

결정이 차단된 DNS 활동 로그 항목 트러블슈팅

목차

문제

다음 증상 중 하나 이상이 보고됩니다.

- Activity Search(DNS 이벤트로 필터링된 Monitor(모니터링) > Activity Search(활동 검색)에서는 도메인에 대해 Decision/Action = Blocked(결정/작업 = 차단됨)를 표시하지만 인터넷 액세스 규칙을 검토하는 경우 해당 규칙을 확실히 차단하는 규칙이 나타나지 않습니다.
- 도메인이 관리자가 유지 관리하는 차단 대상 목록에 없습니다.

환경

- 이 문서의 정보는 다음을 기반으로 합니다.
 - Cisco SSE(Secure Access) 클라우드 플랫폼
 - Cisco Secure Client 5.x - Roaming Security Module이 보안 액세스 조직에 구축되어 등록됨

해결

1단계. 평가된 ID를 확인합니다

- 어떤 신원에 대한 결정이 내려졌는지 확인합니다. 이벤트가 예상 로밍 컴퓨터 또는 사용자 대신 네트워크, 사이트 또는 터널 ID를 표시하는 경우 쿼리가 검토한 규칙과 다른 규칙 집합과 일치합니다.

- 로밍 사용자의 경우 디바이스가 Protected(보호됨)로 등록되고 보고되는지 확인합니다

ID 불일치: 의도한 ID가 적용되도록 구축을 수정합니다. 즉, 로밍 디바이스를 등록하거나, AD/사용자 그룹 매핑을 수정하거나, 네트워크 ID 규칙 집합을 조정합니다. 잘못 일치하는 규칙을 느슨하게 하지 않습니다.

2단계: 보안 카테고리 일치 확인

- 이벤트에 보안 카테고리(악성코드, C2, 피싱, 새로 발견된 도메인, DNS 터널링 등)가 포함되어 있으면, 해당 블록은 일치하는 규칙 집합의 보안 설정에서 가져온 것입니다. 즉, 대상 목록 또는 콘텐츠 규칙이 도메인을 참조하지 않아도 됩니다.
- Cisco Talos Intelligence 포털(<https://talosintelligence.com/>)(Reputation Center 조회)에서 도메인의 현재 평판 및 [범주화](#)를 조회합니다.
- Talos에 표시된 범주화 또는 평판이 올바르지 않은 경우 <https://talosintelligence.com/>을 통해 Talos에 분쟁/재분류 요청(케이스를 열림)을 제출하여 도메인이 재평가되도록 [합니다](#). Talos에서 분류를 업데이트하면 변경 사항이 보안 액세스 시행으로 전파됩니다.

3단계: CNAME 체인 검사

- 필터링되지 않은 유리한 지점에서 도메인을 확인하고 전체 응답 체인을 검사합니다(예: `dig +noall +answer <domain>` 또는 `nslookup -debug <domain>`).
- 대상 목록 및 Talos 범주화를 기준으로 체인의 각 CNAME 대상을 확인합니다. 차단된 CNAME 대상은 분명히 정리된(clean) 쿼리된 도메인에서 차단된(Blocked) 결정을 설명합니다.

4단계: 실제 ID에 대한 정책 하향식 재평가

- 1단계에서 ID로 인터넷 액세스 규칙을 순서대로 살펴보고 각 규칙의 ID 범위, 일정, 활성화 상태 및 보안/콘텐츠/애플리케이션 설정을 기본 규칙까지 확인합니다.
- 정확한 ID 및 대상이 포함된 정책 테스터(예: policy.test.sse.cisco.com/?=cisco.com)를 사용하여 어떤 규칙을 Secure Access가 일치로 보고하는지 확인하고 이를 이벤트에 명명된 규칙과 비교합니다.

특별한 경우: 새로 본 도메인

이벤트의 보안 카테고리가 NSD(New Seen Domains)인 경우

기본 설정 순서대로 교정 옵션:

비즈니스 크리티컬한 도메인인 경우 해당 규칙에서 참조하는 Allow destination 목록에 추가합니다. 허용 항목은 해당 대상의 NSD 보안 블록보다 우선합니다.

암호화된 DNS(DoH) 및 QUIC 비활성화

암호화된 DNS 및 QUIC는 DNS 레이어 가시성 차이를 유발하여 활동 검색 결과를 혼란스럽게 만들 수 있습니다. 브라우저 DoH를 통해 해결된 쿼리는 Secure Access 확인기에 도달하지 않으므로 로그에서 완전히 누락됩니다. 반면 DoH 공급자 도메인 자체는 Blocked 이벤트로 표시될 수 있습니다.

관리되는 엔드포인트에서 이러한 전송을 비활성화하면 모든 DNS가 검사 가능한 상태로 유지되고 작업 로그는 실제 엔드포인트 동작을 반영합니다.

브라우저당 HTTPS(DoH)를 통한 DNS

Google Chrome

- 수동: chrome://settings/security으로 이동하고 Use secure DNS(보안 DNS 사용)를 끕니다.

Microsoft Edge

- 수동: edge://settings/privacy으로 이동하고 Use secure DNS(보안 DNS 사용)를 끕니다.

Mozilla Firefox

- 수동: Menu(메뉴) > Settings(설정) > Privacy & Security(개인정보 및 보안) > DNS over HTTPS(또는 이전 버전의 Network Settings(네트워크 설정))를 선택하고 Off(끄기)/Enable DNS over HTTPS(HTTPS를 통해 DNS 활성화)를 선택 취소합니다.

- 참고: Umbrella/Secure Access Resolvers는 기본적으로 DoH를 해제하도록 Firefox에 신호를 보내는 방식으로 Mozilla 카나리 도메인(use-application-dns.net)에 응답합니다. 사용자 설정 DoH 구성이 카나리아 검사를 재정의하므로 명시적 GPO 설정이 계속 권장됩니다. 주의: mozilla kill-switch/canary 도메인을 차단 대상 목록에 추가하지 마십시오. 차단 페이지 A 레코드 응답은 유효한 것으로 처리되며 Firefox에서 DoH 사용량을 유지하거나 업그레이드하도록 할 수 있습니다.

QUIC(HTTP/3)

QUIC는 UDP/443을 통해 실행되며 일반 웹 트래픽과 DoH3(DNS over HTTP/3)을 모두 전달하면서 TCP가 필요한 검사 경로를 우회할 수 있습니다.

QUIC를 비활성화하면 브라우저가 TCP 기반 HTTP/2 또는 HTTP/1.1로 돌아가게 되어 완전한 가시성이 복원됩니다.

- 크롬 / 엣지: 수동(비영구적, 사용자 변경 가능): `chrome://flags/#enable-quic` / `edge://flags/#enable-quic`를 Disabled로 설정합니다.
- Firefox: `network.http.http3.enable = false`(`about:config` 또는 `policy/AutoConfig`) 환경 설정을 지정합니다.

이러한 단계 후에도 이벤트에 대해 보고된 일치 규칙을 컨피그레이션과 조정할 수 없는 경우, Cisco TAC에서 케이스를 열고 관련 규칙 및 대상 목록의 스크린샷과 함께 활동 검색 이벤트 내보내기(표준 시간대, ID, 일치 규칙, 카테고리, 레코드 유형 및 도메인이 포함된 타임스탬프)를 제공합니다.

원인

Talos 인텔리전스(Security category match) - 관리자가 명시적으로 구성한 대상 목록 또는 콘텐츠 규칙이 아닌 Cisco Talos 평판 및 범주화를 기반으로 하는 보안 설정(예: Malware, Command and Control, Phishing, Cryptomining, DNS Tunneling 또는 Newly Seen Domains)에 의해 도메인이 차단됩니다. 이는 "일치하지 않음" 블록의 가장 빈번한 원인입니다.

ID 속성 불일치 - 쿼리가 예상과 다른 ID(로밍 컴퓨터 대신 네트워크/사이트 ID, 다른 AD 사용자/그룹 또는 등록되지 않은 장치가 네트워크 수준 정책으로 돌아가기 때문)에 다른(대개 더 엄격하거나 기본) 규칙이 일치했습니다.

규칙 순서 및 기본 규칙 - 정책에서 더 높은 범위의 규칙(또는 맨 아래의 기본/모두 탐지 규칙)이 의

도된 허용 규칙보다 먼저 일치합니다. 의도한 규칙을 비활성화하거나, 예약하거나, 영향받는 소스를 포함하지 않는 id로 범위를 지정할 수도 있습니다.

대상 목록 상속 - 차단 대상 목록에는 모든 하위 도메인(app.example.com)을 암시적으로 포괄하는 상위 도메인(example.com)이 포함되어 있거나 도메인이 확인하는 IP/CIDR이 포함되어 있습니다. 정확한 FQDN에 대한 목록 검색만으로는 이를 확인할 수 없습니다.

CNAME 체인 차단 - 쿼리된 도메인이 허용되지만 해당 확인 체인은 차단된 도메인(일반적으로 CDN, 추적기 또는 파킹/차단된 호스트)에 대한 CNAME을 포함합니다. 이 결정이 체인에 적용되고 로그에 원래 쿼리된 도메인이 Blocked로 표시됩니다.

애플리케이션 또는 콘텐츠 범주 일치 - 도메인이 차단된 애플리케이션(애플리케이션 컨트롤) 또는 관리자가 연결하지 않은 콘텐츠 범주에 속합니다. 분류는 직관과는 다를 수 있습니다(예: 파일 공유 또는 프록시/익명기로 분류된 비즈니스 툴).

최근 정책 또는 분류 변경 - 정책 또는 Talos 분류가 최근에 변경되었습니다. 검토 중인 이벤트가 변경 또는 정책 전파/클라이언트 동기화의 전후에 추가되거나 쿼리 시점에 완료되지 않았습니다.

관련 콘텐츠

- [Umbrella에 대한 내부 DNS 서버 구성](#)
- [Umbrella를 사용하여 HTTPS\(DoH\)를 통한 DNS 구성](#)
- [보안 액세스에서 도메인 컨트롤러 추가](#)
- [Cisco Secure Access Block 페이지 정보](#)
- [Cisco 기술 지원 및 다운로드](#)

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.