paloalto NETWORKS | CORTEX XSIAM

XSIAM 구매자 안내서:
AI 시대를 위한 SOC 혁신 방안

목차

격차 줄이기:
최신 SOC의 선제적 예방

사이버 보안 환경이 빠르게 진화하면서 기업들은 지금껏 없었던 거대한 문제를 마주하고 있습니다. 현대 환경의 위협 행위자는 더욱 정교한 기술과 AI를 사용하여 기존의 보안 조치를 우회합니다. 보안 전문가라면 극적으로 변화한 보안 운영 센터(SOC)의 요구 사항을 직접 경험하셨을 것입니다. 1년 전만 해도 24시간이 걸리던 침해 발생 시간[1]은 불과 몇 시간으로 줄어들고, 규제 요건은 더욱 엄격해진 현 시대에 기존의 위협 탐지 및 대응 방식만으로는 결코 충분하지 않습니다.

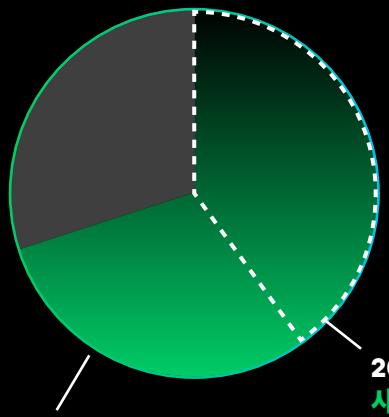
보안팀은 매번 침해가 발생한 후에야 시스템이 어떻게 손상되었는지, 연관된 시스템은 무엇인지, 유출된 데이터는 무엇인지를 비롯하여 어떤 일이 발생했는지 파악할 수 있습니다. 이는 다음과 같은 의문을 제기합니다. 침해 인시던트가 발생한 후 이를 파악할 수 있는 정보가 있다면, 침해가 발생하기 전에 이를 예방하거나 차단할 수는 없는 것일까요? 인시던트 발생 후 분석과 선제적 예방 사이의 격차는 변화하는 최신 SOC 요구 사항의 핵심입니다.

기존의 보안 정보 및 이벤트 관리(SIEM) 솔루션은 한때 많은 보안 운영 시스템의 근간이 되었습니다. 하지만 이제는 그러한 솔루션으로 변화의 속도를 따라잡기는 어렵습니다. 아마도 복잡한 구성과 많은 시간이 소요되는 통합, 탐지 엔지니어링에 대한 막대한 투자 그리고 감당하기 힘들 만큼 많은 양의 알림으로 어려움을 겪고 계실 것입니다.

지속적으로 증가하는 다중 공격 전술

랜섬웨어 공격은 최근 몇 년간 무섭도록 진화했으며, 다중 익스플로잇 전술이 점점 더 확산되고 있습니다.

랜섬웨어 사례의 데이터 탈취:[2]



75% 증가

18개월 동안 랜섬웨어 공격에 의한 데이터 탈취 건수가 75% 증가했습니다.

1. *2025년 Unit 42 글로벌 인시던트 대응 보고서*, Palo Alto Networks, 2025년 2월 25일.
2. *2023년 Unit 42 랜섬웨어 및 갈취 보고서*, Palo Alto Networks Unit 42, 2025년 9월 28일.

이러한 문제는 팀에 부담을 주며, 결과적으로 조직이 취약해질 수 있습니다. 수많은 보안 도구의 사일로적 특성은 비효율적 워크플로와 분석가가 감당해야 하는 인지 부하의 증가로 이어지며, 결국 중요한 위협 요소에 대한 관리가 소홀해질 수 있습니다. 또한, 취약점 관리와 같은 사전 보안 기능과 선제적 도구 간 통합이 부족할 경우 실시간 위협 탐지가 어렵고 인시던트 대응이 지연되어 조직이 위험에 처하게 됩니다.

또한, 방대한 양의 데이터를 고려할 때 정적 상관관계 규칙과 광범위한 탐지 엔지니어링에 주로 의존할 경우 환경 전반의 보안 이벤트 간 유의미한 관계를 파악하기가 쉽지 않으며, 그 결과 위협에 충분히 대응할 수 없습니다. 이러한 환경에서는 알림이 다수의 개별적 데이터 포인트로 표시되는 경우가 많으며, SOC 팀에서 수동으로 상관 관계를 파악해야 하므로 오탐률이 높아집니다. 이처럼 서로 분절된 프로세스는 보안 인프라의 효율성을 저해하며, 보다 발전된 적응형 위협 탐지 방안의 필요성을 강조합니다.

영향의 정량화: SOC 혁신의 실제 ROI

Palo Alto Networks의 의뢰로 Forrester® Consulting에서 진행한 Total Economic Impact™ 연구에서 Cortex XSIAM® 구현을 분석한 결과, 복합 조직이 다음과 같은 측정 가능한 비즈니스 핵심 성과를 달성했습니다.[3]

257% | $560만 | 6개월 미만

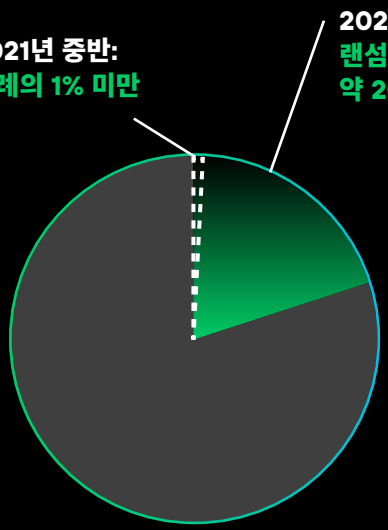
3년 ROI | 순 현재가치 | 투자 회수 기간

85% | 70% | $310만

MTTR 감소 | SOC 조사가 필요한 인시던트 감소 | 도구 통합에 의한 절감액

지속적으로 증가하는 다중 공격 전술(계속)

괴롭힘을 갈취 수단으로 사용:[4]



1900% 증가

같은 기간에 괴롭힘 전술을 사용하는 랜섬웨어 그룹이 1900% 증가했습니다.

이러한 통계는 위협 행위자가 피해자를 갈취하기 위해 보다 다각적인 압박 포인트를 활용하는 방식으로 랜섬웨어 전략이 크게 변화하고 있음을 보여줍니다. 데이터 탈취와 괴롭힘 전술이 모두 급격히 증가한 것은 조직이 마주하는 랜섬웨어 위협의 복잡성과 심각성이 진화하고 있음을 나타냅니다.

암호화	데이터 탈취	DDoS	괴롭힘
피해자는 액세스를 되찾기 위해 돈을 지불	해커는 탈취한 데이터를 공개하겠다고 위협	DDoS 공격은 공개 웹사이트를 폐쇄합니다.	고객, 비즈니스 파트너 및 언론에 연락합니다.

3. *The Total Economic Impact™ Of Palo Alto Networks Cortex XSIAM*, Forrester Consulting, 2025년 10월 13일.
4. Palo Alto Networks Unit 42, *2023 Unit 42 랜섬웨어 및 갈취 보고서.*

보안 운영 혁신

SOC 혁신은 플랫폼화된 SecOps를 위한 확장형 AI 지원 기반인 Cortex® Extended Data Lake(XDL)에서 시작됩니다. Cortex XDL은 SOC의 통합 정보 창구의 역할을 하며, 모든 보안 데이터를 통합하고, 정규화하고, 강화합니다.

이러한 기반을 바탕으로 Cortex XSIAM은 핵심 보안 기능을 혁신적인 단일 플랫폼으로 통합합니다.

- 보안 정보 및 이벤트 관리(SIEM)
- 엔드포인트 탐지 및 대응(EDR)
- 확장형 탐지 및 대응(XDR)
- 보안 오케스트레이션, 자동화 및 대응(SOAR)
- 공격 표면 관리(ASM)
- 사용자 및 개체 행동 분석(UEBA)
- ID 위협 탐지 및 대응(ITDR)
- 클라우드 탐지 및 대응(CDR)
- 위협 인텔리전스 관리(TIM)
- 위협 인텔리전스 플랫폼(TIP)

> “XSIAM 덕분에 가시성이 높아지고 조사 속도가 더 빨라졌습니다. 원활한 데이터 온보딩과 자동화 설정이 정말 획기적입니다.
>
> – Mike Dembek
> 네트워크 아키텍트, Boyne Resorts

그림 1. XSIAM Command Center

Cortex XSIAM은 데이터, AI 기반 방어, 자동화를 하나의 플랫폼으로 중앙 집중화하여 보안 운영을 혁신합니다. XSIAM Command Center에는 엔드포인트와 네트워크, ID, 클라우드, 애플리케이션 원격 분석 등 다양한 데이터 소스가 표시되어 있으며, 이 모두가 데이터 수집 상태와 용량에 대한 인사이트를 제공합니다.

통합이 완료되면 여러 도구를 전환하며 작업할 필요가 없어 업무의 복잡성이 줄어들고 팀의 효율성이 향상됩니다. 여러 콘솔을 번갈아 사용하거나 통합 문제로 골머리를 앓을 필요가 없습니다. 최신 SOC 요구 사항을 고려하여 특수 설계된 일관성 있는 단일 플랫폼에서 전체 보안 운영을 관리할 수 있습니다.

Cortex XSIAM을 도입한 조직은 측정 가능한 성과를 달성했습니다. Forrester Total Economic Impact™ 연구에 따르면, 복합 조직은 **3년 차까지 Tier 1 SOC 주의가 필요한 알림 수를 85% 줄여** 분류 및 Tier 1 운영에서 **93만 달러** 이상을 절감했습니다. 또한 3년 차까지 **SecOps 조사가 필요한 케이스를 70% 줄였으며, 평균 복구 시간(MTTR)을 85% 단축**하여 **120만 달러**가 넘는 가치를 창출했습니다.[5]

XSIAM의 간소화된 에이전틱 AI와 자동화 기능은 보안 인시던트 처리 방식을 근본적으로 변화시킵니다. 이 플랫폼은 데이터 통합, 분석, 분류 과정을 자동화하여 분석가의 수작업을 크게 줄여줍니다. 이러한 자동화를 통해 팀은 우선 순위가 높으며 전문가의 지식을 필요로 하는 인시던트를 해결하는 등 보다 중요한 업무에 집중할 수 있습니다.

XSIAM의 기본 제공 AI 모델은 기존 탐지 방법을 뛰어넘어 다양한 데이터 소스에 걸쳐 이벤트를 연결하고 단일 위치에서 인시던트와 리스크의 포괄적인 개요를 제공합니다. XSIAM은 알림 그룹화 및 AI 기반 인시던트 평가를 활용하여 신뢰도가 낮은 이벤트를 원활하게 연결하고 이를 신뢰도가 높은 인시던트로 전환합니다. 이러한 우선순위는 전체적인 리스크에 기반하여 결정되므로 보안팀은 효율적으로 역량을 집중할 수 있습니다.

XSIAM 플랫폼은 단순한 알림을 넘어 원시 데이터의 지속적인 수집, 연결 및 표준화를 보장합니다. 이를 통해 SOC 팀의 역량이 강화되어 뛰어나면서도 간소화된 조사를 통해 위협을 더 빠르고 효과적으로 식별 및 복구 업데이트할 수 있습니다.

Cortex XSIAM을 활용하면 분석가의 경험과 생산성이 눈에 띄게 향상됩니다. 이 플랫폼의 AI 기반 접근 방식은 노이즈를 차단하여 알림의 피로를 줄이고 정말로 중요한 위협에 집중할 수 있도록 도와줍니다. 이러한 변화로 분석가는 일상적 알림 분류에 소요되는 시간을 절약하여 기술 개발과 심층적 조사, 선제적 위협 추적에 더 많은 시간을 할애할 수 있게 됩니다.

또한 XSIAM의 자동화 기반 접근 방식은 인시던트 복구를 가속화합니다. Cortex Marketplace에는 수백 가지 검증된 콘텐츠 팩이 준비되어 있으며, 네이티브 MCP 서버 및 클라이언트 지원을 통해 전체 보안 에코시스템과 손쉽게 연결하여 인사이트를 통합하고 대응을 조율할 수 있습니다. 기존의 수동 작업을 자동화하면 공격 표면 노출과 같은 인시던트 대응 또는 리스크 관리에 소요되는 시간과 노력을 절약할 수 있습니다.

특정 요구 사항에 따라 자동화를 추가, 사용자 지정 또는 수정할 수 있는 유연성을 누릴 수 있습니다. 플레이북은 예약 실행이나 온디맨드 실행, 알람에 의해 자동으로 트리거되어 적시에 대응하고 리스크를 완화할 수 있습니다.

위협 조사가 필요할 때, Cortex Agentic Assistant는 AI 에이전트 워크포스를 활용해 모든 보안 과제를 해결할 수 있도록 지원합니다. XSIAM에 내장된 이 기능은 Cortex AgentiX™ 에이전트를 활용해 고급 워크플로를 계획하고 실행하며, 반복적인 수작업을 즉각적이고 전문적인 자동 대응으로 전환합니다. 팀은 컨텍스트 인식에 기반한 단계별 안내와 내장 제어 기능을 통해 확신을 바탕으로 더 빠르게 대응하며, 비즈니스를 안전하게 보호할 수 있습니다.

Cortex AgentiX는 실제 전문성을 기반으로 한 역할 중심의 AI 에이전트를 제공하여 팀 구성원 각자의 역량을 몇 배로 강화합니다. 10년 이상의 보안 자동화 리더십과 풍부한 글로벌 위협 인텔리전스, 그리고 12억 건의 플레이북 실행 경험을 바탕으로 구축된 이들 에이전트는 상시 가동되는 보안 전문가의 역할을 수행합니다. 분석가가 자연어 프롬프트만 사용하면 에이전트가 복잡한 다단계 작업을 빠르고 정밀하게 계획하고 실행합니다.

5. Forrester Consulting, *Total Economic Impact™*.

조직을 위한 CORTEX XSIAM 평가

조직을 위한 Cortex XSIAM을 선정할 때 중요하게 고려해야 할 요소가 몇 가지 있습니다. 첫째, 현재 보안 도구 환경과 그 복잡성을 평가합니다. 잡다한 도구 때문에 발생하는 복잡성과 선제적 보안 기능과 대응적 보안 기능 간에 단절된 워크플로로 어려움을 겪고 있다면, XSIAM의 통합 접근 방식은 큰 도움이 될 것입니다. 팀이 여러 도구를 전환하여 사용하며 수동으로 정보의 연관 관계를 파악하는 데 얼마나 많은 시간이 낭비되는지 생각해 보세요. XSIAM의 통합 플랫폼은 이러한 오버헤드를 획기적으로 줄여주고 팀의 효율성을 향상시킬 수 있습니다.

둘째, 조직에서 처리하는 데이터의 양과 다양성을 고려합니다. XSIAM은 다양한 데이터의 대량 처리 및 분석 작업에 탁월하므로 복잡하고 데이터량이 많은 환경의 조직에 특히 적합합니다. 온프레미스 데이터와 클라우드 데이터가 섞여 있어 전반적인 보안 상태를 파악하기가 어렵다면 다양한 소스의 데이터를 수집하고 분석하는 XSIAM은 획기적인 변화를 가져올 수 있습니다.

클라우드 또는 하이브리드 환경에서 사업을 운영하고 있다면 온프레미스 및 클라우드 자산에 대한 포괄적 가시성을 제공하는 XSIAM의 클라우드 네이티브 아키텍처를 통해 보안 운영을 크게 향상시킬 수 있습니다. 많은 조직이 기존 보안 도구로는 클라우드 환경에서 적절한 가시성과 보호 기능을 제공하기 어려워 난관을 겪고 있습니다. XSIAM은 SOC를 클라우드로 확장하여 인프라 전반에 대한 통합적 가시성 및 보안 운영을 보장합니다.

셋째, 준수 요구사항을 검토합니다. 이 역시 중요한 요소입니다. XSIAM의 강력한 보고 기능과 종합적 데이터 분석을 바탕으로 다양한 규제 표준에 효과적으로 대응할 수 있습니다. 현재 규정 준수 보고에 소요되는 시간이 얼마나 많은지 생각해 보세요. 그리고 XSIAM을 통해 이 프로세스를 얼마나 간소화할 수 있을지 생각해 보세요.

기존 SIEM 및 기타 보안 플랫폼과 비교할 때, XSIAM은 AI 기반 접근 방식을 통해 향상된 위협 탐지 기능을 제공합니다. 통합된 도구와 향상된 효율성 덕분에 운영 복잡성이 감소하며 상당한 비용을 절감할 수 있습니다. ROI를 평가할 때는 직접 비용뿐 아니라 절약되는 분석가 시간과 보안 태세 개선의 가치도 함께 고려해야 합니다. XSIAM의 자동 분류 및 대응 기능을 통해 얼마나 더 빠르게 위협을 탐지하고 대응할 수 있을지 생각해 보세요.

Forrester Consulting Total Economic Impact™ 연구는 실제 재무적 성과를 입증했습니다. 연구에 따르면 조직들은 **3년간 257%의 ROI**와 **6개월 미만의 투자 회수 기간**을 달성했습니다. 한 글로벌 보안 부문 부사장은 다음과 같이 밝혔습니다. "탐지 및 복구에 소요되는 평균 시간이 80% 이상 단축되었습니다. 예전에는 탐지에 4시간, 복구에 2시간이 걸렸지만 이제는 총 40~50분이면 충분합니다."[6]

> "Cortex XSIAM은 기존의 SIEM으로는 불가능한 방식으로 보안 운영을 혁신했습니다. XSIAM를 활용하여 탐지, 조사 및 대응 워크플로를 자동화하고 오케스트레이션할 수 있게 되었으며, 이는 LOLC의 생산성과 보안 태세를 크게 향상시켰습니다.
>
> – Prasanna Siriwardena
> 최고 정보 책임자(CIO), LOLC Holdings PLC

6. Forrester Consulting, *Total Economic Impact™*.

SIEM 솔루션을 능가하는 XSIAM의 장점을 확인해 보세요.

시간 절약: 기존 SIEM과 XSIAM의 비교

SIEM XSIAM

위협 탐지 개발

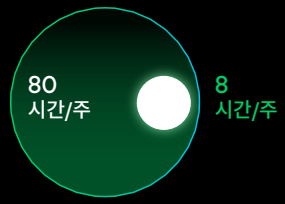
변화하는 위협 환경에 적응하는알림을 생성하는 지속적인 프로세스입니다.

100
시간/주 절약 효과

대부분의 위협 탐지 개발을 XSIAM 연구팀에 아웃소싱했습니다.

알림 조정

충실도 내역을 기반으로알림을 개선하는 지속적인 프로세스입니다.

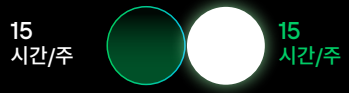


72
시간/주 절약 효과

엔드포인트 알림 조정을 XSIAM 연구팀에 아웃소싱했습니다.

시스템 유지 관리

로그 파싱, 서버 패치 작업 등



변동 없음

분석

고급 알림은복잡한 통계와 머신 러닝을 고려하여 생성됩니다.

SIEM

[기능 격차]
애드온 패키지와 BYOML 모델이 필요합니다. 표준화가 어렵습니다.

XSIAM

[새로운 기능]
XSIAM은 통계와 ML을 통한 자동 기준선 지정과 비정상 알림이 있습니다.

시간 절약 결과:

4.5 FTE
총 노력 감소

그림 2. 기존 SIEM과 XSIAM의 시간 절약 효과

XSIAM을 도입하기에 앞서 AI 기반 보안 운영에 대한 조직의 준비 상태를 평가하세요. 팀의 현재 역량과 프로세스를 고려하고, 보안 운영에 대한 접근 방식의 변화를 준비해야 합니다.

XSIAM은 보안 운영을 크게 개선할 수 있지만, 그 과정에서 팀의 업무 방식에 약간의 조정이 필요할 수 있습니다. 새로운 AI 기반 플랫폼을 도입할 때는 교육과 변경 관리의 측면을 고려해야 합니다.

보안 운영의 미래에 대비

Cortex XSIAM은 제로 트러스트, SASE(Secure Access Service Edge), SSE(보안 서비스 에지)를 비롯하여 진화하는 보안 패러다임에서 중요한 역할을 합니다. 포괄적 가시성과 지능형 분석 기능은 이와 같은 최신 보안 접근 방식과 조화를 이루며 보안 운영의 미래를 대비할 수 있도록 지원합니다. XSIAM은 제로 트러스트 아키텍처로 전환하는 과정에서 사용자 및 엔터티의 행동에 대한 심층적 인사이트를 제공하며, 조직은 이를 활용하여 강력한 제로 트러스트 모델을 구현하고 유지할 수 있습니다.

이 플랫폼은 사후 인시던트 대응과 선제적 보안 태세 관리를 통합함으로써 기업이 직면한 두 가지 핵심 리스크 영역을 다음과 같이 해결합니다.

- **Cortex 노출 관리:** AI 기반 우선순위 지정 및 엔터프라이즈와 클라우드 전반에 걸친 자동 대응을 통해 취약점 관련 알림을 최대 99%까지 축소합니다. 이러한 혁신적 접근 방식은 실제 공격에 활용될 수 있고 보안 조치가 없는 취약점에 집중하여, 가장 중요한 0.01%의 위협에 우선순위를 둘 수 있도록 지원합니다.
- **Cortex 이메일 분석:** LLM 기반 분석과 업계 최고의 탐지 및 대응 기술을 결합하여 고급 피싱 시도와 이메일 기반 공격을 차단합니다. 이메일은 2030년까지 사용자 수가 50억 명에 이를 것으로 예상되는[7] 주요 커뮤니케이션 도구이자 사이버 공격의 최우선 표적입니다. 이 기능은 악성 이메일을 자동으로 제거하고, 침해된 계정을 비활성화하며, 영향을 받은 엔드포인트를 실시간으로 격리합니다.

조직이 성장하고 위협이 진화하더라도, 확장성을 갖추고 있는 XSIAM은 확대되는 데이터를 처리하고 새로운 유형의 위협에 적응할 수 있습니다. 플랫폼의 AI 모델과 탐지기는 지속적으로 업데이트됩니다. 따라서 팀이 수동으로 업데이트하지 않더라도 언제나 최신 위협 인텔리전스 및 탐지 기능을 제공합니다. 즉, 보안 도구를 수동으로 조정하고 업데이트할 필요 없이 항상 최신 위협에 대해 조직을 보호할 수 있습니다.

XSIAM은 수동 애널리스트 작업을 학습하여 향후 자동화를 위한 권장 사항을 제공합니다. 이 기능은 플랫폼의 인시던트 자동 해결 기능을 강화하고 시간 경과에 따라 효율성, 정확성을 향상시켜 조직의 보안 태세를 지속적으로 개선할 수 있도록 지원합니다.

XSIAM은 성숙 단계에 이른 보안 전용 ML 데이터 모델을 활용하여 다양한 소스에서 확보한 대량의 데이터를 자동으로 정규화하고 연관 관계를 파악하여 보안 위협을 탐지합니다. 이러한 모델은 수만에 달하는 환경에서 학습된 행동을 기반으로 구축되어 비정상적인 활동과 악성 행위를 구분할 수 있도록 도와줍니다. 이를 통해 오탐을 크게 줄이고 탐지 및 예방 기능을 개선하여 공격이 보안 인시던트로 발전하기 전에 차단할 수 있습니다.

또한, XSIAM의 BYOML(Bring Your Own Machine Learning) 기능을 사용하면 조직의 자체 ML 도구를 플랫폼에 통합할 수 있습니다. 이를 통해 ML의 강력한 기능을 활용하여 XSIAM에서 중앙 집중화된 정규화 데이터를 사용한 위협 헌팅이 가능하므로 정교한 위협을 더욱 정확하게 탐지하고 대응할 수 있습니다.

통합의 재무적 영향

Forrester Consulting의 *Total Economic Impact™: Palo Alto Networks Cortex XSIAM 연구 결과:*[8]

$310만
20개 이상의 레거시 도구 제거로 절감된 비용(3년 총액)

$220만
보안 태세 60% 개선으로 창출된 가치

$560만
3년간 순 현재가치(NPV)

XSIAM을 도입하면 현대의 보안 과제를 해결하고 미래의 사이버 보안에 필요한 사항을 미리 준비할 수 있습니다. 이러한 미래지향적 접근 방식을 통해 조직은 끊임없이 진화하는 위협 환경으로부터 시스템을 보호할 수 있다는 확신을 가질 수 있습니다. 계속해서 새로운 유형의 위협이 등장하고 요구 사항에 대응하기 위해 성숙 단계의 IT 인프라가 필요한 상황에서, XSIAM의 유연한 AI 기반 접근 방식은 보안 운영을 효과적으로 조정하여 대응할 수 있도록 도와드립니다.

XSIAM은 SOC 팀과 조직의 보안 태세를 계속해서 개선할 수 있도록 지원합니다.

가장 중요한 것은 XSIAM이 AI와 머신 러닝을 통해 지속적 개선을 제공한다는 점입니다. 이 플랫폼은 신규 데이터와 새로운 공격 기법을 기반으로 탐지 및 대응 기능을 정기적으로 개선합니다. 즉, 지속적으로 수동 조정 작업을 진행하지 않아도 새로운 위협과 패턴에 적응하므로 시간이 지남에 따라 보안 운영의 효과는 더욱 강화됩니다.

7. *Email Statistics Report 2025-2030*, cloudHQ, 2025년 4월 24일.
8. Forrester Consulting, *Total Economic Impact™*.

핵심 SOC 지표 개선

Cortex XSIAM은 평균 탐지 시간(MTTD)과 평균 대응 시간(MTTR)을 단축하여 보안 운영을 획기적으로 개선하는 혁신적 접근 방식을 제공합니다. XSIAM은 고급 AI와 머신 러닝을 활용하여 시간이 많이 소요되는 데이터 통합 및 분석 작업을 자동화함으로써 거의 실시간으로 위협을 식별할 수 있도록 지원합니다. 즉, 이전과는 비교할 수 없는 속도로 민첩하게 잠재적 침해를 발견하여 공격자가 조직에 심각한 피해를 입히기 전에 문제를 해결할 수 있습니다.

하지만 공격을 탐지하는 것은 전반전일 뿐입니다. XSIAM의 자동화 우선 접근 방식은 인시던트 대응 프로세스를 가속화함으로써 기존에 몇 시간이 소요되던 수동 조사 과정을 자동 조치를 통해 단 몇 분만에 완료합니다. SOC 팀이 수동 분류 활동에 매달리거나, 여러 소스의 데이터 간 상호 연관성을 찾기 위해 귀중한 시간을 낭비하지 않는 모습을 상상해 보세요. XSIAM의 AI 기반 인시던트 점수화와 지능형 알림 그룹화를 통해 분석가가 중요한 업무에 집중할 수 있도록 지원하세요.

선제적 및 대응적 보안에 통합적으로 접근함으로써 인시던트에 더 빠르게 대응하고 더 많은 인시던트를 사전에 방지할 수 있도록 지원합니다. XSIAM은 SOC 플랫폼에 노출 관리와 이메일 분석 기능을 직접 통합하여 동일한 통합 데이터와 AI, 자동화를 통해 가장 흔한 두 가지 공격 벡터를 해결합니다.

고급 플레이북과 Cortex AgentiX 에이전트를 활용하여 위협에 대해 신속하고 단호한 조치를 취할 수 있으므로 MTTR이 획기적으로 단축됩니다. 가장 중요한 것은 XSIAM이 지속적으로 학습하고 사용자 환경에 적응함에 따라 시간이 지날수록 보안 태세가 더욱 개선된다는 점입니다. XSIAM의 최첨단 AI 모델은 새롭게 등장하는 위협을 마주할 때마다 계속해서 진화하므로 잠재적 공격자보다 한 발 앞서 대응할 수 있습니다.

즉, 현재 MTTD와 MTTR을 개선할 뿐 아니라 미래의 문제에 대비하여 미래지향적 방식으로 보안 운영을 개선할 수 있습니다. Cortex XSIAM을 사용하면 중요 SOC 지표가 지속적으로 최적화되어 조직의 가장 중요한 자산을 보호하고 있다는 믿음을 가지고 복잡한 사이버 보안 환경을 자신감 있게 탐색할 수 있습니다.

연구는 이러한 개선 효과를 입증합니다. 한 전문 소매업체의 SecOps 디렉터에 따르면, 해당 기업의 분기당 알림 수가 **25,000건에서 4,500건으로** 감소했습니다. 또한 인터뷰 대상 고객을 기반으로 한 복합 조직의 경우, 배포에는 **두 달간 세 명의 FTE**가 필요했고, **연간 유지보수에 필요한 FTE는 0.5명**에 불과했습니다.[9]

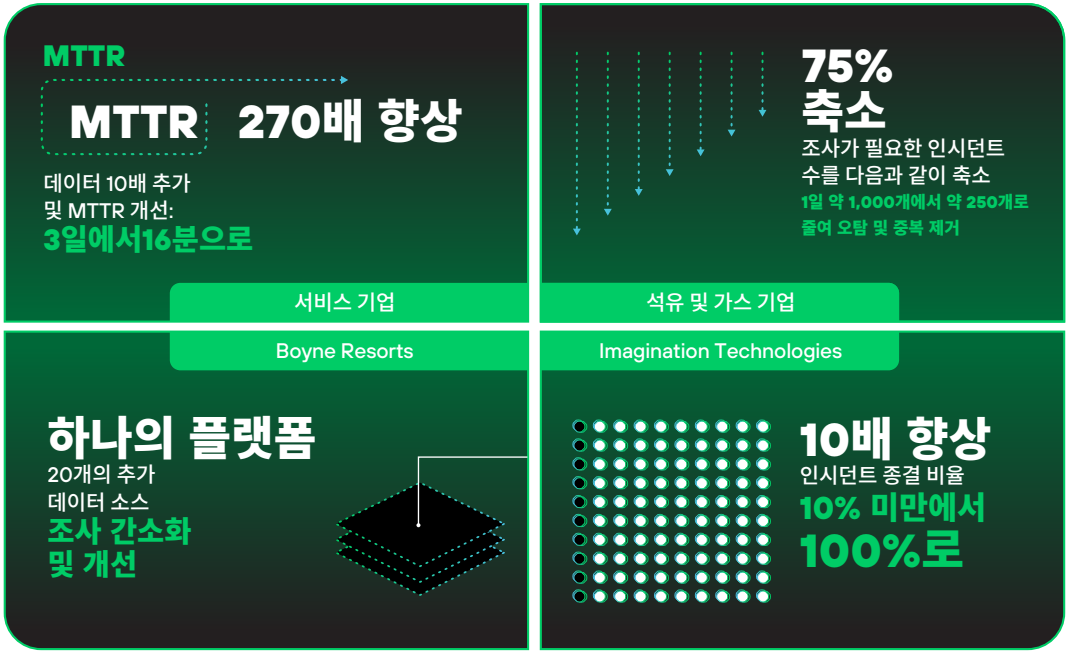


그림 3. XSIAM을 통해 측정 가능한 개선을 이룬 고객 사례

> "다양한 기능을 하나의 통합 플랫폼으로 정리한 XSIAM은 차세대 SOC로 향하는 길을 개척할 것입니다. XSIAM을 통해 자동화를 확대하고 사이버 운영 팀의 역량을 더욱 강화할 수 있을 것으로 기대합니다.
>
> – Rob Jillson
> 사이버 보안 책임자, Resolution Life Australasia

9. Forrester Consulting, *Total Economic Impact™*.

CORTEX XSIAM은 우리 조직에 적합한 솔루션일까요?

1. 현재 SOC 과제

- ☐ 현재 SIEM의 복잡한 구성으로 어려움을 겪고 있나요?
- ☐ 여러 보안 도구의 통합에 많은 시간이 소요되나요?
- ☐ 팀이 너무 많은 양의 알림에 힘들어하고 있나요?
- ☐ 사일로화된 보안 도구 때문에 워크플로가 비효율적인가요?
- ☐ 선제적 보안 기능과 사후 인시던트 대응 간에 단절이 존재하나요?

2. 위협 탐지 및 대응

- ☐ 정적 상관관계 규칙에 크게 의존하고 있나요?
- ☐ 실시간 위협 탐지를 개선할 필요가 있나요?
- ☐ 통합 부족으로 인시던트 대응 프로세스가 지연되고 있나요?
- ☐ 높은 오탐률로 어려움을 겪고 있나요?

3. 데이터 관리

- ☐ 다양한 보안 데이터를 대량으로 처리하나요?
- ☐ 온프레미스 데이터와 클라우드 데이터가 구분되지 않은 채로 처리되고 있나요?
- ☐ 더 나은 데이터 정규화와 상관 관계 기능이 필요한가요?

4. AI 및 자동화 니즈

- ☐ AI를 활용하여 위협 탐지 기능을 개선하고자 하나요?
- ☐ 일상적인 보안 작업을 자동화하고 싶으신가요?
- ☐ 인시던트 분류에서 수작업을 줄이는 것이 중요한가요?
- ☐ AI 기반의 취약점 우선순위 지정 기능으로 불필요한 알림을 줄이고 싶으신가요?

5. 통합 플랫폼 요건

- ☐ SIEM, EDR, XDR, SOAR, 취약점 관리, 이메일 보안 등 여러 보안 기능의 통합이 필요한가요?
- ☐ 단일 플랫폼에서 보안 운영을 관리하고자 하나요?
- ☐ 선제적 보안과 대응적 보안 간 격차를 해소하고 싶으신가요?

6. 클라우드 및 하이브리드 환경

- ☐ 클라우드 또는 하이브리드 환경에서 운영되고 있나요?
- ☐ 온프레미스 및 클라우드 자산 전반에 대한 가시성이 필요한가요?

7. 규정 준수 및 보고

- ☐ 규정 준수 보고 프로세스를 간소화할 필요가 있나요?
- ☐ 규제 표준을 위해 보다 포괄적인 데이터 분석이 필요한가요?

8. 확장성

- ☐ 조직의 성장에 따라 처리해야 하는 데이터 규모가 증가하나요?
- ☐ 진화하는 위협에 적응할 수 있는 솔루션이 필요한가요?

9. 지능형 분석

- ☐ AI 기반 인시던트 점수 책정 및 알림 그룹화에 관심이 있나요?
- ☐ 다양한 데이터 소스에 걸쳐 이벤트의 상관 관계를 보다 정확하게 파악해야 하나요?
- ☐ AI를 통해 가장 중요한 취약점을 우선적으로 처리하고 싶으신가요?

10. 팀의 준비 상태

- ☐ 팀은 AI 기반 보안 운영에 적응할 준비가 되어 있나요?
- ☐ 새로운 최신 플랫폼에 대한 교육에 투자할 의향이 있나요?

11. 미래지향적

- ☐ 제로 트러스트, SASE 또는 SSE 보안 모델로 전환하고 있나요?
- ☐ AI와 ML을 통해 지속적으로 개선되는 솔루션이 필요한가요?

12. 맞춤형 ML 통합

- ☐ 조직의 자체 머신러닝 도구를 통합하는 데 관심이 있나요?

13. 이메일 및 취약점 관리

- ☐ 고급 이메일 위협에 대해 더 나은 보호가 필요하신가요?
- ☐ 취약점 백로그와 우선순위 관리에 어려움을 겪고 계신가요?
- ☐ 중요 취약점의 자동 복구 기능을 활용하고 싶으신가요?

대부분의 질문에 "**예**"라고 답했다면, 특히 조직의 구체적인 보안 과제 및 목표에 부합하는 영역에서 Cortex XSIAM은 귀하의 SOC에 적합한 솔루션입니다.

지금 시작하기

Cortex XSIAM을 활용하여 현재와 미래의 조직에서 운영을 간소화하고, 선제적 보안과 대응적 보안을 통합하고, 대규모 위협을 방지하고, 인시던트 해결을 가속화할 수 있는 방법을 알아보세요.

문의하기 →

Cortex XSIAM 소개

Cortex XSIAM은 현대의 SOC를 위한 AI 기반 SecOps 플랫폼으로서 AI의 파워를 활용하여 SecOps를 간소화하고, 대규모 위협을 차단하고, 인시던트를 더욱 빠르게 해결합니다. 여러 제품을 보안 운영 용도로 특별히 설계한 일관된 단일 플랫폼으로 중앙 집중화하여 리스크를 줄이고 운영 복잡성을 완화합니다.

Cortex XSIAM은 EDR, XDR, SOAR, ASM, UEBA, TIP, SIEM 등 동급 최고의 보안 운영 기능을 모두 통합합니다. XSIAM은 모든 보안 데이터를 중앙 집중화하고, 보안을 위해 특별히 설계된 머신 러닝 데이터 모델을 사용합니다. 이를 통해 데이터 통합, 분석 및 대응 조치를 자동화하면 애널리스트가 중요한 인시던트에 집중할 수 있습니다. Cortex XSIAM에 대한 자세한 내용은 www.paloaltonetworks.com/cortex/cortex-xsiam에서 확인할 수 있습니다.

서울특별시 서초구 서초대로74길 4,
1층 (삼성생명 서초타워)
Tel: +82-2-568-4353
eMail: Sales-KR@paloaltonetworks.com
www.paloaltonetworks.co.kr

cortex_ebook_cortex-xsiam-buyers-guide_102125