위협 분석을 위한 기본 궤도 검색 쿼리

목차

소개

이 문서에서는 위협 분석을 위한 기본 궤도 검색 쿼리에 대해 설명합니다.

사전 요구 사항

요구 사항

위협 및 악성코드에 대한 이해와 SQL(Structured Query Language) 테이블에 대한 기본적인 이해에 관심이 있는 것을 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Windows용 Secure Endpoint Connector 버전 7.1.5 이상
- Mac용 Secure Endpoint Connector 버전 1.16 이상
- Linux용 Secure Endpoint Connector 버전 1.17 이상
- 보안 엔드포인트 사용자에게 Orbital을 배포하는 관리자 역할을 할당해야 합니다.

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

Custom Queries는 Orbital과 Osquery의 기능을 신속하게 학습하여 위협 추적에 활용할 수 있도록 도와야 합니다.

오비탈은 오비탈에 특화된 테이블 외에 오비쿼리스 스톡 테이블을 활용한다. Orbital을 통해 반환된 결과는 Secure Endpoint, Secure Malware Analytics, SecureX Threat Response와 같은 다른 애플리케이션에 전송될 수 있으며 Amazon S3, Microsoft Azure, Splunk와 같은 RDS(원격 데이터 저장소)에 저장될 수 있습니다.

Orbital Investigate 페이지를 사용하여 엔드포인트에서 실시간 쿼리를 작성하고 실행하여 더 많은 정보를 수집합니다. 오비탈은 기본 SQL 명령으로 데이터베이스처럼 기기를 쿼리할 수 있는 오비쿼리를 사용합니다.

다음은 간단한 예입니다. TABLE1, table2 WHERE column2='value'에서 column1, column2를 선택합니다.

이 예제에서 column1과 column2는 데이터를 선택할 테이블의 필드 이름입니다. 테이블에서 사용 가능한 모든 필드를 선택하려면 다음 구문을 사용합니다. 표 1에서 *를 선택합니다.

액세스

다음 사이트에서 직접 궤도 열기:

북미 - https://orbital.amp.cisco.com

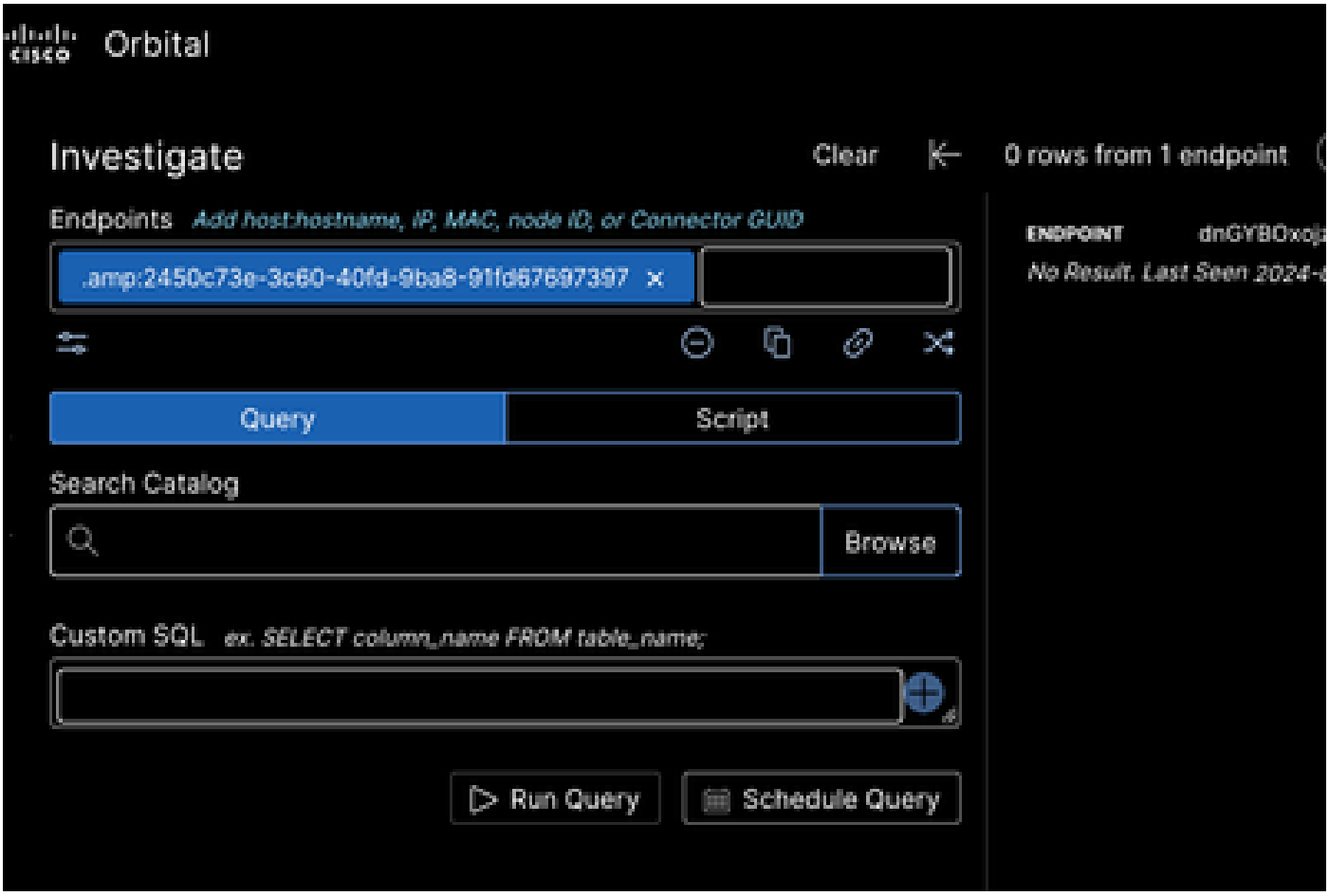
유럽 - https://orbital.eu.amp.cisco.com

아시아 태평양 - https://orbital.apjc.amp.cisco.com

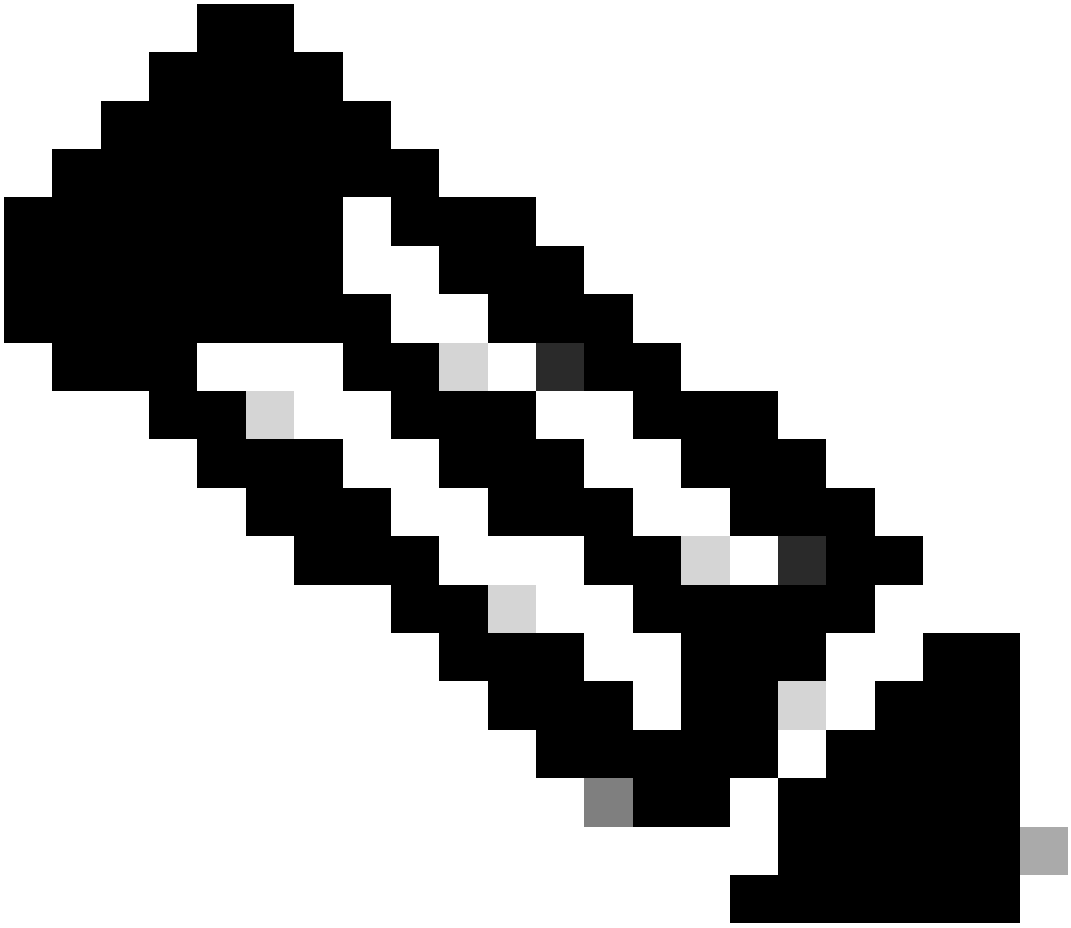
또는

Secure Endpoint Console(보안 엔드포인트 콘솔)에서 영향을 받는 호스트 시스템을 선택하고 Investigate in Orbital을 클릭합니다.

앞서 언급한 대로 Orbital Catalog(찾아보기 클릭) 또는 Custom SQL(사용자 지정 SQL) 섹션에서 사용자 지정 쿼리를 입력할 수 있는 옵션이 있습니다.



사용자 지정 쿼리



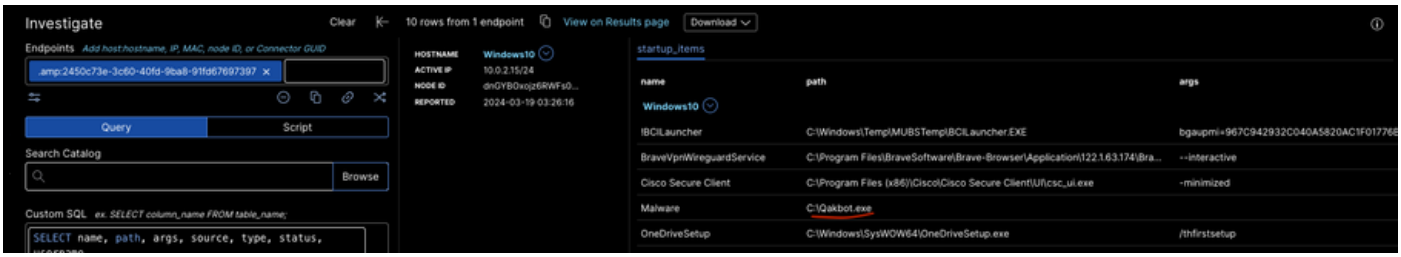
참고: 호스트 시스템이 랩 네트워크에 있으며 시스템/네트워크를 손상시키지 않도록 유지하려고 합니다.

---

1. 시작 항목

공격자는 시작 항목을 악용하여 감염된 시스템에서 지속성을 유지할 수 있습니다. 즉, 시스템을 다시 시작할 때마다 악성 소프트웨어가 계속 실행되거나 자동으로 다시 실행됩니다. 다음 예에서 Qakbot.exe는 호스트 시스템에서 실행됩니다.

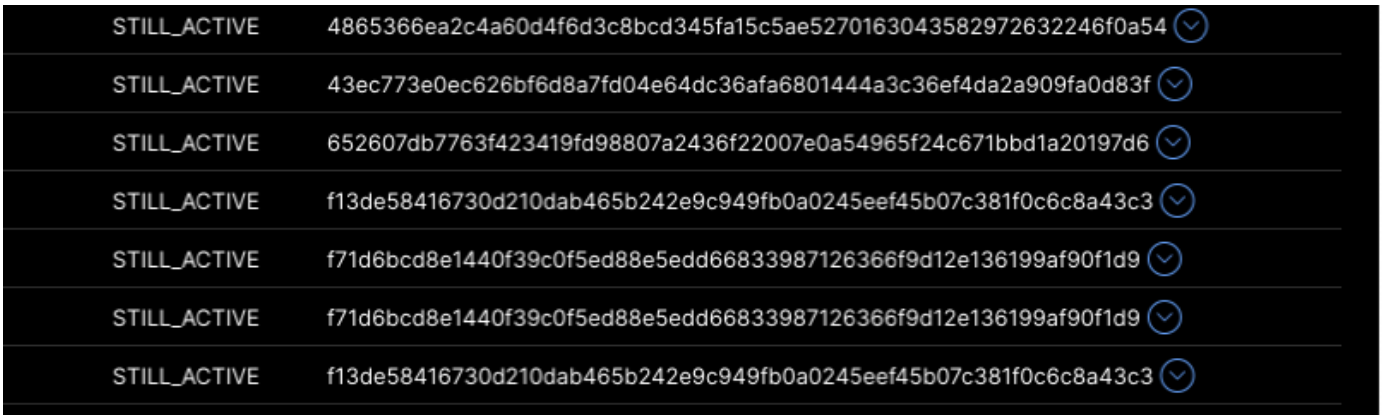
```
SELECT name, path, args, source, type, status, username
FROM startup_items;
```



2. 실행 중인 프로세스의 Sha256 해시

SHA256 해시는 자연 상태에서 실행 중인 프로세스와 기본적으로 연결되지 않습니다. 그러나 보안 소프트웨어 및 시스템 모니터링 툴은 실행 파일의 무결성 및 신뢰성을 확인하기 위해 실행 파일의 실행 중인 프로세스의 SHA256 해시를 계산할 수 있습니다.

```
 SELECT
p.pid, p.name, p.path, p.cmdline, p.state, h.sha256
FROM processes p
INNER JOIN hash h
ON p.path=h.path;
```



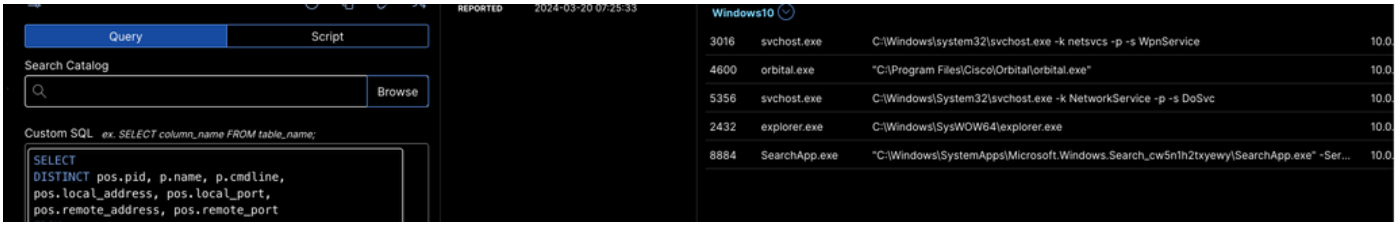
파일의 관련 해시가 악의적인 경우 이 쿼리로 식별할 수 있습니다.

3. 네트워크 연결 프로세스

네트워크 연결이 있는 프로세스는 네트워크 또는 인터넷을 통해 다른 장치와 통신하기 위해 네트워크 인터페이스를 적극적으로 사용하는 프로그램 또는 시스템 서비스입니다.

```
SELECT
```

```
DISTINCT pos.pid, p.name, p.cmdline, pos.local_address, pos.local_port, pos.remote_address, pos.remote_
FROM processes p
JOIN process_open_sockets pos USING (pid)
WHERE
pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1", “0");
```



4. Localhost가 아닌 네트워크 연결을 사용하는 권한 있는 프로세스

관리자 또는 시스템 계정의 권한과 같이 상승된 권한이 있고 네트워크를 통해 외부 장치 또는 서비스와 통신하는 프로그램 또는 서비스를 실행 중입니다. 즉, 127.0.0.1(localhost) 또는 ::1(IPv6 localhost)이 아닌 IP 주소입니다.

```
SELECT DISTINCT p.name, p.cmdline, pos.pid, pos.local_address, pos.local_port, pos.remote_address, pos.
FROM processes p JOIN process_open_sockets pos USING (pid)
WHERE pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1")
```

PID(Packet Identifier) 목록이 있으면 Custom Queries(맞춤형 쿼리)에서 그에 따라 추가할 수 있습니다.

```
SELECT DISTINCT p.name, p.cmdline, pos.pid, pos.local_address, pos.local_port, pos.remote_address, pos.
FROM processes p JOIN process_open_sockets pos USING (pid)
WHERE pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1") and p.uid=1436
```

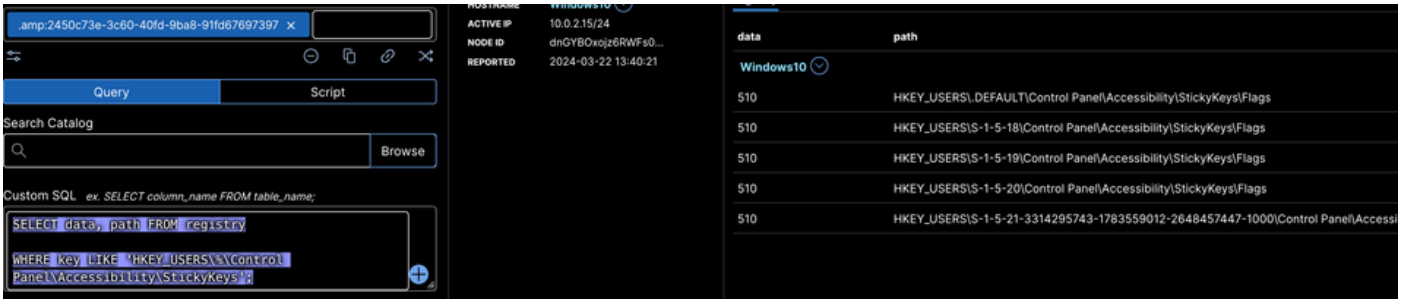
5. 레지스트리 백업/복원 모니터링

백업 또는 복원 작업을 통해 Windows 레지스트리가 변경된 이벤트 추적. Windows 레지스트리는 Microsoft Windows 운영 체제의 구성 설정과 옵션을 저장하는 계층적 데이터베이스입니다.

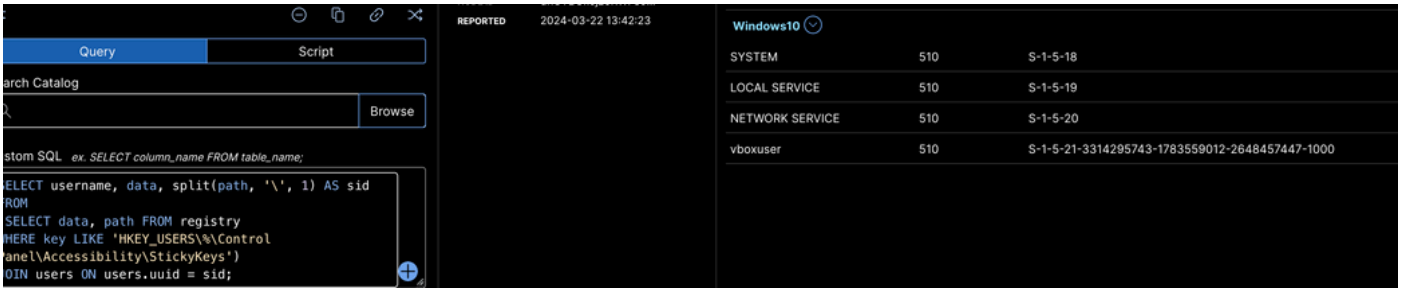
```
SELECT key AS reg_key, path, name, data, DATETIME(mtime, "unixepoch") as last_modified
```

```
FROM registry
WHERE key LIKE "HKEY_LOCAL_MACHINE\system\currentcontrolset\control\backuprestore\filesnottosnapshot";
```

```
SELECT data, path FROM registry
WHERE key LIKE 'HKEY_USERS\%\Control Panel\Accessibility\StickyKeys';
```




```
SELECT username, data, split(path, '\', 1) AS sid
FROM
(SELECT data, path FROM registry
WHERE key LIKE 'HKEY_USERS\%\Control Panel\Accessibility\StickyKeys')
JOIN users ON users.uuid = sid;
```



6. 파일 검색

사용자가 파일 이름, 콘텐츠, 속성 또는 메타데이터 등의 다양한 기준을 사용하여 컴퓨터에서 파일 및 폴더를 찾을 수 있습니다.

```
SELECT
f.directory, f.filename, f.uid, f.gid,
f.mode, f.device, f.size,
f.atime,
f.mtime,
f.ctime,
f.btime,
f.hard_links, f.symlink, f.file_id, h.sha256
FROM file f
LEFT JOIN hash h on f.path=h.path
```

```
WHERE
f.path LIKE (SELECT v from __vars WHERE n="file_path") AND
f.path NOT LIKE (SELECT v from __vars WHERE n="not_file_path");
```

PARAMETERS(매개변수) > File Path(파일 경로)로 이동하고 %.dll 또는 %.exe 또는 %.png를 클릭합니다.

7. Powershell 기록 모니터링

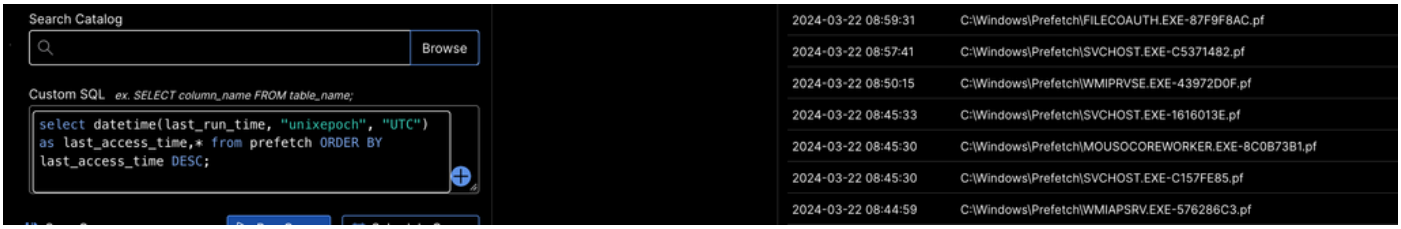
PowerShell 세션에서 실행된 명령을 추적하는 방식입니다. 보안 및 규정 준수를 위해 PowerShell 기록 모니터링이 특히 중요할 수 있습니다.

```
SELECT time, datetime, script_block_id, script_block_count, script_text, script_name, script_path
FROM orbital_powershell_events
ORDER BY datetime DESC
LIMIT 500;
```

8. 프리페치 쿼리

애플리케이션 로딩을 가속화하는 성능 기능. 프리페치에는 시스템에서 소프트웨어를 로드하고 실행하는 방법을 분석한 다음 이에 대한 정보를 특정 파일에 저장하는 것이 포함됩니다.

```
select datetime(last_run_time, "unixepoch", "UTC") as last_access_time,*
from prefetch
ORDER BY last_access_time DESC;
```

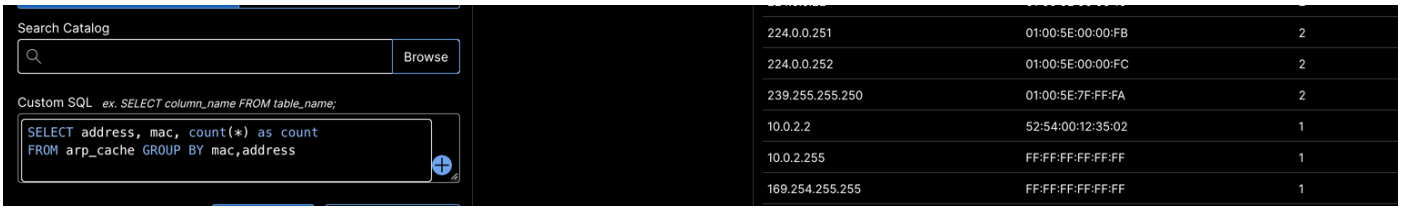


프리페치는 SQL Server가 중첩된 루프 조인에 대해 여러 I/O 요청을 병렬로 실행할 수 있는 메커니즘입니다.

9. ARP(Address Resolution Protocol) 캐시 검사

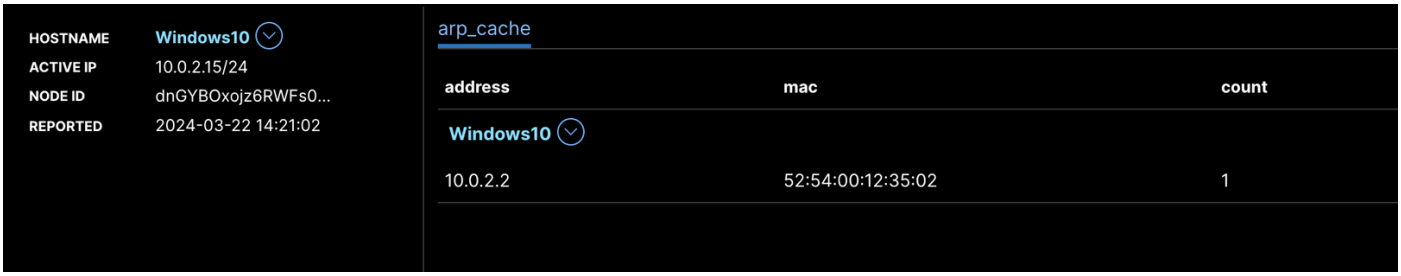
컴퓨터 또는 네트워크 장치에 있는 ARP 캐시의 내용을 검사하는 작업이 포함됩니다. ARP 캐시는 IP 주소와 해당 MAC 주소 간의 매핑을 저장하는 테이블입니다.

```
SELECT address, mac, count(*) as count
FROM arp_cache GROUP BY mac,address;
```



다음 예에서는 ARP 캐시에서 Suspicious MAC 주소 및 그 카운트를 계산합니다.

```
SELECT address, mac, count(*) as count
FROM arp_cache GROUP BY mac,address
HAVING COUNT(mac) >= (SELECT count FROM arp_cache WHERE count>=1)
AND mac LIKE (SELECT mac FROM arp_cache WHERE mac="52:54:00:12:35:02");
```



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.