CUDO COMMUNICATION

paloalto NETWORKS

팔로알토 네트웍스

어제보다 안전한 오늘을 만듭니다.

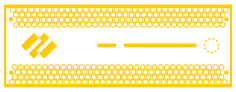
세계적인 사이버보안 전문기업 팔로알토 네트웍스는 사람의 일상과 조직의 운영을 혁신하는 기술로 미래를 만들고 있습니다. 팔로알토 네트웍스의 임무는 디지털 라이프를 보호하는 사이버보안 파트너가 되는 것입니다. 팔로알토 네트웍스는 최신 인공지능(AI), 분석, 자동화, 오케스트레이션 기술을 통한 지속적인 혁신으로 보안 과제 해결을 지원합니다. 전세계 수만여 개 조직이 팔로알토 네트웍스 통합 플랫폼과 광범위한 파트너 생태계를 기반으로 클라우드, 네트워크, 모바일 기기 전반의 보안을 강화하고 있습니다.

팔로알토 네트웍스는 다음과 같이 조직을 보호합니다.

STRATA
BY PALO ALTO NETWORKS

엔터프라이즈 보안

팔로알토 네트웍스 Strata™ 방화벽 플랫폼은 물리적/가상/클라우드 기반 폼팩터로 제공되는 일관되고 효과적인 통합 네트워크 보안 솔루션입니다.


Next-Generation Firewall


App-ID


Content-ID


User-ID

Panorama

DNS Security

Threat Prevention

URL Filtering

WildFire


Zingbox

GlobalProtect

SD-WAN

차세대 방화벽

물리적/가상/클라우드 기반 보안

팔로알토 네트웍스 차세대 방화벽은 사이버 공격을 차단하는 동시에 보안을 간소화합니다. Strata™ 방화벽 플랫폼은 혁신적인 여러 보안 기술을 내부에 통합함으로써 다수의 포인트 제품들을 대체합니다. 물리적 환경, 가상 환경, 클라우드 환경 어디든지 구축이 가능하여 데이터와 앱이 어디에 있든 일관된 보안을 제공합니다. 세계 최고의 사이버보안 기술을 활용하여 정교한 공격을 방어하고 네트워크를 안전하게 혁신하십시오.

App-ID

애플리케이션 분류 기술

App-ID™는 팔로알토 네트웍스 방화벽에서만 제공되는 특허받은 트래픽 분류 기술입니다. 포트, 프로토콜, SSH/SSL 암호화나 기타 우회 기법에 관계없이 애플리케이션을 식별할 수 있습니다. App-ID는 네트워크 트래픽 스트림에 애플리케이션 시그니처, 애플리케이션 프로토콜 디코딩(protocol decoding), 휴리스틱(heuristics) 등 여러가지 분류 메커니즘을 적용하여 애플리케이션을 정확하게 파악합니다. 식별된 애플리케이션에 대해서는 정책 확인(policy check)을 통해 차단, 허용, 위협 스캔, 무단 파일 전송 및 데이터 패턴 조사, QoS 트래픽 쉐이핑 등 처리 방식을 결정할 수 있습니다. 포트 기반의 레거시 방화벽 규칙에서 App-ID™ 기술 기반 규칙으로 전환하면 공격 가능성이 대폭 줄어듭니다. PAN-OS 자체 기능인 Policy Optimizer로 손쉽게 전환이 가능합니다. Policy Optimizer는 단순한 워크플로우와 PAN-OS가 수집한 인텔리전스를 사용하여 레거시 규칙을 App-ID 기반 컨트롤로 전환하고 조직의 보안을 강화합니다.

Content-ID

콘텐츠 분류 기술

Content-ID™ 기술은 다수의 고급 위협 방지 기술을 사용하여 한 번의 스캔으로 허용된 모든 트래픽에 대한 종합적인 분석을 수행합니다. 팔로알토 네트웍스 차세대 방화벽은 Content-ID를 통해 취약점 익스플로잇, 버퍼 오버플로우, 포트 스캔을 방지하고 공격자의 우회 및 난독화 수법을 무력화시킵니다. 또한 멀웨어와 C2 서버의 통신을 막고 알려진 멀웨어, 피싱 다운로드 사이트 액세스를 차단하며 파일과 데이터의 무단 전송에 따른 위험을 감소시킵니다.

User-ID

사용자 분류 기술

User-ID™ 기술은 사용자 또는 사용자 그룹 별로 아웃바운드/인바운드 양방향으로 안전하게 애플리케이션 사용을 지원하는 정책을 정의합니다. 예를 들어 IT 부서만 기본 포트에서 SSH, telnet, FTP 같은 툴을 사용하도록 허용할 수 있습니다. User-ID 기술을 통해 사용자가 본사, 지사, 집 어디에 있든 어떤 디바이스를 사용하든 사용자에 따른 정책이 적용됩니다. 또한 기존 또는 커스텀 템플릿을 사용하여 사용자 활동에 대한 리포트를 생성할 수 있습니다.

User-ID 기술은 단순한 IP 주소가 아닌 사용자 레벨의 애플리케이션 작업 가시성을 제공함으로써 네트워크 상의 애플리케이션을 보다 효과적으로 관리하도록 해줍니다. 비즈니스 요구에 맞게 애플리케이션 사용을 지원하고, 필요하다면 사용자에게 정책 위반을 고지하거나 애플리케이션 사용을 완전히 차단할 수 있습니다. DUG(Dynamic User Groups)는 관리자가 보안 침해 징후나 비즈니스 필요(예: 일부 사용자에게 임시 액세스 허용)로 인한 상황 변화에 따라 동적으로 사용자 액세스를 변경할 수 있도록 해줍니다.

Panorama

관리 솔루션

Panorama™ 네트워크 보안 관리는 여러 위치에서 다양한 형태로 운용되는 모든 팔로알토 네트웍스 방화벽에 대한 중앙 관리를 제공합니다. Panorama는 온보딩에서부터 프로비저닝, 그리고 모든 기능을 활용하는 보안 정책 설정에 이르기까지 방화벽 전반의 구성, 배포, 관리를 간소화함으로써 복잡성을 줄여 줍니다. 또한 Panorama는 중앙에서 네트워크 트래픽, 로그, 위협에 대한 가시성과 종합적인 인사이트를 제공합니다. Panorama는 소프트웨어 업데이트 관리와 콘텐츠 업데이트 자동 예약을 지원함으로써 관리자의 업무 부담을 경감시켜 주며, 결과적으로 최상의 보안 태세를 유지할 수 있도록 해줍니다.

Panorama는 네트워크 경계, 브랜치, 데이터센터, 모바일 사용자, 클라우드 등 구축 위치에 관계없이 모든 방화벽을 관리할 수 있습니다. API를 통해 타사 시스템 및 기존 운영 툴과 손쉽게 통합됩니다. 커스터마이즈 가능한 Application Command Center는 네트워크 및 위협 데이터에 대한 실시간/시간대별 상관분석 인사이트를 제공합니다. 또한 API 기반 통합으로 운영을 간소화하는 정책 기반 액션을 통해 위협 대응 자동화를 지원합니다.

DNS 보안

DNS를 사용한 공격 방지

멀웨어의 80%가 DNS를 사용하여 C2(command-and-control) 채널을 설정합니다. 공격자가 DNS에 숨는 경우가 종종 있는데, 그 이유는 트래픽 양이 너무 많아서 이를 제대로 모니터링할 수 있는 도구가 없는 조직이 태반이기 때문입니다. 팔로알토 네트웍스의 DNS 보안(DNS Security) 서비스는 예측 분석, 머신러닝, 자동화를 적용하여 DNS를 사용하는 공격을 차단합니다. DNS Security는 차세대 방화벽과 결합되어 자동 보호를 제공하고, 공격자가 보안 시스템을 우회하지 못하게 막고, DNS 라우팅을 변경하거나 별도의 툴을 사용할 필요가 없게끔 해줍니다. DNS 보안 서비스를 통해 악성 도메인을 조기에 차단하고, DNS 터널링으로 잠입하는 위협을 무력화시키고, 자동화를 적용하여 감염된 기기를 신속하게 탐지하고 격리할 수 있습니다. DNS 보안 서비스는 클라우드 기반 보안으로 무제한 확장이 가능하며 상시 최신 상태를 유지함으로써 DNS 사용 공격을 차단하는 새로운 컨트롤 포인트를 제공합니다.

위협 방지

익스플로잇, 멀웨어, C2 방지

팔로알토 네트웍스 위협 방지(Threat Prevention) 서비스는 IPS 기능을 통해 알려진 클라이언트/서버 취약점 익스플로잇을 자동으로 차단합니다. 또한 인라인 멀웨어 방지 기능을 제공하며 아웃바운드 C2 트래픽을 차단합니다. 위협 방지 서비스는 포트, 프로토콜, 암호화에 관계없이 모든 트래픽에서 위협 검사를 실행하여 숨겨진 위협을 찾아냅니다. 위협 방지 서비스는 네트워크 진입 시 뿐만 아니라 사이버 공격의 전 과정을 통틀어 위협을 탐지함으로써 제로트러스트(Zero Trust) 모델에 부합되는 다단계 방어를 제공합니다. 모든 위협에 대해 일정한 시그니처 포맷을 유지하기 때문에 한번의 통합 스캔으로 모든 분석을 수행하고 중복된 프로세스를 제거합니다.

따라서 신속한 처리가 보장됩니다. 위협 방지 서비스는 차세대 방화벽을 통과하는 모든 개별 패킷에 대해 패킷 헤더와 페이로드에서 바이트 시퀀스를 면밀히 조사합니다. 이러한 분석을 통해 사용된 애플리케이션, 소스/목적지, 프로토콜의 RFC 준수 여부, 페이로드에 익스플로잇 코드 또는 악성 코드가 포함되어 있는지 여부 등 각 패킷에 대한 중요한 세부 정보를 확인할 수 있습니다. 또한 우회 기술을 포착하고 방지하기 위해 개별 패킷 뿐만 아니라 도착 순서의 컨텍스트와 여러 패킷의 시퀀스를 분석합니다. 이 모든 작업이 한 번의 스캔으로 이루어지므로 네트워크 트래픽 속도가 저하되지 않습니다.

URL 필터링

유해 사이트 및 피싱 방지

URL 필터링(URL Filtering)을 통해 비즈니스 요구에 맞는 안전한 웹 사용을 보장할 수 있습니다. 클라우드에서 제공되는 팔로알토 네트웍스의 URL 필터링 서비스는 머신러닝이 결합된 강력한 정적 분석으로 위협을 식별함으로써 기본 웹 필터링에 비해 훨씬 강력한 효과를 제공합니다. 또한 자동 방어 기능으로 멀웨어를 전송하고 계정을 탈취하는 유해 사이트에 대한 액세스를 차단합니다. 조직은 방화벽 정책을 확장하여 공격 노출을 최소화하고 상시 최신 보안 업데이트를 활용할 수 있습니다. 아울러 애플리케이션 별, 사용자 별 정책을 적용하여 복잡한 웹 보안 규칙을 단순화하고 운영 부담을 줄여줍니다.

URL 필터링은 카테고리와 위험 등급을 정확하게 파악하기 위해 정적 분석, 동적 분석, 머신러닝을 모두 사용하여 웹 사이트를 스캔하고 콘텐츠를 분석합니다. URL 필터링 서비스를 통해 양성 또는 악성으로 분류된 URL 목록을 차세대 방화벽 정책에 손쉽게 적용하여 웹 트래픽을 완벽하게 제어할 수 있습니다. URL 필터링은 새로운 악성 URL을 발견 즉시 차단합니다. 따라서 보안 분석가의 수동 개입이 전혀 필요 없습니다.

WildFire

멀웨어 방지

WildFire® 멀웨어 방지 서비스는 알려지지 않은 위협을 자동으로 탐지하고 차단합니다. WildFire는 기존 샌드박스 방식을 뛰어넘어 머신러닝, 정적 분석, 동적 분석, 네트워크 프로파일링 등 다양한 고급 분석 엔진을 사용함으로써 최신 공격 기술을 무력화시키도록 지원합니다.

WildFire는 커스텀 하이퍼바이저와 업계 최초의 베어메탈 분석 엔진을 사용한 우회 방지 기능을 통해 최신 위협까지 차단합니다. 클라우드에서 제공되는 모듈형 아키텍처의 WildFire는 운영 중단을 야기하는 전통적인 샌드박스 솔루션과 달리 혁신적인 최신 탐지 엔진을 지속적으로 제공합니다.

WildFire는 방대한 글로벌 커뮤니티에서 제공되는 데이터를 통해 알려지지 않은 위협을 탐지합니다. WildFire는 공유 데이터를 사용하여 최신 공격을 신속하게 식별하고 방지합니다. WildFire 글로벌 커뮤니티는 네트워크, 엔드포인트, 클라우드, 써드파티 파트너로부터 전송된 위협 인텔리전스를 활용하는 업계 최대의 엔터프라이즈 멀웨어 분석 커뮤니티입니다.

WildFire는 위협 방지를 자동화하고 지능형 공격에 대한 위협 인텔리전스를 제공합니다. 고객은 몇 초 만에 플랫폼 전반에 대한 즉각적인 자동 보호 기능을 통해 멀웨어, 악성 URL, DNS 기반 공격, C2를 차단할 수 있습니다. WildFire는 AutoFocus 서비스와 완벽하게 통합되어 WildFire가 수집하고 처리하는 모든 데이터에 대한 풍부한 컨텍스트 및 속성 정보를 제공합니다. 보안팀은 식별된 위협의 활동 내역, 보안 침해 지표, 차단 방법에 대한 상세한 인사이트를 통해 시간을 절약할 수 있습니다.

Zingbox

엔터프라이즈 IoT 보안 및 OT 인텔리전스

Zingbox®는 업계 최강의 IoT 보안을 제공하여 관리 사각지대의 기기를 탐색, 보호, 최적화할 수 있도록 해줍니다. 에이전트리스(agentless) 방식으로 머신러닝과 산업별 인텔리전스를 활용하여 IT, 의료, 에너지, 제조, 스마트시티, ICS/SCADA 환경 전반에서 IoT 기기를 노리는 위협으로부터 기업을 보호합니다.

AI, 머신러닝, 통합 인텔리전스가 결합되어 각 기기의 작동을 파악하고 의심스러운 움직임을 자동으로 탐지하며 모든 네트워크 연결 IoT 자산에 대한 보안을 강화합니다. Zingbox를 통해 조직은 IoT 및 OT 인프라 수명주기 전반을 오케스트레이션할 수 있습니다. 아울러 심층적인 운영 인사이트를 통해 IoT 인프라(예: X-ray 기계, 스마트 카메라, 스마트 프린터)를 최적화하고 비즈니스 성과를 향상시킬 수 있습니다.

Zingbox는 자산 관리 전반에 대한 네이티브 통합 기능을 통해 NAC(network access control), SIEM(security information and event management), SOAR(security orchestration, automation, and response), 무선 LAN 컨트롤러, 네트워크 관리, 취약성 스캐너, 산업별 기기 인텔리전스 데이터베이스 등 모든 주요 IT 시스템에 IoT 인텔리전스를 강화합니다.

GlobalProtect

모바일 사용자 보안

엔드포인트를 위한 GlobalProtect™ 네트워크 보안을 사용하면 기기 또는 위치에 관계없이 모든 사용자에게 차세대 방화벽 기능을 확대하여 모바일 사용자를 보호할 수 있습니다. 이 솔루션은 뛰어난 위협 방지 기능으로 우회 애플리케이션 트래픽, 피싱, 계정 탈취 등으로부터 사용자를 보호합니다. 또한 GlobalProtect는 모든 포트에서 모든 애플리케이션 트래픽을 상시 검사하여 상세한 가시성을 제공하므로 보다 효율적인 보안 정책을 작성하고 실행할 수 있습니다. GlobalProtect는 클라이언트리스(clientless) VPN을 통해 클라우드와 데이터센터 애플리케이션 액세스 뿐만 아니라 BYOD(Bring-Your-Own-Device)를 위한 보안 옵션을 제공합니다. GlobalProtect는 AirWatch®, Microsoft Intune®, MobileIron®을 비롯한 엔터프라이즈 모빌리티 관리 제품과 통합되어 앱 별 VPN을 지원합니다.

SD-WAN

브랜치 연결 보안

팔로알토 네트웍스 SD-WAN 솔루션은 세계적 수준의 보안 및 연결 기술이 네이티브 통합된 엔드 투 엔드 SD-WAN 아키텍처를 간편하게 도입할 수 있도록 해줍니다. Prisma Access를 SD-WAN 허브로 사용하여 성능을 최적화하고 사용자 경험을 향상시킬 수 있습니다. 또한 안전한 Prisma Access SD-WAN 허브를 서비스 형태로 사용할 경우, SD-WAN 허브 인프라 구축에 따른 복잡성을 없앨 수 있습니다. 또는 팔로알토 네트웍스 차세대 방화벽을 사용하여 허브 및 인터커넥트 인프라를 자체적으로 구축할 수 있습니다. 어떤 구축 모델을 선택하든 직관적인 단일 인터페이스를 통해 보안과 SD-WAN을 관리할 수 있습니다.

PRISMA
BY PALO ALTO NETWORKS

클라우드 보안

Prisma™는 업계에서 가장 완벽한 클라우드 보안을 제공합니다. 오늘날의 복잡한 IT 환경을 보호하도록 설계된 Prisma 제품군을 통해 안전한 클라우드 전환을 가속화하십시오.


Prisma Access


Prisma Cloud


Prisma SaaS

Data Loss Prevention

Prisma Access

클라우드 기반 모바일 사용자 보안

Prisma™ Access는 재택근무자와 모바일 사용자에게 일관된 보안을 제공하도록 지원하는 SASE(secure access service edge)입니다. Prisma Access는 클라우드 기반 인프라를 사용하여 모든 사용자를 모든 애플리케이션에 연결하는 클라우드 보안을 새로운 차원으로 향상시킵니다. 본사나 지사에 있거나 이동 중인 모든 사용자가 Prisma Access에 연결하여 인터넷은 물론 클라우드와 데이터센터 애플리케이션을 안전하게 사용할 수 있습니다. 전세계 76 개 국 100여 개 로케이션에 위치에 Prisma Access는 모든 포트에서 모든 트래픽을 지속적으로 검사하고 지사와 지사, 지사와 본사 간 트래픽을 지원하는 양방향 네트워킹을 제공합니다.

광범위한 보안을 제공하는 Prisma Access는 전 세계에서 서비스를 제공하므로 지사에 하드웨어 방화벽 배치를 고민할 필요가 없습니다. Prisma Access는 중앙 분석, 리포팅, 포렌식을 위해 Cortex Data Lake를 사용합니다.

Prisma Cloud

클라우드 네이티브 보안 플랫폼

Prisma™ Cloud는 하이브리드 클라우드 및 멀티 클라우드 환경의 클라우드 네이티브 기술 스택, 애플리케이션, 데이터 전반에 대해 업계에서 가장 방대한 보안 및 컴플라이언스 커버리지를 제공하는 클라우드 네이티브 통합 플랫폼입니다. Prisma Cloud는 호스트, 컨테이너, 서버리스(serverless) 구축, 스토리지, 기타 PaaS(platform-as-a-service) 전반의 클라우드 네이티브 애플리케이션과 데이터를 보호합니다.

Prisma Cloud는 리소스를 동적으로 탐색하고 클라우드 서비스가 제공하는 데이터(리소스 구성, 플로우 로그, 감사 로그, 호스트 및 컨테이너 로그 등)를 상호연관시켜 클라우드 애플리케이션에 대한 보안 및 컴플라이언스 인사이트를 제공합니다. 또한 머신러닝을 사용하여 사용자, 워크로드, 앱 활동을 프로파일링함으로써 정교한 위협을 방어합니다.

Prisma Cloud는 CI/CD 툴 체인과 통합되어 라이프사이클 전반의 취약점 관리, IaC(infrastructure-as-code) 스캐닝, 런타임 공격 방어, 클라우드 네이티브 방화벽 기능을 제공합니다. 또한 업계 최고 수준의 컴플라이언스 프레임웍 라이브러리를 통해 규제 준수 업무를 간소화합니다. Prisma Cloud는 인프라, PaaS, 사용자, 개발 플랫폼, 데이터, 애플리케이션 워크로드 전반에서 심층적인 컨텍스트 공유를 통해 이를 제공합니다. 보안 오케스트레이션 툴과 원활하게 통합되어 취약점을 신속하게 수정할 수 있도록 해줍니다.

Prisma SaaS

SaaS 액세스 보안

Prisma™ SaaS는 클라우드 애플리케이션과 민감한 데이터에 대한 가시성, 컴플라이언스 컨트롤, 보안을 제공함으로써 안전한 클라우드 도입을 지원합니다. Prisma SaaS는 쉐도우 IT 사용을 최소화하도록 지원하며 Office 365®, Salesforce®, G-Suite®, Slack®, Box와 같은 기업 SaaS 애플리케이션에 안전하게 액세스할 수 있도록 해줍니다. 또한 클라우드 데이터 유출의 위험을 줄입니다. Prisma SaaS는 다수의 SaaS 애플리케이션에 대한 지속적인 가시성, 컴플라이언스 컨트롤, 보호를 제공하는 클라우드 서비스입니다. Prisma SaaS는 클라우드 사이버 리스크로부터 조직과 데이터를 보호하며, 조직이 SaaS 애플리케이션을 안전하게 도입하고 민감한 데이터를 클라우드에 안전하게 저장하도록 지원합니다.

팔로알토 네트웍스 방화벽의 통합 기능인 Prisma SaaS는 모든 네트워크 트래픽의 인라인 인스펙션(in-line inspection)과 SaaS 애플리케이션을 위한 API 기반(또는 자체 검사 기반) 보안을 위해 모든 인터넷 트래픽과 모든 애플리케이션에서 작동합니다. 그리고 SaaS 애플리케이션으로 가시성, 기업 보안, 컨트롤 및 컴플라이언스, 데이터 보호를 일관되게 확장함으로써 SaaS 보안이 회사 전체의 보안 이니셔티브와 괴리되지 않고 긴밀한 연계 선상에서 유지되도록 해줍니다.

Enterprise DLP

데이터 보호 및 컴플라이언스

팔로알토 네트웍스 엔터프라이즈 데이터 유출 방지(Enterprise Data Loss Prevention)는 모든 트래픽, 모든 애플리케이션, 모든 사용자에 대해 개인식별정보(personally identifiable information, PII), 지적재산과 같은 민감한 데이터의 지속적이고 안정적인 보호를 제공하는 클라우드 서비스입니다. 기존 팔로알토 네트웍스 제품과 네이티브 통합이 가능하여 도입이 간단하며, 최신 머신러닝을 통해 관리 복잡성을 최소화합니다.

Enterprise DLP는 민감한 데이터가 어디에 있든, 어디로 전송되든 지속적인 탐색, 모니터, 관리, 보안이 가능하도록 해줍니다. Office 365나 Box와 같은 클라우드 애플리케이션에서의 데이터 침해 위험을 최소화함으로써 안전한 클라우드 도입을 지원하고 GDPR, CCPA, PCI DSS, HIPAA 등과 같은 엄격한 규제 관련 컴플라이언스와 데이터 프라이버시 준수를 지원합니다.

CORTEX™
BY PALO ALTO NETWORKS

미래의 보안

Cortex™는 업계에서 가장 종합적인 보안 운영 제품군으로서 엔터프라이즈 환경을 위한 최고 수준의 탐지, 조사, 자동화, 대응 기능을 제공합니다.

AutoFocus


Cortex Data Lake


Cortex XDR


Cortex XSOAR

AutoFocus

상황별 위협 인텔리전스

상황별 위협 인텔리전스 서비스 AutoFocus™는 고객이 팔로알토 네트웍스의 방대한 위협 인텔리전스 저장소로부터 피드를 수신할 수 있도록 해줍니다. 업계 최대 규모의 네트워크, 엔드포인트, 클라우드 인텔리전스 소스에서 크라우드소싱을 통해 실제 공격에 대한 인사이트를 얻을 수 있습니다. 세계적으로 알려진 Unit 42의 위협 연구원들이 모든 위협에 대한 심층적 컨텍스트를 제공합니다. 조직의 보안 분석가는 커스텀 위협 피드와 API를 통해 어떤 툴에든 위협 인텔리전스를 임베드함으로써 많은 시간을 절약할 수 있습니다.

Cortex Data Lake

보안 분석을 위한 정규화된 데이터

Cortex™ Data Lake는 엔터프라이즈 보안 데이터를 수집, 통합, 정규화하여 Cortex XDR, Prisma Access, 차세대 방화벽을 비롯한 팔로알토 네트웍스 솔루션에서 활용할 수 있도록 해줍니다.

Cortex XDR

탐지 및 대응 확장

Cortex XDR™은 보안운영팀이 노이즈를 줄이고 실제 위협에 집중할 수 있도록 해줍니다. Cortex XDR은 엔드포인트, 네트워크, 클라우드 데이터를 통합하여 숨어있는 최신 위협을 신속하게 찾아낼 수 있도록 해줍니다. 보안운영팀은 포인트 제품들을 방지, 탐지, 조사, 대응을 위한 통합 플랫폼으로 대체하여 복잡성을 획기적으로 줄일 수 있습니다.

Cortex XDR은 리치 데이터 분석과 행동 분석(BA), 머신러닝을 사용하여 위협을 정확하게 탐지합니다. 그리고 개별 인시던트에 대한 상세 정보와 근본원인을 보여줌으로써 위협 조사에 소요되는 시간을 과거에 비해 8분의 1로 단축합니다. Cortex XDR은 알림 선별에서부터 위협 헌팅까지 보안 운영의 모든 과정을 간소화하며 분석에 필요한 경험과 시간을 줄여줍니다. 또한 기존 정책 집행 지점(enforcement points)과 긴밀하게 통합되어 격리를 가속화하고 피해가 발생하기 전에 신속하게 공격을 중단시킵니다.

Cortex XSOAR

XSOAR(Extended Security Orchestration, Automation, and Response)

Cortex™ XSOAR는 업계 최초의 확장된 SOAR(security orchestration, automation, and response) 플랫폼으로 SOC 효율성을 획기적으로 향상시킵니다. 보안 책임자는 종합적인 통합 케이스 관리, 자동화, 실시간 협업, 위협 인텔리전스 관리를 통해 운영의 모든 측면을 혁신할 수 있습니다. Cortex XSOAR을 통해 보안운영팀은 모든 소스의 경보를 관리하고, 플레이북을 통해 프로세스를 표준화하고, 위협 인텔리전스에 대한 조치를 실행하고, 모든 보안 유스케이스에 대한 대응을 자동화할 수 있습니다. 이렇게 함으로써 대응 시간이 90% 빨라지고 사람의 개입이 필요한 경보가 95% 줄어듭니다.

Memo

Memo

팔로알토 네트웍스 국내 총판사

쿠도커뮤니케이션(주)

CUDO COMMUNICATION

WWW.CUDO.CO.KR
T. 02-525-0481 I F. 02-775-3883 I E. SECURE@CUDO.CO.KR
06665 서울시 서초구 방배로 84 유성빌딩 4층(방배동)

블로그: BLOG.NAVER.COM/CUDO_SECURE
파트너 포탈: PARTNER.CUDO.CO.KR

paloalto® NETWORKS