디바이스 모니터링

시스템에는 디바이스 및 디바이스를 통과하는 트래픽을 모니터링하는 데 사용할 수 있는 대시보드와 이벤트 뷰어가 포함되어 있습니다.

트래픽 통계를 가져오도록 로깅 활성화

모니터링 대시보드 및 이벤트 뷰어를 사용하여 광범위한 트래픽 통계를 모니터링할 수 있습니다. 그러나 시스템에 수집할 통계를 지시하려면 로깅을 활성화해야 합니다. 시스템을 통과하는 연결을 파악할 수 있게 해주는 다양한 유형의 이벤트가 로깅을 통해 생성됩니다.

다음 주제에서는 특히 연결 로깅에 중점을 두어 로깅을 통해 제공되는 이벤트와 정보에 대해 자세히 설명합니다.

이벤트 유형

시스템은 다음 이벤트 유형을 생성할 수 있습니다. 모니터링 대시보드에서 관련된 통계를 확인하려면 이러한 이벤트를 생성해야 합니다.

연결 이벤트

사용자가 시스템을 통과하는 트래픽을 생성할 때 연결에 대한 이벤트를 생성할 수 있습니다. 액세스 규칙에서 연결 로깅을 활성화하여 이러한 이벤트를 생성합니다. 보안 인텔리전스 정책과 SSL 암호 해독 규칙에서 로깅을 활성화하여 연결 이벤트를 생성할 수도 있습니다.

연결 이벤트에는 소스/대상 IP 주소와 포트, 사용한 URL 및 애플리케이션, 전송된 바이트 또는 패킷의 수 등 연결에 대한 여러 가지 정보가 포함됩니다. 수행한 작업(예: 연결 허용 또는 차단) 및 연결에 적용된 정책도 이러한 정보에 포함됩니다.

침입 이벤트

시스템은 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성에 영향을 미칠 수 있는 악성 활동 탐지를 위해 네트워크를 통과하는 패킷을 검토합니다. 시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트를 생성합니다. 침입 이벤트는 호출하는 액세스 제어 규칙의 로깅 컨피그레이션과 관계없이 차단하거나 알리도록 설정된 모든 침입 규칙에 대해 생성됩니다.

파일 이벤트

파일 이벤트는 파일 정책을 기준으로 하여 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 파일을 나타냅니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다.

시스템이 파일 이벤트를 생성하는 경우 호출하는 액세스 제어 규칙의 로깅 컨피그레이션과 관계없이 시스템은 관련 연결의 종료도 로깅합니다.

악성코드 이벤트

시스템은 전체적인 액세스 제어 컨피그레이션의 일부로 네트워크 트래픽에서 악성코드를 탐지할 수 있습니다. 악성코드 대응 는 결과 이벤트의 상태와 악성코드가 탐지된 방법, 위치, 시간에 대한 상황 데이터를 포함하는 악성코드 이벤트를 생성할 수 있습니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다.

파일 상태는 변경될 수 있습니다(예: 정상에서 악성코드로 또는 악성코드에서 정상으로). 악성코드 대응 가 Secure Malware Analytics Cloud에 파일에 대해 쿼리하고, 쿼리한지 일주일 이내에 상태가 변경되었음을 클라우드에서 확인하는 경우, 시스템에서는 회귀적 악성코드 이벤트를 생성합니다.

보안 인텔리전스 이벤트

보안 인텔리전스 이벤트는 정책에 따라 차단되거나 또는 모니터링된 각 연결의 보안 인텔리전스 정책에 의해 생성된 연결 이벤트 유형입니다. 모든 보안 인텔리전스 이벤트에는 내용이 채워진 Security Intelligence Category(보안 인텔리전스 카테고리) 필드가 있습니다.

이러한 각 이벤트에는 해당하는 "일반" 연결 이벤트가 있습니다. 보안 인텔리전스 정책은 액세스 제어를 비롯한 다른 많은 보안 정책보다 먼저 평가되기 때문에 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

구성 가능한 연결 로깅

조직의 보안 및 규정 준수 필요에 따라 연결을 로깅해야 합니다. 사용자가 생성하고 기능을 향상시키는 이벤트의 수를 제한하는 것이 사용자의 목표라면 사용자의 분석에 중요한 연결에 대한 로깅만 사용 설정합니다. 그러나, 자료 수집을 목적으로 사용자의 네트워크 트래픽에 대한 광범위한 견해를 원할 경우, 추가 연결에 대한 로깅을 사용 설정할 수 있습니다.

시스템은 여러 가지 이유로 연결을 로깅할 수 있으므로, 한 곳의 로깅을 비활성화해도 일치하는 연결이 로깅되지 않는 것은 아닙니다.

다음 위치에서 연결 로깅을 구성할 수 있습니다.

- 액세스 제어 규칙 및 기본 작업 — 연결 종료 시 수행되는 로깅은 연결에 대한 대부분의 정보를 제공합니다. 연결 시작 시에 로깅을 수행할 수도 있지만 이러한 이벤트에 포함되는 정보는 불완전합니다. 연결 로깅은 기본적으로 비활성화되므로 추적하려는 트래픽을 대상으로 하는 각 규칙과 기본 작업에 대해 연결 로깅을 활성화해야 합니다.
- 보안 인텔리전스 정책 — 각 차단된 연결에 대한 보안 인텔리전스 연결 이벤트를 생성하도록 로깅을 활성화할 수 있습니다. 보안 인텔리전스 필터링의 결과로 시스템이 연결 이벤트를 로깅할 때 시스템은 또한 일치하는 보안 인텔리전스 이벤트도 로깅합니다. 이는 사용자가 별도로 살펴보고 분석할 수 있는 특수한 연결 이벤트입니다.
- SSL 암호 해독 규칙 및 기본 작업 — 연결 종료 시 수행되는 로깅을 구성할 수 있습니다. 차단된 연결의 경우 시스템에서 즉시 세션을 종료하고 이벤트를 생성합니다. 모니터링된 연결 및 액세스 제어 규칙으로 전달하는 연결의 경우 시스템에서 세션 종료 시 이벤트를 생성합니다.

자동 연결 로깅

시스템은 다른 로깅 컨피그레이션과 관계없이 다음의 연결 종료 이벤트를 자동으로 저장합니다.

- 시스템은 연결이 액세스 제어 정책의 기본 작업에 의해 처리되지 않는 한, 침입 이벤트와 연관된 연결을 자동으로 로깅합니다. 일치하는 트래픽에 대한 침입 이벤트를 얻으려면 기본 작업에서 로깅을 활성화해야 합니다.
- 시스템은 파일 및 악성코드 이벤트와 연관된 연결을 자동으로 로깅합니다. 이는 연결 이벤트만을 위한 작업입니다. 선택적으로 파일 및 악성코드 이벤트의 생성을 비활성화할 수 있습니다.

연결 로깅에 대한 팁

로깅 컨피그레이션 및 관련 통계 평가를 고려할 때는 다음 사항에 유의하십시오.

- 사용자가 액세스 제어 규칙을 통해 트래픽을 허용할 때, 연결된 침입 또는 파일 정책을 (또는 둘 다를) 사용하여 트래픽이 최종 목적지에 도달하기 전에 트래픽 및 침입 차단, 금지된 파일과 악성코드를 자세히 검사할 수 있습니다. 하지만. 기본 파일 및 침입에 의해 암호화된 페이로드를 위한 탐지가 사용 해제되었음을 참고하시기 바랍니다. 침입 또는 파일 정책이 연결을 차단해야 하는 이유를 확인하는 경우, 시스템은 연결 로그 설정과 관계없이 연결 종료 이벤트를 즉시 로깅합니다. 로깅이 허용되는 연결은 네트워크의 트래픽에 대해 가장 많은 통계 정보를 제공합니다.
- 신뢰할 수 있는 연결이란 액세스 제어 정책에서 신뢰 액세스 제어 규칙 또는 기본 작업이 처리한 것입니다. 그러나 신뢰할 수 있는 연결에서는 검색 데이터, 침입 또는 금지된 파일과 악성코드를 검사하지 않습니다. 따라서, 신뢰할 수 있는 연결에 대한 연결 이벤트는 제한된 정보를 포함합니다.
- 트래픽을 차단하는 액세스 제어 규칙 및 액세스 제어 정책 기본 작업의 경우 시스템은 연결 시작 이벤트를 로깅합니다. 일치하는 트래픽은 추가 검사 없이 거부됩니다.
- DoS(서비스 거부) 공격 중에 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며, 데이터베이스가 유사한 다수의 이벤트로 가득 찰 수 있습니다. 차단 규칙에 대한 로깅을

활성화하기 전에 이 규칙이 인터넷 연결 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하는지 여부를 고려하십시오.

- 원격 액세스 VPN 연결 프로파일을 컨피그레이션하거나 **sysopt connection permit-vpn** 명령을 활성화할 때 **Bypass Access Control policy for decrypted traffic(**암호 해독 트래픽에 대한 액세스 제어 우회 정책**)(sysopt permit-vpn)** 옵션을 선택하면 모든 Site-to-Site 또는 원격 액세스 VPN 트래픽이 검사 및 액세스 제어 정책을 우회합니다. 따라서 이 트래픽에 대한 연결 이벤트를 가져오지 못하고, 트래픽은 어떤 통계 대시보드에도 반영되지 않습니다.

외부 **syslog** 서버에 이벤트 전송

device manager(이벤트를 저장하는 기능은 제한되어 있음)를 통해 이벤트를 확인하는 것 외에도 규칙과 정책을 선택적으로 구성하여 이벤트를 외부 시스템 로그 서버에 전송할 수 있습니다. 그러면 선택한 syslog 서버 플랫폼의 추가 스토리지 및 기능을 사용하여 이벤트 데이터를 확인하고 분석할 수 있습니다.

외부 syslog 서버에 이벤트를 전송하려면 각 연결 로깅을 활성화하는 규칙, 기본 작업 또는 정책을 편집하고 로그 설정에서 syslog 서버 개체를 선택합니다. syslog 서버에 침입 이벤트를 전송하려면 침입 정책 설정에서 서버를 컨피그레이션하십시오. syslog 서버에 파일/악성코드 이벤트를 전송하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)**에서 서버를 컨피그레이션하십시오.

자세한 내용은 각 규칙 및 정책 유형에 대한 도움말과 syslog 서버 구성의 내용을 참조하십시오.

Cisco Cloud 기반 서비스를 사용하여 이벤트 평가

Event Viewer 및 자체 syslog 서버를 사용하는 것 외에도 연결 이벤트 및 높은 우선순위 침입, 파일 및 악성코드 이벤트를 Cisco Cloud 기반 서버에 전송할 수 있습니다. Threat Response와 같은 Cisco Cloud 기반 서비스는 해당 클라우드 서버에서 이벤트를 끌어올 수 있으며, 해당 서비스를 사용하여 이러한 이벤트를 평가할 수 있습니다.

이러한 클라우드 기반 서비스는 위협 방어 디바이스 및 device manager과 별개입니다. 이러한 이벤트를 Cisco Cloud로 전송하도록 요구하는 서비스를 사용하도록 선택하는 경우, **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 페이지에서 연결을 활성화해야 합니다. Cisco Cloud로 이벤트 전송의 내용을 참조하십시오.

트래픽 및 시스템 대시보드 모니터링

시스템에는 디바이스를 통과하는 트래픽과 보안 정책의 결과를 분석하는 데 사용할 수 있는 여러 대시보드가 포함되어 있습니다. 대시보드의 정보를 사용하여 컨피그레이션의 전반적인 효율성을 평가하고 네트워크 문제를 식별 및 해결합니다.

고가용성 그룹의 유닛용 대시보드에는 해당 디바이스에 대한 통계만 표시됩니다. 통계는 유닛 간에 동기화되지 않습니다.

참고 트래픽 관련 대시보드에서 사용되는 데이터는 연결 또는 파일 로깅을 활성화하는 액세스 제어 규칙 및 로깅을 허용하는 기타 보안 정책에서 수집됩니다. 로깅이 활성화되어 있지 않은 규칙과 일치하는 트래픽은 대시보드에 반영되지 않습니다. 따라서 중요한 정보를 로깅하도록 규칙을 구성해야 합니다. 또한, 사용자 정보는 사용자 ID를 수집하는 ID 규칙을 구성한 경우에만 사용할 수 있습니다. 그리고 마지막으로 침입, 파일, 악성코드 및 URL 카테고리 정보는 해당 기능용 라이선스가 있고 이러한 기능을 사용하는 규칙을 구성하는 경우에만 사용할 수 있습니다.

프로시저

단계 **1** 주 메뉴에서 **Monitoring(**모니터링**)**을 클릭하여 대시보드 페이지를 엽니다.

지난 1시간, 지난 주 등의 사전 정의된 시간 범위를 선택하거나, 특정 시작 시간과 종료 시간을 사용해 맞춤형 시간 범위를 정의하여 대시보드 그래프와 테이블에 표시되는 데이터를 제어할 수 있습니다.

트래픽 관련 대시보드는 다음과 같은 유형으로 표시됩니다.

- 상위 5개 막대 그래프 - 이러한 그래프는 네트워크 개요 대시보드에 표시되며 대시보드 테이블에서 항목을 클릭하면 나타나는 항목별 요약에도 표시됩니다. 표시되는 정보를 트랜잭션 개수 또는 데이터 사용량(전송 및 수신된 총 바이트 수) 간을 전환할 수 있습니다. 모든 트랜잭션, 허용된 트랜잭션 또는 거부된 트랜잭션이 나타나도록 화면표시를 전환할 수도 있습니다. 더 보기 링크를 클릭하면 그래프와 연결된 테이블이 표시됩니다.
- 테이블 - 테이블에는 특정 유형(예: 애플리케이션 또는 URL 카테고리)의 항목과 해당 항목의 총 트랜잭션, 허용된 트랜잭션, 차단된 트랜잭션, 데이터 사용량, 전송/수신된 바이트 수가 표시됩니다. 표시되는 숫자를 원시 값과 백분율 간을 전환할 수 있으며 상위 10개, 100개, 1000개 항목을 표시할 수 있습니다. 항목이 링크인 경우 링크를 클릭하면 더욱 자세한 정보가 포함된 요약 대시보드를 확인할 수 있습니다.

단계 **2** 목차에서 대시보드 링크를 클릭하여 다음 데이터에 대한 대시보드를 표시합니다.

- **Network Overview(**네트워크 개요**)** - 네트워크의 트래픽에 대한 요약 정보가 표시됩니다. 이러한 정보에는 일치한 액세스 규칙(정책), 트래픽을 생성한 사용자, 연결에 사용된 애플리케이션, 일치한 침입 위협(서명), 액세스한 URL의 URL 카테고리, 연결에서 가장 많이 사용된 대상이 포함됩니다.
- **Users(**사용자**)** - 네트워크를 많이 사용한 사용자가 표시됩니다. 사용자 정보를 확인하려면 ID 정책을 구성해야 합니다. 사용자 ID가 없는 경우, 소스 IP 주소가 포함되어 있습니다. 다음과 같은 특수 엔티티가 표시될 수 있습니다.
  - **Failed Authentication(**실패한 인증**)** - 사용자에게 인증하라는 메시지가 표시되었는데 사용자가 허용되는 최대 횟수 이내에 유효한 사용자 이름/비밀번호 쌍을 입력하지 못했습니다. 인증에 실패해도 사용자의 네트워크 액세스가 차단되지는 않지만, 이러한 사용자의 네트워크 액세스를 제한하는 액세스 규칙을 작성할 수 있습니다.

  - **Guest(**게스트**)** - 게스트 사용자는 ID 규칙이 이러한 사용자를 게스트로 지칭하도록 구성된다는 점을 제외하면 실패한 인증 사용자와 비슷합니다. 즉, 게스트 사용자 역시 인증하라는 메시지가 표시되었지만, 최대 시도 횟수 이내에 인증하지 못한 사용자입니다.
  - **No Authentication Required(**인증 필요 없음**)** - 사용자의 연결이 인증을 지정하지 않은 ID 규칙과 일치하여 인증하라는 메시지가 표시되지 않았습니다.
  - **Unknown(**알 수 없음**)** - IP 주소에 대한 사용자 매핑이 없으며 아직 실패한 인증 기록이 없습니다. 이는 일반적으로 해당 주소에서 HTTP 트래픽이 아직 전송되지 않았음을 의미합니다.

- **Applications(**애플리케이션**)** - 네트워크에서 가장 많이 사용되는 애플리케이션(예: HTTP)이 표시됩니다. 검사된 연결에 대해서만 정보가 제공됩니다. 영역, 주소 및 포트 이외의 기준을 사용하는 차단 규칙이나 "허용" 규칙과 일치하는 연결을 검사합니다. 따라서 검사를 요구하는 규칙에 적중하기 전에 연결이 신뢰 또는 차단되면 애플리케이션 정보가 제공되지 않습니다.
- **Web Applications(**웹 애플리케이션**)** - 네트워크에서 가장 많이 사용되는 애플리케이션(예: Google)이 표시됩니다. 웹 애플리케이션 정보 수집에 필요한 조건은 Application(애플리케이션) 대시보드의 조건과 동일합니다.
- **URL Categories(URL** 카테고리**)** - 방문한 웹 사이트의 분류를 기반으로 네트워크에서 많이 사용되는 웹 사이트 카테고리(예: Gambling(도박) 또는 Educational Institutions(교육 기관))가 표시됩니다. 이 정보를 얻으려면 트래픽 일치 기준으로 URL 카테고리를 사용하는 액세스 제어 규칙이 하나 이상 있어야 합니다. 규칙과 일치하는 트래픽 또는 규칙과 일치하는지를 확인하기 위해 검사해야 하는 트래픽에 대한 정보가 제공됩니다. 첫 번째 웹 범주 액세스 제어 규칙 앞에 오는 규칙과 일치하는 연결에 대해서는 범주 또는 평판 정보가 표시되지 않습니다.
- **Access and SI Rules(**액세스 및 **SI** 규칙**)** - 네트워크 트래픽과 가장 많이 일치하는 액세스 규칙 및 보안 인텔리전스 규칙에 상응하는 규칙이 표시됩니다.
- **Zones(**영역**)** - 트래픽이 디바이스로 들어왔다가 나가는 데 가장 많이 사용되는 보안 영역 쌍이 표시됩니다.
- **Destinations(**목적지**)** - 네트워크 트래픽에서 가장 많이 사용하는 목적지를 표시합니다.
- **Attackers(**공격자**)** - 침입 이벤트를 트리거하는 연결의 소스인 상위 공격자를 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 침입 정책을 구성해야 합니다.
- **Targets(**대상**)** - 공격의 피해자인 침입 이벤트의 상위 대상을 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 침입 정책을 구성해야 합니다.
- **Threats(**위협**)** - 가장 많이 트리거된 침입 규칙을 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 침입 정책을 구성해야 합니다.
- **File Logs(**파일 로그**)** - 네트워크 트래픽에서 가장 많이 확인된 파일 유형을 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 파일 정책을 구성해야 합니다.
- **Malware(**악성코드**)** - 가장 많이 사용되는 악성코드 작업 및 상태의 조합이 표시됩니다. 드릴다운하여 연결된 파일 유형에 대한 정보를 확인할 수 있습니다. 이 정보를 보려면 액세스 규칙에 대한 파일 정책을 구성해야 합니다.

- 가능한 작업: 악성코드 클라우드 조회, 차단, 아카이브 차단(암호화), 탐지, 맞춤형 탐지, 클라우드 조회 시간 제한, 악성코드 차단, 아카이브 차단(깊이 초과), 맞춤형 탐지 차단, TID 차단, 아카이브 차단(검사 실패)
- 가능한 상태: 악성코드, 알 수 없음, 정상, 맞춤형 탐지, 사용할 수 없음

- **SSL Decryption(SSL** 암호 해독**)** - 디바이스를 통과하는 암호화된 트래픽과 일반 텍스트 트래픽의 비교 내용이 표시됩니다. 또한, 암호화된 트래픽이 SSL 암호 해독 규칙에 따라 암호 해독된 방식에 대한 분석 내용도 표시됩니다.
- **System(**시스템**)** - 인터페이스 및 해당 상태(인터페이스 위에 마우스를 올려놓으면 해당 IP 주소가 표시됨), 전반적인 평균 시스템 처리량(최대 1시간 동안 5분의 버킷 기준 및 더 긴 기간 동안 1시간의 버킷 기준), 시스템 이벤트/CPU 사용량/메모리 사용량/디스크 사용량에 관한 요약 정보를 비롯한 전체 시스템 보기가 표시됩니다. 모든 인터페이스가 아닌 특정 인터페이스만 표시하도록 성능 그래프를 제한할 수 있습니다.

  참고 시스템 대시보드에 표시되는 정보는 전체 시스템 레벨의 정보입니다. 디바이스 CLI에 로그인하면 다양한 명령을 사용하여 더욱 자세한 정보를 확인할 수 있습니다. 예를 들어 **show cpu** 및 **show memory** 명령에는 기타 세부 정보를 표시하기 위한 파라미터가 포함된 반면, 이 대시보드에서는 **show cpu system** 및 **show memory system** 명령에서 제공하는 데이터를 표시합니다.

단계 **3** 목차에서 이러한 링크를 클릭할 수도 있습니다.

- **Events(**이벤트**)** - 발생하는 이벤트를 확인할 수 있습니다. 개별 액세스 규칙에서 연결 로깅을 활성화해야 해당 규칙과 관련된 연결 이벤트를 확인할 수 있습니다. 또한, 보안 인텔리전스 정책 및 SSL 암호 해독 규칙에서 로깅을 활성화하여 보안 인텔리전스 이벤트와 추가 연결 이벤트 데이터를 확인합니다. 이러한 이벤트를 확인하면 사용자의 연결 문제를 쉽게 해결할 수 있습니다.
- **Sessions(**세션**)** - device manager 사용자 세션을 보고 관리할 수 있습니다. 자세한 내용은 Device Manager 사용자 세션 관리를 참고하십시오.

커맨드 라인을 사용하여 추가 통계 모니터링

device manager 대시보드에서는 디바이스를 통과하는 트래픽 및 일반 시스템 사용량과 관련된 다양한 통계를 제공합니다. 그러나 CLI 콘솔을 사용하거나 디바이스 CLI에 로그인하면 대시보드에서 통계를 제공하지 않는 영역에 대한 추가 정보를 확인할 수 있습니다(CLI(Command Line Interface) 로그인 참조).

CLI에는 이러한 통계를 제공하는 다양한 **show** 명령이 포함되어 있습니다. **ping**, **traceroute** 같은 명령을 포함해 일반적인 문제해결을 위한 CLI를 사용할 수도 있습니다. 대부분의 **show** 명령에는 통계를 0으로 재설정하기 위해 함께 사용할 수 있는 **clear** 명령이 있습니다. CLI 콘솔에서는 통계를 지울 수 없습니다.

명령에 대한 문서는 Cisco Firepower Threat Defense 명령 참조, http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html에서 찾을 수 있습니다.

일반적으로 유용하게 활용할 수 있는 명령의 예는 다음과 같습니다.

- **show nat** NAT 규칙의 적중 횟수를 표시합니다.
- **show xlate** 활성 상태인 활성 NAT 변환을 표시합니다.
- **show conn** 디바이스를 통과하는 현재 연결에 대한 정보를 제공합니다.
- **show dhcpd** 인터페이스에 대해 구성하는 DHCP 서버에 대한 정보를 제공합니다.
- **show interface** 각 인터페이스의 사용량 통계를 제공합니다.

이벤트 보기

로깅을 활성화하는 보안 정책에서 생성된 이벤트를 확인할 수 있습니다. 트리거된 침입 및 파일 정책에 대해서도 이벤트가 생성됩니다.

이벤트 뷰어 테이블에는 생성되는 이벤트가 실시간으로 표시됩니다. 새 이벤트가 생성되면 이전 이벤트는 테이블에 표시되지 않게 됩니다.

시작하기 전에

특정 유형의 이벤트가 생성되는지 여부는 관련 정책과 일치하는 연결 외에 다음 사항에 따라서도 달라집니다.

- 연결 이벤트 - 액세스 규칙이 연결 로깅을 활성화해야 합니다. 보안 인텔리전스 정책과 SSL 암호 해독 규칙에서 연결 로깅을 활성화할 수도 있습니다.
- 침입 이벤트 - 액세스 규칙이 침입 정책을 적용해야 합니다.
- 파일 및 악성코드 이벤트 - 액세스 규칙이 파일 정책을 적용하고 파일 로깅을 활성화해야 합니다.
- 보안 인텔리전스 이벤트 - 보안 인텔리전스 정책을 활성화 및 구성하고 로깅을 활성화해야 합니다.

프로시저

단계 **1** 주 메뉴에서 **Monitoring(**모니터링**)**을 클릭합니다.

단계 **2** 목차에서 **Events(**이벤트**)**를 선택합니다.

이벤트 뷰어에서는 탭의 이벤트가 이벤트 유형을 기준으로 구성됩니다. 자세한 내용은 이벤트 유형, 1 페이지를 참고하십시오.

단계 **3** 보려는 이벤트의 유형이 표시된 탭을 클릭합니다.

이벤트 목록을 사용하여 다음 작업을 수행할 수 있습니다.

- 이벤트를 보다 쉽게 찾고 분석할 수 있도록 새 이벤트 추가를 중지하려면 **Pause(**일시정지**)**를 클릭합니다. 새 이벤트가 표시되도록 하려면 **Resume(**재시작**)**를 클릭합니다.
- 새 이벤트가 표시되는 속도를 제어하려면 여러 새로고침 속도(5초, 10초, 20초, 60초) 중에서 선택합니다.
- 원하는 열이 포함된 맞춤형 보기를 생성합니다. 맞춤형 보기를 생성하려면 탭 막대에서 **+** 버튼을 클릭하거나 **Add/Remove Columns(**열 추가/제거**)**를 클릭합니다. 사전 설정된 탭은 변경할 수 없으므로 열을 추가하거나 제거하면 새 보기가 생성됩니다. 자세한 내용은 맞춤형 보기 구성, 9 페이지를 참고하십시오.
- 열의 폭을 변경하려면 열 제목 구분선을 클릭하여 원하는 폭으로 끌어옵니다.
- 이벤트 위에 마우스를 올려 놓고 **View Details(**세부정보 보기**)**를 클릭하면 이벤트에 대한 전체 정보를 확인할 수 있습니다. 이벤트 내의 여러 필드에 대한 설명은 이벤트 필드 설명, 11 페이지를 참조하십시오.

단계 **4** 필요한 경우 다양한 이벤트 속성에 따라 원하는 이벤트를 쉽게 찾을 수 있도록 테이블에 필터를 적용합니다.

새 필터를 생성하려면 드롭다운 목록에서 원자성 요소를 선택하고 필터 값을 입력하여 필터를 수동으로 입력하거나, 필터링할 값이 포함된 이벤트 테이블에서 셀 하나를 클릭하여 필터를 작성합니다. 같은 열의 여러 셀을 클릭하여 값 간의 OR 조건을 생성할 수도 있고, 서로 다른 열의 셀을 클릭하여 열 간의 AND 조건을 생성할 수도 있습니다. 셀을 클릭하여 필터를 작성하는 경우에는 결과로 생성되는 필터를 수정하여 미세 조정할 수 있습니다. 필터 규칙 생성에 대한 자세한 내용은 이벤트 필터링, 10 페이지를 참조하십시오.

필터를 작성한 후에는 다음 중에서 원하는 작업을 수행합니다.

- 필터를 적용하고 필터와 일치하는 이벤트만 표시되도록 테이블을 업데이트하려면 **Filter(**필터**)** 버튼을 클릭합니다.
- 적용한 전체 필터를 지우고 테이블을 필터링되지 않은 상태로 되돌리려면 **Filter(**필터**)** 상자에서 **Reset Filters(**필터 재설정**)**를 클릭합니다.
- 필터의 원자성 요소 중 하나를 지우려면 해당 요소 위에 마우스를 올려 놓고 요소에 대해 표시되는 **X**를 클릭합니다. 그런 다음 **Filter(**필터**)** 버튼을 클릭합니다.

맞춤형 보기 구성

이벤트를 확인할 때 원하는 열을 쉽게 볼 수 있도록 맞춤형 보기를 생성할 수 있습니다. 맞춤형 보기는 수정하거나 삭제할 수도 있습니다. 사전 정의된 보기는 수정하거나 삭제할 수 없습니다.

프로시저

단계 **1** **Monitoring(**모니터링**)** > **Events(**이벤트**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 기존 맞춤형 보기 또는 사전 정의된 보기를 기준으로 새 보기를 생성하려면 보기의 탭을 클릭하고 탭 왼쪽에 있는 + 버튼을 클릭합니다.
- 기존 맞춤형 보기를 수정하려면, 보기의 탭을 클릭합니다.

참고 맞춤형 보기를 삭제하려는 경우에는 보기 탭에서 **X** 버튼만 클릭하면 됩니다. 삭제는 취소할 수 없습니다.

단계 **3** 오른쪽의 이벤트 테이블 위에 있는 열 추가/제거 링크를 클릭한 다음, 보기에 포함하려는 열만 선택한 목록에 포함될 때까지 열을 선택하거나 선택을 취소합니다.

열을 클릭한 다음 끌어서 사용할 수 있지만 사용하지 않은 목록과 선택한 목록 간을 이동합니다. 선택한 목록에서 열을 클릭하고 끌어서 테이블 내의 열 순서(왼쪽에서 오른쪽)를 변경할 수도 있습니다. 열에 대한 설명은 이벤트 필드 설명, 11 페이지를 참조하십시오.

작업을 완료한 후 **OK(**확인**)**를 클릭하여 열 변경 사항을 저장합니다.

참고 사전 정의된 보기가 표시된 상태에서 열 선택을 변경하면 새 보기가 생성됩니다.

단계 **4** 필요한 경우 열 구분 기호를 클릭하고 끌어서 열 너비를 변경합니다.

이벤트 필터링

이벤트 테이블에 현재 확인하고자 하는 이벤트만 표시되도록 제한하는 복잡한 필터를 생성할 수 있습니다. 다음과 같은 기술을 단독으로 사용하거나 조합하여 필터를 작성할 수 있습니다.

열 클릭

필터를 작성하는 가장 쉬운 방법은 필터링할 값이 포함된 이벤트 테이블의 셀을 클릭하는 것입니다. 셀을 클릭하면 해당 값 및 필드 조합에 대해 올바르게 작성된 규칙을 사용하여 필터 필드가 업데이트됩니다. 그러나 이 기술을 사용하려면 기존 이벤트 목록에 원하는 값이 포함되어 있어야 합니다.

모든 열을 필터링할 수는 없습니다. 셀의 콘텐츠를 필터링할 수 있는 경우 해당 셀 위에 마우스를 올려놓으면 셀에 밑줄이 표시됩니다.

원자성 요소 선택

필터 필드를 클릭하고 드롭다운 목록에서 원하는 원자성 요소를 선택한 다음 일치 값을 입력하여 필터를 작성할 수도 있습니다. 이러한 요소는 이벤트 테이블에 열로 표시되지 않는 이벤트 필드를 포함합니다. 또한 입력하는 값과 표시할 이벤트 간의 관계를 정의하는 연산자도 포함합니다. 열을 클릭할 때는 항상 "같음(=)" 필터가 적용되는 반면 요소를 선택할 때는 숫자 필드에 대해 "보다 큼(>)" 또는 "보다 작음(<)"도 선택할 수 있습니다.

Filter(필터**)** 필드에 요소를 추가하는 방법과 관계없이 필드에 값을 입력하여 연산자나 값을 조정할 수 있습니다. 테이블에 필터를 적용하려면 필터를 클릭합니다.

이벤트 필터용 연산자

이벤트 필터에서는 다음 연산자를 사용할 수 있습니다.

=	같음. 이벤트가 지정된 값과 일치합니다. 와일드카드는 사용할 수 없습니다.
!=	같지 않음. 이벤트가 지정된 값과 일치하지 않습니다. 같지 않음 식을 작성하려면 !(느낌표)를 입력해야 합니다.
>	보다 큼. 이벤트에 지정된 값보다 큰 값이 포함되어 있습니다. 이 연산자는 포트 및 IP 주소와 같은 숫자 값에만 사용할 수 있습니다.
<	보다 작음. 이벤트에 지정된 값보다 작은 값이 포함되어 있습니다. 이 연산자는 숫자 값에만 사용할 수 있습니다.

복잡한 이벤트 필터에 대한 규칙

여러 원자성 요소가 포함된 복잡한 필터를 작성할 때는 다음 규칙에 주의하십시오.

- 유형이 같은 요소의 경우 해당 유형의 모든 값 간에 OR 관계가 설정됩니다. 예를 들어 이니시에이터 IP=10.100.10.10 및 이니시에이터 IP=10.100.10.11을 포함하는 경우 트래픽 소스로 이러한 주소 중 하나를 포함하는 이벤트가 일치 항목으로 표시됩니다.
- 유형이 다른 요소의 경우 AND 관계가 설정됩니다. 예를 들어 이니시에이터 IP=10.100.10.10 및 대상 포트/ICMP 유형=80을 포함하는 경우 이 소스 주소와 대상 포트를 모두 포함하는 이벤트만 일치 항목으로 표시됩니다. 10.100.10.10에서 다른 대상 포트로 향하는 이벤트는 표시되지 않습니다.
- IPv4 및 IPv6 주소를 포함한 숫자 요소의 경우 범위를 지정할 수 있습니다. 예를 들어 대상 포트 =50-80을 지정하여 해당 범위 내의 포트에 대한 모든 트래픽을 캡처할 수 있습니다. 하이픈을 사용하여 시작 숫자와 종료 숫자를 분리합니다. 모든 숫자 필드에 범위를 사용할 수 있는 것은 아닙니다. 예를 들어 소스 요소에서는 IP 주소 범위를 지정할 수 없습니다.
- 와일드카드나 정규식은 사용할 수 없습니다.

이벤트 필드 설명

이벤트는 다음 정보를 포함할 수 있습니다. 이벤트 세부사항을 볼 때 이 정보를 확인할 수 있습니다. 이벤트 뷰어 테이블에 열을 추가하여 가장 관심이 높은 정보를 표시할 수도 있습니다.

아래에는 사용 가능한 필드의 전체 목록이 나와 있습니다. 모든 이벤트 유형에 모든 필드가 적용되는 것은 아닙니다. 개별 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다.

작업

연결 또는 보안 인텔리전스 이벤트의 경우 연결이 기록된 기본 작업 또는 액세스 제어 규칙과 관련된 작업은 다음과 같습니다.

허용

명시적으로 허용된 연결

신임

신뢰할 수 있는 연결. 첫 번째 패킷의 신뢰 규칙에 의해 탐지된 TCP 연결은 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.

차단

차단된 연결. 다음 상황에서 차단 작업을 허용 액세스 규칙과 연결할 수 있습니다.

- 침입 정책에 따라 익스플로잇이 차단된 연결
- 파일 정책에 따라 파일이 차단된 연결
- 보안 인텔리전스에 의해 차단된 연결.
- SSL 정책에 따라 차단된 연결

기본 작업

연결이 기본 작업에 의해 처리되었습니다.

파일 또는 악성코드 이벤트의 경우, 파일과 일치하는 규칙에 대한 규칙 작업과 관련된 파일 규칙 작업 및 관련된 모든 파일 규칙 작업 옵션

허용된 연결

시스템이 이벤트에 대한 트래픽 흐름을 허용하는지 여부

애플리케이션

연결에서 탐지된 애플리케이션

애플리케이션 비즈니스 관련성

연결에서 탐지된 애플리케이션 트래픽과 연계된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

애플리케이션 범주**,** 애플리케이션 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

애플리케이션 위험성

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

차단 유형

이벤트의 트래픽 흐름과 일치하는 액세스 제어 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

클라이언트 애플리케이션**,** 클라이언트 버전

연결에서 탐지된 클라이언트 애플리케이션 및 클라이언트 버전

클라이언트 비즈니스 관련성

연결에서 탐지된 클라이언트 트래픽과 관련된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 클라이언트 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

클라이언트 범주**,** 클라이언트 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

클라이언트 위험성

연결에서 탐지된 클라이언트 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 클라이언트의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

연결

내부에서 생성되는 트래픽 흐름의 고유 ID

연결 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 액세스 제어 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

연결 바이트

연결에 대한 총 바이트

연결 시간

연결 시작 시간

연결 타임 스탬프

연결이 탐지된 시간

거부된 연결

시스템이 이벤트에 대한 트래픽 흐름을 거부하는지 여부

대상 국가 및 대륙

수신 호스트의 국가와 대륙

목적지 **IP**

침입, 파일 또는 악성코드 이벤트에서 수신 호스트가 사용하는 IP 주소

대상 포트/**ICMP** 코드**,** 대상 포트**,** 대상 **Icode**

세션 responder가 사용하는 포트 또는 ICMP 코드

대상 **SGT(Security Group Tag),** 대상 **SGT(Security Group Tag)** 이름

대상과 연결된 TrustSec SGT(Security Group Tag) 번호 및 이름(있는 경우)

방향

파일의 전송 방향

속성

파일의 속성

악성코드

Secure Malware Analytics Cloud가 파일을 악성코드로 분류했거나, 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다. 로컬 악성코드 분석을 통해 파일을 악성코드로 표시할 수도 있습니다.

정상

Secure Malware Analytics Cloud가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다.

알 수 없음

시스템이 Secure Malware Analytics Cloud를 쿼리했으나 파일에 상태가 할당되지 않았음을 나타냅니다. 즉, Secure Malware Analytics Cloud에서 파일을 분류하지 않았습니다.

맞춤형 탐지

사용자가 파일을 커스텀 탐지 목록에 추가했음을 나타냅니다.

사용 불가능

시스템이 Secure Malware Analytics Cloud를 쿼리하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.

해당 없음

파일 탐지 또는 파일 차단 규칙이 파일을 처리했으며 시스템이 Secure Malware Analytics Cloud를 쿼리하지 않았음을 나타냅니다.

이그레스 인터페이스**,** 이그레스 보안 영역

연결이 디바이스에서 외부로 나간 인터페이스 및 영역

이그레스 가상 라우터

대상 인터페이스가 속한 가상 라우터의 이름(있는 경우)

이벤트**,** 이벤트 유형

이벤트 유형.

이벤트 초**,** 이벤트 마이크로초

이벤트가 탐지된 시간(단위: 초 또는 마이크로초)

파일 카테고리

파일 유형의 일반적인 범주(예: Office 문서, 아카이브, 멀티미디어, 실행 파일, PDF 파일, 인코딩, 그래픽 또는 시스템 파일 등)

파일 이벤트 타임 스탬프

파일 또는 악성코드 파일이 생성된 시간 및 날짜

파일 이름

파일의 이름

파일 규칙 작업

파일을 탐지한 파일 정책 규칙과 연결된 작업 및 관련된 모든 파일 규칙 작업 옵션

파일 **SHA-256**

파일의 SHA-256 해시 값

파일 크기**(KB)**

킬로바이트 단위의 파일 크기. 파일이 완전히 수신되기 전에 시스템에서 파일을 차단한 경우에는 파일 크기를 비워 둘 수 있습니다.

파일 유형

HTML 또는 MSEXE 등의 파일 형식

파일/악성코드 정책

이벤트 생성과 관련된 파일 정책

파일 로그 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 파일 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

방화벽 정책 규칙**,** 방화벽 규칙

연결을 처리한 액세스 제어 규칙 또는 기본 작업

첫 번째 패킷

세션의 첫 번째 패킷이 표시된 날짜 및 시간

HTTP 참조 페이지

연결(다른 URL에 링크를 제공하는 웹사이트 또는 다른 URL에서 링크를 가져온 웹사이트 등)에서 탐지된 HTTP 트래픽에 대해 요청된 URL의 참조 페이지를 나타내는 HTTP 참조 페이지

HTTP 응답

연결을 통해 클라이언트의 HTTP 요청에 대한 응답으로 전송된 HTTP 상태 코드

IDS 분류

이벤트를 생성한 규칙이 속하는 분류

인그레스 인터페이스**,** 인그레스 보안 영역

연결이 디바이스로 들어온 인터페이스 및 영역

인그레스 가상 라우터

소스 인터페이스가 속한 가상 라우터의 이름(있는 경우)

이니시에이터 바이트**,** 이니시에이터 패킷

세션 이니시에이터가 전송한 총 바이트 또는 패킷 수

초기자 국가 및 대륙

세션을 시작한 호스트의 국가 및 대륙. 이니시에이터 IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

초기자 **IP**

연결 또는 보안 인텔리전스 이벤트에서 세션을 시작한 호스트 IP 주소(및 호스트 이름 - DNS 확인을 활성화한 경우)

인라인 결과

인라인 모드에서 작동하는 경우 침입 이벤트를 트리거한 패킷을 시스템에서 삭제했거나 삭제할 수 있었는지 여부. 비워 두는 경우 트리거된 규칙이 삭제 및 이벤트 생성으로 설정되지 않았음을 나타냅니다.

침입 정책

이벤트를 생성한 규칙이 활성화된 침입 정책

IPS 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 침입 규칙의 작업

마지막 패킷

세션의 마지막 패킷이 표시된 날짜 및 시간

MPLS 레이블

이 침입 이벤트를 트리거한 패킷에 연결된 Multiprotocol Label Switching(다중 프로토콜 레이블 스위칭) 레이블

악성코드 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 파일 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

메시지

침입 이벤트의 경우 이벤트를 설명하는 텍스트. 악성코드 또는 파일 이벤트의 경우 악성코드 이벤트와 관련된 모든 추가 정보.

NAT 대상 **IP**

NAT(Network Address Translation) 대상 패킷의 경우 변환된 대상 IP 주소입니다.

NAT 대상 포트

NAT(Network Address Translation) 대상 패킷의 경우 변환된 대상 포트입니다.

NAT 소스 **IP**

NAT(Network Address Translation) 대상 패킷의 경우 변환된 소스 IP 주소입니다.

NAT 소스 포트

NAT(Network Address Translation) 대상 패킷의 경우 변환된 소스 포트입니다.

NetBIOS 도메인

세션에서 사용되는 NetBIOS 도메인

원본 클라이언트 국가 및 대륙

세션을 시작한 원본 클라이언트 호스트의 국가와 대륙. 원본 클라이언트 IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

원본 클라이언트 **IP**

HTTP 연결을 시작한 클라이언트의 원본 IP 주소. 이 주소는 XFF(X-Forwarded-For) 또는 True-Client-IP HTTP 헤더 필드나 그와 동일한 필드에서 파생됩니다.

정책**,** 정책 수정

이벤트와 연결된 액세스(방화벽) 규칙을 포함하는 액세스 제어 정책 및 해당 수정

우선순위

Cisco Talos Intelligence Group(Talos)에서 결정하는 이벤트 우선순위(높음, 보통, 낮음)

프로토콜

연결에 사용된 전송 프로토콜

이유

다음 표에 설명된 상황에서 연결이 로깅된 이유. 해당하지 않는 경우 이 필드는 비어 있습니다.

이유	설명
DNS 차단	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. DNS 차단 이유는 DNS 규칙 작업에 따라 차단, 도메인을 찾을 수 없음 또는 싱크홀과 페어링됩니다.
DNS 모니터링	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.

이유	설명
엘리펀트 플로우	연결은 전체 시스템 성능에 영향을 미칠 만큼 충분히 큰 플로우인 엘리펀트 플로우으로 간주되기에 충분합니다. 기본적으로 엘리펀트 플로우는 1GB/10초보다 큰 상태입니다. **system support elephant-flow-detection** 명령을 사용하여 디바이스 CLI에서 엘리펀트 플로우 식별을 위한 바이트 및 시간 임계값을 조정할 수 있습니다.
파일 차단	시스템이 전송을 차단한 파일 또는 악성코드 파일이 연결에 포함되었습니다. 파일 차단 이유는 항상 차단 작업과 페어링됩니다.
파일 맞춤형 탐지	시스템이 전송을 차단한 맞춤형 탐지 목록의 파일이 연결에 포함되었습니다.
파일 모니터링	시스템이 연결에서 특정 파일 유형을 탐지했습니다.
파일 재시작 허용	파일 전송이 파일 차단 또는 악성코드 차단 파일 규칙에 의해 원래 차단되었다가, 해당 파일을 허용하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 재시작되었습니다.
파일 재시작 차단	파일 전송이 파일 탐지 또는 악성코드 클라우드 조회 파일 규칙에 의해 원래 허용되었다가, 해당 파일을 차단하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 중지되었습니다.
침입 차단	시스템이 연결에서 탐지된 익스플로잇(침입 정책 위반)을 차단했거나 차단할 수도 있었음을 나타냅니다. 침입 차단 이유는 차단된 익스플로잇의 경우 차단 작업과, 차단될 수도 있었던 익스플로잇의 경우 허용과 페어링됩니다.
침입 모니터링	시스템이 연결에서 탐지된 익스플로잇을 탐지했지만 차단하지는 않았습니다. 트리거된 침입 규칙의 상태가 이벤트 생성으로 설정되어 있으면 이러한 현상이 나타납니다.
IP 차단	시스템에서 IP 주소 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. IP 차단 이유는 항상 차단 작업과 페어링됩니다.
SSL 차단	시스템에서 SSL 검사 컨피그레이션을 기준으로 하여 암호화된 연결을 차단했습니다. SSL 차단 이유는 항상 차단 작업과 페어링됩니다.
URL 차단	시스템에서 URL 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. URL 차단 이유는 항상 차단 작업과 페어링됩니다.

수신된 시간

이벤트가 생성된 날짜 및 시간

참조된 호스트

연결의 프로토콜이 HTTP, 또는 HTTPS인 경우 이 필드에는 각 프로토콜이 사용했던 호스트 이름이 표시됩니다.

Responder Bytes, Responder Packets

세션 Responder가 전송한 총 바이트 또는 패킷 수

응답기 국가 및 대륙

세션에 응답한 호스트의 국가 및 대륙. Responder IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

응답기 **IP**

연결 또는 보안 인텔리전스 이벤트에서 세션 응답기의 호스트 IP 주소(및 호스트 이름 - DNS 확인을 활성화한 경우)

SI 카테고리 **ID(**보안 인텔리전스 카테고리**)**

네트워크 또는 URL 개체 이름 등 차단된 항목을 포함하는 개체의 이름 또는 피드 범주의 이름

서명

파일/악성코드 이벤트의 서명 ID

소스 국가 및 대륙

전송 호스트의 국가와 대륙 소스 IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

소스 **IP**

침입, 파일 또는 악성코드 이벤트에서 전송 호스트가 사용하는 IP 주소

소스 포트**/ICMP** 유형**,** 소스 포트**,** 소스 포트 **Itype**

세션 이니시에이터가 사용하는 포트 또는 ICMP 유형

소스 **SGT(Security Group Tag),** 소스 **SGT(Security Group Tag)** 이름

소스와 연결된 TrustSec SGT(Security Group Tag) 번호 및 이름(있는 경우)

SSL 실제 작업

시스템이 연결에 적용한 실제 작업. 이는 정상적인 작업과 다를 수 있습니다. 예를 들어 연결이 암호 해독을 적용하는 규칙과 일치할 수 있으나, 어떠한 이유로든 암호 해독되지 않을 수 있습니다.

작업	설명
차단/차단 및 재설정	차단된 암호화된 연결을 나타냅니다.
암호 해독(재서명)	다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.
암호 해독(대체 키)	대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

작업	설명
암호 해독(알려진 키)	알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.
기본 작업	연결이 기본 작업에 의해 처리되었음을 나타냅니다.
암호 해독 안 함	시스템이 암호 해독하지 않은 연결을 나타냅니다.

SSL 인증서 핑거프린트

인증서를 인증하는 데 사용되는 SHA 해시 값입니다.

SSL 인증서 상태

이는 인증서 상태 SSL 규칙 조건을 구성한 경우에만 적용됩니다. 암호화된 트래픽이 SSL 규칙과 일치할 경우, 이 필드에는 다음 서버 인증서 상태 값 중 하나 이상이 표시됩니다.

- Self Signed(셀프 서명)
- Valid(유효)
- Invalid Signature(잘못된 서명)
- Invalid Issuer(잘못된 발급자)
- Expired(만료됨)
- Unknown(알 수 없음)
- Not Valid Yet(아직 유효하지 않음)
- Revoked(취소됨)

해독 불가능한 트래픽이 SSL 규칙과 일치할 경우, 이 필드는 Not Checked(확인되지 않음)로 표시됩니다.

SSL 암호 그룹

연결에 사용된 암호 그룹입니다.

SSL 예상 작업

연결과 일치하는 SSL 규칙에 지정된 작업입니다.

SSL 플로우 플래그

암호화된 연결에 대한 처음 10개의 디버깅 수준 플래그입니다.

SSL 플로우 메시지

SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환되는 SSL/TLS 메시지(예: HELLO_REQUEST 및 CLIENT_HELLO)입니다. TLS 연결에서 교환되는 메시지에 대한 자세한 내용은 http://tools.ietf.org/html/rfc5246를 참조하십시오.

SSL 정책

연결에 적용되는 SSL 암호 해독 정책의 이름입니다.

SSL 규칙

연결에 적용되는 SSL 암호 해독 규칙의 이름입니다.

SSL 세션 **ID**

SSL 핸드셰이크 도중 클라이언트와 서버 간에 협상된 16진수 Session ID입니다.

SSL 티켓 **ID**

SSL 핸드셰이크 도중 전송된 세션 티켓 정보의 16진수 해시 값입니다.

SSL URL 카테고리

SSL 암호 해독 처리 도중에 확인된 대상 웹 서버의 URL 카테고리입니다.

SSL 버전

연결에 사용된 SSL/TLS 버전입니다.

TCP 플래그

연결에서 탐지된 TCP 플래그

총 패킷

연결에서 전송된 패킷의 총 수(**Initiator Packets(**이니시에이터 패킷**)** + **Responder Packets(**응답기 패킷**)**)

URL, URL 범주**, URL** 평판**, URL** 평판 점수

세션 중에 모니터링된 호스트에서 요청한 URL과 관련 범주, 평판 및 평판 점수(사용 가능한 경우)

DNS 조회 요청 필터링의 경우 DNS Query(DNS 쿼리) 필드에 표시되는 FQDN에 대한 범주 및 평판입니다. 웹 요청이 아닌 DNS 요청에 대해 범주/평판 조회를 수행하므로 URL 필드는 비어 있습니다.

시스템에서 SSL 애플리케이션을 식별하거나 차단한 경우, 요청한 URL은 암호화된 트래픽에 있으므로 시스템은 SSL 인증서를 기준으로 해당 트래픽을 식별합니다. 따라서 SSL 애플리케이션의 경우 URL은 인증서에 포함된 공용 이름을 나타냅니다.

사용자

이니시에이터 IP 주소와 연결된 사용자

VLAN

이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID

웹 애플리케이션 비즈니스 관련성

연결에서 탐지된 웹 애플리케이션 트래픽과 연계된 비즈니스 관련성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음), 또는 Very Low(매우 낮음) 연결에서 탐지된 웹 애플리케

이션의 각 유형은 관련된 비즈니스 관련성을 가지며, 이 필드는 가장 낮은(가장 타당성이 적은) 것을 표시합니다.

웹 애플리케이션 범주**,** 웹 애플리케이션 태그

웹 애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 웹 애플리케이션의 특성을 분류하는 기준

웹 애플리케이션 위험성

연결에서 탐지된 웹 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

웹 애플리케이션

연결에서 탐지된 HTTP 트래픽의 콘텐츠 또는 요청한 URL을 나타내는 웹 애플리케이션

웹 애플리케이션이 이벤트의 URL과 매칭되지 않을 경우, 해당 트래픽은 참조 트래픽(예: 광고 트래픽)일 가능성이 높습니다. 시스템이 참조 트래픽을 탐지할 경우, 시스템은 제공되는 참조 애플리케이션을 저장하고 해당 애플리케이션을 웹 애플리케이션으로 나열합니다.