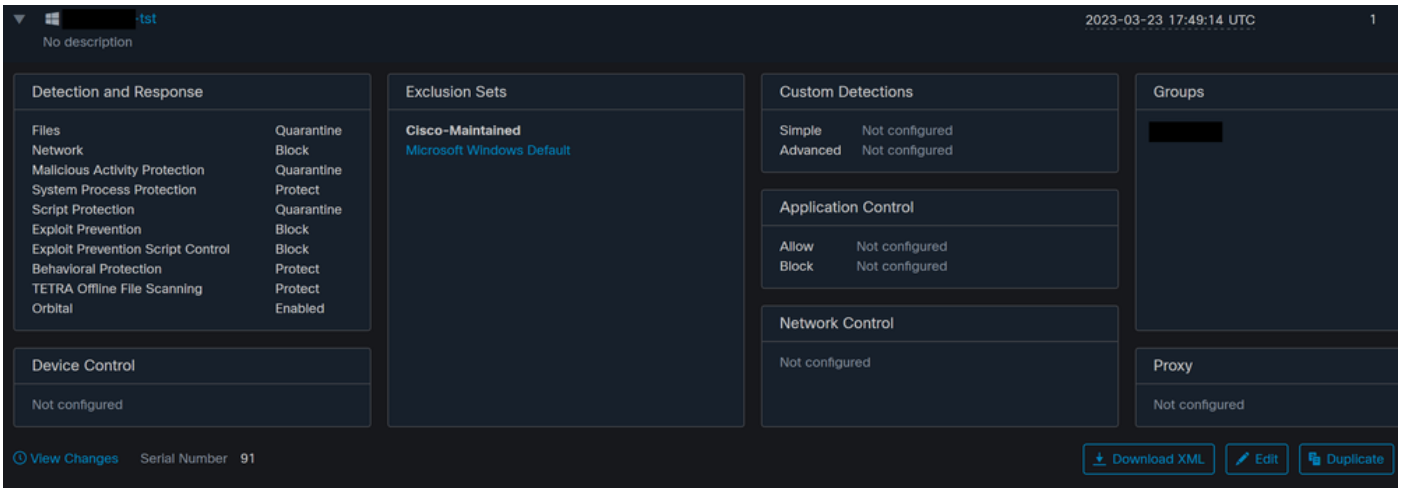
Scan Type

예약된 스캔 컨피그레이션

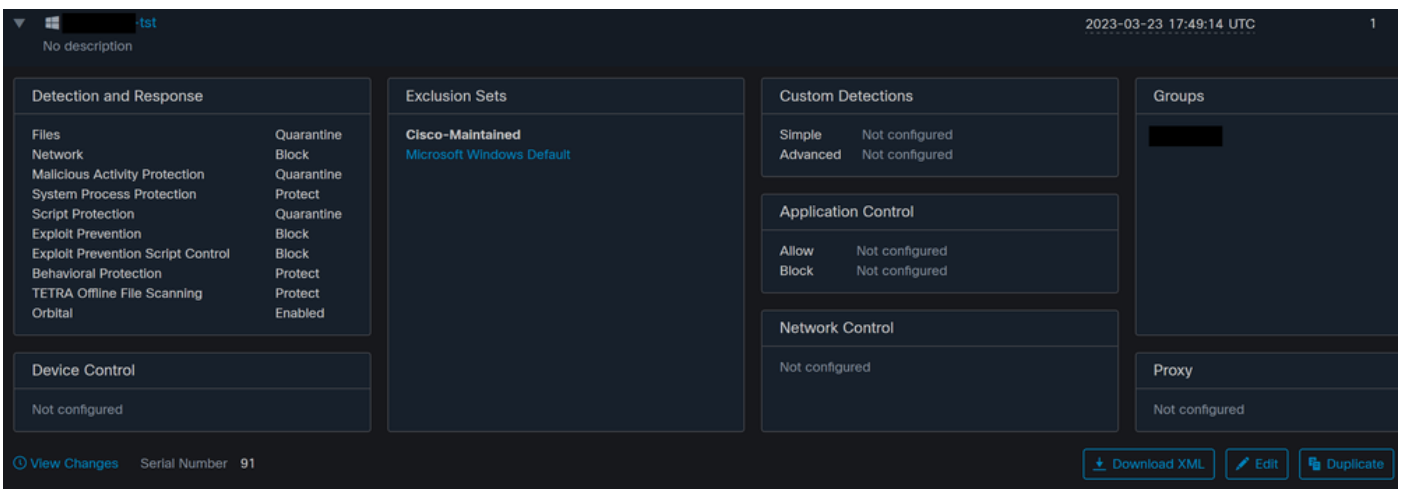
정책 변경 사항을 저장하면 변경 사항을 확인하는 팝업이 나타납니다.

 Policy " [redacted] -tst" successfully updated.

팝업



일련 번호 변경



일련 번호 변경

스캔은 Policy(정책)에서 구성되며, 이 예에서는 Flash(플래시) 스캔과 Full Scan(전체 스캔)의 두 스캔이 구성됩니다.


```
<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>
```

정책 XML

HistoryDB의 스케줄러에 추가됩니다. <scheduled> 태그 옆의 문자는 스캔을 식별하는 Process ID(PID)입니다.

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

프로세스 ID

그림에 표시된 것처럼 대기열에 추가됩니다.

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

스캔 대기 중

로그에서 스캔을 검색할 수 있으며, 스캔을 지금 실행할 수 있는지 여부를 확인할 수 있습니다. 가능한 경우 스캔이 실행됩니다.

```
(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
```

스캔 실행 가능

스캔 옵션이 로드되어 있고 ScanInitiator 프로세스에서 스캔을 시작하도록 요청합니다.

```
(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: -
```

그런 다음 Process Scan::ScanThreadProcess에서 스캔을 시작합니다.

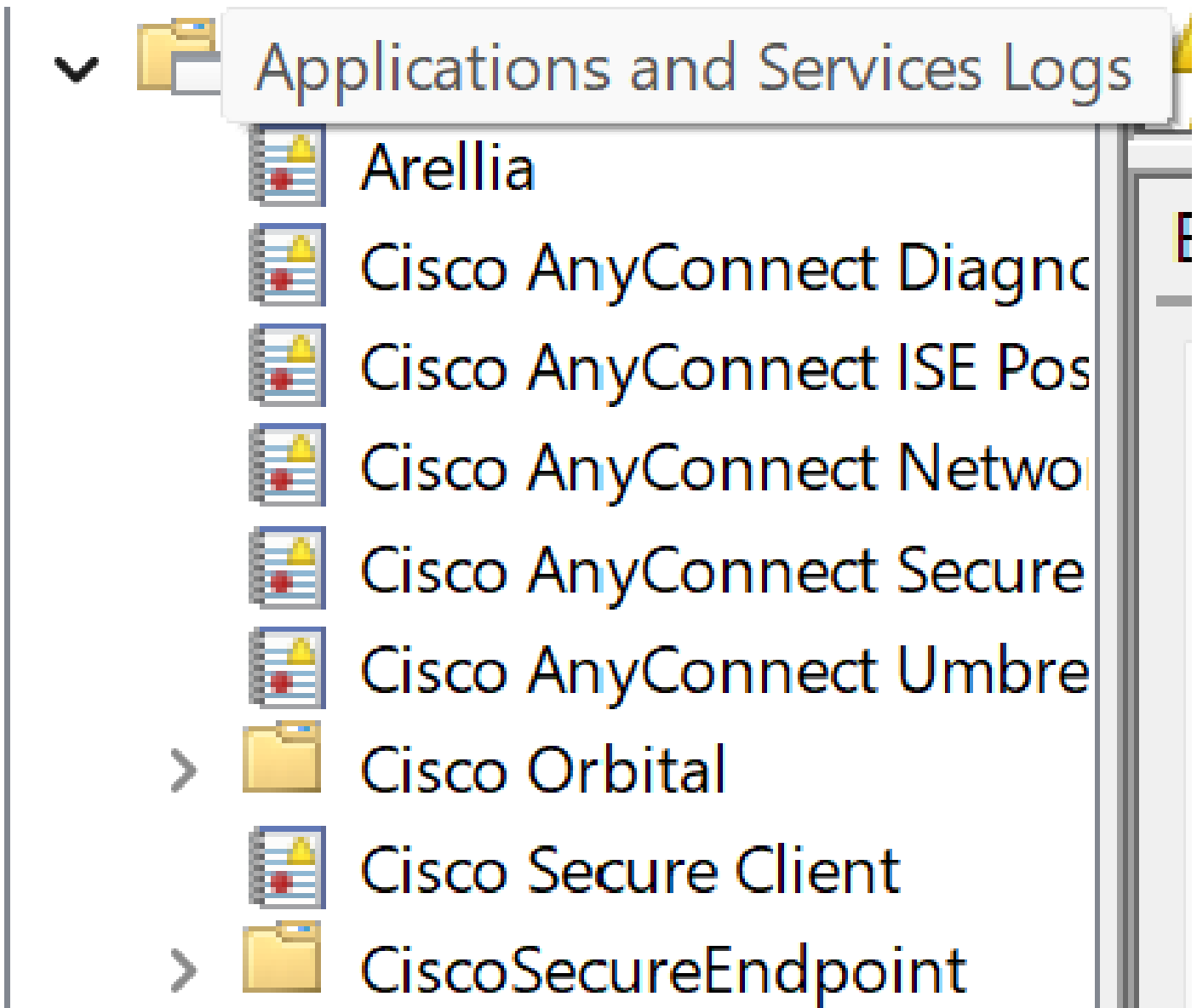
```
(86616093, +0 ms) Aug 25 18:43:59 [15372]: Scan::ScanThreadProcess: beginning scan id: 86616093, [type: 1, options: 3, 3, pid: 1661470488, initiator:
4]
```

이전 이벤트와 마찬가지로 CSE 클라우드에 게시해야 합니다. 로그는 Scan의 유형을 알려주며, 이 경우 Flash입니다.

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

예약된 스캔의 이벤트 게시

다음 위치로 이동 Event Viewer > App and Services Registries.



애플리케이션 및 서비스 로그

Cisco Secure Endpoint를 검색하고 클라우드 및 이벤트를 엽니다. 각 탭은 서로 다른 보기를 제공합니다.

이벤트:

```
- <EventData>
  <Data Name="ScanId">86616093</Data>
  <Data Name="ScanType">1</Data>
  <Data Name="FilesScanned">11575</Data>
  <Data Name="Threats">0</Data>
  <Data Name="ScanInitiator">4</Data>
  <Data Name="ScanContext">Flash Scan</Data>
  <Data Name="ErrorCode">0</Data>
  <Data Name="ErrorContext" />
</EventData>
</Event>
```

이벤트 보기

클라우드:

```
- <EventData>
  <Data Name="JsonEvent">{"iclsa":"0","sce":108,"scx":"Flash Scan","sid":86616093,"sit":4,"sop":3,"stp":1}</Data>
  <Data Name="EventTypeId">554696714</Data>
  <Data Name="TimeStamp">133059446390220000</Data>
  <Data Name="EventId">7135963775756140548</Data>
  <Data Name="Description">EVENT_SCAN_STARTED</Data>
</EventData>
</Event>
```

클라우드 뷰

스캔이 완료되면 클라우드에 게시된 이벤트를 볼 수 있습니다.

```
(86641515, +0 ms) Aug 25 18:44:24 [3116]: imn::CEventManager::PublishEvent: publishing type=554696715, json={"dios":0,"ds":0,"hi":0,"scx":"Flash Scan","sdds":0,"sdfs":11575,"sdps":218,"sid":86616093,"sios":0,"sit":4,"sop":3,"spsc":0,"stp":1}, ui64EventId=7135963883130322951
```

스캔 완료 게시

예약된 전체 스캔

Windows 이벤트 뷰어는 이미지에 표시된 대로 Event Scan Started(이벤트 스캔 시작됨)를 표시합니다.

```

- <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>

```

완료되면 게시된 이벤트를 비교할 수 있습니다.

```

(88165093, +0 ms) Aug 25 19:09:48 [18536]: imn::CEEventManager::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

```

Windows의 이벤트 뷰어에서 이를 볼 수 있습니다.

```

- <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>

```

이벤트 뷰어

기타 스캔

사용자 지정 또는 루트킷 스캔의 경우 이벤트 뷰어 또는 로그의 스캔 유형이 주된 차이점입니다.

문제 해결

Schedule Scan이 발생하지 않는 경우:

- 스캔이 수행될 때까지 엔드포인트를 사용할 수 있는지 확인합니다.
- Policy(정책)에서 Scan(스캔)이 예약되었는지 확인합니다. 표시되지 않으면 정책 동기화를 트리거합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.