FireSIGHT Management Center 스토리 가이드 v1

최종 업데이트: 2016 년 12 월 9 일

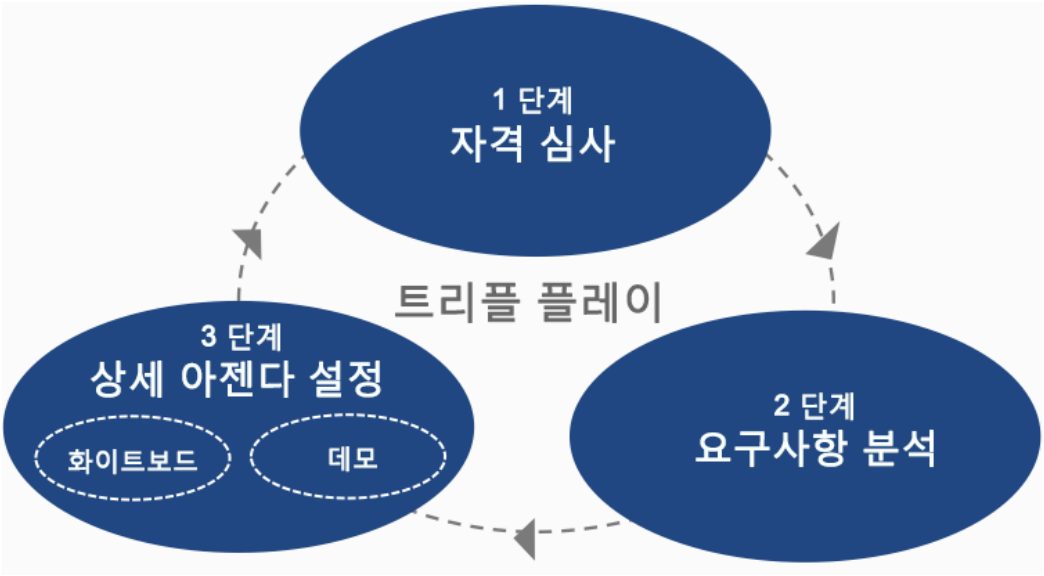
이 데모 가이드 정보

스토리 가이드는 고객의 통찰력을 솔루션에 접목시켜 데모 플랫폼 활용에 대한 샘플 플로우를 제공하기 위한 것입니다. 고객의 문제를 해결하기 위한 오퍼에 대한 기능 및 가능성을 강조하고, 제품이 어떤 방식으로 고객의 구체적인 비즈니스 성과 달성을 지원하는지 집중 조명하는 것을 목표로 합니다. 이 데모 가이드는 고객의 요구 사항을 파악하기 위한 것으로, 화이트 보드 및 제품 데모로 진행되도록 구성되었습니다.

이 데모 가이드는 고객 중심의 간결하고, 흥미로운 내용을 전달하도록 구성되었습니다. 이러한 정보를 설명하는 데 5분 ~ 7분이 소요되며, 필요한 경우 더 자세히 설명할 수 있습니다.

디지털 대비 세일즈 프로세스 요약

디지털 대비 세일즈 프로세스 트리플 플레이



데모가 진행되는 단계에서 다음과 같은 세일즈 요구 사항을 확인해야 합니다.

- **1 단계:** 세일즈 가능성 확인
- **2 단계:** 요구사항 분석
- **3 단계:** 상세 아젠다 설정
    - 화이트보드
    - **사용자의 현재 위치 - 데모**

의제 설정 – 데모 목표

이 사례 가이드에는 다음 시나리오가 포함되어 있습니다.

- **시나리오 1 –** FSMC(FireSIGHT Management Center) Context Explorer 개요. 사용자는 이 대시보드에서 기간에 대한 다양한 보기를 표시할 수 있으며, 이를 통해 공통 필터를 사용하여 모든 영역을 한꺼번에 볼 수 있습니다. 사건 조사를 위해 심층 분석할 때처럼 데이터 중 일부를 변경하려는 경우에 매우 유용합니다.
- **시나리오 2 –** FSMC 요약 대시보드 개요. 애플리케이션 사용량, 현존하는 위협 등 고객의 네트워크에 대한 실시간 상황 정보를 표시하는 데 활용할 수 있습니다. 이 대시보드는 개괄적으로 네트워크를 조명하는 출발점으로 적합합니다.
- **시나리오 3** – 차세대 방화벽 또는 IP 정책 수립. 이 시나리오에서는 간단하면서 효과적으로 방화벽 정책을 생성하는 것을 보여줍니다. 많은 기업은 사용되는 포트 또는 프로토콜에 관계없이 특정 애플리케이션을 허용하거나 차단하는 규칙을 사용하려 합니다. 또한 정의된 IP 주소보다는 사용자의 ID 또는 사용 중인 디바이스의 유형에 따라 트래픽 권한을 적용하려 합니다.

이러한 시나리오를 통해 다음을 수행할 수 있습니다.

- Cisco FireSIGT 기능에 대한 데모 실행
- 고객이 고민하는 최우선 비즈니스 이니셔티브 및 환경을 연관 지어 데모 실행
- 최대한 간결하게 진행하고, 이 단계에서 필요하지 않는 심층적인 기술 설명은 피함
- 간소화된 관리 기능을 적극적으로 강조
- CLI만 사용해 단순히 기능만 풍부하게 제공하는 HW 기업이 아님을 강조

데모 중 고객과의 대화에서는 고객의 위험 감소를 지원하는 데 중점을 두어야 합니다. 일반적인 고객의 당면 과제, 솔루션을 통한 이점, 관련된 데모 플로우는 본 가이드에 함께 포함되어 있습니다.

데모 환경에 대한 참고 사항

이 스토리 가이드는 Cisco FireSIGHT 차세대 보안 솔루션의 몇 가지 주요 기능을 데모로 실행하여 어카운트 매니저를 지원하기 위한 것이며, 다른 구성 요소(SSL 해독, ISE 통합)는 다루지 않습니다. 이 데모는 인터넷에 상시 접속되는 데모 환경으로 dCloud에 구축되었으며 다음 요소로 구성되어 있습니다.

- Cisco ASA with FireSIGHT Services
- Active Directory
- 라이브 고객 환경을 시뮬레이션하는 네트워크 트래픽
    - 데이터 수정 불가
    - 24시간 반복 주기 데이터
    - 알람 변경 > 시뮬레이션 데이터가 24시간 주기에서 어디에 있느냐에 따라 알람이 발효되고 종료됩니다.

이 데모는 범위가 제한적입니다. FireSIGHT 및 Firepower 제품과 솔루션에 대한 자세한 내용은 www.cisco.com/go/security를 참조하십시오.

중요: 이 스토리 가이드는 데모 과정에서 어떤 틀로 상담할 것인지 예를 들어 보여줍니다. 참고: dCloud 표준을 엄격하게 따르지는 않습니다.

솔루션 강점

FSMC System은 위협 중심의 차세대 보안 시스템입니다. 방화벽, IPS, AMP(advanced malware protection)를 통해 매우 강력한 보안 제어 기능을 제공할 뿐 아니라 지능적 위협에 대한 가시성도 높입니다. FSMC는 추측에 의존하지 않고 네트워크 환경, 네트워크에 있는 호스트의 유형, 엔드포인트와 서버에서 사용하는 애플리케이션에 대한 지식을 바탕으로 정책을 구축하고, 보안 디바이스 및 서비스 튜닝을 위한 수고를 덜어줍니다. 그러면 시스템의 정확도가 향상되고 네트워크 또는 보안 팀이 주의가 필요한 문제를 신속하게 집중적으로 다룰 수 있게 됩니다. 사용자는 회귀적 기능을 활용하여 위협과 악성코드가 네트워크에 침투한 경로를 파악하고 악성 파일의 이동을 추적할 수 있습니다.

솔루션 구성 요소

솔루션의 주요 구성 요소는 다음과 같습니다.

- FSMC(FireSIGHT Management Center). FSMC는 중앙 집중식 관리 및 보고 어플라이언스로서 전용 하드웨어 어플라이언스에서 실행되거나 VMware에서 가상 머신의 형태로 실행됩니다.
- Cisco FireSIGHT. Cisco ASA(Adaptive Security Appliance)의 서비스로, 전용 FireSIGHT 어플라이언스로, VMware, Amazon Web Service, KVM에서 실행되는 가상 어플라이언스로 또는 지원되는 하드웨어나 가상 어플라이언스에서 실행되는 Firepower Threat Defense 어플라이언스의 형태로 실행됩니다.

데모 플랫폼에 접속하기

가장 가까운 위치에 있는 **DNA Demo Platform(DNA 데모 플랫폼)** 기본 페이지에 액세스합니다.

참고: 모든 데이터센터를 사용할 수 있지만, 사용자 위치에서 가장 가까운 데이터센터를 선택하는 것이 좋습니다.

표 1. 데이터센터별 기본 페이지 주소

데이터센터	DNA 데모 플랫폼
AMER	https://dcloud2-rtp.cisco.com/dCloud/dna.jsp
EMEAR	https://dcloud2-lon.cisco.com/dCloud/dna.jsp
APJ	https://dcloud2-sng.cisco.com/dCloud/dna.jsp
GC	https://dcloud2-chi.cisco.com/dCloud/dna.jsp

2 단계: VOD 연습 수행 테이블에서 **FSMC** 하이퍼링크를 클릭합니다.

표 2. 2 단계: VOD 연습 수행

2 단계: VOD 연습 수행		
		FSMC

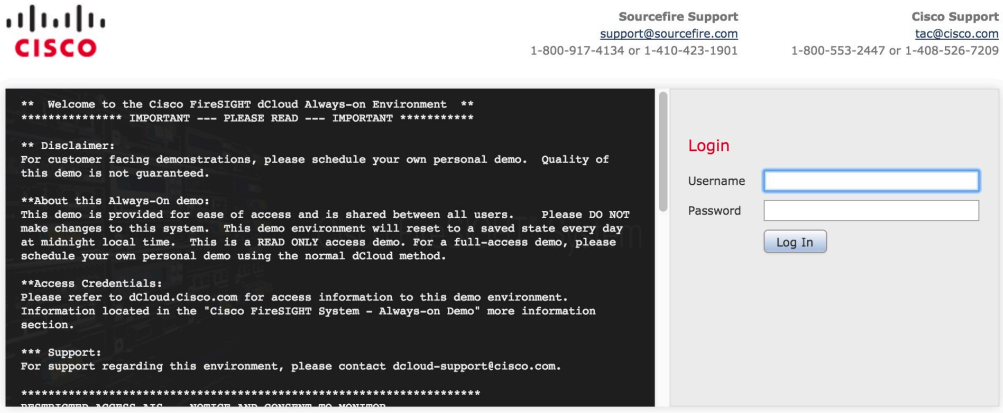
3 단계: 데모 실행 테이블에서 **FSMC** 하이퍼링크를 클릭합니다.

표 3. 3 단계: 데모 실행

3 단계: 데모 실행		
		FSMC

참고: dCloud에 처음 로그인하는 경우 계속하려면 약관에 동의해야 합니다.

계정 **amdemo1**, 비밀번호 **C1sco12345**를 사용하여 로그인하십시오.



Context Explorer 개요

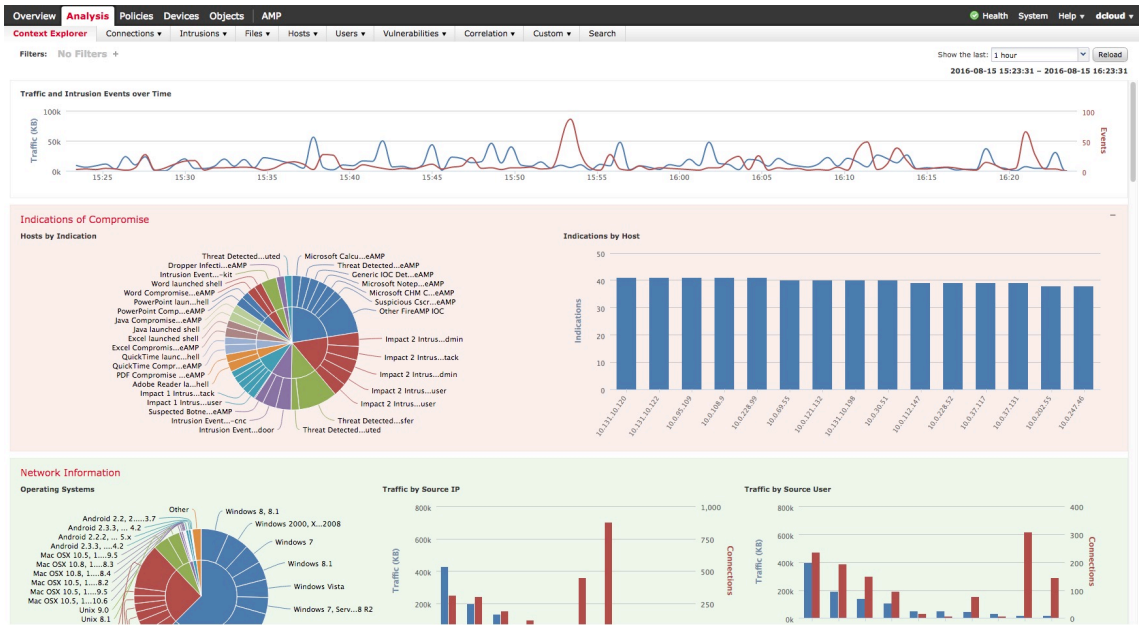
Cisco FSMC는 매우 강력한 대시보드 모음을 제공합니다. Context Explorer는 특별한 종류의 상위 레벨 대시보드로서 공통의 시간 및 필터에 중점을 두고 네트워크에 대한 다양한 보기를 제공합니다. 이러한 보기는 모두 Context Explorer에 패널의 형태로 포함되어 있습니다.

- 시간 경과에 따른 트래픽 및 침입 이벤트
- 보안 침해 지표
- 네트워크 정보(운영 체제 정보, IP 주소 및 사용자 이름 기준 상위 대화자 등)
- 애플리케이션 프로토콜 정보(웹 애플리케이션 및 클라이언트 애플리케이션 포함)
- 보안 인텔리전스
- 침입 정보
- 파일 정보(악성코드 포함)
- 지리위치 정보
- URL 정보

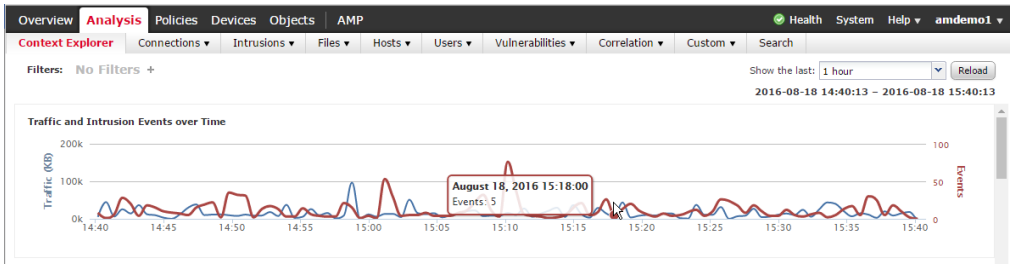
필터가 적용되거나 시간 범위가 수정되면 원하는 정보에 맞게 이 패널 각각의 데이터가 변경됩니다. 예컨대 중앙 사용자의 네트워크 액세스에 대한 트러블슈팅에 이를 활용할 수 있습니다. 사용자의 이름을 필터로 적용할 수 있으며, 위에 표시된 모든 데이터가 필터링됩니다. 즉 사용자 이름의 네트워크 트래픽과 매치하는 데이터만 패널에 나타납니다.

단계

1. Context Explorer 이해 - 처음 로그인하면 Context Explorer 페이지가 표시됩니다. 나중에 이 페이지로 돌아가야 하는 경우, 맨 위 바에서 **Analysis(분석)**를 클릭하기만 하면 됩니다.



이제 페이지 위아래로 스크롤하면서 탐색하겠습니다. 각 패널을 살펴볼 수 있습니다. 색상으로 표시되어 있으므로 원하는 정보를 더 수월하게 찾을 수 있습니다. 각 패널에는 그래프와 차트가 있습니다. 모두 대화형입니다. 마우스를 올려놓으면 관련 정보가 나타납니다. 클릭하면 필터에서 필드를 추가하거나 제거할 수 있습니다. 아래의 그림은 시간의 경과에 따른 트래픽 및 침입 이벤트 그래프입니다. 선 위에 마우스를 놓으면 해당 시점에 확인된 이벤트 수를 볼 수 있습니다.



그럼 빨간색으로 표시된 **Indications of Compromise(보안 침해 지표)** 패널로 가보겠습니다. 여기서는 어떤 호스트가 감염에 취약하게 만드는 행동을 나타냈는지 보여줍니다. 실제 네트워크에서는 이렇게 많은 IOC가 나타나지 않겠지만, 여기서는 호스트가 감염될 수 있는 여러 경로를 집중 조명하기 위해 표시했습니다. IOC 위에 마우스를 놓으면 이 IOC가 나타나는 호스트의 수가 표시됩니다.

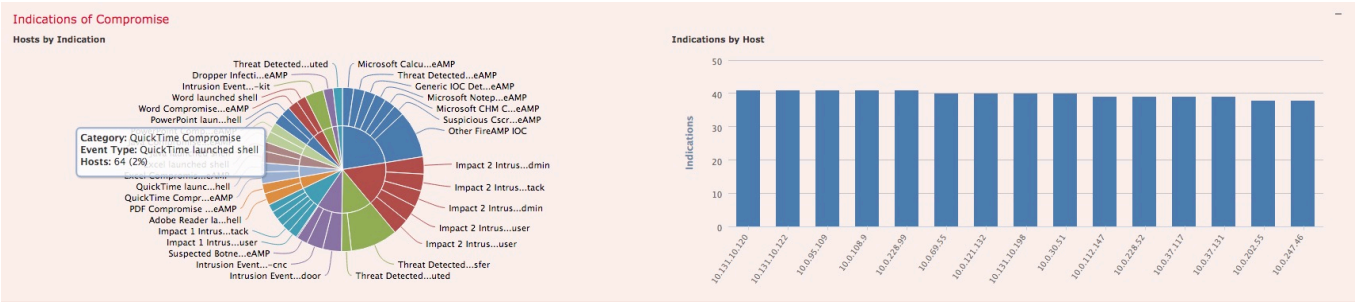
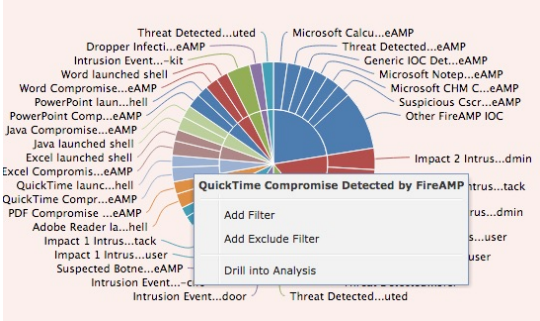
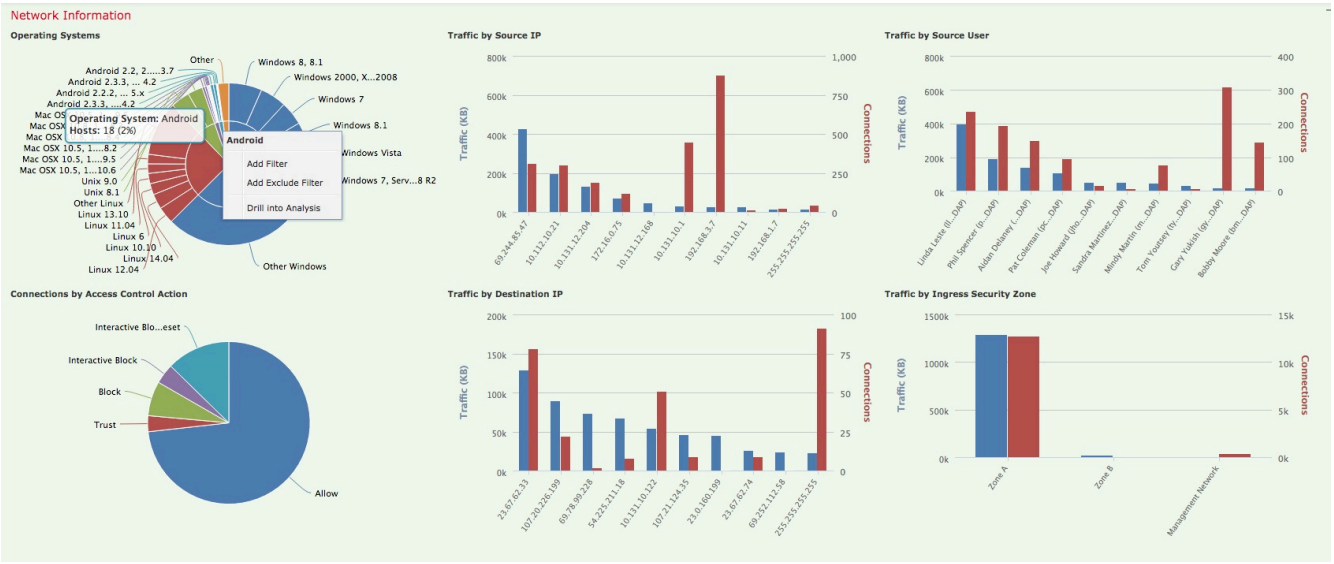


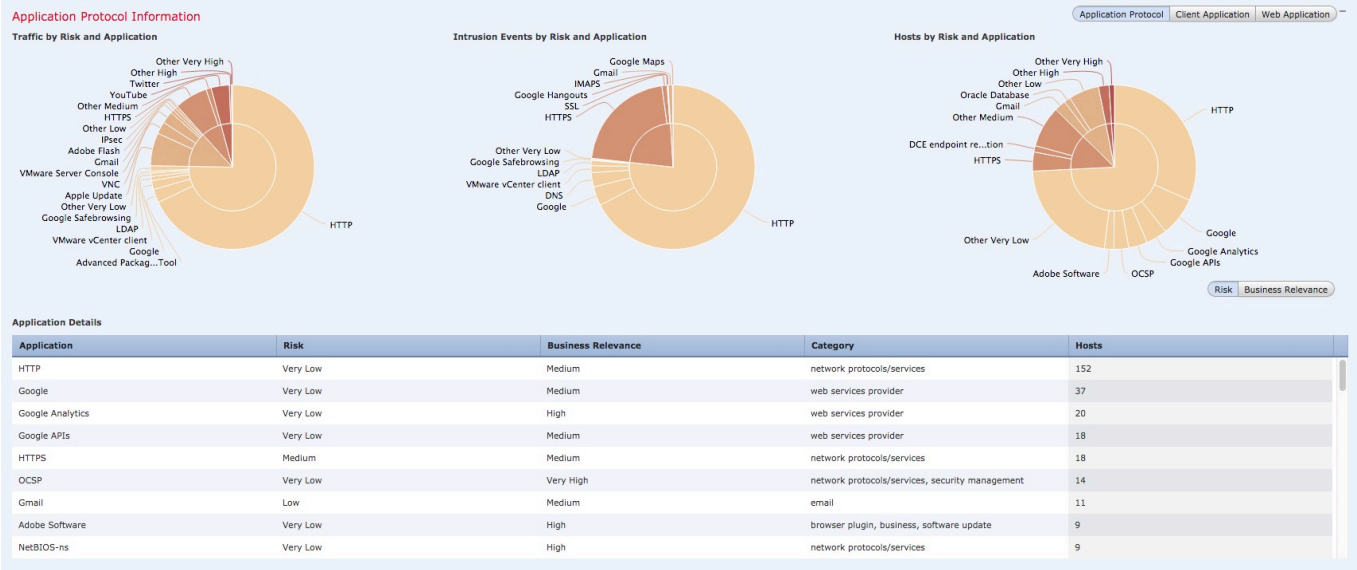
차트 섹션을 클릭해보겠습니다. 이 IOC에서 필터링하거나 ICO를 트리거한 이벤트까지 들어갈 수 있습니다. 이렇게 모든 패널과의 상호 작용이 가능합니다.



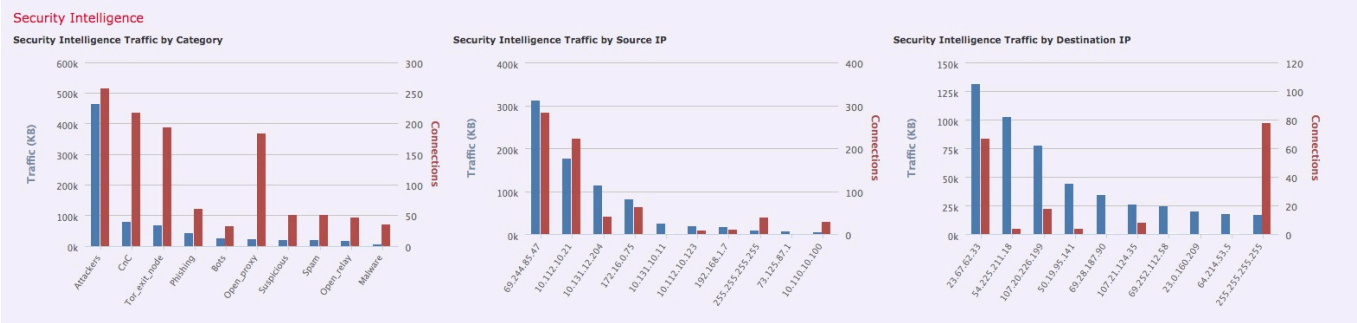
다음으로 녹색 **Network Information(네트워크 정보)** 패널로 이동합니다. 이 패널은 네트워크에서 실행 중인 디바이스의 유형 및 상위 트래픽 소스/대상을 보여줍니다. IP 주소 및 사용자 정보를 쉽게 확인할 수 있습니다. 누가 이 다양한 컴퓨팅 디바이스를 사용하고 있는지 확인해야 한다면 어떨까요? 이를테면 어떤 교육구에서 어떤 학생이 Android 태블릿을 사용하고 있는지 알아야 한다고 가정해 보겠습니다. 이를 위해서는 **Operating Systems(운영 체제)** 차트에서 슬라이스를 클릭하고 필터에 **Android**를 추가하면 됩니다.



이제는 파란색 **Application Protocol Information(애플리케이션 프로토콜 정보)** 패널로 가보겠습니다. 여기서는 패널 오른쪽 위에서 애플리케이션 프로토콜, 클라이언트 애플리케이션 또는 웹 애플리케이션을 표시하도록 선택할 수 있습니다. 계속 **애플리케이션 프로토콜**로 두고 계속 탐색하겠습니다.



자주색 **Security Intelligence(보안 인텔리전스)** 정보 패널을 보십시오. 보안 인텔리전스 기능이 어떻게 작동하는지 알아두어야 합니다. 보안 어플라이언스는 목록 또는 피드를 구독하면서 인터넷에서 위험한 디바이스의 IP 주소 정보를 얻습니다. 이 정보를 사용하여 이러한 곳을 목적지 또는 출발지로 하는 트래픽을 보고하고 차단할 수 있습니다. 화면의 정보를 보면서 어플라이언스가 어떻게 공격자(인터넷에서 적극적으로 다른 호스트를 공격해온 IP 주소), CnC(봇넷 명령 및 제어 활동에 가담하는 IP 주소) 등과 같은 카테고리를 차단하는지 확인합니다. 이러한 피드를 활용하면 훨씬 더 효과적인 보안이 이루어집니다. Cisco Firepower에서는 Cisco 피드, 서드파티 피드 또는 사용자가 직접 생성한 피드 등 개수 제한 없이 피드를 구독할 수 있습니다.



황갈색의 **Intrusion Information(침입 정보)** 패널을 보십시오. 이 패널의 차트와 그래프는 침입 차단 엔진에서 트리거한 이벤트를 나타냅니다. FSMC IPS의 흥미로운 점 중 하나는 영향 레벨 사용입니다. 패널의 왼쪽 위에서 확인할 수 있습니다.

침입 이벤트를 간단하게 분석하고 IPS 정책을 탄력적으로 튜닝할 수 있도록 FSMC는 사용 중인 네트워크 및 애플리케이션에 대한 지식을 활용합니다. 다른 IPS 시스템에서 흔히 나타나는 노이즈와 달리 정말 관심을 가져야 할 이벤트에 집중하게 해줍니다.

영향 레벨의 의미를 정리하면 다음과 같습니다.

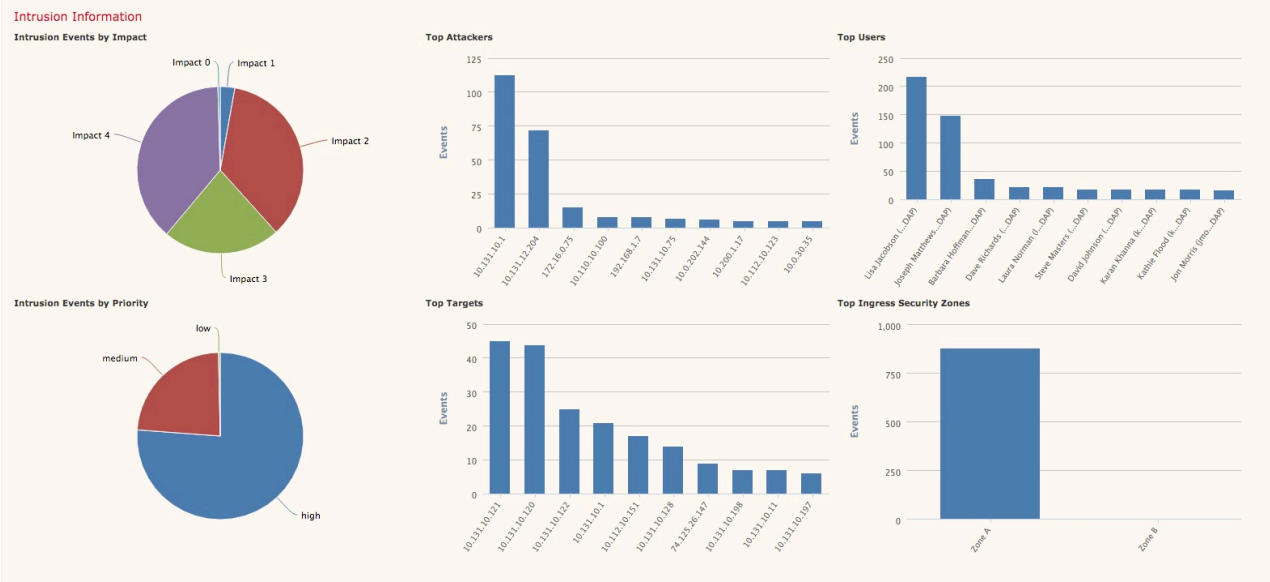
영향 1: 네트워크의 호스트가 공격에 관련되었으며, 해당되는 운영 체제와 애플리케이션의 조합을 실행하는 중입니다. 공격에 취약한 것 같습니다. 조사해야 할 중대한 이벤트입니다.

영향 2: 네트워크의 호스트가 공격에 관련되었습니다. 해당되는 서비스 및 애플리케이션을 실행하고 있으나 공격에 취약한 것 같지 않습니다. 관심을 갖고 지켜볼 만하지만 대개 중대한 것은 아닙니다.

영향 3: 네트워크의 호스트가 공격에 관련되었습니다. 공격의 표적이 된 서비스 또는 애플리케이션을 실행하는 것 같지 않습니다. 아직 취약한 상태가 아닙니다.

영향 4: 네트워크의 호스트가 공격에 관련되었으나, 실제로 네트워크에 존재하지 않거나 새로 추가되었습니다. 그 취약점이 아직 확인되지 않았습니다.

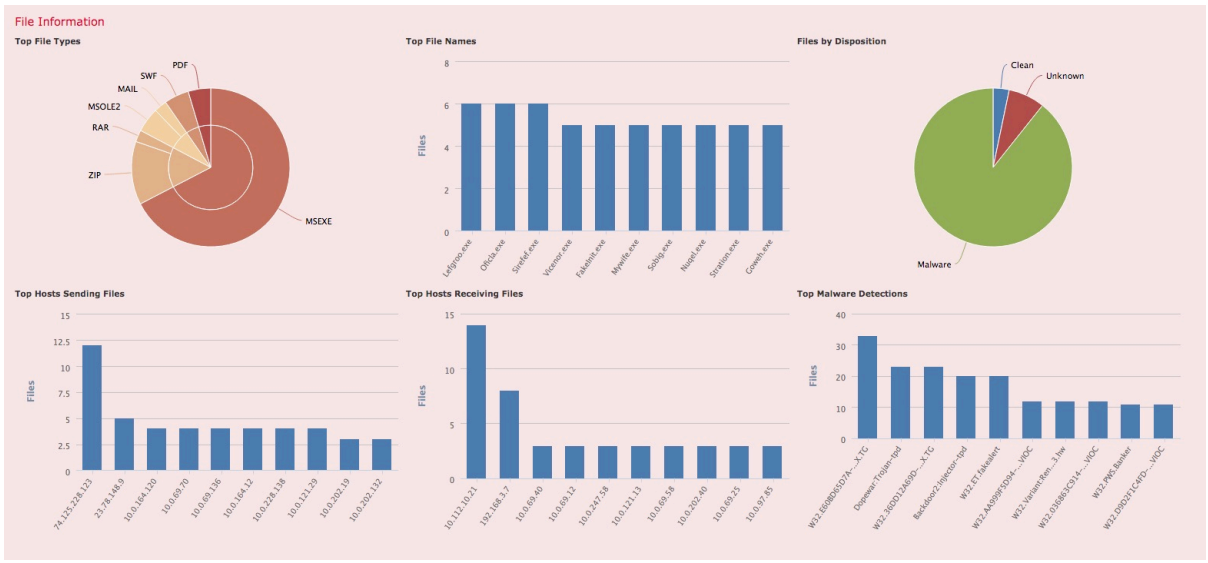
영향 0: 소스 및 대상 IP 주소가 네트워크에 없습니다. 조사해야 할 이벤트입니다. 잘못 구성된 Firepower 시스템 또는 무단 네트워크 트래픽이 원인일 수 있습니다.



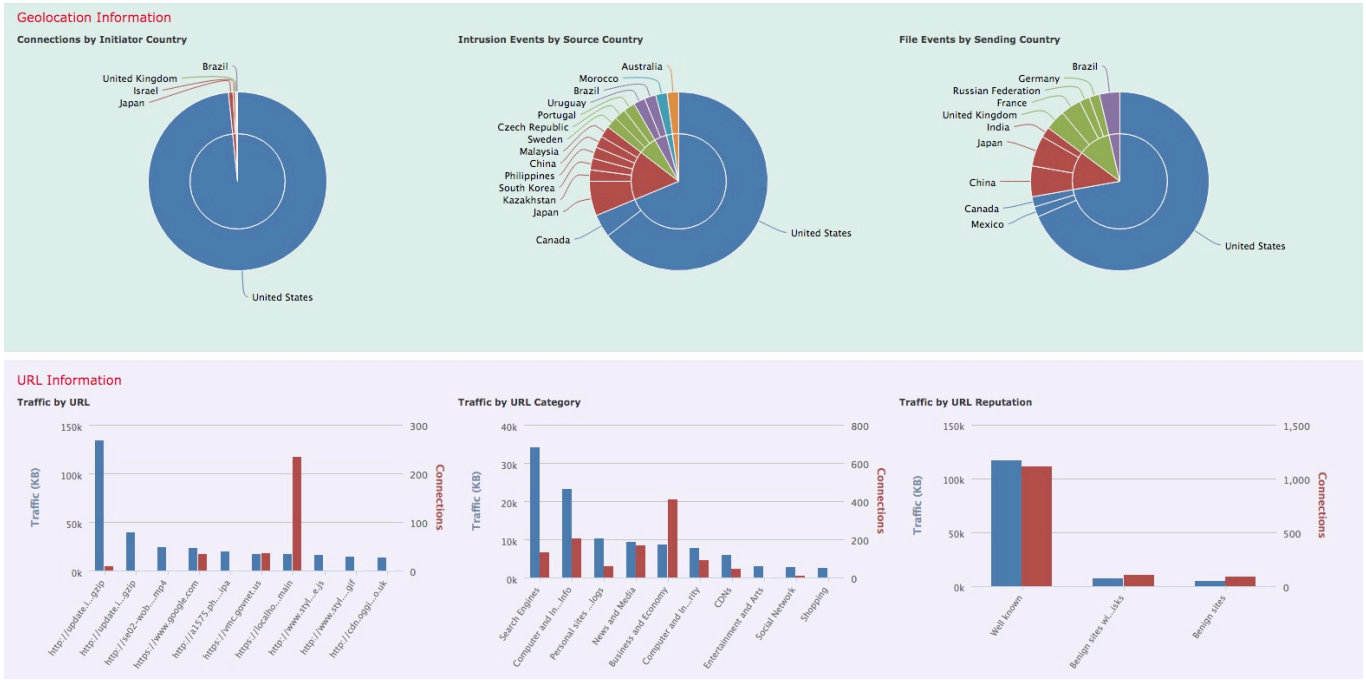
다음 차례는 빨간색 **File Information(파일 정보)** 패널입니다. 이 패널에서는 FSMC 어플라이언스 전반에서 파일 정책이 적용된 모든 파일 복사본을 확인할 수 있습니다. 모든 파일일 수도 있고, 또는 FSMC 관리자가 정의한 일부 파일일 수도 있습니다. 다음과 같은 정보를 확인할 수 있습니다.

- 파일 유형
- 상위 파일 이름
- 파일을 보내거나 받는 상위 호스트
- 성향별 파일 수
- 상위 악성코드 탐지

AMP(Advanced Malware Protection)는 시스템에서 구조 및 행동을 기준으로 삼는 등 여러 방식으로 파일을 분석하여 호스트에 유해한 파일을 신속하게 파악하고 악성 파일의 어플라이언스 통과를 차단하도록 지원합니다.



맨 아래의 두 패널을 간단하게 살펴보겠습니다. 지리위치 및 URL 정보를 확인할 수 있습니다.



요약

FireSIGHT Management Center Context Explorer는 네트워크 트래픽, 애플리케이션, 위협에 대한 다양한 관점을 쉽고 빠르게 시각화할 수 있는 매우 강력한 툴을 제공합니다.

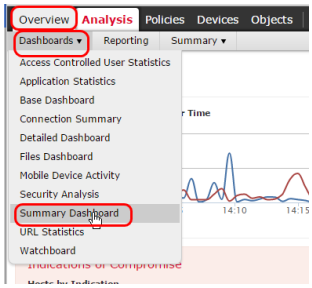
요약 대시보드 개요

Cisco FSMC는 여러 세부 대시보드를 제공합니다. 고도의 맞춤화가 가능하며 고객은 시스템에 대시보드를 추가할 수도 있습니다. 관심을 갖고 살펴볼 네트워크 영역을 통합적으로 모니터링할 수 있게 합니다. FSMC는 역할 기반 액세스 방식의 멀티유저 시스템이므로, 로그인 정보가 있는 각 사용자는 어떤 대시보드에서 필요한 정보를 제공하는지 판단할 수 있습니다. 이 대시보드는 사용자가 어디서 로그인하더라도 랜딩 페이지가 될 수 있습니다.

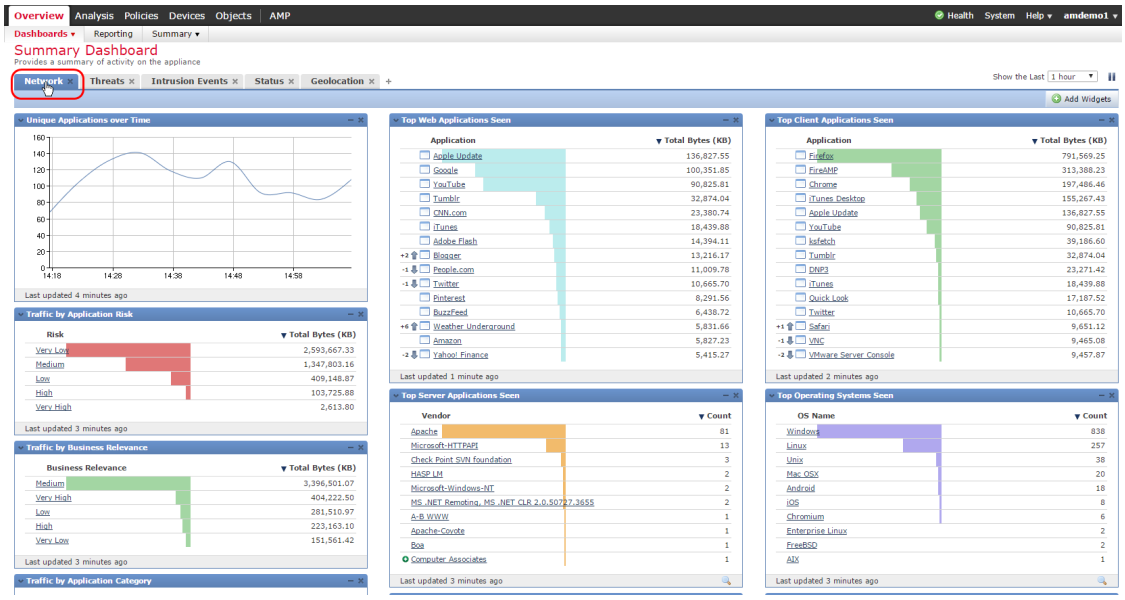
요약 대시보드는 네트워크 및 애플리케이션을 종합적으로 조명하고 확인된 위협을 집중 분석할 수 있게 하므로 훌륭한 출발점이 됩니다. 새로운 사용자에 대한 기본 랜딩 페이지입니다.

단계

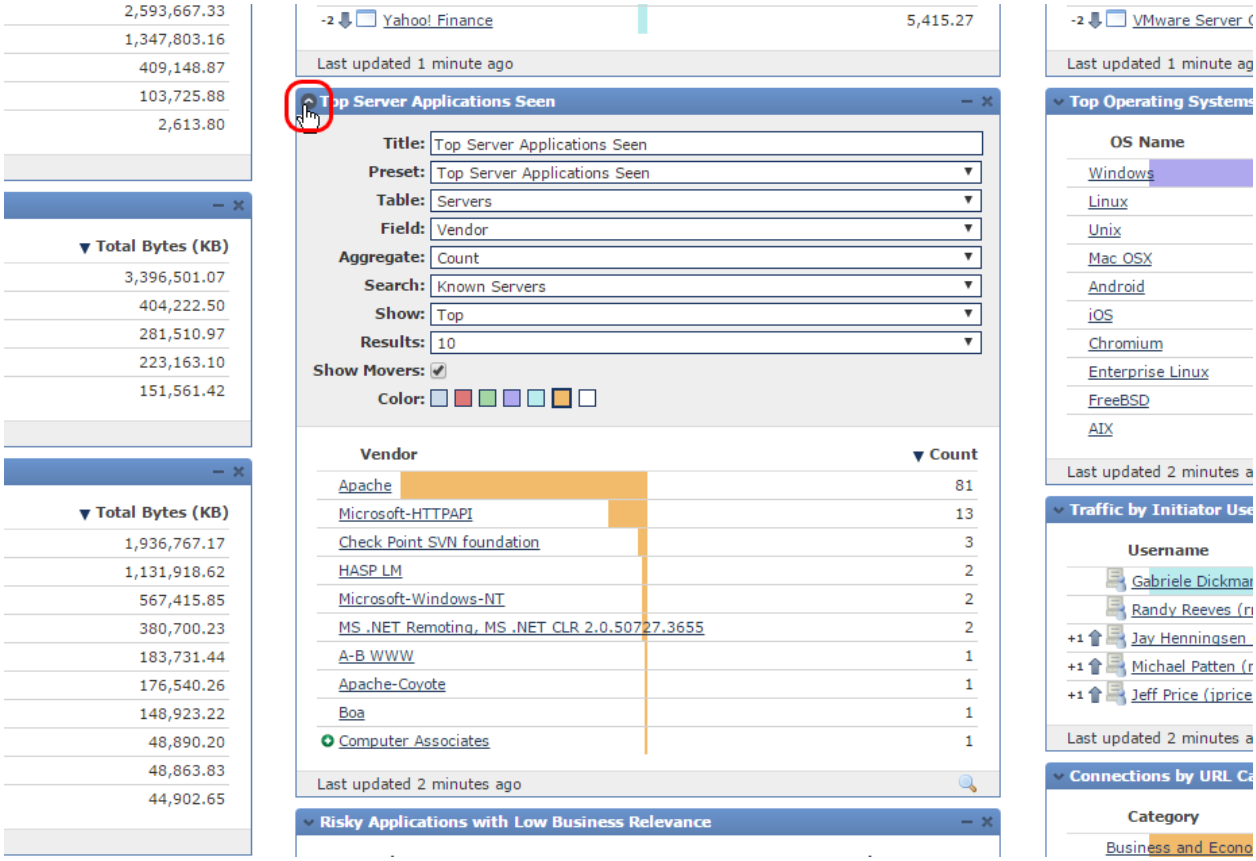
1. 요약 대시보드 탐색 - 맨 위에서 **Overview(개요)**를 클릭하고 **Dashboards(대시보드)**, **Summary Dashboards(요약 대시보드)**를 차례로 선택합니다. 화면이 로드되면 **Network(네트워크)** 탭이 선택되어 있습니다.



이 대시보드에서는 위젯을 볼 수 있는데, 위젯은 거의 모든 유형의 정보를 한눈에 볼 수 있게 해줍니다. 각 대시보드와 위젯은 완전히 맞춤화할 수 있습니다. 특정 이벤트 정보를 들여다보는 데에도 사용할 수 있습니다. 예를 들어 사용량이 많은 사용자나 애플리케이션에 대한 트래픽을 보려는 경우 사용자 이름 또는 애플리케이션을 클릭하여 추가 정보를 표시할 수 있습니다.



Top Server Application Seen(확인된 상위 서버 애플리케이션) 위젯의 왼쪽 위에 있는 작은 화살표를 클릭합니다 이 기본 설정 버튼을 클릭하면 위젯에 표시할 결과 수, 그래프 색상, 사용할 데이터 세트까지 여러 옵션을 설정할 수 있습니다. 이 dCloud 데모에서는 데이터 세트를 변경하지 마십시오. 이 계정을 사용하는 모든 데모에 영향을 줍니다. 또한 화면에서 위젯을 끌어 원하는 위치에 놓는 방법으로 각 대시보드의 레이아웃을 변경할 수 있습니다.



Threats(위협) 탭으로 이동합니다. 이 탭은 악성 트래픽 및 파일에 초점을 맞추므로 매우 유용합니다. 이 탭을 활용하여 어떤 시스템이 감염되었을 가능성이 있는지 확인할 수 있습니다.

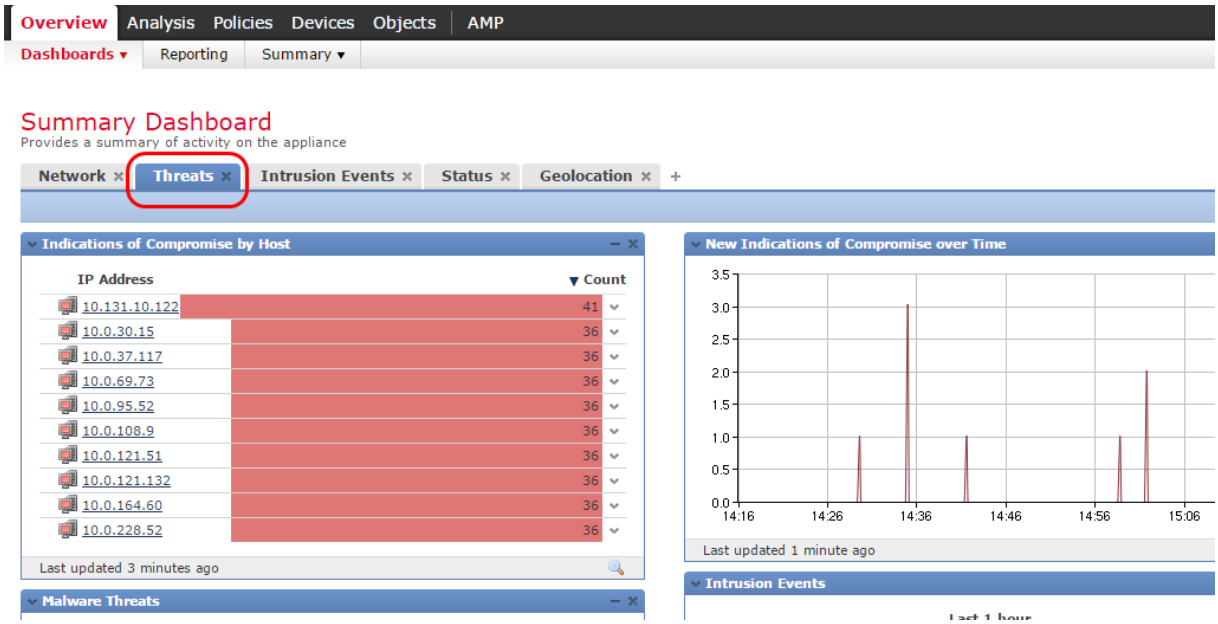
Threats(위협) 탭은 다음 정보를 표시합니다.

Malware Threats(악성코드 위협): 보안 어플라이언스에서 또는 엔드포인트 에이전트로 실행 중인 AMP가 어떤 악성코드 파일을 탐지했습니까?

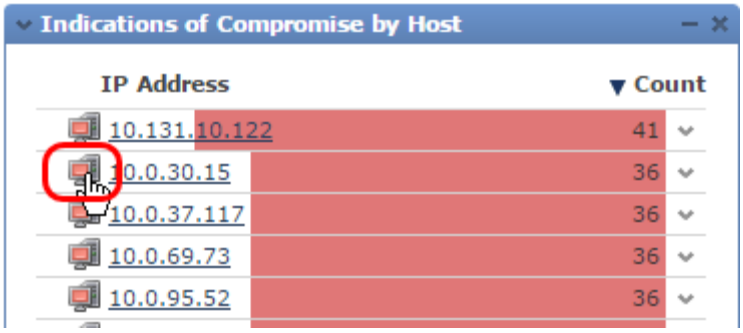
Intrusion Events, by Impact Level(침입 이벤트, 영향 레벨 기준): 다른 방식으로는 허용되었을 트래픽 유형이지만 Snort에서 탐지한 공격은 무엇입니까?

Connections and Traffic by Security Intelligence Category(보안 인텔리전스 카테고리별 연결 및 트래픽): 이전 시나리오에서 설명한 대로, 소스 또는 대상 IP 주소를 기준으로 할 때 어떤 악성 트래픽 카테고리가 네트워크에서 확인되었습니까?

Indications of Compromise(보안 침해 지표): 어떤 호스트가 감염의 원인이 되었을 만한 활동에 참여했습니까? 대개 악성코드 파일 액세스와 같은 행동이 해당됩니다.



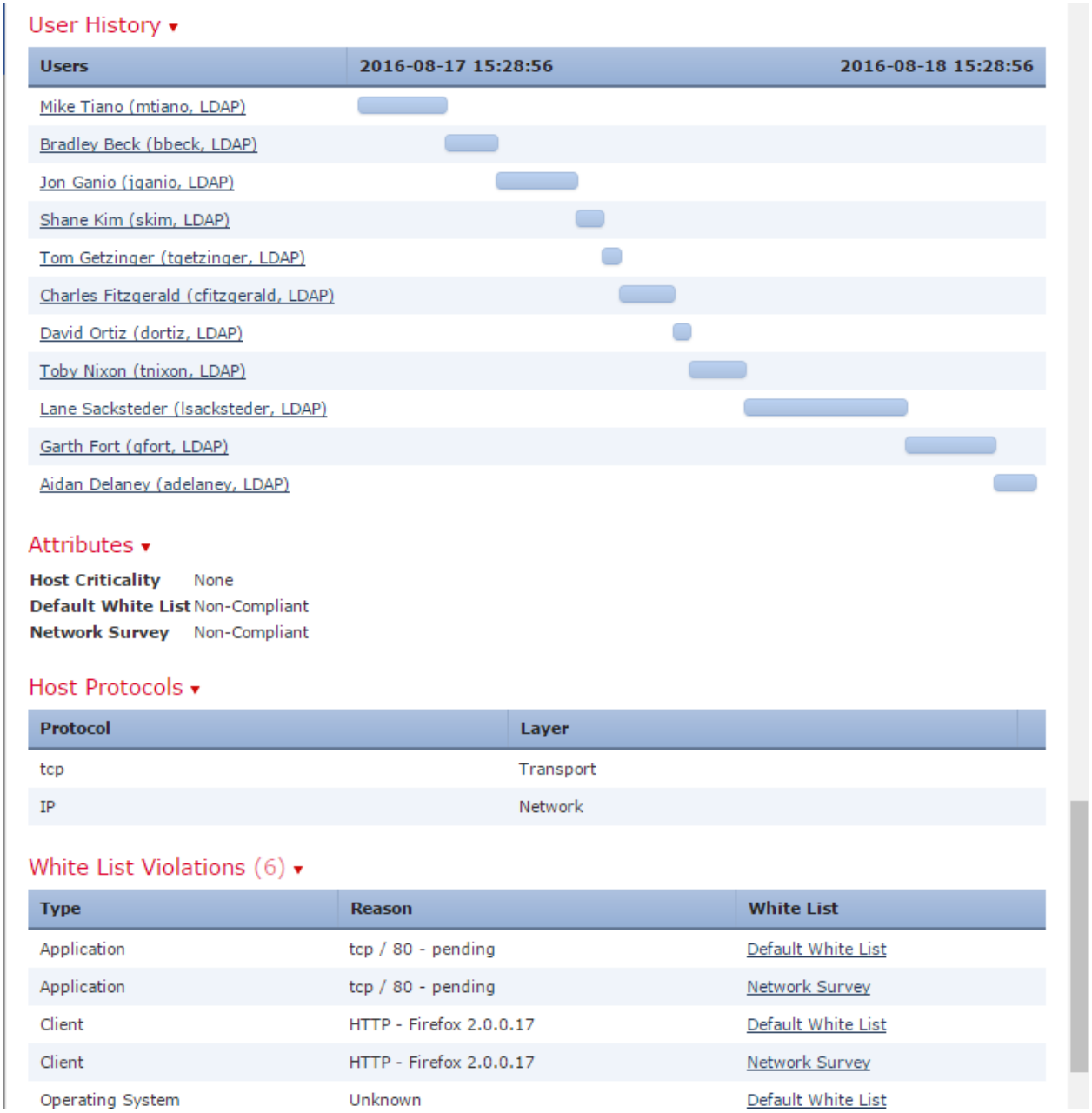
Threats(위협) 탭에서는 보안 침해 지표가 있는 호스트에 대한 추가 세부 정보를 쉽게 얻을 수 있습니다. IP 주소 중 하나의 옆에 있는 빨간색 호스트 아이콘을 클릭하면 호스트 프로파일이 표시됩니다.



새 창이 열립니다. 이 새 창에서 현재 디바이스에 로그인한 사용자를 포함한 여러 정보를 확인할 수 있습니다. 호스트와 관련된 어떤 IoC도 확인할 수 있습니다.

더 아래로 스크롤하면 운영 체제 정보, 사용 중인 애플리케이션 등도 알 수 있습니다.

계속 아래로 스크롤하면 지금까지 이 디바이스에 로그인했던 사용자의 기록까지 볼 수 있습니다.



요약

Cisco FSMC는 사용하기 편리하면서 강력한 대시보드를 제공하며, 네트워크 또는 보안 관리자는 이를 통해 네트워크에서 실행 중인 애플리케이션과 위협을 제대로 이해할 수 있습니다. 대시보드에 표시되는 정보는 정책 엔진 내에서 네트워크 정책 시행에 활용하면서 업계에서 가장 강력하고 정확한 차세대 보안 시스템을 실현할 수 있습니다.

차세대 방화벽 정책 생성

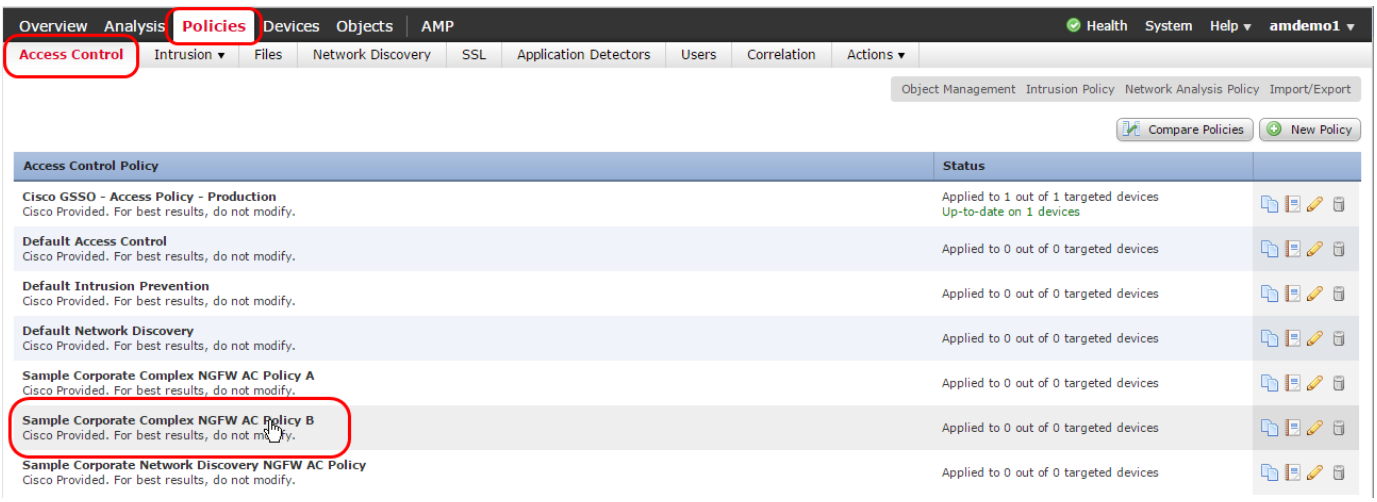
처음 두 시나리오는 가시성 및 보고에 중점을 두었습니다. 이 시나리오는 차세대 정책을 시행하는 방법을 소개합니다. 일반적인 보안 어플라이언스는 IP 주소, 프로토콜, 포트를 기준으로 삼아 트래픽을 시행합니다. 차세대 보안 어플라이언스는 이와 동일한 기능뿐 아니라 상황 기반 정보도 제공합니다. Cisco의 차세대 보안 어플라이언스는 다음을 비롯한 여러 추가 특성을 기준으로 한 정책을 지원합니다.

- 지리적 위치
- VLAN
- Active Directory 내 사용자 이름 또는 그룹
- 애플리케이션 또는 클라이언트 애플리케이션
- URL 카테고리 및 평판
- 보안 그룹 태그
- 네트워크 디바이스 유형

Cisco 차세대 보안 정책은 트래픽 허용 또는 차단과 같은 기존의 제어 기능 외에도 정밀하게 튜닝된 IPS 정책, SSL 해독, AMP 정책을 액세스 제어 전반에 적용할 수 있도록 지원합니다.

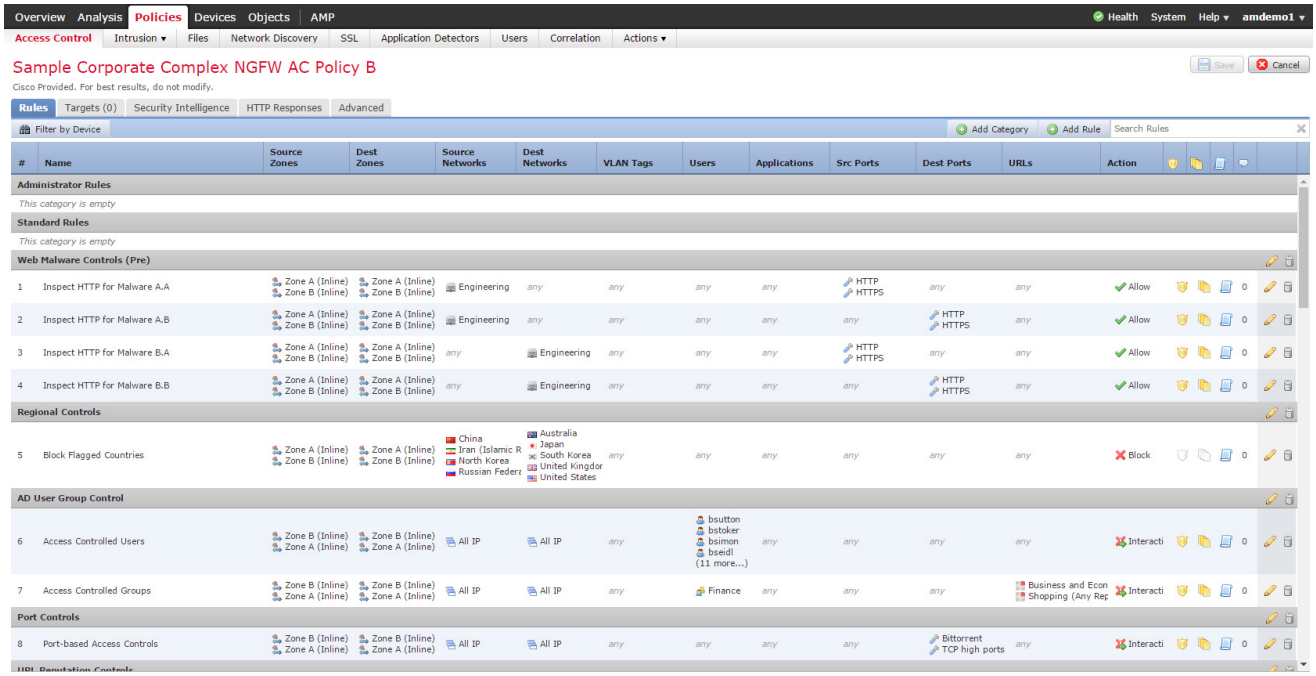
단계

1. 기존 정책에 규칙 추가 - 먼저 맨 위 바에서 **Policies(정책)**를 클릭합니다. 그러면 기본 정책 유형, 즉 **Access Control(액세스 제어)** 정책으로 이동합니다. 목록에서 미리 정의되고 완전히 입력된 정책인 **Sample Corporate Complex NGFW AC Policy B**를 선택합니다.

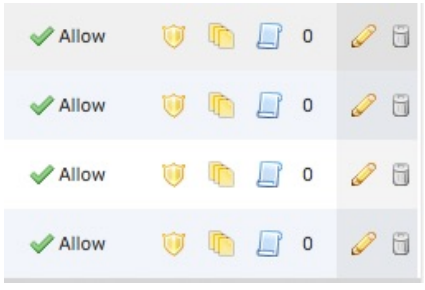


이 샘플 규칙에서는 다음과 같이 여러 제어 유형을 제공합니다.

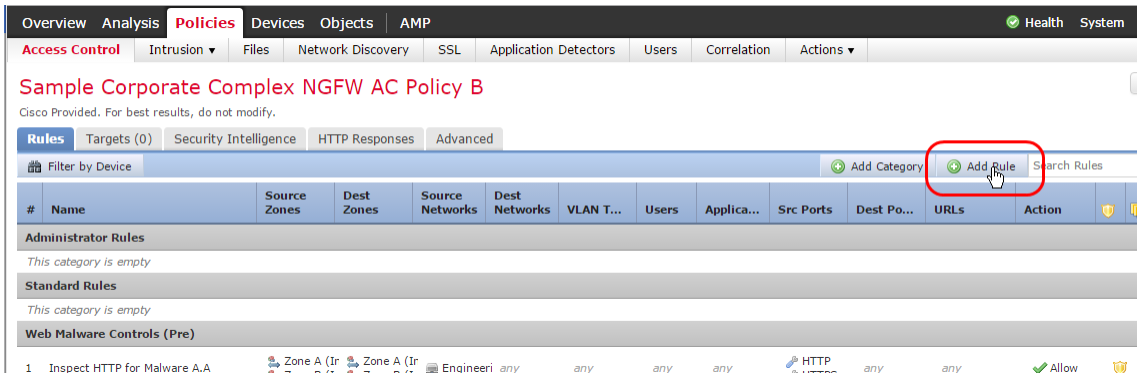
- 포트 및 프로토콜 기반 규칙
- 애플리케이션 전용 규칙
- 사용자 기준 규칙(규칙 또는 27)
- URL 카테고리 필터링 규칙
- 지리위치 규칙



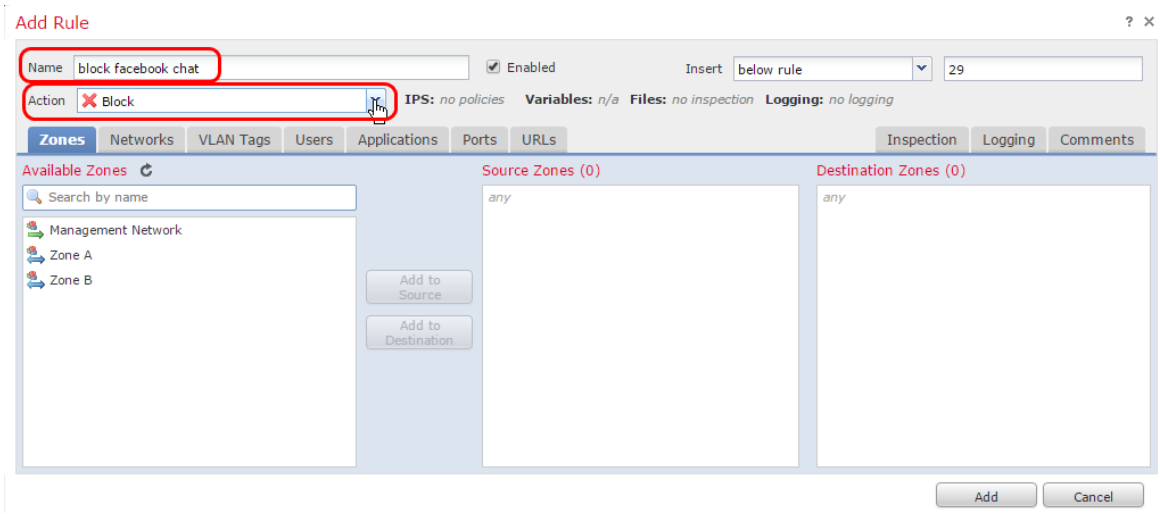
화면의 오른쪽에 주목하십시오. 규칙에 따라 트래픽이 허용되거나 차단되는지 쉽게 확인할 수 있습니다. 또한 **노란색 방패**는 침입 정책임을, **서류더미**는 파일 정책임을 나타냅니다.



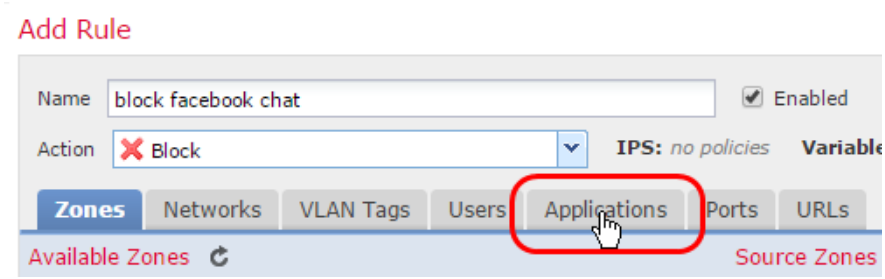
이 정책을 살펴봤으니 규칙을 추가해보겠습니다. 화면 오른쪽에서 **Add Rule(규칙 추가)**을 클릭합니다.



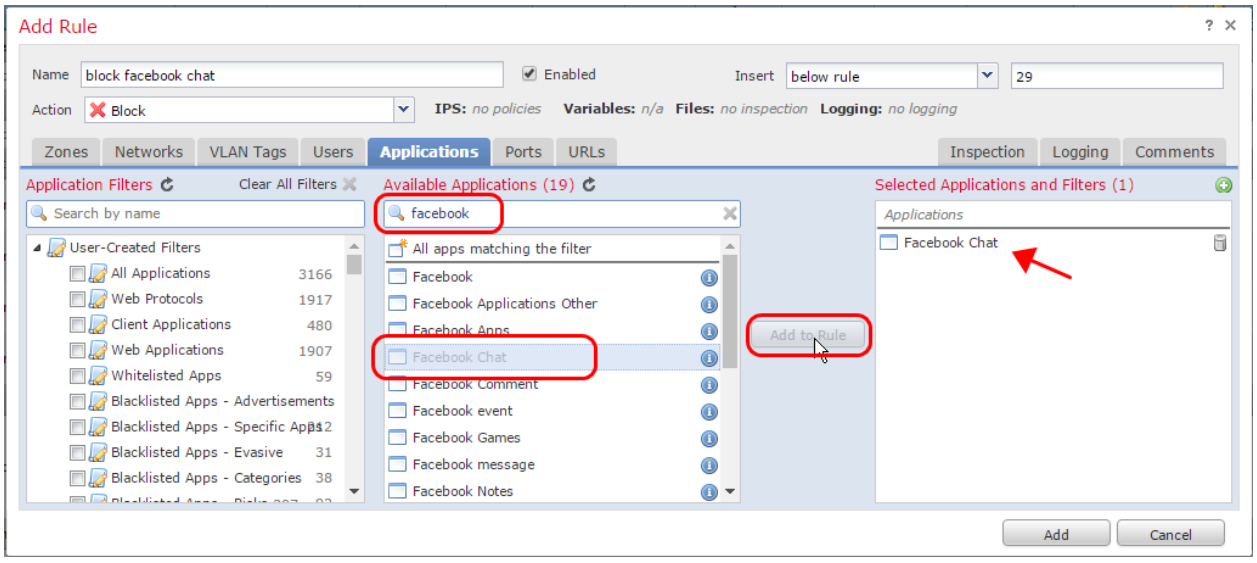
규칙의 이름을 **block facebook chat**로 지정하고 작업을 **Block(차단)**으로 설정합니다.



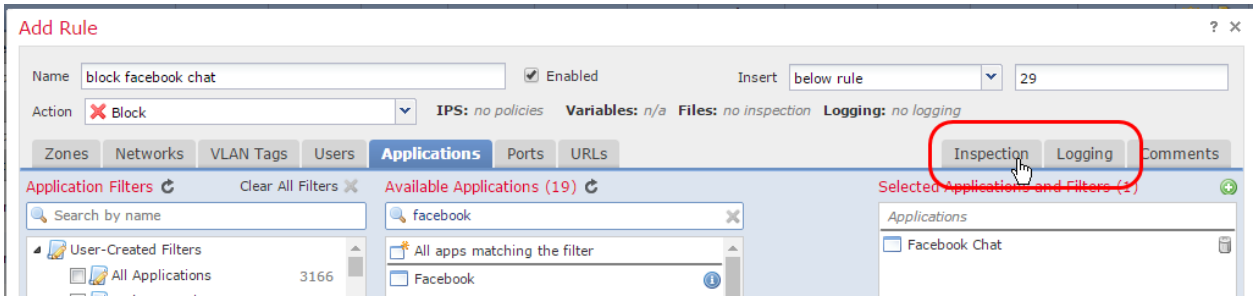
Applications(애플리케이션) 탭을 선택하여 새 규칙을 애플리케이션 규칙으로 만들어보겠습니다.



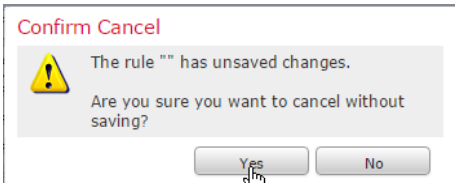
Available Applications(사용 가능 애플리케이션) 필드에 **facebook**이라고 입력합니다. 그러면 Facebook 애플리케이션의 유형만 표시하도록 필터링됩니다. **Facebook Chat(Facebook 차트)**를 선택하고 **Add to Rule(규칙에 추가)**을 클릭합니다.



이제 이 정책이 적용되는 모든 어플라이언스에서 Facebook 차트를 차단하는 규칙이 생성되었습니다. 필요하다면 창 오른쪽의 Inspection(검사) 및 Logging(로깅) 탭을 사용하여 검사 기능을 추가하고 규칙 실행 시점을 로깅할 수도 있습니다. 차단 중인 트래픽을 검사하는 것은 합당하지 않습니다. 그러나 허용 규칙을 새로 설정했다면 악성코드 검사가 필요할 것입니다.



편리하게 차세대 방화벽 규칙을 생성할 수 있음을 확인했으므로 **Cancel(취소)**을 클릭하고 이 변경 내용을 취소하겠습니다.



요약

Cisco FireSIGHT, Firepower Threat Defense, Cisco ASA with Firepower Services 모두 강력하고 편리한 차세대 보안 솔루션으로 고객에게 최고 수준의 보호를 제공합니다. FireSIGHT Management Center는 관리 컴퓨터에서 클라이언트 애플리케이션, 플러그인, Java 요구 사항을 충족해야 하는 부담 없이 중앙의 단일 인터페이스에서 모든 Firepower 기술을 관리하고 보고할 수 있도록 지원합니다.

FSMC는 네트워크의 보안 및 가시성을 크게 향상시킬 뿐 아니라 관리의 오버헤드를 줄입니다.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.