Cortex Copilot

최고의 SecOps 도우미, Cortex Copilot으로 더 스마트하게 보안 유지

보안 운영(SecOps) 팀은 끊임없이 진화하는 디지털 환경을 보호하는 임무를 맡고 있습니다. 위협 환경의 역동적인 특성과 제한된 리소스는 항상 공격자보다 한 발 앞서야 하는 SecOps 팀에게 많은 과제를 안겨줍니다. 이러한 문제에는 긴 조사 시간, 새로운 기술에 대한 가파른 학습 곡선, 위협 헌팅에 필요한 고급 기술 등이 포함됩니다.

SecOps 팀의 과제

조사에 너무 많은 시간 소요

보안 분석가의 기술 수준에 따라 사고를 조사하고 완벽하게 대응하는 데 걸리는 시간이 크게 달라집니다. 사고 세부 정보가 한곳에서 제공되는 경우에도 분석가는 조사할 사고를 파악하고, 제공되는 정보를 해석한 다음 적절한 대응 조치를 결정해야 합니다. 이는 특히 신입 분석가에게 부담이 될 수 있으며, 사고의 세부 사항과 영향을 완전히 이해하는 데 걸리는 시간을 상당히 연장시킵니다. 숙련된 분석가라도 기존의 조사 기법으로는 여러 곳에서 세부 정보를 수집하고 수동 분석을 수행해야 합니다.

가파른 학습 곡선

모든 기능을 갖춘 보안 제품은 특히 새로운 분석가가 합류할 때 보안 팀에 가파른 학습 곡선을 초래하는 경우가 많습니다. 이는 제품의 효과적인 구현과 활용을 방해하여 고급 보안 기능을 충분히 활용하지 못하게 할 수 있습니다. 이는 또한 온보딩 프로세스에 영향을 미치고 조사 시간을 늦추며 궁극적으로 조직의 전반적인 보안 태세에 영향을 미칠 수 있습니다.

고도의 기술이 필요한 위협 헌팅

효과적인 위협 헌팅에 필요한 숙련도 수준이 지나치게 높아서 선제적 위협 탐지를 수행할 수 있는 능력은 가장 숙련되고 경험이 풍부한 분석가에게만 제한되어 있습니다. 위협 헌팅은 일반적으로 위협 행위자 TTP에 대한 깊은 이해가 필요하며 분석가가 사용자 지정 쿼리를 작성하고 포렌식 분석을 수행하며 보안 도구의 기능을 완전히 이해하는 능력에 의존합니다. 이는 보안 분석가의 기술적 진입 장벽을 높이고 궁극적으로 조직이 환경의 지능형 위협이 더 심각한 문제로 발전하기 전에 선제적으로 식별하는 능력을 저해합니다.

Cortex Cloud 소개

SecOps에서 분석가는 공격자보다 한 발 앞서 나가기 위해 가능한 모든 이점을 활용해야 합니다. Cortex® Copilot은 보안 분석가가 수행하는 일상적인 업무의 모든 단계를 지원하는 고급 SecOps 도우미입니다. 신규 사용자든 숙련된 사용자든, Cortex Copilot은 분석가에게 컨텍스트와 단계별 지침을 제공하여 더 빠르게 움직이고, 더 신속하게 사고를 해결하고, 새로운 위협에 앞서 대응할 수 있도록 도와줍니다.

Cortex 플랫폼 내에서 바로 사용할 수 있는 Cortex Copilot은 자연어와 사용자 친화적인 인터페이스를 사용하여 분석가가 정보를 수집하고 보안 조치를 취하는 방법을 단순화하고 가속화합니다. 이 솔루션은 머신 러닝을 적용하여 분석가가 머신 같은 속도로 보안 운영을 탐색할 수 있도록 지원하는 Palo Alto Networks Precision AI™ 기술로 강화된 Cortex 플랫폼의 고급 보안 기능을 기반으로 합니다. 자연어 상호 작용을 사용하면 별도의 목록을 클릭하거나 대시보드 간에 전환할 필요가 없으므로 분석가에게 필요한 정보를 필요할 때 정확하게 제공할 수 있습니다. 제품 설명서 이해와 같은 일반적인 활동부터 위협 대응이나 헌팅과 같은 고급 작업까지, Cortex Copilot은 분석가가 더 신속하게 학습하고 더 빠르게 움직일 수 있도록 도와줍니다.

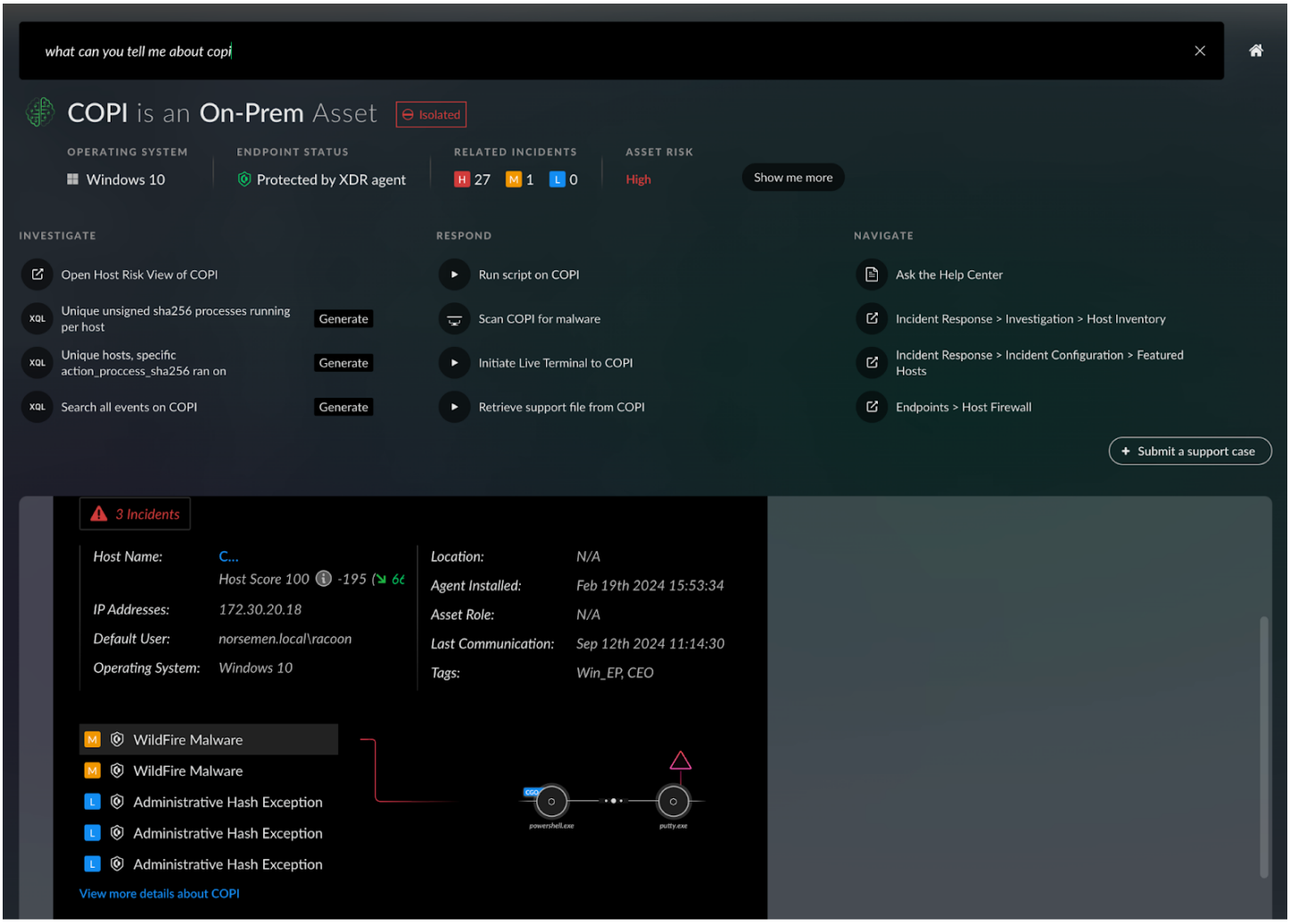

그림 1: 사용하기 쉬운 인터페이스를 통해 보안 운영 분석가의 일상적인 작업을 지원하는 Cortex Copilot

분명한 이점

빨라진 조사 속도

분석가는 플랫폼의 어느 곳에서나 Cortex Copilot에 신속하게 액세스하여 새로운 사고를 검토하고, 영향을 받는 시스템과 사용자를 조사하고, 보기 간에 이동하지 않고도 침해 지표를 식별할 수 있습니다. 위협 인텔리전스로 사고 세부 정보를 자동으로 보강하고 시스템 격리 또는 악성 파일 삭제와 같은 대응 조치를 제안하여 평균 해결 시간(MTTR)을 단축합니다.

조사의 일환으로 분석가는 시스템에서 실행 중인 모든 프로세스를 확인하고자 할 수 있습니다. 일반적으로 이러한 세부 정보를 수집하려면 터미널을 통해 시스템에 연결하거나 여러 명령을 실행하거나 특정 쿼리를 작성해야 합니다. 하지만 Cortex Copilot은 이 작업을 쉽게 해줍니다. 클릭 한 번으로 Cortex Copilot이 자동으로 쿼리를 작성하고 호스트에서 실행 중인 프로세스의 결과를 반환합니다.

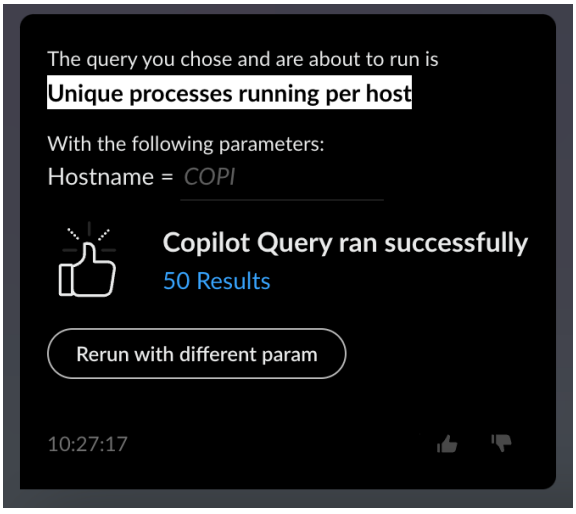

그림 2: Cortex Copilot에 대한 쿼리 예시

분석가 워크플로 최적화

Cortex Copilot은 상황에 맞는 정보와 조치를 제공하여 분석가의 효율성을 높이고 플랫폼의 기능 사용을 최적화합니다. 분석가는 지원 문서를 검색하는 대신 도움말 센터에서 요약된 정보에 빠르게 액세스할 수 있으므로 학습 곡선이 완만해지고 신규 분석가는 복잡한 조사에 집중하여 사람의 개입이 필요한 위협에 현명하게 시간을 사용할 수 있습니다.

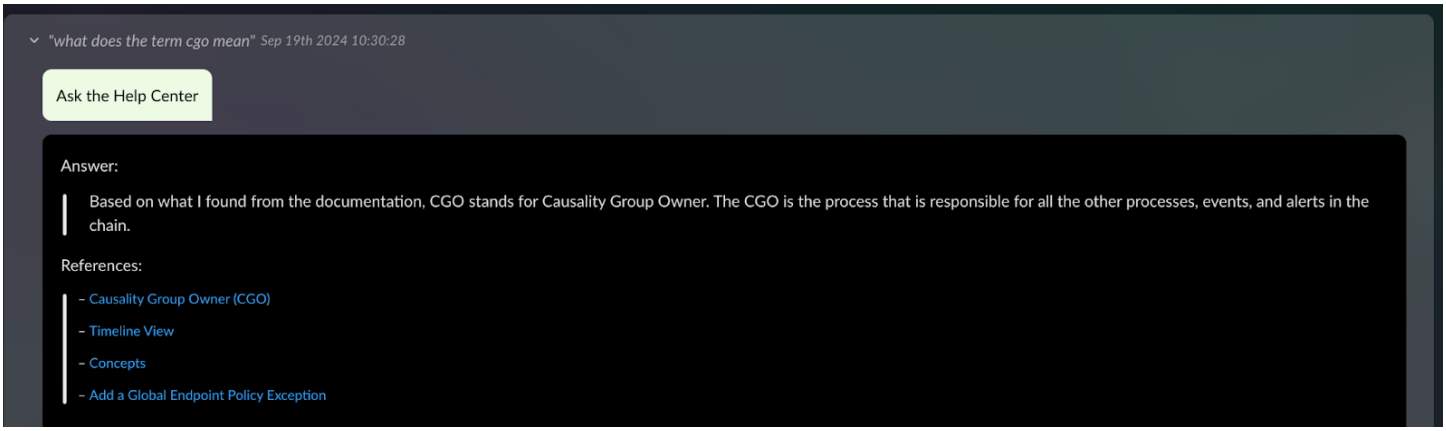

그림 3: Cortex Help Center에 대한 쿼리 예시

이 예에서 분석가는 인과 관계 사슬을 살펴볼 때 'CGO'라는 용어를 접하지만 익숙하지 않은 상황입니다. 분석가가 Cortex Copilot에게 이 용어의 의미를 묻습니다. 분석가가 더 자세히 알아보려는 경우 Cortex Copilot이 Cortex 지원 센터에서 설명과 추가 참조 자료를 제공합니다.

위협 헌팅의 민주화

Cortex Copilot을 사용하면 다양한 기술 수준의 분석가들이 데이터 소스 전반에서 검색을 간소화하고 결과에 따라 헌팅 작업을 안내하여 철저한 위협 탐지를 수행할 수 있습니다. 분석가의 입력을 제품 작업에 통합하여 쿼리 실행(예: 호스트에서 실행된 고유 해시 찾기), 인과관계 사슬 조사, 위협 인텔리전스로 강화된 구성 자산의 추출된 지표 보기, 보안 보호 개선 등 다양한 작업을 수행할 수 있어 분석가가 지능형 위협을 발견하고 보안 효과를 높일 수 있습니다.

위협 헌터는 위협 헌팅 프로세스의 일부로 여러 사용자가 동일한 시스템에 로그인을 시도하는지 확인하려고 할 수 있습니다. Cortex Copilot은 이 정보를 제공할 수 있는 XQL 쿼리를 제안합니다. 결과를 확인하기 위해 위협 헌터는 Cortex Copilot 내에서 직접 이 쿼리를 실행할 수 있습니다.

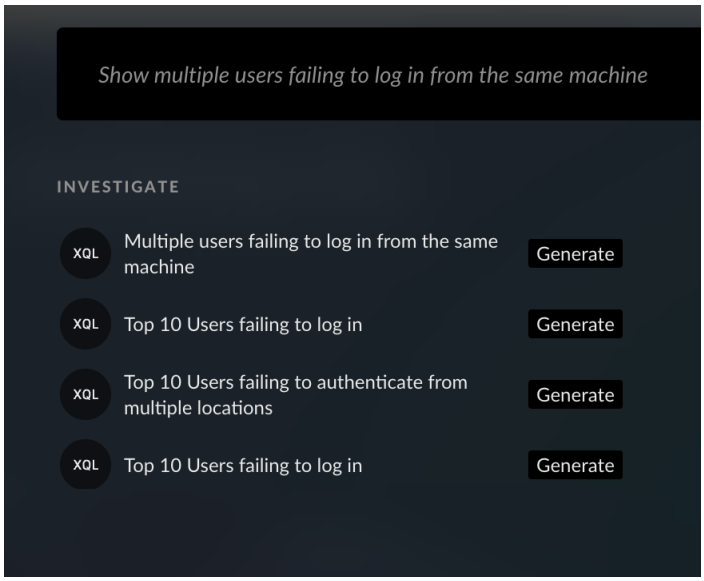

그림 4: XQL 쿼리 예시

조사, 대응 및 탐색

Cortex Copilot은 SecOps 활동을 염두에 두고 구축 및 훈련된 사이버 보안 도구로, 정보와 작업을 "조사", "대응", "탐색"의 카테고리로 구성합니다. 이는 분석가에게 효과적인 보안 운영 단계를 안내하여 조사 및 대응 시간을 단축하는 데 도움이 됩니다. Cortex Copilot은 입력 요소를 자동으로 감지하고 각 입력에 맞게 상황에 맞는 결과를 제공합니다. 끊임없이 학습하는 Cortex Copilot은 제공된 모든 대응에 대해 피드백을 요청하고, 받은 피드백을 바탕으로 결과를 개선합니다. 또한 분석가가 보안 사고를 신속하고 정확하게 조사하고 해결하여 궁극적으로 전체 MTTR을 단축할 수 있도록 설계된 맞춤형 플레이북을 권장합니다.

Copilot 프롬프트 예시

조사

- 동일한 컴퓨터에서 로그인에 실패한 여러 사용자를 표시합니다.
- 호스트별로 실행 중인 고유 프로세스를 표시합니다.
- 특정 해시에서 트리거된 모든 알림을 표시합니다.

대응

- IoC로 추가합니다.
- 멀웨어를 스캔합니다.
- 엔드포인트를 격리합니다.

탐색

- AWS CloudTrail 로그를 수집하려면 어떻게 하나요?
- 엔드포인트 > 호스트 방화벽.
- 자산 > 클라우드 인벤토리.
- Network Configuration > 네트워크 구성 > 내부 IP 주소 범위.

사용 사례

다음은 Cortex Copilot으로 할 수 있는 몇 가지 작업입니다(표 1 참조).

표 1: Cortex Copilot 기능

빨라진 조사 속도	분석가 워크플로 최적화	위협 헌팅의 민주화
• 사고 지표에 대한 상황별 인사이트입니다. • 사용 가능한 조사 경로를 제공합니다. • 맞춤형 인사이트를 통해 사고의 범위를 이해합니다. • 코파일럿 내부에서 대응 조치를 취합니다. • 관련 인과 관계 사슬을 확인합니다.	• 제품 기능에 대한 안내 및 세부 정보를 확인합니다. • 다음 조치에 대한 인사이트를 얻을 수 있습니다. • 조사, 대응 및 탐색을 위한 제품 기능을 나타냅니다. • 제품 내 지원 사례를 생성합니다. • 관련 정보, 파일 및 화면 녹화로 지원 사례를 자동으로 채웁니다.	• 해시의 지역 및 글로벌 확산에 대한 인사이트를 얻을 수 있습니다. • IoC를 검색하고 조직에 미치는 영향을 알아봅니다. • 사용자 및 호스트에 대한 정보를 얻습니다. • 복잡한 쿼리 없이 데이터를 쿼리합니다. • 코파일럿이 쿼리에 필요한 매개변수를 임베드하여 고급 데이터 쿼리를 실행합니다.

요약

세계 최대 규모의 사이버 보안 데이터 세트 중 하나를 기반으로 구축되고 SecOps 활동을 위해 특별히 구조화된 Cortex Copilot은 분석가에게 효과적인 보안 운영 단계를 안내하여 더 빠른 사고 해결을 달성할 수 있는 독보적인 위치를 점하고 있습니다. 방대한 양의 데이터에서 얻은 인사이트를 활용하고 정보를 실행 가능한 카테고리로 정리하여 Cortex Copilot은 보안 효율성을 높일 뿐만 아니라 위협 헌팅 프로세스를 민주화합니다. 사이버 위협이 계속 진화함에 따라 Cortex Copilot과 같은 도구가 있으면 큰 차이를 만들 수 있습니다. 단순히 따라잡는 것이 아니라 앞서나가는 것이 중요합니다. Cortex Copilot을 선택하고 조직이 사이버 보안에 접근하는 방식을 혁신하세요.

더 스마트하게, 더 어렵지 않게 보안을 유지하세요.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

대표 전화: +1.408.753.4000
판매 문의: +1.866.320.4788
지원 문의: +1.866.898.9087

www.paloaltonetworks.com

cortex_ds_cortex-copilot_100924