암호화된 가시성 엔진

EVE(암호화된 가시성 엔진)는 TLS 암호화를 사용하는 클라이언트 애플리케이션 및 프로세스를 식별하는 데 사용됩니다. 이를 통해 가시성이 향상되며 관리자가 작업을 수행하고 환경 내에서 정책을 시행할 수 있습니다. EVE 기술은 악성코드를 식별하고 중지하는 데도 사용할 수 있습니다.

- 암호화된 가시성 엔진, 1 페이지

암호화된 가시성 엔진

EVE(암호화된 가시성 엔진)는 암호를 해독하지 않고도 암호화된 세션에 대한 더 많은 가시성을 제공하는 데 사용됩니다. 암호화된 세션에 대한 이러한 인사이트는 Cisco의 VDB(취약성 데이터베이스)에 패키지된 Cisco의 오픈 소스 라이브러리에서 가져옵니다. 라이브러리는 암호화된 수신 세션을 핑거프린트하고 분석하여 알려진 핑거프린트 집합과 일치시킵니다. 이 알려진 핑거프린트 데이터베이스는 Cisco VDB에서도 사용할 수 있습니다.

액세스 제어 정책의 **Advanced(**고급**)** 탭에 있는 **Encrypted Visibility Engine(EVE)(EVE(**암호화된 가시성 엔진**)** 토글 버튼을 사용하여 EVE를 활성화하거나 비활성화합니다. management center 7.1에서 암호화된 가시성 엔진은 암호화된 트래픽에 대한 더 많은 가시성을 제공하는 데만 사용됩니다. 해당 트래픽에 대한 작업을 시행하지 않습니다.

management center 7.2에서 EVE(암호화된 가시성 엔진)에는 다음과 같은 향상된 기능이 있습니다.

- management center 7.2에서 EVE를 사용하려면 디바이스에 유효한 IPS 라이선스가 있어야 합니다. IPS 라이선스가 없으면 정책에 경고가 표시되고 구축이 허용되지 않습니다.
- EVE에서 파생된 정보를 사용하여 트래픽에 대한 액세스 제어 정책 작업을 수행할 수 있습니다.
- Cisco Secure Firewall 7.2에 포함된 VDB에는 높은 신뢰도 값으로 EVE에서 탐지한 일부 프로세스에 애플리케이션을 할당할 수 있는 기능이 있습니다. 또는 맞춤형 애플리케이션 탐지기를 생성하여 다음을 수행할 수 있습니다.
  - EVE 탐지 프로세스를 새로운 사용자 정의 애플리케이션에 매핑합니다.
  - EVE 탐지 프로세스에 애플리케이션을 할당하는 데 사용되는 프로세스 신뢰도의 기본 제공 값을 재정의합니다.

암호화된 가시성 엔진

Cisco Secure Firewall Device Management 구성 가이드의 애플리케이션 탐지 장에 나와 있는 사용자 지정 애플리케이션 탐지기 구성 및 **EVE** 프로세스 할당 지정 섹션을 참조하십시오.

- EVE는 암호화된 트래픽에서 클라이언트 Hello 패킷을 생성한 클라이언트의 운영 체제 유형 및 버전을 탐지할 수 있습니다.
- EVE는 QUIC(빠른 UDP 인터넷 연결) 트래픽의 핑거프린트 및 분석도 지원합니다. Client Hello 패킷의 서버 이름이 **Connection Events(**연결 이벤트**)** 페이지의 URL 필드에 표시됩니다.

참고 암호화된 가시성 엔진 기능은 Snort 3를 실행하는 management center 매니지드 디바이스에서만 지원됩니다. 이 기능은 Snort 2 디바이스, device manager 매니지드 디바이스 또는 CDO에서 지원되지 않습니다.

암호화된 가시성 엔진 토글 버튼이 활성화되고 액세스 제어 정책이 구축되면 시스템을 통해 라이브 트래픽 전송을 시작할 수 있습니다. **Connection Events(**연결 이벤트**)** 페이지에서 로깅된 연결 이벤트를 볼 수 있습니다. 연결 이벤트에 액세스하려면 management center에서 **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**로 이동하여 **Table View of Connection Events(**연결 이벤트의 테이블 보기**)** 탭을 클릭합니다. **Analysis(**분석 **)** 메뉴 아래에 있는 **Unified Events(**통합 이벤트**)** 뷰어에서 연결 이벤트 필드를 볼 수도 있습니다. 암호화 가시성 엔진은 연결을 시작한 클라이언트 프로세스, 클라이언트의 OS 및 프로세스에 악성코드가 포함되어 있는지 여부를 식별할 수 있습니다.

Connection Events(연결 이벤트**)** 페이지에서 암호화된 가시성 엔진에 대해 다음 열이 추가됩니다. 언급된 열을 명시적으로 활성화해야 합니다.

- 암호화된 가시성 프로세스 이름
- 암호화된 가시성 프로세스 신뢰도 점수
- 암호화된 가시성 위협 신뢰도
- 암호화된 가시성 위협 신뢰도 점수
- 탐지 유형

이러한 필드에 대한 자세한 내용은 Cisco Firepower Management Center 관리 가이드의 연결 및 보안 인텔리전스 이벤트 필드 섹션을 참조하십시오.

참고 **Connection Events(**연결 이벤트**)** 페이지에서 프로세스에 애플리케이션이 할당된 경우 **Detection Type(**탐지 유형**)** 열에 EVE에서 클라이언트 애플리케이션을 식별했음을 나타내는 암호화된 가시성 엔진이 표시됩니다. 프로세스 이름에 애플리케이션을 할당하지 않은 경우 **Detection Type(**탐지 유형**)** 열에 클라이언트 애플리케이션을 식별한 엔진이 AppID임을 나타내는 **AppID**가 표시됩니다.

두 개의 대시보드에서 분석 정보를 볼 수 있습니다. **Overview(**개요**)** > **Dashboards(**대시보드**)** 아래에서 **Dashboard(**대시보드**)**를 클릭합니다. **Summary Dashboard(**요약 대시보드**)** 창에서 스위치 대시보

드 링크를 클릭하고 드롭다운 상자에서 **Application Statistics(**애플리케이션 통계**)**를 선택합니다. 다음 두 개의 대시보드를 보려면 **Encrypted Visibility Engine(**암호화 가시성 엔진**)** 탭을 선택합니다.

- **Top Encrypted Visibility Engine Discovered Processes(**상위 **TLS** 핑거프린트 발견 프로세스**)** - 네트워크에서 사용 중인 상위 TLS 프로세스 이름 및 연결 수를 표시합니다. 표에서 프로세스 이름을 클릭하면 프로세스 이름별로 필터링된 **Connection Events(**연결 이벤트**)** 페이지의 필터링된 보기를 볼 수 있습니다.
- **Connections by Encrypted Visibility Engine(**암호화된 가시성 엔진에 의한 연결**)** — 신뢰 수준(Very High(매우 높음), Very Low(매우 낮음) 등)별로 연결을 표시합니다. 표에서 위협 신뢰도 레벨을 클릭하여 신뢰도 레벨별로 필터링된 **Connection Events(**연결 이벤트**)** 페이지의 필터링된 보기를 볼 수 있습니다.

management center 7.2에서 EVE는 SSL 세션의 운영 체제 유형 및 버전을 탐지할 수 있습니다. 애플리케이션, 패키지 관리 소프트웨어 등을 실행하는 등 운영 체제를 정상적으로 사용하면 OS 탐지가 트리거될 수 있습니다. 클라이언트 OS 탐지를 보려면 EVE 토글을 활성화하는 것 외에도 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**에서 **Hosts(**호스트**)**를 활성화해야 합니다. 호스트 IP 주소에서 가능한 운영 체제 목록을 보려면 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**을 클릭한 다음 필요한 호스트를 선택합니다.

management center 7.3.0부터 암호화된 가시성 엔진 탐지에 대한 호스트의 IoC(보안 침해 지표) 이벤트를 사용하면 EVE에서 보고한 대로 악성코드 신뢰도 수준이 매우 높은 연결 이벤트를 확인할 수 있습니다. IoC 이벤트는 악성 클라이언트를 사용하는 호스트에서 생성된 암호화된 세션에 대해 트리거됩니다. 악성 호스트의 IP 주소, MAC 주소, OS 정보 및 의심스러운 활동의 타임스탬프와 같은 정보를 볼 수 있습니다.

연결 이벤트에서 암호화된 가시성 위협 신뢰도 점수가 'Very High(매우 높음)'인 세션은 IoC 이벤트를 분류합니다. **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**에서 **Hosts(**호스트**)**를 활성화해야 합니다. management center의 다음에서 IoC 이벤트 존재 여부를 확인할 수 있습니다.

- **Analysis(**분석**)** > **Indications of Compromise(**보안 침해 지표**)**
- **Analysis(**분석**)** > **Network Map(**네트워크 맵**)** > **Indications of Compromise(**보안 침해 지표**)** > 선택해야 하는 호스트를 선택합니다.

  다음에서 IoC를 생성한 세션의 프로세스 정보를 볼 수 있습니다.

  Analysis(분석**)** > **Connection Events(**연결 이벤트**)** > **Table View of Connection Events(**연결 이벤트의 테이블 보기**)** > **IoC** 열. Encrypted Visbility(암호화된 가시성) 필드 및 IoC 필드를 수동으로 선택해야 합니다.

Snort는 EVE를 기반으로 QUIC 세션에서 클라이언트 애플리케이션을 식별할 수 있습니다. QUIC 핑거프린트는 다음을 수행할 수 있습니다.

- 암호 해독을 활성화하지 않고 QUIC를 통해 애플리케이션을 탐지합니다.
- 암호 해독을 활성화하지 않고 악성코드를 식별합니다.
- 서비스 애플리케이션을 탐지합니다. QUIC 프로토콜을 통해 탐지된 서비스를 기반으로 액세스 제어 규칙을 할당할 수 있습니다.

EVE(암호화된 가시성 엔진**)** 토글을 활성화하면 그 아래에 다음 토글이 표시됩니다.

- **Use EVE for Application Detection(**애플리케이션 탐지에 **EVE** 사용**)** - 이 토글은 기본적으로 활성화되어 있으며, 이는 EVE가 프로세스에 클라이언트 애플리케이션을 할당할 수 있음을 의미합니다.

  연결 이벤트 또는 통합 이벤트의 **Encrypted Visibility Fingerprint(**암호화된 가시성 핑거프린트**)** 열 헤더에 EVE의 핑거프린트 정보가 추가됩니다. 수집된 EVE 데이터를 추가로 분석하려면 핑거프린트 정보를 마우스 오른쪽 버튼으로 클릭하여 드롭다운 메뉴를 엽니다. 메뉴에서 **View Encrypted Visibility Engine Process Analysis(**암호화된 가시성 엔진 프로세스 분석 보기**)**를 클릭하여 appid.cisco.com으로 이동한 후 핑거프린트, VDB 버전 등의 세부 정보를 확인합니다. 핑거프린트 문자열이 동일한 여러 행과 이러한 행과 관련된 잠재적 프로세스 이름 및 발생률이 표시됩니다. 발생률은 데이터 수집 시스템의 특정 핑거프린트와 관련된 프로세스의 빈도를 나타냅니다. 프로세스 이름을 선택하고 **Submit Request(**요청 제출**)**를 클릭하여 EVE의 프로세스 탐지의 불일치에 대한 피드백을 제공할 수 있습니다. 예를 들어 탐지된 프로세스 이름이 전송되는 트래픽과 일치하지 않거나 특정 핑거프린트에 대해 프로세스 이름이 전혀 탐지되지 않는 경우 요청을 제출할 수 있습니다.

  토글을 비활성화하면 AppID로 식별된 클라이언트가 프로세스에 할당되고 EVE 프로세스 및 점수를 볼 수 있지만 EVE 탐지 프로세스가 애플리케이션에 매핑되지 않으며 작업이 수행되지 않습니다. **Connection Events(**연결 이벤트**)** 또는 **Unified Events(**통합 이벤트**)**에서 이벤트의 상세정보를 볼 수 있습니다. 연결 이벤트(애플리케이션 할당 포함 및 제외)의 차이를 확인하려면 **Client Application(**클라이언트 애플리케이션**)** 열 헤더를 참조하십시오. 토글이 비활성화되면 연결 이벤트 또는 통합 이벤트의 **Encrypted Visibility Fingerprint(**암호화된 가시성 핑거프린트**)** 필드가 비어 있습니다.

- **Block Traffic Based on EVE Score(EVE** 점수 기준으로 트래픽 차단**)** - 이 토글을 활성화하면 EVE의 위협 신뢰도 점수를 기준으로 트래픽을 차단할 수 있습니다. 잠재적인 위협인 모든 수신 트래픽은 기본적으로 차단됩니다. 기본 차단 임계값은 80%이며, 이는 다음을 의미합니다.

  - EVE가 트래픽을 80% 이상의 신뢰도로 악성코드로 탐지하면 트래픽이 차단됩니다.
  - EVE가 트래픽을 80% 미만의 신뢰도로 악성코드로 탐지하는 경우, EVE는 작업을 수행하지 않습니다.

  EVE가 트래픽을 차단한 경우 **Connection Events(**연결 이벤트**)**에서 **Reason(**이유**)** 열 헤더에 **Encrypted Visiblity Block(**암호화된 가시성 차단**)**이 표시됩니다.

  - **Advanced Settings(**고급 설정**) - Block Traffic Based on EVE Score(EVE** 점수 기반 트래픽 차단**)**에서 **Advanced Mode(**고급 모드**)** 토글을 활성화하여 EVE가 트래픽을 차단할 임계값을 맞춤화합니다. 슬라이더를 사용하여 임계값을 차단할 백분율을 조정할 수 있습니다.

⚠ 주의 최적의 성능을 위해 임계값을 50% 미만으로 설정하는 것이 좋습니다.

Client Hello 패킷이 프래그먼트화될 경우 EVE에서 리어셈블하여 클라이언트 정보(클라이언트 프로세스, 클라이언트 OS, 악성코드 신뢰도)를 탐지할 수 있습니다.