CASE STUDY

PAGO NETWORKS

# 파고네트웍스, 스텔라사이버 오픈 XDR 플랫폼을 MDR 서비스에 통합하여 보안 사각지대를 좁히다

치열한 MSSP 경쟁 시장에서, 보안 서비스를 제공하는 벤더는 기존 고객을 유지하고 비즈니스를 성장시키기 위해 차별화된 서비스 제공에 힘써야 합니다. 파고네트웍스는 매니지드 탐지 및 대응 서비스의 진화 필요성을 느껴 XDR 벤더를 선택하기 위한 고된 과정을 시작했습니다. 광범위한 벤더 조사 및 테스트를 거쳐, 파고네트웍스는 고객사에 제공하는 보안 수준을 한 단계 높일 수 있는 역량을 제공하는 스텔라 사이버  오픈 XDR을 채택했습니다. 그 결과, 스텔라 사이버 오픈 XDR은 기대 이상의 성과를 보여주며 파고네트웍스가 제공하는 PAGO DeepACT 매니지드 탐지 및 대응 서비스의 중요한 요소가 되었습니다.

STELLAR CYBER®

PAGO NETWORKS | DeepACT Managed Detection and Response

PAGO NETWORKS

" 파고네트웍스는
PAGO DeepACT 매니지드 탐지 및 대응 서비스와
스텔라 사이버 오픈 XDR이 능동적인 위협 탐지 및 대응 플랫폼의
중추로써 함께 성장하길 기대합니다. "

## *"오픈 XDR 협업 이전"*

### 보안 사각지대 존재

관리되지 않아 보이지 않는 디바이스에 대해서는 PAGO DeepACT 매니지드 탐지 및 대응 서비스에 사각지대를 만들었고, 엔드포인트 에이전트 기반의 서비스에만 의존하게 했습니다.

### 능동적인 위협 헌팅 없음

파고네트웍스는 능동적인 위협 헌팅 서비스를 제공할 수 없었으며 엔드포인트 에이전트가 지원되지 않는 인프라 영역에서의 알려지지 않은 위협에 대한 탐지 및 대응 프로세스의 기반이 약했습니다.

### 멀티 벡터 위협 누락

보안 분석가는 네트워크 트래픽, 시스템 로그 등의 다양한 이벤트와 실제 위협을 연관 지을 멀티벡터에 대한 단서가 부족하여, 고객사에서 발생하는 위협 환경의 완벽한 도식화를 얻는데 까지 많은 시간을 할당했습니다.

## *"스텔라 사이버 오픈 XDR 협업 이후"*

### 통합 탐지 대응 프로세스

네트워크, 어플리케이션, 가상화, 클라우드, 사용자 데이터를 엔드포인트 데이터와 통합하여 전반적인 위협 탐지 및 대응 프로세스를 향상시켰습니다.

### 간소화

NG-SIEM, NDR, IDS, UEBA, SOAR 및 멀웨어/피싱 탐지 기능 등의 필수 보안 툴을 하나로 통합하였습니다.

### 높은 가시성

교차 환경 가시성을 통해 관리되지 않은 디바이스에서 오는 사각지대를 없애고, 침해 위협을 감소시켰습니다.

### 빠른 결과

침해 범위를 파악하고 추가 피해를 완화시키기 위해 활동 중인 랜섬웨어 및 크리티컬한 위협에 대응하는 수준을 향상시켰습니다.

"

이미 많은 고객들이
파고네트웍스의 PAGO DeepACT 매니지드 탐지 및 대응 서비스와 함께,
스텔라 사이버 오픈 XDR의 통합 운영에 대한 성공 스토리 공유를 요청하고 있습니다.

"

STELLAR CYBER®

PAGO NETWORKS | DeepACT Managed Detection and Response

파고네트웍스는 매니지드 탐지 및 대응 서비스 전문기업으로 노트북, 데스크탑, 서버(데이터센터/클라우드)를 타겟으로 하는 침해 위협에서 고객들을 보호하기 EPP/EDR 기반 보호 플랫폼과 서비스를 구축했습니다. 자체 MDR 서비스를 이용한 고객 성공 사례 외에, 다른 보안 제품에서 탐지된 위협 상세 분석을 추가로 제공하여 신속한 대응 계획을 수립했습니다.

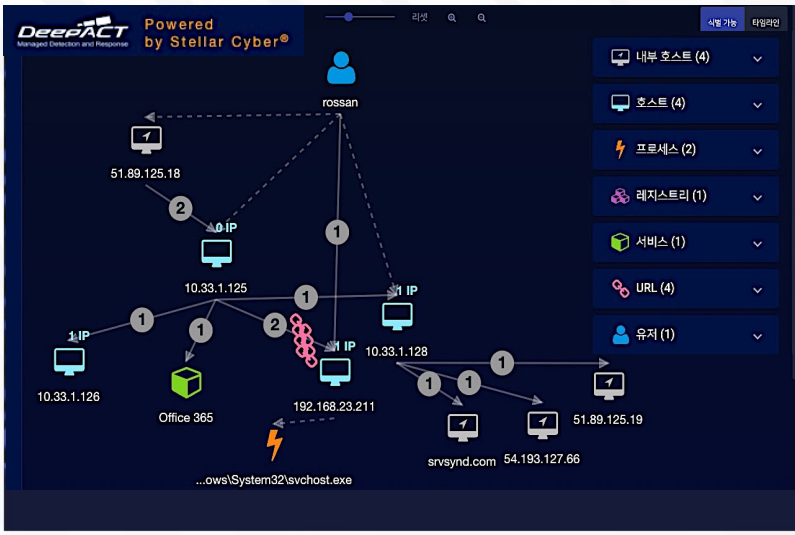
파고네트웍스 권영목 대표는 "많은 고객들은 이미 다양한 보안 솔루션을 적용하고 있지만, 상당수의 고객들은 알려지지 않은 잠재적 위협을 탐지하고, 신속한 위협 헌팅 및 대응을 위한 인적/물적 리소스와 시간이 절대적으로 부족합니다. 파고네트웍스는 EPP/EDR 기반 위협 탐지 및 대응 서비스로 고객에게 더 나은 가치를 제공하고 있었지만, 추가적으로 전체적인 솔루션과 방향성을 업그레이드해야 할 시기였습니다." 라고 의견을 제시했습니다.

> "스텔라사이버 오픈 XDR은 동-서 트래픽이건 남-북 트래픽이건 관계없이 뛰어난 가시성을 보여주고 있습니다. 그렇기 때문에, 발생한 보안 인시던트에서 이 인시던트가 어떻게 발생하게 된 것인지 원인을 찾아낼 수 있습니다."

**파고네트웍스는 XDR 평가 기준으로 다음 항목을 정했습니다.**

- 관리되지 않아서, 보이지 않는 디바이스로부터 시작하는 보안 사각지대 제거
- 자체 PAGO DeepACT 탐지 및 대응 서비스에 위협 헌팅 역량을 업그레이드 할 수 있는 플랫폼 제공
- 고객사 환경의 다양한 보안 이벤트와 로그 데이터를 기존 제공중인 EPP/EDR 기반의 위협 탐지 및 대응 프로세스에 쉽고 빠르며 유연한 통합 가능 여부

파고네트웍스의 신규 솔루션 테스트 팀은 특정 벤더 의존형 XDR 방식과 오픈형(개방형) XDR 방식 모두 테스트 했습니다. "특정 벤더 의존형 XDR 플랫폼은 고객이 특정 벤더의 다양한 보안 솔루션을 보유하고 있을 때 적합합니다. 하지만, 이기종 벤더 제품을 사용하는 고객 환경에서는 적합하지 않습니다. 오픈형(개방형) XDR 플랫폼은 고객이 도입한 솔루션에 구애받지 않고 쉽게 구축할 수 있으며, 이것은 파고네트웍스의 매니지드 탐지 및 대응 서비스 방법론과 고객의 보안 수준 향상에 모두 적합합니다. 상당히 많은 주요 테스트 과정을 거쳐 스텔라 사이버를 채택하였습니다." 라고 파고네트웍스 권영목 대표는 말했습니다.




"고객사 환경에 스텔라 사이버 오픈 XDR 플랫폼을 구축 후, PAGO DeepACT 매니지드 탐지 및 대응 서비스를 확장 제공하여, 보안 분석 가시성 대폭 확대, 위협 탐지 및 대응 속도 증가, 그리고 고객에게 효율적이고 즉각적인 보안 서비스를 제공하게 되었습니다."

스텔라 사이버 오픈 XDR 플랫폼의 가치를 보여준 특정 사례는 모 고객사에서 발생했었던 대규모 랜섬웨어 공격에 스텔라 사이버 오픈 XDR 플랫폼으로 처음 대응했던 날입니다. "스텔라 사이버의 쉽고 빠른 적용으로, 고객사 환경에서 랜섬웨어 다중 인스턴스를 신속하게 파악하고, 추가적으로 다양한 위협과 악성행위를 완화시켰습니다."

스텔라 사이버는 AI 머신러닝 기반으로 위협 탐지 및 대응 과장을 단순화합니다. 먼저, 자동화된 프로세스로 플랫폼 안에 통합된 모든 탐지 센서 및 보안 툴로부터 데이터를 정규화하고 보강 합니다. 그리고, AI 머신러닝 엔진이 보안 이벤트의 위험도를 책정 및 관련 있는 이벤트를 그룹화하고, 사용자와 자산의 비정상 행위에 기반한 새로운 위협을 찾아내며, 플랫폼에서 제공하는 직관적인 대시보드에서 상관 관계 인시던트의 우선 순위 리스트를 표현합니다.

스텔라 사이버는 Log4j 취약점 이슈에서도 가치를 증명했습니다. "Log4j 취약점을 파악하는 스캐닝 트래픽과 익스플로잇 공격 트래픽을 정확히 탐지하였고, 파고네트웍스는 PAGO DeepACT 매니지드 탐지 및 대응 서비스를 통해 고객에게 즉각적인 IOC/IOA를 제공했습니다.

스텔라사이버 오픈 XDR 플랫폼은 파고네트웍스가 제공하는 매니지드 탐지 및 대응 서비스에서 기존에 존재하던 보안 사각지대를 좁힐 수 있도록 지원하여 고객에게 양질의 경험을 제공하고 있습니다.

STELLAR CYBER®

PAGO NETWORKS | DeepACT Managed Detection and Response