DOOSAN

cybereason©

MITRE ATT&CK 평가 결과

2023 엔터프라이즈 부문

더 정교해진 해커의 공격을 막아냅니다

준비되지 않은 보안 환경은 더욱 정교해진 위협에 당할 수 밖에 없습니다. 교묘한 위협에 대응하기 위해서는 효과적인 보안 솔루션에 투자해야합니다.

MITRE ATT&CK 평가는 보안 효과를 측정하는 테스트이며, 2023년 평가에는 30개의 글로벌 벤더사가 참가했습니다. 5가지 주요 평가 항목은 보호 커버리지, 탐지 커버리지, 가시성, 실시간 탐지 및 즉시 사용 가능한 성능이었습니다.

100%

보호 커버리지

사이버리즌은 Windows 및 Linux 시스템 전반에 걸친 **13개 공격 시퀀스를 모두 발견하고 방어**했습니다.

100%

탐지 커버리지

사이버리즌은 유명 해커 단체인 Turla의 **19개 공격 단계를 모두 탐지**했습니다.

100%

가시성

사이버리즌은 Windows 및 Linux 시스템에서 공격 탐지 누락 0건으로 **143건의 모든 공격 행위를 가시화했습니다.**

100%

실시간 탐지

모든 사이버리즌 탐지는 실시간으로 진행되었으며, 가장 빠르게 응답했습니다.

100%

즉시 사용 가능

사이버리즌은 구성 변경 필요 없이 **즉시 사용 가능한 완벽한 성능을 제공**했습니다.

MITRE ATT&CK은 왜 중요할까요?

MITRE ATT&CK 는 보안 솔루션 기능을 중점적으로 평가하는 테스트입니다.

모든 벤더사가 각사의 보안 솔루션을 제출하면 동일한 평가 방식으로 공정하게 평가합니다. 매년 진행되는 이 테스트는 오늘날 사이버 공격 예방과 탐지 기술력을 입증하는 기준이 되었습니다.

ATT&CK는 악의적인 도구, 전술 및 과정(TTP'S)을 매핑하는 표준화된 프레임워크이자 보안 벤더사 및 보안 실무자가 인정하는 평가 기준입니다. 이 TTP 카탈로그는 이전에는 없었던 탐지 및 대응 구조와 조직을 만들고, ATT&CK는 항상 새로운 위협을 통합시키기 위해 확장되고 있습니다.

ATT&CK은 탐지와 대응 효과를 평가하기 위해 매년 진행되는 테스트입니다.

MITRE는 매우 명성이 높고, 공격 시뮬레이션을 바탕으로 평가를 실시합니다. MITRE의 미션은 글로벌 사용자들이 공격자들의 행동을 더 잘 이해할 수있도록 돕는 것입니다. MITRE는 벤더사가 많은 비용을 지불한다고 해서 좋은 평가를 내리지 않습니다. MITRE 평가는 공정하고 투명하게 진행됩니다.

2023년 엔터프라이즈 평가는 민감 정보를 유출하기 위해 타겟을 감시하는 것으로 알려진 매우 정교한 공격 단체인 Turla를 활용해 실시되었습니다. Turla는 운영 보안을 유지하기 위해 새롭고 정교한 기술을 사용하는데, 여기에는 오픈 소스 및 인하우스 툴들을 이용하는 레퍼토리와 함께 독특한 명령 및 제어 네트워크를 사용하는 것이 포함됩니다.

평가 결과

Turla

100% 보호

공격에 적절히 대응하지 못하는 보안 솔루션은 보안 팀에 오히려 혼란을 일으킵니다. 위협을 더 많이 방지할수록 보안팀이 직접 조사하고 대응해야 하는 상황이 줄어듭니다.

사이버리즌은 2023 엔터프라이즈 평가에서 100% 보호력을 인정 받았습니다.

100% 가시성

정교한 공격을 탐지하고 방지하는 것은 정말 어려운 일이기 때문에 보안 솔루션에서 공격의 전체적인 흐름을 볼 수 있는 능력은 매우 중요합니다.가시성이 높으면 어디서 공격이 시작되었고, 어떤 영향을 미쳤는지를 포함해 전체 공격 타임라인 확인할 수 있습니다.

사이버리즌은 MITRE ATT&CK 프레임워크에 매핑되어 있으며 2023년 엔터프라이즈 평가에서 진행한 143개 공격 행위를 100% 가시화했습니다.

100% 실시간 탐지

탐지 지연은 즉각적인 탐지가 불가능하며 탐지 및 공격 식별에 추가적인 시간이 요구됩니다. Turla와 같은 정교한 위협 방어에 있어 가장 중요한 요소는 시간입니다.

2023년 엔터프라이즈 평가에서 사이버리즌은 100% 실시간으로 탐지하고 지연 없이 즉각적으로 가시성을 제공했습니다.

100% 탐지

공격자가 노이즈 속에 숨지 못하도록 공격 행위를 즉각적으로 감지할 수 있는 보안 도구는 필수입니다.

사이버리즌은 Turla의 19 공격 단계를 100% 탐지해냈으며, 이 중 거의 모든 탐지(97%)를 공격자의 정확한 행위를 나타내는 주요 ATT&CK 기술에 매핑시켰습니다.

100% 즉시 사용 가능

모의 공격에서는 보안 솔루션의 첫 시도에 실수가 있어도, 구성을 다르게 조정해 공격을 방어할 수 있습니다. 그러나 현실에서 보안 솔루션이 공격을 탐지하지 못하면 더 이상의 기회는 없습니다. 보안팀은 보안 시스템을 만지작거리면서 시간을 보내는 대신 바로 사용이 가능한 솔루션을 활용해 중요한 대응 작업에 집중해야합니다.

2023년 평가에서 사이버리즌은 구성 변경 없이 즉시 사용 가능한 성능을 선보였습니다.

왜 사이버리즌일까요?

중요한 순간에 발휘되는 높은 성능
사이버리즌은 가장 정교한 적을 상대로 높은 성능을 제공하는 매우 효과적인 보안 솔루션입니다.

랜섬웨어에 준비된 솔루션
사이버리즌은 사전예방과 다계층 방어로 랜섬웨어와의 싸움에서 패배하지 않습니다.

즉시 제공되는 가시성
실시간으로 위협 요소를 확인하고 즉각적으로 대응하여 공격의 영향과 위험을 최소화합니다.

완벽한 방어력
보안팀은 수작업으로 조사하고 대응하는 대신 사이버리즌 기술을 이용하여 공격을 차단하고 예방할 수 있습니다.

실행력 강한 탐지
MalOp™는 실행력이 뛰어나며 공격 범위, 시간대, 공격자가 사용한 도구 및 위협이라 판단하는데 도움이 되는 모든 원격 측정 기능이 포함되어 있습니다.

한번의 클릭으로 대응
한 번의 클릭으로 공격에 대응해 영향 받은 모든 시스템과 조직 전체 사용자에 대한 신뢰를 즉시 회복할 수 있습니다.

사이버리즌은 ATT&CK 프레임워크와 긴밀하게 연계되어 있으며, 효율적인 대응을 위해 모든 ATT&CK 관련 탐지에 MITRE 태깅을 포함하고 있습니다.

사이버리즌은 지금까지 모든 ATT&CK 평가에 꾸준히 참가했으며, 최고의 평가를 받았습니다.

MITRE ATT&CK 평가에서 인정받은 사이버리즌 EDR 솔루션이 궁금하시다면 APAC 파트너사인 두산디지털이노베이션으로 문의 부탁드립니다.

두산디지털이노베이션에 문의하기
✉ ddi.marketing@doosan.com

DOOSAN 두산디지털이노베이션