# 8곳의 조직에서 Cortex®를 통해 보안 운영을 혁신한 방법

paloalto® NETWORKS | CORTEX®

서문

# 지금부터 미래의 SOC를 준비하세요

## 이제 인력으로는 사이버 보안을 따라갈 수 없는 시대에 접어들었습니다.

SOC(보안 운영 센터) 팀의 규모나 팀원들의 능력 여부는 더 이상 중요하지 않습니다. 인력만으로는 진행 중인 공격을 차단할 만큼 빠른 속도로 대응할 수 없습니다.

따라서 우리에게는 사이버 보안을 자동화할 올바른 모델, 올바른 리소스, 올바른 데이터로 오늘날 네트워크에서 발견되는 위협의 양과 정교함을 처리할 수 있는 AI가 필요합니다.

이것이 Cortex®를 구축한 이유입니다. 보안 위협의 탐지와 대응 시간을 며칠에서 몇 초로 단축할 수 있도록 설계된 사이버 보안의 새로운 비전이라 할 수 있습니다.

이 전자책에서 확인할 수 있듯이, Cortex를 사용하는 고객은 SOC 팀을 강화하고 성과를 높이는 동시에, 더욱 가시적이고 포괄적이며 미래에 대비한 보안으로 발전하고 있습니다.

당사는 보안 공급업체로서 해당 기업들과 협력하며 이들의 사례를 소개할 기회를 갖게 된 것을 매우 영광으로 생각합니다.

paloalto® NETWORKS

스냅샷 1: 노스다코타주

# 공공 부문의 미래에 대비하는 SOC

노스다코타주는 시민들이 이용할 수 있는 기술을 제공하기 위해 최선을 다하고 있습니다. 이 임무 수행을 위해 노스다코타 정보 기술(NDIT)은 도심에서 농촌 지역에 이르는 모든 정부 기관에 보안을 제공합니다. 이 네트워크의 규모와 복잡성은 Fortune 30대 기업의 네트워크와 견줄 수 있을 정도이기 때문에 보안이 최우선 과제일 뿐만 아니라 매우 어려운 과제이기도 합니다.

NORTH Dakota
Be Legendary.

**업종**
공공 부문

**국가**
미국

**웹사이트**
www.ndit.nd.gov

**80만+**
시민

**1,600+**
도시 및 행정구역

**183**
독립 학군


paloalto NETWORKS

스냅샷 1: 노스다코타주


# NDIT는 주요 인시던트 없이 주 시민과 기관을 위한 자동화되고 선제적인 보호 기능을 제공함으로써 공공 부문의 성공적인 보안 운영 모델이 되었습니다.

> 현재 우리는 Fortune 30대 기업과 비슷한 규모를 약 절반의 리소스로 운영하고 있습니다. 이것은 머신 러닝을 사용하는 최신 플레이북과 자동화를 통해 가능합니다. 이를 통해 SOC 팀은 비즈니스에 가치를 더하는 더 높은 우선순위 작업에 집중할 수 있습니다."
>
> **— Michael Gregg, 노스다코타 정보 기술 최고 정보 보안 책임자**

## 과제

수십만 명의 사용자, 수천 개의 통합 및 애플리케이션, 무수한 엔드포인트를 가진 NDIT는 독보적인 효율성으로 시스템 전체에서 작동할 수 있는 자체 SOC를 계획, 설계 및 구축해야 했습니다.

- 점점 더 정교해지는 사이버공격이 시민 데이터와 기관 운영을 위협했습니다.
- 2021년 45억 건으로 두 배가 된 위협 탐지를 관리할 통합 솔루션이 필요했습니다.
- 솔루션은 확장 가능하고 포괄적이며 미래를 대비할 수 있어야 했습니다.

## 솔루션

NDIT는 Palo Alto Networks와의 협력으로 3년 간 자체 SOC를 구축했습니다. Cortex XDR, XSOAR 및 Xpanse를 포함한 완전한 Cortex 제품 포트폴리오를 통합함으로써 엔드포인트 보안, 작업 자산 검색 및 워크플로 자동화를 위한 포괄적인 기반을 제공했습니다.

- 통합 프레임워크로 첫 호출 해결이 향상되고 평균 대응 시간(MTTR)이 단축되었습니다.
- 2.17 FTE의 업무를 백그라운드의 시스템으로 전환하여 팀원들이 더 높은 우선순위의 분석과 위협 복구에 집중할 시간을 확보했습니다.
- 더 투명한 운영 구조로, 미국 국립표준기술연구소 프레임워크를 매핑했습니다.

스냅샷 2: HEALTHPARTNERS

# 의료 서비스 리더로서의 보안 혁신

미네소타 블루밍턴 소재의 HealthPartners는 수상 경력을 자랑하는 통합 의료 시스템으로 임상 서비스와 의료 보험을 제공합니다. 기업 목표는 회원, 환자 및 지역 사회의 건강과 복지 증진입니다. 25,000명의 직원을 보유한 미국 최대의 소비자 관리 비영리 단체인 HealthPartners는 180만명의 의료 및 치과 회원에게 서비스를 제공합니다. 임상 서비스에는 120만명 이상의 환자를 담당하는 약 1,800명의 의사들의 다중 전문 그룹 실습이 포함되어 있습니다.

**업종**
의료

**국가**
미국

**웹사이트**
www.healthpartners.com

**25,000**
직원 수

**180만**
회원

**1,800**
의사

스냅샷 2: HEALTHPARTNERS

# Cortex는 SOC 강화를 통해 취약점을 선제적으로 제거하고 탐지 및 조사를 자동화하며 수동 개입이 필요한 위협의 극히 일부에만 직원 시간을 집중할 수 있도록 하여 HealthPartners의 디지털 이니셔티브를 가속화했습니다.

> Palo Alto Networks 플랫폼에서 얻고 있는 높은 비율의 일관성과 높은 탐지 정확도 덕택에 이제 위협 완화를 자동화할 수 있다는 확신을 갖게 되었습니다. 지금까지 한 번도 기회가 없던 일이죠."

**— Joel Pfeifer, HealthPartners 수석 보안 애널리스트**

## 과제

사이버공격이 임상 서비스와 의료 보험의 개인 환자 데이터를 끊임없이 위협함에 따라, HealthPartners는 새로운 하드웨어에 대한 대규모 투자 없이 전체 보안 솔루션을 개선해야 했습니다.

- 레거시 방화벽은 HealthPartners가 필요로 하는 보안을 더 이상 제공하지 못했습니다.
- 부족한 엔드포인트 보호로 인해 기업 디바이스 전체에 취약점이 생겨났습니다.
- 필터링되지 않은 알림의 세부 사항 부족으로 SOC의 수동 분석이 필요했습니다.

## 솔루션

HealthPartners는 Cortex XDR, XSOAR 및 Xpanse를 비롯한 Palo Alto Networks Cortex 포트폴리오를 구현했습니다.

- Cortex는 경쟁사의 절반에 불과한 비용으로 여러 시스템을 하나의 플랫폼으로 통합했습니다.
- 통합 위협 인텔리전스가 첫 한 해 동안 수십 건의 사이버공격을 차단했습니다.
- 사이버위협 활동과 시작 지점에 대한 전반적인 가시성과 심층적인 인사이트로 SOC가 강화되었습니다.

스냅샷 3: BETTER.COM

# 금융 혁신 기업을 위한 원활한 보안

빠르게 성장 중인 미국 내 디지털 주택 보유 플랫폼 중 하나인 Better.com은 더 빠르고 투명하며 접근성 높은 프로세스를 구축하기 위한 기술을 사용하여 고객의 주택담보대출과 보험의 보안 방식을 간소화하고 있습니다. 950억 달러가 넘는 주택 대출 자금으로, 고객의 데이터와 비즈니스를 주도하는 기술을 보호하는 것이 그 무엇보다 중요합니다.

Better

**업종**
금융

**국가**
미국

**웹사이트**
www.better.com

**5,000+**
직원 수

**10,000+**
엔드포인트

**$950억**
대출

스냅샷 3: BETTER.COM

# Cortex를 통해 Better.com의 보안 속도와 효율이 향상되었으며, SOC 팀은 반응적 태세가 아닌 선제적 대세로 전환하여 기업이 고객의 주택 보유 업무를 간소화할 수 있는 이니셔티브에 집중할 시간을 확보했습니다.

"XDR과 함께 사용할 수 있는 XSOAR 조사와 자동화를 통해 워크플로 내에서의 명령 실행이 대폭 원활해지고, 완전한 킬 체인 이벤트를 구축했으며, 정말 빠른 속도로 복구 업데이트가 가능했습니다."

**— Jeff White, Better.com 보안 책임자**

## 과제

Better.com은 빠르게 성장 중인 대규모 네트워크 전체에서 취약점을 평가하고 위협을 복구 업데이트할 수 있도록 더 빠르게 움직일 수 있는 SOC 팀을 강화해야 했습니다.

- 기존 EDR 솔루션에서 생성하는 알림은 세부 정보의 부족으로 인해 신뢰할 수 없었습니다.
- SOC는 수동 워크플로와 복구 단계로 인한 과중한 업무에 시달렸습니다.
- 회사는 모든 데이터에 대한 전반적인 가시성이 필요했습니다.

## 솔루션

Better.com은 Cortex XDR, XSOAR, NGFW, Panorama®, Prisma® Access를 비롯한 Palo Alto Networks의 포괄적인 보안 솔루션 세트를 도입하여 보다 간단하고 선제적인 보안으로 전환했습니다.

- 데이터, 사용자, 애플리케이션, 인프라 및 엔드포인트 전체를 단일 창을 통해 확인할 수 있습니다.
- EDR 자동화와 대응 오케스트레이션으로 워크플로가 향상되고 범위가 넓어집니다.
- 솔루션이 모든 공격을 차단하고 네트워크 전체와 침투 테스트에서 공격 시도를 완벽하게 파악할 수 있도록 지원합니다.

스냅샷 4: KHIPU NETWORKS

# 보안 고객이 신뢰할 수 있는 기업

수상 경력에 빛나는 국제 사이버 보안 기업 KHIPU Networks는 여러 부문의 고객을 대상으로 글로벌 시장 전체에 전 세계적 수준의 보안 네트워크를 제공합니다. 사이버공격으로 인한 데이터 손상, 디지털 전략의 중단, 명성의 피해 가능성을 우려하는 고객을 위해 KHIPU Networks는 2019년 영국 최초로 eXtended Managed Detection and Response(XMDR) 서비스를 출시했습니다.

By Appointment to
Her Majesty the Queen
Network Security Provider
KHIPU Networks Limited
Hampshire

KHIPU CYBER SECURITY

**업종**
사이버 보안

**국가**
영국

**웹사이트**
www.khipu-networks.com

**1ST**
영국 내 XMDR 공급업체

**19+**
사이버 보안 경력

**500+**
고객

paloalto NETWORKS

# Cortex를 기반으로 KHIPU Networks는 다양한 전 세계 고객층의 보안 인사이트에 대한 확신을 가지고 이를 종합하여 탐지와 대응을 강화하고 지속적인 위협 인텔리전스를 구축하고 있습니다.

> Palo Alto Networks 포트폴리오는 단순성, 자동화, 정확성이라는 특성으로 다른 보안 운영 솔루션보다 훨씬 더 매력적입니다. 전체 환경에서 단일 데이터 소스의 완벽한 가시성과 관리형 서비스로서의 대응 능력을 고객에게 제공할 수 있습니다."
>
> **— Guy Jermany, KHIPU Networks 최고 정보 책임자**

## 과제

성공을 위해 KHIPU Networks는 복잡하면서 각기 다른 요구 사항을 가진 다양한 산업의 고객에게 관리형 서비스로 사내 SOC의 이점을 제공해야 했습니다.

- 고객들은 IT 복잡성의 증가, 팬데믹 이후의 원격 근무, 하이브리드 온프레미스와 클라우드 인프라 및 기타 문제로 인해 보안에 어려움을 겪었습니다.
- 각 고객의 요구 사항, 환경, 우선순위 및 예산을 충족하기 위해서는 솔루션의 유연성이 필요했습니다.
- 고객은 인력 채용과 실질적인 사이버 보안 전문가 보유에 난항을 겪었으며, 특히 대응 및 조사를 위한 상시 가용성이 필수로 요구되는 상황에 어려움을 호소했습니다.
- KHIPU Networks는 증가하는 사이버공격 환경에서 랜섬웨어에 대응하는 동시에 이를 억제해야 했습니다.

## 솔루션

KHIPU Networks는 Palo Alto Networks Cortex XDR과 XSOAR을 중심으로 자체적인 XMDR 서비스를 구축하여, SOC 지원에 필요한 분석, 워크플로 및 작업 관리와 함께 선제적인 탐지 및 대응을 보장합니다.

- 여러 포인트 제품과의 향상된 통합으로 KHIPU Networks는 위협에 대한 즉각적인 대응, 억제 및 조사 기능을 제공합니다.
- 자동화된 AI 및 ML 프로세스가 위협을 예방, 탐지 및 제거하며 이를 통해 KHIPU Networks는 수많은 기업을 위한 SOC 역할을 수행하고 있습니다.
- 모든 단계의 공격을 표면화하여 조사 시간을 줄이고 KHIPU Networks 애널리스트의 가치를 극대화합니다.
- 경제적이고 유연하고 확장 가능한 사이버 보안 서비스로, 규모에 관계없이 모든 업종의 기업이 KHIPU Networks의 XMDR 서비스에 자신 있게 투자합니다.

스냅샷 5: ASCEND MONEY

# 핀테크 유니콘의 SOC 자동화

Ascend Money는 2013년 설립되어 동남아시아 전역에서 은행이 부족한 지역에 최첨단 금융 기술을 도입하였으며, 현재는 태국에서 빠르게 성장 중인 스타트업입니다. 현재, 기업의 디지털 전자 지갑인 TrueMoney Wallet은 태국, 인도네시아, 베트남, 미얀마, 캄보디아, 필리핀에서 5천만 명이 넘는 사람들이 사용하고 있습니다.


ascend money

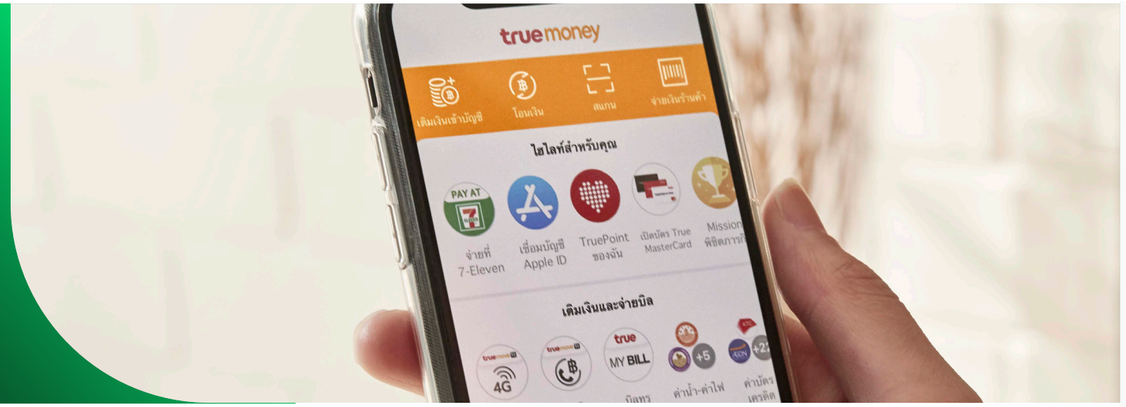
**업종**
금융

**국가**
태국

**웹사이트**
www.ascendmoneygroup.com

| 2,000 | 5,000만 | 6 |
| --- | --- | --- |
| 직원 수 | 고객 | 국가 수 |

paloalto NETWORKS




## 최근 국제적 위기 상황에서 위협이 급증하는 가운데, Cortex XDR과 XSOAR은 Ascend Money를 보호하고 자사 파트너와 고객의 데이터가 안전하게 유지되고 있다는 확신을 심어 주었습니다.

> Palo Alto Networks의 Cortex XDR은 간소화된 통합과 보안 자동화 기능을 제공하여 운영 시간을 크게 단축할 수 있었습니다."
>
> **— Kanokwan Aimsumang, Ascend Money IT 보안 및 거버넌스 책임자**

### 과제

핀테크 기업은 끊임없이 공격의 대상이 되어 왔으며, Ascend Money는 자산을 보호하고 빠르게 확대되는 자사 고객층의 금융 정보를 보호할 솔루션이 필요했습니다.

- 네트워크의 성장은 엔드포인트 보안의 잠재적 격차에 대한 우려를 낳았습니다.
- SOC는 대용량의 필터링되지 않은 알림으로 인해 고군분투했습니다.
- 사이버 공격 상황에서도 비즈니스가 중단되지 않아야 했습니다.
- AI 및 ML 사용을 위해 기술 업그레이드 지원이 필요했습니다.

### 솔루션

Ascend Money는 보안 파트너인 True Digital Cyber Security를 통해 제공되는 Cortex XSOAR과 함께 Cortex XDR을 활용하여 엔드포인트 탐지 및 대응을 자동화했습니다.

- XDR의 확장된 엔드포인트 보호를 통해 커버리지를 넓혀 잠재적 격차를 해소합니다.
- AI 및 ML 기반 보안 자동화로 SOC에서 더 높은 가치의 작업에 집중할 수 있습니다.
- XDR과 XSOAR의 확장성으로 계속되는 증가세에 보안의 속도를 맞출 수 있습니다.
- 간소화된 통합과 보안 자동화로 운영 시간이 크게 줄어들었습니다.

스냅샷 6: FORVIA FAURECIA

# 제조업체의 디지털 혁신에 맞는 보안

세계 최고의 자동차 부품 제조업체 중 하나인 Forvia Faurecia는 자율 주행, 전기화, 연결성 및 기타 트렌드를 향한 업계의 변화에 발맞춘 차세대 기술을 빠르게 구축하고 있습니다. 전 세계에서 운영되는 기업으로서, 디지털 혁신을 주도하고 가동 시간을 보장하며 리스크를 줄일 수 있는 회복력 있는 최신 사이버 보안 전략을 필요로 합니다.

**업종**
제조

**국가**
프랑스

**웹사이트**
www.faurecia.com

**10만+**
직원 수

**30+**
국가 수

**250+**
산업 현장

스냅샷 6: FORVIA FAURECIA

# Cortex XSOAR은 SOC 팀의 대응을 보다 지능적이고 효율적이며 통합된 방식으로 발전시키며 70% 더 높아진 생산성을 이끌어냈습니다.

"새로운 내부 솔루션의 최근 릴리스에서 생성되는 알림은 거의 20,000개에 달하지만 이 중 수동으로 처리하는 것은 200개도 되지 않습니다. 나머지는 모두 자동으로 처리되죠. 이로써 수동 워크로드가 99% 감소했으며, 우리는 XSOAR 투자에 대한 즉각적인 수익을 달성한 셈입니다."

**— Matthieu Favris, Forvia Faurecia 인시던트 대응 관리자**

## 과제

EDR 및 SIEM 시스템, 멀티 클라우드 환경, 최종 사용자로부터의 필터링되지 않은 알림으로 인해 SOC 팀은 과중한 업무 부담에 시달렸습니다.

- SOC 팀은 낮은 우선순위 알림과 실제 긴급 상황을 구분할 수 없었습니다.
- 알림을 수신 및 처리할 수 있는 단일 플랫폼이 부족했습니다.
- 모든 알림에 응답하지 않으면 비즈니스가 위험에 노출됩니다.

## 솔루션

Forvia Faurecia는 Cortex XSOAR을 구현하여 알림을 통합하고 자사의 SOC를 위한 작업 관리를 지원했습니다.

- XSOAR은 SIEM, EDR 및 기타 소스로부터 수집되는 알림을 완전히 통합합니다.
- 디지털 워크플로를 사용하여 인시던트 분석 및 대응 절차를 정의함으로써 SOC가 전략적으로 가치 있는 작업에 집중할 수 있습니다.
- 위협 인텔리전스와 자동화로 SOC 워크로드가 대폭 감소했습니다.

스냅샷 7: BANCO DE GALICIA Y BUENOS AIRES

# 금융 선도 기업의 SOC 향상

Banco de Galicia y Buenos Aires는 자국 내 최대 민간 은행 중 하나로, 아르헨티나 전역의 350개 이상 지사에서 기업 및 개인에게 종합 금융 서비스를 제공합니다. 이 기업은 300만 명 이상 고객의 신뢰를 받으며 고객의 투자 관계를 관리하고, 최신 고객이 기대하는 유연성과 디지털 연결을 제공하고 있습니다. 디지털화를 통해 지사, 온라인, Galicia 앱을 막론하고 고객이 있는 곳이라면 어디서든 은행 서비스를 제공하기 위해 최선을 다하고 있습니다.

**업종**
금융

**국가**
아르헨티나

**웹사이트**
www.bancogalicia.com

**350**
지사

**5,000+**
직원 수

**300만**
고객

스냅샷 7: BANCO DE GALICIA Y BUENOS AIRES

# XSOAR의 도입으로 SOC의 시간이 절약되고 팀이 심각한 위협에 집중하며 이를 빠르게 복구 업데이트할 수 있게 되었습니다. 이에 따라 은행 직원의 업무 중단이 감소하고 기업 전체의 생산성이 증가했습니다.

> Cortex XSOAR를 구현함으로써 [일상적인 알림]을 거의 자동으로 관리할 수 있게 되었습니다. 이 덕분에 몇 분이 소요되던 작업이 단 몇 초 만에 관리되었습니다."
>
> **— Ezequiel Invernon, Banco de Galicia y Buenos Aires SOC 및 IR 관리자**

## 과제

기업 전반에 걸쳐 디지털화와 자동화를 추구하는 은행의 노력은 피싱, 데이터 유출, 랜섬웨어 및 기타 공격의 지속적인 위협으로 인해 혼란을 빚고 있습니다.

- 사일로화된 수많은 보안 제품의 알림으로 인해 가장 심각한 위협의 식별이 불가능해졌습니다.
- 낮은 수준의 알림에 대한 수동 복구는 SOC 팀의 리소스를 소진시켰습니다.
- 팀이 심각한 위협을 놓치는 리스크에 빠지며 은행의 보안이 위태로워졌습니다.

## 솔루션

Banco de Galicia y Buenos Aires는 Cortex XSOAR을 도입하여 보안 솔루션과 콘텐츠 서비스 전체의 알림을 통합했습니다.

- XSOAR을 통해 보안 제품과 은행 기술 전체의 알림이 원활하게 통합하여 통합된 단일 보기를 제공합니다.
- IoC, 피싱 인시던트, DLP, 권한 에스컬레이션을 위한 플레이북이 SOC 워크플로를 자동화하고 오케스트레이션합니다.
- 자동 인시던트 대응으로 팀의 리소스가 더 높은 우선순위 알림에 집중할 수 있습니다.

스냅샷 8: AVRASYA TÜNELI

# 대륙 간 횡단을 위한 보안 자동화

터키 이스탄불과 괴즈테페 사이의 보스포러스 해협 아래를 지나는 Avrasya Tüneli(유라시아 터널)는 유럽과 아시아 대륙을 연결합니다. 정교한 기술 인프라가 통행료, 카메라, 환기, 사고 대응 및 수많은 기타 기능을 관리하며 하루에 여행객 65,000명을 위한 경로 안전을 책임지고 있습니다. 사이버 위협으로부터 인프라를 보호해야 했으며, 정보 기술(IT) 책임자 Murat Çalışırişçi는 터널 자체만큼이나 최첨단 보안 솔루션이 필요했습니다.

**업종**
교통

**국가**
튀르키예

**웹사이트**
www.avrasyatuneli.com

**150**
직원 수

**200+**
엔드포인트

**2,000+**
IOT 디바이스


# Avrasya Tüneli에서 발생하는 모든 보안 인시던트는 일일 65,000명 이상 운전자의 안전에 영향을 줄 수 있습니다. Cortex XDR을 통해 추가 인력을 채용하지 않고도 터널의 확실한 보안 태세를 유지할 수 있습니다.

> 통합되어 있고 자동이며 간편합니다. [Palo Alto Networks의] 통합 플랫폼은 단일 창을 통해 모든 주요 보안 데이터를 연결하는 전체적인 보호 기능을 제공합니다. 플랫폼의 모든 구성 요소가 동급 최고이며, 미래에 대비한 제품 구상은 이들이 비전 있는 파트너임을 입증하기에 충분했습니다."
>
> **— Emrah Dündar, Avrasya Tüneli 정보 기술(IT) 부문 선임 관리자**

## 과제

Avrasya Tüneli는 세 명의 보안 전문가로 이루어진 직원에 대한 충원 없이 터널을 지원하는 기술 인프라를 보호해야 했습니다.

- 보안 팀은 단일 인터페이스를 통한 전반적인 가시성이 필요했습니다.
- 상시 모니터링을 위해 200개 이상의 엔드포인트와 2,000개 이상의 IoT 디바이스가 필요했습니다.
- 터널 안전 보장을 위해 대응 시간이 매우 중요했습니다

## 솔루션

Avrasya Tüneli는 Cortex XDR을 구현하는 동시에 Palo Alto Networks 보안 제품의 통합 제품군과의 조합을 통해 탐지 및 대응을 확장했습니다.

- XDR은 사용자 지정 실험 환경에서의 솔루션 테스트 중에 발생한 모든 위협을 차단했습니다.
- 자동화를 통해 수동 워크로드가 감소하고 직원 생산성이 극대화되었습니다.
- 통합 ML 기반 네트워크 트래픽 분석, 엔드포인트 탐지, 사용자 행동 분석으로 IoT 디바이스를 포함하여 모니터링이 간소화되었습니다.

# 보안을 한 단계 업그레이드

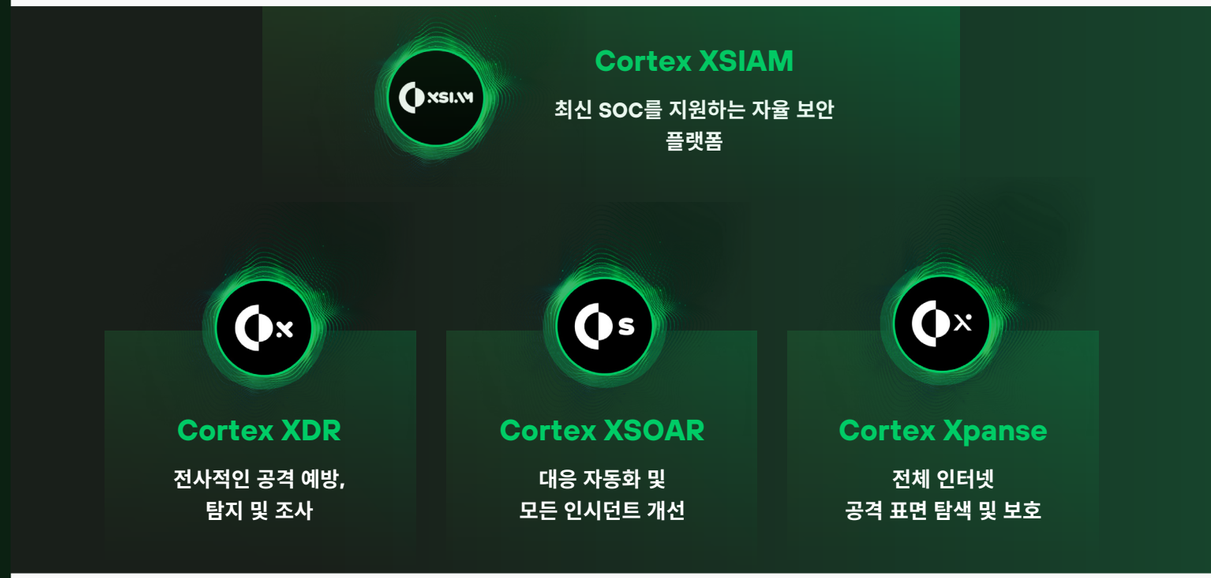
Cortex는 업계 최고의 위협 탐지, 예방, 공격 표면 관리, 보안 자동화 기능을 하나의 통합 플랫폼에 모았습니다. 이를 통해 지속적으로 진화하는 위협 환경에 적응하는 효율적이고 반응이 빠른 보안 운영 센터(SOC)를 구축할 수 있습니다.

위 고객 경험에서 알 수 있듯이 모든 규모의 기업으로 이루어진 Cortex 파트너는 보안 운영과 인시던트 대응을 간소화, 자동화, 가속화하고 있습니다.

**Cortex를 통해 SOC를 강화하는 방법을 자세히 알아보세요.**

여기를 클릭 ⟶

**Cortex 포트폴리오는 기업의 디지털화 전략 추구에 힘을 실어주는 동시에 SOC 팀이 안심하고 안전을 유지할 수 있도록 지원하며 보안 환경을 혁신하고 있습니다.**




- **Cortex XDR®**은 엔드포인트, 네트워크, 클라우드 및 타사 데이터를 기본 통합하여 정교한 공격을 차단하는 업계 최초의 XDR 솔루션입니다.
- **Cortex XSOAR®**은 업계에서 가장 포괄적인 보안 오케스트레이션 플랫폼으로, 모든 보안 사용 사례를 위한 자동 워크플로를 통해 보안 운영을 향상시킵니다.
- **Cortex Xpanse®**는 진화하는 인터넷 공격 표면 전반의 알려지지 않은 요소들을 매핑하며 보이지 않는 요소를 가시화함으로써 모든 보안 투자의 ROI를 높입니다.
- **Cortex XSIAM®**은 AI 기반 자동화의 강력한 기능을 활용하는 자율 SOC 플랫폼으로, 보안 성과를 대폭 개선하고 보안 운영을 혁신합니다.
- **Unit 42® MDR**은 다년간의 경험을 적용하여 환경을 모니터링하고 의심스러운 모든 것을 확인합니다. 상시 근무하는 애널리스트와 Cortex XDR의 데이터를 통한 정렬 기능으로 전체 상황을 파악할 수 있습니다.

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


cortex_eb_how-eight-corporations_101724