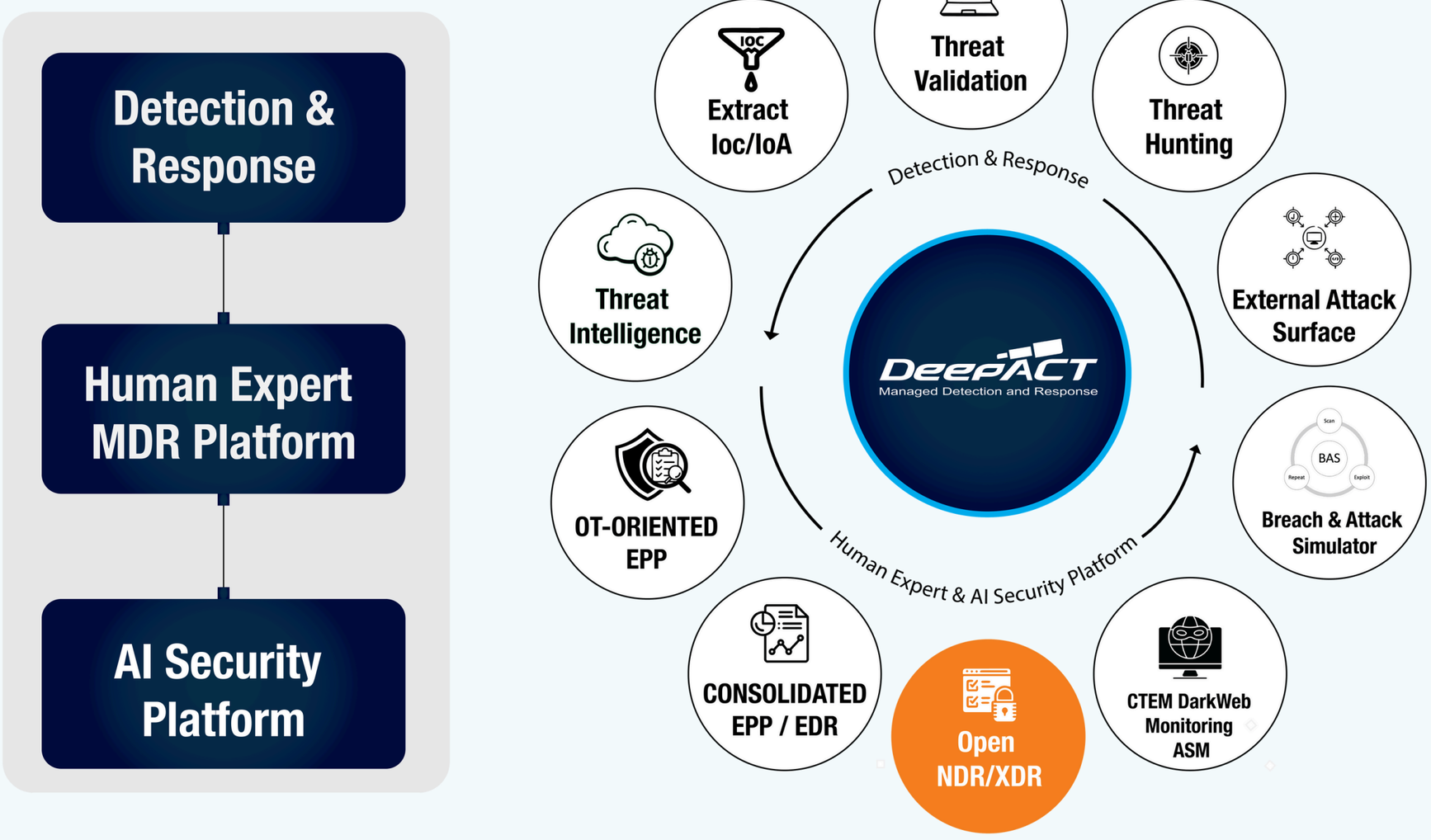
AI 기반, Open XDR 통합 보안 운영 및 분석

NDR(NW 트래픽), AD/FW 이벤트 연동 및 지능형 위협 탐지 대응

PAGO의 MDR(Managed Detection and Response) 플랫폼인 DeepAct와 Stellar Cyber의 Open XDR/NDR의 결합으로, 기업은 고급 위협 탐지 및 대응 능력을 강화할 수 있으며, 단일 대시보드에서 여러 보안 도구를 효과적으로 관리할 수 있게 해 주며, 복잡한 보안 환경에서도 빠르고 정확한 위협 탐지 및 대응을 가능하게 합니다.



보안 운영/분석, 무엇이 문제?

MDR센터는 급변하는 공격을 탐지/방어하기 위해, 다양한 보안 탐지 및 분석 툴을 배치해 왔고 생각보다 복잡한 보안 탐지 환경을 구성하게 되었습니다. 그 결과, 다양한 보안 솔루션에서 수많은 보안 이벤트를 발생시키고 있으며, 이 모든 보안 이벤트 중에서 실제로 대응해야 할 이벤트를 짚어내지 못하는 것이 현실입니다. 더불어 최근 IT 인프라 환경은 온 - 프레미스뿐만 아니라, 퍼블릭/프라이빗 가상화 및 클라우드 환경, 컨테이너 워크로드, 수많은 애플리케이션 등으로부터 엄청난 보안 관련 이벤트가 발생하지만, 보안팀이 모두 대응하기에는 역부족인 상태이며 “더 빠르고, 정확하며, 효율적인 통합 보안 운영 및 분석 플랫폼” 이 필요한 상황입니다.

pago's choice

- **통합된 위협 탐지 및 대응:** 다양한 보안 툴과 시스템을 통합하여 위협을 보다 광범위하고 정교하게 탐지 가능
- **고급 분석 및 가시성:** 다양한 환경에서 발생하는 위협을 실시간으로 분석하여, 복잡한 보안 환경에서도 종합적인 가시성 확보
- **자동화된 대응:** 실시간으로 고도화된 공격을 빠르게 차단 및 격리 가능
- **스케일러빌리티와 유연성:** 다양한 환경과 규모에 맞게 유연하게 확장 가능
- **관리 용이성:** 중앙 집중식 대시보드 활용

pago's Added Value

- 24/7 전문가 모니터링 및 위협 대응 자동화로 누락될 수 있는 잠재적인 위협 관리
- 고도화된 위협 분석 및 대응: 특정 환경과 위협 모델에 맞춘 고도화된 분석 서비스 제공
- 고객 맞춤형 보고서 및 인사이트 제공
- 실시간 위협 대응 및 사고 관리: 사고 발생시, 고객에게 실시간 알림과 함께 최적화된 대응 방안 제공
- 위협 인텔리전스 및 트렌드 분석
- 확장 가능하고 유연한 보안 솔루션 제공: 고객의 요구에 맞춘 맞춤형 보안 서비스 제공
- 효율적인 보안 운영과 비용 절감: 고객의 보안 인프라를 간소화해 관리 및 운영 비용 절감

www.pagonetworks.com

스텔라사이버의 Open XDR/NDR 플랫폼은 기업의 사이버 보안 환경을 강화하기 위한 다양한 기능을 제공하는 고도화된 보안 아키텍처를 갖추고 있으며, 주요 특장점은 다음과 같습니다:

- **통합된 보안 데이터 수집:** Open XDR/NDR 플랫폼은 네트워크 엔드포인트, 클라우드, 이메일 등 다양한 보안 데이터 소스를 통합하여 중앙 집중적으로 관리할 수 있는 기능을 제공합니다. 이를 통해 여러 보안 툴에서 발생하는 데이터를 실시간으로 수집하고, 중복 없이 중요한 보안 인사이트를 추출하여 보안 운영의 효율성을 크게 향상시킵니다.
- **고도화된 위협 탐지 기능:** 스텔라사이버는 AI와 머신러닝을 활용하여 실시간으로 고도화된 사이버 위협을 탐지하는 고유한 알고리즘을 구현하고 있습니다. 이 플랫폼은 알려지지 않은 공격 및 제로데이 공격을 포함한 다양한 고급 위협을 효과적으로 식별할 수 있으며, 위협의 정확성을 극대화하여 false positive를 최소화합니다.
- **자동화된 대응 및 조치 기능:** Open XDR/NDR은 위협을 자동으로 탐지하고 이를 실시간으로 대응하는 기능을 제공합니다. 공격이 발생했을 때, 시스템은 자동으로 위협을 분류하고, 해당 위협에 맞는 대응 절차를 자동으로 실행할 수 있습니다. 이러한 자동화된 대응 과정은 보안 팀의 부담을 경감시키며, 보안 사고에 대한 반응 시간을 단축시킵니다.
- **AI 기반의 상관 관계 분석:** Open XDR/NDR 플랫폼은 AI 기반의 고급 상관 관계 분석 기능을 통해, 다양한 보안 데이터 소스에서 발생하는 이벤트들을 실시간으로 분석하고 상관 관계를 파악하여 위협을 식별합니다. 이를 통해 공격의 원인 및 경로를 빠르게 추적할 수 있으며, 보다 정교한 보안 인사이트를 제공합니다.
- **확장성 및 유연성:** 본 플랫폼은 클라우드 및 온프레미스 환경을 모두 지원하며, 다양한 보안 도구와의 원활한 통합을 통해 기업의 보안 구사항에 맞춰 유연하게 확장 가능합니다. 또한, 플랫폼은 기업 규모와 보안 환경 변화에 대응할 수 있는 높은 확장성을 제공하여, 점진적인 보안 환경 개선을 지원합니다.
- **사용자 친화적인 대시보드 및 관리 인터페이스:** 스텔라사이버의 Open XDR/NDR은 직관적이고 사용자 친화적인 대시보드 및 관리 인터페이스를 제공합니다. 이를 통해 보안 운영팀은 실시간으로 위협을 모니터링하고, 사건 발생 시 신속하게 대응할 수 있는 정보를 제공합니다. 대시보드는 다양한 보안 데이터를 시각적으로 효과적으로 제공하며, 운영자가 적시에 필요한 조치를 취할 수 있도록 돕습니다.
- **개방형 아키텍처:** Open XDR/NDR 플랫폼은 개방형 아키텍처를 채택하고 있어, 기존의 보안 인프라와의 통합이 용이하고, 새로운 보안 툴이나 기술을 추가하는 데 높은 유연성을 제공합니다. 이를 통해 기업은 지속적으로 변화하는 보안 위협에 대응하고, 필요한 경우 보안 환경을 확장하거나 개선할 수 있는 유연성을 확보할 수 있습니다.

이와 같은 특장점들 덕분에 스텔라사이버의 Open XDR/NDR 플랫폼은 고도화된 사이버 위협을 신속하고 정확하게 탐지하고 대응하는 능력을 제공하며, 기업의 보안 관리 효율성과 효과성을 크게 향상시키는 데 기여합니다.