paloalto NETWORKS | CORTEX

SOC 혁신을 위한 5 가지 필수 단계

최신 위협 환경에 맞게 설계된 자동화 및 AI 기능으로 SOC 업그레이드

빠르게 변화하는 최신 보안 환경

보안 운영 센터(SOC)가 최초로 건립된 1970년대 중반 이래, 엔터프라이즈 내에서의 SOC 기능과 역할은 계속 진화해 왔습니다. 지금은 거의 모든 비즈니스 부서에서 디지털화가 보편적으로 이루어지고 있어 업종과 관계없이 기업의 전반적인 상태와 성장 잠재력에 SOC가 매우 중요한 의미를 가지고 있습니다.

공격자는 확장된 공격 표면을 기반으로 점점 더 복잡하고 오래 지속되는 공격 방법을 키워 왔지만, SOC 중에는 그 속도를 따라잡지 못한 경우가 있습니다. 많은 기업에서는 아직도 오래전에 개발한 SOC 구성과 도구를 운용하고 있습니다. 이러한 시스템은 많은 수작업과 복잡한 프로세스를 거쳐 예전의 위협에 맞서도록 고안되었습니다.

하지만 이제 이러한 시스템으로는 역부족이며, 머지않아 무너질 수도 있습니다. 오래된 SOC로는 서버, 네트워크, 애플리케이션, 엔드포인트 디바이스, 웹사이트 등 사방에서 끊임없이 겨냥하고 있는 위협을 도저히 따라잡을 수 없습니다.

"더 많은" 폭격에 시달리는 오늘날의 SOC

- **공격 자체가 더 많아졌습니다.** 사이버 공격의 규모가 커졌음에도 불구하고 아직 많은 기업에서는 수작업으로 이를 조사하고 완화하고 있습니다. 이것은 지는 싸움일 수밖에 없습니다.
- **공격자는 점점 더 체계적으로 움직입니다.** 오늘날의 사이버 범죄자는 대중문화에서 소위 말하는 "외로운 늑대" 스타일과는 거리가 멉니다. 오히려 자금을 충분히 확보한 법인에 소속되어 활동하고, 지속적으로 정교한 공격을 감행하는 경우가 많습니다.
- **보호해야 할 디바이스와 데이터가 더 많아집니다.** 보안팀은 네트워크부터 엔드포인트, 에지에 이르기까지 기업 방화벽으로는 감당할 수 없는 대규모의 자산을 보호해야 합니다. 하이브리드 근무가 보편화되면서 공격도 업무처리와 마찬가지로 어디서나 가능한 일이 되었습니다.
- **보안 도구가 많아지면서 복잡성이 더 심화됩니다.** 최근 몇 년 사이에 보안 솔루션과 공급업체가 폭증하면서 제품 종류가 엄청나게 많아졌는데, 그중에는 서로 호환되지 않는 것도 있습니다. 이러한 제품의 경우 통합, 관리, 유지 등 작업이 필요합니다.
- **더 많은 기관에서 더 많은 규제를 적용합니다.** SEC는 물론 주정부, 지자체 기관의 보고 요구 사항이 점점 더 부담스러워지고 있습니다. 보안팀은 공격을 탐지하고, 그 영향을 평가하고, 관련 정보를 보고해야 합니다. 어느 하나 누락될 경우, 벌금이나 징계를 받게 될 수 있습니다.
- **특수화된 중점 영역이 많아지면서 사일로가 더 늘어납니다.** 보안 전문가마다 전문 분야가 다르기 때문에 점점 더 서로 고립되어 각자의 전문 분야에만 주력하며 인사이트를 공유하지 않거나 본인의 시야에만 갇혀 그 이상을 바라보지 못하는 경우가 많습니다.

최신 위협, 요구, 압력에 부응하여 SOC를 현대화하려면 어떻게 해야 할까요?

96%

의 전문가가 작년 한 해 동안 침해나 인시던트를 한 번 이상 경험했습니다. 3건 이상을 보고한 경우는 57%, 10건 이상을 인식한 경우는 24%였습니다.[1]

84%

의 보안 전문가가 하이브리드 근무 방식으로 인해 보안 인시던트가 늘었다는 데 동의합니다.[1]

SOC를 검토하여 해결해야 하는 사항 판단

지금의 SOC는 대응력이 뛰어나고, 빠르게 움직일 수 있어야 합니다. 그러려면 각종 위협을 예방, 탐지, 조사, 제거하는 도구와 위협 인텔리전스를 결합해야 합니다. 그런데 이처럼 이상적인 상태에 이르려면 보안팀은 어떻게 해야 할까요? 동급 최고의 SOC를 개발하려면 지금의 보안 운영 센터에서 직면한 니즈를 처리하기 위해 레거시 모델을 어떻게 혁신할지 판단하는 세심한 검토가 필요합니다.

이 가이드에서는 SOC 효율성과 효과를 제한하는 5가지 주요 문제점과 이를 해결하기 위한 현실적인 해결책, 그리고 기업에서 SOC 혁신을 통해 실현할 수 있는 실질적인 이점을 간략히 소개합니다.

영향의 정량화: SOC 혁신의 실제 ROI

Forrester TEI 연구[2]에서 Cortex XSIAM 배포를 조사한 결과에 따르면 한 복합 조직이 측정 가능한 비즈니스 핵심 성과를 달성한 것으로 나타났습니다.

257%
3년 ROI

$560만
순 현재가치

6개월 미만
투자 회수 기간

85%
MTTR 감소율

70%
SOC 조사가 필요한 인시던트 감소

$310만
도구 통합을 통한 비용 절감 효과

1. *사이버의 다음 단계: 2022년 글로벌 설문 조사(What's Next In Cyber: 2022 Global Survey)*, Palo Alto Networks, 2022
2. *Palo Alto Networks Cortex XSIAM의 Total Economic Impact™, Palo Alto Networks를 대신해 Forrester Consulting에서 실시한 위탁 연구, 2025년 9월. 이 결과는 인터뷰에 참여한 고객의 이야기를 토대로 구성된 복합 조직의 사례입니다.*

아무리 까다로운 SOC 문제점이라도 해결책은 있는 법

	문제점	솔루션
1	도구 확산으로 인해 복잡성과 리스크 발생	통합형 보안 스택으로 SOC 간소화
2	알림은 잡음만 계속 유발할 뿐 인사이트는 거의 제공하지 못함	AI 기반 인텔리전스로 명확성 확보
3	번아웃에 가까운 상태로 일하는 보안 애널리스트	자동화 및 AI 기반 솔루션으로 SecOps 업그레이드
4	컨텍스트 간극으로 인해 사각지대 발생	데이터의 배후 사정 파악
5	위협 억제에 시간이 너무 오래 걸림	통합형 인시던트 대응으로 빠르게 반응

도구 확산으로 인해 복잡성과 리스크 발생

대부분의 SOC는 장기간에 걸쳐 보안 리더와 우선순위가 바뀌면서 방향이 달라집니다. 몇 년 동안 소프트웨어를 유지관리하면서 발생하는 어려움을 감안하지 않고 최신 보안 접근 방식이나 솔루션이 나올 때마다 무작정 도입하는 경우가 많습니다.

하지만 세심하게 감독하지 않으면 SOC는 중도에 그친 실험으로 가득한 차고와 같은 형상을 띠게 될 수 있습니다. 보안 스택은 다양한 공급업체의 포인트 솔루션이 뒤섞인 형태가 되며, 각 솔루션에는 고유한 데이터세트, UI, 에이전트가 있습니다. 이러한 각각의 요소를 유지관리하고 모니터링해야 하며, 작업 스트림부터 스킬 요구사항, 학습 곡선에 이르기까지 각자 운영 비용도 동반됩니다.

여러 솔루션을 한꺼번에 최대한 활용하려다 보니 시간이 오래 걸리고 리소스가 지나치게 소모될 뿐만 아니라, SOC의 효율성도 떨어지게 됩니다.

여러 가지 도구로 인한 가시성 저하

일반적인 SOC에서 사용되는 솔루션은 대체로 상호 운용이 불가능합니다. 데이터를 공유하지도 않고, 같은 사물에서 데이터를 수집해 서로 다른 방식으로 다양한 조사 결과를 제공하는 도구도 많습니다. 이렇게 제각각인 도구에서 이벤트와 알림을 기반으로 실수 없이 결론을 내리기란 쉽지 않습니다. 이러한 문제가 매일 발생하게 됩니다.

따라서 환경에 대해 혼란스럽거나 때로는 상충하기까지 하는 견해가 생기는 것입니다. 애널리스트마다 자기가 다루는 도구에 따라 서로 다른 결론을 내릴 수도 있기 때문에 공통된 견해를 공유하기 어려워집니다.

복잡성으로 인한 비용 상승

SOC는 시간이 지날수록 점점 더 복잡해지고 다층적인 형태가 되어 조직에서 필요한 수준으로 키우고 구성하려면 규격화된 지식이 많이 필요하게 됩니다. 살다 보면 여러 가지 일을 겪게 마련입니다. 팀원이 바뀌고 사원이 입사하거나 퇴사하기도 하며 경영진의 주력 분야가 바뀌고, 그러다 보면 잊히는 솔루션도 있고 방치되는 경우도 있습니다.

궁극적으로, 이와 같은 조직의 순환 때문에 이동이 발생하고 새로운 보안 노출과 리스크가 생기게 됩니다. 이 정도의 복잡성을 오류 없이 유지관리하기란 불가능에 가깝기 때문입니다.

따라서 필연적으로 알림을 놓치거나 도구를 잘못 구성하거나 침해를 탐지하지 못하여 비즈니스에 피해나 손실이 발생합니다.

통합형 보안 스택으로 SOC 간소화

혼란을 줄이려면 복잡성을 해소해야 합니다. 하지만 실천하기가 쉽지 않습니다. 무엇을 없애고 무엇을 유지할지 결정하려면 세심하고 체계적인 프로세스를 거쳐야 합니다.

환경 감사

네트워크, 서버에서 엔드포인트까지 현재 SOC가 보호 중인 모든 자산을 파악해야 합니다. 그중 리스크가 높은 것과 낮은 것은 각각 무엇입니까? 이 목록에서 누락된 부분은 무엇입니까? 어디에 간극이 존재합니까?

공급업체와 도구 통합

현재 사용 중인 도구, 시스템, 데이터 세트의 종류는 몇 가지입니까? 그중 동급 최고로 간주할 수 있는 것은 무엇이고, 수명이 다 된 것은 무엇입니까? 어느 도구가 같은 대상을 모니터링하고 있습니까? 제거하고 통합할 수 있는 지점은 어디입니까?

관리에 대한 통합형 접근 방식 구현

"단일 창"(a single pane of glass)이라는 단어는 이제 업계 전문용어가 되었지만, 아직도 의미 있는 은유입니다. 데이터 소스를 모두 통합하고 그러한 소스에 임베디드 인텔리전스를 적용하며 통합된 워크플로를 제공하는 일관된 시스템이 있으면 SOC 효율을 대폭 강화할 수 있습니다.

이점

애널리스트 집중력 강화

컨텍스트를 계속 전환할 필요가 없고, 애널리스트가 일관된 도구 세트에 집중할 수 있습니다. 명확성을 확보하면 문제를 더 빨리 파악하고 중요하거나 긴급한 정보를 식별하는 역량도 향상됩니다.

통합형 보기

중앙 콘솔에서 전사에 걸쳐 인시던트, 문제, 노출을 일관된 보기로 제공합니다. 모든 사람이 같은 시야를 확보하면 더 빨리 결정을 내릴 수 있습니다.

정보에 기반한 접근 방식

데이터 소스, 인텔리전스, 분석을 하나의 공유된 시스템으로 가져오는 도구를 도입하면 간극이 줄어듭니다. SOC가 단절된 여러 시스템을 모아놓은 컨테이너가 아니라, 계속 개선되는 지능형 허브로 거듭나게 됩니다.

계속 잡음만 유발할 뿐 인사이트는 거의 제공하지 못하는 알림

많은 사이버 범죄자 집단은 APT(Advanced Persistent Threat) 전략을 구사하는데, 이는 광범위한 리소스를 갖춘 전문가 공격자로 원하는 목표를 달성하기 위해 다양한 공격 벡터를 활용합니다.

당연히 보안팀은 쏟아지는 알람에 곤란을 겪게 됩니다. 보안 인시던트가 끊임없이 발생하므로 연중 24시간 내내 쉬지 않고 알림이 생성됩니다. 애널리스트는 알림을 조사하여 신뢰성을 판단하는 데 몇 시간을 보내야 합니다.

모든 것이 '긴급'이라면 결국 아무것도 급하지 않다는 뜻

상당수의 알림 도구가 제대로 조율되지 않고 중복되어 있어 오탐(false-positive)을 연이어 도출하더라도 애널리스트는 알림을 무시할 수가 없습니다. 수백, 수천 개의 알림을 살펴보며 심각할 수도 있는 알림을 찾아내야 합니다.
실제로 잠재적인 위협을 식별하면 수동으로 상관관계를 정립해 일관된 보기를 만들어야 합니다.

한편, 애널리스트가 이렇게 많은 불필요한 알림을 살펴보는 동안 진짜 위협은 탐지되지 않은 채 방치되는 시간이 길어집니다. Palo Alto Networks Unit 42® 에서 수집한 데이터에 따르면, 랜섬웨어 공격의 평균 체류시간은 28일이라고 합니다.
공격자가 저지하는 사람 없이 막대한 손해를 입히는 동안 팀원들은 공격자의 존재도 모릅니다.

평균적으로 SOC 팀원은 진짜 위협이 아닌 인시던트를 조사하고 검증하는 데만 **근무일의 3분의 1**을 소요합니다.[3]

전체 대기업 중 56%가 **매일 1,000개 이상의 알림**을 받습니다.[4]

Forrester TEI 연구에 따르면 Cortex XSIAM을 구축한 복합 조직은 알림 수가 **3년 차까지 85%** 감소했으며 평균 해결 시간도 **85%** 단축했습니다.[5]

3. *글로벌 보안 운영 센터 연구 결과(Global Security Operations Center Study Results)*, IBM, 2023년 3월
4. *"대기업의 56%는 매일 보안 알림을 1,000건 이상 처리(56% of Large Companies Handle 1,000+ Security Alerts Each Day)"* Dark Reading, 2020년 7월 10일
5. *Palo Alto Networks Cortex XSIAM의 Total Economic Impact™, Palo Alto Networks를 대신해 Forrester Consulting에서 실시한 위탁 연구, 2025년 9월. 이 결과는 인터뷰에 참여한 고객의 이야기를 토대로 구성된 복합 조직의 사례입니다.*

AI 기반 인텔리전스로 명확성 확보

SOC를 혁신하려는 팀이라면 오탐(false-positive) 알림을 줄이는 것이 최우선이어야 합니다.

플레이북을 활용해 알림 처리 자동화

- 동작 탐지와 위협 인텔리전스를 활용하는 플레이북을 이용해 신속하게 알림을 분류하세요.
- 중요하다고 생각하는 구체적인 특성을 정해 이 분류를 사용자 지정할 수 있습니다.
- ML 기반 솔루션은 데이터를 수집, 통합, 분석하여 빠른 속도로 결론을 도출할 수 있고, 사람이 개입하지 않고도 많은 알림을 종결할 수 있습니다.

알림을 신속하게 조정해 정확도 향상

- 알림을 빠르고 간편하게 조정하는 솔루션을 이용해 오탐(false-positive)을 줄이세요. 알림 수가 적어지고 양질의 알림이 제공되기 때문에 애널리스트가 실제 위협일 가능성이 있는 알림에만 시간을 할애하고 집중할 수 있습니다.

이점

선제적인 태도

애널리스트가 알림을 수동으로 분류하는 작업이 해소되므로, SOC가 반응적인 태도에서 선제적인 태도로 전환됩니다.

애널리스트 생산성 강화

티켓 양이 대폭 줄어들기 때문에 애널리스트가 실제 위협일 가능성이 있는 문제에 집중할 수 있는 시간이 확보됩니다.

비즈니스 지속성 향상

진짜 위협을 빨리 식별할 수 있어 SOC 팀원들이 비즈니스에 발생하는 피해를 줄일 수 있습니다.

SOC 효과 개선

인력을 추가하지 않아도 결과가 개선됩니다.

정량화된 결과

연구에 따르면 Palo Alto Networks의 AI 기반 SOC 플랫폼은 알림 분류 효율성을 향상하여 3년간 $93만 규모의 생산성 가치를 창출했으며, 알림 검토 작업량도 85% 감소했습니다.[6]

6. Palo Alto Networks Cortex XSIAM의 Total Economic Impact™, Palo Alto Networks를 대신해 Forrester Consulting에서 실시한 위탁 연구, 2025년 9월. 이 결과는 인터뷰에 참여한 고객의 이야기를 토대로 구성된 복합 조직의 사례입니다.

번아웃에 가까운 상태로 일하는 보안 애널리스트

높은 기술을 갖춘 SOC에는 사이버 보안 전문가가 꼭 필요합니다. 하지만, 솔직히 말해 그중에는 심한 업무 스트레스에 시달리는 사람이 많습니다. 사이버 보안 전문가는 공격자를 끝까지 추격해 유의미한 영향력을 행사하고 싶어 하지만, 정확도가 낮은 알림을 면밀히 조사하거나 다음 날 또 반복해야 하는 일상적인 작업을 완료하는 데 대부분의 시간을 할애하고 있습니다.

온종일에 걸친 수동 조사와 중요도 낮은 분류에 시달리다 보면 효율성이 떨어진다는 기분이 들기 마련입니다. 마치 끝나지 않는 두더지 잡기 게임 속에 갇힌 느낌일 겁니다. 수많은 잡무로 인해 바쁘기만 하고, 이렇다 할 성과는 없습니다.

하지만 잡다한 워크플로는 문제 중 한 가지에 불과합니다. 사용하기 어렵고 짜증을 유발하는 오래된 도구도 문제입니다. 게다가 애널리스트는 SOC 팀 내 다른 사람들과 떨어져 자기만의 영역에 고립되어 있을 때가 많습니다. 모두 자기 도구나 분야에만 집중하다 보니, 시너지 효과나 공통된 성취감을 기대하기 어렵습니다.

직원 수가 10,000명 이상인 6개 기업 중 1개는 **현장 팀 인원이 겨우 1~3명밖에 되지 않습니다.**[7]

평균적으로 오늘날의 SecOps 팀은 **40가지 이상의 업무**를 담당합니다.[8] 보안 전문가가 한 기업에 근속하는 평균 기간은 **겨우 26개월**에 불과합니다.[9]

7. *보안 자동화 상태 보고서(State of Security Automation Report)*, Palo Alto Networks.
8. Kathryn Knerler, Ingrid Parker, Carson Zimmerman, *세계적인 사이버 보안 운영 센터의 11가지 전략(11 Strategies of a World-Class Cybersecurity Operations Center)*, MITRE, 2022
9. Christopher Crowley, Barbara Filkins, *SANS 2022년 SOC 설문 조사*, SANS, 2022년 5월 16일

애널리스트의 감각이 무뎌질 위험성

애널리스트가 반복적인 업무에 압도되고 지루하다고 느끼게 되면 공격자처럼 생각하기 어려워집니다. 능력이나 의지가 없어서가 아니라, 기계처럼 반복되는 작업을 하다 보면 긴급성과 집중력이 무뎌지기 때문입니다. 알림 티켓을 1,000개쯤 받고 나면 범죄자를 저지하고 비즈니스를 보호해야 한다는 시야가 흐릿해지기 시작합니다.

이렇게 되면 비즈니스에 리스크가 발생할 뿐만 아니라, 애널리스트가 스카우트 제의에 흔들리기도 쉬워집니다. 사이버 보안 인재가 부족하기 때문에 노련한 애널리스트에게는 항상 이직 제안의 유혹이 따릅니다. 사용을 꺼리는 레거시 기술밖에 없는 기업에 머무를 이유가 없기 때문입니다.

이 또한 비즈니스에 리스크를 발생시킵니다. SOC 팀은 대개 규모가 작기 때문에 전문 지식을 보유한 애널리스트가 퇴사하면 그 간극으로 인해 취약점이 생기게 됩니다. 팀 내 다른 누군가가 그 자리를 대신하기 위해 고군분투하지만 새로 배정된 사람은 뭔가 놓칠 가능성이 큽니다.

자동화 및 AI 기반 솔루션으로 SecOps 업그레이드

SOC 팀에 활기를 불어넣고 전략적 사고 능력을 회복하려면 우선 중요하지 않은 작업부터 배제해야 합니다.

AI를 활용해 위협 해결, 인시던트 대응 지원

- 여러 데이터 소스에서 이상 패턴을 자동으로 탐지하고 컨텍스트를 포함한 알림을 제공하여 인간의 의사 결정에 따라 작용하는 자동화를 구현할 수 있습니다.
- 수백만 건의 공격에서 확보한 인텔리전스를 토대로 데이터를 수집, 구성, 해석할 수 있는 AI 기반 솔루션을 이용하여 SOC 팀원들의 전문 지식을 보강하고 뒷받침할 인사이트를 제공할 수 있습니다.
- AI 솔루션을 도입하여 보안 전문가의 역량을 강화하고 보완함으로써 조사 속도를 개선하고 사각지대를 줄일 수 있습니다.

주요 기능을 자동화하여 잡무 감소

- 자동화를 스마트하게 활용하면 직원의 번아웃을 예방하고 직원 유지율을 개선할 수 있습니다.
- 반복적이고 수준 낮은 작업을 자동화하는 솔루션을 도입하면 애널리스트를 대신하는 것이 아니라, 애널리스트가 원래 수행해야 하고 즐길 수 있는 일, 바로 진짜 위협 조사에 집중할 시간을 확보할 수 있습니다.

애널리스트에게 더 몰입되고 만족스러운 업무 환경 제공

- 자동화로 인해 발생하는 우려 사항과 변화를 인지하고, 이러한 도구가 궁극적으로 애널리스트의 업무에 더 큰 의미를 부여해 준다는 점에 집중할 수 있습니다.
- 여러 팀을 통합하고 사일로를 분해해 SOC 전반에 대한 주인의식과 공동 책임 의식을 갖도록 할 수 있습니다.
- 지속적인 학습 문화를 조성할 수 있습니다. 다양한 분야(알림 분류, 인시던트 대응, 위협 헌팅, 컨텍스트 등)에 걸쳐 모든 팀원에게 교차 교육을 제공하여 SOC 전체에 더 넓은 커버리지를 확보하고 모두가 공격자처럼 생각하는 법을 배우도록 지원할 수 있습니다.
- 팀원이 빠르게 스킬을 향상하고 새로운 공간에서 일하며 새로운 기술을 습득하도록 지원할 수 있습니다. 그러면 자동화로 업무량 부담을 다소 덜게 되었을 때 필요한 역량을 갖추게 됩니다.

이점

애널리스트 지원

보안 애널리스트가 실제로 좋아하는 일에 집중할 수 있으면 성과가 더 좋아질 수 있습니다.

가시적 효율성 향상

연구 모델링 결과에 따르면 AI 기반 자동화는 인시던트 관리 효율을 높여 3년간 $150만 규모의 생산성 가치를 창출했으며, 조사가 필요한 인시던트를 70% 감소시키고 해결 속도를 85% 높였습니다.[10]

보안 태세 강화

고성능, 최신 SOC를 갖춘 기업은 유능한 팀원을 고용하고 유지할 가능성이 큽니다.

인시던트 처리 간소화

인시던트 티켓을 자동화하고 필요할 때 적절한 담당자에게 빨리 전달할 수 있으면 인시던트를 처리, 종결하는 속도가 빨라집니다.

사일로 감소, 지식 공유 확대

특정 지식을 보유한 한 사람이나 여러 사람에 대한 의존도를 낮추세요. 그보다는 더 많은 사람이 큰 그림을 파악하고 조치를 취할 수 있는 역량을 갖추도록 해야 합니다.

10. *Palo Alto Networks Cortex XSIAM의 Total Economic Impact™, Palo Alto Networks를 대신해 Forrester Consulting에서 실시한 위탁 연구, 2025년 9월. 이 결과는 인터뷰에 참여한 고객의 이야기를 토대로 구성된 복합 조직의 사례입니다.*

컨텍스트 간극으로 인해 사각지대 발생

레거시 SOC에는 위협 인텔리전스 데이터를 수집, 처리, 컨텍스트를 부여할 능력이 없는 경우가 많습니다. 네트워크, 디바이스, 다른 엔드포인트가 늘어나면서 공격 표면이 확장됨에 따라 SOC에 그 모든 소스를 받아들일 수도 없고, 대량의 데이터를 수용하기 위해 확장하기도 어렵습니다.

하지만 컨텍스트가 빠진 데이터 포인트는 그저 숫자에 불과합니다. 공격자가 특정 소스에서 유입되는 이유가 무엇인지, 여러 공격이 서로 어떤 관계인지 파악해야만 올바른 대응책을 수립할 수 있습니다. 예를 들어 해외로 사업을 확대하는 기업의 경우, 이전에는 위협으로 인식한 적 없던 해외 공격자의 표적이 될 수 있습니다. 그러면 새로운 공격을 예상할 수 있고, 관리도 쉽습니다.

컨텍스트에서는 관계도 중요합니다. 여러 디바이스나 데이터 개체, 또는 환경이 서로 어떻게 관련되는지 알아야 합니다. 컨텍스트에는 과거 데이터와 현재 이벤트를 연결 짓는 능력이 필요합니다. 여기에는 실제 출처에서 얻은 실시간 데이터도 포함되며, 이러한 데이터를 기반으로 위협의 성격과 의도를 더 잘 파악할 수 있습니다.

모든 데이터 소스를 수집하여 하나의 전체로서 분석할 수 있는 단일 시스템이 없으면 SOC의 가시성이 제한됩니다. 비즈니스 전체에 걸친 일관된 컨텍스트 인식형 보기를 확보하지 못하면 진정한 리스크 수준과 그 의미를 파악하기 어렵습니다.

가시성 부족은 의사 결정과 위협 대응 속도를 둔화하는 원인

가시성과 컨텍스트가 한정되어 있으면 보안팀이 매사를 수동으로 다시 확인하지 않는 이상 빨리 결정을 내리거나 대응하기 어렵습니다. 이것이 옳은 선택일 수도 있지만, 공격자가 데이터를 빼낼 시간을 더 벌어주는 격이 될 수도 있습니다.

포괄적인 가시성이 확보되지 않을 경우 조직은 훨씬 높은 침해 리스크에 직면하게 됩니다. Forrester TEI 연구에 따르면 통합 데이터 레이크를 갖춘 AI 기반 플랫폼은 보안 태세를 60% 개선하고, $220만이 넘는 침해 리스크 비용을 절감할 수 있습니다.[11]

가시성과 컨텍스트는 인시던트가 발생한 뒤에도 매우 중요합니다. 분리된 여러 보안 도구에서 각각 수집한 정보로 데이터 소스를 통합하고, 일관된 타임라인을 작성하려면 추측에 의존해야 할 수밖에 없습니다.

실제로는 무슨 일이 벌어지고 있는 것일까요? 레거시 SOC에서도, 보통은 일이 벌어지고 난 뒤에 실태를 파악하게 됩니다. 하지만 실시간으로 상황을 파악하기가 매우 어렵습니다. 기업에서는 통합형, 컨텍스트 인식형 플랫폼 없이는 가장 중요한 순간에 대한 종합적인 데이터 기반 인사이트를 확보할 수 없습니다.

11. *Palo Alto Networks Cortex XSIAM의 Total Economic Impact™, Palo Alto Networks를 대신해 Forrester Consulting에서 실시한 위탁 연구, 2025년 9월. 이 결과는 인터뷰에 참여한 고객의 이야기를 토대로 구성된 복합 조직의 사례입니다.*

데이터의 배후 사정 파악

데이터가 통합되고 동기화되면 무엇이, 언제, 어떻게 일어났는지 상황을 전할 수 있으므로 SOC 팀에서 다음에 어떤 조치를 취해야 할지 확신을 가질 수 있습니다.

데이터 소스를 한곳에 통합

- 네트워크, 클라우드, 엔드포인트 디바이스 등에서 데이터를 수집해 비즈니스에 영향을 미치는 모든 것에 대한 완벽한 보기를 생성하세요.
- 위협, 취약점, 비즈니스 컨텍스트에 관한 데이터를 한 개의 통합된 보기로 제공하는 플랫폼을 구현해야 합니다.

컨텍스트와 인사이트를 얻기 위해 지능형 분석 활용

- 단편적인 정보를 연결해 완전한 타임라인을 도출하는 도구를 사용하면 위협이 어떻게 이동했고, 어떤 전략을 이용했는지, 전반적인 패턴, 접근 방식, 영향은 무엇인지 알 수 있습니다.
- 데이터 포인트의 경계를 넘는 수준 높은 머신 러닝 기능을 적극 활용하여 모든 요소가 어떻게 연결되어 있는지 자세한 정보를 제공해야 합니다.

이점

중요 컨텍스트

전체 사정을 보면 취약점을 지목하고, 위협이 어떤 식으로 진화하는지 보여주는 인사이트를 확보할 수 있습니다.

영향 명확성

애널리스트가 완전한 컨텍스트 기반 정보를 확보하면 인시던트의 범위와 영향을 파악하는 데 도움이 됩니다.

준비 상태 강화

컨텍스트와 가시성을 보유한 팀은 향후 공격에 대비해 방어 능력을 키워 준비성을 갖출 수 있습니다.

위협 차단에 시간이 너무 오래 걸림

애널리스트가 알림을 조사하고 종결하려 애쓰는 동안, 진짜 위협이 몇 주, 심지어 몇 달 동안 탐지되지 않은 채 방치될 때가 많습니다. 실제로 침해를 탐지했다고 해도 위협을 억제하려면 잘 조율된 대응이 필요한데 여러 포인트 솔루션을 보유하고 있는 경우 어려운 작업일 수 있습니다.

네트워크, 클라우드, 엔드포인트 전체에서 액세스 포인트를 차단하려면 여러 시스템과 팀원이 동원되어야 합니다. 복잡성이 높다는 것은 결국 공격자를 온전히 억제하고 제거하는 데 시간이 더 오래 걸린다는 뜻입니다.

지연이 발생하면 손실과 타격이 가중됨

위협이 여전히 활성 상태이고, 데이터를 빼내거나 피해를 입히려 활동하고 있다면, 한순간도 허비할 수 없습니다. 지연이 발생하면 비즈니스에 비싼 대가, 데이터 손실, 평판 훼손 등 중대한 피해가 발생할 위험이 있습니다. 억제 시간이 길어지지 않도록 방지하는 가장 좋은 방법은 예방 조치이지만, 침해가 발생했다면 무엇보다 속도가 최우선입니다.

위협을 차단했으면, 바로 전체 범위를 파악해야 합니다. 유출된 데이터가 있는지, 비즈니스의 어느 부분이 영향을 받았는지, 피해를 입은 고객이 있는지 등의 정보는 모두 담당 팀원들이 대응 계획을 세우고 다음 단계를 결정하는 데 도움이 되므로 매우 중요합니다.

평균적으로 보안팀이 **보안 알림 한 건을 해결하는 데 145시간(약 6일)**이 소요됩니다. 전체 기업의 60%는 보안 문제를 해결하는 데 4일 이상 걸립니다.[12]

Forrester TEI 연구에 따르면 AI 기반 플랫폼 도입 시 **MTTR이 85% 단축**되어 조사 시간이 몇 시간에서 분 단위로 줄어듭니다.[13]

연구 모델링 결과에 따르면 포괄적인 AI 기반 SOC 플랫폼을 구축할 경우 **전반적 보안 태세가 60% 개선**되며, 이는 약 $220만 상당의 침해 리스크 감소 효과에 해당합니다.[13]

12. *클라우드 위협 보고서(Cloud Threat Report)*, Unit 42, 2023
13. *Palo Alto Networks Cortex XSIAM의 Total Economic Impact™, Palo Alto Networks를 대신해 Forrester Consulting에서 실시한 위탁 연구, 2025년 9월. 이 결과는 인터뷰에 참여한 고객의 이야기를 토대로 구성된 복합 조직의 사례입니다.*

통합형 인시던트 대응으로 빠르게 반응

랜섬웨어, 공급망 공격부터 DNS 스푸핑까지, 미리 잘 조율된 계획을 준비해 두면 SOC가 빠르고 확고하게 대처할 수 있습니다.

전체 영향 파악

- 고급 AI 기반 도구를 사용해 인시던트와 그 범위에 관한 증거를 수집하여 분석하세요.

공격자 억제 및 제거

- 통합형 해결 기능이 있는 솔루션을 통해 네트워크, ID 관리, 디바이스를 중앙에서 격리하세요.
- 정책이나 적용 지점 하나를 업데이트하려고 각 시스템에 따로 접속하는 것이 아니라, 글로벌 업데이트를 구현하여 이점을 누릴 수 있습니다.

위협 예방 기능 강화

- 상시 위협 모니터링 서비스를 구현하세요.
  - › 대부분의 SOC 팀은 상시 근무하지 않지만, 공격자는 쉼 없이 활동합니다. MDR 서비스를 이용하면 팀에 과중한 업무 부담을 주지 않고도 항상 가시성을 유지할 수 있습니다.
- 미리 대비하세요.
  - › 공격을 시뮬레이션하여 실제로 인시던트가 발생했을 때 신속하고 효과적으로 대응하는 방법을 팀원들에게 교육할 수 있습니다.

이점

리스크 감소

신속한 억제로 비즈니스에 미치는 영향을 줄이고 잠재적 피해 범위를 제한할 수 있습니다.

보안 태세 강화

인시던트 인텔리전스에서 입수한 인사이트로 취약점을 파악하여 문제를 해결할 수 있습니다.

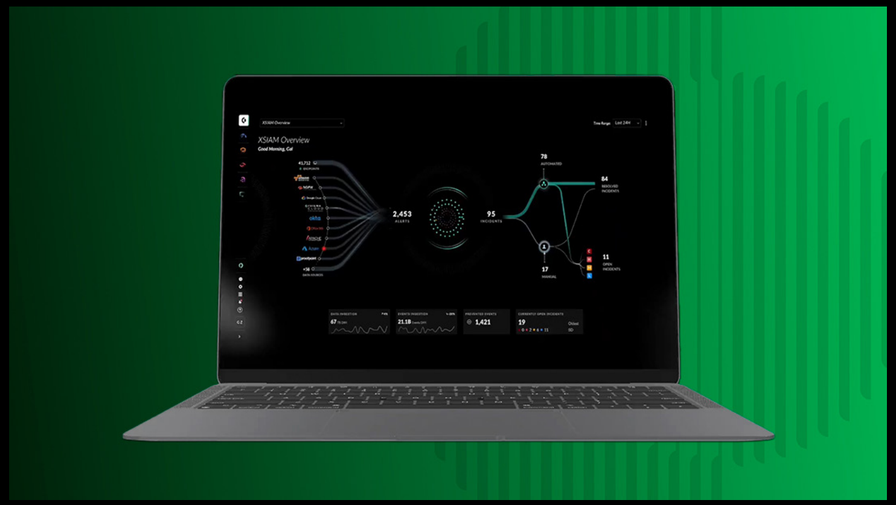
확신 보강

고급 교육과 시뮬레이션을 통해 팀원들의 준비 상태를 구축할 수 있습니다.

총체적 SOC 혁신을 위한 솔루션

Palo Alto Networks®는 레거시 SOC의 어려움과 불만 사항을 잘 알고 있습니다. Cortex XSIAM®은 최신 SOC에 적합한 AI 기반 보안 운영 플랫폼으로 AI 기능을 활용하여 보안 운영을 간소화하고 대규모 위협을 차단하며 인시던트 해결 속도를 높입니다.

여러 제품을 보안 운영 용도로 특별히 설계한 일관된 단일 플랫폼으로 중앙 집중화하여 리스크를 줄이고 운영 복잡성을 완화합니다. XSIAM은 지금의 IT 환경에 맞춰 개발하여 클라우드 및 엔터프라이즈 보안 운영 전체에서 작동하며 어디서든 종합적인 위협 관리를 지원합니다.



Cortex XSIAM:
필수 보안 기능 융합

XSIAM은 SOC 복잡성 문제를 해결하기 위해 보통은 여러 가지 다른 제품을 통해 제공되는 여러 기능을 하나로 모아 줍니다. 예를 들면 다음과 같습니다.

- 보안 정보 및 이벤트 관리(SIEM)
- 엔드포인트 탐지 및 대응(EDR)
- 보안 오케스트레이션, 자동화 및 대응(SOAR)
- 공격 표면 관리(ASM)
- ID 위협 탐지 및 대응(ITDR)
- 위협 인텔리전스 관리(TIM)

XSIAM에서는 이러한 핵심 보안 기능을 단일 플랫폼으로, 인텔리전스 자동화로 지원되는 직관적인 사용자 경험에서 제공합니다.

SOC 팀이 최신 위협보다 우위를 차지하도록 지원

XSIAM은 SOC 내에서 보안 스택을 간소화하고 AI 기반 기능을 도입하여 팀원의 효율성과 능률을 높여주는 것부터 시작합니다. 애널리스트는 자율 보안 플랫폼을 통해 진짜 위협을 식별하고 더 빨리 대응하며 공격자에 맞서 비즈니스를 안전하게 지킬 수 있습니다.

융합형 플랫폼으로 보안 운영 간소화

XDR, SOAR, ASM, SIEM과 같은 다양한 SOC 기능을 단일 플랫폼으로 융합하면 보안 운영에 획기적인 결과를 얻을 수 있습니다. 번거로운 콘솔 전환이 없어지고 간소화된 경험을 제공합니다. 게다가 폭넓은 통합 지원을 제공하여 광범위한 엔지니어링과 인프라 작업 없이도 다양한 데이터 소스를 더 쉽게 온보딩할 수 있습니다.

SOC는 이를 통해 더 많은 보안 관련 데이터를 쉽게 수집할 수 있어 분석 기능이 향상됩니다. 또한 단순한 알림을 넘어 원시 데이터의 지속적인 수집, 연결 및 표준화를 보장합니다. 이를 통해 SOC 팀의 역량이 강화되어 뛰어나면서도 단순화된 조사를 통해 위협을 더 빠르고 효과적으로 파악하여 해결할 수 있습니다.

연구에 따르면 20개가 넘는 서로 다른 보안 도구를 Cortex XSIAM으로 통합할 경우 3년간 약 $310만의 비용을 절감할 수 있습니다. 통합 플랫폼 접근 방식은 공급업체 관련 복잡성을 제거하고 운영 부담을 줄이며, 전반적인 보안 태세를 강화합니다.[14]

AI 기반 결과를 사용해 위협 차단

기본 제공 AI 모델은 기존 탐지 방법을 뛰어넘어 다양한 데이터 소스에 걸쳐 이벤트를 연결하고 단일 위치에서 인시던트와 리스크의 포괄적인 개요를 제공합니다.
이를 통해 조직은 탐지, 분석 및 대응 역량을 강화할 수 있습니다.

Cortex XSIAM은 알림 그룹화 및 AI 기반 인시던트 평가를 활용하여 신뢰도가 낮은 이벤트를 원활하게 연결하고 이를 신뢰도가 높은 인시던트로 전환합니다. 이 우선순위는 전체 리스크를 기반으로 하기 때문에, 보안팀이 효율적으로 작업에 집중할 수 있습니다.

자동화 우선주의 방식으로 인시던트 해결 가속화

SOC는 Cortex Marketplace에서 시도 및 테스트된 수백 개의 콘텐츠 팩을 통해 전체 보안 프로그램 전반의 프로세스와 상호 작용을 최적화할 수 있습니다. 기존의 수동 작업을 자동화하면 공격 표면 노출과 같은 인시던트 대응 또는 리스크 관리에 소요되는 시간과 노력을 절약할 수 있습니다.

또한 사용자는 특정 요구 사항에 따라 자동화를 추가, 사용자 지정 또는 수정할 수 있는 유연성을 갖게 됩니다. 플랫폼에는 자동으로 트리거되는 알림별 플레이북이 포함되어 있어 애널리스트가 참여하기 전이라도 보안 작업이 신속하게 실행되고 리스크가 해결됩니다. 뿐만 아니라, XSIAM은 수동 애널리스트 작업을 학습하여 향후 자동화를 위한 권장 사항을 제공합니다. 이러한 지속적인 학습 프로세스는 플랫폼이 인시던트를 자동으로 해결하는 기능을 강화하며 시간이 지남에 따라 효율성과 정확성이 높아집니다.

14. *Palo Alto Networks Cortex XSIAM의 Total Economic Impact™, Palo Alto Networks를 대신해 Forrester Consulting에서 실시한 위탁 연구, 2025년 9월. 이 결과는 인터뷰에 참여한 고객의 이야기를 토대로 구성된 복합 조직의 사례입니다.*

사례 연구 스포트라이트

Cortex XSIAM으로 자사 SOC를 대대적으로 혁신한 석유 가스 기업

이 회사의 레거시 SIEM은 오탐(false-positive)을 비롯한 알림 과부하를 초래하여 보안팀이 여러 보안 도구에서 수동으로 조사해야 하는 부담을 안겨주었습니다.

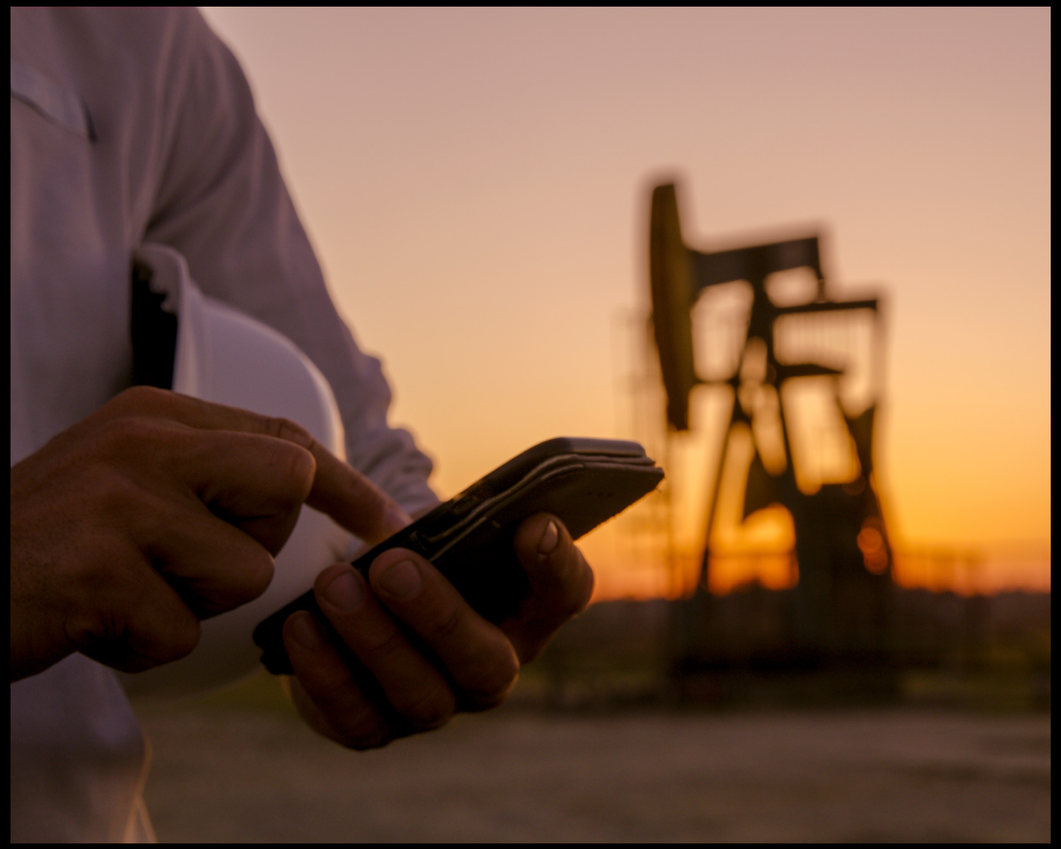
XSIAM을 구현한 후, 이 회사는 빠른 속도로 다음과 같은 결과를 실현했습니다.

- 오탐률이 **약 90%에서 0에 가까운 수준**으로 감소
- 조사가 필요한 인시던트 **75% 감소**

지금은 전보다 더 빨리 잠재적 위협을 탐지 및 예방하고 공격에 대응할 수 있으며 동급 최고 SOC로 성장 중입니다.

"원래는 쓸모없는 알림을 수천 개씩 받곤 했습니다. 이제는 꼭 조사해야 하는 이벤트 수가 일주일에 5건 정도 됩니다. 그 정도로 시스템 성능이 훌륭합니다."

– 석유 및 가스 기업 IT 보안 책임자



전체 사례 읽기

사례 연구 스포트라이트

Cortex XSIAM으로 애널리스트 효율을 높이고 준비 상태를 보강한 Boyne Resorts

미국과 캐나다 전역에 스키, 골프 리조트를 운영 중인 기업에서는 증원 없이 SOC 역량을 강화하고 분산된 환경 전체에 대한 가시성을 보강하고자 했습니다.

Boyne Resorts에서 XSIAM을 구현한 후 실현한 이점은 다음과 같습니다.

- 데이터 수집량 **70배 증가**
- 오탐률이 낮아지고 중복 인시던트를 줄인 덕분에 미결 인시던트 수를 일일 80~100건에서 35건으로 **65% 감소**
- 조사에 필요한 도구와 대시보드를 20여 종에서 하나로 줄여 공급업체와 도구 **95% 감소**

요즘은 SOC가 전보다 더 간결해지고 성능이 개선되어 보안팀에서도 최신 위협에 맞서기 위해 가시성과 인사이트를 강화하고 대비를 잘 갖추고 있습니다.

"XSIAM 덕분에 가시성이 높아지고 조사 속도가 빨라졌습니다. 원활한 데이터 온보딩과 자동화 설정이 정말 획기적입니다."

– Mike Dembek, Boyne Resorts 네트워크 아키텍트

전체 사례 읽기

사례 연구 스포트라이트

Forrester TEI 연구: 글로벌 기술 서비스 기업, Cortex XSIAM으로 3년 ROI 257% 달성

Cortex XSIAM의 가치를 정량화하기 위해 Forrester Consulting은 Palo Alto Networks의 의뢰로 4개 조직에 대한 인터뷰를 바탕으로 Total Economic Impact™ 연구를 수행했습니다. 이 연구는 직원 10,000명, 연매출 50억 달러 규모의 글로벌 기술 서비스 회사를 모델로 하여 분산된 보안 아키텍처, 과도한 알림 양, 레거시 SIEM 플랫폼에 의한 비용 증가 등 현대적 SOC가 일반적으로 마주하는 과제에 직면한 복합 조직으로 모델링했습니다. 이 조직은 높은 오탐률, 사일로화된 도구 간 수동 상관관계 분석, 반복적 분류 작업에 의한 애널리스트 번아웃 문제로 어려움을 겪고 있었습니다.

그러나 Cortex XSIAM을 도입해 SIEM, SOAR, XDR, 위협 인텔리전스 기능을 통합한 후, 이 복합 조직은 3년간 다음과 같은 정량적 성과를 달성했습니다.

재무적 영향:

- 3년 투자 수익률(ROI) **257%**
- 순 현재가치 **560만 달러**
- 투자 회수 기간 **6개월 미만**
- 총 이익 **$770만**, 총 비용 **$220만**

운영 효율 향상:

- Tier 1 SOC 주의가 필요한 알림 **85%** 감소
- 조사가 필요한 인시던트 **70%** 감소
- 평균 해결 시간(MTTR) **85%** 단축
- 보안 태세 **60%** 개선($220만 가치)

출처: Palo Alto Networks Cortex XSIAM의 Total Economic Impact™, Palo Alto Networks를 대신해 Forrester Consulting에서 실시한 위탁 연구, 2025년 9월. 이 결과는 인터뷰에 참여한 고객의 이야기를 토대로 구성된 복합 조직의 사례로 실제 결과를 보장하지 않습니다.

"플랫폼의 AI 기반 분석과 통합 데이터 모델 덕분에 오탐과 수동 분류 작업이 크게 줄었습니다. 당사의 애널리스트들은 반복 작업 대신 전략적 위협 헌팅 및 선제적 방어에 집중할 수 있게 되었습니다. 몇 개월 만에 ROI가 눈에 띄게 달라졌고 이사회는 우리의 민첩하고 효율적인 변화를 명확히 인식하고 있습니다."

– 기술 서비스, 전문 소매, IT 서비스, BPO 기업 부문에서 연구를 위해 인터뷰에 참여한 보안 리더들의 종합 의견

비용 절감:

- 레거시 SIEM, SOAR, EDR/XDR, 기타 포인트 도구 제거로 **$310만** 절감
- 분류 효율 개선으로 **$93만** 가치 창출
- 사례 관리 향상으로 **$150만** 가치 창출

Forrester TEI 연구 읽어보기

고성능 SOC를 향한 진전

동급 최고의 SOC 도구를 결합한 통합형 플랫폼이므로 보안팀이 XSIAM을 믿고 비즈니스를 보호하는 데 필요한 강력한 탐지, 대응, 조사 기능을 활용할 수 있습니다. 어떤 미래가 기다리고 있든 걱정하지 않아도 됩니다.

Palo Alto Networks Cortex XSIAM에 관해 자세히 알아보기

시작하기

paloalto NETWORKS | CORTEX

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