파일/악성코드 이벤트 및 네트워크 파일 경로 분석

다음 주제에서는 파일 및 악성코드 이벤트, 로컬 악성코드 분석, 동적 분석, 캡처된 파일, 네트워크 파일 경로 분석의 개요를 제공합니다.

파일/악성코드 이벤트 및 네트워크 파일 경로 분석 정보

파일 정책은 일치된 트래픽에 대한 파일 및 악성코드 이벤트를 자동으로 생성하고 캡처된 파일 정보를 로깅합니다. 파일 정책이 파일 또는 악성코드 이벤트를 생성하거나 파일을 캡처하면 시스템도 연결된 연결 종료를 Secure Firewall Management Center 데이터베이스에 자동으로 로깅합니다. 이 데이터를 분석하여 모든 부정적 영향을 해결하고 향후 공격을 차단할 수 있습니다.

파일 분석 결과를 바탕으로 Analysis(분석) > Files(파일) 메뉴에서 사용할 수 있는 페이지의 테이블을 사용하여 캡처된 파일과 생성된 악성코드 및 파일 이벤트를 검토할 수 있습니다. 사용 가능한 경우, 파일의 구성, 속성, 위협 점수, 동적 분석 요약 보고서를 검사하여 악성코드 분석에 대한 추가 통찰을 얻을 수 있습니다.

보다 집중적인 분석을 위해 악성코드 파일의 네트워크 파일 경로 분석(파일이 호스트를 통과하여 네트워크에서 이동한 방법과 다양한 파일 속성을 보여주는 맵)을 사용하여 시간이 지남에 따른 호스트에서의 개별 위협의 확산을 추적할 수 있으며, 이를 통해 가장 유용한 보안 침해 통제 및 방지에 집중할 수 있습니다.

파일 규칙에서 로컬 악성코드 분석 또는 동적 분석을 구성하는 경우, 시스템은 규칙과 일치 하는 파일을 사전 분류하고 파일 구성 보고서를 생성합니다.

조직에서 *AMP for Endpoints*를 구축하여 해당 구축을 Secure Firewall Management Center에 통합한 경우, 해당 제품이 식별한 보안 침해 지표(IOC)뿐 아니라 스캔, 악성코드 탐지, 격리 레코드를 가져올 수 있습니다. 이 데이터는 네트워크에서 악성코드를 더 완벽하게 파악할 수 있도록 Firepower가 수집한 이벤트 데이터와 함께 표시됩니다.

Context Explorer, 대시보드, 보고 기능도 탐지, 캡처, 차단된 파일과 악성코드를 더욱 깊이 이해하는 데 도움이 됩니다. 이벤트를 사용하여 상관관계 정책 위반을 트리거하거나 이메일, SNMP 또는 syslog를 통해 알림을 받을 수도 있습니다.

참고 악성코드를 탐지하고 파일 및 악성코드 이벤트를 생성하도록 시스템을 구성하려면 Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 네트워크 악성코드 보호 및 파일 정책을 참고하십시오.

파일 및 악성코드 이벤트

Secure Firewall Management Center는 다양한 유형의 파일 및 악성코드 이벤트를 로깅할 수 있습니다. 개별 이벤트에 사용 가능한 정보는 정보 생성 방법과 이유에 따라 달라질 수 있습니다.

- 파일 이벤트는 Firepower system이 탐지한 악성코드를 포함한 파일을 나타냅니다(악성코드 대응 .) 파일 이벤트는 AMP for Endpoints 관련 필드를 포함하지 않습니다.
- 악성코드 이벤트는 악성코드 대응 또는 AMP for Endpoints에 의해 탐지된 악성코드를 나타냅니다. 악성코드 이벤트에는 스캔과 격리 등 AMP for Endpoints 구축이 제공하는 위협 외의 레코드 데이터도 포함될 수 있습니다.
- 회귀적 악성코드 이벤트는 악성코드 대응 에 의해 탐지된, 속성(파일이 악성코드인지 여부)이 변경된 파일을 나타냅니다.

참고

- 악성코드 대응 에 의해 악성코드로 식별된 파일은 파일 이벤트와 악성코드 이벤트를 모두 생성합니다. AMP for Endpoints에 의해 생성된 악성코드 이벤트에는 상응하는 파일 이벤트가 없습니다.
- 클라이언트와 서버에 지속적인 연결이 설정되어 있기 때문에 NetBIOS-ssn (SMB) 트래픽 검사에 의해 생성된 파일 이벤트가 즉시 연결 이벤트를 생성하지는 않습니다. 시스템은 클라이언트 또는 서버가 세션을 종료한 후 연결 이벤트를 생성합니다.
- Firepower System은 유니코드(UTF-8) 문자를 사용하는 파일 이름의 표시와 입력을 지원합니다. 다만 유니코드 파일 이름은 문자 번역된 형식으로 PDF 보고서에 표시됩니다. 또한 SMB 프로토콜은 파일 이름에 있는 인쇄할 수 없는 문자를 마침표로 대체합니다.

파일 및 악성코드 이벤트 유형

파일 이벤트

시스템은 매니지드 디바이스가 네트워크 트래픽에서 파일을 탐지하거나 차단할 때 생성되는 파일 이벤트를 현재 구축된 파일 정책의 규칙에 따라 로깅합니다.

시스템은 파일 이벤트를 생성할 때 호출하는 액세스 제어 규칙의 로깅 구성과 관계없이 연결된 연결의 종료도 Secure Firewall Management Center 데이터베이스에 로깅합니다.

악성코드 이벤트

Firepower System(특히 악성코드 대응 기능)은 전체 액세스 제어 구성의 일부로 네트워크 트래픽에서 악성코드를 탐지할 때 악성코드 이벤트를 생성합니다. 악성코드 이벤트에는 결과 이벤트의 속성과 악성코드가 탐지된 방법, 위치, 시간에 대한 상황 데이터가 포함됩니다.

표 *1:* 악성코드 이벤트 생성 시나리오

시스템이 파일을 탐지하고 다음을 수행하는 경우	속성
AMP 클라우드(악성코드 클라우드 조회 수행)에서 파일의 속성을 성공적으로 쿼리	Malware(악성코드), Clean(정상) 또는 Unknown(알 수 없음)
AMP 클라우드를 쿼리하지만 연결을 설정할 수 없거나 연결을 사용할 수 없음	사용 불가능 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.
파일에 연결된 위협 점수가 파일을 탐지한 파일 정책에서 정의한 악성코드 임계값 위협 점수를 초과하거나 로컬 악성코드 분석이 악성코드를 식별	악성코드
맞춤형 탐지 목록에 있음(수동으로 악성코드로 표시됨)	맞춤형 탐지
정상 목록에 있음(수동으로 정상으로 표시됨)	정상

악성코드 이벤트의 파일 속성 및 파일 작업

각 파일 규칙에는 시스템이 규칙의 조건과 일치하는 트래픽을 처리하는 방법을 결정하는 관련 작업이 포함됩니다. 파일 규칙 작업으로 *Block Malware(*악성코드 차단*)* 또는 *Malware Cloud Lookup(*악성코드 클라우드 조회*)*을 선택하면 시스템이 AMP 클라우드를 쿼리하여 네트워크를 통과하는 파일에 악성코드가 포함되어 있는지 확인한 다음, 위협이 되는 파일을 차단합니다. 클라우드 조회를 사용하면 SHA-256 해시 값을 기반으로 한 파일의 속성을 가져오고 로깅할 수 있습니다.

다음 테이블에서는 AMP 클라우드에서 반환한 파일 속성과 연결되는 파일 작업을 설명합니다.

표 *2:* 악성코드 이벤트의 파일 속성 및 파일 작업

파일 규칙 작업 선택됨	파일 속성	악성코드 이벤트의 파일 작업
• 악성코드 차단 • 악성코드 클라우드 조회	악성코드	차단
	• 정상 • 알 수 없음 • 사용 불가능 • 해당 없음	클라우드 조회 참고 파일 정책 편집기 Advanced Settings(고급 설정)에서 **If AMP Cloud disposition is Unknown, override disposition based upon threat score(AMP Cloud** 속성이 **Unknown(**알 수 없음**)**인 경우 위협 점수를 기반으로 속성 재정의**)** 옵션의 임계값 위협 점수를 설정할 수 있습니다. 임계값 위협 점수를 설정한 경우 동적 분석 점수가 임계값과 같거나 이보다 나쁘면 AMP 클라우드가 알 수 없음으로 판정된 파일은 악성코드로 간주됩니다.

회귀적 악성코드 이벤트

네트워크 트래픽에서 탐지된 악성코드의 경우, 속성이 변경될 수 있습니다. 예를 들어 AMP 클라우드는 이전에는 정상으로 간주되었던 파일이 지금은 악성코드로 식별되는 경우 또는 그 반대의 경우(악성코드로 식별된 파일이 실제로 정상임)를 결정할 수 있습니다. 지난주에 쿼리한 파일의 속성이 변경되면 AMP 클라우드가 시스템에 알립니다. 그러면 두 가지가 발생합니다.

- Secure Firewall Management Center는 새로운 회귀적 악성코드 이벤트를 생성합니다.

  이 새로운 회귀적 악성코드 이벤트는 지난주에 탐지된 SHA-256 해시 값이 동일한 모든 파일의 속성 변경을 나타냅니다. 따라서 이러한 이벤트에는 Secure Firewall Management Center에 속성 변경을 알린 날짜와 시간, 새로운 속성, 파일의 SHA-256 해시 값 및 위협 이름 등 제한된 정보가 포함됩니다. IP 주소나 기타 컨텍스트 정보는 포함되지 않습니다.

- Secure Firewall Management Center은 이전에 탐지된 파일의 파일 속성을 회귀적 이벤트에 연결된 SHA-256 해시 값으로 변경합니다.

  파일의 속성이 Malware(악성코드)로 변경되면 Secure Firewall Management Center은 새 악성코드 이벤트를 데이터베이스에 기록합니다. 새 속성 외에도 이 새 악성코드 이벤트의 정보는 파일이 처음 탐지됐을 때 생성된 파일 이벤트의 정보와 동일합니다.

  파일의 속성이 Clean(정상)으로 변경되는 경우, Secure Firewall Management Center은 악성코드 이벤트를 삭제하지 않습니다. 대신 해당 이벤트는 속성의 변경을 반영합니다. 즉, 정상 속성의 파일이 악성코드 테이블에 나타날 수 있지만 원래 악성코드로 파악된 경우에 한합니다. 악성코드로 식별된 적이 없는 파일은 파일 테이블에만 나타납니다.

AMP for Endpoints에 의해 생성된 악성코드 이벤트

조직에서 AMP for Endpoints를 사용하는 경우, 개별 사용자가 엔드포인트(컴퓨터 및 모바일 디바이스)에 경량 커넥터를 설치합니다. 커넥터는 파일 업로드, 다운로드, 실행, 열기, 복사, 이동 등을 수행할 때 파일을 검사할 수 있습니다. 이러한 커넥터는 AMP 클라우드와 통신하여 검사된 파일에 악성코드가 포함되었는지 확인합니다.

파일이 악성코드로 식별되면 AMP 클라우드는 위협 식별 정보를 Secure Firewall Management Center에 전송합니다. 또한 AMP 클라우드는 검사, 격리, 차단된 실행, 클라우드 회수에 대한 데이터를 비롯한 다른 종류의 정보도 Secure Firewall Management Center에 전송할 수 있습니다. Secure Firewall Management Center는 이러한 정보를 악성코드 이벤트로 로깅합니다.

참고 AMP for Endpoints에 의해 생성된 악성코드 이벤트에서 보고된 IP 주소는 네트워크 맵에 없을 수 있으며, 모니터링되는 네트워크에도 없을 수 있습니다. 구축, 규정 준수 수준, 기타 요인에 따라 AMP for Endpoints가 모니터링하는 조직 내 엔드포인트가 악성코드 대응 에서 모니터링하는 것과 같은 호스트가 아닐 수 있습니다.

Secure Endpoint를 사용한 악성코드 이벤트 분석

조직에서 Cisco Secure Endpoint를 구축한 경우:

- management center 이벤트 페이지에 Secure Endpoint가 탐지한 이벤트와 함께 악성코드 대응 가 탐지한 악성코드 이벤트를 표시하도록 시스템을 구성할 수 있습니다.
- AMP 퍼블릭 클라우드를 사용 중인 경우, 파일 경로 분석과 Secure Endpoint의 특정 SHA에 대한 기타 정보를 볼 수 있습니다.

위의 기능을 구성하려면 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Firepower* 및 *Secure Endpoint* 통합을 참조하십시오.

Secure Endpoint의 이벤트 데이터

조직에서 악성코드 방지를 위해 Secure Endpoint를 구축한 경우, Secure Endpoint의 파일 및 악성코드 데이터를 사용하여 management center에서 작업을 수행할 수 있도록 시스템을 구성할 수 있습니다.

다만 Secure Endpoint의 파일 및 악성코드 데이터와 시스템 악성코드 대응 기능의 파일 및 악성코드 데이터 간의 차이를 알아야 합니다.

Secure Endpoint 악성코드 탐지는 다운로드 또는 실행 시 엔드포인트에서 수행되지만, 매니지드 디바이스는 네트워크 트래픽에서 악성코드를 탐지하기 때문에 두 가지 유형의 악성코드 이벤트에 있는 정보는 서로 다릅니다. 예를 들어 Secure Endpoint가 탐지하는 악성코드 이벤트("엔드포인트 기반 악성코드")에는 파일 경로, 클라이언트 애플리케이션 호출 등에 대한 정보가 포함됩니다. 반면 네트워크 트래픽에서의 악성코드 탐지에는 포트, 애플리케이션 프로토콜, 파일 전송에 사용되는 연결에 대한 원래 IP 주소 정보가 포함됩니다.

또 다른 예로 악성코드 대응 가 탐지하는 악성코드 이벤트("네트워크 기반 악성코드 이벤트")의 경우, 사용자 정보에는 네트워크 검색에서 확인된 내용에 따라, 악성코드가 목표로 한 호스트에 가장 최근

에 로그인한 사용자가 표시됩니다. 하지만 Secure Endpoint에서 보고하는 사용자는 악성코드가 탐지된 엔드포인트에 현재 로그인한 사용자를 나타냅니다.

참고 배포에 따라 Secure Endpoint에서 모니터링하는 엔드포인트는 악성코드 대응 에서 모니터링하는 엔드포인트와 동일한 호스트가 아닐 수 있 습니다. 따라서 Secure Endpoint에서 생성한 악성코드 이벤트는 네트워크 맵에 호스트를 추가하지 않습니다. 그러나 시스템은 IP 및 MAC 주소 데이터를 사용하여 Secure Endpoint 배포에서 가져온 보안 침해 지표로 모니터링되는 호스트에 태그를 지정합니다. 서로 다른 악성코드 솔루션을 통해 모니터링되는 두 호스트의 IP 및 MAC 주소가 같은 경우에는 시스템이 Secure Endpoint IOC로 모니터링되는 호스트에 태그를 잘못 지정할 수 있습니다.

다음 테이블에는 악성코드 방어 라이선스 사용 시 Firepower에서 생성되는 이벤트 데이터와 Secure Endpoint에서 생성되는 이벤트 데이터의 차이점이 요약되어 있습니다.

표 ***3: AMP*** 제품 간 데이터 차이점 요약

기능	악성코드 대응	**Secure Endpoint**
생성되는 이벤트	파일 이벤트, 캡처된 파일, 악성코드 이벤트, 회귀적 악성코드 이벤트	악성코드 이벤트
악성코드 이벤트의 정보	기본적인 악성코드 이벤트 정보 및 연결 데이터(IP 주소, 포트, 애플리케이션 프로토콜)	심층적인 악성코드 이벤트 정보, 연결 데이터 없음
네트워크 파일 경로	management center기반	management center 및 Secure Endpoint 관리 콘솔에는 각각 네트워크 파일 경로 분석이 있습니다. 두 가지 모두 유용합니다.

관련 주제

Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *Integrate Firepower* 및 *Secure Endpoint* 통합

파일 및 악성코드 이벤트 워크플로 사용

테이블에서 파일 및 악성코드 이벤트를 보고 분석에 관련된 정보에 따라 이벤트 보기를 조작하려면 이 절차를 사용하십시오. 이벤트에 액세스할 때 볼 수 있는 페이지는, 넓은 보기에서 좀 더 집중된 보기로 이동하여 이벤트를 평가하는 데 사용할 수 있는 일련의 페이지인 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

다음 중 하나를 선택합니다.

- **Analysis(**분석**)** > **Files(**파일**)** > **File Events(**파일 이벤트**)**
- **Analysis(**분석**)** > **Files(**파일**)** > **Malware Events(**악성코드 이벤트**)**

팁 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 이벤트 보기에서 숨겨진 필드를 표시하려면 검색 제한 사항을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 필드 이름을 클릭합니다.

팁 특정 파일이 탐지된 연결을 신속하게 보려면 테이블의 확인란을 사용하여 파일을 선택한 다음 **Jump to(**이동**)** 드롭다운 목록에서 **Connections Events(**연결 이벤트**)**를 선택합니다.

팁 옵션을 보려면 테이블에서 항목을 마우스 오른쪽 버튼으로 클릭합니다. (옵션을 제공하지 않는 열도 있습니다.)

관련 항목

파일 및 악성코드 이벤트 필드, 7 페이지
사전 정의 파일 워크플로
사전 정의 악성코드 워크플로
이벤트 보기 구성

파일 및 악성코드 이벤트 필드

워크플로를 사용하여 확인 및 검색할 수 있는 파일 및 악성코드 이벤트는 이 섹션에서 열거하는 필드를 포함합니다. 개별 이벤트에 사용 가능한 정보는 정보 생성 방법과 이유에 따라 달라질 수 있습니다.

참고 악성코드 대응 에 의해 악성코드로 식별된 파일은 파일 이벤트와 악성코드 이벤트를 모두 생성합니다. Secure Endpoint가 생성한 악성코드 이벤트에는 대응하는 파일 이벤트가 없으며, 파일 이벤트는 Secure Endpoint 관련 필드를 포함하지 않습니다.

시스템 로그 메시지는 초기 값으로 채워지며, management center 웹 인터페이스의 해당 필드가 회고 판정 등으로 업데이트되더라도 시스템 로그 메시지는 업데이트되지 않습니다.

작업**(**시스템 로그**: FileAction)**

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

AMP 클라우드

AMP for Endpoints 이벤트 출처인 AMP 클라우드의 이름.

애플리케이션 파일 이름

AMP for Endpoints 탐지가 발생했을 때 악성코드 파일에 액세스하는 클라이언트 애플리케이션. 이러한 애플리케이션은 네트워크 검색 또는 애플리케이션 제어에 연결되지 않습니다.

애플리케이션 파일 **SHA256**

탐지가 발생했을 때 AMP for Endpoints를 탐지 또는 격리하는 파일에 액세스한 상위 파일의 SHA-256 해시 값.

통합 이벤트 뷰어에서 이 필드는 **Application File SHA-256(**애플리케이션 파일 **SHA-256)**으로 표시됩니다.

애플리케이션 프로토콜**(**시스템 로그**: ApplicationProtocol)**

매니지드 디바이스가 파일을 탐지한 트래픽에 의해 사용되는 애플리케이션 프로토콜.

애플리케이션 프로토콜 카테고리 또는 태그

애플리케이션의 기능을 파악하도록 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.

아카이브 깊이**(**시스템 로그**: ArchiveDepth)**

아카이브 파일에 중첩되는 파일의 레벨(해당되는 경우).

아카이브 이름**(**시스템 로그**: ArchiveFileName)**

악성코드 파일을 포함하는 아카이브 파일의 이름(해당되는 경우).

아카이브 파일의 내용을 보려면 **Analysis(**분석**) > Files(**파일**)**에 있는 아카이브 파일 목록 표로 이동하고 아카이브 파일의 테이블 행을 마우스 오른쪽 단추로 클릭한 다음 **View Archive Contents(**아카이브 내용 보기**)**를 클릭합니다.

아카이브 **SHA256(**시스템 로그**: ArchiveSHA256)**

악성코드 파일을 포함하는 아카이브 파일(해당되는 경우)의 SHA-256 해시 값.

아카이브 파일의 내용을 보려면 Analysis(분석) > Files(파일)에 있는 아카이브 파일 목록 표로 이동하고 아카이브 파일의 테이블 행을 마우스 오른쪽 단추로 클릭한 다음 **View Archive Contents(**아카이브 내용 보기**)**를 클릭합니다.

ArchiveFileStatus(시스템 로그만 있음**)**

검사 중인 아카이브의 상태. 다음과 같은 값을 사용할 수 있습니다.

- Pending(보류 중) - 아카이브를 검사하는 중

- Extracted(추출됨) - 문제없이 검사함
- Failed(장애 발생함) - 시스템 자원이 부족하여 검사하지 못함
- Depth Exceeded(수준 초과됨) - 검사는 성공했으나 아카이브에서 중첩 검사 수준이 초과됨
- Encrypted(암호화됨) - 검사가 일부분 성공함(아카이브가 암호화된 아카이브이거나 암호화된 아카이브를 포함함)
- Not Inspectable(검사 불가) - 검사가 일부분 성공함(파일이 손상되었거나 형식이 잘못되었을 수 있음)

사업 타당성

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.

카테고리/파일 유형 카테고리

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

클라이언트(시스템 로그**: Client)**

한 호스트에서 실행되며 서버에 의존하여 파일을 전송하는 클라이언트 애플리케이션.

클라이언트 카테고리 또는 태그

애플리케이션의 기능을 파악하도록 애플리케이션의 특성을 분류하는 기준.

Connection Counter (시스템 로그만 해당**)**

다른 동시 연결에서 하나의 연결을 구분하는 카운터입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

Connection Instance ID (시스템 로그만 해당**)**

연결 이벤트를 처리한 Snort 인스턴스입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

개수

동일한 행을 둘 이상 생성하는 제약 조건을 적용하는 경우, 각 행의 정보와 일치하는 이벤트의 수.

탐지 이름

탐지된 악성코드의 이름.

탐지기

악성코드를 식별하는 AMP for Endpoints 탐지기(예: ClamAV, Spero 또는 SHA).

디바이스

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에서 파일을 탐지한 디바이스의 이름.

AMP for Endpoints에 의해 생성된 악성코드 이벤트 및 AMP 클라우드에 의해 생성된 회귀적 악성코드 이벤트에서 management center의 이름.

DeviceUUID (시스템 로그만 해당**)**

이벤트를 생성한 Firepower 디바이스의 고유 식별자입니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

속성/파일 속성**(**시스템 로그**: SHA_Disposition)**

파일의 속성:

Malware(악성코드**)**

AMP 클라우드가 파일을 악성코드로 분류했거나, 로컬 악성코드 분석에서 악성코드가 식별되었거나, 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다.

정상

AMP 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. 정상 파일은 정상으로 변경된 경우에만 악성코드 테이블에 나타납니다.

알 수 없음

시스템이 AMP 클라우드를 쿼리했으나 파일에 상태가 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드에서 파일을 분류하지 않았습니다.

맞춤형 탐지

사용자가 파일을 커스텀 탐지 목록에 추가했음을 나타냅니다.

사용 불가능

시스템이 AMP 클라우드를 쿼리하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.

해당 없음

파일 탐지 또는 파일 차단 규칙이 파일을 처리했으며 Secure Firewall Management Center이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.

파일 속성은 시스템이 AMP 클라우드를 쿼리하지 않은 파일에 대해서만 표시됩니다.

시스템 로그는 초기 속성만 반영합니다. 회귀적 판정을 반영하도록 업데이트 되지 않습니다.

도메인

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에서 파일을 탐지한 디바이스의 도메인. AMP for Endpoints에 의해 생성된 악성코드 이벤트 및 AMP 클라우드에 의해 생성된 회귀적 악성코드 이벤트에서 해당 이벤트를 보고한 AMP 클라우드 연결과 관련된 도메인.

이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

DstIP(시스템 로그만 있음**)**

연결에 응답한 호스트의 IP 주소. FileDirection 필드 값에 따라 파일 발신자나 수신자의 IP 주소일 수 있습니다.

FileDirection이 **`Upload`(**업로드**)** 인 경우 파일 수신자의 IP 주소입니다.

FileDirection이 **`Download`(**다운로드**)** 인 경우 파일 발신자의 IP 주소입니다.

SrcIP도 참조하십시오.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침도 참조하십시오.

DstPort(시스템 로그만 있음**)**

DstIP아래 설명된 연결에 사용되는 포트.

이그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에서 벗어날 때 사용하는 가상 라우터의 이름입니다.

이벤트 하위 유형

악성코드 탐지로 이어진 AMP for Endpoints 작업(예: Create(생성), Execute(실행), Move(이동) 또는 Scan(스캔)).

이벤트 유형

악성코드 이벤트 하위 유형.

파일 이름(시스템 로그: **FileName)**

파일의 이름

파일 경로

AMP for Endpoints에 의해 탐지된 악성코드 파일의 파일 경로(파일 이름 제외).

파일 정책**(**시스템 로그**: FilePolicy)**

파일을 탐지한 파일 정책.

파일 스토리지**/**저장됨**(**시스템 로그**: FileStorageStatus)**

이벤트와 관련 된 파일의 저장 상태:

Stored(저장됨**)**

관련된 파일이 현재 저장되어 있는 모든 이벤트를 반환합니다.

Stored in connection(연결에 저장됨**)**

관련된 파일이 현재 저장되어 있는지와 상관없이, 시스템이 관련된 파일을 캡처 및 저장한 모든 이벤트를 반환합니다.

Failed(TLS 필수 실패**)**

시스템이 관련된 파일을 저장하지 못한 모든 이벤트를 반환합니다.

시스템 로그 필드는 초기 상태만 포함합니다. 변경된 상태를 반영하도록 업데이트되지 않습니다.

File Timestamp(파일 타임스탬프**)**

AMP for Endpoints가 악성코드 파일이 생성된 것으로 탐지한 시간 및 날짜.

FileDirection(시스템 로그만 있음**)**

연결 중 파일이 업로드되거나 다운로드되었는지 여부. 가능한 값은 다음과 같습니다.

- Download(다운로드) — DstIP에서 SrcIP로 파일이 전송되었습니다.
- Upload(업로드) — SrcIP에서 DstIP로 파일이 전송되었습니다.

FileSandboxStatus(시스템 로그만 있음**)**

동적 분석을 위해 파일이 전송되었는지 여부와 그러한 경우 해당 상태를 나타냅니다.

첫 번째 패킷 시간 **(**시스템 로그만 해당**)**

시스템이 첫 번째 패킷을 수신한 시간입니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

FirstPacketSecond(시스템 로그만 있음**)**

파일 다운로드 또는 업로드 플로우가 시작된 시간으로, .

이벤트가 발생한 시간이 메시지 헤더 타임스탬프에 캡처됩니다.

HTTP 응답 코드

파일이 전송된 경우 클라이언트의 HTTP 요청에 대한 응답으로 제출된 HTTP 상태 코드.

인그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에 진입할 때 사용하는 가상 라우터의 이름입니다.

IOC

악성코드 이벤트가 연결과 관련된 호스트에 대해 IOC(indication of compromise)를 트리거했는지 여부. AMP for Endpoints 데이터 IOC 규칙을 트리거하는 경우, 전체 악성코드 이벤트가 AMP IOC 유형으로 생성됩니다.

메시지

악성코드 이벤트와 연결된 추가 정보. 파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트의 경우, 이 필드는 속성이 변경되어 관련 회귀적 이벤트가 있는 파일에 대해서만 입력됩니다.

MITRE

클릭하여 해당 계층 내에서 MITRE 전략 및 기술의 전체 목록을 나타내는 모달을 표시할 수 있는 기술의 수입니다.

Protocol(시스템 로그만 있음)

연결에 사용된 프로토콜(예: TCP 또는 UDP).

Receiving Continent(수신 대륙)

파일을 수신하는 호스트의 대륙.

Receiving Country(수신 국가)

파일을 수신하는 호스트의 국가.

수신 **IP**

management center 웹 인터페이스에서 파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에 대해 파일을 수신하는 호스트의 IP 주소. 이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침도 참조하십시오.

AMP for Endpoints에 의해 생성된 악성코드 이벤트에서 커넥터가 이벤트를 보고한 엔드포인트의 IP 주소.

시스템 로그에 해당하는 항목(Firepower 디바이스에서 생성된 이벤트만 해당)은 **DstIP** 및 **SrcIP**를 참조하십시오.

수신 포트

management center 웹 인터페이스에서 파일이 탐지된 트래픽에 의해 사용된 대상 포트.

시스템 로그 해당 정보는 **DstIP**, **SrcIP**, **DstPort**, **SrcPort**를 참조하십시오.

보안 상황(시스템 로그: **Context**)

트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터입니다. 다중 상황 모드에서 실행되는 ASA FirePOWER 디바이스를 최소한 한 개 관리하는 경우 시스템에 이 필드만 표시됩니다.

Sending Continent(송신 대륙)

파일을 전송하는 호스트의 대륙.

Sending Country(송신 국가)

파일을 전송하는 호스트의 국가.

송신 **IP**

management center 웹 인터페이스에서 파일을 보내는 호스트의 IP 주소. 이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침도 참조하십시오.

시스템 로그 해당 정보는 **DstIP** 및 **SrcIP**를 참조하십시오.

송신 포트

management center 웹 인터페이스에서 파일이 탐지된 트래픽에 의해 사용된 소스 포트.

시스템 로그 해당 정보는 **DstIP**, **SrcIP**, **DstPort**, **SrcPort**를 참조하십시오.

SHA256/파일 **SHA256**(시스템 로그: **FileSHA256**)

파일의 SHA-256 해시 값

SHA256 값을 생성하려면 다음 중 하나를 통해 파일을 처리해야 합니다.

- **Store files**(파일 저장)가 활성화된 Detect Files(파일 탐지) 파일 규칙
- **Store files**(파일 저장)가 활성화된 Block Files(파일 차단) 파일 규칙
- Malware Cloud Lookup file(악성코드 클라우드 검색) 파일 규칙
- Block Malware file(악성코드 차단) 파일 규칙
- AMP for Endpoints

이 열에는 가장 최근에 탐지된 파일 이벤트 및 파일 속성을 나타내고 네트워크 파일 경로로 링크되는 네트워크 파일 경로 아이콘도 표시됩니다.

크기(**KB**)/파일 크기(**KB**)(시스템 로그: **FileSize**)

management center 웹 인터페이스에서 킬로바이트 단위의 파일 크기.

시스템 로그 메시지에서 바이트 단위의 파일 크기.

파일을 완전히 수신하기 전에 시스템에서 파일 유형을 결정하는 경우, 파일 크기가 계산되지 않을 수 있습니다. 그러한 경우 이 필드는 공란입니다.

SperoDisposition(시스템 로그만 있음**)**

파일 분석에 SPERO 서명이 사용되었는지를 나타냅니다. 가능한 값은 다음과 같습니다.

- 파일에서 수행되는 Spero 탐지
- 파일에서 수행되지 않는 Spero 탐지.

SrcIP(시스템 로그만 있음**)**

연결을 시작한 호스트의 IP 주소. FileDirection 필드 값에 따라 파일 발신자나 수신자의 IP 주소일 수 있습니다.

FileDirection이 **Upload(**업로드**)** 인 경우 파일 발신자의 IP 주소입니다.

FileDirection이 **Download(**다운로드**)** 인 경우 파일 수신자의 IP 주소입니다.

DstIP도 참조하십시오.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침도 참조하십시오.

SrcPort(시스템 로그만 있음**)**

SrcIP아래 설명된 연결에 사용되는 포트.

SSL 실제 작업**(**시스템 로그**: SSLActualAction)**

시스템이 암호화된 트래픽에 적용하는 작업.

Block or Block with reset(차단 또는 차단 후 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.

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.

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL 인증서 정보

트래픽 암호화에 사용하는 공개 키 인증서에 저장된 정보로 다음을 포함합니다.

- Subject/Issuer Common Name(대상자/발급자 공용 이름)
- Subject/Issuer Organization(대상자/발급자 기관)
- Subject/Issuer Organization Unit(대상자/발급자 기관 부서)
- Not Valid Before/After(유효기간)
- Serial Number, Certificate Fingerprint(일련 번호, 인증서 지문)
- Public Key Fingerprint(공개 키 지문)

시스템 로그는 **SSLCertificate**를 참조하십시오.

SSL 실패 이유**(**시스템 로그**: SSLFlowStatus)**

시스템이 암호화된 트래픽의 암호 해독에 실패한 이유:

- Unknown(알 수 없음)
- No Match(일치하지 않음)
- Success(TLS 필수 성공)
- Uncached Session(캐시되지 않은 세션)
- Unknown Cipher Suite(알 수 없는 암호 그룹)
- Unsupported Cipher Suite(지원되지 않는 암호 그룹)
- Unsupported SSL Version(지원되지 않는 SSL 버전)
- SSL Compression Used(SSL 압축 사용됨)
- Session Undecryptable in Passive Mode(패시브 모드에서 세션 암호 해독 불가)
- Handshake Error(핸드셰이크 오류)
- Decryption Error(암호 해독 오류)
- Pending Server Name Category Lookup(서버 이름 카테고리 조회 보류 중)
- Pending Common Name Category Lookup(공용 이름 카테고리 조회 보류 중)
- Internal Error
- Network Parameters Unavailable(네트워크 파라미터 사용 불가)
- Invalid Server Certificate Handle(유효하지 않은 서버 인증서 처리)
- Server Certificate Fingerprint Unavailable(서버 인증서 지문 사용 불가)
- Cannot Cache Subject DN(대상자 DN 캐시 불가)

- Cannot Cache Issuer DN(발급자 DN 캐시 발가)
- Unknown SSL Version(알 수 없는 SSL 버전)
- External Certificate List Unavailable(외부 인증서 목록 사용 불가)
- External Certificate Fingerprint Unavailable(외부 인증서 지문 사용 불가)
- Internal Certificate List Invalid(내부 인증서 목록이 유효하지 않음)
- Internal Certificate List Unavailable(내부 인증서 목록 사용 불가)
- Internal Certificate Unavailable(내부 인증서 사용 불가)
- Internal Certificate Fingerprint Unavailable(내부 인증서 지문 사용 불가)
- Server Certificate Validation Unavailable(서버 인증서 검증 사용 불가)
- Server Certificate Validation Failure(서버 인증서 검증 장애)
- Invalid Action(유효하지 않은 작업)

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL 상태

암호화된 연결을 로깅한 **SSL Actual Action(SSL** 실제 작업**)**(해독 규칙, 기본 작업 또는 암호 해독이 불가능한 트래픽 작업)과 관련된 작업. 잠금 아이콘이 TLS/SSL 인증서 세부 사항으로 연결됩니다. 인증서를 사용할 수 없는 경우(예: TLS/SSL 핸드셰이크 오류로 연결 차단), 잠금 아이콘이 흐리게 표시됩니다.

시스템이 암호화된 연결을 해독하지 못할 경우, 실행된 **SSL Actual Action(SSL** 실제 작업**)** (해독 불가능한 트래픽 작업)과 **SSL Failure Reason(SSL** 실패 이유**)**가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)`(암호 해독 하지 않음(알려지지 않은 암호화 그룹))로 표시됩니다.

이 필드를 검색할 때 **SSL Actual Action(SSL** 실제 작업**)** 중 하나 이상과 **SSL Failure Reason(SSL** 실패 이유**)**를 입력하고 시스템이 처리했거나 암호 해독에 실패한 암호화된 트래픽을 확인합니다.

SSL 대상자**/**발급자 국가

암호화 인증서와 관련된 대상자 또는 발급자 국가의 2자 ISO 3166-1 alpha-2 국가 코드.

SSLCertificate(시스템 로그만 있음**)**

TLS/SSL 서버의 인증서 지문.

위협 이름**(**시스템 로그**: ThreatName)**

탐지된 악성코드의 이름.

위협 점수(시스템 로그: **ThreatScore**)

이 파일과 가장 최근에 연결된 위협 점수. 동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 값입니다.

위협 점수 아이콘이 Dynamic Analysis Summary(동적 분석 요약) 보고서로 링크됩니다.

시간

이벤트가 생성된 날짜 및 시간 이 필드는 검색할 수 없습니다.

시스템 로그 메시지에서 **FirstPacketSecond**를 참조하십시오.

유형/파일 유형(시스템 로그: **FileType**)

HTML 또는 MSEXE 등의 파일 형식

URI/파일 **URI**(시스템 로그: **URI**)

파일 트랜잭션과 관련된 연결의 URI(예: 사용자가 파일을 다운로드하는 URL).

사용자(시스템 로그: **User**)

연결을 시작한 IP 주소에 연결된 사용자 이름입니다. 이 IP 주소가 네트워크 외부에 있는 경우, 일반적으로 연결된 사용자 이름을 알 수 없습니다.

해당하는 경우 사용자 이름 앞에 `<realm>\`을 입력합니다.

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트의 경우, 이 필드에는 ID 정책 또는 권한 있는 로그인에 의해 결정된 사용자 이름이 표시됩니다. ID 정책이 없는 경우, No Authentication Required(인증 필요 없음)가 표시됩니다.

AMP for Endpoints에 의해 생성된 악성코드 이벤트에서 AMP for Endpoints가 사용자 이름을 결정합니다. 이러한 사용자는 사용자 검색 또는 제어에 연결할 수 없습니다. 이러한 사용자는 Users(사용자) 테이블에 나타나지 않으며 세부 사항도 확인할 수 없습니다.

웹 애플리케이션(시스템 로그: **WebApplication**)

연결에서 탐지된 HTTP 트래픽의 콘텐츠 또는 요청된 URL을 나타내는 웹 애플리케이.

웹 애플리케이션 카테고리 또는 태그

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

악성코드 이벤트 하위 유형

다음 표에는 악성코드 이벤트 하위 유형, AMP for Networks가 생성하는 악성코드 이벤트("네트워크 기반 악성코드 이벤트") 또는 AMP for Endpoints가 생성하는 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")에 해당 하위 유형이 있을 수 있는지 여부, 시스템이 해당 하위 유형을 사용하여 네트워크 파일 경로 분석을 작성하는지 여부가 나열되어 있습니다.

표 *4:* 악성코드 이벤트 유형

악성코드 이벤트 하위 유형/검색 값	악성코드 대응	**AMP for Endpoints**	파일 경로 분석
네트워크 파일 전송에서 탐지된 위협	예	아니요	예
네트워크 파일 전송에서 탐지된 위협(회귀적)	예	아니요	예
위협 탐지됨	아니요	예	예
제외에서 위협 탐지	아니요	예	예
위협 격리됨	아니요	예	예
AMP IOC(보안 침해 지표)	아니요	예	아니요
차단된 실행	아니요	예	아니요
Cloud Recall 격리	아니요	예	아니요
Cloud Recall 격리 시도 실패	아니요	예	아니요
클라우드 리콜 격리 시작	아니요	예	아니요
격리에서 Cloud Recall 복원	아니요	예	아니요
격리에서 Cloud Recall 복원 실패	아니요	예	아니요
격리에서 클라우드 리콜 복원 시작	아니요	예	아니요
격리 실패	아니요	예	아니요
격리 항목 복원	아니요	예	아니요
격리 복원 실패	아니요	예	아니요
격리 복원 시작	아니요	예	아니요
스캔 완료, 탐지 항목 없음	아니요	예	아니요
스캔 완료, 탐지 항목 있음	아니요	예	아니요
스캔 실패	아니요	예	아니요
스캔 시작	아니요	예	아니요

파일 및 악성코드 이벤트 필드에서 사용할 수 있는 정보

다음 표에는 시스템이 각 파일 및 악성코드 이벤트 필드에 정보를 표시하는지 여부가 나열되어 있습니다.

조직이 AMP for Endpoints를 구축하고 해당 제품을 Firepower 구축에 통합한 경우:

- AMP for Endpoints 구축에서 가져온 악성코드 이벤트 및 보안 침해 지표 (IOC)에는 컨텍스트 연결 정보가 포함되지 않지만 파일 경로와 호출 클라이언트 애플리케이션 등 다운로드 또는 실행 시 얻는 정보는 포함됩니다.
- 파일 이벤트 테이블 보기에는 AMP for Endpoints 관련 필드가 표시되지 않습니다.

표 ***5:*** 파일 및 악성코드 이벤트 필드에서 사용할 수 있는 정보

필드	파일 이벤트	**Firepower System**에서 탐지되는 악성코드 이벤트	**Firepower System**에서 탐지되는 회귀적 이벤트	**AMP for Endpoints**에서 탐지되는 악성코드 이벤트
작업	예	예	예	아니요
AMP 클라우드	아니요	아니요	아니요	예
애플리케이션 파일 이름	아니요	아니요	아니요	예
애플리케이션 파일 SHA256	아니요	아니요	아니요	예
Application Protocol(애플리케이션 프로토콜)	예	예	아니요	아니요
애플리케이션 프로토콜 카테고리 또는 태그	예	예	예	아니요
애플리케이션 위험성	예	예	예	아니요
아카이브 수준	예	예	아니요	예
아카이브 이름	예	예	아니요	예
아카이브 SHA256	예	예	아니요	예
Business Relevance	예	예	예	아니요
카테고리/파일 유형 카테고리	예	예	아니요	예
클라이언트	예	예	예	아니요
클라이언트 카테고리 또는 태그	예	예	예	아니요
개수	예	예	예	예
탐지 이름	아니요	예	아니요	아니요
탐지기	아니요	아니요	아니요	예
디바이스	예	예	예	예

필드	파일 이벤트	**Firepower System**에서 탐지되는 악성코드 이벤트	**Firepower System**에서 탐지되는 회귀적 이벤트	**AMP for Endpoints**에서 탐지되는 악성코드 이벤트
속성/파일 속성	예	예	예	아니요
도메인	예	예	예	예
이벤트 하위 유형	아니요	아니요	아니요	예
이벤트 유형	아니요	예	예	예
파일 이름	예	예	아니요	예
파일 경로	아니요	아니요	아니요	예
파일 정책	예	아니요	아니요	아니요
파일 타임스탬프	아니요	아니요	아니요	예
HTTP 응답 코드	예	예	아니요	아니요
IOC(보안 침해 지표)	아니요	예	예	예
메시지	예	예	아니요	예
수신 대륙	예	예	예	아니요
수신 국가	예	예	아니요	아니요
수신 IP	예	예	아니요	예
수신 포트	예	예	아니요	아니요
보안 상황	예	예	예	예
송신 대륙	예	예	예	아니요
송신 국가	예	예	아니요	아니요
송신 IP	예	예	아니요	아니요
송신 포트	예	예	아니요	아니요
SHA256/파일 SHA256	예	예	예	예
크기(KB)/파일 크기(KB)	예	예	아니요	예
SSL 실제 작업(검색만 해당)	예	예	아니요	아니요
SSL 인증서 정보(검색만 해당)	예	예	아니요	아니요

필드	파일 이벤트	**Firepower System**에서 탐지되는 악성코드 이벤트	**Firepower System**에서 탐지되는 회귀적 이벤트	**AMP for Endpoints**에서 탐지되는 악성코드 이벤트
SSL 실패 이유(검색만 해당)	예	예	아니요	아니요
SSL Status	예	예	아니요	아니요
SSL 주체/발급자 국가(검색만 해당)	예	예	아니요	아니요
파일 스토리지/저장됨(검색만 해당)	예	예	아니요	아니요
위협 이름	아니요	예	예	예
위협 점수	예	예	아니요	아니요
시간	예	예	예	예
파일/파일 형식	예	예	아니요	예
URI/파일 URI	예	예	아니요	아니요
사용자	예	예	아니요	예
웹 애플리케이션	예	예	예	아니요
웹 애플리케이션 카테고리 또는 태그	예	예	예	아니요

분석된 파일에 대한 세부 정보 보기

팁 추가 옵션을 보려면 이벤트 페이지의 테이블에서 파일 SHA를 마우스 오른쪽 버튼으로 클릭합니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사 섹션을 참조해 주십시오.

파일 구성 보고서

로컬 악성코드 분석 또는 동적 분석을 구성하는 경우, 시스템은 파일을 분석한 후 파일 구성 보고서를 생성합니다. 이 보고서를 사용하면 추가로 파일을 분석하여 포함된 악성 코드를 파일이 전달할 수 있는지 여부를 확인할 수 있습니다.

파일 구성 보고서에는 파일 속성, 파일에 포함된 개체, 탐지된 바이러스가 나열됩니다. 파일 구성 보고서에는 해당 파일 유형과 관련된 추가 정보도 나열될 수 있습니다. 시스템은 저장된 파일을 정리할 때 연결된 파일 구성 보고서도 정리합니다.

파일 구성 정보를 보려면 네트워크 파일 경로 분석 사용, 33 페이지를 참조하십시오.

AMP 프라이빗 클라우드에서 파일 세부 정보 보기

AMP 프라이빗 클라우드를 구축한 경우, 프라이빗 클라우드에서 분석된 파일에 대한 추가 세부 정보를 볼 수 있습니다.

자세한 내용은 프라이빗 클라우드 설명서를 참조하십시오.

프로시저

AMP 프라이빗 클라우드 콘솔에 직접 로그인합니다.

위협 점수 및 동적 분석 요약 보고서

위협 점수

표 *6:* 위협 점수 평가

위협 점수	숫자 점수	아이콘
Low	0-24	**Low**
Medium	25-69	**Medium**
High	70-94	**High**
Very High	95-100	매우 높음

Secure Firewall Management Center은 파일의 속성과 동일한 시간 동안 파일의 위협 점수를 캐시합니다. 이러한 파일이 나중에 탐지되는 경우, 시스템은 Secure Malware Analytics 클라우드 또는 Secure Malware Analytics 어플라이언스를 다시 쿼리하는 대신 캐시된 위협 점수를 표시합니다. 위협 점수가 정의된 악성코드 임계값 점수를 초과하는 파일에 자동으로 악성코드 파일 속성을 할당할 수 있습니다.

동적 분석 요약

동적 분석 요약을 사용할 수 있는 경우 위협 점수 아이콘을 클릭하여 위협 점수를 볼 수 있습니다. 여러 보고서가 존재하는 경우, 이 요약은 정확한 위협 점수와 일치하는 최근 보고서를 기반으로 합니다. 정확한 위협 점수와 일치하는 보고서가 없으면 위협 점수가 가장 높은 보고서가 표시됩니다. 보고서가 둘 이상이면 위협 점수를 선택하여 각각의 보고서를 볼 수 있습니다.

요약에는 위협 점수를 구성하는 각 구성 요소 위협이 나열되어 있습니다. 각 위협 요소를 확장하여 AMP 클라우드에서 발견한 내용 및 이 구성 요소 위협과 관련된 프로세스를 나열할 수 있습니다.

프로세스 트리에는 Secure Malware Analytics 클라우드가 파일 실행을 시도했을 때 시작된 프로세스가 표시됩니다. 이는 악성코드가 포함된 파일이 예상을 뛰어넘어 프로세스 및 시스템 리소스에 대한

액세스를 시도했는지(예: Word 문서를 실행하여 Microsoft Word를 열고, Explorer를 시작한 다음 Java Runtime Environment 시작) 여부를 파악하는 데 도움이 될 수 있습니다.

나열된 각 프로세스에는 실제 프로세스 확인에 사용할 수 있는 프로세스 식별자가 포함되어 있습니다. 프로세스 트리의 하위 노드는 상위 프로세스의 결과로 시작된 프로세스를 나타냅니다.

동적 분석 요약에서 **View Full Report(**전체 보고서 보기**)**를 클릭하여 AMP 클라우드의 전체 분석이 자세히 설명된 전체 분석 보고서를 볼 수 있습니다. 여기에는 일반 파일 정보, 탐지된 모든 프로세스에 대한 보다 심층적인 검토, 파일 분석의 분류 및 기타 관련 정보가 포함되어 있습니다.

Cisco Secure Malware Analytics 클라우드에서 동적 분석 결과 보기

Secure Malware Analytics는 분석된 파일에 대해 management center에서 제공하는 것보다 자세한 보고를 제공합니다. 조직이 Secure Malware Analytics 클라우드 계정을 가지고 있다면 Secure Malware Analytics 포털에 직접 액세스하여 매니지드 디바이스에서 분석을 위해 전송한 파일에 대한 추가 세부 정보를 볼 수 있습니다.

시작하기 전에

- management center를 Secure Malware Analytics 클라우드 계정과 연결합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 퍼블릭 클라우드의 동적 분석 결과에 대한 액세스 활성화를 참조하십시오.
- 라이선스 요구 사항: 악성코드
- 이 작업을 수행하려면 전역 도메인에 있어야 합니다.
- 관리, 액세스 관리, 네트워크 관리 사용자 역할 중 하나가 있어야 합니다.

프로시저

단계 **1** Secure Malware Analytics 설명서에서 제공하는 주소에서 Secure Malware Analytics 클라우드 포털에 액세스합니다.

단계 **2** 이 작업의 사전 요구 사항에서 연결을 생성하는 데 사용한 계정 자격 증명을 사용하여 로그인합니다.

단계 **3** 조직이 전송한 파일을 보거나 SHA를 사용하여 특정 파일을 검색합니다.

질문이 있는 경우 Secure Malware Analytics 설명서를 참조하십시오.

캡처된 파일 워크플로 사용

매니지드 디바이스는 네트워크 트래픽에서 탐지된 파일을 캡처할 때 이벤트를 로깅합니다.

참고 악성코드가 포함된 파일을 디바이스가 캡처하는 경우, 디바이스는 2개의 이벤트를 생성합니다. 즉, 파일을 탐지하면 파일 이벤트를 생성하고 악성코드를 탐지하면 악성코드 이벤트를 생성합니다.

테이블에서 캡처된 파일 목록을 보고 분석과 관련된 정보에 따라 이벤트 보기를 조작하려면 이 절차를 사용하십시오. 캡처된 파일에 액세스할 때 볼 수 있는 페이지는, 넓은 보기에서 좀 더 집중된 보기로 이동하여 이벤트를 평가하는 데 사용할 수 있는 일련의 페이지인 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

파일 정책 업데이트 등 구성 변경 후 시스템이 파일을 다시 캡처하는 경우, 시스템은 해당 파일의 기존 정보를 업데이트합니다.

예를 들어 악성 코드 클라우드 조회 작업을 사용하여 파일을 캡처하도록 파일 정책을 구성하는 경우, 시스템은 파일과 함께 파일 속성 및 위협 점수를 저장합니다. 그런 다음 파일 정책을 업데이트하고 시스템이 새로운 **Detect Files(**파일 탐지**)** 작업으로 인해 동일한 파일을 다시 캡처하는 경우, 시스템은 파일의 **Last Changed(**마지막으로 변경된**)** 값을 업데이트합니다. 하지만 사용자가 다른 악성코드 클라우드 조회를 수행하지 않았더라도 시스템은 기존 속성과 위협 점수를 제거하지 않습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

Analysis(분석**)** > **Files(**파일**)** > **Captured Files(**캡처된 파일**)**을(를) 선택합니다.

팁 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 이벤트 보기에서 숨겨진 필드를 표시하려면 검색 제한 사항을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 필드 이름을 클릭합니다.

관련 항목

캡처된 파일 필드, 25 페이지
사전 정의 캡처 파일 워크플로
이벤트 보기 구성

캡처된 파일 필드

사전 정의된 캡처된 파일 워크플로의 마지막 페이지이며 맞춤형 워크플로에 추가할 수 있는 캡처된 파일의 테이블 보기에는 캡처된 파일 테이블의 각 필드에 대한 열이 포함됩니다.

이 테이블을 검색할 때는 검색하는 이벤트에서 사용할 수 있는 데이터에 따라 검색 결과가 달라짐에 유의하십시오. 사용 가능한 데이터에 따라 검색 제약 조건이 적용되지 않을 수도 있습니다. 예를 들어 동적 분석을 위해 제출된 적이 없는 파일에는 연결된 위협 점수가 없을 수 있습니다.

표 *7:* 캡처된 파일 필드

필드	설명
아카이브 검사 상태	아카이브 파일의 경우 아카이브 검사의 상태: • Pending(보류 중)은 시스템이 아카이브 파일 및 내용을 여전히 검사 중임을 나타냅니다. 파일이 시스템을 다시 통과하면 완전한 정보를 이용할 수 있게 됩니다. • Extracted(추출됨)는 시스템이 아카이브의 내용을 추출 및 검사할 수 있게 되었음을 나타냅니다. • 매우 드물지만 시스템이 추출을 처리할 수 없는 경우 Failed(실패함)가 발생할 수 있습니다. • Depth Exceeded(수준 초과)는 아카이브에 허용되는 최대 깊이를 초과하여 중첩된 아카이브 파일이 포함되어 있음을 나타냅니다. • Encrypted(암호화됨)는 아카이브 파일의 내용이 암호화되어 검사할 수 없음을 나타냅니다. • Not Inspectable(검사 불가능)은 시스템이 아카이브의 내용을 추출 및 검사할 수 없음을 나타냅니다. 이 상태의 세 가지 주요 원인은 정책 규칙 작업, 정책 구성 및 손상된 파일입니다. 아카이브 파일의 내용을 보려면 테이블에서 해당 행을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 표시한 다음 **View Archive Contents(**아카이브 내용 보기**)**를 선택합니다.
카테고리	파일 유형의 일반적인 범주(예: Office 문서, 아카이브, 멀티미디어, 실행 파일, PDF 파일, 인코딩, 그래픽 또는 시스템 파일 등)
탐지 이름	탐지된 악성코드의 이름.
속성	파일의 악성코드 대응 속성: • Malware(악성코드)는 AMP 클라우드가 파일을 악성코드로 분류했거나 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다. • Clean(정상)은 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • Unknown(알 수 없음)은 시스템이 AMP 클라우드를 쿼리했지만 파일에 속성이 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드에서 파일을 분류하지 않았습니다. • Custom Detection(사용자 지정 탐지)은 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • Unavailable(사용할 수 없음)은 시스템이 AMP 클라우드를 쿼리할 수 없음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다. • N/A는 Detect Files(파일 탐지) 또는 Block Files(파일 차단) 규칙이 파일을 처리했고 Secure Firewall Management Center이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.

필드	설명
도메인	캡처된 파일이 탐지된 도메인입니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
동적 분석 상태	파일이 동적 분석을 위해 제출되었는지 여부를 나타내는 다음 값 중 하나 이상: • Analysis Complete(분석 완료) - 위협 점수 및 동적 분석 요약 보고서를 받은, 동적 분석을 위해 제출된 파일 • Capacity Handled(처리된 용량) - 현재 제출할 수 없어서 저장된 파일 • Capacity Handled (Network Issue)(처리된 용량(네트워크 문제)) - 네트워크 연결 문제로 인해 제출할 수 없어서 저장된 파일 • Capacity Handled (Rate Limit)(처리된 용량(속도 제한)) - 최대 제출 수에 도달했기 때문에 제출할 수 없어 저장된 파일 • Device Not Activated(디바이스가 활성화되지 않음) - 디바이스가 온프레미스 Secure Malware Analytics 어플라이언스에서 활성화되지 않아 제출되지 않은 파일 이 상태가 표시되면 지원팀에 문의하십시오. • Failure (Analysis Timeout)(실패(분석 시간 초과)) - AMP 클라우드가 아직 결과를 반환하지 않은 제출된 파일 • Failure (Cannot Run File)(실패(파일 실행 불가)) - AMP 클라우드가 테스트 환경에서 실행할 수 없는 제출된 파일 • Failure (Network Issue)(실패(네트워크 문제)) - 네트워크 연결 오류로 인해 제출되지 않은 파일 • Not Sent for Analysis(분석을 위해 제출되지 않음) - 제출되지 않은 파일 • Not Suspicious (Not Sent For Analysis)(의심스럽지 않음(분석을 위해 제출되지 않음)) - 악성코드가 아닌 것으로 사전 분류된 파일 • 이전에 분석됨 - 캐시된 위협 점수가 있는 파일로, 이전에 전송되었음을 나타냅니다. • 분석이 거부됨 - 정적 분석을 기반으로 하는 파일은 예를 들어 동적 요소가 포함되어 있지 않으므로 위험할 가능성이 낮습니다. • Sent for Analysis(분석을 위해 전송) - 악성코드로 사전 분류되고 동적 분석을 위해 대기열에 넣은 파일
동적분석상태변경됨	파일의 동적 분석 상태가 마지막으로 변경된 시간.
파일 이름	파일의 SHA-256 해시 값에 연결된, 가장 최근에 탐지된 파일 이름.
마지막 변경 날짜	이 파일에 연결된 정보가 마지막으로 업데이트된 시간.
마지막 전송	동적 분석을 위해 파일이 가장 최근에 클라우드에 제출된 시간.

필드	설명
로컬 악성코드 분석 상태	시스템이 파일에서 로컬 악성코드 분석을 수행했는지 여부를 나타내는 다음 값 중 하나: • Analysis Complete(분석 완료) - 시스템이 로컬 악성코드 분석을 사용하여 파일을 검사하고 사전 분류했습니다 • Analysis Failed(분석 실패) - 시스템이 로컬 악성코드 분석을 사용하여 파일 검사를 시도하고 실패했습니다 • Manual Request Submitted(수동 요청 제출됨) - 사용자가 로컬 악성코드 분석을 위해 파일을 제출했습니다 • Not Analyzed(분석되지 않음) - 시스템이 로컬 악성코드 분석을 사용하여 파일을 검사하지 않았습니다
SHA256	파일의 SHA-256 해시 값 및 가장 최근에 탐지된 파일 이벤트 및 파일 속성을 나타내는 네트워크 파일 경로 분석 아이콘. 네트워크 파일 경로 분석을 보려면 경로 분석 아이콘을 클릭합니다.
스토리지 상태	파일이 매니지드 디바이스에 저장되는지 여부를 나타냅니다. • 파일 저장됨 • 저장되지 않음(속성 보류 중)
위협 점수	이 파일과 가장 최근에 연결된 위협 점수. 동적 분석 요약 보고서를 보려면 위협 점수 아이콘을 클릭합니다.
유형	파일 형식(예: HTML 또는 MSEXE).

저장된 파일 다운로드

디바이스가 파일을 저장하면 Secure Firewall Management Center가 해당 디바이스와 통신할 수 있고 파일을 삭제하지 않은 한 사용자는 장기 스토리지 및 분석을 위해 파일을 로컬 호스트에 다운로드하고 수동으로 파일을 분석할 수 있습니다. 연결된 파일 이벤트, 악성코드 이벤트, 캡처된 파일 보기 또는 파일의 경로 분석에서 파일을 다운로드할 수 있습니다.

악성코드는 유해하므로 기본적으로 모든 파일 다운로드를 확인해야 합니다. 하지만 사용자 환경설정에서 확인을 비활성화할 수 있습니다.

Unknown(알 수 없음) 속성의 파일에는 악성코드가 포함되어 있을 수 있으므로 파일을 다운로드할 때 시스템은 먼저 해당 파일을 `.zip` 패키지에 아카이브합니다. `.zip` 파일 이름에는 파일 속성과 파일 형식 및 SHA-256 값(사용 가능한 경우)이 포함됩니다. 실수로 압축을 해제하지 못하도록 `.zip` 파일을 비밀번호로 보호할 수 있습니다. 사용자 환경설정에서 기본 `.zip` 파일 비밀번호를 수정하거나 제거할 수 있습니다.

주의 Cisco에서는 악성코드를 다운로드하지 않을 것을 적극 권장합니다. 유해한 결과를 초래할 수 있습니다. 파일을 다운로드할 때는 주의하십시오. 악성코드가 포함되었을 수 있습니다. 파일을 다운로드하기 전에 다운로드 대상을 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

분석을 위해 수동으로 파일 제출

분석을 위해 파일을 수동으로 제출하면 시스템은 로컬 분석을 실행한 다음 동적 분석을 위해 클라우드에 이 파일을 제출합니다. 하지만 파일 정책에서 로컬 분석이 활성화되어 있지 않고 분석을 위해 수동으로 파일을 제출하는 경우, 파일은 동적 분석을 위해서만 전송됩니다.

실행 파일 외에 .swf, .jar 등과 같이 자동 제출에 적합하지 않은 파일 형식도 제출할 수 있습니다. 이렇게 하면 속성에 상관없이 광범위한 파일을 더욱 신속히 분석하고 인시던트의 정확한 원인을 파악할 수 있습니다.

참고 시스템은 AMP 클라우드에서 동적 분석 대상 파일 형식 목록(하루에 한 번)과 제출 가능한 최소 및 최대 파일 크기 업데이트를 확인합니다.

상황에 따라 분석을 위해 두 가지 방법으로 파일을 제출할 수 있습니다.

시작하기 전에

분석을 위해 캡처된 파일을 수동으로 제출하려면, 하나 이상의 파일 규칙을 파일을 저장하도록 구성해야 합니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 악성코드 보호 및 파일 정책 장을 참고하십시오.

프로시저

단계 **1** 분석을 위해 단일 파일을 제출하려면:

a) 다음 중 하나를 선택합니다.

- **Analysis(**분석**) > Files(**파일**) > File Events(**파일 이벤트**)**
- **Analysis(**분석**) > Files(**파일**) > Malware Events(**악성코드 이벤트**)**
- **Analysis(**분석**) > Files(**파일**) > Captured Files(**캡처된 파일**)**

b) <이벤트 유형 또는 파일>의 테이블 보기를 클릭합니다.

c) 테이블에서 파일을 마우스 오른쪽 버튼으로 클릭하고 **Analyze File(**파일 분석**)**을 선택합니다.

단계 **2** 캡처된 여러 파일을 제출하려면(한 번에 최대 25개):

a) **Analysis(**분석**) > Files(**파일**) > Captured Files(**캡처된 파일**)**를 선택합니다.

b) 분석할 각 파일 옆의 확인란을 선택합니다.

c) **Analyze(**분석**)**를 클릭합니다.

네트워크 파일 전파 흔적 분석

네트워크 파일 경로 분석 기능은 호스트가 네트워크에서 악성코드 파일을 포함한 파일을 전송한 방법을 매핑합니다. 경로 분석은 파일 전송 데이터, 파일의 속성, 파일 전송의 차단 여부 또는 파일의 격리 여부를 차트로 표시합니다. 어떤 호스트와 사용자가 악성코드를 전송했는지, 어떤 호스트가 위험한지를 확인하고 파일 전송 추세를 관찰할 수 있습니다.

AMP 클라우드가 속성을 할당한 모든 파일의 전송을 추적할 수 있습니다. 시스템은 악성코드 대응 및 AMP for Endpoints의 악성코드 탐지 및 차단 관련 정보를 사용하여 경로 분석을 작성할 수 있습니다.

최근 탐지된 악성코드 및 분석된 경로 분석

Network File Trajectory List(네트워크 파일 경로 분석 목록) 페이지에는 네트워크에서 가장 최근에 탐지된 악성코드는 물론 가장 최근에 경로 분석 맵을 살펴본 파일도 표시됩니다. 네트워크에서 각 파일을 가장 최근에 본 시간, 파일의 SHA-256 해시 값, 이름, 형식, 현재 파일 속성, 내용(아카이브 파일의 경우), 파일에 연결된 이벤트 수를 이러한 목록에서 확인할 수 있습니다.

이 페이지에는 SHA-256 해시 값이나 파일 이름을 기반으로, 또는 파일을 전송하거나 수신한 호스트의 IP 주소별로 파일을 찾을 수 있는 검색 상자도 포함되어 있습니다. 파일을 찾은 후 **File SHA256** 값을 클릭하여 자세한 경로 분석 맵을 볼 수 있습니다.

네트워크 파일 경로 분석 상세정보 보기

자세한 네트워크 파일 경로 분석을 살펴봄으로써 네트워크를 통해 파일을 추적할 수 있습니다. 파일의 세부 정보를 보려면 파일의 SHA 256 값을 검색하거나 Network File Trajectory(네트워크 파일 경로 분석) 목록에서 **File SHA 256** 링크를 클릭합니다.

네트워크 파일 경로 분석 세부 정보 페이지는 세 부분으로 구성됩니다.

- Summary Information(요약 정보) - 파일의 경로 분석 페이지에는 파일 식별 정보, 파일을 처음 본 시간과 네트워크에서 가장 최근에 본 시간, 파일을 본 사용자, 파일에 연결된 관련 이벤트 및 호스트 수, 파일의 현재 속성을 비롯하여 파일에 대한 요약 정보가 표시됩니다. 매니지드 디바이스가 파일을 저장한 경우, 이 섹션에서 로컬로 파일을 다운로드하거나 동적 분석을 위해 파일을 제출하거나 파일 목록에 파일을 추가할 수 있습니다.
- Trajectory Map(경로 분석 맵) - 파일의 경로 분석 맵은 네트워크에서 처음 탐지될 때부터 가장 최근까지 파일을 시각적으로 추적합니다. 맵에는 호스트가 파일을 전송하거나 수신한 시간, 파일 전송 빈도, 파일이 차단되거나 격리된 시간이 표시됩니다. 데이터 포인트 사이의 세로 줄은 호스트 간 파일 전송을 나타냅니다. 데이터 포인트를 연결하는 가로 줄은 시간에 따른 호스트의 파일 활동을 보여줍니다.

또한 파일의 파일 이벤트가 발생한 빈도와 시스템이 속성 또는 회귀적 속성을 할당한 시간도 표시됩니다. 맵에서 데이터 포인트를 선택하고 호스트가 해당 파일을 처음 전송한 인스턴스로 역추적하는 경로를 강조 표시할 수 있습니다. 이 경로는 또한 파일의 전송자 또는 수신자로서 호스트와 관련된 모든 시점과 교차하며, 관련된 사용자를 식별합니다.

- Related Events(관련 이벤트) - Events(이벤트) 테이블에는 맵의 각 데이터 포인트에 대한 이벤트 정보가 나열됩니다. 테이블과 맵을 사용하면 특정 파일 이벤트, 이 파일을 전송하거나 수신한 네트워크의 호스트와 사용자, 맵의 관련 이벤트, 선택한 값으로 제한된 테이블의 기타 관련 이벤트를 정확히 파악할 수 있습니다.

네트워크 파일 경로 분석 요약 정보

Network File Trajectory(네트워크 파일 경로 분석) 목록에 표시되는 파일의 세부 정보 페이지 상단에는 다음 요약 정보가 표시됩니다.

팁 관련 파일 이벤트를 보려면 필드 값 링크를 클릭하십시오. File Events(파일 이벤트) 기본 워크플로의 첫 번째 페이지가 새 창에서 열리고, 선택한 값도 포함된 모든 파일 이벤트가 표시됩니다.

표 ***8: Network File Trajectory Summary Information(***네트워크 파일 경로 분석 요약 정보***)*** 필드

이름	설명
아카이브 콘텐츠	검사된 아카이브 파일의 경우, 아카이브에 포함된 파일 수입니다.
현재 폐기	다음 악성코드 대응 파일 속성 중 하나: • `Malware(악성코드)`는 AMP 클라우드가 파일을 악성코드로 분류했거나 로컬 악성코드 분석에서 악성코드로 식별했거나 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다. • `Clean(정상)`은 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • `Unknown(알 수 없음)`은 시스템이 AMP 클라우드를 쿼리했지만 파일에 속성이 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드에서 파일을 분류하지 않았습니다. • `Custom Detection(사용자 지정 탐지)`은 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • `Unavailable(사용할 수 없음)`은 시스템이 AMP 클라우드를 쿼리할 수 없음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다. • `N/A`는 Detect Files(파일 탐지) 또는 Block Files(파일 차단) 규칙이 파일을 처리했고 Secure Firewall Management Center이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.
탐지 이름	로컬 악성코드 분석에서 탐지된 악성코드의 이름입니다.

이름	설명
이벤트 수	네트워크에 표시되는, 파일에 연결된 이벤트의 수, 그리고 탐지된 이벤트가 250개가 넘는 경우 맵에 표시되는 이벤트의 수.
파일 카테고리	파일 형식의 일반 카테고리(예: `Office 문서` 또는 `시스템 파일`).
파일 이름	네트워크에 표시되는, 이벤트와 연결된 파일의 이름. 여러 파일 이름이 하나의 SHA-256 해시 값에 연결되어 있으면 가장 최근에 탐지된 파일 이름이 나열됩니다. `more(더 보기)`를 클릭하여 이 항목을 확장하면 나머지 파일 이름을 볼 수 있습니다.
파일 SHA256	파일의 SHA-256 해시 값 해시는 기본적으로 압축된 형식으로 표시됩니다. 전체 해시 값을 보려면 포인터를 값 위로 이동합니다. 파일 이름 하나에 여러 SHA-256 해시 값이 연결되어 있는 경우 모든 해시 값을 보려면 포인터를 링크 위로 이동합니다.
파일 크기(KB)	킬로바이트 단위의 파일 크기.
파일 유형	파일의 파일 형식(예: `HTML` 또는 `MSEXE`).
처음 표시	악성코드 대응 또는 AMP for Endpoints가 처음으로 파일을 탐지한 시간, 파일을 처음 업로드한 호스트의 IP 주소 및 관련 사용자의 식별 정보.
최종 확인	악성코드 대응 또는 AMP for Endpoints가 가장 최근에 파일을 탐지한 시간, 파일을 마지막으로 다운로드한 호스트의 IP 주소 및 관련 사용자의 식별 정보.
상위 애플리케이션	AMP for Endpoints의 탐지가 발생했을 때 악성코드 파일에 액세스한 클라이언트 애플리케이션. 이러한 애플리케이션은 네트워크 검색 또는 애플리케이션 제어에 연결되지 않습니다.
표시	파일을 전송했거나 수신한 호스트의 수. 한 호스트가 서로 다른 시간에 파일을 업로드 및 다운로드할 수 있으므로 총 호스트 수는 `Seen On Breakdown` 필드에 지정된 총 전송자 수와 총 수신자 수의 합과 일치하지 않을 수 있습니다.
상세 분석에 표시	파일을 보낸 호스트의 수와 파일을 받은 호스트의 수.
위협 이름	AMP for Endpoints가 탐지한 악성코드에 연결된 위협의 이름.
위협 점수	파일의 위협 점수.

네트워크 파일 경로 분석 맵 및 관련 이벤트 목록

파일 궤적 맵의 y 축은 파일과 상호 작용 한 모든 호스트 IP 주소의 목록을 포함 합니다. IP 주소는 시스템이 해당 호스트에서 파일을 처음 탐지한 시점을 기준으로 내림차순으로 나열됩니다. 각 행에는 단일 파일 이벤트, 파일 전송 또는 회귀적 이벤트 등 해당 IP 주소에 연결된 모든 이벤트가 포함됩니다. x축에는 시스템이 각 이벤트를 탐지한 날짜와 시간이 포함됩니다. 타임스탬프는 시간순으로 나열됩니다. 1분 내에 여러 이벤트가 발생한 경우 모두가 동일한 열에 나열됩니다. 맵을 가로와 세로로 스크롤하면 추가 이벤트 및 IP 주소를 볼 수 있습니다.

맵에는 파일 SHA-256 해시에 연결된 최대 250개의 이벤트가 표시됩니다. 이벤트가 250개가 넘으면 처음 10개가 표시되고 추가 이벤트는 **Arrow(**화살표**)**와 함께 생략됩니다. 그런 다음 나머지 이벤트 240개가 표시됩니다.

File Events(파일 이벤트) 기본 워크플로의 첫 번째 페이지는 파일 형식을 기반으로 제한된 모든 추가 이벤트와 함께 새 창에 나타납니다. AMP for Endpoints에 의해 생성된 악성코드 이벤트가 표시되지 않으면 Malware Events(악성코드 이벤트) 테이블로 전환하여 이러한 이벤트를 표시해야 합니다.

각 데이터 포인트는 맵 아래의 범례에 설명된 대로 이벤트 및 파일 속성을 나타냅니다. 예를 들어 Malware Block 이벤트 아이콘은 Malicious Disposition 아이콘과 Block Event 아이콘을 결합합니다.

AMP for Endpoints에 의해 생성된 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")에는 하나의 아이콘이 포함됩니다. 회귀적이벤트는 파일이 탐지되는 각 호스트에 대한 열에 아이콘을 표시합니다. 파일 전송 이벤트에는 항상 두 개의 아이콘, 즉 파일 보내기 아이콘과 파일 받기 아이콘이 포함되며, 이 둘은 세로 선으로 연결됩니다. 화살표는 전송자에서 수신자로의 파일 전송 방향을 나타냅니다.

네트워크에서 파일의 진행 상황을 추적하려면 원하는 데이터 포인트를 클릭하여 선택한 데이터 포인트와 관련된 모든 데이터 포인트를 포함하는 경로를 강조 표시할 수 있습니다. 여기에는 다음 이벤트 유형에 연결된 데이터 포인트가 포함됩니다.

- 연결된 IP 주소 가 전송자 또는 수신자인 파일 전송
- 연결된 IP 주소와 관련하여 AMP for Endpoints가 생성한 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")
- 또 다른 IP 주소가 관련된 경우, 연결된 해당 IP 주소가 전송자 또는 수신자인 모든 파일 전송
- 다른 IP 주소가 관련된 경우, 다른 IP 주소와 관련하여 AMP for Endpoints가 생성한 안성코드 이벤트("엔드포인트 기반 악성코드 이벤트")

강조 표시된 데이터 포인트와 연결된 모든 IP 주소 및 타임스탬프도 강조 표시됩니다. Events(이벤트) 테이블의 해당 이벤트도 강조 표시됩니다. 경로에 생략된 이벤트가 포함된 경우 경로 자체는 점선으로 강조 표시됩니다. 생략된 이벤트는 경로와 교차할 수도 있지만 맵에는 표시되지 않습니다.

네트워크 파일 경로 분석 사용

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

팁 조직이 Secure Endpoint를 구축한 경우, 해당 제품에도 네트워크 파일 경로 분석 기능이 있습니다. management center에서 Secure Endpoint으로 피벗하려면 Secure Endpoint 콘솔의 이벤트 데이터 작업, 35 페이지의 내용을 참고하십시오. Secure Endpoint의 파일 경로 분석 기능에 대한 자세한 내용은 Secure Endpoint 설명서를 참고하십시오.

시작하기 전에

악성코드 대응 를 사용하는 경우 악성코드 방어 라이선스가 필요합니다.

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Files(**파일**)** > **Network File Trajectory(**네트워크 파일 경로**)**을(를) 선택합니다.

팁 Context Explorer, 대시보드 또는 파일 정보가 포함된 이벤트 보기에서도 파일의 분석 경로에 액세스할 수 있습니다.

단계 **2** 목록에서 **File SHA 256** 링크를 클릭합니다.

단계 **3** 원하는 경우, 전체 SHA-256 해시 값, 호스트 IP 주소 또는 추적할 파일의 파일 이름을 검색 필드에 입력하고 Enter 키를 누릅니다.

팁 일치하는 결과가 하나뿐이면 해당 파일의 Network File Trajectory(네트워크 파일 분석 경로) 페이지가 나타납니다.

단계 **4** Summary Information(요약 정보) 섹션에서 다음을 수행할 수 있습니다.

- 파일을 파일 목록에 추가 - 정상 목록 또는 맞춤형 탐지 목록에 파일을 추가 또는 제거하려면 **Edit(**수정**)** ( )을 클릭합니다.
- 파일 다운로드 - 파일을 다운로드하려면 **Download(**다운로드**)** ( )을 클릭하고 메시지가 표시되면 파일을 다운로드하려 한다고 확인합니다. 파일을 다운로드할 수 없는 경우에는 이 다운로드 파일이 흐리게 표시됩니다.
- 보고 - 동적 분석 요약 보고서를 보려면 위협 점수를 클릭합니다.
- 동적 분석을 위해 제출 - 동적 분석을 위해 파일을 제출하려면 **AMP** 클라우드를 클릭합니다. 파일을 제출할 수 없거나 AMP 클라우드에 연결할 수 없는 경우 이 AMP 클라우드가 흐리게 표시됩니다.
- 아카이브 내용 보기 - 아카이브 파일의 내용에 대한 정보를 보려면 **View(**보기**)** ( )을 클릭합니다.
- 파일 구성 보기 - 파일의 구성을 보려면 파일 목록을 클릭합니다. 시스템이 파일 구성 보고서를 생성하지 않은 경우, 이 파일 목록이 흐리게 표시됩니다.
- 위협 점수가 동일한 캡처된 파일 보기 - 해당 위협 점수의 모든 캡처 파일을 보려면 위협 점수 링크를 클릭합니다.

참고 Cisco에서는 악성코드를 다운로드하지 않을 것을 적극 권장합니다. 유해한 결과를 초래할 수 있습니다. 파일을 다운로드할 때는 주의하십시오. 악성코드가 포함되었을 수 있습니다. 파일을 다운로드하기 전에 다운로드 대상을 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

단계 **5** 경로 분석 맵에서 다음을 수행할 수 있습니다.

- 첫 번째 인스턴스 찾기 - IP 주소와 관련하여 파일 이벤트가 처음 발생한 때를 찾으려면 IP 주소를 클릭합니다. 그러면 해당 데이터 포인트 경로는 물론 첫 번째 파일 이벤트와 관련된 중간 파

일 이벤트 및 IP 주소도 강조 표시됩니다. Events(이벤트) 테이블의 해당 이벤트도 강조 표시됩니다. 해당 데이터 포인트가 현재 보이지 않는 경우, 맵이 해당 데이터 포인트로 스크롤됩니다.

- 추적 - 데이터 포인트를 클릭하여 선택한 데이터 포인트와 관련된 모든 데이터 포인트를 포함하는 경로를 강조 표시하여 네트워크에서 파일의 진행 상황을 추적할 수 있습니다.
- 숨겨진 이벤트 보기 - File Summary(파일 요약) 이벤트 보기에 표시되지 않은 모든 이벤트를 보려면 화살표를 클릭합니다.
- 일치하는 파일 이벤트 보기 - 일치하는 파일 이벤트 위에 마우스 포인터를 올려놓으면 해당 이벤트의 요약 정보를 볼 수 있습니다. 이벤트 요약 정보 링크를 클릭할 경우, File Events(파일 이벤트) 기본 워크플로의 첫 번째 페이지가 파일 형식을 기반으로 제한된 모든 추가 이벤트와 함께 새 창에 나타납니다. File Summary(파일 요약) 이벤트 보기가 새 창에서 열리며, 클릭한 기준에 일치하는 모든 파일 이벤트가 표시됩니다.

단계 **6** Events(이벤트) 테이블에서 다음을 수행할 수 있습니다.

- 강조 표시 - 맵에서 데이터 포인트를 강조 표시하려면 테이블 행을 선택합니다. 선택한 파일 이벤트가 현재 보이지 않는 경우 해당 이벤트를 표시하도록 맵이 스크롤됩니다.
- 정렬 - 오름차순 또는 내림차순으로 이벤트를 정렬하려면 열 머리글을 클릭합니다.

Secure Endpoint 콘솔의 이벤트 데이터 작업

조직이 Secure Endpoint를 구축한 경우, Secure Endpoint 콘솔에서 악성코드 이벤트 데이터를 볼 수 있으며, 해당 애플리케이션의 전역 네트워크 파일 분석 경로 도구를 사용하거나.

팁 Secure Endpoint 및 콘솔 사용 방법은 콘솔의 온라인 도움말 또는 https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html에서 사용 가능한 기타 설명서를 참조하십시오.

Secure Firewall Management Center에서 Secure Endpoint 콘솔에 액세스하려면 다음 중 하나를 수행하십시오.

시작하기 전에

- Secure Endpoint에 대한 연결이 구성되어야 하며(Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Firepower* 및 *Secure Endpoint* 통합 참조) Secure Firewall Management Center가 AMP 클라우드에 연결할 수 있어야 합니다.
- Secure Endpoint 자격 증명이 필요합니다.
- 이 작업을 수행하려면 관리자 사용자여야 합니다.

- management center의 악성코드 이벤트에서 피벗하려는 경우, Secure Endpoint 상황별 크로스 실행 옵션이 적절히 활성화되어 있어야 합니다. 웹 기반 리소스를 사용한 이벤트 조사의 항목을 참조하십시오.

프로시저

단계 **1** 방법 1:

a) **Integration(통합)** > **AMP** > **AMP Management(AMP 관리)**을(를) 선택합니다.
b) 테이블에서 클라우드 이름을 클릭합니다.

단계 **2** 방법 2:

a) **Analysis(분석)** > **Files(파일)**아래 테이블에서 악성코드 이벤트로 이동합니다.
b) 파일 SHA를 마우스 오른쪽 버튼으로 클릭하고 Secure Endpoint 옵션을 선택합니다.

파일, 악성코드 이벤트 및 네트워크 파일 경로 분석 기록

기능	최소 **Management Center**	최소 **Threat Defense**	세부 사항
파일 및 악성코드 이벤트의 MITRE 정보.	7.4	7.4	이제 시스템은 로컬 악성코드 분석에서 얻은 MITRE 정보를 파일 및 악성코드 이벤트에 포함합니다. MITRE 정보를 클래식 보기 및 통합 이벤트 보기 모두에서 볼 수 있습니다. MITRE 열은 두 이벤트 보기 모두에서 기본적으로 숨겨져 있습니다.
동적 분석을 위해 파일 사전 분류가 개선되었습니다.	6.7	Any(모든)	추가 평가를 통해 동적 분석을 위해 불필요한 파일 전송이 방지됩니다. 이 평가를 기반으로 클라우드로 전송되지 않은 파일에 대한 새로운 동적 분석이 **Rejected for Analysis(분석을 위해 거부)** 상태가 됩니다. 신규/수정된 화면: **Analysis(분석)** > **Captured Files(캡처된 파일)** > **Table View of Captured Files(캡처된 파일 테이블 보기)**
시스템 로그의 연결 이벤트 통합 식별자.	6.4.0.4	Any(모든)	다음 시스템 로그 필드는 연결 이벤트를 전체적으로 고유하게 식별하며, 파일 및 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)의 경우에는 시스템 로그에 표시됩니다.
시스템 로그를 통해 파일 및 악성코드 이벤트를 전송합니다.	6.4	Any(모든)	이 장의 필드 설명은 시스템 로그 메시지에 포함된 필드를 지정합니다. 구성 정보는 파일 및 악성코드 이벤트에 대한 시스템 로그 설정 위치의 내용을 참조하십시오.