MITRE ATT&CK 평가

업계 최고의 성능을 보여주는 IBM Security ReaQta

하이라이트

보안 팀에서 사이버 공격을 메뉴얼로 분석할 필요 없이 비즈니스 연속성을 유지합니다

필요한 위협 경고를 최소한으로 생성하여 경고 피로를 줄이고 사이버 보안을 간결화합니다

엔드포인트에 대한 완벽한 가시성을 확보하여 모든 단계에서 신속하게 응답할 수 있도록 합니다

보고서 정보

IBM ReaQta에서 MITRE ATT&CK 평가를 성공적으로 완료했습니다. 이 보고서는[1] ReaQta가 가장 뛰어난 품질의 경고를 생성하면서 작업자의 개입 없이 가상으로 정교한 공격을 완벽하게 다루는 모습을 보여줍니다.

MITRE ATT&CK 평가란 무엇인가?

MITRE ATT&CK는 사이버 공격 중 발생하는 일련의 단계를 정의하고 위협을 감지하는 능력에 대한 솔루션을 평가합니다. 나열된 각 단계는 킬 체인에 따른 “전술”을 나타냅니다.

- 초기 액세스
- 실행
- 지속성
- 권한 에스컬레이션
- 방어 회피
- 권한 정보 액세스
- 감지
- 측면 이동
- 콜렉션
- 유출
- 명령 및 제어

REAQTA
an IBM Company

IBM

MITRE의 평가 방법

본 평가는 각 솔루션에 점수를 매기거나 등급을 결정하지 않고, 기업의 특정 보안 문제를 해결하는 데 가장 적합한 솔루션이 무엇인지 확인할 수 있도록 합니다. 평가 대상들의 평가는 별도의 독립된 환경에서 이루어지고 제한 사항이 있으며, 솔루션의 특정 기능이 연구실 인프라에서 지원되지 않아 비활성화 되는 경우도 있습니다. 예를 들어 ReaQta NanoOS에서는 높은 수준의 악성 동작을 감지하는데 사용되는 라이브 하이퍼바이저를 사용할 수 없지만, 그럼에도 불구하고, ReaQta 플랫폼은 작업을 잘 수행합니다.

MITRE에는 일련의 식별된 기술이 있으며 각 기술은 평가를 진행하기 위해 선택된 위협 행위자를 기반으로 한 전술 그룹에 소속됩니다. MITRE는 이번 평가를 위해 APT29를 선택했습니다.

손상

콜렉션 및 회피

탐색

액세스 확장

유출

정리

보안 팀에서 사이버 공격을 메뉴얼로 분석할 필요 없이 비즈니스 연속성을 유지합니다

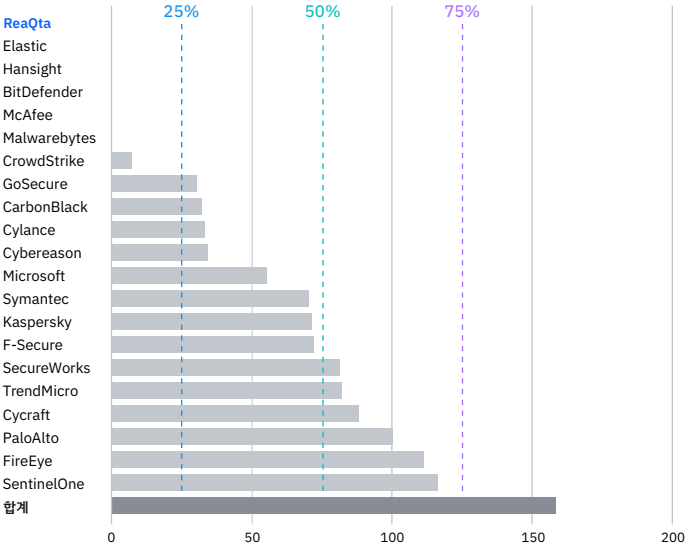
ReaQta는 관리형 보안 서비스 제공자(MSSP) 없이, 즉 공격 중에는 사람의 개입 없이 참여하기로 결정했습니다. MITRE는 기술 평가 프레임워크이며 사람(작업자)을 루프에 도입하는 것은 옳지 않다고 보았습니다. 왜냐하면 MSSP 감지는 평가를 크게 왜곡시켰습니다.

MSSP 접근 방식은 ReaQta 고객들에게 공정한 기술 평가를 제공하지 않았기에. MITRE는 이러한 피드백들을 적극적으로 받아들였으며, 라운드 3 평가를 시작으로 모든 회사는 사람(작업자) 없이 평가될 것입니다.

고객들은 MSSP와 독립형 배포 중에서 자유롭게 선택할 수 있어야 합니다.

아래 그래프에 표시된 대로 사람(작업자)이 수행한 감지 횟수는 생성된 감지에 큰 영향을 미쳤습니다. 몇 가지 사례에서 감지의 50% 이상(최대 73%)이 메뉴얼로 생성되었습니다. 본 평가에서 사람(작업자) 없이 참여하기로 한 벤더는 6개 회사뿐이었습니다.

MSSP 감지(메뉴얼로 생성됨)



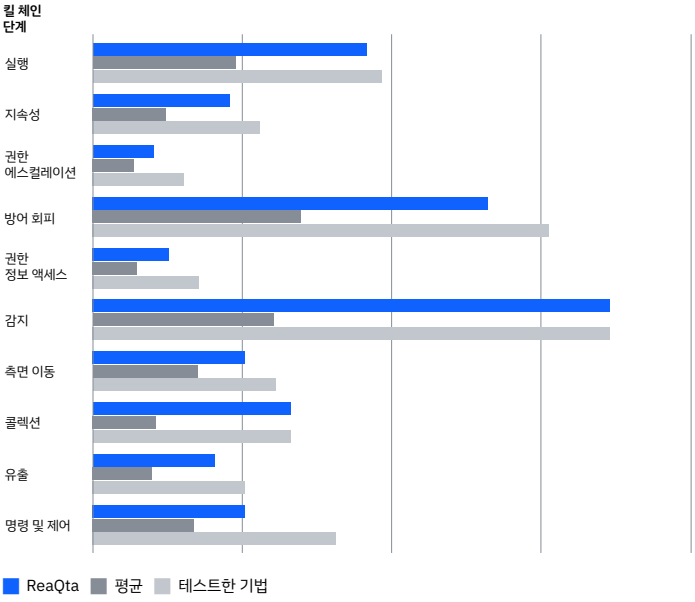
각 벤더가 생성한 메뉴얼 감지

MITRE 평가
라운드 2—APT29

벤더들은 눈에 잘 띄지 않는 접근 방식으로 잘 알려진 정교한 국가 규모의 상대 APT29(The Dukes, Cozy Bear 및 CozyDuke라고도 함)에서 사용하는 전술과 기법을 감지하는 능력에 대한 테스트를 받았습니다. APT29는 다음과 같이 주목할 만한 공격의 배후로도 유명합니다. (2015년 미국 국방부, 2016년 미국 민주당 전국위원회, 2017년 노르웨이 및 네덜란드 정부)

이전 라운드에서의 변화가 중요했습니다. APT3(라운드 1)는 잡음이 많은 위협 행위자이며 다양한 툴을 사용하지만 로우 프로파일을 유지하는 데 훨씬 덜 신경을 씁니다. 반면 APT29는 매우 은밀하게 작동하며 프로파일이 매우 낮고 LOLBins와 파일이 없는 맬웨어에 크게 의존합니다.

기법 감지 범위(자동화됨)



평균과 비교한 ReaQta 자동 감지 범위

ReaQta 평가 결과

공격은, 공격자가 초기 액세스 권한을 획득한 후 이틀에 걸쳐 점차 네트워크에 깊숙히 침투하는 방식으로 진행되었습니다. 대부분의 작업은 낮은 감지 프로파일을 유지하기 위해 사용자 정의 도구 및 멀웨어와 달리, Microsoft PowerShell을 사용하여 수행되었습니다. 이 평가의 목표는 테스트한 솔루션이 공격에 어떻게 대응하고 전체 킬 체인에 따라 어떤 종류의 가시성이 제공되는지를 보여주는 것입니다.

평가 결과 요약에서 알 수 있듯이, ReaQta는 전체 킬 체인에 걸쳐 완벽한 가시성을 제공합니다. ReaQta는 테스트한 전술과 기법의 90%를 감지하여 모든 공격 단계에서 위협에 대응하고 개선하는 능력을 입증했습니다.

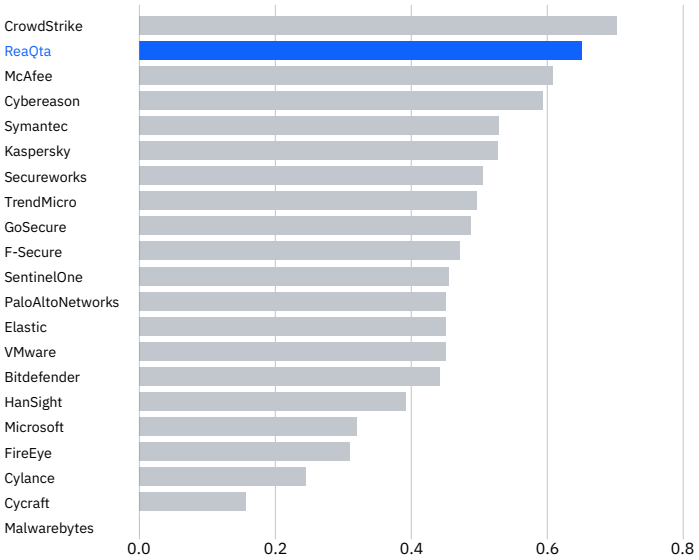
ReaQta는 MSSP의 메뉴얼 감지에 의존하는 벤더와 비교할 때도 세계 최고 수준의 조치 가능성을 보여줍니다.

필요한 위협 경고를 최소한으로 생성하여 경고 피로를 줄이고 사이버 보안을 간결화합니다

그 플랫폼은 실행, 지속성, 권한 에스컬레이션 및 방어 회피 단계에서 바로 경고를 감지하고 생성하므로, 보안 팀이 APT29와 해당 동작을 추적할 수 있습니다. 플랫폼 경고는 측면 이동, 콜렉션, 유출, 명령 및 제어 등 이후 킬 체인 단계에서 일관되게 발생하여 사이버 공격의 후반 단계에서도 ReaQta가 피해에 대응하고 이를 제한할 수 있는 능력을 보여줍니다.

조치 가능성 비율은 생성되는 경고 수를 줄임으로써 잡음을 감소시키는 플랫폼의 기능을 강조했습니다. 이 플랫폼은 전술과 기법당 하나의 경고와 비교하여 몇 가지 상관관계가 있는 경고에서 모든 전술과 기술을 캡처했는데, 이는 SOC 팀이 검사하고 대응해야 하는 관리할 수 없는 경고 수에 해당합니다.

경고 조치 가능성

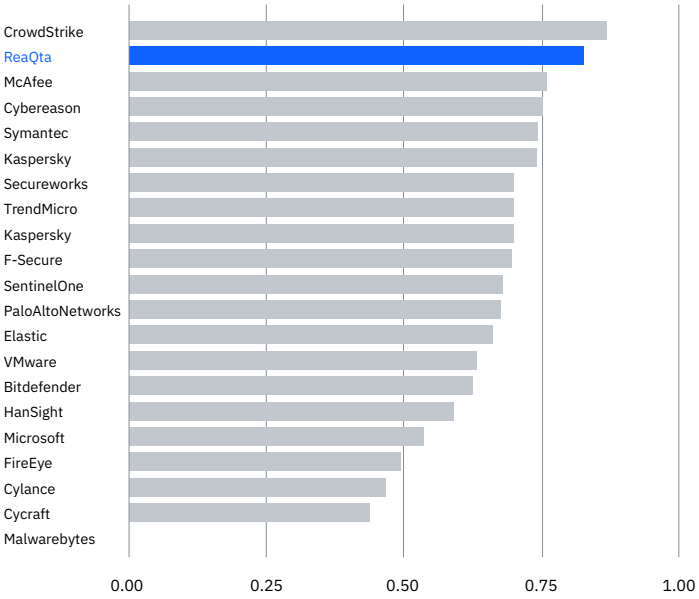


조치 가능성 비율(데이터에는 MSSP에 의존하는 벤더의 메뉴얼 감지 포함)

다시 한번, ReaQta는 작업자의 개입 없이 고품질 경고를 제공하는 반면 첫 번째와 세 번째 벤더는 모두 평가 중에 메뉴얼 분석에 의존했습니다.

ReaQta에서 제공하는 가시성 규모로 인해 데이터를 필터링하고 상관분석을 지정하며 각각 가장 많은 양의 관련 정보를 포함하는 가능한 가장 작은 수의 경고를 생성해야 합니다. ReaQta AI 엔진의 목적은 다음과 같습니다. 원격 측정 수집, 상관분석, 요약, 경고 퀄리티는 아래 차트에 있는 Forrester의 분석으로도 확인됩니다.

경고 퀄리티



경고 퀄리티(데이터에는 MSSP에 의존하는 벤더의 메뉴얼 감지 포함)

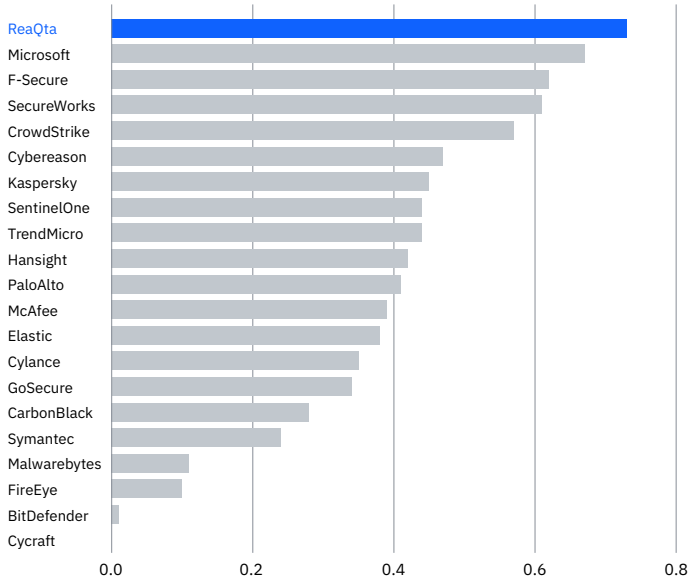
"조치 가능성은 경고 효율성과 경고 쿼리티의 결과이며 경고 효율성 (너무 많지 않음)과 경고 쿼리티(스토리를 이해하는 데 얼마나 도움이 되는지)는 모두 특정 경고가 얼마나 '조치 가능'한지 이해하는 데 관련되어 중요한 역할을 합니다."

Forrester [2]

높은 충실도의 포괄적인 경고를 제공하는 것은 좋은 플랫폼을 단순한 잡음 생성기와 구별하는 기준입니다.

아래 그래프는 메뉴얼 감지가 제거되었을 때 다른 솔루션과 비교하여 ReaQta가 작동하는 방식을 보여줍니다. 각 막대는 생성된 각각의 경고에서 캡처된 인시던트 관련 정보량을 나타냅니다. ReaQta의 엔진은 가장 많은 양의 정보를 캡처하여 실제 환경에서 상당한 양의 워크로드를 줄였습니다.

생성된 경고당 공격 범위(신호 대 잡음 비율)



경고당 제공되는 공격 범위의 백분율

ReaQta는 테스트한 기법당 하나씩 158개의 경고를 생성하는 대신, 25개의 경고만 생성하고 각 경고 내에 공격자를 추적하는 데 필요한 모든 정보를 올바르게 수집했습니다.

통합된 인시던트 해결 워크플로우를 제공하는 기능은 경고 피로를 줄이는 데 매우 중요합니다.

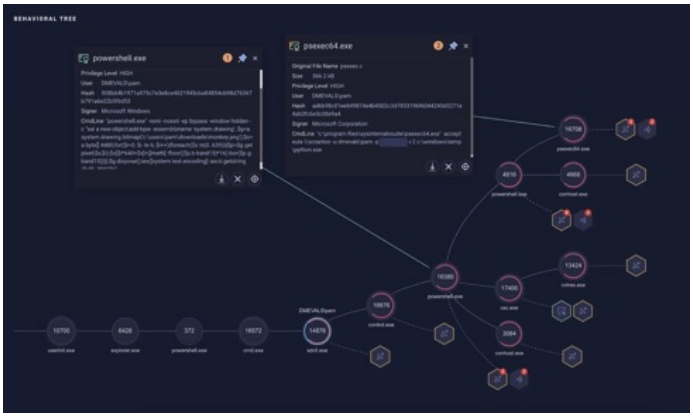
ReaQta는 MITRE 평가 도중 스토리라인을 상관분석합니다. 이를 통해 분석가는 원래 인시던트와의 직접적인 상관분석 없이 생성되는 수백 개의 경고에 주의를 분산시키지 않고도 활성 공격자를 쉽게 이해하고 연구할 수 있습니다. 이는 실제 분석 중에 처리하기 훨씬 더 어려웠을 것입니다.

ReaQta 접근 방식은 전체 공격에 걸쳐 완벽한 가시성을 유지하면서 경고 피로도를 85% 줄였습니다. ReaQta는 인시던트당 최소 경고 수를 생성하도록 특별히 설계되어 원활하고 중단 없는 분석 경험이 가능합니다. 단일 뷰에서 모든 것을 유지할 수 있는 기능은 분석가가 이벤트를 완벽하게 이해하기 위해 다른 화면 뷰로 이동할 필요 없이 더 빠르게 응답할 수 있도록 도와줍니다.

엔드포인트에 대한 완벽한 가시성을 확보하여 모든 단계에서 신속하게 응답할 수 있도록 합니다

플랫폼은 ATT&CK 킬 체인의 모든 단계에서 조치 간 상관분석을 유지할 수 있습니다. 자동으로 이벤트 상관분석을 지정하면 공격자가 실행하는 다양한 조치를 하나로 모으는 데 필요한 시간이 줄어들고 궁극적으로는 실제 공격 시 대응하는 시간을 줄일 수 있습니다.

작동 트리



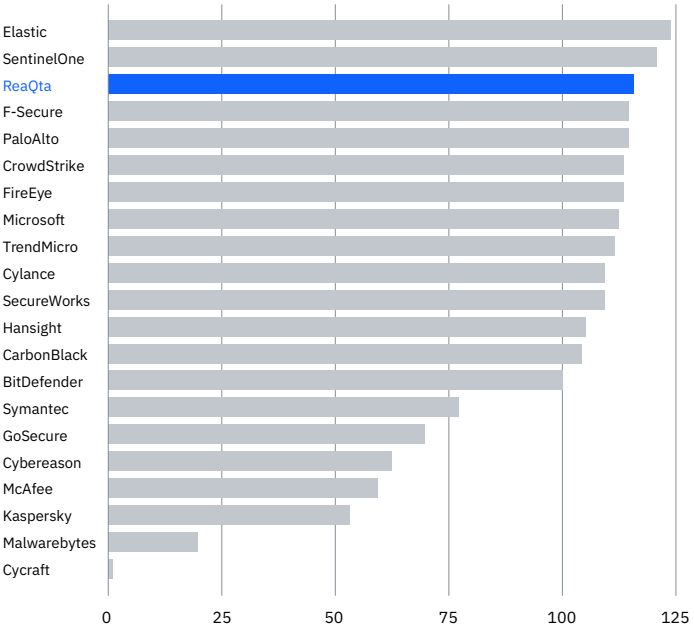
MITRE 평가 도중 ReaQta에서 스토리라인 상관분석

평가와 관련된 예를 제공하기 위해 위 그래프는 단일 경고 내에서 공격의 전체 단계를 캡처한 방법을 보여줍니다. ReaQta는 모든 정보를 쉽게 이해할 수 있는 스토리라인으로 상관분석하여 SOC 팀에게 적시에 분류할 수 있도록 모든 정보를 제공했습니다. 작업자의 개입이 필요하지 않았으며 공격이 명확하게 설명되었고, 메뉴얼 작업 없이도 위험이 평가되었습니다.

APT29 전술과 기법 감지를 자세히 살펴보면 ReaQta에서 킬 체인의 초기 단계부터 감지하기 어려운 더 정교한 단계까지의 가시성을 제공한 것을 알 수 있습니다. 여기서 주목할 점은 플랫폼이 모든 단계에서 위협을 균일하게 감지하여 각 단계마다 대응 및 수정의 기회를 제공한 능력입니다.

ReaQta는 정보를 축약하고 위험을 평가하는 인상적인 AI 엔진과 결합된 최고의 원격 측정 방법 중 하나임을 보여주었습니다. 지속적으로 경고를 관리하는 대신 위협 차단에 시간을 할애하려는 모든 SOC나 팀에게 강력한 툴이 될 것입니다.

ReaQta에서 최고의 원격 측정 중 하나를 보여주었습니다.



ReaQta에서 제공한 원격 측정량

결론

ReaQta의 AI 기반 플랫폼은 보안 팀에게 고급 감지 및 신속 대응 기능을 제공하여 작업자의 개입을 최소화하고 전체 사이버 보안 프로세스를 단순화함으로써 규모에 관계없이 조직의 비즈니스 연속성을 촉진합니다.

이 평가는 정교한 위협 행위자를 감지하는 ReaQta의 접근 방식을 검증했습니다. ReaQta는 앞으로도 독립적인 써드파티 테스트에 계속 참여할 것입니다.

ReaQta는 기업들이 이러한 평가 결과를 기반으로 결정을 내릴 수 있도록 도와주는 MITRE 노력에 감사하고 있습니다.

자세한 정보는 다음을 참조하세요.
ibm.com/products/reaqta

IBM Corporation
(07326) 서울특별시 영등포구 국제금융로 10
서울국제금융센터(3IFC)

미국에서 생산됨
2022년 3월

1 MITRE ATT&CK evaluation, The MITRE Corporation and MITRE Engenuity, 2020.
2 Further Down the Rabbit Hole With MITRE’s ATT&CK Eval Data, Forrester blog, 4 May 2020.