Lancope®

Lancope가 이제 Cisco 의 회사가 되었습니다.

Cisco Stealthwatch

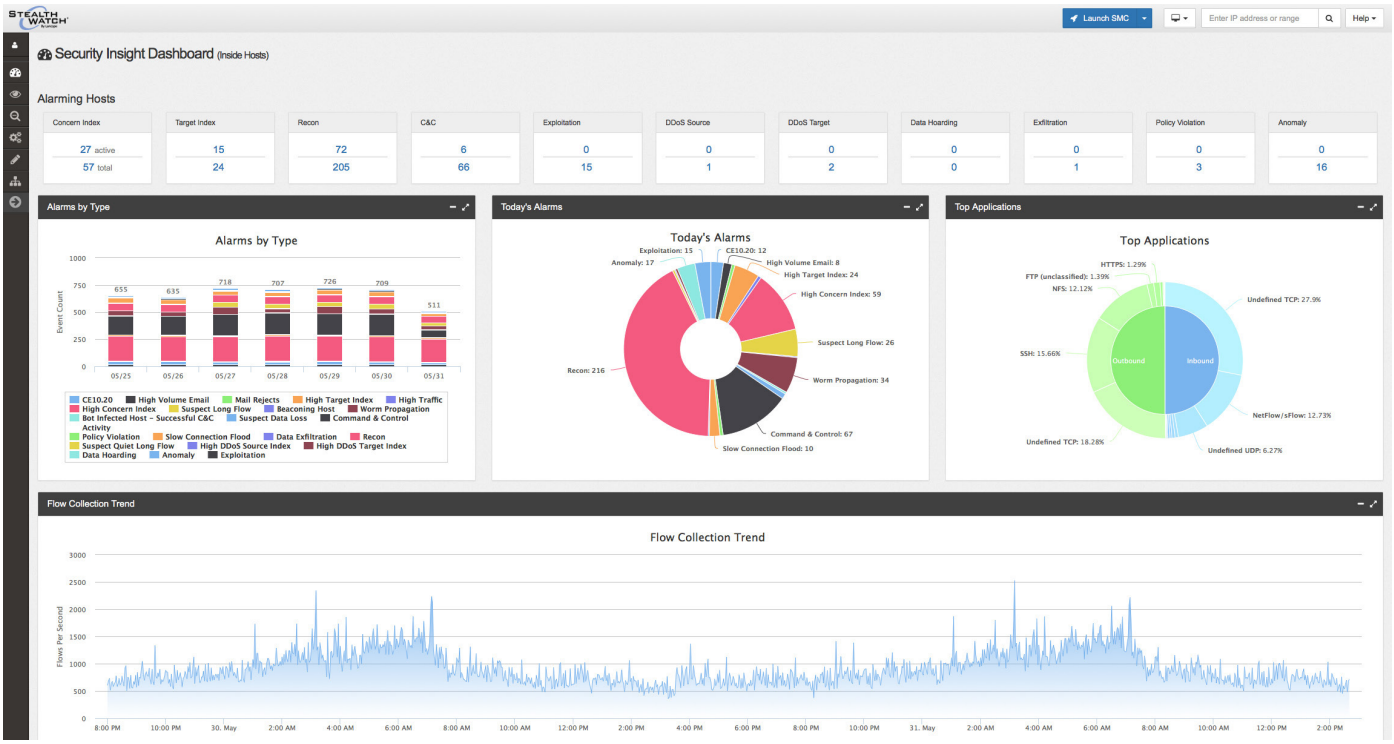
6.8의 새로운 기능

Cisco Stealthwatch는 향상된 위협 탐지, 사고 대응 및 포렌식을 위해 심층적인 네트워크 가시성을 제공합니다. Stealthwatch 6.8의 새로운 기능은 사용자 경험과 알람 정확도를 대폭 개선합니다. 이제 고객은 새로운 Cloud License와 Cisco TrustSec과의 추가 통합을 통해 확장된 가시성 및 보안 상황을 확보할 수 있습니다.

"Stealthwatch System v6.8의 기능은 알람 정확도를 대폭 향상하고, 사용자 경험을 개선하며 클라우드 및 Cisco TrustSec 통합을 통해 가시성을 확대합니다."

새로운 기능:

- Cisco Stealthwatch™ Cloud License - 클라우드에 대한 포괄적인 가시성 확장
- Cisco TrustSec 통합 - 보안 상황 확장
- 저작권 침해 대시보드 - 위험한 파일 공유를 정확히 찾아내도록 지원
- 시스템 알람 개선 - 인사이트 향상 및 알람 정확도 개선
- Flow Collector 5020 사용 가능



Stealthwatch 6.8은 향상된 위협 탐지, 사고 대응 및 포렌식을 위해 새로운 수준의 네트워크 가시성 및 보안 상황을 제공합니다.

Cisco Stealthwatch™ Cloud License - 클라우드에 대한 포괄적인 가시성 확장

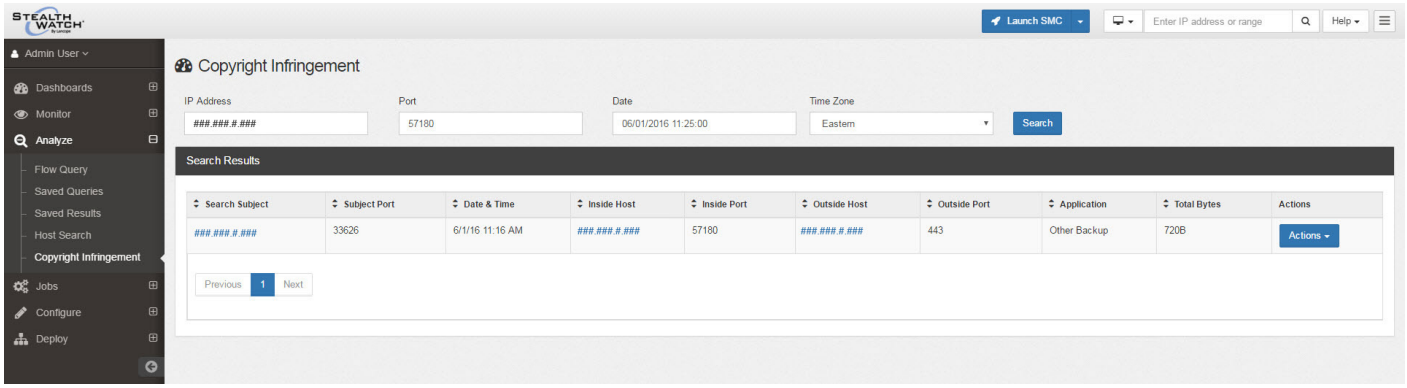
클라우드 환경은 네트워크를 표적으로 삼는 잠재적인 보안 위협에 대해 새로운 기회를 창출합니다. 새로운 Cisco Stealthwatch Cloud License는 퍼블릭, 프라이빗, 하이브리드 클라우드 환경에 대한 포괄적인 가시성을 제공하여 네트워크 사각지대를 줄입니다. Cloud License는 Stealthwatch에 사용하는 가상 애드온으로, 사용자는 Cloud License를 사용하여 기존 네트워크와 같이 클라우드에서 텔레메트리를 수집할 수 있습니다. 클라우드 데이터는 클라우드에서 지속적인 탐지 및 대응 기능을 제공하면서 물리적 네트워크에서 NetFlow와 동일한 검사를 거칩니다. Cloud License는 고객이 클라우드에서 NaaS(Network as a Security Sensor) 및 NaaE(Network as an Enforcer)의 사용 범위를 확장하도록 지원합니다. Stealthwatch Cloud License가 있으면 퍼블릭, 프라이빗 및 하이브리드 클라우드 환경에서 Cisco Stealthwatch의 모든 네트워크 가시성, 위협 탐지 및 분석 기능을 이용할 수 있습니다. Cloud License가 있는 Stealthwatch를 사용하여 물리적, 가상 및 클라우드를 비롯한 모든 환경에서 단일 보기를 통해 위협을 모니터링할 수 있습니다. 이렇게 확장된 가시성을 통해 실시간 위협 탐지, 포렌식 조사, 사고 대응 및 규정 준수를 크게 개선할 수 있습니다.

Cisco TrustSec 통합 - 보안 상황 확장

Cisco TrustSec 기술은 소프트웨어 정의 세그멘테이션을 사용해 네트워크 액세스 프로비저닝을 간소화하고, 보안 운영을 가속화하며, 네트워크의 어느 곳에서나 일관된 정책을 시행합니다. Stealthwatch Flow Sensor는 정책 시행을 위해 TrustSec에서 사용하는 역할 기반 분류인 SGT(Security Group Tag)를 캡처할 수 있습니다. 이 새로운 기능은 네트워크 및 사용자 활동이 정상적인지 또는 의심스러운지를 판단하기 위해 Stealthwatch에 추가 상황 레이어를 제공합니다. 또한 Stealthwatch를 통한 정책 기반 모니터링은 TrustSec 사용자가 TrustSec 구축을 최대한 활용할 수 있도록 정책을 더욱 정확하게 시행하고 업데이트하도록 지원할 수 있습니다.

저작권 침해 대시보드 - 위험한 파일 공유를 정확히 찾아내도록 지원

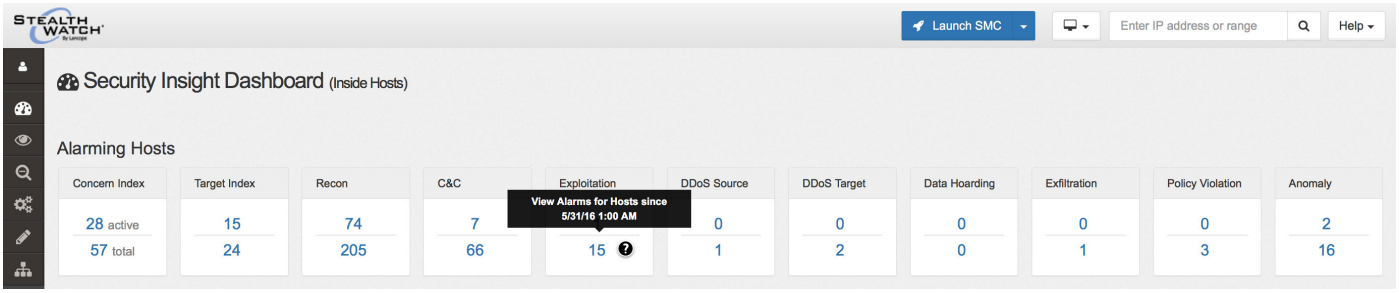
Copyright Infringement Dashboard(저작권 침해 대시보드)를 통해 Stealthwatch 관리자는 네트워크 사용자가 저작권으로 보호되는 자료를 다운로드하거나 배포하기 위해 연결한 호스트 IP 주소를 식별할 수 있습니다. 이 대시보드를 통해 관리자는 저작권 침해 쿼리를 구축 및 실행하고 쿼리 결과를 확인하여 이전 쿼리를 검사할 수 있습니다. 이러한 인사이트는 조직이 비용이 많이 드는 저작권 침해 소송 및 벌금을 피하도록 돕는 데 있어 가장 중요합니다.



Copyright Infringement Dashboard(저작권 침해 대시보드)는 저작권으로 보호받는 자료의 불법 배포 사실을 조사하는 데 드는 시간을 줄여줍니다.

시스템 알람 개선 - 인사이트 향상 및 알람 정확도 개선

Stealthwatch 알람의 정확성과 정확도를 개선하기 위해 Management Console(관리 콘솔) 인터페이스에 여러 가지 보안 이벤트 카테고리가 재구성되었습니다. 이전에는 일부 보안 이벤트만 직접 알람을 시작할 수 있었습니다. 이제는 모든 이벤트에서 직접 알람을 시작하도록 맞춤 설정할 수 있습니다. 따라서 사용자는 알람 통지를 조정하는 옵션을 통해 네트워크 환경 내 노이즈를 줄일 수 있습니다. 다른 Stealthwatch 알람 개선 사항을 통해 사용자는 웹 인터페이스에서 각 보안 카테고리에 대한 총 알람 수를 확인할 수 있습니다. 사용자는 이 기능을 사용하여 알람 유형에 따라 필터링된 결과를 확인할 수 있습니다. Stealthwatch 6.8은 바쁜 보안 팀이 잠재적으로 중요한 문제를 간과하지 않도록 보안 알람에 대한 이력 보기를 제공합니다. 이력 알람 데이터를 사용하면 시간 경과에 따른 카테고리별 알람 트렌트를 분석할 수 있어 상황에 대한 인식 수준을 높이고 반복적인 공격 패턴을 완화하는 데 도움이 됩니다.



알람 호스트 섹션에서 사용자는 각 보안 범주에 대한 총 알람 수를 확인할 수 있습니다.

Flow Collector 5020 사용 가능

새로운 Cisco Stealthwatch Flow Collector 5020은 Cisco UCS 플랫폼에서 사용 가능한 최초의 Stealthwatch 어플라이언스입니다. Flow Collector 5020은 확장성이 뛰어나고 대규모 엔터프라이즈 구축을 위한 대량의 스토리지 기능을 갖추고 있습니다. 어플라이언스는 초당 최대 240,000개의 플로우를 처리할 수 있으며 최대 보안 성능을 위해 최대 6TB의 데이터를 저장할 수 있습니다.

추가 개선 사항

- Stealthwatch 사용자 경험을 개선하기 위해 관리 콘솔 웹 애플리케이션 대시보드에 여러 개선 사항과 새로운 기능이 추가되었습니다.
- 고객은 이제 용량 요구사항을 기준으로 다양한 크기의 Flow Sensor Virtual Edition 모델을 구매할 수 있습니다.

자세히 보기. 데모 요청.

stealthwatch-customersuccess@cisco.com