Cisco Secure Cloud Analytics 포털 사용

이 장에서는 Cisco Secure Cloud Analytics 포털에 대한 정보를 제공합니다.

Cisco Secure Cloud Analytics 포털 프로비저닝

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Logging Analytics and Detection(로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매한 경우, SEC(Secure Event Connector)를 구축하고 구성한 후 Secure Cloud Analytics 포털을 Security Cloud Control 포털에 연결해야 Secure Cloud Analytics 알림을 볼 수 있습니다. 기존 Secure Cloud Analytics 포털이 있는 경우 라이선스를 구매할 때 Secure Cloud Analytics 포털 이름을 제공하고 Security Cloud Control 포털에 즉시 연결할 수 있습니다.

그렇지 않은 경우 Security Cloud Control UI에서 새 Secure Cloud Analytics 포털을 요청할 수 있습니다. Secure Cloud Analytics 알림에 처음 액세스하면 시스템은 Secure Cloud Analytics 포털을 요청할 수 있는 페이지로 이동합니다. 이 포털을 요청하는 사용자에게는 포털에서 관리자 권한이 부여됩니다.

Procedure

단계 **1** 왼쪽 창에서 분석 > **Secure Cloud Analytics**를 클릭하여 Secure Cloud Analytics UI를 새 창에서 엽니다.

단계 **2** **Start Free Trial(**무료 평가판 시작**)**을 클릭하여 Secure Cloud Analytics 포털을 프로비저닝하고 Security Cloud Control 포털과 연결합니다.

Note

포털을 요청한 후 프로비저닝에 몇 시간이 걸릴 수 있습니다.

다음 단계로 이동하기 전에 포털이 프로비저닝되었는지 확인합니다.

1. 왼쪽 창에서 분석 > **Secure Cloud Analytics**를 클릭하여 Secure Cloud Analytics UI를 새 창에서 엽니다.
2. 다음 옵션을 이용할 수 있습니다.
   - Secure Cloud Analytics 포털을 요청했는데 시스템에서 포털을 프로비저닝하는 중이라고 표시되면 기다렸다가 나중에 알림에 액세스해 보십시오.
   - Secure Cloud Analytics 포털이 프로비저닝된 경우 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)**를 입력하고 **Sign in(**로그인**)**을 클릭합니다.

Note 관리자 사용자는 다른 사용자를 초대하여 Secure Cloud Analytis 포털 내에서 계정을 생성할 수 있습니다. 자세한 내용은 Security Cloud Control에서 Cisco Secure Cloud Analytics 알림 보기, on page 4를 참조하십시오.

What to do next

- **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 라이선스를 구매한 경우 구성이 완료된 것입니다. Secure Cloud Analytics 포털 UI에서 Security Cloud Control 통합 또는 센서 상태를 보려면 Secure Cloud Analytics에서 센서 상태 및 Security Cloud Control통합 상태 검토, on page 2에서 자세한 내용을 확인하십시오. Secure Cloud Analytics 포털에서 알림으로 작업하려는 경우 자세한 내용은 Security Cloud Control에서 Cisco Secure Cloud Analytics 알림 보기, on page 4 및 Firepower 이벤트 기반 알림 작업을 참조하십시오.
- **Total Network Analytics and Monitoring** 라이선스를 구매한 경우 내부 네트워크에 하나 이상의 Secure Cloud Analytics 센서를 구축하여 네트워크 플로우 데이터를 클라우드에 전달합니다. 클라우드 기반 네트워크 플로우 데이터를 모니터링하려면 플로우 데이터를 Secure Cloud Analytics로 전달하도록 클라우드 기반 구축을 구성합니다. 자세한 내용은 전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축, on page 3를 참조하십시오.

Secure Cloud Analytics에서 센서 상태 및 Security Cloud Control통합 상태 검토

센서 상태

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytis 웹 UI의 Sensor List(센서 목록) 페이지에서 Security Cloud Control 통합 상태 및 구성된 센서를 볼 수 있습니다. Security Cloud Control 통합은 읽기 전용 연결 이벤트 센서입니다. Stelathwatch Cloud는 기본 메뉴에서 센서의 전반적인 상태를 제공합니다.

- 녹색 클라우드 아이콘() - 모든 센서와 연결 설정됨, 구성된 경우 Security Cloud Control
- 노란색 클라우드 아이콘() - 일부 센서 또는 Security Cloud Control(구성된 경우)와의 연결이 설정되었으며 하나 이상의 센서가 제대로 구성되지 않음
- 빨간색 클라우드 아이콘() - 구성된 모든 센서 및 Security Cloud Control(구성된 경우)와의 연결 끊김

센서 또는 Security Cloud Control 통합에서 녹색 아이콘은 설정된 연결을 나타내고, 빨간색 아이콘은 연결 끊김을 나타냅니다.

프로시저

단계 **1** 1. Secure Cloud Analytis 포털 UI에서 **Settings(**설정**)(** **) > Sensors(**센서**)**를 선택합니다.

단계 **2** **Sensor List(**센서 목록**)**를 선택합니다.

전체 네트워크 분석 및 보고를 위한 **Cisco Secure Cloud Analytics** 센서 구축

Secure Cloud Analytics 센서 개요 및 구축

필수 라이선스: 전체 네트워크 분석 및 모니터링

Total Network Analytics and Monitoring(전체 네트워크 분석 및 모니터링**)** 라이선스를 취득한 경우 Secure Cloud Analytics 포털을 프로비저닝한 후 다음을 수행할 수 있습니다.

- 분석을 위해 네트워크 플로우 데이터를 클라우드에 전달하기 위해 온프레미스 네트워크 내에 Secure Cloud Analytics 센서를 구축하고 구성합니다.
- 분석을 위해 네트워크 플로우 로그 데이터를 Secure Cloud Analytics에 전달하도록 클라우드 기반 구축을 구성합니다.

네트워크 경계의 방화벽은 내부 네트워크와 외부 네트워크 간의 트래픽에 대한 정보를 수집하는 반면, Secure Cloud Analytics 센서는 내부 네트워크 내의 트래픽에 대한 정보를 수집합니다.

Note FDM 관리Secure Firewall Threat Defense 디바이스가 NetFlow 데이터를 전달하도록 구성할 수 있습니다. 센서를 구축할 때, 이벤트 정보를 Security Cloud Control로 전달하도록 구성한 FDM 관리Secure Firewall Threat Defense 디바이스에서 NetFlow 데이터를 전달하도록 센서를 구성하지 마십시오.

센서 구축 지침 및 권장 사항은 Secure Cloud Analytics 센서 설치 가이드를 참조하십시오.

클라우드 기반 구축 구성 지침 및 권장 사항은 Secure Cloud Analytics 퍼블릭 클라우드 모니터링 가이드를 참조하십시오.

Note Secure Cloud Analytics 포털 UI의 지침을 검토하여 센서 및 클라우드 기반 구축을 구성할 수도 있습니다.

Secure Cloud Analytics에 대한 자세한 내용은 Secure Cloud Analytics 무료 평가판 가이드를 참조하십시오.

다음 단계

- Security Cloud Control에서 Cisco Secure Cloud Analytics 알림 보기, on page 4를 계속 진행합니다.

Security Cloud Control에서 Cisco Secure Cloud Analytics 알림 보기

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Events logging(이벤트 로깅) 페이지에서 방화벽 이벤트를 검토할 수 있지만 Security Cloud Control 포털 UI에서 Cisco Secure Cloud Analytics 알림을 검토할 수는 없습니다. Security Analytics(보안 분석) 메뉴 옵션을 사용하여 Security Cloud Control에서 Secure Cloud Analytics 포털로 교차 실행하고, 방화벽 이벤트 데이터(전체 네트워크 분석 및 모니터링을 활성화한 경우 네트워크 플로우 데이터)에서 생성된 알림을 볼 수 있습니다. Security Analytics(보안 분석) 메뉴 옵션은 하나 이상의 열려 있는 워크플로우 상태의 Secure Cloud Analytics 알림 수와 함께 배지를 표시합니다.

Security Analytics and Logging(보안 분석 및 로깅) 라이선스를 사용하여 Secure Cloud Analytics 알림을 생성하고 새 Secure Cloud Analytics 포털을 프로비저닝한 경우, Security Cloud Control에 로그인한 다음 Cisco Secure Cloud Sign-On을 사용하여 Secure Cloud Analytics를 교차 실행합니다. URL을 통해 Secure Cloud Analytics 포털에 직접 액세스할 수도 있습니다.

자세한 내용은 Cisco Security Cloud Sign On을 참조하십시오.

Secure Cloud Analytics 포털에 사용자 초대

Secure Cloud Analytics 포털 프로비저닝을 요청하는 초기 사용자는 Secure Cloud Analytics 포털에서 관리자 권한을 갖습니다. 해당 사용자는 이메일로 다른 사용자를 초대하여 포털에 참여할 수 있습니다. 이러한 사용자에게 Cisco Secure Cloud Sign-On 자격증명이 없는 경우 초대 이메일의 링크를 사용하여 생성할 수 있습니다. 그러면 사용자는 Cisco Secure Cloud Sign-On 자격증명을 사용하여 Security Cloud Control에서 Secure Cloud Analytics로 교차 실행하는 동안 로그인할 수 있습니다.

이메일로 다른 사용자를 Secure Cloud Analytics 포털에 초대하려면 다음을 수행합니다.

Procedure

단계 **1** Secure Cloud Analytics 포털에 관리자로 로그인합니다.

단계 **2** **Settings(**설정**)** > **Account Management(**계정 관리**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **3** 이메일 주소를 입력합니다.

단계 **4** **Invite(**초대**)**를 클릭합니다.

Security Cloud Control에서 Secure Cloud Analytics로 교차 실행

Security Cloud Control에서 보안 알림을 보려면 다음을 수행합니다.

Procedure

단계 **1** Security Cloud Control 포털에 로그인합니다.

단계 **2** 왼쪽 창에서 분석 > **Secure Cloud Analytics**를 선택합니다.

단계 **3** Secure Cloud Analytics 인터페이스에서 **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

Cisco Secure Cloud 분석 및 동적 엔티티 모델링

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytics는 온프레미스 및 클라우드 기반 네트워크 구축을 모니터링하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

동적 엔티티 모델링

동적 엔티티 모델링은 방화벽 이벤트 및 네트워크 플로우 데이터에 대한 동작 분석을 수행하여 네트워크의 상태를 추적합니다. Secure Cloud Analytics의 컨텍스트에서 엔티티는 네트워크의 호스트 또는 엔드포인트와 같이 시간이 지남에 따라 추적할 수 있는 항목입니다. 동적 엔터티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔터티에 대한 정보를 수집합니다. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 라이선스와 통합된 Secure Cloud Analytics는 엔티티가 일반적으로 전송하는 트래픽 유형을 확인하기 위해 방화벽 이벤트 및 기타 트래픽 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매한 경우 Secure Cloud Analytics는 엔티티 트래픽 모델링에 NetFlow 및 기타 트래픽 정보도 포함할 수 있습니다. Secure Cloud Analytics는 각 엔터티의 최신 모델을 유지하기 위해 엔터티가 계속해서 트래픽을 전송하고 잠재적으로 다른 트래픽을 전송하므로 시간이 지남에 따라 이러한 모델을 업데이트합니다. 이 정보에서 Secure Cloud Analytics는 다음을 식별합니다.

- 엔티티의 역할 - 엔티티가 일반적으로 수행하는 작업을 설명합니다. 예를 들어 엔티티가 일반적으로 이메일 서버와 연결된 트래픽을 전송하는 경우, Secure Cloud Analytics는 엔티티를 이메일 서버 역할로 할당합니다. 엔터티는 여러 역할을 수행할 수 있으므로 역할/엔티티 관계는 다대일일 수 있습니다.
- 엔티티에 대한 관찰 - 외부 IP 주소와의 하트비트 연결 또는 다른 엔티티와 설정된 원격 액세스 세션과 같이 네트워크에서의 엔티티 동작에 대한 팩트입니다. Security Cloud Control와 통합하는 경우 방화벽 이벤트에서 이러한 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스도 구매한 경우, 시스템은 NetFlow에서 팩트를 가져오고 방화벽 이벤트와 NetFlow 모두에서 관찰을 생성할 수 있습니다. 관찰 자체는 관찰이 나타내는 것 이상의 의미를 전달하지 않습니다. 일반적인 고객은 수천 개의 관찰 및 몇 가지 알림을 가질 수 있습니다.

알림 및 분석

역할, 관찰 및 기타 위협 인텔리전스의 조합을 기반으로 Secure Cloud Analytics는 시스템에서 식별한 가능한 악의적인 행동을 나타내는 실행 가능한 항목인 알림을 생성합니다. 하나의 알림이 여러 관찰을 나타낼 수 있습니다. 방화벽이 동일한 연결 및 엔터티와 관련된 여러 연결 이벤트를 로깅하는 경우 하나의 알림만 생성될 수 있습니다.

예를 들어, 새 내부 디바이스 관찰 자체는 악의적인 행동을 구성하지 않습니다. 그러나 시간이 지남에 따라 엔티티가 도메인 컨트롤러와 일치하는 트래픽을 전송하면 시스템은 해당 엔티티에 도메인 컨트롤러 역할을 할당합니다. 이후에 엔티티가 비정상적인 포트를 사용하여 이전에 연결을 설정하지 않은 외부 서버에 연결하고 대량의 데이터를 전송하는 경우, 시스템은 새로운 대규모 연결(외부) 관찰 및 예외적인 도메인 컨트롤러 관찰을 로깅합니다. 해당 외부 서버가 Talos 감시 목록에 있는 것으로 식별된 경우, 이 모든 정보의 조합으로 인해 Secure Cloud Analytics가 이 엔티티의 동작에 대한 알림을 생성하고, 악성 동작을 조사하고 교정하기 위한 추가 작업을 수행하라는 메시지가 표시됩니다.

Secure Cloud Analytics 웹 포털 UI에서 알림을 열면 시스템이 알림을 생성하도록 유도한 지원 관찰을 볼 수 있습니다. 이러한 관찰을 통해 관련 엔터티에 대한 추가 컨텍스트(전송한 트래픽 포함) 및 외부 위협 인텔리전스(사용 가능한 경우)도 볼 수 있습니다. 또한 엔티티가 관련된 다른 관찰 및 알림을 보고 이 동작이 다른 잠재적인 악의적인 동작과 관련이 있는지 확인할 수 있습니다.

Secure Cloud Analytics에서 알림을 보고 닫을 때는 Secure Cloud Analytics UI의 트래픽을 허용하거나 차단할 수 없습니다. 디바이스를 액티브 모드로 구축한 경우에는 트래픽을 허용하거나 차단하도록 방화벽 액세스 제어 규칙을 업데이트하고, 패시브 모드에서 디바이스를 구축한 경우에는 방화벽 액세스 제어 규칙을 업데이트해야 합니다.

방화벽 이벤트 기반 알림 작업

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 워크플로우

알림의 워크플로우는 상태를 기반으로 합니다. 시스템에서 알림을 생성할 때 기본 상태는 Open(열림)이며 사용자가 할당되지 않습니다. Alerts(알림) 요약을 볼 때 즉시 문제가 되는 모든 열린 알림이 기본적으로 표시됩니다.

참고: **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 알림은 NetFlow에서 생성된 관찰, 방화벽 이벤트에서 생성된 관찰 또는 두 데이터 소스의 관찰을 기반으로 할 수 있습니다.

알림 요약을 검토할 때 알림에 대한 상태를 초기 분류로 할당, 태그 지정 및 업데이트할 수 있습니다. 필터 및 검색 기능을 사용하여 특정 알림을 찾거나, 다른 상태의 알림을 표시하거나, 다른 태그 또는 담당자와 연결할 수 있습니다. 알림의 상태를 스누즈로 설정할 수 있습니다. 이 경우 스누즈 기간이 경과할 때까지 미해결 알림 목록에 다시 나타나지 않습니다. 알림에서 스누즈 상태를 제거하여 미해결 알림으로 다시 표시할 수도 있습니다. 알림을 검토할 때 자신 또는 시스템의 다른 사용자에게 할당할 수 있습니다. 사용자는 사용자 이름에 할당된 모든 알림을 검색할 수 있습니다.

Alerts(알림) 요약에서 알림 상세정보 페이지를 볼 수 있습니다. 이 페이지에서는 이 알림을 생성한 지원 관찰에 대한 추가 컨텍스트 및 이 알림과 관련된 엔터티에 대한 추가 컨텍스트를 검토할 수 있습니다. 이 정보는 네트워크에서 문제를 추가로 조사하고 잠재적으로 악의적인 동작을 해결하기 위해 실제 문제를 정확히 찾아내는 데 도움이 될 수 있습니다.

Security Cloud Control 및 네트워크에서 Stealthwatch Cloud 웹 포털 UI 내에서 조사할 때 결과를 설명하는 알림과 함께 코멘트를 남길 수 있습니다. 이렇게 하면 나중에 참조할 수 있는 연구 기록을 만드는 데 도움이 됩니다.

분석을 완료한 경우 상태를 Closed(닫힘)로 업데이트하고 더 이상 기본적으로 미결 알림으로 표시되지 않도록 할 수 있습니다. 상황이 바뀌면 나중에 닫힌 알림을 다시 열 수도 있습니다.

다음은 지정된 알림을 조사하는 방법에 대한 일반적인 지침 및 제안 사항입니다. Secure Cloud Analytics는 알림을 로깅할 때 추가 컨텍스트를 제공하므로 이 컨텍스트를 조사에 활용할 수 있습니다.

이러한 단계는 포괄적이거나 모든 것을 포함하지 않습니다. 이는 알림 조사를 시작하는 데 사용할 수 있는 일반적인 프레임워크를 제공할 뿐입니다.

일반적으로 알림을 검토할 때 다음 단계를 수행할 수 있습니다.

1. 열린 알림 분류, on page 8
2. 나중에 분석하기 위해 알림 일시 중지, on page 8

3. 추가 조사를 위해 알림 업데이트, on page 9
4. 알림 검토 및 조사 시작, on page 10
5. 엔터티 및 사용자 검사, on page 12
6. Secure Cloud Analytics를 사용하여 문제 해결, on page 12
7. 알림 업데이트 및 닫기, on page 13

열린 알림 분류

특히 둘 이상의 알림이 아직 조사되지 않은 경우, 미해결 알림을 분류합니다.

- Security Cloud Control에서 Secure Cloud Analytics으로의 교차 실행 및 알림 보기에 대한 자세한 내용은 FTD 이벤트에서 생성된 Secure Cloud Analytics 알림 모니터링을 참조하십시오.

다음 질문을 합니다.

- 이 알림 유형을 높은 우선순위로 구성했습니까?
- 영향을 받는 서브넷에 대해 높은 감도를 설정했습니까?
- 네트워크의 새 엔터티에서 발생하는 비정상적인 동작입니까?
- 엔터티의 일반적인 역할은 무엇이며 이 알림의 동작이 해당 역할과 어떻게 일치합니까?
- 이 엔터티의 정상적인 동작에서 예외적으로 벗어났습니다.
- 사용자가 관련된 경우, 이는 사용자의 예상된 동작입니까, 아니면 예외적인 것입니까?
- 보호되거나 민감한 데이터가 손상될 위험이 있습니까?
- 이 동작이 계속 허용되는 경우 네트워크에 미치는 영향은 어느 정도입니까?
- 외부 엔터티와 통신하는 경우, 이러한 엔터티가 과거에 네트워크의 다른 엔터티와 연결을 설정했습니까?

우선순위가 높은 알림인 경우 조사를 계속하기 전에 인터넷에서 엔티티를 격리하거나 연결을 닫는 것을 고려하십시오.

나중에 분석하기 위해 알림 일시 중지

다른 알림에 비해 우선 순위가 낮은 알림을 스누즈합니다. 예를 들어 조직에서 이메일 서버를 FTP 서버로 용도를 변경하고 시스템에서 긴급 프로파일 알림(엔티티의 현재 트래픽이 이전에 일치하지 않았던 행동 프로파일과 일치함을 나타냄)을 생성하는 경우 이 알림을 나중에 다시 확인할 수 있습니다. 스누즈된 알림은 열린 알림과 함께 표시되지 않습니다. 이러한 스누즈된 알림을 검토하려면 특별히 필터링해야 합니다.

알림 스누즈:

Procedure

단계 **1** **Close Alert(**알림 닫기**)**를 클릭합니다.
단계 **2** Snooze this alert(이 알림 스누즈) 창의 드롭다운에서 스누즈 기간을 선택합니다.
단계 **3** **Save(**저장**)**를 클릭합니다.

What to do next

이러한 알림을 검토할 준비가 되면 다시 알림을 해제할 수 있습니다. 이렇게 하면 상태가 Open(열림)으로 설정되고 다른 Open(열림) 알림과 함께 알림이 표시됩니다.

스누즈된 알림의 스누즈를 해제합니다.

- 스누즈된 알림에서 **Unsnooze Alert(**알림 스누즈 해제**)**를 클릭합니다.

추가 조사를 위해 알림 업데이트

알림 세부 정보를 엽니다.

Procedure

단계 **1** **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.
단계 **2** 알림 유형 이름을 클릭합니다.

What to do next

초기 분류 및 우선순위에 따라 알림을 할당하고 태그를 지정합니다.

1. **Assignee(**담당자**)** 드롭다운에서 사용자를 선택하여 알림을 할당하면 사용자가 조사를 시작할 수 있습니다.
2. 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택하여 알림에 태그를 추가하여 향후 식별을 위해 알림을 더 잘 분류하고 알림에서 장기적 패턴을 설정합니다.
3. 이 알림에 대한 코멘트를 입력한 다음 **Comment(**코멘트**)**를 클릭하여 초기 결과를 추적하고 알림에 할당된 사람을 지원하는 데 필요한 코멘트를 남깁니다. 알림은 시스템 코멘트와 사용자 코멘트를 모두 추적합니다.

알림 검토 및 조사 시작

할당된 알림을 검토하는 경우 알림 세부 정보를 검토하여 Stealthwatch Cloud에서 알림을 생성한 이유를 파악합니다. 지원 관찰을 검토하여 이러한 관찰이 소스 엔터티에 미치는 영향을 파악합니다.

경고가 방화벽 이벤트를 기반으로 생성된 경우, 시스템은 방화벽 구축이 이 경고의 소스임을 인식하지 않습니다.

이 소스 엔터티에 대한 모든 지원 관찰을 확인하여 일반 동작 및 패턴을 파악하고 이 활동이 더 긴 추세의 일부일 수 있는지 확인합니다.

SUMMARY STEPS

1. 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(➔)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.
2. **All Observations for Network(**네트워크에 대한 모든 관찰**)** 옆에 있는 화살표 아이콘(➔)을 클릭하여 이 알림의 소스 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

DETAILED STEPS

프로시저

단계 **1** 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(➔)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.

단계 **2** **All Observations for Network(**네트워크에 대한 모든 관찰**)** 옆에 있는 화살표 아이콘(➔)을 클릭하여 이 알림의 소스 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

이러한 관찰에 대한 추가 분석을 수행하려면 쉼표로 구분된 값 파일로 지원 관찰을 다운로드합니다.

- 알림 세부 정보의 Supporting Observations(지원 관찰) 창에서 **CSV**를 클릭합니다.

관찰 결과에서 소스 엔터티 동작이 악의적인 동작을 나타내는지 확인합니다. 소스 엔터티가 여러 외부 엔터티와의 연결을 설정한 경우, 외부 엔터티가 어떤 식으로든 관련이 있는지 확인합니다(예: 모든 엔터티가 유사한 지리위치 정보를 가지고 있거나 해당 IP 주소가 동일한 서브넷에 있는지 여부).

소스 엔터티 IP 주소 또는 호스트 이름에서 소스 엔터티와 관련된 추가 컨텍스트를 확인합니다. 여기에는 관련될 수 있는 기타 알림 및 관찰, 디바이스 자체에 대한 정보, 전송 중인 세션 트래픽 유형이 포함됩니다.

- 엔티티와 관련된 모든 알림을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Alerts(**알림**)**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Observations(**관찰**)**를 선택하여 엔티티와 관련된 모든 관찰을 확인합니다.
- 디바이스에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Device(**디바이스**)**를 선택합니다.

- 이 엔터티와 관련된 세션 트래픽을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 소스 엔티티는 항상 네트워크 내부에 있습니다. 이를 방화벽 이벤트의 Initiator IP(이니시에이터 IP)와 비교해 보십시오. 이 IP는 연결을 시작한 엔티티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

관찰에서 다른 외부 엔터티에 대한 정보를 검토합니다. 지리위치 정보를 검토하고 지리위치 데이터 또는 Umbrella 데이터가 악성 엔티티를 식별하는지 확인합니다. 이러한 엔터티에 의해 생성된 트래픽을 확인합니다. Talos, AbuseIPDB 또는 Google에 이러한 엔터티에 대한 정보가 있는지 확인합니다. 여러 날짜의 IP 주소를 찾고 외부 엔터티가 네트워크의 엔터티와 설정한 다른 유형의 연결을 확인합니다. 필요한 경우 이러한 내부 엔터티를 찾아 보안 침해 또는 의도하지 않은 행동의 증거가 있는지 확인합니다.

소스 엔티티가 연결을 설정한 외부 엔티티 IP 주소 또는 호스트 이름에 대한 컨텍스트를 검토합니다.

- 이 엔티티에 대한 최근 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **IP Traffic(IP** 트래픽**)**을 선택합니다.
- 이 엔티티에 대한 최근 세션 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- **AbuseIPDB**웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 AbuseIPDB를 선택합니다.
- Cisco Umbrella 웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Cisco Umbrella**를 선택합니다.
- Google에서 이 IP 주소를 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Google Search(Google** 검색**)**를 선택합니다.
- Talos 웹사이트에서 이 정보에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Talos Intelligence**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Add IP to watchlist(**감시 목록에 **IP** 추가**)**를 선택하여 이 엔터티를 감시 목록에 추가합니다.
- 이 엔티티의 지난 달 트래픽을 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Find IP on multiple days(**여러 날짜의 **IP** 찾기**)**를 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 연결된 엔터티는 항상 네트워크 외부에 있습니다. 이를 방화벽 이벤트의 Responder IP(응답자 IP)와 비교해 보십시오. 이는 연결 요청에 응답한 엔티티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

엔터티 및 사용자 검사

Stealthwatch Cloud 포털 UI에서 알림을 검토한 후 소스 엔터티, 이 알림과 관련되었을 수 있는 사용자 및 기타 관련 엔터티에 대해 직접 추가 검사를 수행할 수 있습니다.

- 소스 엔터티가 물리적으로 또는 클라우드에서 네트워크의 어느 위치에 있는지 확인하고 직접 액세스합니다. 이 엔터티에 대한 로그 파일을 찾습니다. 네트워크의 물리적 엔터티인 경우 디바이스에 액세스하여 로그 정보를 검토하고 이 동작의 원인에 대한 정보가 있는지 확인합니다. 가상 엔터티이거나 클라우드에 저장된 경우 로그에 액세스하여 이 엔터티와 관련된 항목을 검색합니다. 무단 로그인, 승인되지 않은 구성 변경 등에 대한 자세한 내용은 로그를 검사합니다.
- 엔터티를 검사합니다. 엔터티 자체에서 멀웨어 또는 취약성을 식별할 수 있는지 확인합니다. 조직에서 승인하지 않은 USB 스틱과 같이 디바이스에 대한 물리적 변경이 있는지를 포함하여 악의적인 변경이 있는지 확인합니다.
- 네트워크의 사용자 또는 네트워크 외부의 사용자가 관련되었는지 확인합니다. 가능한 경우 사용자에게 무엇을 하고 있었는지 물어봅니다. 사용자가 사용할 수 없는 경우, 액세스 권한이 있어야 했는지, 그리고 퇴사한 직원이 퇴사 전에 외부 서버에 파일을 업로드하는 등의 상황이 발생했는지 확인합니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

Secure Cloud Analytics를 사용하여 문제 해결

악의적인 행동으로 인해 알림이 발생한 경우 악의적인 행동을 교정합니다. 예를 들면 다음과 같습니다.

- 악의적인 엔터티 또는 사용자가 네트워크 외부에서 로그인을 시도한 경우 엔터티 또는 사용자가 네트워크에 액세스하지 못하도록 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 엔터티가 무단 도메인 또는 악의적인 도메인에 액세스하려고 시도한 경우 영향을 받는 엔터티를 검사하여 멀웨어가 원인인지 확인합니다. 악의적인 DNS 리디렉션이 있는 경우 네트워크의 다른 엔터티 또는 봇넷의 일부가 영향을 받는지 확인합니다. 사용자가 이러한 작업을 수행하려는 경우 방화벽 설정을 테스트하는 등 합법적인 이유가 있는지 확인합니다. 도메인에 대한 추가 액세스를 방지하려면 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 엔터티가 기록 엔터티 모델 동작과 다른 동작을 보이는 경우 동작 변경이 의도된 것인지 확인합니다. 의도하지 않은 작업인 경우 네트워크의 다른 권한이 있는 사용자가 변경을 담당하는지 확인합니다. 의도하지 않은 동작이 네트워크 외부의 엔터티와의 연결과 관련된 경우 이를 해결하기 위해 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 취약성 또는 익스플로잇을 식별한 경우, 영향을 받는 엔터티를 업데이트 또는 패치하여 취약성을 제거하거나 무단 액세스를 방지하도록 방화벽 구성을 업데이트합니다. 네트워크의 다른 엔

터티가 유사하게 영향을 받을 수 있는지 확인하고 해당 엔터티에 동일한 업데이트 또는 패치를 적용합니다. 현재 취약성 또는 익스플로잇에 수정 사항이 없는 경우 해당 벤더에 문의하십시오.

- 멀웨어가 확인되면 엔티티를 격리하고 멀웨어를 제거합니다. 방화벽 파일 및 멀웨어 이벤트를 검토하여 네트워크의 다른 엔터티가 위험에 노출되어 있는지 확인하고, 이 멀웨어가 확산되지 않도록 엔터티를 격리 및 업데이트합니다. 이 멀웨어 또는 이 멀웨어를 유발한 엔티티에 대한 정보로 보안 인텔리전스를 업데이트합니다. 향후 이 멀웨어가 네트워크를 감염시키는 것을 방지하려면 방화벽 액세스 제어와 파일 및 멀웨어 규칙을 업데이트하십시오. 필요에 따라 벤더에 알립니다.
- 악의적인 행동으로 인해 데이터가 유출된 경우 무단 소스로 전송되는 데이터의 특성을 확인합니다. 무단 데이터 유출에 대한 조직의 프로토콜을 따르십시오. 이 소스에 의한 향후 데이터 유출 시도를 방지하려면 방화벽 구성을 업데이트하십시오.

알림 업데이트 및 닫기

결과에 따라 태그를 추가합니다.

Procedure

단계 **1** Secure Cloud Analytics 포털 UI에서 **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택합니다.

조사 결과 및 수행한 교정 단계를 설명하는 최종 코멘트를 추가합니다.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

알림을 닫고 유용하거나 도움이 되지 않음으로 표시합니다.

1. 알림 세부 정보에서 **Close Alert(**알림 닫기**)**를 클릭합니다.
2. 알림이 도움이 되었으면 **Yes(**예**)**를 선택하고, 알림이 도움이 되지 않았다면 **No(**아니요**)**를 선택합니다. 이는 알림이 악의적인 행동으로 인해 발생했음을 의미하는 것이 아니라 해당 알림이 조직에 도움이 되었음을 의미합니다.
3. **Save(**저장**)**를 클릭합니다.

What to do next

종료된 알림 다시 열기

종료된 알림과 관련된 추가 정보를 발견하거나 알림과 관련된 코멘트를 더 추가하려는 경우 알림을 다시 열어 상태를 Open(열림)으로 변경할 수 있습니다. 그런 다음 필요에 따라 알림을 변경한 다음 추가 조사가 완료되면 알림을 닫을 수 있습니다.

종료된 알림을 다시 엽니다.

- 닫힌 알림의 세부 사항에서 **Reopen Alert(**알림 다시 열기**)**를 클릭합니다.

알림 우선순위 수정

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 유형은 기본 우선순위와 함께 제공되며, 이는 시스템이 이 유형의 알림 생성에 대한 민감도에 영향을 미칩니다. 알림은 기본적으로 Cisco 인텔리전스 및 기타 요인에 따라 낮음 또는 보통으로 설정됩니다. 네트워크 환경에 따라 알림 유형의 우선순위를 다시 지정하여 우려되는 특정 알림을 강조할 수 있습니다. 모든 알림 유형을 낮음, 보통 또는 높음 우선순위로 구성할 수 있습니다.

- **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.
- Settings(설정) 드롭다운 아이콘()을 클릭한 다음 **Alert Types and Priorities(**알림 유형 및 우선순위**)**를 선택합니다.
- 알림 유형 옆에 있는 편집 아이콘()을 클릭하고 낮음, 중간 또는 높음을 선택하여 우선순위를 변경합니다.