paloalto NETWORKS | CORTEX

필수 엔드포인트 보안 구매자 가이드

엔터프라이즈 엔드포인트 보안의 핵심 기능 알아보기

목차

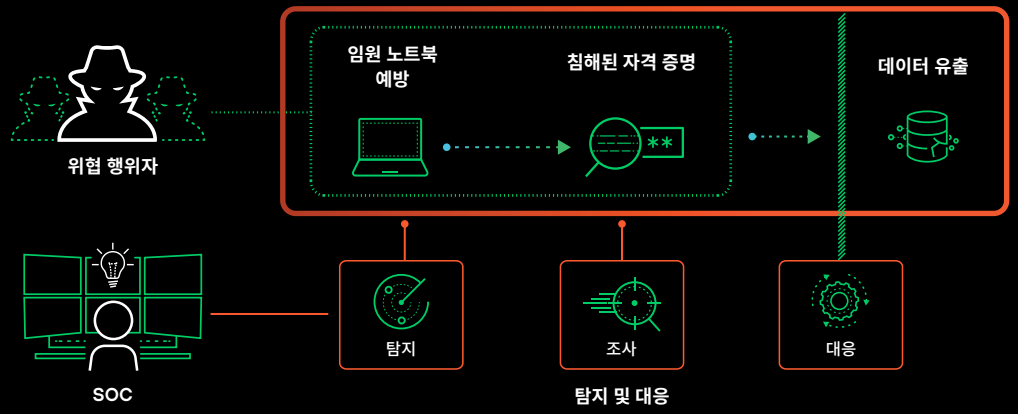
개요

지능형 지속 위협과 서비스형 랜섬웨어, AI 기반 공격은 보안 환경을 새롭게 정의하며 조직은 보안 위협에 선제적으로 대응해야 한다는 과제를 마주하고 있습니다. 안타깝게도 오늘날의 사일로화된 보안 솔루션으로는 진화하는 위협의 속도를 따라가기 어려우며, 그 결과 조직의 많은 취약점이 노출되어 있는 상태입니다. 이는 공격자가 조직에 액세스하는 것이 "발생 여부"의 문제가 아니라 "시간 문제"임을 의미합니다.

보안팀은 무수한 알림과 복잡한 조사, 그리고 공격을 놓칠 위험에 끊임없이 시달리고 있습니다. 클라우드 및 기타 환경에서 디지털 발자국이 확장됨에 따라 분석이 필요한 보안 원격 분석 데이터의 양과 다양성이 기하급수적으로 증가하고 있으며, 이러한 상황에서 '데이터의 홍수'라는 표현은 결코 과장이 아닙니다.

엔드포인트 보안은 사이버 방어의 기초입니다. 엔드포인트는 공격의 최초 침입이 성공하거나 저지되는 곳이며, 공격의 추적에 가장 유용한 데이터를 확보할 수 있는 곳입니다. 침입이 발생하기 전에 사이버 공격을 확인하고 차단해야 하는 보안 운영(SecOps)과 전반적 보안 태세에 매우 중요한 지점이기도 합니다.

이런 점에서, 강력한 **엔드포인트 보안 전략**은 더욱 앞서가는 보안 체계를 구축하기 위해 필수적입니다. 기존 엔드포인트, 네트워크, 클라우드 워크로드, 모바일 디바이스, ID 등을 포괄적으로 파악하고 분석할 수 있어야 하며, 통합적 접근 방식을 통해 신속한 탐지 및 대응을 지원하며 점점 중요성이 커지는 보안 운영을 효과적으로 뒷받침해야 합니다.



> "2028년까지 기업의 30%는 단일 공급업체가 제공하는 예방적 엔드포인트 보안, 엔드포인트 탐지 및 대응, ID 위협 탐지 및 대응 기능을 도입할 것으로 예상되며, 이는 2024년의 약 5%에서 크게 증가한 수치입니다.
>
> - Gartner[1]

[1] Evgeny Mirolyubov et al., Magic Quadrant for Endpoint Protection Platforms, Gartner, 2024년 9월.

엔드포인트 보안 알아보기:
보안 담당자의 주요 과제

보안 담당자의 주요 과제

CISO

최고 정보 보안 책임자(CISO)는 조직의 보안 태세를 실질적으로 강화하면서 이사회를 대상으로 보안 투자의 필요성을 설명해야 한다는 과제를 안고 있습니다. 그들은 기술적 지표를 비즈니스 가치로 전환하고, 끊임없이 진화하는 위협 환경의 리스크를 관리하며, 다양한 규정을 준수해야 합니다. 또한 강력한 보안 조치의 필요성과 비즈니스 민첩성, 사용자 생산성 간의 균형을 유지해야 하며, 제한적인 예산 내에서 조직을 운영하며 사이버 보안 기술 격차를 해소해야 합니다.

SecOps 책임자

SecOps 또는 보안 운영 센터(SOC) 책임자는 팀에게 적절한 지식과 프로세스, 도구를 제공하여 위협에 효과적으로 대응할 수 있도록 지원해야 합니다. 이들은 공격자의 전술과 기법을 파악하고, 다양한 도구와 플랫폼을 통해 대응을 조율하고, 막대한 알림에 의한 팀 내부의 피로와 팀원들의 번아웃을 관리하는 데 어려움을 겪고 있습니다. 또한 SecOps 책임자는 새로운 유형의 위협에 대처하고, 리소스 할당을 최적화하고, 평균 탐지 시간(MTTD)과 평균 대응 시간(MTTR)을 개선해야 합니다.

보안 아키텍트

보안 아키텍트는 진화하는 위협에 대응할 수 있으면서도 기존 인프라 및 보안 운영과 원활하게 통합되는 포괄적 엔드포인트 보안 전략을 설계하고 구현해야 합니다. 이들은 보안 제어의 잠재적 사각지대를 파악하고 해결하며, 보안 도구의 확산을 관리하고, 다양한 솔루션 간의 상호 운용성을 지원하는 데에 어려움을 겪고 있습니다. 이들의 주요 관심사는 조직의 보안 태세를 지속적으로 개선하고 효과, 비용, 사용자 경험의 적절한 균형을 맞추는 것입니다.

보안 애널리스트

보안 애널리스트는 위협 탐지 및 대응의 최전선에서 끊임없이 발생하는 알림과 잠재적인 보안 인시던트를 처리합니다. 이들은 알림 피로에 시달리며, 오탐을 추적하는 데 귀중한 시간을 소모하곤 합니다. 이들의 주요 과제는 알림의 우선순위를 효과적으로 지정하고, 조사 시간을 단축하며, 일상적 작업과 선제적 위협 헌팅, 중요한 인시던트의 심층 분석 사이에서 적절한 균형을 확보하는 것입니다.

엔드포인트 보안 제공업체의 역량 평가를 위한 10가지 질문

1. 정교한 공격을 탐지하는 방식

엔드포인트 탐지 및 대응(EDR) 기능

최신 엔드포인트 탐지 및 대응 기능을 제공하는 솔루션을 선택하세요. 엔드포인트를 지속적으로 모니터링하여 악성 활동의 징후를 감지하며, 정교한 위협에 대한 신속한 탐지 및 대응을 지원해야 합니다.

풍부한 엔드포인트 데이터 수집

효과적인 솔루션은 엔드포인트에서 광범위한 원격 분석 정보를 수집하여 잠재적인 위협을 찾아냅니다. 프로세스 정보, 파일 활동, 네트워크 연결, 레지스트리 변경, 사용자 활동 등을 수집하여 초점 범위가 좁은 도구는 탐지할 수 없는 위협을 파악합니다.

머신 러닝(ML) 및 동작 분석 기법

지속적으로 업데이트되는 수많은 머신 러닝 모델을 활용하여 위협 방지 및 탐지를 자동화하는 솔루션을 선택하세요. 이러한 솔루션은 사이버 보안 전문가의 실제 인사이트를 활용하여 최신 위협 인텔리전스를 자동으로 통합합니다. 이러한 접근 방식은 수동 분석 시간을 크게 단축하고, 위협 탐지 및 대응을 가속화함으로써 애널리스트가 중요한 인시던트에 집중할 수 있도록 도와줍니다.

사용자 지정 탐지 규칙 및 사전 정의된 탐지

네이티브로 제공되는 풍부한 분석 및 탐지 규칙을 제공하되 사용자 정의에 따른 맞춤 구성이 가능하도록 유연성을 갖추고 있어야 합니다. 보안팀은 조직 고유의 요구 사항과 위협 환경에 따라 탐지 규칙을 만들고 조정할 수 있어야 합니다. 사전 정의된 탐지 기능과 사용자 지정 탐지 기능의 조합을 통해 광범위한 지능형 공격을 포괄적으로 방어합니다.

2. 고급 위협 방지 기능의 이점

다층적 접근 방식

익스플로잇 방지, AI 기반 멀웨어 분석, 클라우드 기반 파일 검사, 행동 기반 위협 탐지, 랜섬웨어 보호 기능을 통합하는 심층 방어 전략을 구축하여 공격이 하나의 계층을 우회하더라도 다른 계층에서 포착되도록 합니다. 이를 통해 멀웨어에서 파일리스 공격에 이르는 정교한 위협으로부터 조직을 보호하는 포괄적인 보안 메쉬를 구축합니다.

행동 기반 보호 및 익스플로잇 방지

솔루션이 고급 행동 기반 위협 보호 기능을 활용하여 상호 연관된 프로세스 동작을 분석하고, 진행 중인 공격을 효과적으로 탐지할 수 있도록 해야 합니다. 이러한 포괄적인 모니터링을 통해 개별 프로세스 분석 시 놓칠 수 있는 다단계 위협을 탐지할 수 있으며, 강력한 익스플로잇 보호 모듈은 OS 및 애플리케이션 취약점에 대한 핵심 방어 기능을 제공합니다.

AI 및 머신 러닝 기반 보호

수신한 모든 파일을 면밀히 조사하고 새롭게 등장하는 공격 패턴에 대응하는 방법을 지속적으로 학습하는 AI 기반 보안 엔진을 구축합니다. 이를 통해 기존의 서명 기반 방어 시스템으로 알아채기 어려운 정교한 위협을 탐지하고 차단할 수 있습니다.

3. 조사 및 대응에 대한 접근 방식

인시던트에 대한 자동 알림 상관관계 분석

머신 러닝을 활용하여 관련 알림을 통합 인시던트로 자동 그룹화하는 솔루션을 선택하세요. 이를 통해 알림 피로를 크게 줄일 수 있으며, 우선순위가 높은 보안 문제에 집중할 수 있습니다.

리스크에 따른 인시던트 우선순위 지정 및 점수 평가

리스크 요소를 기반으로 인시던트를 분석하고 점수를 매기는 머신 러닝 기반 시스템을 배포하여 공격 범위와 영향을 신속하게 평가함으로써 보안 리소스를 최적으로 할당합니다.

근본 원인 분석 및 공격 체인 시각화

각 인시던트에 대한 평판 데이터와 시각적 공격 체인 매핑을 제공하는 솔루션을 선택하세요. 이러한 솔루션은 근본 원인을 자동으로 분석하여 위협의 컨텍스트와 범위를 신속하게 파악할 수 있도록 지원합니다.

자동 및 수동 대응 옵션

일상적 위협에 대한 자동 조치와 복잡한 시나리오에 대한 수동 개입 옵션을 결합한 유연한 대응 프레임워크를 구축합니다. 이를 통해 보안팀은 위협 상황에 따라 신속하게 자동으로 문제를 해결하거나 신중하게 조정된 대응을 실행할 수 있습니다.

SOAR 플랫폼과의 통합

SOAR 플랫폼과 원활하게 통합되어 자동 워크플로를 강화하고 보안 스택 전반에 걸쳐 인시던트 대응 프로세스를 간소화하는 솔루션을 선택하세요.

4. 알림 피로 및 오탐 문제 해결 방법

AI 기반 알림 분류 및 우선순위 지정을 통해 지능형 알림 그룹화 및 인시던트 점수 평가 기능을 제공하는 솔루션

알림을 지능적으로 그룹화하여 점수를 매기고, 관련 이벤트의 연관관계를 자동으로 파악하고, 영향력 및 위협 가능성에 따라 리스크를 평가하는 AI 기반 솔루션을 선택하세요. 이러한 시스템은 자산의 중요도, 사용자 행동, 위협 인텔리전스에 대한 컨텍스트 분석을 활용합니다. 또한 애널리스트의 피드백을 통해 지속적으로 학습하여 우선순위 지정의 정확도를 높이고 고급 행동 분석을 통해 오탐을 줄입니다.

지능형 분석을 통한 오탐 감소

이상적인 시스템은 AI 기반 분석과 엔드포인트, 네트워크, 클라우드 환경의 교차 데이터 상관관계를 활용하여 실제적인 위협과 무해한 이상 징후를 정확하게 구분하고 컨텍스트 분석을 통해 오탐을 최소화합니다.

5. 기존의 EDR를 넘어 XDR 기능으로 확장하는 방식

엔드포인트 데이터만으로도 효과적이지만, 컨텍스트 확장을 통해 더욱 포괄적인 탐지 및 워크플로 통합 지원

엔드포인트 데이터만으로 강력한 보호 기능을 제공하면서도, 사용 가능한 네트워크, ID, 클라우드 데이터 소스를 원활하게 통합하여 위협 탐지 컨텍스트를 강화하고 보안 워크플로를 간소화하는 솔루션을 선택하세요.

확장된 소스의 데이터 통합

네트워크, 클라우드 환경, ID 시스템 등 다양한 소스의 데이터를 원활하게 통합하는 기능이 필요합니다. 공격자는 여러 환경에서 활동하기 때문에 단일 소스에 대한 가시성으로는 위험한 사각지대를 제거할 수 없습니다.

교차 데이터 분석 및 위협 상관관계 분석

다양한 데이터 소스의 위협 간 상관관계를 파악할 수 있는 지능형 분석을 제공함으로써 현재 진행 중인 보안 인시던트에 대해 보다 포괄적인 시각을 제공해야 합니다.

공격의 완전한 컨텍스트

이상적인 솔루션은 MITRE ATT&CK와 같은 공통 프레임워크를 사용하여 초기 침입부터 내부망 이동 및 데이터 유출 시도에 이르기까지 전체 공격 체인에 대한 완벽한 가시성을 제공해야 합니다.

통합 SOC 플랫폼으로의 전환

SOAR, 차세대 SIEM, 공격 표면 관리 등 주요 SOC 기술 전반에 대한 확장성을 보장하면서, 여러 보안 도구를 단일 인터페이스와 데이터 소스로 통합하는 플랫폼을 선택하세요.

6. 클라우드 탐지 및 대응 방식

클라우드별 아키텍처에 맞춰 조정된 런타임 보안 (예: 컨테이너, Kubernetes, VM)

컨테이너, Kubernetes를 비롯한 클라우드 아키텍처에 최적화되어야 하며, 이러한 클라우드 네이티브 아키텍처에 맞춰 조정된 런타임 보안을 제공하여 다양한 클라우드 워크로드를 포괄적으로 보호해야 합니다.

런타임 원격 분석과 에이전트리스 스캐닝, 클라우드 서비스 제공업체(CSP) 로그 데이터를 결합하여 클라우드 활동을 포괄적으로 이해합니다.

런타임 원격 분석, 에이전트리스 스캐닝, CSP 로그 데이터와 CNAPP 보안 인사이트를 통합하여 클라우드 활동과 워크로드 행동에 대해 완벽한 가시성을 제공하는 포괄적 클라우드 모니터링 솔루션을 선택하세요.

ML 기반 탐지/대응 및 인시던트 관리 워크플로

ML 기반 보안 플랫폼에서 실행되며, 하이브리드 및 멀티 클라우드 아키텍처를 지원하고, 클라우드와 온프레미스 환경 전반에 걸쳐 통합적인 탐지 및 대응 기능을 제공하며, 보안팀의 일관적 워크플로를 지원하는 솔루션을 선택하세요.

7. ID 기반 보안 통합 방식

ID 제공업체와의 통합

Active Directory, Okta와 같은 주요 ID 제공업체와 원활하게 통합되며, 포괄적 사용자 활동 데이터를 수집함으로써 전사적 위협 탐지 및 대응에 필수적인 컨텍스트를 제공하는 솔루션을 선택하세요.

ID 데이터 및 기타 보안 원격 분석과의 상관관계

ID 데이터와 보다 광범위한 보안 원격 분석의 상관관계를 파악하여 포괄적인 사용자 활동 가시성을 제공하는 솔루션을 선택하세요. 이러한 솔루션은 리스크 점수 평가 및 UEBA 기능을 통합하여 의심스러운 행동 패턴을 신속하게 파악합니다.

침해된 ID에 대해 ML 기반의 자동 탐지 및 대응

비정상적인 사용자 및 엔터티 행동을 자동으로 식별하여 침해된 자격 증명 및 내부자 위협을 발견하며, 신속한 자동 대응으로 ID 기반 공격을 완화하는 ML 기반 ID 위협 탐지 및 대응(ITDR) 시스템을 배포하세요.

8. 배포 및 관리 간소화 방식

단일 에이전트 설치, 배포 후 재부팅 배제

최종 사용자의 업무 중단이 최소화되며, 대규모 환경에서 신속한 배포와 업데이트가 가능합니다.

기본적으로 적용되는 모범 보안 정책

첫날부터 강력한 보안 태세를 보장하며, 사용자 정의를 허용하므로 구체적인 요구 사항을 충족할 수 있습니다.

보안 콘텐츠 업데이트 배포의 상세한 단계적 제어

새로운 보안 콘텐츠의 단계적 테스트 및 배포를 지원합니다. 따라서 안정성을 보장하고 잠재적인 중단을 최소화할 수 있습니다.

통합 관리 콘솔

직관적인 단일 콘솔을 통해 종합적 보안 관리를 제공하는 솔루션을 선택하세요. 엔드포인트 정책 관리부터 위협 탐지, 조사, 대응에 이르기까지 전반적인 관리 업무를 간소화하면서 조직의 보안 태세를 일관성 있게 파악할 수 있습니다.

엔드포인트 성능에 미치는 영향

에이전트 작동 시 낮은 CPU 사용률과 I/O로 엔드포인트 성능에 미치는 영향을 최소화해야 합니다. 그러면 사용자 생산성이나 시스템 성능을 저해하지 않으면서 강력한 보안을 확보할 수 있습니다.

대규모 기업을 위한 확장성

막대한 인프라 투자가 필요하지 않으면서도 증가하는 엔드포인트 및 데이터 볼륨을 손쉽게 수용할 수 있어야 합니다.

9. 솔루션의 효과를 뒷받침하는 업계 검증 및 독립적 검사

MITRE Engenuity ATT&CK 평가 결과

최신 MITRE Engenuity ATT&CK 평가를 통해 솔루션의 성능을 확인해 보세요. 종합적 보호 및 탐지 점수가 높은 솔루션을 선택하세요. 이상적인 솔루션은 구성 변경 없이도 강력한 효과를 발휘합니다. 분석 범위, 탐지 지연 여부 등의 지표를 주의하여 검토하세요.

AV-Comparatives 및 기타 독립 테스트 결과

실제 시나리오에서 솔루션의 효과를 검증하는 엔드포인트 탐지 및 대응 테스트에서 높은 점수를 기록한 솔루션을 선택하세요.

고객 추천 및 애널리스트의 인정

업계별 고객 사례를 바탕으로 실제 성능을 입증하는 동종업계의 피드백을 고려하고, Forrester Wave™, Gartner® Magic Quadrant™와 같은 애널리스트 보고서를 통해 시장에서 솔루션이 점하고 있는 위치와 기술력에 대한 평가도 참고해야 합니다.

10. EDR에서 XDR로, 그리고 궁극적으로 AI 및 자동화 기반의 완전한 SOC 혁신의 발전 지원

점진적 성장을 위한 기반

고급 위협 방지, 탐지 및 대응을 포함한 핵심 EDR 기능과 호스트 방화벽, 디스크 암호화 지원, 디바이스 제어 등 필수 엔드포인트 보호 기능을 결합하여 엔드포인트 수준에서 포괄적인 보안을 제공하는 솔루션을 선택하세요.

XDR 기능으로의 발전

네트워크, 클라우드, ID 및 타사 데이터를 통합하여 모든 보안 원격 분석 데이터에 대한 포괄적 가시성을 확보하고 자동 상관관계 분석을 수행함으로써 XDR로 확장되는 방식을 평가해야 합니다.

완전한 SOC 혁신을 향한 길

SOAR 및 차세대 SIEM 기능으로 확장하여 완전한 자동화를 구축하고, 공격 대응 시간을 며칠에서 몇 분 수준으로 단축할 수 있는 플랫폼인지 확인하세요.

미래지향적 아키텍처

EDR에서 XDR, 진정한 SOC 플랫폼에 이르는 3단계의 진행을 지원하는 통합 백엔드를 제공하며, 일관된 워크플로를 유지하고 AI 기반 자동화를 활용하는 솔루션을 선택하세요.

미래형 엔드포인트 보안 전략을 위한 CORTEX 고려

엔드포인트 보안 전략을 혁신하기 위한 10가지 핵심 질문을 검토한 결과, 급변하는 현대의 위협 환경에서 포괄적인 지능형 접근 방식이 반드시 필요하다는 것은 분명해 보입니다.

Cortex XDR®은 기존 엔드포인트 보안을 크게 상회하는 고급 위협 방지, 탐지 및 대응 기능을 제공하며, 이러한 핵심 고려 사항을 충족하는 솔루션으로 부상하고 있습니다.

Cortex XDR의 AI 기반 접근 방식은 이 문서에서 강조된 모든 사항을 충족합니다. 2024년 MITRE Engenuity ATT&CK 평가에서 100% 탐지율을 기록하며 업계 최고의 위협 방어 성능을 보여주었습니다. Cortex XDR은 알림 피로와 오탐을 크게 줄이고, 다양한 소스의 데이터를 통합하여 종합적 관점을 제공하며, 자동 및 수동 대응 옵션을 모두 제공합니다. 이러한 기능이 클라우드 지원 아키텍처 및 ID 보안 통합과 결합된 Cortex XDR은 현대 보안팀을 위한 강력한 도구로 자리잡고 있습니다.

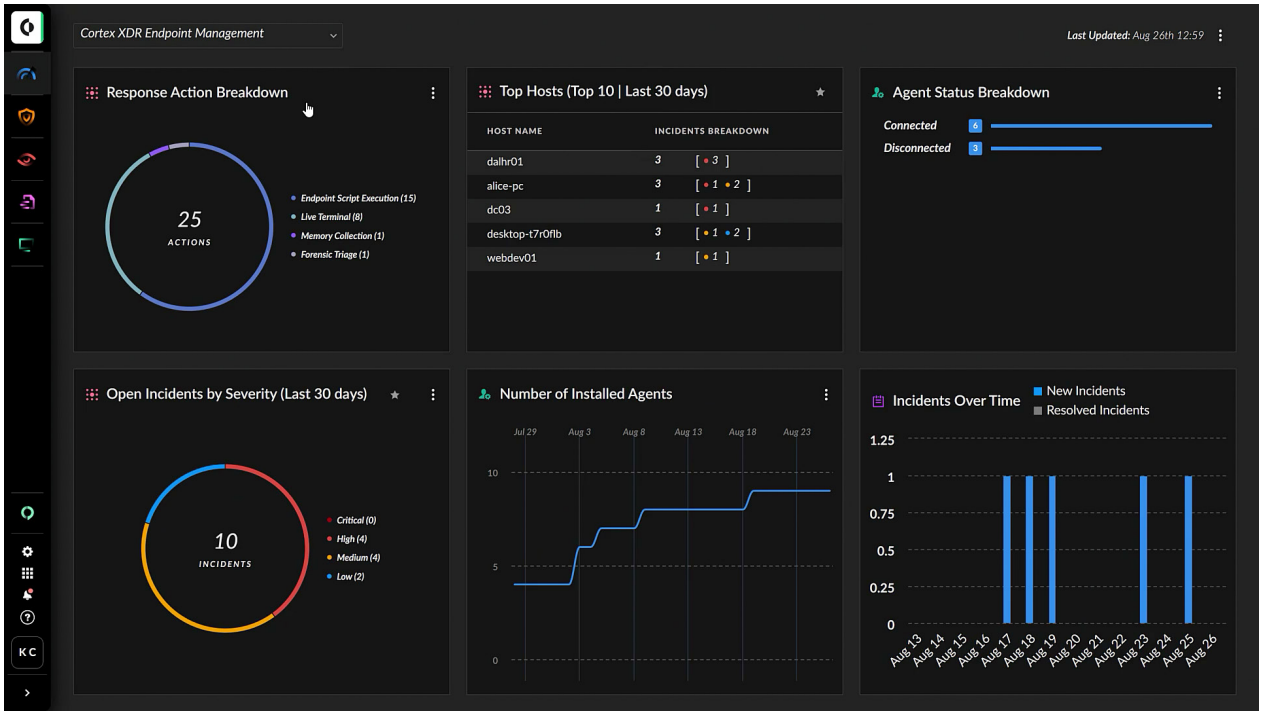


그림 1: Cortex XDR 엔드포인트 관리

Cortex XDR은 SOC 혁신을 추구하는 조직을 위해 확장 가능한 기반을 제공합니다. 이 아키텍처를 통해 보안팀은 핵심 EDR 기능으로 시작한 후 조직의 변화하는 요구 사항에 따라 전체 XDR 기능을 확장할 수 있습니다.

보안 여정의 다음 단계로, Cortex XSIAM®은 SOAR을 통해 자동 대응을 확장하고 AI 기반 차세대 SIEM 접근 방식을 통해 데이터 수집 기능을 강화함으로써 Cortex XDR을 한층 업그레이드한 혁신적 솔루션을 제공합니다. XSIAM 플랫폼은 AI와 자동화를 통해 보안 운영을 혁신함으로써 공격 차단 속도를 며칠이나 몇 주에서 몇 분으로 단축합니다.

Palo Alto Networks Cortex® 솔루션을 선택하는 것은 현재의 요구 사항을 충족하는 동시에 미래의 도전 과제에 대응할 수 있는 보안 전략에 투자하는 것입니다. 지속적 연구개발, 새로운 위협에 대한 조정, 미래의 보안 요구를 충족하기 위한 명확한 로드맵을 바탕으로 Cortex XDR과 XSIAM은 점점 더 복잡해지는 디지털 세계에서 보다 탄력적이고 효율적이며 효과적인 보안 태세를 구축할 수 있는 방안을 제공합니다.

Cortex XDR 제품 투어를 통해 이러한 기능을 직접 경험해 보세요. 플랫폼의 고급 기능을 살펴보고, 이 플랫폼을 활용하여 엔드포인트 보안 작업을 변화시키는 방안을 확인할 수 있습니다.

포괄적 MDR
연중무휴로 제공되는 전문 보안 운영

Cortex XDR 기술에 기반한 관리형 탐지 및 대응(MDR) 서비스는 인간의 전문성과 첨단 위협 탐지 및 대응 기능을 결합하여 연중무휴로 포괄적인 보안 범위를 제공합니다. 당사는 알림 관리, 인시던트 대응, 선제적 위협 헌팅 기능을 통해 모든 규모의 조직이 보안 태세를 강화할 수 있도록 도와드립니다.

성과 중심의 유연한 접근 방식에는 조직의 고유한 요구 사항에 따라 조정된 맞춤형 규칙과 플레이북이 포함되어 있으며, 시간 기반 SLA를 통한 탐지 및 대응 기능으로 이를 지원합니다. 당사와 파트너십을 맺으면 보안 운영의 성숙도를 즉시 향상시킬 수 있습니다. 그리고 당사가 현대적 보안 위협의 복잡성을 처리하는 동안 보다 중요한 전략적 이니셔티브에 집중할 수 있습니다.

Cortex XDR Unit 42 MDR로 미래를 보호하세요.

자세히 알아보기 →

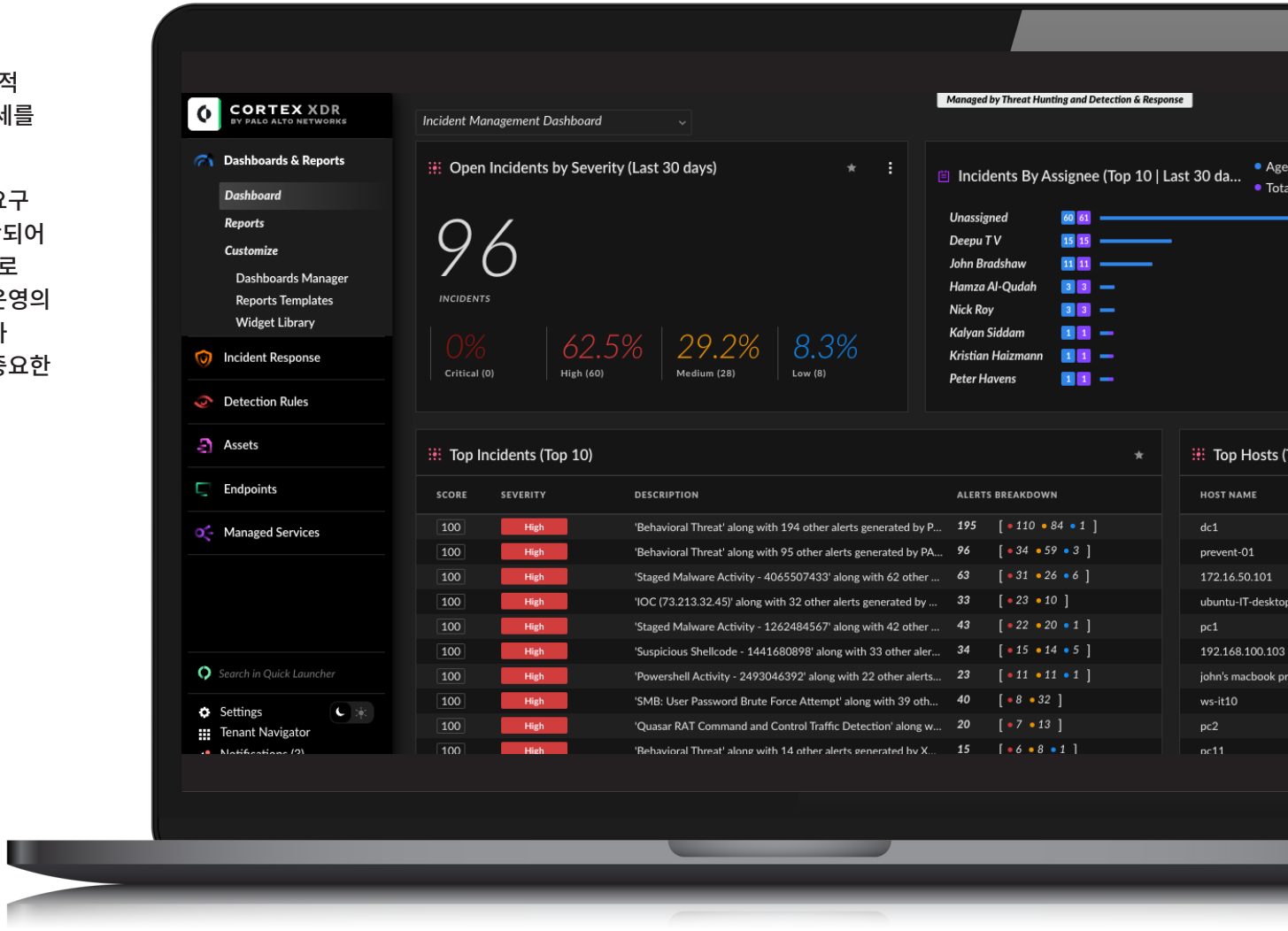


그림 2: Cortex XDR 및 Unit 42 관리형 탐지 및 대응(MDR) 대시보드

엔드포인트 보안을 위한 필수 평가 체크리스트

고급 위협 방지

다층적 보호 기능
- ☐ 차세대 안티바이러스 기능
- ☐ 랜섬웨어 방지
- ☐ 파일리스 공격 방지
- ☐ 익스플로잇 방지 모듈
- ☐ 행동 기반 보호

AI/ML 기반 보호 엔진
- ☐ 로컬 샌드박스 기능
- ☐ 지속적으로 업데이트되는 모델

추가 보안 기능
- ☐ 호스트 방화벽 기능
- ☐ 디스크 암호화 지원
- ☐ 디바이스 제어 기능

탐지 기능

EDR 기본 사항
- ☐ 실시간 모니터링
- ☐ 포괄적 엔드포인트 원격 분석 수집
- ☐ 교차 소스 이벤트 상관관계 분석

머신 러닝 및 분석
- ☐ 동작 분석 기능
- ☐ 다양한 위협 유형에 대한 다중 ML 모델
- ☐ 정기적 모델 업데이트

탐지 유연성
- ☐ 사전 구축된 탐지 규칙
- ☐ 사용자 지정 탐지 생성 옵션
- ☐ MITRE ATT&CK 프레임워크 조정

조사 및 대응

알림 관리
- ☐ 자동 알림 상관관계 분석
- ☐ 리스크 기반 우선순위 지정
- ☐ 오탐률 감소 기능

조사 도구
- ☐ 근본 원인 분석 기능
- ☐ 공격 체인 시각화
- ☐ 상세한 인시던트 컨텍스트

대응 옵션
- ☐ 자동 대응 기능
- ☐ 수동 대응 도구
- ☐ SOAR 플랫폼 통합

확장형 탐지 및 대응

데이터 통합
- ☐ 네트워크 데이터 수집
- ☐ 클라우드 보안 통합
- ☐ ID 공급업체 통합

교차 데이터 분석
- ☐ 다중 소스 상관관계 분석
- ☐ 통합 인시던트 보기
- ☐ 조사 컨텍스트 확장

클라우드 보안

클라우드 워크로드 보호
- ☐ 컨테이너 보안
- ☐ Kubernetes 보호
- ☐ VM 보안

클라우드 통합
- ☐ 클라우드 제공업체 로그 통합
- ☐ CNAPP 통합
- ☐ 멀티 클라우드 지원

배포 및 관리

구현
- ☐ 단일 에이전트 아키텍처
- ☐ 재부팅 없는 배포
- ☐ 기본 보안 정책

관리
- ☐ 통합 관리 콘솔
- ☐ 역할 기반 액세스 제어
- ☐ 정책 관리 도구

성능
- ☐ 낮은 시스템 영향
- ☐ 엔터프라이즈를 위한 확장성
- ☐ 대역폭 최적화

검증 및 테스트

업계 인식
- ☐ MITRE ATT&CK 평가 결과
- ☐ 독립적 테스트 점수(AV-Comparatives 등)
- ☐ 애널리스트 인정(Gartner, Forrester)

고객 검증
- ☐ 관련 업계의 고객 추천
- ☐ 사례 연구
- ☐ 프로덕션 환경 테스트 결과

미래지향적

공급업체 평가
- ☐ R&D 투자
- ☐ 기능 출시 주기
- ☐ 위협 연구 역량

로드맵 평가
- ☐ 예정된 기능 추가 사항
- ☐ 기술 파트너십
- ☐ 통합 기능

플랫폼 진화
- ☐ 완전한 SOC 플랫폼으로의 확장 가능성
- ☐ AI/ML 개발 계획
- ☐ 자동화 기능

비용 및 지원

가격 구조
- ☐ 라이선싱 모델
- ☐ 추가 모듈 비용
- ☐ 대량 구매 할인

지원 서비스
- ☐ 상시 기술 지원
- ☐ 구현 지원
- ☐ 교육 리소스

규정 준수 및 보고

규정 준수
- ☐ 내장된 규정 준수 보고 기능
- ☐ 주요 규정 지원(GDPR, HIPAA, PCI DSS 등)
- ☐ 맞춤형 규정 준수 보고서 생성

감사 지원
- ☐ 감사 추적 기능
- ☐ 과거 데이터 보존 옵션
- ☐ 증거 수집 도구

통합 기능

보안 도구 통합
- ☐ SIEM 통합
- ☐ 위협 인텔리전스 플랫폼 통합
- ☐ 티켓팅 시스템 통합

API 가용성
- ☐ REST API 문서
- ☐ 맞춤형 통합 지원
- ☐ API 속도 제한 및 할당량

데이터 내보내기
- ☐ 맞춤형 보고서 생성
- ☐ 원시 데이터 내보내기 기능
- ☐ 데이터 포맷 옵션

공급업체 평가

회사 안정성
- ☐ 재무 건전성
- ☐ 시장 점유율
- ☐ 고객 유지율

지원 인프라
- ☐ 글로벌 지원 범위
- ☐ 지원 대응 SLA
- ☐ 기술 자료 품질

커뮤니티 리소스
- ☐ 사용자 커뮤니티 규모
- ☐ 커뮤니티 포럼
- ☐ 타사 통합 마켓플레이스

운영 요구 사항

오프라인 기능
- ☐ 오프라인 보호 기능
- ☐ 로컬 탐지 기능
- ☐ 데이터 캐싱 메커니즘

백업 및 복구
- ☐ 에이전트 백업 옵션
- ☐ 구성 백업
- ☐ 재해 복구 지원

리소스 최적화
- ☐ CPU 사용량 제어
- ☐ 메모리 최적화
- ☐ 네트워크 대역폭 관리

종합적인 엔드포인트 보안 솔루션을 선택하는 과정에서 이 체크리스트를 참고하여 현재의 요구 사항을 충족하는 동시에 미래의 보안 운영 혁신을 위한 기반을 제공하는 솔루션을 선택하세요. 올바른 솔루션은 현재의 조직을 보호하고 미래에 등장할 새로운 위협에 대응할 수 있도록 확장성을 제공합니다.

지금 시작하기

데모를 예약하고 Cortex XDR을 활용하여 현재와 미래의 조직에서 운영을 간소화하고, 대규모 위협을 방지하고, 인시던트 해결을 가속화할 수 있는 방법을 알아보세요.

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