단일 플랫폼으로 모든 위협에 대응

Cortex 포트폴리오

CORTEX XDR | CORTEX XPANSE | CORTEX XSIAM | CORTEX XSOAR

Precision AI 기반 SecOps 플랫폼

Cortex® 포트폴리오는 최신 SOC(Security Operations Center)를 위한 통합 플랫폼을 제공하며, 위협 환경을 통제할 수 있는 기능을 제공하도록 설계되었습니다. 이제 SOC 팀은 풍부한 데이터와 보안 전문 모델을 사용하는 Palo Alto Networks Precision AI™ 기반 플랫폼을 통해 인공지능과 도메인 전문성이 결합된 AI 모델로 대량의 데이터를 중앙화하고 분석함으로써 탐지, 예방, 대응을 자동화할 수 있습니다.

Precision AI는 다음과 같은 강력한 AI 기능의 결합으로 고객에게 이점을 제공합니다.

- 조직 환경의 명확하고 구체적인 과거 및 현재 데이터를 인풋으로 사용하여 새로운 상황을 예측함으로써 보다 정확한 예방, 예측, 해결을 지원하는 **머신러닝**
- 방대한 양의 보안 데이터를 학습하여 실시간으로 보안 문제를 예측하고 탐지하는 예측 모델을 구현하는 **딥러닝**
- 코파일럿이 인간과 대화할 수 있도록 지원하는 **생성형 AI**로 UX 단순화, 대량의 위협 인텔리전스 요약, 평균 해결 시간 단축

신속한 플랫폼화 전환이 필요한 이유

"기업은 잡다한 여러 가지 프로세스와 솔루션에서 탈피하여 단순한 기술 스택이 아닌 중요한 비즈니스 메커니즘이자 성공의 원동력으로 연결된 플랫폼의 이점을 인식하고 신속하게 전환해야 합니다. 이를 위해 필요한 접근 방식이 플랫폼화(Platformization)이며, AI를 보호하고 활용할 수 있는 통합 솔루션이 성과를 달성하는데 필수적입니다."

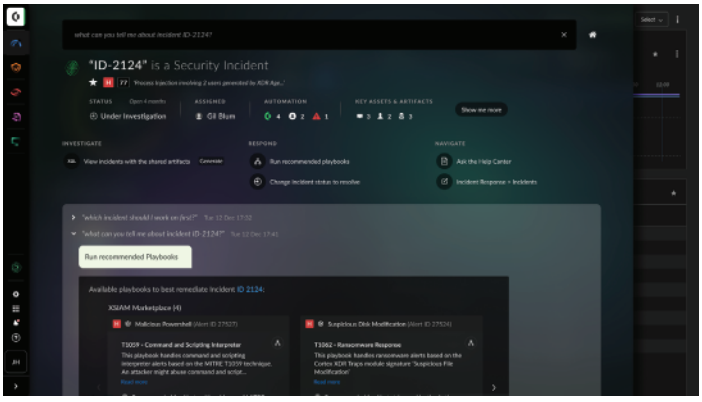
—Nikesh Arora, CEO, Palo Alto Networks

플랫폼 접근 방식을 통해 보안 환경 전반에 대한 포괄적인 가시성을 확보하고 다양한 소스의 데이터를 통합하여 효과적인 위협 식별 및 상관관계 분석이 가능합니다. 이러한 보안 플랫폼은 보안 운영을 간소화하고 효율성을 향상시켜 보안 팀이 우선순위가 높은 업무에 집중할 수 있도록 해줍니다.

보안 플랫폼은 통합 위협 인텔리전스, 분석, 자동화를 활용하여 복잡한 다단계 공격을 비롯한 다양한 위협을 신속하고 정확하게 탐지하고 대응합니다. 플랫폼화는 포인트 제품들을 수동으로 통합하고 유지 관리하는 불편을 없애고 원활한 데이터 플로우를 보장합니다. 또한 장기적인 측면에서 보안 스택을 통합하여 비용을 절감하고 전문 교육 필요성을 최소화하여 보다 경제적입니다.

Cortex Copilot: AI 어시스턴트

Cortex Copilot은 보안 운영 방식을 혁신하는 최첨단 AI 기반 어시스턴트입니다. Cortex Copilot은 보안 분석가의 일상적인 업무 전반에서 컨텍스트와 단계별 지침을 제공함으로써 더욱 신속한 작업과 사고 해결, 선제적인 최신 위협 대응을 지원합니다.



보안 분석가는 Cortex Copilot을 사용하여 사고 검토, 해당 시스템 및 사용자 조사, 침해 지표 식별을 수행하고 플랫폼 어디서나 대응 제안을 받을 수 있습니다.

Precision AI 기반 통합 보안 운영 플랫폼으로 SOC 혁신

보안 운영에 있어서 사람이 중심이 되는 기존 접근 방식은 더 이상 효과적이지 않습니다. 이러한 환경에서는 보안 분석가가 쏟아지는 알림에 압도되고 맙니다. 그리고 각각 특정 기능을 수행하도록 설계된 다양한 보안 도구들을 일일이 다뤄야 합니다. 데이터는 사일로화되고 프로세스는 수동으로 진행됩니다. 이로 인해 사고 대응이 느려지고 SOC에 영향을 미치는 모든 보안 사고에 실시간 대응이 불가능해집니다. 설상가상으로 급속히 도입되는 AI가 비즈니스에 새로운 위험을 초래합니다. 공격자들 또한 AI를 사용하여 갈수록 빠르고 광범위하며 효과적인 사이버 공격을 시도하고 있습니다.

Cortex XDR: 지능형 위협 방지, 탐지, 대응

- 엔드포인트 보안
- XDR(Extended Detection and Response)
- AI 탐지 분석
- 취약성 관리
- Identity 위협 탐지 및 대응
- 임베디드 포렌식

Cortex XDR®은 Cortex 플랫폼의 기반으로서 조직 전반의 컨텍스트를 통해 엔드포인트 및 클라우드 워크로드에 대한 세계 최고 수준의 예방, 탐지, 대응 기능을 제공합니다. XDR은 Precision AI를 사용하여 공격을 방어하고, 기계보다 빠른 속도로 탐지를 가속화하며, 경보 분류의 패러다임을 전환하여 보안 분석가가 공격자보다 앞서 나가도록 지원합니다.

Cortex XSOAR: 자동화

- 통합 케이스 관리
- 위협 인텔리전스 관리
- 멀웨어 분석 및 대응
- 신속한 침해 대응
- 네트워크 보안 운영
- SaaS, 온-프레미스 및 멀티테넌트 지원

Cortex XSOAR®은 사고 대응 관리를 위한 강력하고 유연한 SOAR 솔루션으로 보안 운영 효율성을 향상시킵니다. 모든 규모의 보안팀이 XSOAR을 사용하여 대응 워크플로우 자동화, 실시간 조사 협업, 위협 피드 관리를 실행할 수 있습니다.

Cortex Xpanse: 공격 표면 보호 및 최소화

- 공격 표면 관리 자동화
- 랜섬웨어 노출 복원
- 취약성 테스트
- 관리되지 않는 클라우드 보안
- 써드파티 공격 표면 관리
- M&A 사이버 보안 실사

Cortex Xpanse®는 공격자가 탈취하기 전에 인터넷에 연결된 자산의 위협 노출을 선제적으로 찾아내어 교정하는 고급 공격 표면 관리 솔루션입니다.

XSIAM: AI 기반 보안 운영 플랫폼

- SIEM(Security Information and Event Management)
- AI 기반 분석
- 임베디드 자동화
- 사용자 행동 분석(UBA)
- 위협 인텔리전스 관리
- 공격 표면 관리(ASM)
- 인시던트 관리
- 클라우드 보안 운영

Cortex XSIAM®은 보안 운영 간소화, 대규모 위협 차단, 사고 대응 가속화를 위해 AI를 활용하는 현대화된 SOC를 위한 AI 기반 보안 운영 플랫폼입니다. XSIAM은 EDR, XDR, SOAR, ASM, UEBA, TIP, SIEM 등 동급 최고의 보안 운영 기능을 통합합니다. XSIAM은 모든 보안 데이터를 중앙화하고 보안 전문으로 설계된 머신러닝 데이터 모델을 사용합니다.

매니지드 서비스를 위한 전문가 지원

10년 이상 멀웨어 분석으로 축적된 업계 최고의 위협 인텔리전스를 기반으로 매일 추가되는 3천만 개 이상의 새로운 멀웨어 샘플과 5천억 개의 이벤트를 처리하는 Unit 42® 전문가들이 조직이 최신 위협보다 앞서 나갈 수 있도록 지원합니다. Unit 42 MDR(Managed Detection and Response) 및 MTH(Managed Threat Hunting) 서비스는 Cortex XSIAM 또는 Cortex XDR 구독에 쉽게 추가할 수 있습니다.

AI, 분석, 자동화를 활용하여 조직의 미래를 보호하십시오

Cortex 제품(XDR, Xpanse, XSOAR) 중 하나를 선택하여 기존 보안 스택에 추가하거나, XSIAM을 통해 완전한 플랫폼화를 구현할 수 있습니다. Cortex는 조직의 보안 혁신 여정을 지원합니다. 현재 환경을 강화하고 스마트 플랜을 계획하여 내일의 보안에 대비할 수 있도록 지금 바로 Cortex가 도와드리겠습니다. QR 코드를 스캔하여 자세한 내용을 확인하세요.