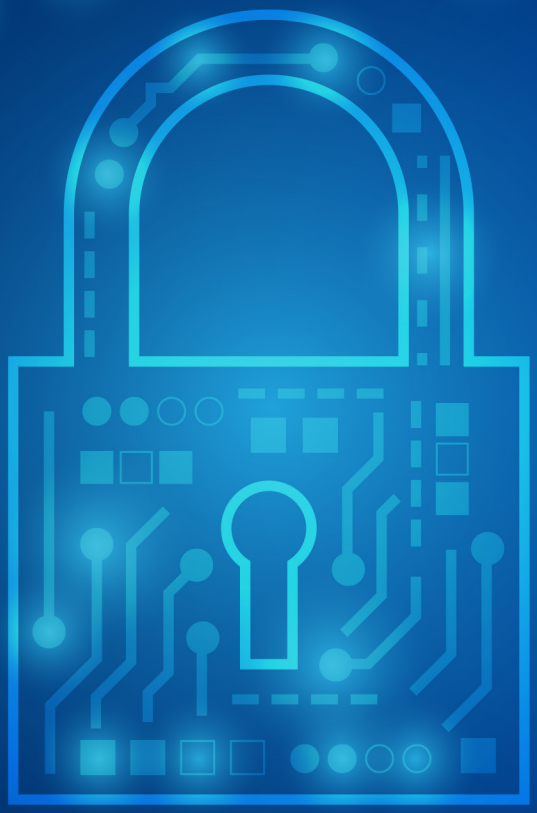
SECURITY INSIGHT

DOOSAN



완벽한 사이버 보안을 위해

보안 담당자가 체크해야 할 5가지 요소

사이버리즌(Cybereason),
마이터 어택(MITRE ATT&CK)
평가에서 최고 등급 달성

C Y B E R
S E C U R I T Y

완벽한 사이버 보안을 위해 보안 담당자가 체크해야 할 5가지 요소

사이버리즌(Cybereason), 마이터 어택(MITRE ATT&CK) 평가에서 최고 등급 달성

원문 출처 : 사이버리즌 웹사이트

사이버 보안 공격은 준비가 덜 된 환경에 효과적으로 침투해 공격합니다. 아직도 많은 기업이 보안 사고가 발생하고 나서야 보안에 대한 투자를 고려합니다. 하지만 우리 일상 생활에서도 집이나 회사를 지키기 위해 미리 자물쇠를 채우고, 보안에 신경을 쓰듯 사이버 보안도 미리미리 준비하고 투자해야 합니다. 공격당하고 나면 복구와 보완에 엄청난 시간과 비용이 들기 때문입니다.

기업 보안 담당자가 사이버 보안을 위해 꼭 알고 있어야 할 5가지 요소에 대해 알아봅니다. 또한 이 5가지 요소에 대한 국제 기구 마이터 어택(MITRE ATT&CK) 평가에 대해 알아보며, 이 평가에서 우수한 등급을 받은 솔루션은 무엇이 있는지 알 수 있습니다.

[목차]

1 사이버 보안 평가에 고려해야 할 5가지

- 위협 요소 사전 차단을 위한 방어 (Protection)
- 보안 위협이 발견되지 않도록 사전 탐지 (Detection)
- 실시간 탐지로 빠른 응답을 제공 (Real-Time Detection)
- 사이버 공격의 맥락 파악을 위한 가시성 (Visibility)
- 보안 프레임워크에 대응 가능한 분석 범위 (Analytic)

2 대표적인 사이버 보안 성능 평가, 마이터 어택(MITRE ATT&CK)

3 MITRE ATT&CK 평가에서 가장 우수한 등급을 받은 솔루션, 사이버리즌

4 사이버리즌 및 두산디지털이노베이션 소개

1

사이버 보안 평가에 고려해야 할 5가지

많은 기업이 사이버 보안에 솔루션을 도입하고, 자체적인 시스템을 구축하는 등 다방면 노력하고 있습니다. 여러가지 요인에 대해 고려하지만 반드시 생각해봐야 할 5가지는 아래와 같습니다.

① 보안 위협 요소를 사전에 차단하는, **방어(Protection) 역량**

초기에 차단 및 방어할 수 있는 위협이 많을수록 사후 조사 및 대응이 줄어들 수 있습니다. 때문에 우리 조직의 사이버 보안 방어 역량에 대해 평가하고, 이를 높일 수 있는 방안을 마련해야 합니다.

② 보안 위협이 발견되지 않도록 사전에 **탐지(Detection)하는 기능**

사이버 보안 위협 탐지는 기업의 IT 환경을 주시하고 있다가 시스템을 손상시킬 수 있는 악의적인 활동을 식별하는 것을 말합니다. 위협이 감지되면 즉각 담당자에게 전달되어야 하고, 시스템의 취약점을 악용하기 전에 위협을 무력화하기 위한 대응이 필요합니다.

③ 사람의 개입 없이 **실시간으로 위협 탐지(Real-Time Detection) 기술**

위협 탐지에서 가장 중요한 요인은 탐지 시간 및 대응 속도입니다. 몇몇 사이버 보안 솔루션 벤더들은 AI 또는 머신러닝 기술을 활용해 실시간으로 악의적인 공격을 탐지하고 즉각적인 가시성을 제공하고 있습니다. 특히 랜섬웨어의 경우, 시간과의 싸움이기 때문에 실시간으로 위협을 탐지하고 대응하는 기술이 매우 중요합니다.

④ 사이버 공격의 전체 맥락을 파악할 수 있는 **가시성(Visibility) 확보**

사이버 보안 전략 중 가시성은 매우 중요한 요소입니다. 많은 기업이 철저한 보안 정책, 거버넌스, 컴플라이언스 및 대응 방안을 수립하고 있지만 이를 가시적으로 구축하고 관리하는 기업은 많지 않습니다. 특히 많은 기업들이 팬데믹 이후 재택근무를 하게 되면서 보안에 대해 가시성을 확보하는게 더욱 중요해졌습니다. 업무 시간에 누가 어떤 데이터에 어떻게 접근하는지 알아야 합니다.

⑤ 보안 프레임워크에 대응 가능한 **분석(Analytic) 범위**

분석은 사이버 위협을 더 잘 이해하기 위해 구체적인 정보 및 컨텍스트를 제공하는 것을 말합니다. 분석 적용 범위 평가는 공격과 관련해 풍부한 컨텍스트를 제공하는 것이 좋으며, 예로 MITRE 프레임워크에 대응 및 주요 ATT&CK 기술에 탐지되는 능력을 말합니다. 이런 분석에 넓은 커버리지를 가지고 있는 솔루션 또는 벤더는 사이버 공격에 대한 더 큰 통찰력을 제공한다고 볼 수 있습니다.

2
대표적인 사이버 보안 평가, 마이터 어택(MITRE ATT&CK)

(이미지 출처 : MITRE 웹사이트)

마이터(MITRE)는 미국의 사이버 보안 비영리 단체이며 항공, 의료, 국토 안보 등 다분야에 걸쳐 미국 정부 기관을 지원하는 단체입니다. 마이터(MITRE)의 어택(ATT&CK) 평가는 정부 기관, 대기업 및 각종 사회 분야에서 발생하는 악의적인 공격 행위를 분류한 프레임워크로, 보안 기업 및 전문가들은 ATT&CK를 토대로 실제 발생하는 악의적인 공격, 악의적인 공격의 징후를 추적, 탐지하고 예방조치를 실시하는 필수적인 요소로 활용하고 있습니다.

마이터 어택(MITRE ATT&CK) 엔터프라이즈 평가는 보안 업계에서 활용하는 가장 대표적인 공정하고 투명한 평가며, 많은 회사들이 이 평가를 통해 자신들의 보안 솔루션의 탐지 능력을 입증하는데 활용하고 있습니다.
2022년 평가에서 가장 우수한 결과를 나타낸 벤더는 사이버리즌(Cybereason)으로 사이버 보안평가에 고려해야 할 5가지 사이버 보안 역량을 기준으로 대부분이 100%에 달하는 점수를 나타냈습니다.

3
MITRE ATT&CK 평가에서 가장 우수한 등급을 받은 솔루션, 사이버리즌

(이미지 출처 : 사이버리즌 웹사이트)

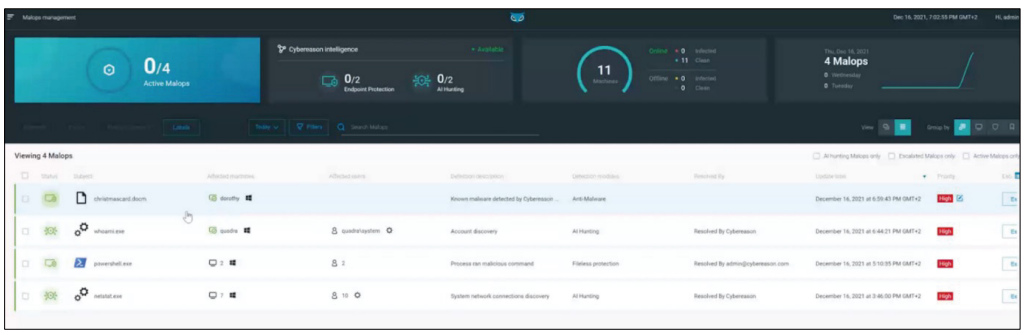
2022년 사이버리즌의 보안 솔루션은 가장 우수한 결과를 얻었습니다.

올해 평가에는 30개 벤더가 참가했으며, 악명 높은 2가지 랜섬웨어(Wizard Spider, Sandworm)를 대상으로 실제 시뮬레이션 했습니다.
30개 벤더 솔루션 중 사이버리즌은 가장 높은 수준의 방어력을 나타냈습니다. 이 말은 기업 고객이 사이버리즌을 활용하는 경우, 랜섬웨어나 보안 위협으로부터 회사 자산을 안전하게 지킬 수 있다는 것을 의미합니다.

아래에서 각 5개의 평가 항목에 대해 자세히 알아보실 수 있습니다.

● 100% 보호 : 위협 요소를 사전에 차단

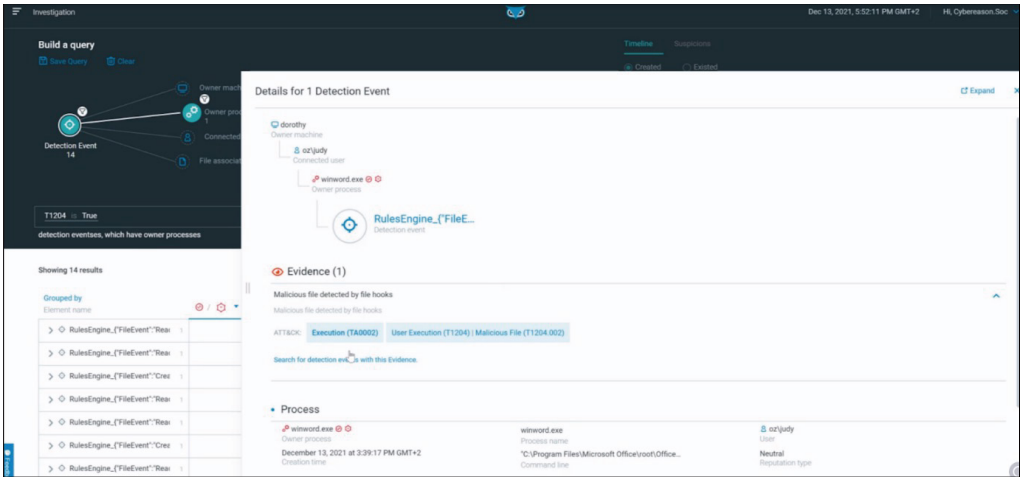
사이버리즌은 모든 벤더 솔루션 중 가장 높은 예방 효과를 보였습니다.
보안 예방 평가(Prevention Test)는 데이터가 손상되기 전 보안 위협 요인이 실행되지 않도록 하는 솔루션의 능력을 말합니다. 만약 공격을 조기에 발견해 사전에 보호한다면 보안팀이 분류해야 하는 경고 수가 크게 줄어들고, 이는 팀의 효율 향상으로 이어질 수 있습니다.
사이버리즌은 이 부분에서 100%를 달성한 유일한 벤더로 모든 사이버 공격이 발생하기 전에 방지할 수 있습니다.



사이버리즌 솔루션에서 악성코드 트로이목마 중 하나인 이모텟(Emotet)을 방지한 화면

● 100% 탐지 : 위협이 발견되지 않도록 보장

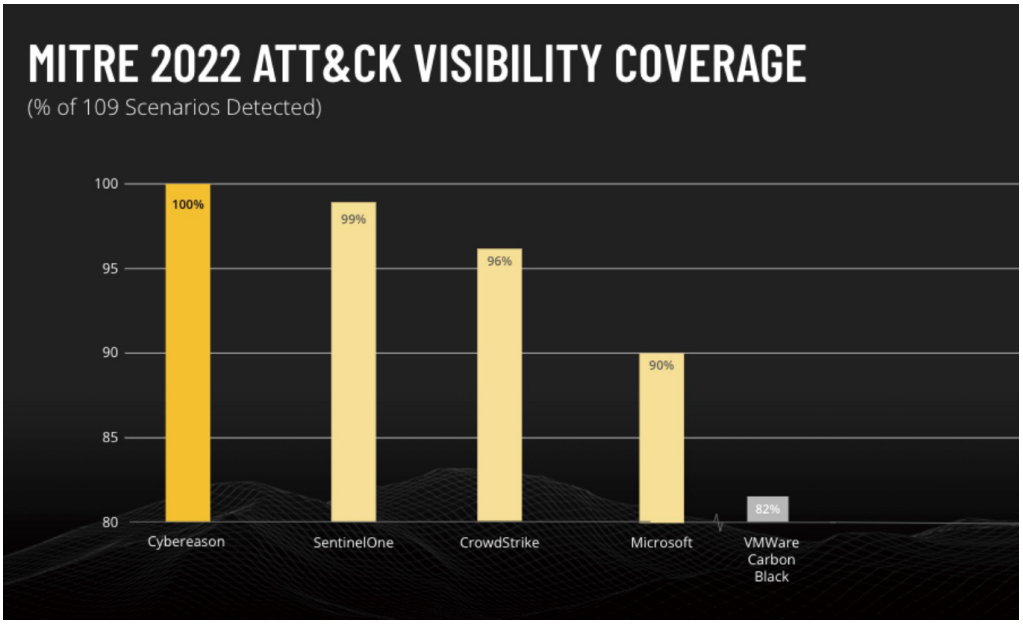
사이버리즌의 솔루션은 모든 공격 단계를 완벽하게 감지해냈습니다.
악의적인 공격은 여러 하위 단계로 나눠질 수 있고 대부분 자동으로 혹은 수동으로도 이루어집니다. 이 평가에서는 악의적인 랜섬웨어인 Wizard Spider와 Sandworm이 사용하는 19개의 공격 행동을 담았고, 이를 탐지해낼 수 있는지 평가했습니다.
사이버리즌의 솔루션은 이 19개의 공격 행동을 모두 탐지했습니다.



사이버리즌의 악성 파일 실행 감지 화면

● 100% 가시성 : 사이버 공격의 전체 맥락 파악

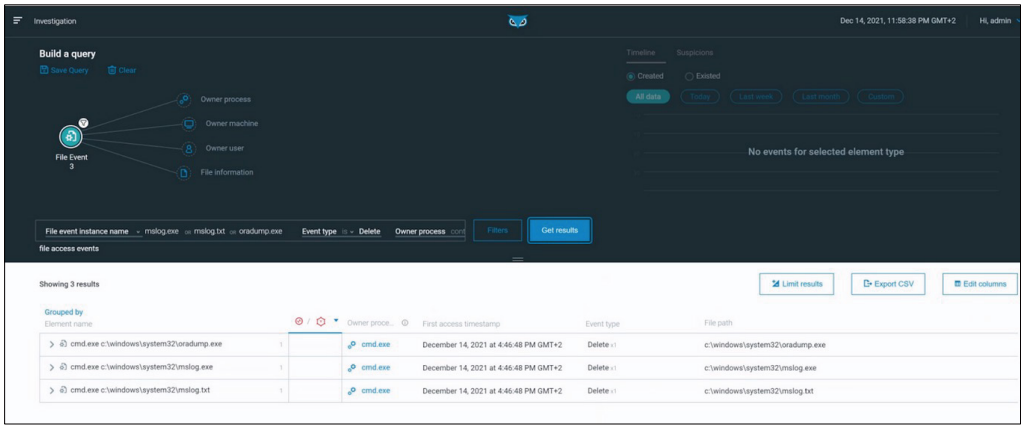
Cybereason은 벤더 중 유일하게 모든 운영 체제에서 사이버 공격에 대한 100% 가시성을 제공합니다. 공격의 전체 맥락을 파악하면 공격 발생 위치, 영향, 타임라인 등 세부 정보를 파악할 수 있게 됩니다. 사이버리즌의 MalOp Detection Engine은 완벽한 가시성 점수를 보여준 유일한 솔루션입니다. 보안 담당자는 더 이상 경고를 추적하느라 시간을 소비하지 않아도 되며, 악의적인 작업을 발견 즉시 중지할 수 있어 효율적인 보안 운영이 가능합니다.



사이버리즌이 타 솔루션들보다 우월하게 높은 점수를 받은 100% 가시성

● 100% 실시간 탐지 : 사람의 개입이 필요 없는 감지 능력

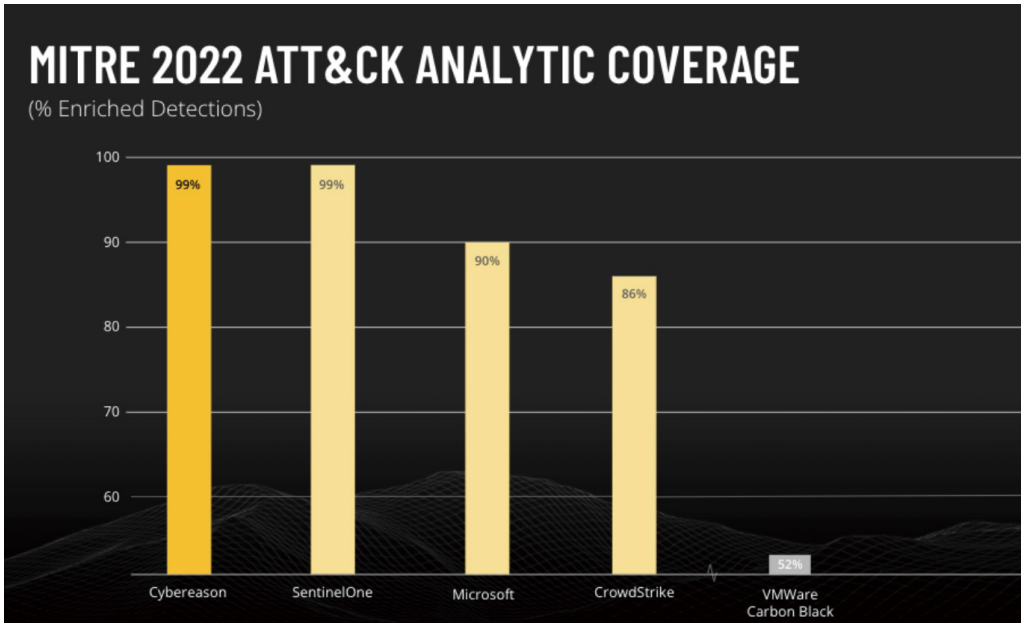
사이버리즌은 제로(ZERO) 지연 감지를 제공합니다.
제로 지연 감지가 중요한 이유는 날로 정교해지는 위협, 특히 랜섬웨어와 같은 위협에 대해 처리 시간이나 분석가의 개입을 기다리지 않고 즉시 악성 활동을 탐지할 수 있어야 하기 때문입니다.
다른 벤더의 솔루션의 경우 중요한 이벤트에 대한 데이터를 필터링 한 반면, 사이버리즌의 솔루션은 모든 관련 데이터를 실시간으로 탐지합니다. 특히 인공지능과 머신러닝을 활용해 포괄적인 뷰(View)를 구축해 위협이 발생하는 즉시 실시간으로 위협을 감지하도록 합니다.



사이버리즌 솔루션, 실시간으로 삭제되는 파일을 감지하는 화면

● 99% 분석 커버리지 : 마이터 어택(MITRE ATT&CK) 프레임워크에 가장 완전하게 맵핑

사이버리즌은 모든 경쟁 솔루션에서 가장 높은 품질의 분석 커버리지를 제공했습니다. 이 평가 영역에서 우수한 성능을 보여준 솔루션은 마이터 어택(MITRE ATT&CK) 프레임워크에도 효과적으로 맞출 수 있습니다. 방대한 양의 데이터를 상호 연결해 위협을 예측하고, 이해하며, 해결합니다.



4
사이버리즌(Cybereason), 두산 디지털이노베이션 소개

사이버리즌은 2012년 이스라엘 군 첩보부대 (Unit 8200)출신의 군인 Lior Div가 설립한 사이버 보안 기술 회사입니다. 미국 메사추세츠주 보스턴에 본사를 두고 있으며, 이스라엘 텔아비브, 일본 도쿄, 영국 런던, 호주 시드니에 지사가 있습니다.

– 창업 연도 : 2012
– 위치 : 매사추세츠주 보스턴
– 창업자 : 리오르 디브(Lior Div), 요나단 아밋(Yonatan Amit), 요시 나르(Yossi Naar)
– 최종 투자 이력 : 시르지F (누적 투자액 : 6억 6360만 달러)
– 공식 웹사이트 : www.cybereason.com

㈜두산 디지털이노베이션은 사이버리즌의 APAC 및 한국 파트너사로 △엔드포인트탐지대응(EDR) △매니지드탐지대응(MDR) △차세대안티바이러스(NGAV) △랜섬웨어와 파일리스 악성코드 방지 등 통합 보안 솔루션을 두산 그룹 및 대외 고객에게 제공하고 있습니다.

- ㈜두산 디지털이노베이션의 보안 오퍼링 (바로가기)
- 문의하기 (바로가기)

사이버 보안, 두산 디지털이노베이션에 물어보세요!
보안을 가장 잘 아는 전문가가 친절하게 설명해드립니다.
https://www.doosandigitalinnovation.com/kr/support/contact-us

두산디지털이노베이션의 채널을 팔로우하세요! 새로운 소식과 유익한 정보를 전해드립니다.