< Security Consumer Report>

- EDR(Endpoint Detection & Response) 솔루션

2019. 2.

(사)한국침해사고대응팀협의회

(사)한국CPO포럼

본 "Security Consumer Report - EDR 솔루션" 은 한국침해사고대응팀협의회 (CONCERT : CONsortium of CERT) 회원과 한국CPO포럼 회원으로 활동하는 보안 담당자를 중심으로 EDR 솔루션을 이미 도입해서 운용 중이거나 도입예정인 보안 담당자들이 자발적으로 보고서 위원회를 구성한 후 국내에서 출시된 EDR 솔루션 제품들을 조사한 것으로, 보고서 편집위원들의 경험과 필요를 살려 EDR 솔루션을 도입하기 원하는 기업을 위해 EDR 솔루션이 갖추어야 할 필요사항 및 도입 시 유의사항을 정리한 것입니다.

본 "Security Consumer Report - EDR"은 EDR 솔루션에 대한 종합적인 비교분석 보고서이자 UTM, DLP, APT대응 솔루션에 이은 CONCERT에서 작성한 네 번째 Security Consumer Report입니다. 테스트베드를 통한 EDR 솔루션에 대한 성능평가 등 정량적인 평가를 담지 못해 아쉬운 점이 있지만, 추후 계속적인 업데이트 과정을 거쳐 사용자에게 실질적으로 도움이 되는 Security Consumer Report가 될 것입니다.

위원회 구성

< CONCERT Security Consumer Report - EDR 솔루션 >

- 강우준 매니저(포스코ICT)
- 김후언 과장(S-Oil)
- 배기웅 차장(한국암웨이)
- 윤경준 차장(KCB)
- 최재규 차장(kt)
- 편승철 차장(에스원)
- 허원석 과장(푸르덴셜생명)
- 홍보성 팀장(CDNetworks)

이름 가나다순

CONCERT에서는 기업·기관 보안 담당자를 위해 정기적으로 사용자 관점의 정보보호 솔루션 및 서비스 분석 보고서 <Security Consumer Report>를 제작 하고 있습니다. 향후 보고서 제작에 참여를 원하는 회원은 사무국으로 연락(02-3474-2490~1, info@concert.or.kr) 주시기 바랍니다.

<본 보고서에 대한 오류 및 개선 의견이 있을 경우 사무국으로 연락 주시기 바랍니다.>

< 목 차 >

Part Ⅰ. Security Consumer Report 개요

1 . Security Consumer Report-EDR 솔루션 제작배경

O 본 보고서는 한국침해사고대응팀협의회(CONCERT)의 회원과 한국 CPO 포럼 회원을 주축으로 구성된 위원회 활동을 통해 제작되었다.

O 엔드포인트에 대한 보안은 AntiVirus(AV)면 충분하다고 여겨진 때가 있었다. 하지만 AV 는 시그니처, 패턴 기반의 사후처리 방식으로 동작하기 때문에 패턴 업데이트 속도가 변종 악성코드의 등장속도를 못따라가고 있고 신종 악성코드에 의한 위협은 상존하고 있다. 악성코드가 실제 동작하고 활동하는 거점이 되고, 공격대상이기도 한 엔드포인트에 대한 보호를 강화하고 엔드포인트 전반에 대한 위협 가시성을 높여주는 솔루션인 EDR(Endpoint Detection & Response)이 등장했다.

O 정보보호 기업들이 EDR 솔루션을 표방한 제품을 출시하고 시장 활성화를 촉진하고 있지만, EDR 이 알려지지 않은 모든 공격을 차단할 수 있는 것처럼 포장되고 있다. EDR 은 침해를 탐지하고 대응해 보안조직과 침해사고 대응 업무를 지원하는 역할을 한다. EDR 은 엔드포인트와 지능형 공격에 대한 특화된 전문성을 갖고 있어야 하는 솔루션인데 실제 시장에 출시된 솔루션들을 보면 과연 제대로 된 EDR 인지, 기존의 솔루션에 EDR 적인 요소만 살짝 추가한 것인지 알기 어렵다.

O 이에 CONCERT 에서는 EDR 솔루션이라면 갖추어야 할 기능들을 살펴보고, 시장에서 유통되고 있는 EDR 솔루션들을 대상으로 주요 기능 및 평가 영역과 평가 세부 항목을 도출하고 비교 분석하는 Consumer Report(CR)보고서 제작을 추진하게 되었다.

2 . CR-EDR 제작 목적

O CR-EDR 는 EDR 솔루션의 도입을 검토 또는 이미 도입한 기업을 위해 솔루션에 대한 사용자 입장에서의 비교 기준 및 분석자료를 제시하고, EDR 솔루션 활용 방법에 대한 참고자료를 제공하는데 그 목적이 있다.

O CR-EDR 의 목차 역시 이를 충족하기 위한 항목으로 구성되었다.

1) 솔루션의 주요 기능을 선정하고 판단하는 기준 제시

2) EDR 솔루션을 도입하고자 하는 기업 또는 보안 담당자를 위한 솔루션 별 검토자료

3) EDR 솔루션의 적절한 활용을 위한 도입 전·후 유의 사항

3 . CR-EDR 제작의 객관성 확보

O CR-EDR 제작위원회 전체회의에서 EDR 솔루션의 정의에 따른 필수 기능 및 평가 항목과 평가방법을 공동으로 선정하고 이를 조사 및 평가수행에 활용했다.

O 벤더의 1 차 답변을 기초로, 솔루션 별로 답변을 검토하고 벤더와의 추가 인터뷰를 통해 확인한 내용을 전체회의에서 재 공유해 전체 제작위원의 동의를 얻는 등 객관성 확보가 가능한 방법으로 평가를 진행했다.

O CR-EDR 에서는 솔루션의 기능과 성능을 검증하기 위한 BMT 또는 PoC 는 생략했다. BMT 나 PoC 를 진행하는 데 있어 동일한 환경구축, 특정 솔루션에 편향되지 않은 샘플데이터 확보 등 공정한 테스트 환경을 구축하기 어렵다는 점을 반영했다.

4. CR-EDR 제작 절차

O CR-EDR 제작은 3 단계에 걸쳐 제작되었다.

1) 사전 조사 : CR 위원회 구성 → EDR 솔루션의 정의 및 EDR 솔루션의 범위 조사 → 솔루션 특징 및 기능 분석 → 보고서 구성 및 조사 항목 선정 → EDR 의 정의에 따른 CR 대상 솔루션 (벤더) 선정

2) 진행 : 벤더 참여 요청 → 조사 항목 제공 및 1 차 답변 요청 → 자료 검토 → 조사 항목 추가 질의 및 2 차 답변 요청

3) 검토 및 작성 : 자료 취합 → 최종 검토 → 보고서 작성

5. CR-EDR 솔루션 대상 선정

O EDR 솔루션을 표방하거나 CR 위원회가 정의한 EDR 솔루션의 기능을 충족하는 국내외 솔루션 전체를 1 차 조사 대상으로 파악하였다.

O 2019 년 1 월을 기준으로 언론기사에 EDR 솔루션 제품으로 소개되거나 제품 홍보 (브로셔, 홈페이지 등) 시 EDR 이라는 용어를 사용하는 25 개사 28 개 솔루션을 대상으로 참여를 요청하였다.

- 그 결과 일부 업체는 보고서 참여 요청 당시 '평가 참여의사가 없다'고 응답하거나,

- 일부 업체는 '제품 기능 개선이 예정되어 있어 지금 참여하는 것이 적절하지 않다'는 이유로 참여하지 않았으며,

- 일부 업체는 '해당 솔루션은 EDR 의 기능을 일부 가지고 있을 뿐 원래의 목적은 따로 있어 EDR 솔루션과 직접 비교하기에는 적절하지 않다'는 이유로 참여하지 않았고,

- 일부 업체는 '평가표를 보고 참여여부를 결정하겠다'고 하여 평가표를 송부하였으나 마감일까지 아무 연락이 없어 참여 대상에서 제외했다.

O 조사대상 제품은 벤더 참여요청 및 최종 벤더의 참여의사를 반영하여 8 개 회사가 확정되었으며, 참여 벤더 명은 다음과 같다.

  - 사이버리즌
  - 시만텍
  - 엔피코어
  - 지니언스
  - 카스퍼스키
  - 트렌드마이크로
  - 파이어아이
  - 팔로알토 (이상 업체명 기준 가나다 순)

6. 보고서 활용 시 유의 사항

O 본 보고서는 2019 년 2 월 기준의 검토 결과로서, 해당 연월 이후 독자가 보고서를 읽는 시점에서는 각 EDR 솔루션의 기능이 개선되거나 변경될 수 있다.

O 앞서 기술했듯이 각 업체의 솔루션이 CR 위원회가 정의한 EDR 솔루션에 해당하는지에 대한 판단과 본 조사에 대한 참여 여부는 전적으로 업체의 의사를 반영하였다.

O 본 보고서에서 사용한 조사항목은, EDR 솔루션을 도입함에 있어 필요하다고 판단되는 기능으로 구성해 솔루션들이 만족하는지 여부를 확인하기 위해 개발된 것이며, 주관식이 필요한 일부 항목을 제외하고는 O, △, X, NA 로 정성적인 평가를 진행했다. 다만, 평가기준에서 말하는 기능구현의 방식은 다양할 수 있기 때문에 O, △, X, NA 답변에 붙여 어떤 방식으로 구현되는지 부가설명을 기재하여 독자의 이해를 도왔다.

O 제품별로 순위를 정하는 것은 본 보고서의 작성 취지에 부합하지 않는다.

O 본 보고서는 사용자들이 EDR 솔루션을 도입할 경우, 시장에 존재하는 다양한 솔루션에 대한 선택기준과 이해를 위한 것으로 도입의사결정 단계나 BMT 전 단계에서 활용할 것을 권한다.

O 본 보고서에 등재된 솔루션의 기능, 성능에 대해 CONCERT 는 어떠한 보장도 하지 않으며, 본 보고서의 내용을 솔루션 벤더들이 영업을 위한 상업적 용도로 활용하는 것을 금지한다.

O EDR 의 범위가 넓기 때문에 본 보고서에 사용한 평가기준이 EDR 전 영역을 모두 포함하지 못하는 한계가 있다. 하지만 실질적인 도움이 되고자 현재 보안담당자로 근무 중이며, EDR 솔루션을 도입했거나 도입 예정인 8 명의 위원들이 협의해 공통의 적정 수준으로 추출하고자 노력했다.

O 다만, EDR 솔루션을 도입하고자 하는 각 회사의 상황과 조건에 따라 요구사항 및 판단기준은 달라지기 때문에 기업이 본 보고서의 조사항목만으로 솔루션을 선정 할 수는 없다고 판단되며, 해당 기업의 환경에 맞게 필요한 부분을 발췌·조합해 활용하는 것이 바람직하다고 판단된다.

Part Ⅱ. EDR 솔루션의 정의와 주요 기능

1 . EDR(Endpoint Detection & Response) 솔루션의 정의

O 본 보고서에서 사용되는 EDR 솔루션의 기준을 설정하기 위해서는 먼저 EDR이 어떤 범위까지를 지칭하는지가 먼저 정해져야 EDR 솔루션의 범위가 결정되기 때문에 EDR 솔루션의 정의를 먼저 내려 보았다.

O 가트너에 따르면 EDR솔루션은 "엔드포인트 시스템 레벨의 동작을 기록 및 저장하고 의심스러운 시스템 동작을 탐지하고 상황에 맞는 정보를 제공하며 악성활동을 차단하고 영향을 받는 시스템을 복원하기 위한 개선 제안을 제공하는 다양한 데이터 분석 기술을 사용하는 솔루션"이라고 한다.

O 위원회에서 논의한 EDR솔루션이 반드시 가져야 할 기능으로는
- 엔드포인트 시스템 레벨 동작: 이벤트를 기록하고 중앙 데이터베이스에 저장하고
- 알려진 IOC(침해지표) 와 행위 분석 기술을 사용하여 침해를 조기에 식별하기 위한 지속적인 검색을 수행하며
- 공격의 범위를 신속하게 조사하고 빠른 대응 기능을 가지는

솔루션으로 정해졌다.

O 위험을 관리하고 통제하기 위해서는 예측(Predict)-예방(Prevention)-탐지(Detect)-대응(Response)에 이르는 전 사이클을 다 아우르는 것이 이상적이겠지만, 단일 솔루션만으로 모든 기능을 기대하기 어려운 만큼, EDR솔루션이 제공하는 탐지와 대응, 엔드포인트 단에서의 가시화 부분에 초점을 맞추어 평가표를 만들었다.

2 . EDR 솔루션의 주요 평가항목

O CR위원회에서는 각 위원이 회원사에서 도입 제품선정을 위해 평가에 사용했거나, EDR 솔루션에 필요하다고 생각하는 기능 및 그 기능을 평가할 수 있는 방법을 취합한 다음, 위원회 토의를 통해 EDR 솔루션의 필수적인 기능을 선정하고, 이를 범주화해 평가항목을 정리했다. 평가항목 중 BMT를 통해 측정할 수 있는 성능항목은 제외한 결과, 총 6개 영역, 58개 평가항목을 선정했다. 선정된 항목과 평가기준을 <표 1>에 표시했다.

O 평가항목 중 중요하다고 생각되는 항목은 붉은색으로 표시하였다.

<표1> EDR 솔루션 평가항목

분류	기능	내용
탐지엔진 및 기술	알려진 악성코드 탐지 기술 제공	알려진 악성코드에 대한 탐지명 및 해당 정보를 제공해야함
	네트워크 IPS 공격 탐지 기술제공	네트워크레벨의 취약점 공격등의 위협을 탐지해야함
	평판데이터를 이용한 신종 위협 탐지	파일에 대한 정보를 기반으로 알려지지 않은 위협을 탐지 해야함
	파일리스 공격 탐지	파워쉘등을 이용한 파일리스 공격을 탐지 해야 함
	행위기반분석을 이용한 신종 위협 탐지	문서 및 실행 파일을 가상 환경 및 물리 시스템에서 실행 및 분석하여 알려지지 않은 위협을 탐지 해야함
	상관관계 분석기술을 이용한 연계분석	Endpoint/network/Email 에서 유입되는 위협을 통합하여 분석 및 조치가 가능해야함
	심각도 제공	관리자가 우선 조치를 위해 각 탐지한 이벤트별 확인가능 한 심각도 정보를 제공해야함 (critical 에서 -information 등급까지)
	지역별 공격정보 표시	지역별 실제 공격 정보를 표시
	unknown 탐지 대쉬보드	알려지지 않은 파일에 대한 분석수 대쉬보드 표시
인시던트 분석 정보	알려진 악성코드 탐지 기술	
	- 바이러스 탐지명	확인가능한 바이러스 탐지명 제공
	- 바이러스 위험도 표시	해당 악성코드의 위험도 표시 제공
	- 개괄 탐지 내용 표시	탐지한 알려진 악성코드에 관련된 내용이 설명된 페이지를 제공해야함
	네트워크 IPS 공격 탐지 기술	
	- 내부 사용자 IP 표시	내부 사용자의 주소를 표시해야함

분류	기능	내용
	- 외부 공격자 IP 표시	외부 공격자 IP 의 정보를 표시해야함
	- 외부 공격자 IP 의 정보 제공	공격자 IP 의 평판 및 위협정보, 위치등을 제공해야함
	- 다운로드/접속 URL 표시	접속 URL 을 표시해야함
	- 다운로드/접속 URL 의 정보 제공	표시된 URL 에 대해서 평판 정보 및 위협 상태를 표시해야함
	평판데이터를 이용한 신종 위협 탐지 기술	
	- 의심스러운 파일의 탐지	의심스러운 파일의 탐지가 가능해야함
	- 발생시간 표시	처음 발견된 시간을 표시해야함
	- 사용자수 표시	현재 해당파일을 사용하고 있는 사용자수를 표시해야함
	- 파일 서명 정보 표시	발견된 파일의 제작자 서명이 있는 경우 표시가 가능해야함
	행위분석 탐지 기술	
	- 전체 행위 데이터 표시	프로세스가 실행되어 하는 모든 동작을 분석 및 표시
	- 의심스러운 행위만 분류하여 표시	의심스러운 행위만 분류하여 표시
	- 악성행위만 분류하여 표시	악의적인 행위만 분류하여 표시
	상관관계 분석	
	- 인시던트 분석을 위한 개요 표시	공격자, 표적공격 여부, 영향받은 시스템, 공격에 사용된 파일 정보를 한눈에 파악할 수 있도록 제공
	- 내부 IP 와 관련된 인시던트 표시	내부 IP 와 관련된 인시던트 정보를 같이 표시 해야함
	- 외부 IP 와 관련된 인시던트 표시	외부 IP 와 관련된 인시던트 정보를 같이 표시 해야함
	- 해당 파일과 관련된 인시던트 표시	파일과 관련된 인시던트 정보를 같이 표시 해야함
	- 동일한 공격의 그룹핑 지원	동일한 파일 IP 등의 정보를 묶어서 캠페인으로 관리할수 있는 기능을 지원해야함

분류	기능	내용
	활성화된 공격의 표시	실제 활동중인 공격을 Active 로 표시가 가능해야함
	인텔리전스 기술	
	- 공격자 정보 제공	인텔리전스 평판 지수, 악의적 행위(말웨어 또는 C&C 등), 국가정보, 해당 도메인으로부터 다운로드 받은 파일 수, 연결된 마지막 IP
	- 동일한 hash 파일의 다른 이름 표시	추가분석을 위한 같은 해쉬값을 가진 다른 파일명의 표시
	- 안티바이러스에서 차단여부 확인	안티바이러스에서 차단 되었는지 확인가능
EDR Endpoint	의심스러운 파일 분류	단말에서 의심스러운 파일 을 분류
	Hash 검색	단말에서 디스크 Hash 검색
	파일검색	단말에서 디스크 파일검색
	레지스트리 검색	단말에서 디스크 레지스트리 검색
	파일 실행차단	단말에서 의심파일 실행차단
	시스템격리 및 복원	단말 시스템을 네트웍에서 격리하고 다시 복원
	파일 삭제	의심파일을 악성파일로 확정시 삭제
	파일 수집	추가 분석을 위해 단말에서 의심파일 수집
	타사 악성코드 탐지 내용 조회	VirusTotal 에 Hash 값 조회하여 타사 엔진에서 검출 여부 확인
	행위분석 요청	행위분석 요청을 위한 파일 전달
	시스템 덤프	시스템에 저장된 전체 덤프로그 수집
	프로세스 덤프	의심되는 프로세스의 덤프로그 수집
	단일에이전트	별도에이전트 설치 여부

분류	기능	내용
인시던트 처리	악성코드 샘플 처리 자동화 지원	탐지한 신종파일의 경우 자동으로 단말의 안티바이러스에서 샘플을 신고하는 기능이 제공되야 함
	안티바이러스 처리 지원	단말 안티바이러스에서 처리되는 인시던트는 차단이 완료된것으로 관리자에게 표시해야함
	인시던트 예외처리	발생한 인시던트가 오탐일 경우 예외처리 하는 기능을 제공
	인시던트 종료지원	관리자가 발생한 이벤트를 처리하고 케이스를 종료하는 케이스 상태 변환 기능을 제공해야함
	인시던트 차단지원	관리자가 차단한 이벤트를 endpoint / network / Email 에서 차단이 지원되야함
	인시던트 대응 내용 기입	인시던트의 처리 내용을 기입할수 있어야함
관리	NTP 설정 지원	시간 동기화를 위해 지원이 가능해야함
	SIEM 장비와 연계	Splunk 등의 장비로 로그 전송 지원
	관리콘솔 SSL 지원	관리 콘솔은 SSL 로 접속이 가능해야함
리포팅	심각한 인시던트에 대한 리포팅	다양한 분류로 보고가 지원되야함
	전체 인시던트 리포팅	전체 리포트 보고
	리포팅 및 알림 이메일 전송	이메일로 전송이 가능해야함

Part Ⅲ. EDR 솔루션 별 검토결과

■ 검토결과 활용 시 참고사항

O 본 보고서는 평가에 참여한 솔루션의 우열을 가리지 않으며, 기본적이고 공통적인 기능에 대한 평가를 수행하는 한편, 해당 평가기준으로 나타나지 않는 각 제품의 특징을 알릴 수 있도록 위원회의 총평과 벤더 측의 특장점을 소개했다.

O 본 보고서는 제품도입을 위한 BMT를 시행하기 앞서 사용자가 수많은 EDR 솔루션 중에서 자사의 환경과 목적에 적합한 솔루션을 1차 필터링 하는데 참고자료로 활용이 가능하다.

O EDR 솔루션을 도입하기 이전에 점검하고 검토할 사항에 대한 이해를 돕기 위해 본 보고서에서는 평가에 참여한 7개 벤더의 EDR 솔루션에 대한 기술자료와 응답자료를 통해 다음과 같은 형식으로 솔루션을 검토해 정리하였다.

- 업체명 / 제품명
- 위원회 솔루션 총평
- 벤더가 말하는 솔루션 특장점
- 솔루션 별 EDR 솔루션 세부 평가항목 검토결과

※ 소개 순서는 업체명 기준 가나다순

O 이 중 '위원회 총평'은 벤더의 제품에 대해 기술적인 자료 수집 및 벤더와의 인터뷰를 통해서 제품에 대한 전체적인 평가를 내린 것이며, '세부항목 검토결과'표는 EDR 솔루션의 기능과 평가기준을 정리한 표를 벤더에게 보내어 질의를 하고, 이에 대한 답변을 검토해 반영한 결과이다.

※ 개별 솔루션의 특성 상 해당 솔루션이 목적으로 하지 않는 분야의 평가 항목에 대해서는 NA(해당 없음)으로 처리함.

■ 총괄표

O 본 평가에 참여한 솔루션을 한눈에 비교할 수 있도록 동일 항목에 대한 답변을 정리해 총괄표에 기재했다.

O 동일 항목에 대한 답변이 O 로 같다고 해서 똑같이 구현되어 있다는 뜻은 아니다. 구현되는 방법이나 지원되는 항목은 차이가 있을 수 있으므로, 반드시 솔루션 별 평가자료를 참고하여 부가설명 등을 확인해야 할 필요가 있다.

O 카스퍼스키의 경우 제조사의 요구에 따라 총괄표에 "-"로 기재하고 "EDR 솔루션 별 검토결과"에서 모든 내용을 삭제하였다.

분류	기능	사이버 리즌	시만텍	엔피코어	지니언스	트렌드 마이크로	파이어 아이	팔로알토 네트웍스
탐지엔진 및 기술	알려진 악성코드 탐지 기술 제공	O	O	O	O	O	O	△
	네트워크 IPS 공격 탐지 기술제공	O	O	O	△	O	△	O
	평판데이터를 이용한 신종 위협 탐지	O	O	O	O	O	X	O
	파일리스 공격 탐지	O	O	O	O	O	O	O
	행위기반분석을 이용한 신종 위협 탐지	△	O	O	O	O	O	O
	상관관계 분석기술을 이용한 연계분석	O	O	O	△	O	△	O
	심각도 제공	O	O	O	O	O	O	O
	지역별 공격정보 표시	O	O	O	O	O	X	△
	unknown 탐지 대쉬보드	O	O	O	O	O	△	△
인시던트 분석 정보	알려진 악성코드 탐지 기술							
	- 바이러스 탐지명	O	O	O	O	O	O	O
	- 바이러스 위험도 표시	O	O	O	O	O	X	O
	- 개괄 탐지 내용 표시	O	O	O	△	O	O	O
	네트워크 IPS 공격 탐지 기술							
	- 내부 사용자 IP 표시	O	O	O	O	O	O	O
	- 외부 공격자 IP 표시	O	O	O	O	O	O	O
	- 외부 공격자 IP 의 정보 제공	O	O	O	O	O	△	O
	- 다운로드/접속 URL 표시	O	O	O	O	O	O	O
	- 다운로드/접속 URL 의 정보 제공	O	O	O	O	O	△	O

분류	기능	사이버 리즌	시만텍	엔피코어	지니언스	트렌드 마이크로	파이어 아이	팔로알토 네트웍스
	평판데이터를 이용한 신종 위협 탐지 기술							
	- 의심스러운 파일의 탐지	O	O	O	O	O	O	O
	- 발생시간 표시	O	O	O	O	O	O	O
	- 사용자수 표시	O	O	O	O	O	O	O
	- 파일 서명 정보 표시	O	O	O	O	O	O	O
	행위분석 탐지 기술							
	- 전체 행위 데이터 표시	O	O	O	O	O	O	O
	- 의심스러운 행위만 분류하여 표시	O	O	O	O	O	△	O
	- 악성행위만 분류하여 표시	O	O	O	O	O	O	O
	상관관계 분석							
	- 인시던트 분석을 위한 개요 표시	O	O	O	O	O	O	O
	- 내부 IP 와 관련된 인시던트 표시	O	O	O	O	O	O	O
	- 외부 IP 와 관련된 인시던트 표시	O	O	O	O	O	O	O
	- 해당 파일과 관련된 인시던트 표시	O	O	O	O	O	O	O
	- 동일한 공격의 그룹핑 지원	O	O	O	△	O	X	△
	활성화된 공격의 표시	O	O	O	△	O	O	O
	인텔리전스 기술							
	- 공격자 정보 제공	O	O	O	O	O	O	△
	- 동일한 hash 파일의 다른 이름 표시	O	O	O	O	O	O	O
	- 안티바이러스에서 차단여부 확인	△	O	O	X	O	O	O

분류	기능	사이버 리즌	시만텍	엔피코어	지니언스	트렌드 마이크로	파이어 아이	팔로알토 네트웍스
EDR Endpoint	의심스러운 파일 분류	O	O	△	O	O	X	O
	Hash 검색	O	O	X	O	O	O	O
	파일검색	O	O	X	O	O	O	O
	레지스트리 검색	O	O	X	O	O	O	O
	파일 실행차단	O	O	O	O	O	O	O
	시스템격리 및 복원	O	O	O	O	O	O	O
	파일 삭제	O	O	O	O	O	O	O
	파일 수집	O	O	O	O	O	O	X
	타사 악성코드 탐지 내용 조회	O	O	O	O	O	O	O
	행위분석 요청	△	O	O	O	O	X	O
	시스템 덤프	O	O	X	X	X	O	O
	프로세스 덤프	O	O	X	X	O	O	O
	단일에이전트	O	O	O	O	O	O	O
인시던트 처리	악성코드 샘플 처리 자동화 지원	△	O	O	O	X	X	O
	안티바이러스 처리 지원	△	O	O	X	O	O	O
	인시던트 예외처리	O	O	O	O	O	O	O
	인시던트 종료지원	O	O	O	O	O	O	O
	인시던트 차단지원	O	O	O	O	O	△	O
	인시던트 대응 내용 기입	O	O	O	O	O	O	O
관리	NTP 설정 지원	O	O	O	O	O	O	X

분류	기능	사이버 리즌	시만텍	엔피코어	지니언스	트렌드 마이크로	파이어 아이	팔로알토 네트웍스
	SIEM 장비와 연계	O	O	O	O	O	O	O
	관리콘솔 SSL 지원	O	O	O	O	O	O	O
리포팅	심각한 인시던트에 대한 리포팅	O	O	O	O	O	O	△
	전체 인시던트 리포팅	O	O	O	O	O	O	O
	리포팅 및 알림 이메일 전송	O	O	O	O	O	O	O

■ EDR 솔루션 별 검토결과

1. 사이버리즌(Cybereason) / Cybereason EDR

■ 위원회 제품 총평

사이버리즌 EDR은 엔드포인트 기기에서 수집한 정보를 바탕으로 상관분석 및 머신러닝을 통해 사이버 공격의 징후를 실시간으로 자동 탐지하고 대응할 수 있는 보안 플랫폼이다. 엔드포인트 호스트의 데이터 수집을 통한 위협 분석이 가능하며 실제 '공격'만을 탐지하여 알려주고 한 번의 클릭으로 모든 공격 단계를 치료할 수 있다고 한다. 이스라엘 사이버정보부대 출신들이 만들었다고 해서 그런지 빠른 대응을 위해 진행되고 있는 공격을 직관적으로 시각화한 대시보드를 채택하고 있고 하나의 공격을 드릴다운하여 상세정보를 확인할 수 있는 점은 잘 구성되어 있으나, 대시보드가 세련된 디자인은 아닌 것 같다. 샌드박스를 사용하지 않고 행위분석 만으로 머신러닝 기술을 이용해 알려지지 않은 새로운 공격을 탐지하고 대응하는 부분은 새롭다. 초당 800만 건 이상의 빅데이터 분석이 가능한 점은 기술력을 증명하는 것 같다. 다만 EDR과 NGAV가 같은 센서를 사용하고 제공할 수 있는 모든 기능을 사용하기 위해서는 사이버리즌의 EDR과 NGAV를 함께 사용해야 하는 점은 국내 레퍼런스가 많지 않은 상황에서는 조금 망설이게 하는 점이라 하겠다.

■ 벤더가 말하는 제품 특징

Cybereason의 목표는 공격 라이프 사이클의 모든 단계(사이버 킬체인)에서 복잡한 위협을 구체적으로 자동 탐지하고 공격자가 공격을 성공시키기 전에 신속하게 위협에 대응하는 것입니다.

Windows, Mac 및 Linux 시스템을 포함하여 엔터프라이즈의 모든 최종 사용자 시스템과 서버에서 상세 정보를 지속적으로 수집하여 공격의 모든 단계(초기감염, 명령 및 제어(C&C), 권한 상승 및 확장 감염, 데이터 유출, 랜섬웨어등)에서 악성 활동을 식별하여 운영자에게 알려주며, 탐지된 위협을 시간대별로 직관적으로 표시하여 근본 원인, 감염된 호스트 및 사용자, 관련 통신 및 사용된 도구 등에 대한 가시성을 완벽하게 제공합니다.

*Collect(효율적인 분석 데이터 수집)
*Analyze(빅데이터 자동 분석)
*Relate(효과적인 가시성 및 상관관계)
*Present (최적화된 대응력)

위와 같이 Cybereason은 자동화된 탐지, 완벽한 상황 인식 및 공격자 활동에 대한 깊은 이해와 대응 방안을 제공합니다.

분류	기능	내용	답변 (O,X,△, N/A)
탐지 엔진 및 기술	알려진 악성코드 탐지 기술 제공	알려진 악성코드에 대한 탐지명 및 해당 정보를 제공해야함 -->악성코드 탐지명 및 상세 정보 제공합니다.	O
	네트워크 IPS 공격 탐지 기술제공	네트워크레벨의 취약점 공격등의 위협을 탐지해야함 -->Cybereason Sensor 에는 DPI 모듈이 추가되어 있습니다. DPI 모듈은 Proxy 가시성을 활성화 시키고 네트워크를 통한 확장 공격(Ex: NTLM & Kerberos 프로토콜등의 트래픽을 분석하여 Pass the Hash, Pass the Ticket 등)을 탐지합니다. 이 기능은 지속적으로 확장 업데이트 되고 있습니다.	O
	평판데이터를 이용한 신종 위협 탐지	파일에 대한 정보를 기반으로 알려지지 않은 위협을 탐지 해야함 -->AI 분석엔진이 파일의 행위를 분석하여 알려지지 않은 위협을 자동으로 탐지합니다. * 평판(Reputation)정보는 주로 알려진 위협을 탐지하는 기반 데이터로 활용됩니다.	O
	파일리스 공격 탐지	파워쉘등을 이용한 파일리스 공격을 탐지 해야 함 -->단순히 스크립트나 명령 줄을 보는 것이 아니라 Powershell 엔진에서 실행되는 코드에 의해 수행되는 모든 작업을 보기 위해 프로세스 수준의 행동뿐만 아니라 더 깊은 코드 수준의 행동을 분석 할 수 있습니다. *Fileless 악성 코드 방지 기능의 특징 -모든 종류의 난독 스크립트 탐지 -모든 버전 PowerShell 지원 (버전 2 포함) -명령 줄 대화 스크립트, System.Management.Automation.dll 로드 등 모든 방법의 호출 방법에 대응	O

분류	기능	내용	답변 (O,X,△, N/A)
	행위기반분석을 이용한 신종 위협 탐지	문서 및 실행 파일을 가상 환경 및 물리 시스템에서 실행 및 분석하여 알려지지 않은 위협을 탐지 해야함 -->인공지능 분석엔진에서 파일들의 행위를 분석하여 자동으로 신종위협(UnKnown Malware)을 탐지합니다. * SandBox와 같이 파일을 직접 실행하지 않고 파일이 실행된 행위를 분석하여 탐지합니다.	△
	상관관계 분석기술을 이용한 연계분석	Endpoint/network/Email에서 유입되는 위협을 통합하여 분석 및 조치가 가능해야함 -->센서가 설치된 호스트의 모든 행위에 대해 상관관계 분석을 통하여 위협을 탐지하고 근원분석 및 위협과 연관된 모든 행위(파일로딩, Child 프로세스 생성 , 네트워크 통신, Injection 등)를 확인할 수 있고 적절한 대응 방안을 제공합니다.	O
	심각도 제공	관리자가 우선 조치를 위해 각 탐지한 이벤트별 확인가능 한 심각도 정보를 제공해야함 (critical에서 -information등급까지) -->Cybereason은 두단계로 위협을 분류하여 관리자에게 보여줍니다. 1. Evidence : 행위사실 추출단계 2. Suspicions : 의심단계 3. Malop(Malware Operation) : 위협 확정단계	O
	지역별 공격정보 표시	지역별 실제 공격 정보를 표시 -->공격과 관련된 IP의 Geo 정보 및 센서의 설치 위치(본사/지사등)의 정보를 확인할 수 있습니다.	O

분류	기능	내용	답변 (O,X,△, N/A)
	unknown 탐지 대쉬보드	알려지지 않은 파일에 대한 분석수 대쉬보드 표시 -->알려지지 않은(Unknown) 위협에 대한 정보를 취합하여 별도로 표시됩니다.	O
인시던트 분석 정보	**알려진 악성코드 탐지 기술**		
	- 바이러스 탐지명	확인가능한 바이러스 탐지명 제공 -->바이러스 탐지명을 제공합니다.	O
	- 바이러스 위험도 표시	해당 악성코드의 위험도 표시 제공 -->바이러스 위험도를 표시합니다.	O
	- 개괄 탐지 내용 표시	탐지한 알려진 악성코드에 관련된 내용이 설명된 페이지를 제공해야함 -->탐지된 위협(악성코드)에 대한 Overview 정보를 제공합니다.	O
	네트워크 IPS 공격 탐지 기술		
	- 내부 사용자 IP 표시	내부 사용자의 주소를 표시해야함 -->표시 지원.	O
	- 외부 공격자 IP 표시	외부 공격자 IP 의 정보를 표시해야함 -->표시 지원.	O
	- 외부 공격자 IP 의 정보 제공	공격자 IP 의 평판 및 위협정보, 위치등을 제공해야함 -->해당 정보를 제공합니다.	O
	- 다운로드/접속 URL 표시	접속 URL 을 표시해야함 -->해당 정보를 제공합니다.	O
	- 다운로드/접속 URL 의 정보 제공	표시된 URL 에 대해서 평판 정보 및 위협 상태를 표시해야함 -->해당 정보를 제공합니다.	O

분류	기능	내용	답변 (O,X,△, N/A)
	평판데이터를 이용한 신종 위협 탐지 기술		
	- 의심스러운 파일의 탐지	의심스러운 파일의 탐지가 가능해야함 -->파일의 행위 및 평판정보를 분석하여 의심스러운 파일을 탐지합니다.	O
	- 발생시간 표시	처음 발견된 시간을 표시해야함 -->타임라인상에 발생시간 및 이후 행위 시간을 표시합니다.	O
	- 사용자수 표시	현재 해당파일을 사용하고 있는 사용자수를 표시해야함 -->인시던트(위협)과 관련된 모든 사용자를 표시합니다.	O
	- 파일 서명 정보 표시	발견된 파일의 제작자 서명이 있는 경우 표시가 가능해야함 -->서명정보를 표시합니다.	O
	행위분석 탐지 기술		
	- 전체 행위 데이터 표시	프로세스가 실행되어 하는 모든 동작을 분석 및 표시 -->추가파일 로딩, 인젝션, 통신 등 해당 프로세스가 행위한 모든 동작을 확인 가능합니다.	O
	- 의심스러운 행위만 분류하여 표시	의심스러운 행위의 분류하여 표시 -->의심스러운 행위(Suspicions)를 분류하여 표시합니다.	O
	- 악성행위만 분류하여 표시	악의적인 행위만 분류하여 표시 -->악성행위(Malops)를 분류하여 표시합니다.	O
	상관관계 분석		
	- 인시던트 분석을 위한 개요 표시	공격자, 표적공격 여부, 영향받은 시스템, 공격에 사용된 파일 정보를 한눈에 파악할 수 있도록 제공	O

분류	기능	내용	답변 (O,X,△, N/A)
		-->해당 인시던트(위협)과 관련된 모든 정보를 그래픽컬하게 연결하여 운영자가 한눈에 확인할 수 있도록 요약/정리하여 표시됩니다.	
	- 내부 IP 와 관련된 인시던트 표시	내부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->내부 IP 및 외부 IP 와 관련된 인시던트(위협, 의심등) 정보를 같이 표시합니다.	O
	- 외부 IP 와 관련된 인시던트 표시	외부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->내부 IP 및 외부 IP 와 관련된 인시던트(위협, 의심등) 정보를 같이 표시합니다.	O
	- 해당 파일과 관련된 인시던트 표시	파일과 관련된 인시던트 정보를 같이 표시 해야함 -->파일(프로세스)와 관련된 인시던트(위협)정보를 같이 표시합니다.	O
	- 동일한 공격의 그룹핑 지원	동일한 파일 IP 등의 정보를 묶어서 캠페인으로 관리할수 있는 기능을 지원해야함 -->동일한 공격은 대상호스트등 관련이 있는 모든 항목에 대해 그룹핑하여 한화면에서 확인할 수 있도록 지원합니다.	O
	활성화된 공격의 표시	실제 활동중인 공격을 Active 로 표시가 가능해야함 -->현재 활성상태의 공격 및 위협 탐지 후 비활성화 상태에서 다시 활성화 될경우도 표시(Reopened)됩니다.	O
	인텔리전스 기술		
	- 공격자 정보 제공	인텔리전스 평판 지수, 악의적 행위(말웨어 또는 C&C 등), 국가정보, 해당 도메인으로부터 다운로드 받은 파일 수, 연결된 마지막 IP -->상세한 공격자의 정보(위협행위, IP, Domain, Geo 정보 등)을 제공합니다.	O
	- 동일한 hash 파일의 다른 이름 표시	추가분석을 위한 같은 해쉬값을 가진 다른 파일명의 표시 -->Hash 값 조회등을 통하여 확인 할 수 있습니다.	O

분류	기능	내용	답변 (O,X,△, N/A)
	- 안티바이러스에서 차단여부 확인	안티바이러스에서 차단 되었는지 확인가능 -->Cybereason 의 NGAV 를 사용할 경우 지원합니다.	△
EDR Endpoint	의심스러운 파일 분류	단말에서 의심스러운 파일을 분류 -->의심스러운 파일은 Suspicions 로 분류되어 표시됩니다.	O
	Hash 검색	단말에서 디스크 Hash 검색 -->Hash 검색을 지원합니다.	O
	파일검색	단말에서 디스크 파일검색 -->파일 검색을 지원합니다.	O
	레지스트리 검색	단말에서 디스크 레지스트리 검색 -->레지스트리 검색을 지원합니다.	O
	파일 실행차단	단말에서 의심파일 실행차단 -->실행차단(Prevention) 기능을 지원합니다.	O
	시스템격리 및 복원	단말 시스템을 네트웍에서 격리하고 다시 복원 -->네트워크 격리(Isolate) 및 복원을 지원합니다.	O
	파일 삭제	의심파일을 악성파일로 확정시 삭제 -->악성파일 확정시 해당 파일을 암호화하여 삭제(격리)시킵니다.	O
	파일 수집	추가 분석을 위해 단말에서 의심파일 수집 -->파일 수집 기능을 지원합니다.	O
	타사 악성코드 탐지 내용 조회	VirusTotal 에 Hash 값 조회하여 타사 엔진에서 검출 여부 확인 -->Hash 값의 Virustotal link 를 제공합니다.	O

분류	기능	내용	답변 (O,X,△, N/A)
	행위분석 요청	행위분석 요청을 위한 파일 전달 -->Cybereason 이 직접 3rd-Parth 솔루션으로 전달하는 기능은 제공하지 않으나, API 를 통하여 원하는 파일을 가져갈 수 있습니다.	△
	시스템 덤프	시스템에 저장된 전체 덤프로그 수집 -->시스템(에이전트가 설치된 단말)의 모든 덤프로그 정보를 수집합니다. 이 정보를 기반으로 각각의 덤프로그를 직접 수집할 수 있습니다.	O
	프로세스 덤프	의심되는 프로세스의 덤프로그 수집 -->Remote Shell(원격 쉘실행) 기능을 통하여 프로세서의 덤프로그 수집을 지원합니다.	O
	단일에이전트	별도에이전트 설치 여부 -->단일에이전트(센서)로 모든 기능 설치를 지원합니다.	O
인시던트 처리	악성코드 샘플 처리 자동화 지원	탐지한 신종파일의 경우 자동으로 단말의 안티바이러스에서 샘플을 신고하는 기능이 제공되야 함 -->Cybereason 의 NGAV 를 사용할 경우 지원.	△
	안티바이러스 처리 지원	단말 안티바이러스에서 처리되는 인시던트는 차단이 완료된것으로 관리자에게 표시해야함 -->Cybereason 의 NGAV 를 사용할 경우 지원.	△
	인시던트 예외처리	발생한 인시던트가 오탐일 경우 예외처리 하는 기능을 제공 -->File Hash, IP, Domain 기반의 Whitelist 및 행위기반의 Whitelisting 기능을 지원합니다.	O
	인시던트 종료지원	관리자가 발생한 이벤트를 처리하고 케이스를 종료하는 케이스 상태 변환 기능을 제공해야함 -->탐지된 위협 이벤트에 대해 다음과 같이 Prevention(차단), Suspended(멈춤), Remediated(조치완료) 로 상태변환을 지원합니다.	O

분류	기능	내용	답변 (O,X,△, N/A)
	인시던트 차단지원	관리자가 차단한 이벤트를 endpoint / network / Email 에서 차단이 지원되야함 -->네크워크 격리(isolate)기능 및 Blacklist 기능을 통하여 해당기능을 지원합니다.	O
	인시던트 대응 내용 기입	인시던트의 처리 내용을 기입할수 있어야함 -->인시던트(탐지된 위협)에 대해 처리내용 기입을 지원합니다.	O
관리	NTP 설정 지원	시간 동기화를 위해 지원이 가능해야함 -->NTP 설정을 지원합니다.	O
	SIEM 장비와 연계	Splunk 등의 장비로 로그 전송 지원 -->Splunk, Qrader 등의 SIEM 솔루션 및 Demisto, Phantom 등의 SOAR 솔루션들과 연동을 지원합니다. 또한 RestAPI 를 제공합니다.	O
	관리콘솔 SSL 지원	관리 콘솔은 SSL 로 접속이 가능해야함 -->SSL 접속을 지원합니다.	O
리포팅	심각한 인시던트에 대한 리포팅	다양한 분류로 보고가 지원되야함 -->인시던트(탐지된 위협)에 대한 리포팅을 지원합니다.(pdf, csv)	O
	전체 인시던트 리포팅	전체 리포트 보고 -->전체 인시던트(위협)에 대한 리포팅을 지원합니다. (pdf, csv)	O
	리포팅 및 알림 이메일 전송	이메일로 전송이 가능해야함 -->이메일로 지원합니다.	O

2. 시만텍 / EDR

■ 위원회 제품 총평

성능평가 지표들을 늘어놓고 EDR이 본래의 목적을 달성하기 위해 이 지표, 이 기능이 필요한가를 논의한 끝에 꼭 필요하거나, 필수는 아니더라도 유의미한 지표들로 구성한 평가항목을 구성했는데, 시만텍 EDR의 평가결과는 모든 평가항목을 만족하는 것으로 나왔다. 다만, 평가항목을 만족한다고 평가했다고 하더라도 어떤 식으로 구현되어 있는지에 따라 실제 평가항목을 충족하는 수준이 달라질 수 있으나 응답에서는 구체적인 구현 방법에 대한 설명이 조금 부족했다. 평과결과를 가지고 작성자와 인터뷰를 하였으나, 작성하면서 마치 자신들이 만든 평가표로 평가를 하는 것 같다는 느낌이었다고 한다. 어떻게 보면 EDR의 목적에 충실한 제품이라고 할 수 도 있겠지만, 실제 테스트베드에 올려놓지 않고 기능의 유무 만으로 판단하는 지면 BMT의 한계라고 할 수 있겠다. 그리고 타 솔루션과 비교할 때 결정적인 차이는 시만텍 EDR를 사용하기 위해서는 반드시 SEP(Symantec Endpoint Protection)을 사용해야 한다는 점이다. EDR의 기능만을 평가하기 위해 별도로 존재하는 솔루션(AV, 인텔리전스 서비스 등)과 연동해서 구현 가능한 기능은 부분적용(△)으로 표기하는 원칙을 세웠으나, 시만텍은 타사 AV를 사용하면서 시만텍 EDR만 사용할 수 없기 때문에 SEP연동 기능의 경우에도 기능구현으로 평가한 점을 감안해서 도입시 경제성을 생각해야 한다. 이미 시만텍의 SEP를 사용하고 있는 기업의 경우에는 EDR 도입 시 우선 검토하는 것이 좋겠다.

■ 벤더가 말하는 제품 특징

탐지 및 규명 - 보안 위반 사고 발견까지의 시간을 단축하고 신속하게 범위 파악
· 머신 러닝과 행위 분석을 적용하여 의심스러운 활동 규명, 침해사고 탐지 및 우선 순위 지정
· 실시간 쿼리를 통해 감염 데이터 증거 수집, 엔드포인트 에이전트에 직접 전달
· 의심스러운 스크립트 및 메모리 익스플로잇을 자동으로 식별하고 침해 사고 생성

조사 및 억제 - 침해 사고 대응 팀의 생산성 향상 및 확실하게 보안 위협 억제
· 엔드포인트 활동을 중단 없이 기록하여 완벽한 침해 사고 재연 보장, 구체적인 엔드포인트 프로세스 모니터링
· 실시간으로 모든 엔드포인트에서 보안 침해 지표를 검색하면서 보안 위협 추적
· 조사 과정에서 감염 가능성이 있는 엔드포인트 억제 및 격리

해결 - 신속하게 엔드포인트의 문제를 해결하여 보안 위협 재발 방지
· 공격받은 모든 엔드포인트에서 악성 파일 및 관련 아티팩트 삭제
· 엔드포인트의 파일 블랙리스팅/화이트리스팅
· 향상된 리포팅 기능으로 원하는 테이블에 대한 내보내기를 수행하여 침해 사고 해결 리포트 작성

분류	기능	내용	답변 (O,X,△,N/A)
탐지엔진 및 기술	알려진 악성코드 탐지 기술 제공	알려진 악성코드에 대한 탐지명 및 해당 정보를 제공해야함 -->Symantec Antivirus, Machine Learning 엔진	O
	네트워크 IPS 공격 탐지 기술제공	네트워크레벨의 취약점 공격등의 위협을 탐지해야함 -->IPS 기술 제공	O
	평판데이터를 이용한 신종 위협 탐지	파일에 대한 정보를 기반으로 알려지지 않은 위협을 탐지 해야함 -->파일 평판 기술 제공	O
	파일리스 공격 탐지	파워쉘등을 이용한 파일리스 공격을 탐지 해야 함 -->Powershell 공격 탐지 기능	O
	행위기반분석을 이용한 신종 위협 탐지	문서 및 실행 파일을 가상 환경 및 물리 시스템에서 실행 및 분석하여 알려지지 않은 위협을 탐지 해야함 -->클라우드, On-prem 분석 장비 지원	O
	상관관계 분석기술을 이용한 연계분석	Endpoint/network/Email 에서 유입되는 위협을 통합하여 분석 및 조치가 가능해야함 -->Synapse 기술로 상관관계 분석 제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	심각도 제공	관리자가 우선 조치를 위해 각 탐지한 이벤트별 확인가능 한 심각도 정보를 제공해야함 (critical 에서 -information 등급까지) -->4 단계의 심각도 정보 제공 (High to Inform)	O
	지역별 공격정보 표시	지역별 실제 공격 정보를 표시 -->제공	O
	unknown 탐지 대쉬보드	알려지지 않은 파일에 대한 분석수 대쉬보드 표시 -->제공	O
인시던트 분석 정보	알려진 악성코드 탐지 기술		
	- 바이러스 탐지명	확인가능한 바이러스 탐지명 제공 -->악성코드 탐지명 제공	O
	- 바이러스 위험도 표시	해당 악성코드의 위험도 표시 제공 -->악성코드 위험도 표시 제공	O
	- 개괄 탐지 내용 표시	탐지한 알려진 악성코드에 관련된 내용이 설명된 페이지를 제공해야함 -->Web 으로 제공	O
	네트워크 IPS 공격 탐지 기술		
	- 내부 사용자 IP 표시	내부 사용자의 주소를 표시해야함 -->제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	- 외부 공격자 IP 표시	외부 공격자 IP 의 정보를 표시해야함 -->제공	O
	- 외부 공격자 IP 의 정보 제공	공격자 IP 의 평판 및 위협정보, 위치등을 제공해야함 -->제공	O
	- 다운로드/접속 URL 표시	접속 URL 을 표시해야함 -->제공	O
	- 다운로드/접속 URL 의 정보 제공	표시된 URL 에 대해서 평판 정보 및 위협 상태를 표시해야함 -->제공	O
	평판데이터를 이용한 신종 위협 탐지 기술		
	- 의심스러운 파일의 탐지	의심스러운 파일의 탐지가 가능해야함 -->평판 정보 제공	O
	- 발생시간 표시	처음 발견된 시간을 표시해야함 -->제공	O
	- 사용자수 표시	현재 해당파일을 사용하고 있는 사용자수를 표시해야함 -->제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	- 파일 서명 정보 표시	발견된 파일의 제작자 서명이 있는 경우 표시가 가능해야함 -->제공	O
	행위분석 탐지 기술		
	- 전체 행위 데이터 표시	프로세스가 실행되어 하는 모든 동작을 분석 및 표시 -->전체 동작에 대한 분석 제공	O
	- 의심스러운 행위만 분류하여 표시	의심스러운 행위를 분류하여 표시 -->제공	O
	- 악성행위만 분류하여 표시	악의적인 행위만 분류하여 표시 -->제공	O
	상관관계 분석		
	- 인시던트 분석을 위한 개요 표시	공격자, 표적공격 여부, 영향받은 시스템, 공격에 사용된 파일 정보를 한눈에 파악할 수 있도록 제공 -->제공	O
	- 내부 IP 와 관련된 인시던트 표시	내부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->제공	O
	- 외부 IP 와 관련된 인시던트 표시	외부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	- 해당 파일과 관련된 인시던트 표시	파일과 관련된 인시던트 정보를 같이 표시 해야함 -->Drill Down 기능 제공	O
	- 동일한 공격의 그룹핑 지원	동일한 파일 IP 등의 정보를 묶어서 캠페인으로 관리할수 있는 기능을 지원해야함 -->연관이 있는 이벤트에 대한 묶음으로 Incident 제공	O
	활성화된 공격의 표시	실제 활동중인 공격을 Active 로 표시가 가능해야함 -->제공	O
	인텔리전스 기술		
	- 공격자 정보 제공	인텔리전스 평판 지수, 악의적 행위(말웨어 또는 C&C 등), 국가정보, 해당 도메인으로부터 다운로드 받은 파일 수, 연결된 마지막 IP -->제공	O
	- 동일한 hash 파일의 다른 이름 표시	추가분석을 위한 같은 해쉬값을 가진 다른 파일명의 표시 -->제공	O
	- 안티바이러스에서 차단여부 확인	안티바이러스에서 차단 되었는지 확인가능 -->제공	O
EDR Endpoint	의심스러운 파일 분류	단말에서 의심스러운 파일 을 분류 -->제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	Hash 검색	단말에서 디스크 Hash 검색 -->제공	O
	파일검색	단말에서 디스크 파일검색 -->제공	O
	레지스트리 검색	단말에서 디스크 레지스트리 검색 -->제공	O
	파일 실행차단	단말에서 의심파일 실행차단 -->제공	O
	시스템격리 및 복원	단말 시스템을 네트웍에서 격리하고 다시 복원 -->제공	O
	파일 삭제	의심파일을 악성파일로 확정시 삭제 -->제공	O
	파일 수집	추가 분석을 위해 단말에서 의심파일 수집 -->제공	O
	타사 악성코드 탐지 내용 조회	VirusTotal 에 Hash 값 조회하여 타사 엔진에서 검출 여부 확인 -->제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	행위분석 요청	행위분석 요청을 위한 파일 전달 -->제공	O
	시스템 덤프	시스템에 저장된 전체 덤프로그 수집 -->제공	O
	프로세스 덤프	의심되는 프로세스의 덤프로그 수집 -->제공	O
	단일에이전트	별도에이전트 설치 여부 -->Symantec Endpoint Protection Agent 와 통합	O
인시던트 처리	악성코드 샘플 처리 자동화 지원	탐지한 신종파일의 경우 자동으로 단말의 안티바이러스에서 샘플을 신고하는 기능이 제공되야 함 -->자동 신고 프로세스 제공	O
	안티바이러스 처리 지원	단말 안티바이러스에서 처리되는 인시던트는 차단이 완료된것으로 관리자에게 표시해야함 -->차단된 경우 우선순위 낮음으로 조정	O
	인시던트 예외처리	발생한 인시던트가 오탐일 경우 예외처리 하는 기능을 제공 -->예외처리 기능 제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	인시던트 종료지원	관리자가 발생한 이벤트를 처리하고 케이스를 종료하는 케이스 상태 변환 기능을 제공해야함 -->제공	O
	인시던트 차단지원	관리자가 차단한 이벤트를 endpoint / network / Email 에서 차단이 지원되야함 -->제공	O
	인시던트 대응 내용 기입	인시던트의 처리 내용을 기입할수 있어야함 -->제공	O
관리	NTP 설정 지원	시간 동기화를 위해 지원이 가능해야함 -->제공	O
	SIEM 장비와 연계	Splunk 등의 장비로 로그 전송 지원 -->제공	O
	관리콘솔 SSL 지원	관리 콘솔은 SSL 로 접속이 가능해야함 -->제공	O
리포팅	심각한 인시던트에 대한 리포팅	다양한 분류로 보고가 지원되야함 -->제공	O
	전체 인시던트 리포팅	전체 리포트 보고 -->제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	리포팅 및 알림 이메일 전송	이메일로 전송이 가능해야함 -->제공	O

3. 엔피코어 / 좀비제로 EDR for APT

■ 위원회 제품 총평

좀비제로(ZombieZERO) EDR for APT 솔루션은 사용자 PC를 비롯한 엔드포인트에서 실행되는 파일을 분석 서버로 업로드 한 다음 정상/악성 여부를 판단하여 실행/차단을 하는 방식으로 작동한다. 타사 EDR솔루션의 작동방식과 다른 점은 타 솔루션은 실행되는 것을 모니터링 해 악성행위를 신속히 탐지하고 대응하는 방식인데 반해 좀비제로의 작동방식은 실행되기 전에 파일을 분석단으로 업로드 해 악성행위유무를 먼저 판단하는 방식이다. 분석이 완료되기 까지는 사용자 PC단에서 실행보류 기능이 작동되기 때문에 사용자 수, 분석량, 분석장비에서 지원하는 가상머신의 수에 영향을 많이 받는 방식이다. 엔드포인트단에서 모니터링이나 로그를 쌓지 않기 때문에 PC단에서는 가볍다는 장점이 있지만, 분석장비에서 탐지/차단되지 않은 위협에 대해서는 사후 모니터링이 어려운 단점이 존재한다. 기능 평가표상에서도 엔드포인트 단의 메모리덤프, 프로세스 덤프 등을 지원하지 않고 엔드포인트 단의 레지스트리, 파일, 해시 검색을 지원하지 않는 점에서 실행 전 차단이라는 좀비제로 솔루션의 명확한 철학이 드러난다.

좀비제로는 국내 뿐 아니라 미국, 일본, 베트남, 말레이시아 등에도 많은 레퍼런스를 가지고 있으므로 엔드포인트 공격방어를 고려하는 기업/기관이라면 검토해 볼 만한 것으로 판단한다.

■ 벤더가 말하는 제품 특징

1. 악성 파일 즉각 차단

IOC (침해지표) 방식은 이미 침입한 악성코드가 남겨 놓은 흔적을 모아, 분석 시스템에서 패턴 분석하는 사후 대처 방식. 반면, 엔피코어 EDR은 실행 보류 기능을 통해 감염 되기 이전 악성 코드 즉각 대응.

2. PC 영향 최소화

에이전트 운영 시 기존 시스템 영향 최소화. 충돌 가능성이 높은 후킹 (hooking), dll injection 등의 기술 사용하지 않음.

3. 교육부 Yara Rule 연동

교육부 사이버안전센터 표준연동규격 테스트 통과(MTM 부분). 교육부로부터 YARA rule 수집, 이에 대한 탐지 정책 설정, 결과에 대해서도 재전송 가능.

4. 가상 분석 환경 맞춤 구성

일부 외산 제품은 가상 분석 환경이 정형화 되어 ALZ, HWP 등 환경은 추가되지 않는 경우가 있음. 엔피코어 EDR은 현지에서 주로 사용하는 어플리케이션으로 가상 / 환경 구성 가능하여 탐지율 상승.

분류	기능	내용	답변 (O,X,△,N/A)
탐지엔진 및 기술	알려진 악성코드 탐지 기술 제공	알려진 악성코드에 대한 탐지명 및 해당 정보를 제공해야함 -->AV 엔진 이용	O
	네트워크 IPS 공격 탐지 기술제공	네트워크레벨의 취약점 공격등의 위협을 탐지해야함 -->CnC 서버 및 악성 URL 접속 탐지	O
	평판데이터를 이용한 신종 위협 탐지	파일에 대한 정보를 기반으로 알려지지 않은 위협을 탐지 해야함 -->Virustotal 을 통한 평판 탐지 기능 제공	O
	파일리스 공격 탐지	파워쉘등을 이용한 파일리스 공격을 탐지 해야 함 -->파워쉘 분석	O
	행위기반분석을 이용한 신종 위협 탐지	문서 및 실행 파일을 가상 환경 및 물리 시스템에서 실행 및 분석하여 알려지지 않은 위협을 탐지 해야함 -->동적분석을 통한 신종 위협 탐지	O
	상관관계 분석기술을 이용한 연계분석	Endpoint/network/Email 에서 유입되는 위협을 통합하여 분석 및 조치가 가능해야함 -->패턴 풀링 기능을 통해 분석 및 조치	O
	심각도 제공	관리자가 우선 조치를 위해 각 탐지한 이벤트별 확인가능 한 심각도 정보를 제공해야함 (critical 에서 -information 등급까지) -->1~5 단계 표시	O
	지역별 공격정보 표시	지역별 실제 공격 정보를 표시	O
	unknown 탐지 대쉬보드	알려지지 않은 파일에 대한 분석수 대쉬보드 표시 -->따로 필터링 가능	O

분류	기능	내용	답변 (O,X,△,N/A)
인시던트 분석 정보	알려진 악성코드 탐지 기술		
	- 바이러스 탐지명	확인가능한 바이러스 탐지명 제공 -->바이러스명 표기	O
	- 바이러스 위험도 표시	해당 악성코드의 위험도 표시 제공 -->항시 5 단계로 표기	O
	- 개괄 탐지 내용 표시	탐지한 알려진 악성코드에 관련된 내용이 설명된 페이지를 제공해야함 -->바이러스 이름을 비롯한 일부 정보 제공	O
	네트워크 IPS 공격 탐지 기술		
	- 내부 사용자 IP 표시	내부 사용자의 주소를 표시해야함 -->악성코드를 다운로드 받은 IP 를 알 수 있음	O
	- 외부 공격자 IP 표시	외부 공격자 IP 의 정보를 표시해야함 -->악성코드를 배포한 IP / URL 을 알 수 있음	O
	- 외부 공격자 IP 의 정보 제공	공격자 IP 의 평판 및 위협정보, 위치등을 제공해야함	O
	- 다운로드/접속 URL 표시	접속 URL 을 표시해야함 -->분석 로그 표기	O
	- 다운로드/접속 URL 의 정보 제공	표시된 URL 에 대해서 평판 정보 및 위협 상태를 표시해야함	O
	평판데이터를 이용한 신종 위협 탐지 기술		
	- 의심스러운 파일의 탐지	의심스러운 파일의 탐지가 가능해야함 -->Virustotal 및 McAfee 연동을 통해 탐지 가능	O

분류	기능	내용	답변 (O,X,△,N/A)
	- 발생시간 표시	처음 발견된 시간을 표시해야함 -->최초 내부로 파일 유입된 시간 알 수 있음	O
	- 사용자수 표시	현재 해당파일을 사용하고 있는 사용자수를 표시해야함 -->어디서 얼마나 다운로드 받았는지로 카운팅 가능	O
	- 파일 서명 정보 표시	발견된 파일의 제작자 서명이 있는 경우 표시가 가능해야함 -->전자서명 표시함	O
	행위분석 탐지 기술		
	- 전체 행위 데이터 표시	프로세스가 실행되어 하는 모든 동작을 분석 및 표시 -->행위 로그 기록함	O
	- 의심스러운 행위만 분류하여 표시	의심스러운 행위의 분류하여 표시 -->행위 로그에 따라 위험도 표기	O
	- 악성행위만 분류하여 표시	악의적인 행위만 분류하여 표시 -->4,5 단계 위험도 행위는 악성으로 표기	O
	상관관계 분석		
	- 인시던트 분석을 위한 개요 표시	공격자, 표적공격 여부, 영향받은 시스템, 공격에 사용된 파일 정보를 한눈에 파악할 수 있도록 제공	O
	- 내부 IP 와 관련된 인시던트 표시	내부 IP 와 관련된 인시던트 정보를 같이 표시 해야함	O
	- 외부 IP 와 관련된 인시던트 표시	외부 IP 와 관련된 인시던트 정보를 같이 표시 해야함	O
	- 해당 파일과 관련된 인시던트 표시	파일과 관련된 인시던트 정보를 같이 표시 해야함	O

분류	기능	내용	답변 (O,X,△,N/A)
	- 동일한 공격의 그룹핑 지원	동일한 파일 IP 등의 정보를 묶어서 캠페인으로 관리할수 있는 기능을 지원해야함	O
	활성화된 공격의 표시	실제 활동중인 공격을 Active 로 표시가 가능해야함	O
	인텔리전스 기술		
	- 공격자 정보 제공	인텔리전스 평판 지수, 악의적 행위(말웨어 또는 C&C 등), 국가정보, 해당 도메인으로부터 다운로드 받은 파일 수, 연결된 마지막 IP	O
	- 동일한 hash 파일의 다른 이름 표시	추가분석을 위한 같은 해쉬값을 가진 다른 파일명의 표시	O
	- 안티바이러스에서 차단여부 확인	안티바이러스에서 차단 되었는지 확인가능 -->AV 엔진에 의해 검사 로그 제공	O
EDR Endpoint	의심스러운 파일 분류	단말에서 의심스러운 파일 을 분류 -->의심스러운 파일 3 단계 이상으로 분류	△
	Hash 검색	단말에서 디스크 Hash 검색	X
	파일검색	단말에서 디스크 파일검색	X
	레지스트리 검색	단말에서 디스크 레지스트리 검색	X
	파일 실행차단	단말에서 의심파일 실행차단	O
	시스템격리 및 복원	단말 시스템을 네트웍에서 격리하고 다시 복원 -->옵션 추가로 구현 가능	O

분류	기능	내용	답변 (O,X,△,N/A)
	파일 삭제	의심파일을 악성파일로 확정시 삭제 -->격리 기능 제공	O
	파일 수집	추가 분석을 위해 단말에서 의심파일 수집 -->분석 파일 업로드 기능 제공	O
	타사 악성코드 탐지 내용 조회	VirusTotal 에 Hash 값 조회하여 타사 엔진에서 검출 여부 확인 -->virustotal 평판 조회 기능 제공	O
	행위분석 요청	행위분석 요청을 위한 파일 전달 -->파일 업로드 후 행위 분석 진행	O
	시스템 덤프	시스템에 저장된 전체 덤프로그 수집	X
	프로세스 덤프	의심되는 프로세스의 덤프로그 수집	X
	단일에이전트	별도에이전트 설치 여부 -->별도의 에이전트 설치	O
인시던트 처리	악성코드 샘플 처리 자동화 지원	탐지한 신종파일의 경우 자동으로 단말의 안티바이러스에서 샘플을 신고하는 기능이 제공되야 함 -->신종 악성코드 보안센터 업로드 기능 제공	O
	안티바이러스 처리 지원	단말 안티바이러스에서 처리되는 인시던트는 차단이 완료된것으로 관리자에게 표시해야함 -->차단 로그 제공	O
	인시던트 예외처리	발생한 인시던트가 오탐일 경우 예외처리 하는 기능을 제공 -->오탐처리를 위한 화이트리스트 제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	인시던트 종료지원	관리자가 발생한 이벤트를 처리하고 케이스를 종료하는 케이스 상태 변환 기능을 제공해야함	O
	인시던트 차단지원	관리자가 차단한 이벤트를 endpoint / network / Email 에서 차단이 지원되야함 -->패턴풀링 블랙리스트를 통해 차단 기능 제공	O
	인시던트 대응 내용 기입	인시던트의 처리 내용을 기입할수 있어야함	O
관리	NTP 설정 지원	시간 동기화를 위해 지원이 가능해야함	O
	SIEM 장비와 연계	Splunk 등의 장비로 로그 전송 지원 -->Syslog 를 통한 연동 지원	O
	관리콘솔 SSL 지원	관리 콘솔은 SSL 로 접속이 가능해야함 -->HTTPS	O
리포팅	심각한 인시던트에 대한 리포팅	다양한 분류로 보고가 지원되야함 -->엑셀, 워드, PDF 로 제공	O
	전체 인시던트 리포팅	전체 리포트 보고	O
	리포팅 및 알림 이메일 전송	이메일로 전송이 가능해야함 -->이메일 경보(알람) 기능 제공	O

4. 지니언스 / Genian Insights E

■ 위원회 제품 총평

방어 위주의 보안 전략의 한계때문에 모든 공격을 100% 방어하는 것은 불가능하다는 것을 전제로 방어가 실패했을 경우의 대응전략으로 침입을 단계별로 구분하여 단계별 대응 프로세스를 도입하는 것이 필요하다. 원천적인 보안위협 차단이 불가능한 지능형 공격에 대한 신속한 탐지와 대응이 대형 보안사고를 막기 위한 해답이라고 말한다. EDR 솔루션 도입과 운영에서 탐지 정확도 만큼 오탐을 최소화하는 것이 중요한 부분인데 지니안 인사이츠 E는 딥러닝으로 대표되는 머신러닝 기술을 도입해 정확도를 많이 끌어올렸다고 한다. 데이터 시각화에 신경을 많이 쓰고 있고 유연한 위젯 제공을 통해 사용자의 필요에 맞게 적용할 수 있다. 평가표 응답에 있어서도 모든 평가항목에 기능 구현 화면 증적을 첨부해 추가 인터뷰 없이도 어떤 방식으로 어떤 수준까지 기능을 제공하는지 알 수 있었다. 지니안NAC과 함께 사용할 경우에 악성행위 탐지, 대응에 이어 실질적인 차단, 격리 등 악성행위를 통제할 수 있게 된다. 국산 EDR 솔루션 중 초창기부터 나온 솔루션인 만큼 기능 개선이 많이 이루어 졌고, 머신러닝 기능 추가 후 초기버전 고객 대상 무상 업그레이드 사례가 알려져 있어, 제품 선택에 있어 버전관리/업데이트에 관해서는 신뢰할 만 하다는 인상을 준다.

■ 벤더가 말하는 제품 특징

Genian Insights E는 사용자 단말(엔드포인트)의 가시성을 확보하고 이를 통해 지능형 위협의 탐지, 조사, 대응을 위한 솔루션 입니다.

사용자의 행위부터 데이터수준에 이르는 단계적이고 세밀한 가시성을 확보할 수 있습니다.

또한 침해사고지표(IOC), 머신러닝(ML), 행위기반분석(XBA), 야라(YARA) 등의 다양한 위협탐지 및 분석기술이 적용되어 알려진 또는 알려지지 않은 모든 공격을 탐지하고 대응할 수 있습니다.

뿐만 아니라 단순히 위협의 탐지와 차단이 아닌 사고 대응, 위협 추적, 엔드포인트 컴플라이언스, 유연한 관리 콘솔 기능 등을 포함하여 엔드포인트 보안 플랫폼으로 활용이 가능합니다.

다년간의 사업경험을 통해 (현재)국내에서 가장 많은 EDR 고객 사를 확보하고 있으며 단말 보안수준을 높이고자 하는 고객의 요구사항과 다양한 업무환경을 잘 이해하고 있습니다.

향후 적극적인 투자와 지속적인 연구개발을 통해 국내 1등을 넘어 글로벌 수준의 EDR로 거듭날 것 입니다.

분류	기능	내용	답변 (O,X,△,N/A)
탐지엔진 및 기술	알려진 악성코드 탐지 기술 제공	알려진 악성코드에 대한 탐지명 및 해당 정보를 제공해야함 -->알려진 악성코드에 대해서 탐지명 및 추가 상세 정보를 제공합니다.	O
	네트워크 IPS 공격 탐지 기술제공	네트워크레벨의 취약점 공격등의 위협을 탐지해야함 -->네트워크 패킷을 분석하여 Lateral Movement 에 이용되는 특정 패턴의 SMB 패킷 (Remote Service, Remote TaskScheduler, Remote WMI, atsvc) 및 Half-open 방식의 스텔스 포트스캐닝 등 비정상적인 트래픽을 탐지합니다.	△
	평판데이터를 이용한 신종 위협 탐지	파일에 대한 정보를 기반으로 알려지지 않은 위협을 탐지 해야함 -->자체 CTI 및 Ecosystem 을 통한 평판서비스를 제공합니다. Ecosystem 은 Insights E 제품을 위해 운영되는 백엔드 서비스이며 내부 및 외부(ReversingLabs, VirusTotal 등과 연동) CTI 서비스와 연동되어 운영됩니다.	O
	파일리스 공격 탐지	파워쉘등을 이용한 파일리스 공격을 탐지 해야 함 -->파워쉘, 매크로, 스크립트 등을 이용한 파일리스 공격에 대한 탐지 기능을 제공합니다.	O
	행위기반분석을 이용한 신종 위협 탐지	문서 및 실행 파일을 가상 환경 및 물리 시스템에서 실행 및 분석하여 알려지지 않은 위협을 탐지 해야함 -->실제 단말내에서 발생하는 문서 및 실행파일의 행위를 분석하여 신종위협을 탐지하는 XBA 엔진을 탑재하고 있으며, 샌드박스 제품과	O

분류	기능	내용	답변 (O,X,△,N/A)
		연동을 통해 수집한 샘플을 분석요청하여 가상환경에서 분석하고 그결과를 관리콘솔을 통해 확인 할 수 있는 기능을 제공합니다.	
	상관관계 분석기술을 이용한 연계분석	Endpoint/network/Email 에서 유입되는 위협을 통합하여 분석 및 조치가 가능해야함 -->이벤트 조사로 탐지된 파일 또는 행위가 어디에서 유입 됐는지 확인할 수 있는 기능을 제공합니다.	△
	심각도 제공	관리자가 우선 조치를 위해 각 탐지한 이벤트별 확인가능 한 심각도 정보를 제공해야함 (critical 에서 -information 등급까지) -->I.E(Insights E)에서는 악성코드 탐지에 대해 위험도, 신뢰도, 머신러닝 탐지 지표를 제공합니다. 위험도 : Low, Medium, High 신뢰도 : 0~100% 행위기반 탐지의 대해서는 동일하게 위험도, 신뢰도 지표를 제공하며 악성코드가 아닌 컨플라이언스 관점에서의 행위정보(USB 사용, USB 파일이동등)에 대해 Info 등급의 정보도 제공합니다.	O
	지역별 공격정보 표시	지역별 실제 공격 정보를 표시 -->악성으로 탐지된 IP 의 위치정보(GeoIP DB)를 이용하여 MAP 에 표시하는 대시보드 위젯을 제공합니다.	O

분류	기능	내용	답변 (O,X,△,N/A)
	unknown 탐지 대쉬보드	알려지지 않은 파일에 대한 분석수 대쉬보드 표시 -->알려진/알려지지않은 파일 전체에 대한 대시보드와 알려지지않은 파일에 대해서만 전용을 생성하여 대시보드로 표현할 수 있습니다. 기본 제공되는 대시보드외에 사용자정의 대시보드를 생성하여 관리자가 원하는 데이터를 적절한 형태로 표시할 수 있습니다.	O
인시던트 분석 정보	알려진 악성코드 탐지 기술		
	- 바이러스 탐지명	확인가능한 바이러스 탐지명 제공 -->악성코드로 탐지된 파일에 대해서 바이러스 명이 제공됩니다.	O
	- 바이러스 위험도 표시	해당 악성코드의 위험도 표시 제공 -->악성코드에 대한 위험도와 신뢰도를 제공합니다.	O
	- 개괄 탐지 내용 표시	탐지한 알려진 악성코드에 관련된 내용이 설명된 페이지를 제공해야함 -->탐지된 악성코드에 대한 개괄 탐지내용을 표시하고 사용자 정의 가능한 외부링크를 통해 추가적인 정보를 얻을 수 있도록 기능을 제공합니다.	△
	네트워크 IPS 공격 탐지 기술		
	- 내부 사용자 IP 표시	내부 사용자의 주소를 표시해야함 -->내부 사용자의 이름과 사용하고 있는 IP 정보를 제공합니다.	O
	- 외부 공격자 IP 표시	외부 공격자 IP 의 정보를 표시해야함 -->외부 공격자의 IP 정보를 제공합니다.	O

분류	기능	내용	답변 (O,X,△,N/A)
	- 외부 공격자 IP 의 정보 제공	공격자 IP 의 평판 및 위협정보, 위치등을 제공해야함 -->악성 IP 에 대한 위협정보 및 위치정보를 제공합니다.	O
	- 다운로드/접속 URL 표시	접속 URL 을 표시해야함 -->사용자가 접속한 외부 IP 에 대한 URL 정보를 제공합니다.	O
	- 다운로드/접속 URL 의 정보 제공	표시된 URL 에 대해서 평판 정보 및 위협 상태를 표시해야함 -->외부로 접속한 URL, 다운로드 정보와 IP 에 대한 평판 및 위협 상태 정보를 제공합니다.	O
	평판데이터를 이용한 신종 위협 탐지 기술		
	- 의심스러운 파일의 탐지	의심스러운 파일의 탐지가 가능해야함 -->머신러닝(ML)을 통해 의심파일(알려지지 않은 악성코드 파일)에 대한 탐지 기능을 제공합니다.	O
	- 발생시간 표시	처음 발견된 시간을 표시해야함 -->사내에서 처음 발견된 시각과 최근 발견 시간을 제공하며, 평판정보를 통해 글로벌하게 발견된 최초/최근 시간도 추가로 제공합니다.	O
	- 사용자수 표시	현재 해당파일을 사용하고 있는 사용자수를 표시해야함 -->탐지된 악성파일이 존재하는 사용자 및 해당 PC 내의 경로정보도 함께 제공합니다. 또한 Hash 값, 파일명 등을 이용한 검색을 통해 해당 파일의 PC 정보, 사용자 및 경로등 추가정보를 확인 할 수 있습니다.	O

분류	기능	내용	답변 (O,X,△,N/A)
	- 파일 서명 정보 표시	발견된 파일의 제작자 서명이 있는 경우 표시가 가능해야함 -->파일의 코드사인 정보와 발급자, 주최, 신뢰여부에 대한 정보도 같이 제공합니다.	O
	행위분석 탐지 기술		
	- 전체 행위 데이터 표시	프로세스가 실행되어 하는 모든 동작을 분석 및 표시 -->프로세스가 실행되어 동작하는 모든 행위에 대해 확인이 가능하며 이벤트체인을 통해 프로세스-파일간의 연결도 확인 가능합니다. 프로세스간 이동 기능을 통해 해당 프로세스의 모든행위를 시각화하여 분석할 수 있습니다.	O
	- 의심스러운 행위만 분류하여 표시	의심스러운 행위의 분류하여 표시 -->의심스러운 행위에 대한 정의가 되어 있으며 정의된 행위에 대해 분류하여 관리자에게 정보를 제공합니다.	O
	- 악성행위만 분류하여 표시	악의적인 행위만 분류하여 표시 -->악성으로 직접 판단한 결과만 선택적으로 확인할 수 있는 기능을 제공합니다. 알려진 위협/알려지지지 않은 위협을 구분하여 확인할 수 있습니다.	O
	상관관계 분석		
	- 인시던트 분석을 위한 개요 표시	공격자, 표적공격 여부, 영향받은 시스템, 공격에 사용된 파일 정보를 한눈에 파악할 수 있도록 제공	O

분류	기능	내용	답변 (O,X,△,N/A)
		-->위협탐지시 분석을 위해 관련 정보를 한눈에 파악할 수 있고 해당 인시던트를 처리할 수 있는 관리화면을 제공합니다.	
	- 내부 IP 와 관련된 인시던트 표시	내부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->내부 IP 정보와 사용자 정보를 포함한 인시던트 정보를 제공합니다.	O
	- 외부 IP 와 관련된 인시던트 표시	외부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->외부로 접속한 외부 IP 정보와 URL 정보, 인시던트 정보를 제공합니다.	O
	- 해당 파일과 관련된 인시던트 표시	파일과 관련된 인시던트 정보를 같이 표시 해야함 -->특정 파일과 관련된 파일 또는 프로세스, 레지스트리, 세션 정보등을 같이 제공합니다. 다이어그램 형태의 체인이벤트와 표 형태의 이벤트 조사를 동시에 할 수 있습니다.	O
	- 동일한 공격의 그룹핑 지원	동일한 파일 IP 등의 정보를 묶어서 캠페인으로 관리할수 있는 기능을 지원해야함 -->탐지된 동일한 위협 파일 및 IP 는 하나로 묶어서 관리할 수 있습니다.	△
	활성화된 공격의 표시	실제 활동중인 공격을 Active 로 표시가 가능해야함 -->현재 Active 한 프로세스에 대해서는 아이콘 하위에 별도의 점으로 표시되어 실행 중인 지, 중지가 된 프로세스인지에 대한 정보를 제공합니다.	△

분류	기능	내용	답변 (O,X,△,N/A)
	인텔리전스 기술		
	- 공격자 정보 제공	인텔리전스 평판 지수, 악의적 행위(말웨어 또는 C&C 등), 국가정보, 해당 도메인으로부터 다운로드 받은 파일 수, 연결된 마지막 IP -->공격자에 대한 평판정보를 제공하여 국가, URL, 탐지유형, 위험에 관한 추가 정보를 제공하며 VirusTotal 등의 외부링크를 통해 추가적인 정보를 획득할 수 있습니다.	O
	- 동일한 hash 파일의 다른 이름 표시	추가분석을 위한 같은 해쉬값을 가진 다른 파일명의 표시 -->분석화면에서 동일 Hash 값을 가진 다른이름의 파일경로 표시기능을 제공하며 Hash 값에 대한 이벤트 검색을 통해 서로다른 이름을 확인 할 수 있습니다.	O
	- 안티바이러스에서 차단여부 확인	안티바이러스에서 차단 되었는지 확인가능 -->개발 로드맵 추가	X
EDR Endpoint	의심스러운 파일 분류	단말에서 의심스러운 파일 을 분류 -->알려진 위협과 알려지지 않응 위협(의심)을 구분하여 관리자에게 제공합니다.	O
	Hash 검색	단말에서 디스크 Hash 검색 -->수집한 이벤트에 대한 HASH 검색 기능을 제공하며 YARA 룰 검사기능을 통해 관리자가 단말의 디스크에서 해당 Hash 의 파일을 검색할 수 있습니다.	O

분류	기능	내용	답변 (O,X,△,N/A)
	파일검색	단말에서 디스크 파일검색 -->수집한 이벤트에 대한 파일(이름, size, 위치 등) 검색 기능을 제공하며 YARA 룰 검사기능을 통해 관리자가 단말의 디스크에서 해당 조건의 파일을 검색할 수 있습니다.	O
	레지스트리 검색	단말에서 디스크 레지스트리 검색 -->레지스트리 검색 기능을 제공합니다.	O
	파일 실행차단	단말에서 의심파일 실행차단 -->정책에 의해 의심파일 또는 확정된 파일에 대해 프로세스 실행 차단을 하며 사용자에게 화면과 같은 알람을 제공합니다.	O
	시스템격리 및 복원	단말 시스템을 네트웍에서 격리하고 다시 복원 -->정책에 의해 의심파일 또는 확정된 파일이 탐지된 PC 는 네트워크 격리를 할 수 있으며, 사용자에게 알람창을 제공합니다. PC 에 대한 조사완료 후 네트워크 격리에서 복원할 수 있습니다.	O
	파일 삭제	의심파일을 악성파일로 확정시 삭제 -->위협관리를 통해 확정된 악성파일에 대응 정책을 설정하면 프로세스 중지, 파일 격리 후 삭제 기능을 제공합니다. 동일한 악성파일 탐지시에 자동으로 설정한 정책이 적용될 수 있는 기능도 옵션으로 제공합니다.	O
	파일 수집	추가 분석을 위해 단말에서 의심파일 수집 -->의심되는 파일샘플을 수동 또는 자동으로 수집할 수 있습니다.	O

분류	기능	내용	답변 (O,X,△,N/A)
	타사 악성코드 탐지 내용 조회	VirusTotal 에 Hash 값 조회하여 타사 엔진에서 검출 여부 확인 -->VirusTotal 등 Hash 를 검색할 수 있는 링크를 제공하며 링크 클릭 시 자동으로 해시값을 조회하여 결과를 알려줍니다. 또한 관리자가 Hash, FileName, IP 등 탐지된 정보를 기반으로 외부링크와 연계하여 추가 조사를 할 수 있도록 사용자정의 외부링크기능을 제공합니다.	O
	행위분석 요청	행위분석 요청을 위한 파일 전달 -->관리자는 수집된 샘플을 다운로드하여 추가분석 할 수 있으며 연동된 외부 분석시스템에 샘플을 전달하고 분석된 결과를 관리콘솔을 통해 확인할 수 있습니다.	O
	시스템 덤프	시스템에 저장된 전체 덤프로그 수집 -->개발 로드맵 추가	X
	프로세스 덤프	의심되는 프로세스의 덤프로그 수집 -->개발 로드맵 추가	X
	단일에이전트	별도에이전트 설치 여부 -->하나의 Agent 에서 모든 기능을 수행합니다.	O
인시던트 처리	악성코드 샘플 처리 자동화 지원	탐지한 신종파일의 경우 자동으로 단말의 안티바이러스에서 샘플을 신고하는 기능이 제공되야 함 -->탐지한 파일을 분석요청 할 경우 분석된 결과를 확인할 수 있는 기능을 제공합니다.	O

분류	기능	내용	답변 (O,X,△,N/A)
	안티바이러스 처리 지원	단말 안티바이러스에서 처리되는 인시던트는 차단이 완료된것으로 관리자에게 표시해야함 -->개발 로드맵 추가	X
	인시던트 예외처리	발생한 인시던트가 오탐일 경우 예외처리 하는 기능을 제공 -->발생한 인시던트가 오탐일 경우 별도로 오탐에 대한 예외처리(악성코드 및 행위탐지 오탐)를 할 수 있으며, 오탐 보고 기능 제공으로 자동으로 오탐처리를 할 수 있습니다.	O
	인시던트 종료지원	관리자가 발생한 이벤트를 처리하고 케이스를 종료하는 케이스 상태 변환 기능을 제공해야함 -->발생한 이벤트를 관리하기 위한 별도의 화면을 제공하며, 처리 상태, 결과, 변경 이력등을 제공합니다. 악성, 안전, 보류로 위협에 대한 판정을 할 수 있으며, 판정된 이벤트에 대한 변경이 필요할 경우 변경할 수 있는 기능도 제공합니다.	O
	인시던트 차단지원	관리자가 차단한 이벤트를 endpoint / network / Email 에서 차단이 지원되야함 -->1) 엔드포인트에서의 프로세스 중지, 격리 기능을 제공합니다. 2) 악성코드 감염 시 네트워크 차단 기능을 제공합니다.	O
	인시던트 대응 내용 기입	인시던트의 처리 내용을 기입할수 있어야함 -->인시던트에 대한 위협 대응 내용을 관리하는 기능을 제공합니다.	O

분류	기능	내용	답변 (O,X,△,N/A)
관리	NTP 설정 지원	시간 동기화를 위해 지원이 가능해야함 -->시간 동기화를 위한 NTP 설정 기능을 제공합니다.	O
	SIEM 장비와 연계	Splunk 등의 장비로 로그 전송 지원 -->타 솔루션으로의 syslog 전송 기능을 제공합니다. 특정 이벤트를 필터 전송, 다중 전송 기능을 제공합니다.	O
	관리콘솔 SSL 지원	관리 콘솔은 SSL 로 접속이 가능해야함 -->관리 콘솔은 https 를 사용하며 관리자별 접속가능 IP 제한을 위한 ACL 설정 기능도 제공합니다.	O
리포팅	심각한 인시던트에 대한 리포팅	다양한 분류로 보고가 지원되야함 -->인시던트 처리 상태, 탐지엔진 기준의 다양한 분류로 보고를 할 수 있는 기능을 제공합니다.	O
	전체 인시던트 리포팅	전체 리포트 보고 -->전체 위협 현황을 한눈에 볼 수 있는 화면과 대시보드를 이용한 리포트 보고 기능을 제공합니다.	O
	리포팅 및 알림 이메일 전송	이메일로 전송이 가능해야함 -->메일 연동으로 위협 리포트를 자동 생성하여 관리자에게 전송하는 기능을 제공합니다.	O

~~5. 카스퍼스키 / Kaspersky EDR~~

~~■ 위원회 제품 총평~~

~~■ 벤더가 말하는 제품 특징.~~

카스퍼스키랩에서 각 평가항목에 대한 기술적 의견 공개를 취하함에 따라 해당제품에 대한 평가내용을 삭제하였다.

(회원사에서 해당 자료를 별도 요청하는 경우 제조사와 협의 후 제공 예정)

6. 트렌드마이크로 / Apex One

■ 위원회 제품 총평

트렌드마이크로는 통합된 사이버 보안 기술 아키텍처로서 개별 엔드포인트, 네트워크 및 클라우드 제품을 함께 제공하는 연계된 위협 방어를 할 수 있다. 한 조사에 따르면 조직 중 62 %가 단일 엔터프라이즈급 벤더로부터 사이버 보안 제품의 대부분을 구매할 의사가 있다고 했다. 예를 들어 TippingPoint IDS / IPS는 트렌드마이크로의 멀웨어 탐지 샌드박스인 Deep Discovery와 긴밀하게 통합되어 있으며 Trend Micro의 클라우드 워크로드 보안 솔루션인 Deep Security는이 두 제품과 통합되어 있다. 비즈니스 전략의 일환으로 개별 도구를 트랜드마이크로 제품으로 교체하고 향상된 위협 예방 / 탐지와 같은 통합 이점을 활용하여 보안 작업을 간소화할 수 있다.

EDR을 이용하는 조직 중 자체적으로 탐지/대응 도구를 배포, 학습 또는 작동 할 수 있는 자원이나 기술이 없는 경우가 많다. 이러한 고객을 도와주기 위해 트렌드마이크로는 자사 제품을 보완하는 Managed Detection & Reponse (MDR)서비스를 제공한다고 한다.

■ 벤더가 말하는 제품 특징

트렌드마이크로의 엔드포인트 보안제품을 리브랜딩하여 출시한 Apex One™은SaaS형태와 On-Premise 구축 환경에서 단일 에이전트로 구현된 보안 기능을 통해 엔드포인트 보안을 재정의한다. Apex One™ 탐지 및 대응을 자동화하고 상세 분석과 구현 가능한 인텔리전스를 제공한다. 지난 몇 년 동안 EDR (Endpoint Detection & Response) 시장이 확장되며, 보안 분석가들은 엔드포인트 위협 탐지의 상황과 원인을 더 잘 파악할 수 있었고 위협 인텔리전스 및 가설을 기반으로 위협 검색을 수행 할 수 있게 되었다. 하지만, EDR 기능은 자동화된 탐지 및 응답 기능과 분리된 영역에 있어 결과적으로 수동 처리를 더욱 더 요구하고 있다.

Trend Micro Apex One™은 고객이 직면 한 가장 긴급한 엔드포인트 보안 문제를 해결할 수 있는 솔루션이 될 것으로 기대를 모으고 있다. 효과적으로 기업의 엔드포인트를 보호하기 위해서는 다계층(Multi-Layered)의 보안이 필요하며, 이는 Trend Micro Apex One™ 의 기본적인 특징 중 하나이다. Apex One™은 전통적인 AV를 대체하거나 차세대 엔드포인트 보안 그리고 EDR 적용에 어려움을 겪고있는 기업에게 최적화된 차세대 EDR이다.

Trend Micro Apex One ™은 다음 세 가지 주요 기능을 제공한다.
자동화 된 탐지 및 대응(Automated Detection & Response)
가시성 및 실행 가능한 통찰력 제공(Insightful investigation and visibility)
올인원(All-in-one)

분류	기능	내용	답변 (O,X,△,N/A)
탐지엔진 및 기술	알려진 악성코드 탐지 기술 제공	알려진 악성코드에 대한 탐지명 및 해당 정보를 제공해야함 -->트렌드마이크로 자체 패턴을 사용하여 탐지되는 악성코드명(BKDR_BINLODR.ZNFJ-A, TSPY_TRICKBON.THOIBEAI 등)으로 표시되며, 해당 탐지명을 클릭하면 트렌드마이크로 Virus Encylopedia 웹페이지로 링크되어 해당 악성코드의 정보 페이지를 표시함.	O
	네트워크 IPS 공격 탐지 기술제공	네트워크레벨의 취약점 공격등의 위협을 탐지해야함 -->호스트 기반 IPS 인 Integrated Vulnerability Protection(iVP)에 의하여 네트워크 레벨의 취약점 공격을 탐지하고 차단함.	O
	평판데이터를 이용한 신종 위협 탐지	파일에 대한 정보를 기반으로 알려지지 않은 위협을 탐지 해야함 -->2008 년부터 사용되고 있는 파일 평판 기반의 클라우드 패턴을 이용하여 신종 악성코드를 탐지함	O
	파일리스 공격 탐지	파워쉘등을 이용한 파일리스 공격을 탐지 해야 함 -->Dynamic Memory Scan 을 포함한 동작모니터링 기능으로 파워쉘을 이용한 파일리스 공격 탐지	O
	행위기반분석을 이용한 신종 위협 탐지	문서 및 실행 파일을 가상 환경 및 물리 시스템에서 실행 및 분석하여 알려지지 않은 위협을 탐지 해야함 -->자사 샌드박스 분석장비(Deep Discovery Analyzer)와 연동하여 의심스러운 파일을 샌드박스 분석장비로 전송하고, 분석결과 악성으로 판단된 경우 해당 파일을 의심파일(Suspicious	O

분류	기능	내용	답변 (O,X,△,N/A)
		Object)로 분류하고 전체 엔드포인트에서 이를 탐지시 격리하도록 조치	
	상관관계 분석기술을 이용한 연계분석	Endpoint/network/Email 에서 유입되는 위협을 통합하여 분석 및 조치가 가능해야함 -->네트워크 APT 장비(Deep Discovery Inspector), 이메일 APT 장비(Deep Discovery Email Inspector)에서 유입되는 악성코드와 엔드포인트에서 수집되는 악성코드를 상호간 연계하여 악성일 경우 격리 조치함.	O
	심각도 제공	관리자가 우선 조치를 위해 각 탐지한 이벤트별 확인가능 한 심각도 정보를 제공해야함 (critical 에서 -information 등급까지) -->Critical Threat 타입을 Ransomware, Known APT, Social engineering attack, Vulnerability attack, Lateral movement, Unknown threat, C&C callback 으로 구분하여 심각도를 제공함	O
	지역별 공격정보 표시	지역별 실제 공격 정보를 표시 -->대시보드의 Operation Center 에서 지역별 또는 Active Directory 그룹별, IP 주소 세그먼트별로 공격 정보를 표시	O
	unknown 탐지 대쉬보드	알려지지 않은 파일에 대한 분석수 대쉬보드 표시 -->대시보드에서 Unknown Threats 위협 탐지수 표시	O
	알려진 악성코드 탐지 기술		

분류	기능	내용	답변 (O,X,△,N/A)
인시던트 분석 정보	- 바이러스 탐지명	확인가능한 바이러스 탐지명 제공 -->악성코드 탐지명 제공	O
	- 바이러스 위험도 표시	해당 악성코드의 위험도 표시 제공 -->악성코드 탐지명에 링크된 Virus Encyclopedia 에 위험도 명시	O
	- 개괄 탐지 내용 표시	탐지한 알려진 악성코드에 관련된 내용이 설명된 페이지를 제공해야함 -->악성코드 탐지명에 링크된 Virus Encyclopedia 에 악성코드 정보 명시	O
	네트워크 IPS 공격 탐지 기술		
	- 내부 사용자 IP 표시	내부 사용자의 주소를 표시해야함 -->Destination IP 주소(내부 사용자 주소)와 Source IP 주소를 모두 표시함	O
	- 외부 공격자 IP 표시	외부 공격자 IP 의 정보를 표시해야함 -->Destination IP 주소와 Source IP 주소(주로 공격자 주소)를 모두 표시함	O
	- 외부 공격자 IP 의 정보 제공	공격자 IP 의 평판 및 위협정보, 위치등을 제공해야함	O
	- 다운로드/접속 URL 표시	접속 URL 을 표시해야함	O
	- 다운로드/접속 URL 의 정보 제공	표시된 URL 에 대해서 평판 정보 및 위협 상태를 표시해야함	O

분류	기능	내용	답변 (O,X,△,N/A)
	평판데이터를 이용한 신종 위협 탐지 기술		
	- 의심스러운 파일의 탐지	의심스러운 파일의 탐지가 가능해야함 -->평판정보 조회와 머신러닝을 통하여 패턴에 포함되어 있지 않은 의심스러운 파일을 탐지	O
	- 발생시간 표시	처음 발견된 시간을 표시해야함	O
	- 사용자수 표시	현재 해당파일을 사용하고 있는 사용자수를 표시해야함	O
	- 파일 서명 정보 표시	발견된 파일의 제작자 서명이 있는 경우 표시가 가능해야함	O
	행위분석 탐지 기술		
	- 전체 행위 데이터 표시	프로세스가 실행되어 하는 모든 동작을 분석 및 표시 -->샌드박스 분석레포트를 통하여 프로세스의 동작 정보 표시	O
	- 의심스러운 행위만 분류하여 표시	의심스러운 행위의 분류하여 표시 -->High, Medium, Low 레벨로 나누어 의심스러운 행위 표시	O
	- 악성행위만 분류하여 표시	악의적인 행위만 분류하여 표시 -->샌드박스 분석 레포트에서 악의적인 행위 강조	O
	상관관계 분석		
	- 인시던트 분석을 위한 개요 표시	공격자, 표적공격 여부, 영향받은 시스템, 공격에 사용된 파일 정보를 한눈에 파악할 수 있도록 제공	O
	- 내부 IP 와 관련된 인시던트 표시	내부 IP 와 관련된 인시던트 정보를 같이 표시 해야함	O

분류	기능	내용	답변 (O,X,△,N/A)
	- 외부 IP 와 관련된 인시던트 표시	외부 IP 와 관련된 인시던트 정보를 같이 표시 해야함	O
	- 해당 파일과 관련된 인시던트 표시	파일과 관련된 인시던트 정보를 같이 표시 해야함	O
	- 동일한 공격의 그룹핑 지원	동일한 파일 IP 등의 정보를 묶어서 캠페인으로 관리할수 있는 기능을 지원해야함	O
	활성화된 공격의 표시	실제 활동중인 공격을 Active 로 표시가 가능해야함	O
	인텔리전스 기술		
	- 공격자 정보 제공	인텔리전스 평판 지수, 악의적 행위(말웨어 또는 C&C 등), 국가정보, 해당 도메인으로부터 다운로드 받은 파일 수, 연결된 마지막 IP	O
	- 동일한 hash 파일의 다른 이름 표시	추가분석을 위한 같은 해쉬값을 가진 다른 파일명의 표시	O
	- 안티바이러스에서 차단여부 확인	안티바이러스에서 차단 되었는지 확인가능	O
EDR Endpoint	의심스러운 파일 분류	단말에서 의심스러운 파일 을 분류 -->RCA 로부터 의심스러운 파일 추출	O
	Hash 검색	단말에서 디스크 Hash 검색 -->특정 Hash 파일 존재 단말 검색	O
	파일검색	단말에서 디스크 파일검색 -->특정 파일 존재 단말 검색	O

분류	기능	내용	답변 (O,X,△,N/A)
	레지스트리 검색	단말에서 디스크 레지스트리 검색 -->특정 레지스트리 존재 단말 검색	O
	파일 실행차단	단말에서 의심파일 실행차단 -->RCA 로부터 의심스러운 파일을 실행차단 조치	O
	시스템격리 및 복원	단말 시스템을 네트웍에서 격리하고 다시 복원 -->대시보드 및 RCA 로부터 의심스러운 악성파일/C&C 가 발견된 단말을 네트워크로부터 격리 및 향후 복원	O
	파일 삭제	의심파일을 악성파일로 확정시 삭제 -->샌드박스 분석 결과 악성으로 탐지될 경우 격리. 또는 바이러스 패턴에 반영될 경우 격리 또는 삭제.	O
	파일 수집	추가 분석을 위해 단말에서 의심파일 수집	O
	타사 악성코드 탐지 내용 조회	VirusTotal 에 Hash 값 조회하여 타사 엔진에서 검출 여부 확인 -->STIX/MITRE Attack 공유 가능	O
	행위분석 요청	행위분석 요청을 위한 파일 전달 -->샌드박스 분석장비로 파일 수집.	O
	시스템 덤프	시스템에 저장된 전체 덤프로그 수집 -->향후 기능 지원 예정	X
	프로세스 덤프	의심되는 프로세스의 덤프로그 수집	O

분류	기능	내용	답변 (O,X,△,N/A)
	단일에이전트	별도에이전트 설치 여부 -->단일에이전트 지원(백신+호스트 IPS+애플리케이션제어+EDR)	O
인시던트 처리	악성코드 샘플 처리 자동화 지원	탐지한 신종파일의 경우 자동으로 단말의 안티바이러스에서 샘플을 신고하는 기능이 제공되야 함	X
	안티바이러스 처리 지원	단말 안티바이러스에서 처리되는 인시던트는 차단이 완료된것으로 관리자에게 표시해야함	O
	인시던트 예외처리	발생한 인시던트가 오탐일 경우 예외처리 하는 기능을 제공 -->의심스러운 파일, IP 주소, URL 을 예외목록에 추가	O
	인시던트 종료지원	관리자가 발생한 이벤트를 처리하고 케이스를 종료하는 케이스 상태 변환 기능을 제공해야함	O
	인시던트 차단지원	관리자가 차단한 이벤트를 endpoint / network / Email 에서 차단이 지원되야함 -->연동하는 엔드포인트 백신, IPS 장비, 이메일보안 솔루션에서 의심 객체를 차단	O
	인시던트 대응 내용 기입	인시던트의 처리 내용을 기입할수 있어야함	O
관리	NTP 설정 지원	시간 동기화를 위해 지원이 가능해야함 -->중앙관리서버는 윈도우 서버에 탑재됨. 윈도우서버의 NTP 사용	O
	SIEM 장비와 연계	Splunk 등의 장비로 로그 전송 지원 -->Syslog 를 통한 로그 전송 지원	O

분류	기능	내용	답변 (O,X,△,N/A)
	관리콘솔 SSL 지원	관리 콘솔은 SSL 로 접속이 가능해야함 -->HTTPS 관리 콘솔 사용	O
리포팅	심각한 인시던트에 대한 리포팅	다양한 분류로 보고가 지원되야함 -->커스터마이즈가 가능한 레포트 제공	O
	전체 인시던트 리포팅	전체 리포트 보고 -->커스터마이즈가 가능한 레포트 제공	O
	리포팅 및 알림 이메일 전송	이메일로 전송이 가능해야함 -->이메일(SMTP), SNMP 를 통한 알림 제공	O

7. 파이어아이/ HX

■ 위원회 제품 총평

파이어아이 HX는 악성코드를 사용해 정찰부터 정보수집, 침투가 이뤄지는 공격 초기 단계뿐만 아니라 권한 상승, 내부 정찰, 내부 확산, 연결 유지(콜백), 목적 달성까지 지능형 공격과 해킹이 이뤄지는 전 단계를 아우른다. 위협 인텔리전스는 공격이 일어나는 순간에 작용해야 그 효력을 발휘할 수 있다. 머신러닝의 품질은 보유한 데이터의 양과 질에 기반한다. 파이어아이는 전 세계에 설치된 센서를 통해 수많은 정보를 수집하고, 그 데이터를 이용해 머신러닝을 학습시켜 나가는 것이다. APT공격 방어에 큰 성과를 보였던 NX, EX에 비해 HX는 이전의 솔루션만큼 파급력이 크지 않은 것이 사실이다. 주변에 HX를 도입하고 있는 곳을 몇 군데 살펴봐도 "잘" 사용하고 있다고 할 수 있는 곳은 그리 많지 않은 것 같다. 계속해서 인텔리전스가 쌓이고, 기술력이 발달하고, 전문가의 조사 분석이 지속되는 사이클이 정착되면 그리 오래지 않아 HX 적용 우수사례를 찾을 수 있을 것 같다.

■ 벤더가 말하는 제품 특징

FireEye HX는 시그니처 기반의 Anti-Virus 엔진과 행동기반의 Exploit Guard 엔진, 인텔리전스 기반 침해 지표를 포함한 다단계 방어기술로 엔드포인트의 위협을 가장 효과적으로 방어가 가능합니다. 또한 공격의 최일선에서 얻은 FireEye의 전문 지식을 바탕으로한 머신러닝 기반의 Malware Guard 엔진을 새롭게 탑재하여 랜섬웨어를 포함한 다양한 신종/변종의 위협들에 대해 효과적으로 차단이 가능합니다.

인텔리전스 기반의 침해 지표들은 단순한 악성코드들에 대한 시그니쳐 정보가 아니라 FireEye의 Mandiant 컨설턴트들이 실제 APT공격에 대한 침해조사를 수행하면서 수집된 공격자의 공격기술들과 프로세스 등을 위협 탐지 정보로 활용하여 실제 조직이 공격그룹의 APT 공격을 가장 빠르고 정확하게 탐지할 수 있는 기술입니다.

FireEye HX는 4개의 탐지 엔진과 침해시스템의 대응을 위한 EDR기능을 모두 단 하나의 에이전트 설치만으로도 운영이 가능하며, 에이전트 형태의 보안프로그램 간의 충돌 회피를 위해 국내 엔드포인트 전문회사와 기술협력관계를 유지하며, 현재 국내 대부분의 보안솔루션 에이전트와 금융권과 관공서의 홈페이지 접속 시 ActiveX 형태로 자동 설치되는 보안프로그램과의 충돌테스트를 모두 완료하여 최고의 안정성을 제공하고 있습니다.

마지막으로 이미 FireEye의 제품을 사용하고 있는 고객사라면, 현재 사용중인 NX와 EX를 연동하여 가상머신에서 분석된 알려지지 않은 위협에 대해 자동으로 침해지표(IOC)를 생성하여 HX와 공유 후 전체 호스트 시스템에 대한 위협 존재유무를 빠르게 조사할 수 있습니다.

분류	기능	내용	답변 (O,X,△,N/A)
탐지엔진 및 기술	알려진 악성코드 탐지 기술 제공	알려진 악성코드에 대한 탐지명 및 해당 정보를 제공해야함 -->OEM 백신 사용	O
	네트워크 IPS 공격 탐지 기술제공	네트워크레벨의 취약점 공격등의 위협을 탐지해야함 -->FireEye NX 와 연동하여 NX 에서 탐지된 위협이 자동으로 HX 로 전송 후 탐지가 가능	△
	평판데이터를 이용한 신종 위협 탐지	파일에 대한 정보를 기반으로 알려지지 않은 위협을 탐지 해야함 -->파일에 대한 평판정보만을 기반으로 위협을 탐지하지는 않음. 이러한 기능은 엄청난 오탐의 위험이 있으므로 제공하지 않음	X
	파일리스 공격 탐지	파워쉘등을 이용한 파일리스 공격을 탐지 해야 함 -->메모리 및 어플리케이션들의 취약점 모니터링 및 IOC 를 통해 파일리스 위협 탐지	O
	행위기반분석을 이용한 신종 위협 탐지	문서 및 실행 파일을 가상 환경 및 물리 시스템에서 실행 및 분석하여 알려지지 않은 위협을 탐지 해야함 -->Exploit Guard 를 통해 알려지지 않은 위협 탐지	O
	상관관계 분석기술을 이용한 연계분석	Endpoint/network/Email 에서 유입되는 위협을 통합하여 분석 및 조치가 가능해야함 -->FireEye CM 을 통해 NX/EX 와의 상관관계 분석을 제공	△

분류	기능	내용	답변 (O,X,△,N/A)
	심각도 제공	관리자가 우선 조치를 위해 각 탐지한 이벤트별 확인가능 한 심각도 정보를 제공해야함 (critical 에서 - information 등급까지) -->HX 에서는 위협이 실제 실행되고 있는 "EXC", "XPLT"와 위험도가 낮은 단순 파일 존재에 대해 "PRS"의 테크로 표시	O
	지역별 공격정보 표시	지역별 실제 공격 정보를 표시 -->지역별 공격정보 표시기능은 제공되지 않음	X
	unknown 탐지 대쉬보드	알려지지 않은 파일에 대한 분석수 대쉬보드 표시 -->알려지지 않은 파일에 대한 분석수는 표시하지 않으며, 알려지지 않은 위협에 감염된 시스템 현황을 대시보드에 표시	△
인시던트 분석 정보	알려진 악성코드 탐지 기술		
	- 바이러스 탐지명	확인가능한 바이러스 탐지명 제공 -->OEM 백신의 탐지명을 통해 정보 제공	O
	- 바이러스 위험도 표시	해당 악성코드의 위험도 표시 제공 -->HX 에서 탐지된 알려진 악성코드에 대해서는 별도의 위험도 표시를 제공하지 않음	X
	- 개괄 탐지 내용 표시	탐지한 알려진 악성코드에 관련된 내용이 설명된 페이지를 제공해야함 -->탐지시간, 탐지 경로, 탐지 파일명 등의 정보 제공	O
	네트워크 IPS 공격 탐지 기술		

분류	기능	내용	답변 (O,X,△,N/A)
	- 내부 사용자 IP 표시	내부 사용자의 주소를 표시해야함 -->내부 victim 시스템의 IP 표시	O
	- 외부 공격자 IP 표시	외부 공격자 IP 의 정보를 표시해야함 -->외부 공격자의 IP 표시	O
	- 외부 공격자 IP 의 정보 제공	공격자 IP 의 평판 및 위협정보, 위치등을 제공해야함 -->FireEye iSight 와 연동 시 기능제공	△
	- 다운로드/접속 URL 표시	접속 URL 을 표시해야함 -->사용자가 접속한 URL 정보를 제공	O
	- 다운로드/접속 URL 의 정보 제공	표시된 URL 에 대해서 평판 정보 및 위협 상태를 표시해야함 -->FireEye iSight 와 연동 시 기능제공	△
	평판데이터를 이용한 신종 위협 탐지 기술		
	- 의심스러운 파일의 탐지	의심스러운 파일의 탐지가 가능해야함 -->Exploit Guard, Malware Guard 등을 통해 의심파일 탐지	O
	- 발생시간 표시	처음 발견된 시간을 표시해야함 -->최초 탐지된 이벤트의 발생시간을 표시	O
	- 사용자수 표시	현재 해당파일을 사용하고 있는 사용자수를 표시해야함 -->특정 파일의 IOC 매칭이 있을 경우 해당 파일이 존재하는 호스트를 표시	O
	- 파일 서명 정보 표시	발견된 파일의 제작자 서명이 있는 경우 표시가 가능해야함 -->파일에 대한 디지털 서명정보 제공	O

분류	기능	내용	답변 (O,X,△,N/A)
	행위분석 탐지 기술		
	- 전체 행위 데이터 표시	프로세스가 실행되어 하는 모든 동작을 분석 및 표시 -->Timeline 을 통한 행위 데이터 표시	O
	- 의심스러운 행위만 분류하여 표시	의심스러운 행위의 분류하여 표시 -->Triage Summary 를 통해 위협 이벤트와 관련된 의심행위 표시	△
	- 악성행위만 분류하여 표시	악의적인 행위만 분류하여 표시 -->악의적인 행위에 대해 태그를 통한 악의적인 행위 표시	O
	상관관계 분석		
	- 인시던트 분석을 위한 개요 표시	공격자, 표적공격 여부, 영향받은 시스템, 공격에 사용된 파일 정보를 한눈에 파악할 수 있도록 제공 -->분석가가 위협을 손쉽게 분석가능하도록 IOC 를 통해 악성파일 정보, C&C 정보, 감염 시스템 등에 대한 정보 제공	O
	- 내부 IP 와 관련된 인시던트 표시	내부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->이벤트별로 내부 대상 시스템의 IP 가 표기되어 제공되며, Enterprise Search 를 통해 특정 인시던트에 영향받은 내부 시스템 조회 가능	O
	- 외부 IP 와 관련된 인시던트 표시	외부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->특정 외부 IP 정보를 통해 위협에 대한 정보조회가 가능함	O

분류	기능	내용	답변 (O,X,△,N/A)
	- 해당 파일과 관련된 인시던트 표시	파일과 관련된 인시던트 정보를 같이 표시 해야함 -->특정 파일 정보를 통해 위협에 대한 정보조회가 가능함	O
	- 동일한 공격의 그룹핑 지원	동일한 파일 IP 등의 정보를 묶어서 캠페인으로 관리할수 있는 기능을 지원해야함 -->해당 기능은 제공하지 않음	X
	활성화된 공격의 표시	실제 활동중인 공격을 Active 로 표시가 가능해야함 -->실행-Execution, 존재-Presense 태그 표시	O
	인텔리전스 기술		
	- 공격자 정보 제공	인텔리전스 평판 지수, 악의적 행위(말웨어 또는 C&C 등), 국가정보, 해당 도메인으로부터 다운로드 받은 파일 수, 연결된 마지막 IP -->FireEye 의 intelligence 정보를 통해 제작된 IOC 가 지속적으로 업데이트 됨	O
	- 동일한 hash 파일의 다른 이름 표시	추가분석을 위한 같은 해쉬값을 가진 다른 파일명의 표시 -->해시값을 통한 Enterprise Search 전수조사	O
	- 안티바이러스에서 차단여부 확인	안티바이러스에서 차단 되었는지 확인가능 -->백신을 통해 탐지된 파일들을 격리소에서 확인 가능	O
EDR Endpoint	의심스러운 파일 분류	단말에서 의심스러운 파일 을 분류 -->현재는 미지원이나, MVX 연동을 통한 행위분석 지원예정(2019 년 4 분기내)	X

분류	기능	내용	답변 (O,X,△,N/A)
	Hash 검색	단말에서 디스크 Hash 검색 -->Enterprise Search 기능 제공	O
	파일검색	단말에서 디스크 파일검색 -->Enterprise Search 기능 제공	O
	레지스트리 검색	단말에서 디스크 레지스트리 검색 -->Enterprise Search 기능 제공	O
	파일 실행차단	단말에서 의심파일 실행차단 -->Exploit Guard 를 통해 위협파일 실행 차단	O
	시스템격리 및 복원	단말 시스템을 네트웍에서 격리하고 다시 복원 -->시스템 격리와 해제 기능 제공	O
	파일 삭제	의심파일을 악성파일로 확정시 삭제 -->악성으로 탐지된 파일 삭제기능 제공	O
	파일 수집	추가 분석을 위해 단말에서 의심파일 수집 -->의심파일 수집기능 제공	O
	타사 악성코드 탐지 내용 조회	VirusTotal 에 Hash 값 조회하여 타사 엔진에서 검출 여부 확인 -->HX Tools 에서 해당 기능 제공	O
	행위분석 요청	행위분석 요청을 위한 파일 전달 -->현재는 미지원이나, MVX 연동을 통한 행위분석 지원예정(2019 년 4 분기내)	X

분류	기능	내용	답변 (O,X,△,N/A)
	시스템 덤프	시스템에 저장된 전체 덤프로그 수집 -->시스템의 메모리 덤프, 디스크 덤프 등의 수집 기능을 제공	O
	프로세스 덤프	의심되는 프로세스의 덤프로그 수집 -->의심되는 프로세스의 덤프파일 수집 기능 제공	O
	단일에이전트	별도에이전트 설치 여부 -->단일 에이전트 설치를 통해 EDR, EPP 의 모든 기능을 사용	O
인시던트 처리	악성코드 샘플 처리 자동화 지원	탐지한 신종파일의 경우 자동으로 단말의 안티바이러스에서 샘플을 신고하는 기능이 제공되야 함 -->자동으로 파일을 신고할 경우, 내부의 중요 문서파일이 외부로 유출될 위험이 있으므로 해당 기능은 제공하지 않습니다 .	X
	안티바이러스 처리 지원	단말 안티바이러스에서 처리되는 인시던트는 차단이 완료된것으로 관리자에게 표시해야함 -->안티바이러스에서 탐지한 악성파일은 자동으로 치료하여 Quarantines 폴더로 자동 격리	O
	인시던트 예외처리	발생한 인시던트가 오탐일 경우 예외처리 하는 기능을 제공 -->오탐된 파일이나 이벤트에 대해서 원클릭을 통해 손쉬운 예외처리 기능 제공	O
	인시던트 종료지원	관리자가 발생한 이벤트를 처리하고 케이스를 종료하는 케이스 상태 변환 기능을 제공해야함	O

분류	기능	내용	답변 (O,X,△,N/A)
		-->HX Tools 에서 발생된 이벤트에 대해 케이스 상태 변환 기능 제공	
	인시던트 차단지원	관리자가 차단한 이벤트를 endpoint / network / Email 에서 차단이 지원되야함 -->탐지된 이벤트를 호스트에서 차단하는 방식이 아닌, 이벤트가 발생한 시스템을 차단하는 기능을 제공	△
	인시던트 대응 내용 기입	인시던트의 처리 내용을 기입할수 있어야함 -->HX Tools 에서 발생된 이벤트에 대해서 분석가 코멘트를 기입할 수 있음	O
관리	NTP 설정 지원	시간 동기화를 위해 지원이 가능해야함 -->NTP 지원	O
	SIEM 장비와 연계	Splunk 등의 장비로 로그 전송 지원 -->syslog 전송을 통해 Splunk 와 연동 지원	O
	관리콘솔 SSL 지원	관리 콘솔은 SSL 로 접속이 가능해야함 -->SSL 을 통한 관리콘솔 접속	O
리포팅	심각한 인시던트에 대한 리포팅	다양한 분류로 보고가 지원되야함 -->Email, http, syslog 등 다양한 방식으로 심각한 이벤트에 대한 리포팅이 가능	O

분류	기능	내용	답변 (O,X,△,N/A)
	전체 인시던트 리포팅	전체 리포트 보고 -->HX Tools 에서 특정 기간에 대한 전체 탐지된 위협을 CSV, Excel 형태로 리포팅 가능	O
	리포팅 및 알림 이메일 전송	이메일로 전송이 가능해야함 -->Notification 을 이메일로 전달 가능	O

8. 팔로알토네트웍스 / XDR

■ 위원회 제품 총평

팔로알토네트웍스는 EDR은 실패했고 탐지 및 대응에 대한 새로운 접근법을 해야 한다며 XDR을 들고 나왔다. 기존 팔로알토네트웍스의 엔드포인트 보안솔루션인 Traps와 팔로알토네트웍스에서 인수한 기업 섹도의 EDR솔루션을 통합해 "EDR을 뛰어넘는 XDR"을 만들어냈다. 단순 엔드포인트(E)를 넘어서 엔드포인트, 네트워크 및 클라우드 전반에 걸쳐 보안 운영을 개선하는 데 초점을 둔 기술이 XDR이라는 것인데, 아직 명확하게 무엇을 어떻게 하겠다는 것인지 잘 와닿지 않는다. 팔로알토네트웍스의 설명에 따르면 XDR은 SOC 운용을 위한 새로운 제안이며, 상관관계 분석 방식의 SIEM을 도입 한 기업의 수작업에 의한 환경 구축 및 운용을 지원한다고 한다. AI를 사용하여 활성 로그를 받아쓰기도 하고 엔드포인트와 네트워크의 평소 상태를 학습하고, AI가 전문가를 대신하여 비정상적인 행동을 자동으로 감지하는 시나리오로 제공된 Magnifier를 통해 침입 경로와 수단을 시각화 할 수 있다고 한다. 앞으로 새로운 세대의 위협 분석 작업을 자동화·기반화하는 것으로, EDR처럼 사람의 손을 통하지 않고 보안 시스템의 운용이 가능하게 된다고 한다. 기존의 Traps와 비교하여 어떻게 바뀐 것인지에 대해 선언적인 내용 외에 찾아볼 수 있는 정보가 부족했다. 대체적으로 평가기준 전반을 만족하고 있었으나, 별도 인텔리전스 서비스인 AutoFocus를 이용해야만 충족하는 기준이 일부 있었다.

■ 벤더가 말하는 제품 특징

기업의 사이버 보안팀은 인공 지능, 머신러닝 및 자동화 등을 활용하여 설계된 새로운 유형의 탐지 및 대응 제품을 필요로 한다. 올바른 솔루션을 통해 보안 팀은 보안을 강화하고 복잡성을 줄이고, ROI를 획기적으로 향상시킬 수 있다. 팔로알토 네트웍스의 XDR은 위협 탐지 및 대응에 능동적으로 접근한다. 이 솔루션은 네트워크, 클라우드 및 엔드포인트 전반에 걸쳐 데이터에 대한 가시성을 제공하는 동시에 분석 및 자동화 기능을 적용하여 점점 더 정교해지는 오늘날의 위협을 해결한다. XDR은 조직이 성공적인 사이버 공격을 방지하고 보안 프로세스를 강화하고 단순화 시킨다. 사용자, 데이터 및 애플리케이션을 보호함으로써 회사가 전략적 우선 순위에 집중할 수 있기 때문에 사용자에게 더 나은 서비스를 제공하고 디지털 변환 이니셔티브를 가속화 할 수 있다.

기업의 사이버보안팀은 XDR을 통해 다음을 수행할 수 있다.
· 숨겨진, 정교한 위협을 사전에 신속하게 파악할 수 있다.
· 조직 내에서 위협의 모든 소스 또는 위치를 추적한다.
· 보안팀을 운영하는 사람들의 생산성을 높인다.
· 보안에 대한 투자 효과를 극대화 시킨다.

분류	기능	내용	답변 (O,X,△,N/A)
탐지엔진 및 기술	알려진 악성코드 탐지 기술 제공	알려진 악성코드에 대한 탐지명 및 해당 정보를 제공해야함 -->Endpoint Security Solution Traps 와 차세대방화벽 Threat Prevention(IPS/AV/Anti-Spyware) 의 기능과 연동하여 탐지 및 정보 제공	△
	네트워크 IPS 공격 탐지 기술제공	네트워크레벨의 취약점 공격등의 위협을 탐지해야함 -->네트워크 센서 역할을 하는 차세대방화벽의 Treat Prevention(IPS/AV/Anti-Spyware)기능을 통해 네트워크레벨의 알려진 취약점 공격 대응 Endpoint 단에서는 Exploit 이 취약성을 야기 할시 발생되는 OS 의 이상 현상을 탐지는 독자적인 기능을 통해 Signauture 가 없는 zero-day Exploit 도 탐지 차단 가능(Traps 가 해당 기능 수행)	○
	평판데이터를 이용한 신종 위협 탐지	파일에 대한 정보를 기반으로 알려지지 않은 위협을 탐지 해야함 -->일부 평판 정보를 참조/제공 하나 평판 기술은 비교적 부정확한 경우가 많으므로 악성 파일 형태적 특성의 머신러닝 결과의 시그니처 기반이 우선	○
	파일리스 공격 탐지	파워쉘등을 이용한 파일리스 공격을 탐지 해야 함 -->Endpoint Security solution Traps + Behaviour Indication of Compromised(BIoCs : 행동기반 이상 행위 탐지 패턴) 기능으로 탐지	○
	행위기반분석을 이용한 신종 위협 탐지	문서 및 실행 파일을 가상 환경 및 물리 시스템에서 실행 및 분석하여 알려지지 않은 위협을 탐지 해야함	○

분류	기능	내용	답변 (O,X,△,N/A)
		-->Endpoint Security solution Traps + Behaviour Indication of Compromised(BIoCs : 행동기반 이상 행위 탐지 패턴) 기능으로 탐지	
	상관관계 분석기술을 이용한 연계분석	Endpoint/network/Email 에서 유입되는 위협을 통합하여 분석 및 조치가 가능해야함 -->EDR 솔루션 자체적 기능으로 제공	○
	심각도 제공	관리자가 우선 조치를 위해 각 탐지한 이벤트별 확인가능 한 심각도 정보를 제공해야함 (critical 에서 -information 등급까지) -->탐지된 이벤트(악성코드)별 분석 보고서에서 심각도 정보를 제공	○
	지역별 공격정보 표시	지역별 실제 공격 정보를 표시 -->Threat Intelligence Service "AutoFocus"를 추가 연동하여 해당 정보 제공 가능	△
	unknown 탐지 대쉬보드	알려지지 않은 파일에 대한 분석수 대쉬보드 표시 -->Query 기능을 이용해 해당 정보를 확인 할수 있도록 지원, GUI 기반의 Query builder 인터페이스를 제공함으로 손쉬운 사용 가능	△
인시던트 분석 정보	알려진 악성코드 탐지 기술		
	- 바이러스 탐지명	확인가능한 바이러스 탐지명 제공 -->AV Signature 패턴에서 정보 제공	○
	- 바이러스 위험도 표시	해당 악성코드의 위험도 표시 제공 -->AV Signature 패턴에서 정보 및 Unknown 분석 결과 레포트에서 제공	○

분류	기능	내용	답변 (O,X,△,N/A)
	- 개괄 탐지 내용 표시	탐지한 알려진 악성코드에 관련된 내용이 설명된 페이지를 제공해야함 -->AV Signature 패턴 정보, Sandbox 분석(Unknown) 레포트, EDR, Virustotal 등의 정보를 UI 상에서 링크 및 페이지 형태로 제공	○
	네트워크 IPS 공격 탐지 기술		
	- 내부 사용자 IP 표시	내부 사용자의 주소를 표시해야함 -->기본 기능으로 제공	○
	- 외부 공격자 IP 표시	외부 공격자 IP 의 정보를 표시해야함 -->기본 기능으로 제공	○
	- 외부 공격자 IP 의 정보 제공	공격자 IP 의 평판 및 위협정보, 위치등을 제공해야함 -->기본 제공 및 Threat Intelligence Service "AutoFocus"를 추가 시 더 확장된 정보를 제공	○
	- 다운로드/접속 URL 표시	접속 URL 을 표시해야함 -->기본 제공 및 Threat Intelligence Service "AutoFocus"를 추가 시 더 확장된 정보를 제공	○
	- 다운로드/접속 URL 의 정보 제공	표시된 URL 에 대해서 평판 정보 및 위협 상태를 표시해야함 -->네트워크 행위 분석 결과로 해당 정보 제공	○
	평판데이터를 이용한 신종 위협 탐지 기술		
	- 의심스러운 파일의 탐지	의심스러운 파일의 탐지가 가능해야함 -->기본 기능으로 제공	○

분류	기능	내용	답변 (O,X,△,N/A)
	- 발생시간 표시	처음 발견된 시간을 표시해야함 -->기본 기능으로 제공	○
	- 사용자수 표시	현재 해당파일을 사용하고 있는 사용자수를 표시해야함 -->Query 기능을 통해 도출, GUI 기반의 Query builder 인터페이스 지원하여 직관적으로 사용 가능	○
	- 파일 서명 정보 표시	발견된 파일의 제작자 서명이 있는 경우 표시가 가능해야함 -->기본 기능으로 제공	○
	행위분석 탐지 기술		
	- 전체 행위 데이터 표시	프로세스가 실행되어 하는 모든 동작을 분석 및 표시 -->기본 기능으로 제공	○
	- 의심스러운 행위만 분류하여 표시	의심스러운 행위의 분류하여 표시 -->BIoCs(행동 기반 이상행위 패턴) 및 UBA(머신 러닝 기반의 행위 분석) 기능을 통하여 도출	○
	- 악성행위만 분류하여 표시	악의적인 행위만 분류하여 표시 -->BIoCs(행동 기반 이상행위 패턴) 및 UBA(머신 러닝 기반의 행위 분석) 기능을 통하여 도출	○
	상관관계 분석		
	- 인시던트 분석을 위한 개요 표시	공격자, 표적공격 여부, 영향받은 시스템, 공격에 사용된 파일 정보를 한눈에 파악할 수 있도록 제공 -->기본 기능으로 제공	○

분류	기능	내용	답변 (O,X,△,N/A)
	- 내부 IP 와 관련된 인시던트 표시	내부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->Query 기능을 통해 도출, GUI 기반의 Query builder 인터페이스 지원하여 직관적으로 사용 가능	○
	- 외부 IP 와 관련된 인시던트 표시	외부 IP 와 관련된 인시던트 정보를 같이 표시 해야함 -->Query 기능을 통해 도출, GUI 기반의 Query builder 인터페이스 지원하여 직관적으로 사용 가능	○
	- 해당 파일과 관련된 인시던트 표시	파일과 관련된 인시던트 정보를 같이 표시 해야함 -->Query 기능을 통해 도출, GUI 기반의 Query builder 인터페이스 지원하여 직관적으로 사용 가능	○
	- 동일한 공격의 그룹핑 지원	동일한 파일 IP 등의 정보를 묶어서 캠페인으로 관리할수 있는 기능을 지원해야함 -->Threat Intelligence Service "AutoFocus"를 추가 연동하여 해당 정보 제공 가능	△
	활성화된 공격의 표시	실제 활동중인 공격을 Active 로 표시가 가능해야함 -->기본 기능으로 제공	○
	인텔리전스 기술		
	- 공격자 정보 제공	인텔리전스 평판 지수, 악의적 행위(말웨어 또는 C&C 등), 국가정보, 해당 도메인으로부터 다운로드 받은 파일 수, 연결된 마지막 IP -->Threat Intelligence Service "AutoFocus"를 추가 연동하여 해당 정보 제공 가능	△

분류	기능	내용	답변 (O,X,△,N/A)
	- 동일한 hash 파일의 다른 이름 표시	추가분석을 위한 같은 해쉬값을 가진 다른 파일명의 표시 -->Query 기능을 통해 도출, GUI 기반의 Query builder 인터페이스 지원하여 직관적으로 사용 가능	○
	- 안티바이러스에서 차단여부 확인	안티바이러스에서 차단 되었는지 확인가능 -->Endpoint Security solution Traps 와의 연동하여 기능 제공	○
EDR Endpoint	의심스러운 파일 분류	단말에서 의심스러운 파일 을 분류 -->Endpoint Security solution Traps 를 통해 지원	○
	Hash 검색	단말에서 디스크 Hash 검색 -->Endpoint Security solution Traps 를 통해 hash 기반의 Disk search 수행	○
	파일검색	단말에서 디스크 파일검색 -->파일명/확장자명 등으로 검색이 가능하며 와일드 카드 사용 가능	○
	레지스트리 검색	단말에서 디스크 레지스트리 검색 -->기본 기능으로 제공	○
	파일 실행차단	단말에서 의심파일 실행차단 -->EndPoint Security solution Traps 가 EDR 호스트 로그 수집기능과 악성코드 탐지 기능을 수행 하여 지원	○
	시스템격리 및 복원	단말 시스템을 네트웍에서 격리하고 다시 복원 -->EndPoint Security solution Traps 가 EDR 호스트 로그 수집기능과 해당 기능을 수행 하여 지원	○

분류	기능	내용	답변 (O,X,△,N/A)
	파일 삭제	의심파일을 악성파일로 확정시 삭제 -->EndPoint Security solution Traps 가 EDR 호스트 로그 수집기능과 악성코드 탐지 기능을 수행 하여 지원	○
	파일 수집	추가 분석을 위해 단말에서 의심파일 수집 -->해당기능 차기 버전에서 지원 예정	X
	타사 악성코드 탐지 내용 조회	VirusTotal 에 Hash 값 조회하여 타사 엔진에서 검출 여부 확인 -->UI 상에 링크를 통하여 제공	○
	행위분석 요청	행위분석 요청을 위한 파일 전달 -->기존 분석 이력이 없는 파일은 Unknown 으로 정의하고 자동으로 분석 시스템(Sandbox)에 전달	○
	시스템 덤프	시스템에 저장된 전체 덤프로그 수집 -->이벤트 발생시 메모리 덤프 생성 및 필요 시 UI 상에서 수집 요청 가능	○
	프로세스 덤프	의심되는 프로세스의 덤프로그 수집 -->이벤트 발생시 메모리 덤프 생성 및 필요 시 UI 상에서 수집 요청 가능	○
	단일에이전트	별도에이전트 설치 여부 -->Endpoint Security Solution Traps agent 가 EDR 에 대한 단일 Agent 역할을 수행	○

분류	기능	내용	답변 (O,X,△,N/A)
인시던트 처리	악성코드 샘플 처리 자동화 지원	탐지한 신종파일의 경우 자동으로 단말의 안티바이러스에서 샘플을 신고하는 기능이 제공되야 함 -->신종 Unknown 악성파일은 자동으로 분석시스템(Sandbox 으로 전달 분석 되고 AV 패턴 작성으로 위한 샘플로 제공 됨	○
	안티바이러스 처리 지원	단말 안티바이러스에서 처리되는 인시던트는 차단이 완료된것으로 관리자에게 표시해야함 -->EndPoint Security solution Traps 가 EDR 호스트 로스 수집기능과 악성코드 탐지 기능을 수행 하여 지원	○
	인시던트 예외처리	발생한 인시던트가 오탐일 경우 예외처리 하는 기능을 제공 -->다양한 형태의 Exception 및 White list 처리 기능 제공	○
	인시던트 종료지원	관리자가 발생한 이벤트를 처리하고 케이스를 종료하는 케이스 상태 변환 기능을 제공해야함 -->인시던트 관리 워크플로우 인터페이스를 제공	○
	인시던트 차단지원	관리자가 차단한 이벤트를 endpoint / network / Email 에서 차단이 지원되야함 -->Endpoint 는 Traps 의 기능, Network 과 Email 은 차세대 방화벽의 기능으로 차단 기능 제공	○
	인시던트 대응 내용 기입	인시던트의 처리 내용을 기입할수 있어야함 -->인시던트 관리 워크플로우 인터페이스를 제공	○

분류	기능	내용	답변 (O,X,△,N/A)
관리	NTP 설정 지원	시간 동기화를 위해 지원이 가능해야함 -->EDR 시스템에 분석을 위한 정보(로그)를 제공하는 시스템 시간으로 시간 기록, 자체는 NTP 동기화 기능 미제공	X
	SIEM 장비와 연계	Splunk 등의 장비로 로그 전송 지원 -->로그 포워딩 기능을 제공	○
	관리콘솔 SSL 지원	관리 콘솔은 SSL 로 접속이 가능해야함 -->기본 기능으로 제공	○
리포팅	심각한 인시던트에 대한 리포팅	다양한 분류로 보고가 지원되야함 -->고위협 파일과 Host 에 대한 보고서 제공	△
	전체 인시던트 리포팅	전체 리포트 보고 -->기본 기능으로 제공	○
	리포팅 및 알림 이메일 전송	이메일로 전송이 가능해야함 -->기본 기능으로 제공	○

Part IV. 보고서 제작 후기

EDR 솔루션에 대한 Security Consumer Report 를 만들기 시작할 때만 해도 이렇게 시간이 많이 걸리고, 힘든 작업이 될 줄은 미처 몰랐다. 시작은 이상징후 탐지 시스템에 대한 CR 제작이었으나, n 논의 과정에서 "이상징후"라는 단어에서 오는 인식의 차이가 굉장히 큼을 알게 되었고, 그 결과 CR 의 주제의 범위를 좁혀 EDR 로 정해졌다.

가트너는 일찍부터 EPP(Endpoint Prevention Platform)와 EDR(Endpoint Detection & Response)를 구분해서 시장을 나눴지만, 국내에서는 EPP 와 EDR 을 구분하지 않고 EDR 로 통칭해서 부른 적도 있었다. 지금은 어느정도 교통정리가 된 것 같지만...

기업 입장에서 백신(AV)은 참 편한 보안 솔루션이다. 도입을 하기만 하면 바로 사용가능하고, 효과도 즉시 발생한다. 패턴업데이트만 정기적으로 해 주면 별도로 시간을 들일 필요가 없다. 그런데 EDR 은 그렇지 않다. 벤더마다 용어는 다르지만 학습기간이 필요하고 정책을 수립하고 적용하는 기간이 필요하다. 완전 자동화면 얼마나 좋을까 싶지만 오탐의 우려도 있고, 인공지능의 성능도 많이 좋아졌지만 가치판단의 문제에 있어서는 아직 기계를 100% 신뢰할 수는 없는 단계라 사람의 손을 빌릴 수 밖에 없다. 단순 오퍼레이터가 필요한 것이 아니라 분석역량이 있는 전담 담당자가 있어야 EDR 에서 쏟아지는 정보들을 제대로 처리하고 활용할 수 있는 것이다. POC, BMT 를 거쳐 도입했으니 초기 세팅 후에는 알아서 돌아가기를 바란다면 너무 큰 욕심이라 하겠다.

더 많은 EDR 솔루션을 담고 싶었지만, 솔루션 업데이트 일정관계로, 제품 컨셉과 평가 항목과의 차이 등으로 CR-EDR 에 관심을 보여주고도 보고서에 참여하지 못한 솔루션들이 있는 점이 아쉽다. 추후에 본 보고서에 대한 업데이트가 이루어진다면, 해당 시점에 솔루션을 추가해서 보고서를 보강했으면 했으면 하는 바람이 있다.

업무가 바쁜 와중에도 퇴근 이후에 사무국 회의실에 모여 샌드위치 하나로 허기를 달래가며 보고서 작성에 참여해 준 제작위원회 분들께 정말 큰 감사를 드린다. 이번 CR-EDR 제작을 위해 온라인 협업도구를 처음 사용했다. 생각만큼 잘 활용하기가 쉽지 않았는데. 다음 번 보고서에서는 보다 높은 수준의 활용을 할 수 있게 되길 희망한다.

올해 만들게 될 다음 Consumer Report 의 주제는 아직 정해지지 않았지만, Consumer Report 를 만들어보고 싶은 주제가 있으면 언제든지 사무국으로 연락주시라. 너무나도 당연한 얘기지만, Consumer Report 의 주제는 회원들이 원하는 주제로 결정된다. 그리고 함께 참여하고 싶은 분들의 신청도 언제나 환영이다.