paloalto NETWORKS | CORTEX

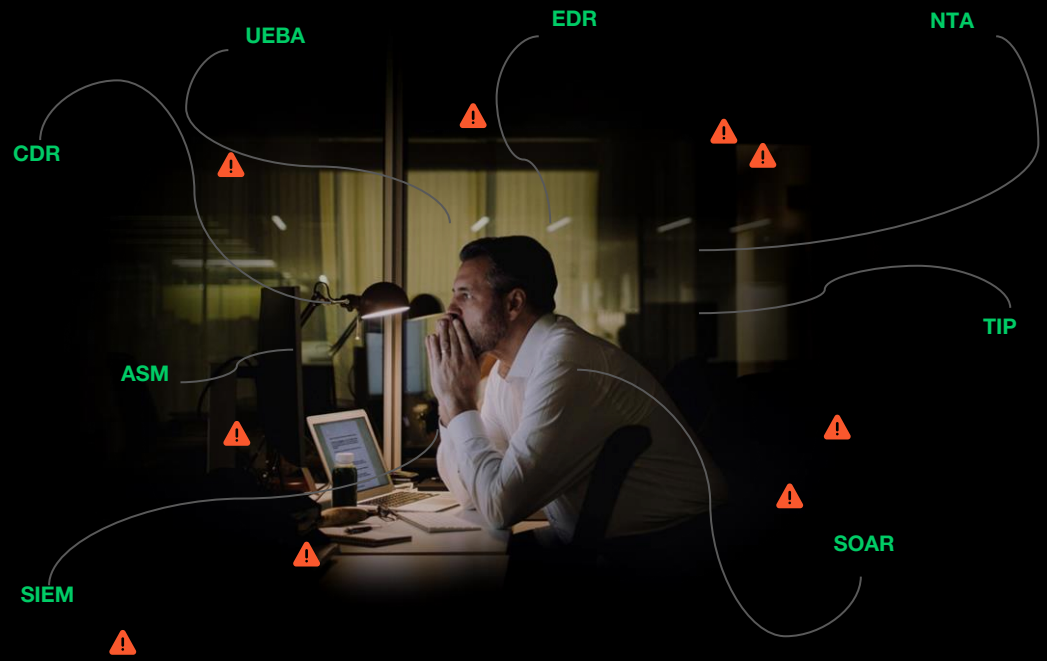
SOC의 한계를 넘어서

Precision AI와 XSIAM의 차세대 SOC 혁신

장성민, Ph.D, Director, Security Strategy & Technology

이상적인 SOC의 꿈의 실현은 가능합니다!

인간 중심 SOC 아키텍처는 이제 한계에 이르렀습니다...



현재 SOC로 모든 인시던트에 대한 실시간 대응이 불가능합니다.

모든 도구는 하나의 기능을 수행하도록 제작되었습니다.

탐지, 조사 및 대응에 대한 전체적인 End-to-End 관리가 .부족합니다.

팀은 최우선 순위 문제를 해결하려고 합니다.

~11K[1] ALERTS PER DAY

~93%[2] SOCS STILL DEPENDENT ON MANUAL PROCESSES

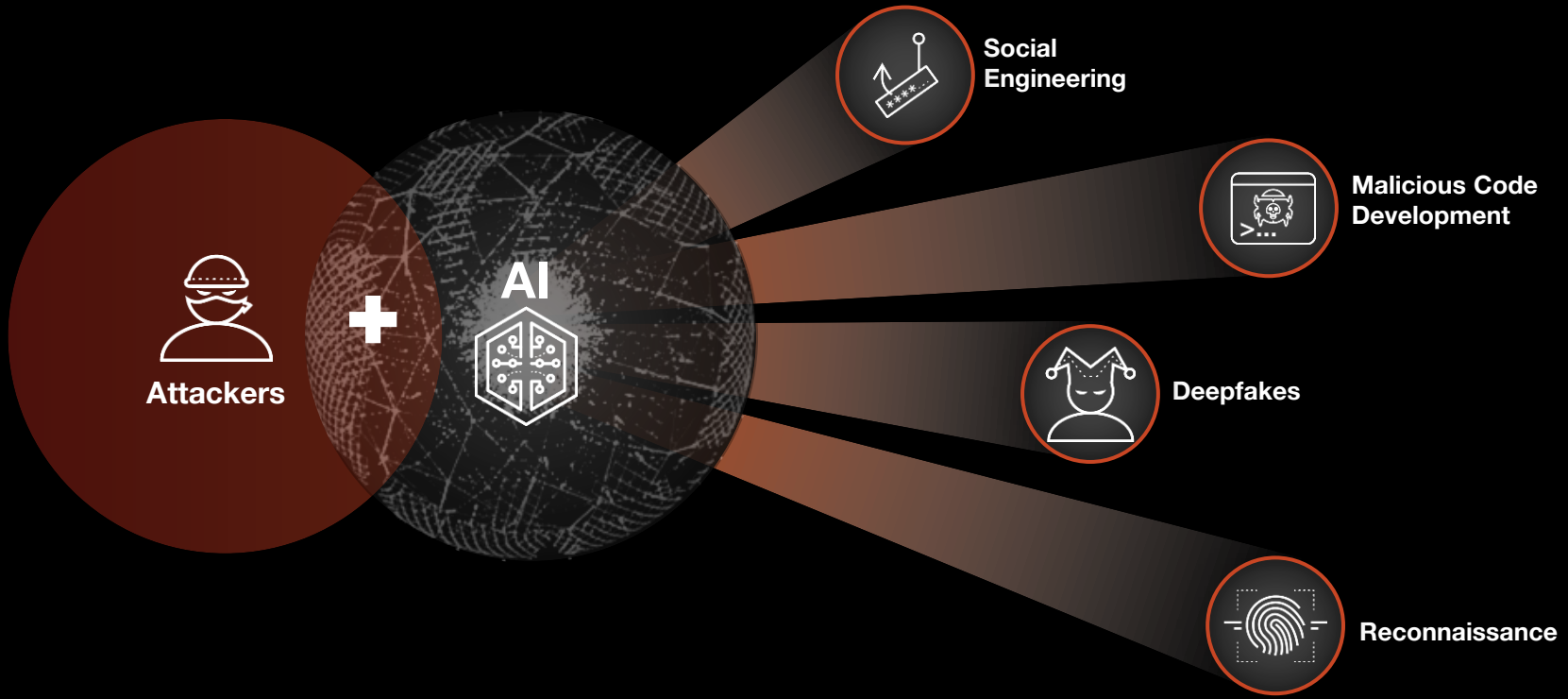
~23%[3] ALERTS GET IGNORED / NOT INVESTIGATED

Sources:
[1] "The 2020 State of Security Operations," Forrester
[2] "In Cybersecurity Every Alert Matters," IDC, Oct 2021
[3] "SOC Modernization and the Role of XDR," ESG, Oct 2022

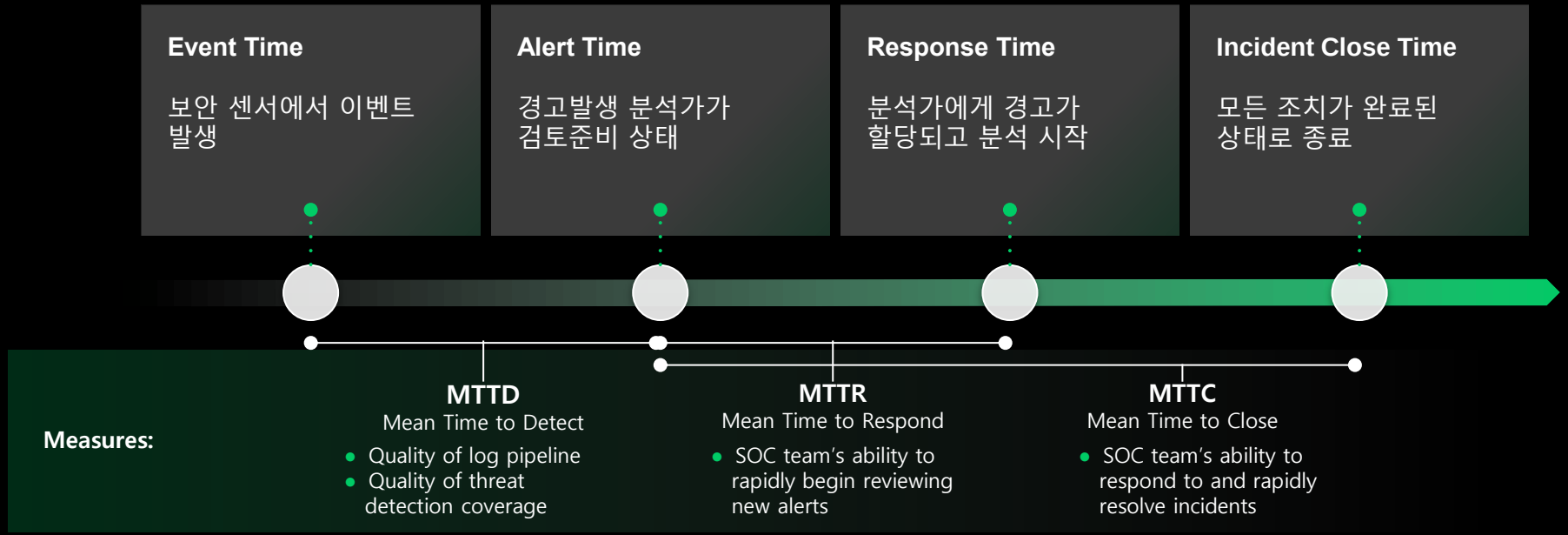
paloalto NETWORKS | CORTEX

적대적 AI의 등장으로 SOC 운영에 어려움을 겪고 있습니다..

공격자들도 AI 기술을 사용하여 더 빠르고 광범위하며 효과적인 사이버 공격을 시도하고 있습니다.



Time 기반 SOC 매트릭스



이상적인 SOC의 꿈

위협이 발생하기 전에 예방...

치명적인 인시던트를 몇 시간이 아닌 몇 분 안에 식별하고 해결...

사전 대응과 빠르게 진행되는 위협에 대처할 시간을 확보...

AI와 자동화로 신속한(Machine Speed) 대응이 해답입니다!!

스티칭 및 상관관계를 통해 향상된 대용량 데이터는 알림 수를 획기적으로 줄입니다.

NETWORK →
ENDPOINT →
IDENTITY →
CLOUD →
ATTACK SURFACE →
OTHER →

STITCH AND NORMALIZE DATA

탐지, 조사 및 대응을 자동화하고 권장 사항을 제시합니다.

ANALYTICS (AI/ML)

DETECTION

INVESTIGATION

RESPONSE

AUTOMATION

강화된 분석가는 더욱 선제적인 대응을 가능하게합니다

paloalto NETWORKS | CORTEX

Cortex XSIAM

Extended Security Intelligence and Automation Management

paloalto NETWORKS | CORTEX

Security Operations Centers of Today

Cortex XSIAM: AI기반 SOC 플랫폼

SOC를 위한 단일
프런트엔드 및 백엔드

AUTOMATION
1,000+ actions and integrations

AI
5,000 detectors and over **2,000 ML models**

DATA
4x more data ingested

XSIAM

업계에서 가장 광범위한 SOC 도구 세트 제공

- SIEM ✓
- NTA ✓
- EDR ✓
- ASM ✓
- SOAR ✓
- UEBA ✓
- TIP ✓
- CDR ✓

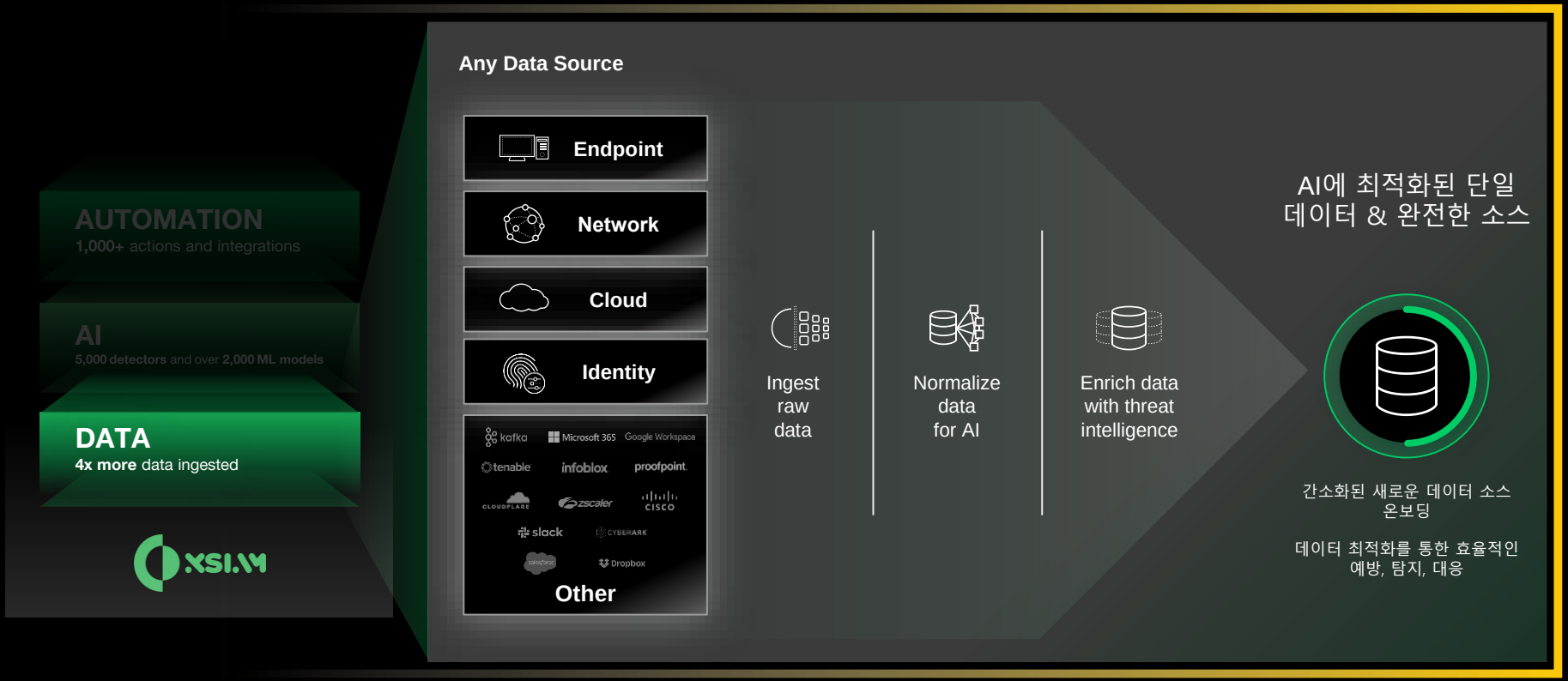
단일 백엔드, 단일 프런트엔드,
통합 UI

Unified Tools & Data
To enhance
productivity

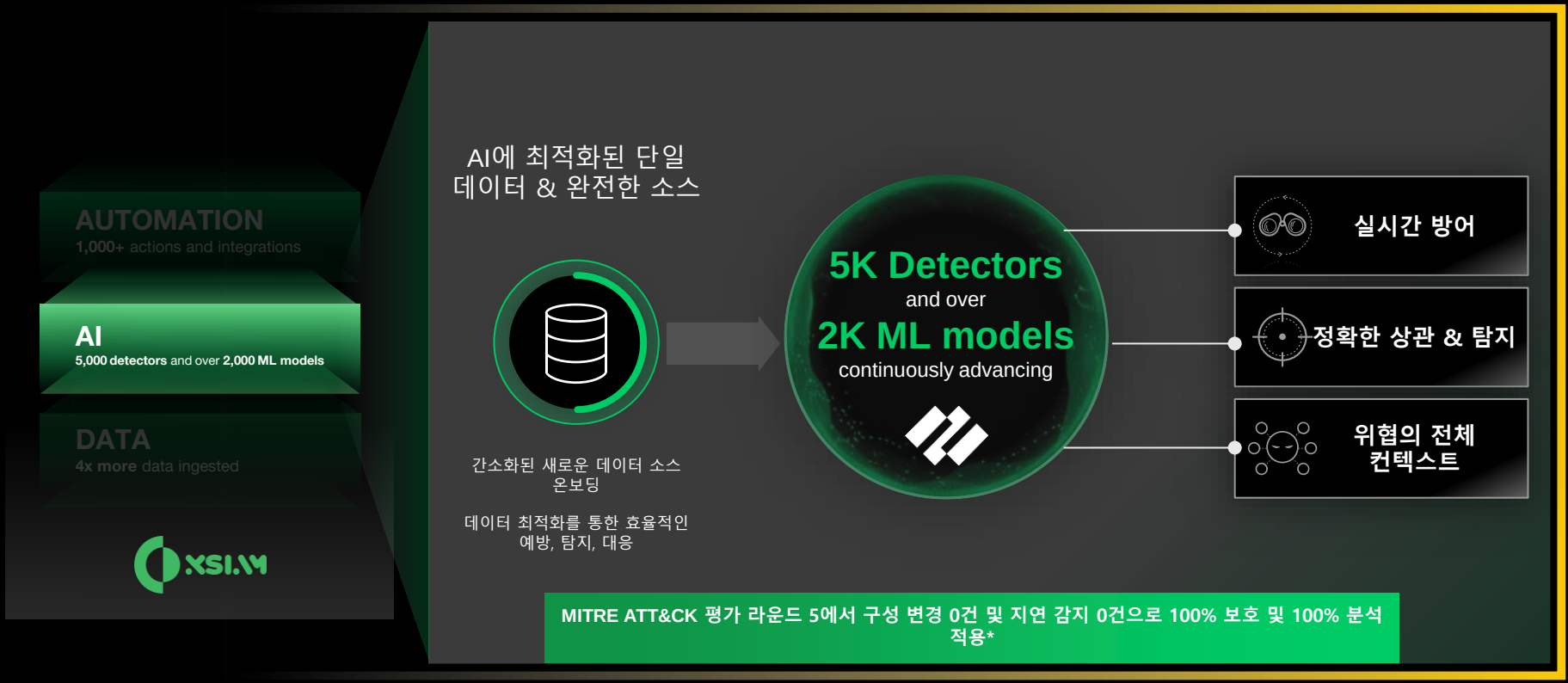
AI Powered Defense
To stop Threats
from hours → minutes

Automated Operations
To accelerate SOC
outcomes

Data: AI & 자동화를 위한통합 도구 및 데이터

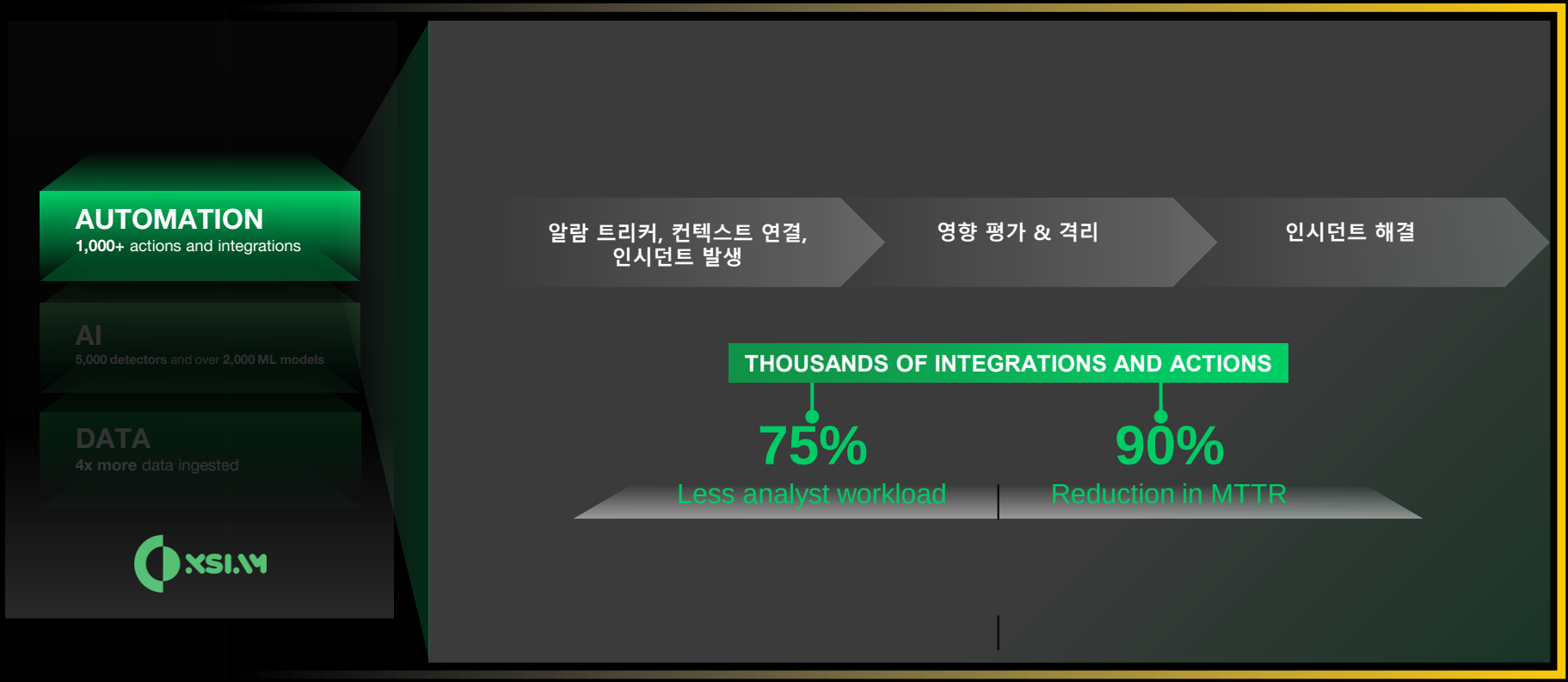


AI: 몇 분 안에 위협을 차단하는 AI 기반 방어



*MITRE Engenuity Enterprise ATT&CK Evaluation Round 5 Turla evaluation,

Automation: SOC 워크플로우를 위한 자동화



Cortex 플랫폼

Best-in-Class Products Available Standalone

Cortex XDR

Prevent, detect and investigate attacks across the enterprise

Cortex XSOAR

Automate response and improve with every incident

Cortex XPANSE

Discover and protect your entire internet attack surface

Converged SecOps Platform for Ultimate SecOps

Cortex XSIAM

AI-driven SecOps platform for the modern SOC

INCIDENT RESPONSE

Proactive & Reactive services
OEM Agnostic
Credits & SLA-based retainers

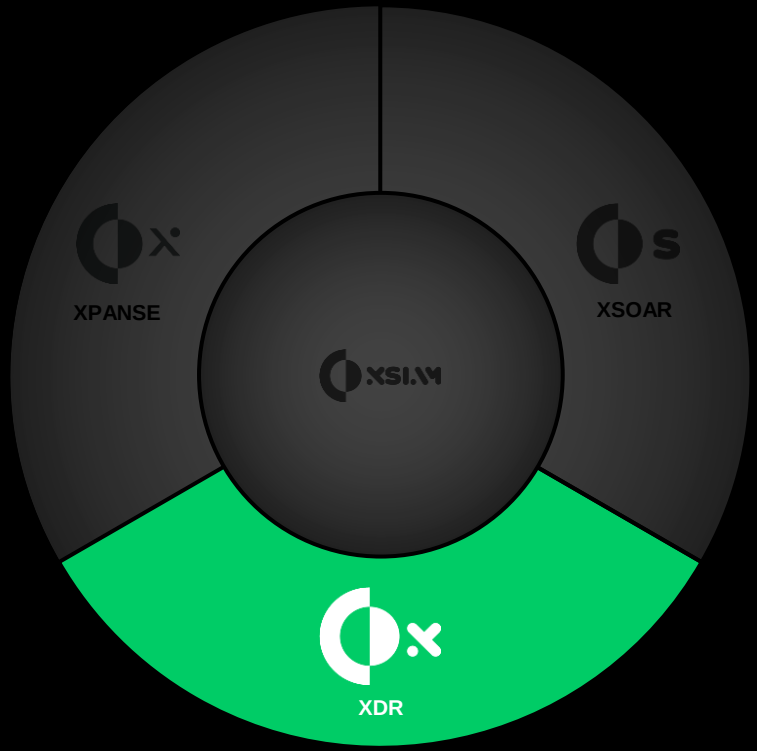
paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

MDR

Built on Cortex
Managed by Unit-42
Enriched with Context

Cortex XDR: 위협 탐지 및 대응 가속화

- 검증된 엔드포인트 보안으로 공격 방어[1]
- 행위 분석 & 머신 러닝을 통한 AI 기반 분석
- RCA & 타임라인 분석을 통한 신속한 조사
- 라이브 터미널 및 통합 시행을 통한 대응



Sources:
1) MITRE Engenuity™ ATT&CK® Enterprise Evaluations 2023

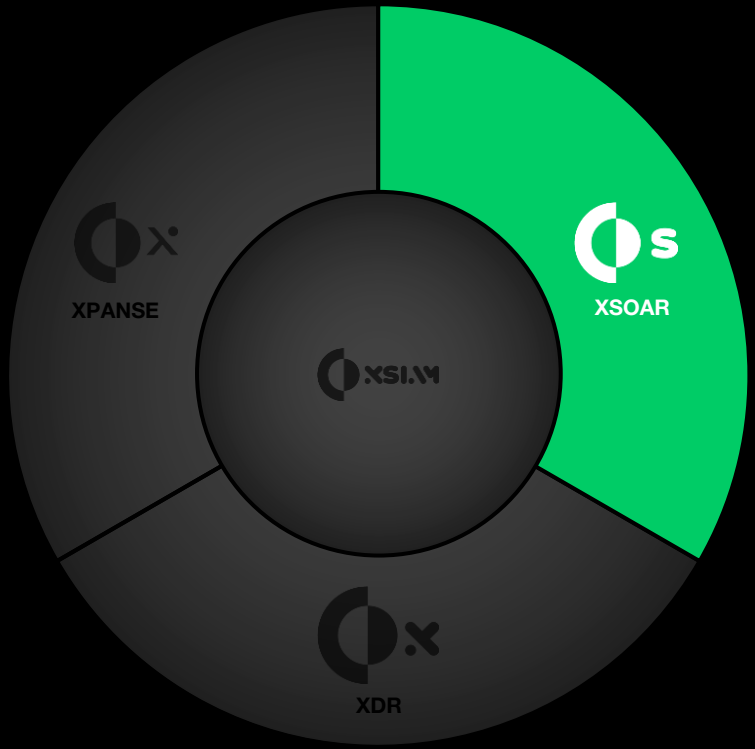
XSOAR: 보안 운영 자동화

Automation and orchestration
인시던드 대응 가속화 & 운영 효율성

Real-time collaboration
용이한 분석 & 결과 도출

Case management
인시던트 인사이트 수집, 배포 & 분석

Threat intel management
외부 텔리전스 소스 연계 & 우선순위 지정

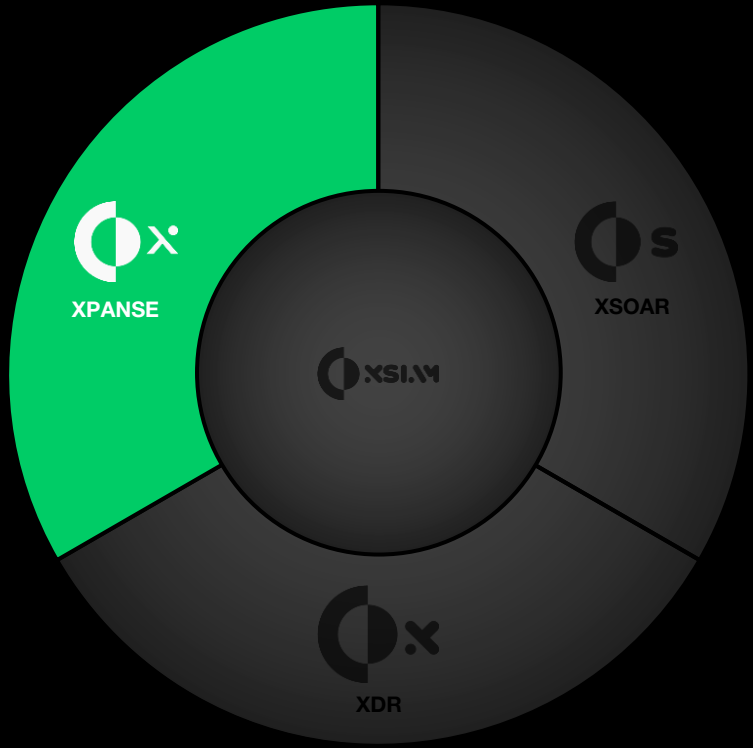


XPANSE: 공격 표면에 대한 신속한 자동대응

Discovery
알려지지 않은 연결된 모든 시스템과 노출된 서비스를 외부에서 검색

Assessment
즉각적인 제로데이 대응을 위한 ML 기반 자산 귀속 & 자동화된 위험 우선 순위 지정

Remediation
서비스 소유자를 식별하고 머신 속도로 수정하기 위한 자동화된 AI 기반 플레이북 제공



XSIAM: AI 기반 SOC 플랫폼

Converged platform
SIEM을 포함한 Cortex의 모든 핵심 기능이 단일 플랫폼으로 통합됨

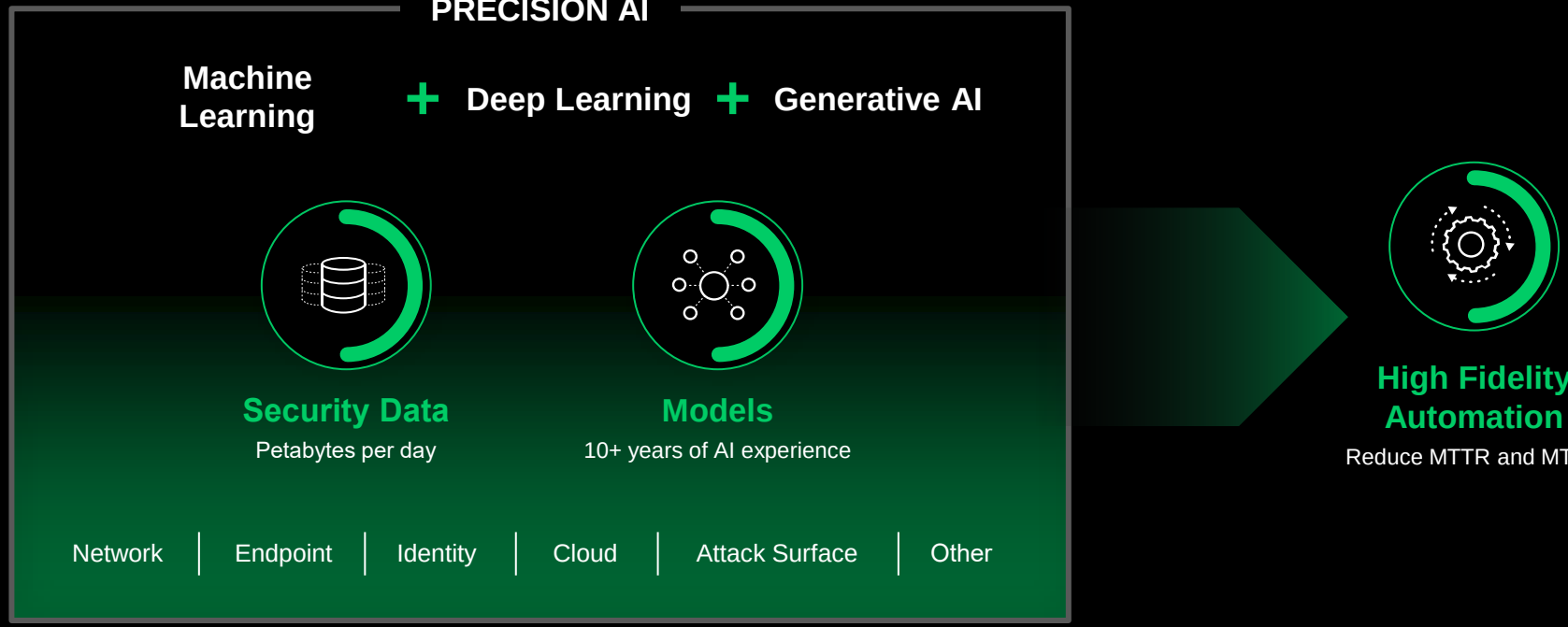
AI-driven outcomes
즉시 적용 가능한 AI 모델 적용 & 이벤트 연결, 대규모 위협에 대한 정확한 탐지 & 차단

Automation-first approach
사고 대응 자동화

XSIAM Powered by Precision AI™

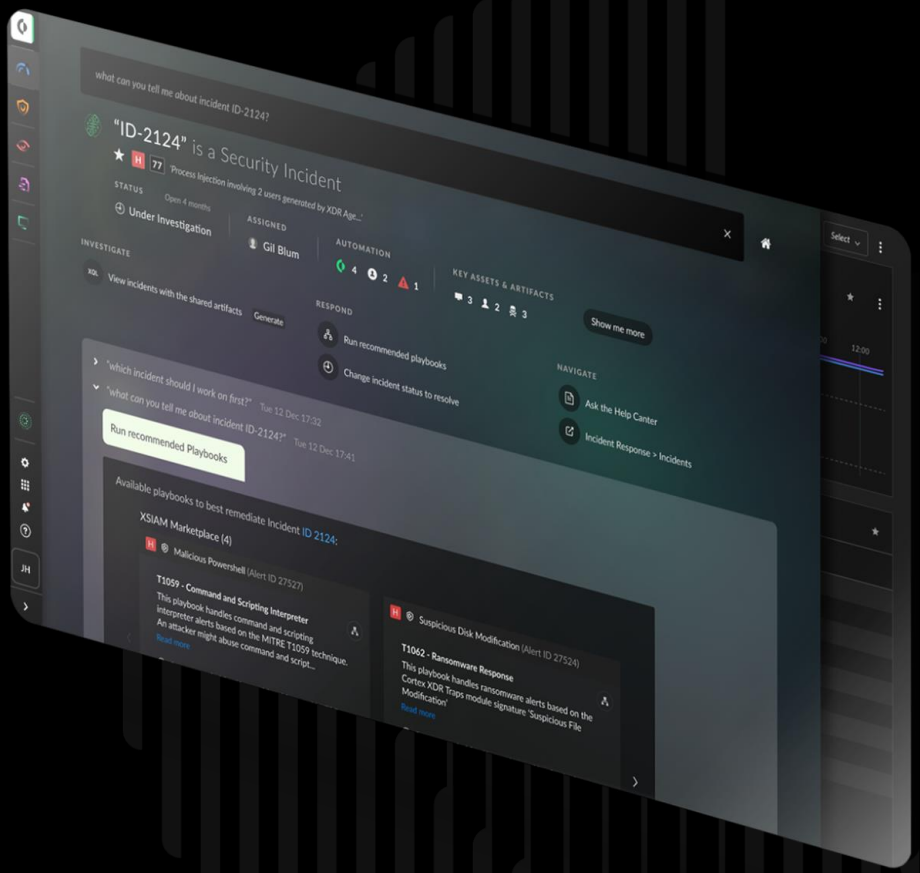
paloalto NETWORKS | CORTEX

Precision AI: 고객의 AI여정을 안전하게 보호



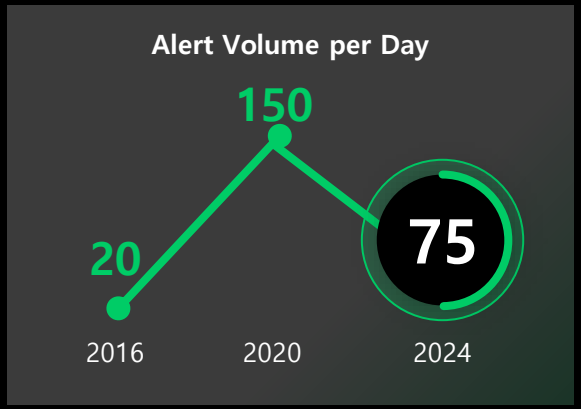
Cortex Copilot:
Your Advanced SecOps Assistant
Secure Smarter. Not harder

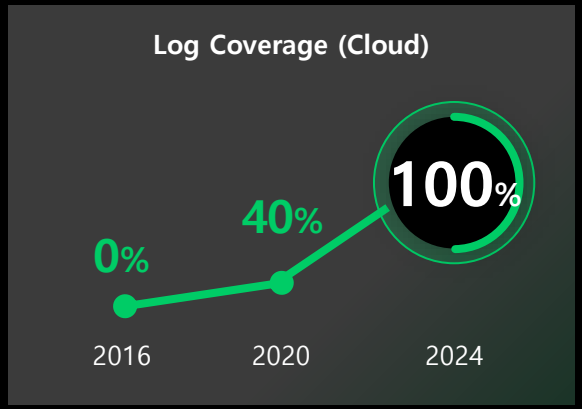
- 신속한 조사 & 분석
- 분석 워크플로우 최적화
- 편리하고 똑똑한 위협 헌팅

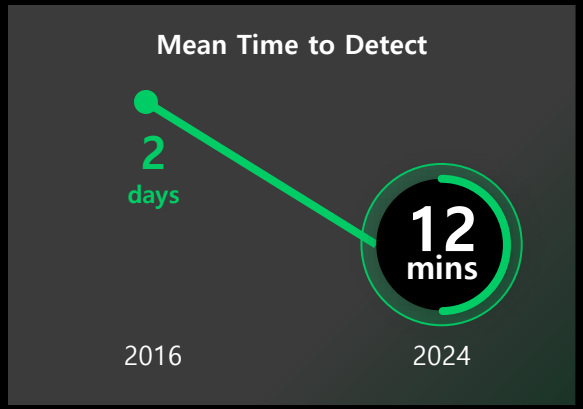


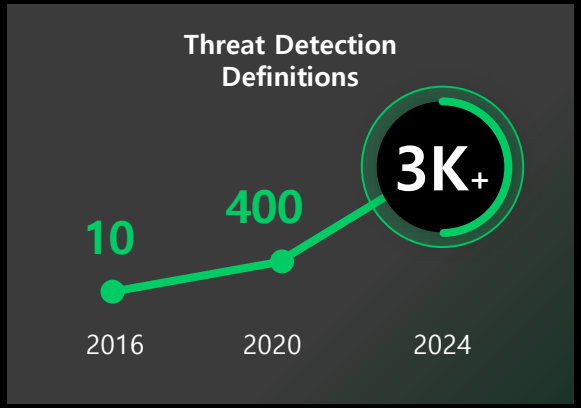
XSIAM - 검증된 SOC 플랫폼

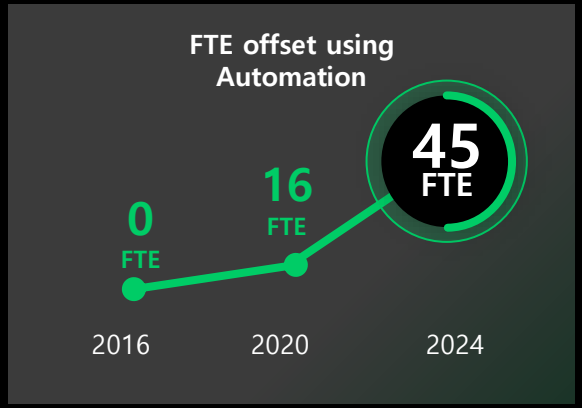
PANW's SOC의 혁신

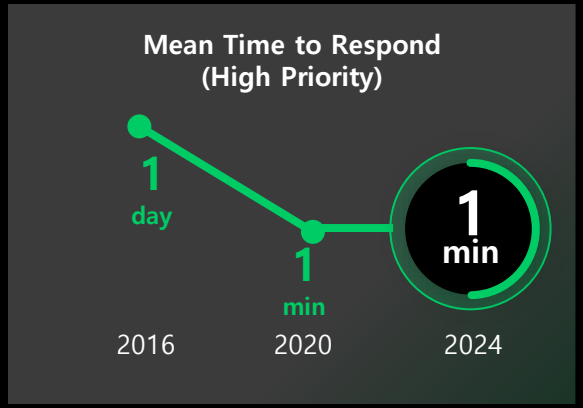












Cortex: 검증된 SOC 플랫폼

Recognized Leadership

Gartner

A Leader in Magic Quadrant for Endpoint Protection Platforms[1]

Recognized Leadership

FORRESTER

A Leader in Wave for Attack Surface Management Solutions[4]

Recognized Leadership

FORRESTER

A Leader in Wave for Endpoint Security[2]

Recognized Leadership

GIGAOM

Leader in GigaOm's Security Orchestration, Automation and Response Radar[5]

Recognized Leadership

GIGAOM

Leader in GigaOm's Autonomous Security Operations Center (SOC) Radar[3]

Recognized Leadership

FORRESTER

A Leader in Wave for Extended Detection and Response[6]

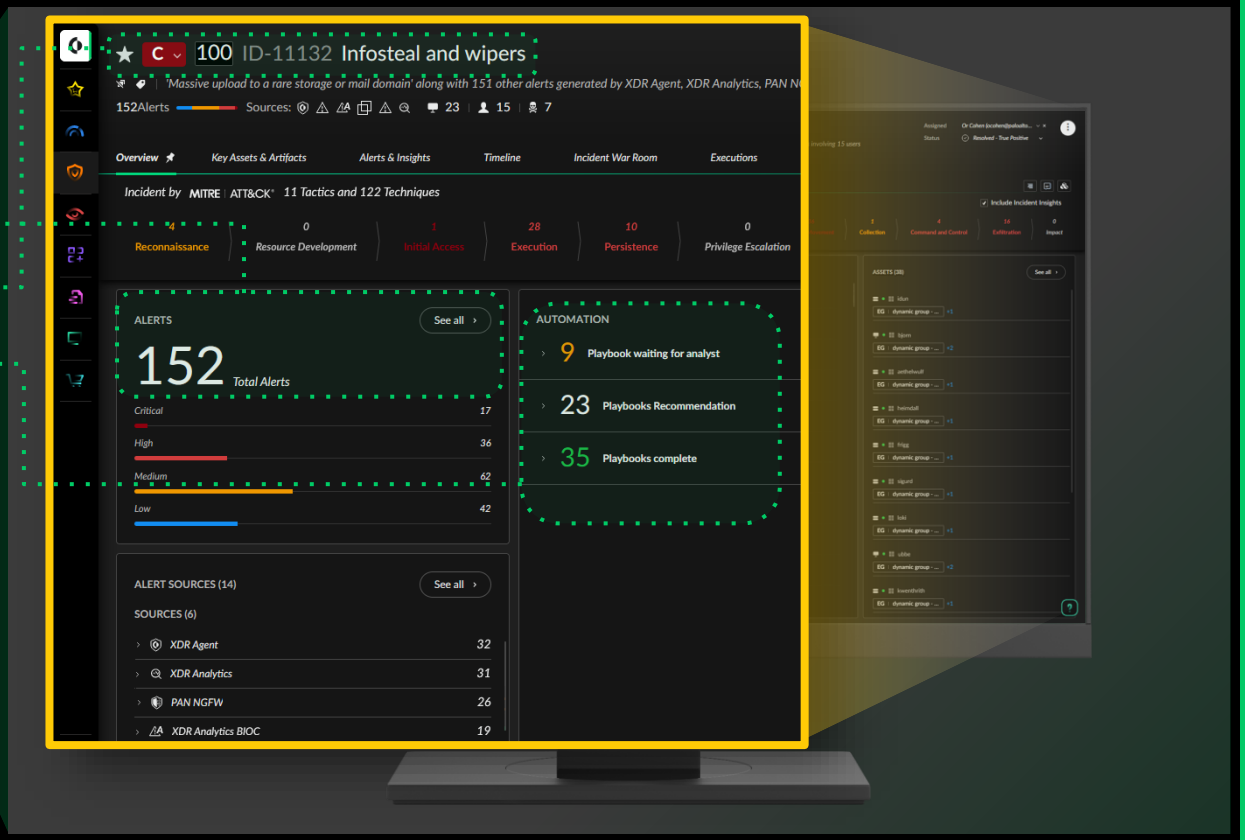
Sources:
1) 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms
2) The Forrester Wave™: Endpoint Security, Q4 2023
3) GigaOm Radar for Autonomous Security Operations Center (SOC), Nov 2023

Sources:
4) Forrester Wave™: Attack Surface Management Solutions, Q3 2024
5) GigaOm Radar for Security Orchestration, Automation, and Response, Sept 2023
6) The Forrester Wave™: Extended Detection And Response Platforms, Q2 2024

CASE STUDY

Anatomy of an Attack: 고객사례 #1

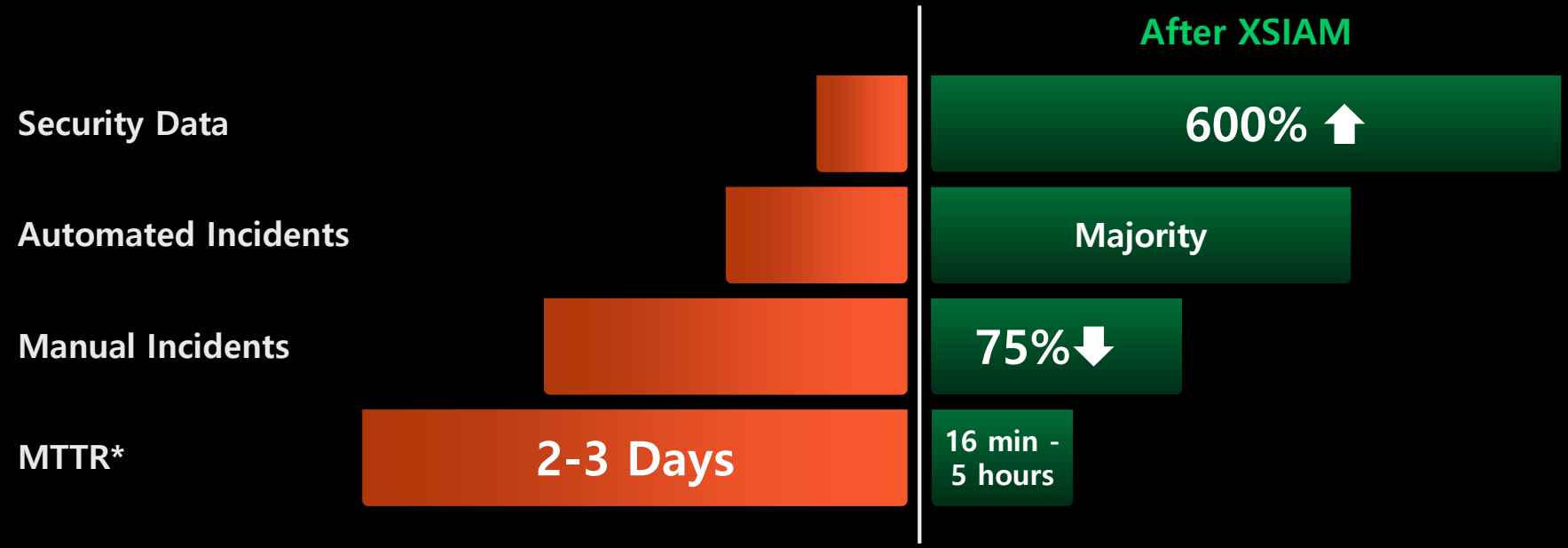
- SmartGrouping elevates **150+ alerts** from **14 sources**
- Created **one critical priority incident**
- Automatically:
  - Presented **9 response automations** to resolve the incident
  - **Recommended 23 playbooks** for increased automation in the future
  - Ran **35 actions** to prepare for response



paloalto NETWORKS | CORTEX

CASE STUDY

Putting it all Together: 고객 사례 #2



*Median Time to Resolve (time from incident creation to incident resolution).
Incidents Resolved by automation: partially or fully addressed with automation.
Source: XSIAM customer interviews and XSIAM product telemetry for customers.

CASE STUDY

ADT consolidates security operations with Cortex

Challenge: Modernize security and drive greater efficiency

+ 포인트 제품의 패치워크 전반에 걸쳐 보안을 현대화
+ 보안 팀이 성장하고 진화하는 위협에 대처하도록 역량강화
+ 워크플로를 단순화하고 중복 작업 제거

Solution: Work smarter and accomplish more

+ 보안 플랫폼 통합(Platformization)
+ 원활한 통합용
+ Customer Service

ADT
Home and business security | United States

Results

보안 팀을 확장하지 않고도 증가하는 위협으로부터 보호 가능

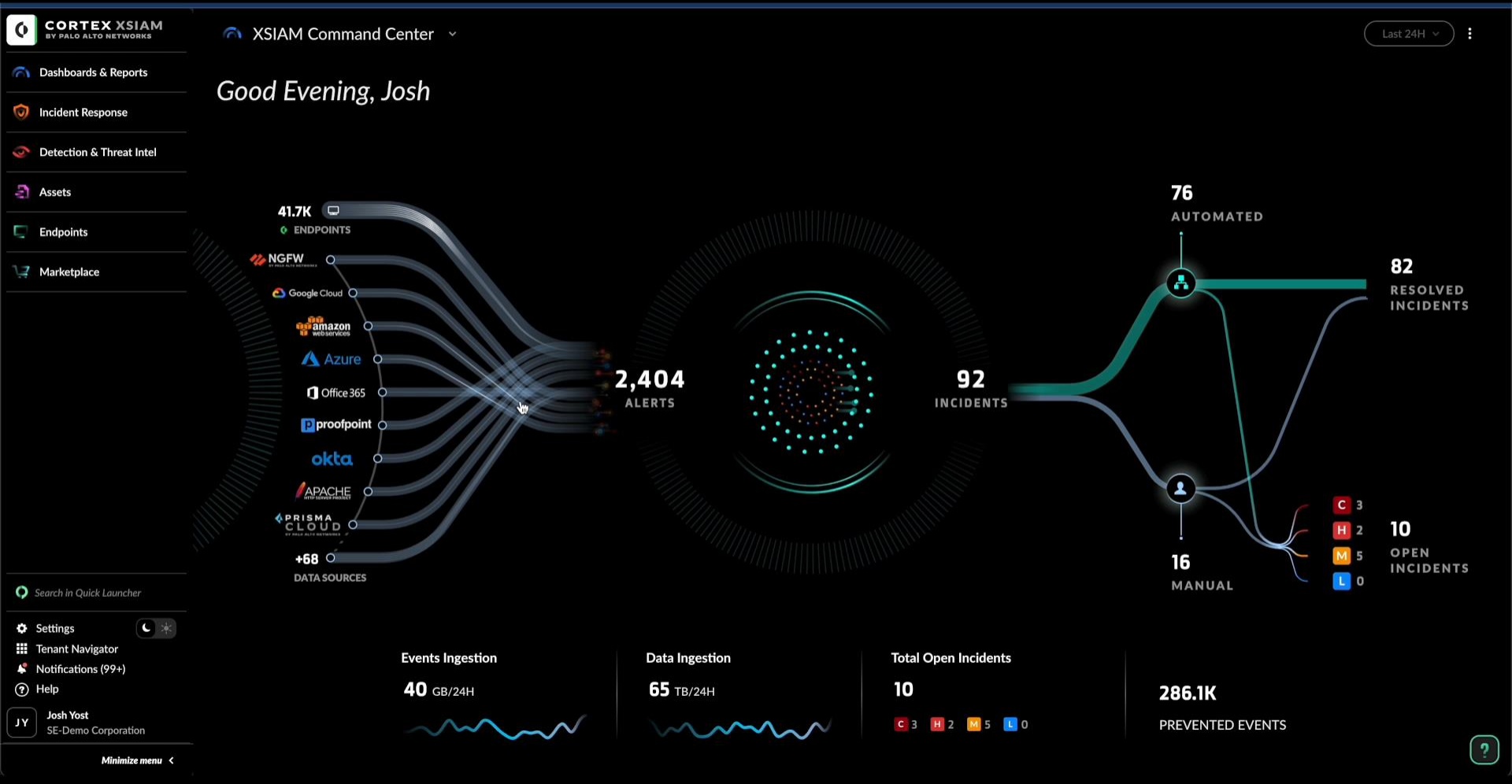
우선순위에 집중할 수 있는 시간이 더 많아 운영 효율성 향상

MTTR 의 획기적인 단축 몇일에서
3.3 시간으로

> XSOAR has been our platform for eight or nine years now. It continues to drive efficiency and deliver wins every year.

Rick DeLoach
Director of IT Security, ADT

paloalto NETWORKS | CORTEX


CORTEX XSIAM
BY PALO ALTO NETWORKS
XSIAM Command Center
Last 24H
Dashboards & Reports
Incident Response
Detection & Threat Intel
Assets
Endpoints
Marketplace
Good Evening, Josh
41.7K
ENDPOINTS
NGFW
Google Cloud
amazon web services
Azure
Office 365
proofpoint
okta
APACHE
PRISMA CLOUD
+68
DATA SOURCES
2,404
ALERTS
92
INCIDENTS
76
AUTOMATED
82
RESOLVED INCIDENTS
16
MANUAL
C 3
H 2
M 5
L 0
10
OPEN INCIDENTS
Search in Quick Launcher
Settings
Tenant Navigator
Notifications (99+)
Help
JY
Josh Yost
SE-Demo Corporation
Minimize menu
Events Ingestion
40 GB/24H
Data Ingestion
65 TB/24H
Total Open Incidents
10
C 3 H 2 M 5 L 0
286.1K
PREVENTED EVENTS

XSIAM – SOC(SIEM)의 한계를 넘어서

통합 SOC 플랫폼

더 빠른 조사 및 대응을 위한 통합 워크플로

더 쉬운 데이터 온보딩

AI 기반 탐지 & 대응 엔진

탐지 엔지니어링의 오버헤드 감소

상관 규칙의 복잡성 & 관리비용 감소

자동화 우선

통합 자동화 워크플로를 사용하여 수동 작업 감소

전체 SOC 워크플로에 걸쳐 자동화,최적화

획기적인 MTTD & MTTR 개선

Cortex XSIAM을 통해 QRadar 고객에게 더 큰 가치 제공

Simplification & Faster Time to Value

Ease of onboarding data and integrations, resulting in up to

12 mo.

quicker onboarding than legacy SIEM models

Improved Engineering Efficiency

Boost efficiency by slashing tool integration effort by up to

70%

resulting in less downtime

paloalto NETWORKS | CORTEX

Thank You

paloaltonetworks.com