전문가 기반의 미래형 보호 시스템에 의한 차세대 보안 운영

공인 MSSP는 Cortex® 플랫폼의 고급 기능을 활용하여 빠르게 진화하는 AI 기반의 위협 환경에서 항상 조직을 보호합니다.

이것이 중요한 이유는 무엇인가?

사이버 보안을 제공하고 비즈니스를 보호하는 일은 점점 더 어려워지고 있습니다. 새로운 위협 요소가 빠르게 등장하면서 보안팀은 진화하고 확장하는 위협 환경을 마주하고 있습니다. 또한 원격 근무와 IoT의 도입으로 디바이스가 급증하고 IT 환경이 분산되면서 업무 비중이 늘어나고 공격 범위가 확대되며 오탐 경보가 증가하고 있습니다. 이미 과도하게 늘어난 보안 리소스에 의해 위협에 대한 대응이 지연되고 문제 해결이 느려지며 침해 리스크가 증가합니다.

특히 기술 인력이 부족하며 전문가 확보에 높은 비용이 필요한 상황에서 더 많은 리소스를 고용하는 것은 해답이 될 수 없습니다. 기업은 이미 보유하고 있는 보안 도구와 솔루션에 더 많은 보안 도구를 추가하여 비용과 복잡성, 통합 문제를 더욱 키우기보다는 하나로 통합된 시스템을 원합니다.

패러다임의 전환이 필요한 시점입니다. 기업은 보안 작업과 모니터링, 프로세스를 자동화하고 위협의 선제적 평가 및 해결을 지속할 수 있는 혁신적이며 현대적인 보안 운영 센터(SOC)를 구축하는 것을 시작으로 사이버 보안을 발전시키고 현대화해야 합니다. AI 기반의 위협이 증가하면서 미래의 SOC를 도입하여 비용 효율적이며 강력한 사이버 보안을 확보하는 것은 비즈니스의 필수 과제가 되었습니다. 민첩성과 효율성을 모두 갖춘 사이버 보안을 통해 기술 환경과 위협 환경의 지속적 진화에 발맞춰 미래에 대응해야 합니다. 그러나 SOC 혁신은 그 자체로 막대한 도전과 같이 느껴질 수 있습니다.

- 2026년까지 지속적 위협 노출 관리 프로그램을 기반으로 보안 투자를 우선적으로 적용하는 조직은 침해 사고의 2/3를 방지할 수 있을 것입니다.[1]
- 2025년까지 생성형 AI의 활용에 따라 보안에 필요한 사이버 보안 리소스가 급증하면서 애플리케이션 및 데이터 보안에 대한 지출이 15% 이상 증가할 것으로 예상됩니다.[2]

보안 운영 센터의 혁신 시작하기

지금 바로 리소스 및 기술의 압박을 완화하고 차세대 SOC 혁신을 시작하세요. Palo Alto Networks Cortex 플랫폼의 지능형 AI 지원 기능을 갖춘 Palo Alto Networks 관리형 보안 서비스 제공업체(MSSP) 파트너를 통해 조직에 필요한 컨설팅과 기술 전문성, 광범위한 보안 서비스를 이용해 보세요.

Cortex 플랫폼은 **하나의 AI 기반 보안 운영 플랫폼에서 엔드투엔드 보안을 제공하는 유일한 솔루션**입니다. 이 플랫폼은 고급 오케스트레이션 및 자동화(XSOAR), AI 기반 SOC(XSIAM), 확장 탐지 및 대응(XDR), 선제적 공격 표면 관리(Xpanse)를 하나로 통합하여 제공합니다.

이들 솔루션은 **독립적으로 도입할 수도 있고 모두 함께 도입할 수도 있습니다**. 그리고 **네 가지 솔루션 모두 기능의 결합**을 통해 원활한 총체적 탐지 및 보호를 지원하도록 설계되었습니다. 단기적으로 Palo Alto Networks MSSP 파트너는 Cortex의 일부 기능을 도입하여 **가장 시급한 사이버 보안 문제를 즉시 해결**합니다. 이와 동시에 장기적으로는 비용 절감, 더욱 강력하고 민첩한 사이버 방어, 그리고 **SOC 혁신을 위한 기반**을 제공합니다.

Palo Alto Networks MSSP 파트너는 Cortex 기능을 활용하여 고급 보안 서비스 및 솔루션을 제공함으로써 사이버 보안 자산이 원활하게 통합될 수 있도록 지원합니다. 전문성과 기술력, Cortex 플랫폼의 강력한 성능을 두루 갖춘 Palo Alto Networks 공인 MSSP는 실행 가능한 전략과 원활한 경로를 구축하여 AI 기반의 SOC 혁신을 구현합니다.

1. Richard Addiscott, et al., *Top Trends in Cybersecurity for 2024*, Gartner, 2024년 1월 2일.
2. 출처 동일

공동의 고객에게 의미하는 것

현황과 우선순위를 파악하여 명확하고 효과적인 SOC 혁신 전략과 로드맵을 구축함으로서 가시성 부족의 문제와 투자에 대한 불안감을 극복할 수 있습니다.

Palo Alto Networks MSSP 파트너는 전문 컨설팅, 전문성, 업계 지식, 사용 사례에 중점을 두고 고객의 요구 사항을 고려하여 적절한 보안 전략과 로드맵을 수립할 수 있도록 도와드립니다. MSSP 파트너는 Cortex 플랫폼의 강력한 기능과 자체 제품을 결합하여 현존하는 리스크 및 위협 요인을 파악하고, 현재 구축된 요소를 고려하여 우선순위를 규정하고, 고객의 프로필과 성숙도에 따라 최고의 접근 방식을 결정하기 위해 고객과 협력합니다.

- 리스크 평가를 통해 중요 데이터와 규제 환경을 파악하고, 노출 리스크를 식별하고, 리스크 프로필을 작성하고, 중요 데이터를 보호하기에 가장 적절한 접근 방식을 추천합니다.
- 공격 표면 평가는 특정 시점을 평가하거나 지속적으로 공격 표면을 관리함으로써 공격 표면을 축소하거나 보다 효과적으로 보호하기 위한 전략 수립에 활용됩니다.
- 공급망 리스크 평가는 설문조사, 감사, 알려진 취약점이 있는 기술을 자동으로 식별함으로써 중요한 공급업체를 파악하고 보안 리스크를 평가합니다.
- 레드, 블루, 퍼플 팀 구성 연습.
- 알려진 리스크와 알려지지 않은 리스크 매핑.

이러한 가시성과 인사이트를 바탕으로 MSSP 파트너는 다음과 같이 긴급한 개선이 필요한 영역에 대해 우선순위를 정하고, 계획을 작성하고, 플래그를 지정하여 최고의 **실행 전략과 로드맵**을 수립합니다.

- 성숙도 평가 또는 로드맵 개발.
- 비즈니스 전략, 리스크 및 규제 환경, 조직 리스크 성향, 현재 IT 환경 및 계획된 IT 환경, 숙련된 인하우스 리소스의 가용성, 소싱 전략을 비롯한 보안 혁신 컨설팅.
- 보안 운영 현대화 계획(예: AI 및 자동화를 적용할 위치와 방법).
- SOC 기술 선택 및 도구 통합 계획.
- 전략 실행 서비스, 배포, 통합, 엔지니어링 등(예: 자동화 플레이북 생성).

MSSP 파트너 및 Cortex를 통해 고객은 다음을 수행할 수 있습니다.

- 전체적인 현대 태세 및 성숙도 평가를 진행하여 자체적인 AI 지원 SOC를 구축하는 전략과 MSSP에 SOC를 아웃소싱하는 전략 중 비즈니스에 적합한 것을 결정할 수 있습니다.
- 리스크 우선순위에 따라 격차와 취약점을 파악하고 이를 해결하기 위한 계획을 수립함으로써 공격 표면을 축소하고 리스크 및 보안 부담을 축소합니다.
- 보안이 혁신의 걸림돌로 작용할 위험을 줄입니다.
- 전반적 자산의 데이터로 작동하는 클라우드, 네트워크, 솔루션, 애플리케이션 보안 태세에 대한 종합적 가시성을 확보하여 지식의 공백 없이 엔드투엔드 보호를 지원합니다.

알고 계셨나요?

4/10

조직 10개 중 4개 이상은 MDR 서비스 제공업체의 작업이 인하우스 리소스를 사용하는 것보다 더 나은 성과를 낼 수 있다고 생각합니다. 1/3은 보안 프로그램이 미숙하며 필요한 도구와 시스템도 부족하다고 말합니다.[3]

3. Dave Gruber, *What Security Teams Want from MDR Providers*, ESG, 2022년 9월.

SOC의 혁신 및 운영에 필요한 기술과 기능을 활용하고 자체 IT 리소스를 보강하며 강화할 수 있습니다.

Palo Alto Networks MSSP 파트너는 Cortex의 강력한 AI 지원 자동화 및 광범위한 모니터링 기능을 활용하여 **많은 시간이 소요되며 리소스 집약적**인 **SOC 작업**과 **프로세스**를 처리합니다. MSSP는 전문 리소스를 제공하고 Cortex 기능을 바탕으로 광범위한 보안 서비스를 제공하며, **Cortex 기반의 중요한 인사이트와 제어 기능을 이용할 수 있도록** 팀을 지원합니다. 또한 MSSP 파트너는 AI, 머신 러닝, IoT 또는 특정 업종의 사례에 대한 전문성과 같은 전문적 역량을 제공하기도 합니다. Cortex를 통해 클라우드, 네트워크, 디바이스, 애플리케이션을 비롯한 전체 IT 환경의 데이터를 활용하여 **목표에 적합한 혁신 프로젝트를 지원**하며, 이 모든 것은 보안 종속성과 그 영향에 대한 포괄적 이해를 바탕으로 합니다.

Cortex Palo Alto Networks MSSP 파트너 서비스 제공 사항:

- 관리형 SOC.
- 관리형 보안 서비스 제공업체.
- 인시던트 대응.
- 리테이너 조사 서비스.
- MDR 서비스(미래의 문제를 예방하고, 새로운 위협에 대응하고, 고객이 공격이나 악의적인 활동으로 위험한 상태인지 여부를 판단하는 위협 헌팅 및 취약성 관리 포함).
- 탐지 및 대응.
- 인시던트 관리.
- 선제적 위협 헌팅.
- 유연한 위협 탐지 및 대응 지원(탐지된 위협의 대부분을 처리하며, 특정 위협은 인하우스 팀에 이관하거나 고객의 선호도 및 사이버 보안 정책에 따라 다른 방식으로 처리).

MSSP 파트너 및 Cortex를 통해 고객은 다음을 수행할 수 있습니다.

- 확보하기 어려운 기술 및/또는 고가의 기술을 활용하여 오버헤드 및 리소스 제한을 제거합니다.
- 더 많은 리소스를 고용하지 않고도 더욱 강력하고 완벽한 보안을 달성할 수 있습니다.
- 진행 중인 문제를 신속하게 해결하며, 잠재적인 문제가 리스크를 초래하거나 비즈니스에 영향을 미치기 전에 파악할 수 있습니다.
- 사이버 보안에 대한 이해와 자신감을 강화합니다.
- 전체 자산의 데이터와 인사이트를 한 눈에 파악하여 보다 종합적이며 효과적이고 비용 효율적인 보안 접근 방식을 도입할 수 있습니다.
- 상세한 심층적 조사를 수행하여 더 적은 리소스로 더 나은 실적을 달성합니다.
- '관리자'의 업무 부담을 줄여 직원에게 필요한 정보와 인사이트를 신속하게 제공합니다. 이를 통해 보다 가치 있는 업무에 집중할 수 있으며 직원의 이직률을 개선할 수 있습니다.
- 확장된 탐지 및 대응으로 보안을 더욱 강화합니다(Cortex XDR®).

알고 계셨나요?

42% 관리형 보안 서비스 제공업체와 협력한 결과 공격 성공률이 현저히 낮아졌다고 응답한 비율.[4]

38% 관리형 보안 서비스 제공업체와 협력한 결과 보안 운영 비용이 절감되었다고 응답한 비율.[5]

50% 관리형 보안 서비스 제공업체와 협력한 결과 보안 담당자의 기술이 향상되었다고 응답한 비율.[6]

4. *What Security Teams Want from MDR Providers*, 2022년 9월.
5. 출처 동일
6. 출처 동일

동급 최고 수준의 Cortex 플랫폼을 통해 AI 기반 SOC를 향한 여정을 시작하고 미래의 새로운 AI 기반 공격과 새로운 위협에 한발 앞서 대응하세요.

관리형 AI 기반 SOC 플랫폼으로 SOC 혁신을 가속화하세요. 서비스형 자동화를 통해 위협 관리를 개선하고 공격 표면을 최소화하세요. Palo Alto Networks Cortex 플랫폼을 사용하면 **차세대 보안 기능**을 빠르게 도입하고, 새로운 기능을 신속하게 추가하고, 머신 러닝을 통해 시스템을 지속적으로 개선하며 강화할 수 있습니다.

MSSP는 Cortex를 통해 AI 지원 프로필과 ID를 생성하고 클라우드, 네트워크, 엔드포인트, ID 및 액세스 전반의 분석을 정의하여 목표한 보안 정책을 효과적으로 자동화할 수 있습니다. 프로필, 사용자, 애플리케이션, 위협에 따라 최신 상태로 자동 조정되므로 **강력한 보안 및 방어 태세를 유지**할 수 있습니다.

사이버 보안을 손쉽게 현대화하고 업그레이드하여 클라우드, 신기술, AI, IoT의 요구 사항을 충족하고 공급망 취약점이 발생할 경우 신속하게 해결할 수 있습니다. Cortex를 사용하면 MSSP와 조직 내부의 팀이 자동화 및 오케스트레이션을 통해 신속하게 문제에 대응하고 수정함으로써 몇 주가 걸리던 문제를 몇 시간 만에 해결할 수 있습니다.

MSSP 파트너 및 Cortex를 통해 고객은 다음을 수행할 수 있습니다.

- 완전히 통합된 여러 솔루션을 제공하는 하나의 플랫폼을 활용하여 하나의 포괄적 보안 에코시스템으로 전환함으로써 도구를 통합하고 성능을 개선할 수 있습니다.
- Cortex 에코시스템 전반에 걸친 솔루션의 시너지 효과를 활용하여 위협에 대한 대응 시스템을 완성합니다. 개별 제품이 유기적으로 작동하여 위협 환경을 모니터링하고 가장 강력한 탐지, 대응 및 조사 기능을 제공합니다.
- 하나의 시야를 확보하여 복잡성을 제거하고 중요한 사항이 누락되거나 우선순위가 간과될 위험을 줄입니다.

알고 계셨나요?

Palo Alto Networks Cortex XDR은 2024년 2분기 Forrester Wave™: 확장형 탐지 및 대응(XDR) 플랫폼 보고서에서 리더로 선정되며 SOC 플랫폼의 효율성과 신뢰성을 다시 한 번 인정받았습니다.

Cortex XDR을 통해 Palo Alto Networks는 2023 Gartner® Magic Quadrant™ 보고서에서 엔드포인트 보호 플랫폼(EPP) 부문 리더로 선정되었습니다.

2023 MITRE Engenuity ATT&CK® 평가에서 보호와 가시성을 조합하여 가장 우수한 성과를 보여준 Cortex XDR는 구성 변경과 탐지 지연 없이 100% 보호 및 100% 분석 범위를 달성한 유일한 솔루션이었습니다.

Cortex 관련 정보

Palo Alto Networks의 Cortex®는 보안 운영 솔루션을 새롭게 정의하여 조직이 최신 보안 운영 센터(SOC) 환경을 구축할 수 있도록 지원합니다. Cortex는 머신 러닝과 Unit 42® 위협 인텔리전스를 기반으로 하는 통합 플랫폼에서 동급 최고의 위협 탐지, 예방, 공격 표면 관리, 보안 자동화 기능을 제공합니다. 전 세계의 수많은 기업이 신뢰하고 주요 분석업체의 인정을 받은 Cortex XDR®, Cortex XSOAR®, Cortex Xpanse®, Cortex XSIAM®은 독립형 솔루션으로서 보호 기능이 입증되었을 뿐 아니라 SOC 전반에서 포스 멀티플라이어로서 원활하게 작동합니다. 자세한 내용은 www.paloaltonetworks.com/cortex에서 확인할 수 있습니다.

Palo Alto Networks 소개

Palo Alto Networks는 세계적인 사이버 보안 리더입니다. 사이버위협으로부터 극복하기 위한 혁신을 추구하기에 기업이 안심하고 기술을 수용할 수 있습니다. 전 세계 모든 부문의 수천 곳의 고객에게 차세대 사이버 보안을 제공합니다. 당사의 동급 최고 사이버 보안 플랫폼 및 서비스는 업계 최고의 위협 인텔리전스의 지원을 받으며 최첨단 자동화를 통해 강화됩니다. 당사는 제로 트러스트 기업 지원을 위한 제품 구축, 보안 인시던트에 대응, 세계적 수준의 파트너 에코시스템을 통한 더 우수한 보안 성과 제공에 이르는 모든 분야에서 언제나 전례 없는 가장 확실한 안전을 보장할 수 있도록 최선을 다하고 있습니다. 이것이 Palo Alto Networks가 최고의 사이버 보안 파트너인 이유입니다.

서울시 강남구 테헤란로 518, 10층
(위워크 삼성역 2호점, 섬유센터빌딩)
영업 문의
Tel: 82-2-568-4353 /
eMail: Sales-KR@paloaltonetworks.com
www.paloaltonetworks.co.kr

cortex_sb_next-generation-security-operations_080524