2021-04-09(금) 제 45회 GIT Web Talk_센티넬원

NO	Name(질문)	질문내용	Name(답변)	답변내용
1	김도윤	코로나 시대로 재택근무는 이제 일상이 되었습니다. 이로인해 엔드포인트에서 보안문제가 점차 대두되고 있습니다. 빠르게 늘어나는 신/변종 악성코드는 기존 시그니처 기반 백신을 무력화시키고 있고 파일리스형태의 공격은 파일 검사 기반 백신을 우회하여 침투할 수도 있고요. 보안의 최전선에 있는 보안담당자들에겐 이런 기존 백신의 탐지/치료만으로는 한계를 뼈저리게 느끼고 있습니다. 센티넬원은 어떻게 악성파일 및 행위를 사전 차단하고 사후 대응 및 사고분석을 어떻게 처리하는지 궁금합니다.	조소연	여러 방식의 차단 기능을 지원 합니다. 차단 방식은 Mitre Att&ck에서 정의한 악성행위 자체를 차단 하는 기능에 더해 Reputation 에 의한 차단 동작도 합니다. 그리고 모든 프로세스 및 Endpoint 행위의 모든 것을 기록하기 때문에 EDR 기능으로 사후 대응이 가능합니다.
2	임지현	지능형 공격인 APT 공격의 경우 EPP만으로는 막기 어렵습니다 그렇기 때문에 가시화 및 대응이 가능한 EDR 솔루션 얘기도 나오는 건데, 모든 보안 위협에 대해서 센티넬원은 하나의 통합 엔드포인트 보안프로그램으로 가능한가요?	센티넬원 유세종	센티넬원은 EPDR(Endpont Protection Dectection Response)라고 부르며, EPP의 기능과 EDR의 기능을 하나의 Agent와 하나의 관리 ui에서 위협의 대한 탐지 및 차단, 분석이 가능 합니다.
3	이형준	스스로 판단하여 자동 처리한다면 False positive 이벤트는 좀 문제가 있지 않을까요?	센티넬원 최충성	탐지는 기본적으로 Mitre Att&ck에서 정의한 정보를 기반으로 행위를 탐지하기 때문에 오탐률은 거의 없다고 보셔도 무방합니다. 추가적으로 정상행위에 대한 다양한 예외처리 기능을 지원합니다.
4	손정환	자율형의 의미를 인공지능 적용으로 봐도 되는가요	센티넬원 최충성	네 AI를 이용하여 행위 탐지 및 차단 기능을 제공합니다.
5	이세원	보안에서 가장 중요한 것이 결국 보안정책을 강화하여 여러가지 다양한 루트로 접근하는 유해요소를 막아내는 것일텐데요 계속 진화하는 악성 바이러스, 랜섬웨어, 해킹공격들이 늘어나고 있는 추세에서 이러한 부분에 대한 보안관리 정책은 어떻게 가져가시는지 궁금합니다.	센티넬원 최충성	AI 기반의 탐지 기술을 보유하고 있으므로 비지도학습 및 지도학습의 데이터를 통해 자동화 정책 적용을 받고 있습니다.
6	김홍준	기존의 사용하는 백신을 완벽하게 대체하려면 기존의 백신과의 성능비교를 했을텐데요 백신성능은 어느정도라고 봐야할까요?	센티넬원 최충성	시그니처 및 HASH 기반의 탐지 기술을 보유한 기존 백신의 기능을 모두 포함하고 있으며, 추가적으로 SentinelOne 스토리라인을 가지는 악성 행위를 탐지하는 솔루션으로 기존 백신과는 차별성이 있습니다.
7	임지현	Threat 가운데 대부분을 차지하는 Zero day attack에 대한 솔루션과 static AI 솔루션으로 탐지하지 못하지만 SentinelOne의 솔루션으로 탐지하는 Threat의 비율은 어느정도 인가요?	센티넬원 유세종	센티넬원은 Static AI 엔진과, Behavioral AI 엔진을 해서 위협의 대해서 탐지 및 차단 기능을 제공 합니다. 일반적으로 Static AI엔진에서 위협 탐지가 되며, 행위 분석이 필요한 랜썸웨어, fileless 등의 공격 등은 Behavioral AI엔진에서 탐지 및 차단이 가능합니다.
8	정광진	자율적으로 엔드포인트 악성 행위에 대해 탐지 차단할 경우 오탐 행위에 대한 차단율은 어느정도나 되는지?와 설치된 에이전트의 자원 점유율은 어느정도나 되는지? 궁금합니다.	센티넬원 최충성	오탐 비율은 거의 없다고 보셔도 무방합니다. 에이전트 자원 점유율은 초기 Disk Full scan을 제외하고 1~3% 미만입니다.
9	전승호	자율형 사이버 보안 SentinelOne 솔루션 관련 최근 이슈와 해결사례가 궁금합니다.	센티넬원 유세종	작년말 전세계 크게 위협이 된 SolarWinds의 대한 솔루션 업체의 대한 해킹 사례가 컸으며, 전통적인 안티바이러스 솔루션에서는 탐지를 못 하였습니다. 센티넬원은 행위분석을 통해 위협 분석을 하여 사전에 차단이 되는 좋은 사례가 있습니다.
10	윤성원	최근에 Scalyr 를 인수한것을 알고 있는데 Scalyr이 실시간으로 로그를 분석하는데 강점이 있는 회사인데 Scalyr를 인수하면서 센티넬원의 XDR에 어떤 부분에 영향을 주었는지 궁금합니다. 그러면 향후에는 빅데이터 로그 분석 기능이 추가될 가능성이 있는지요?	센티넬원 최충성	Autonomous나 머신러닝의 수준을 업그레이드 했다고 볼 수 있습니다. 향후의 빅데이터 로그 분석 기능은 확인이 필요합니다.
11	김홍준	기존의 제품을 센티넬원으로 교체하려면 가격경쟁력도 무시하지 못할텐데 이에 대한 의견도 듣고싶습니다.	센티넬원 유세종	새로운 위협의 대해서는 기존 안티바이러스 솔루션으로는 방어하기 힘듭니다. 센티넬원은 새로운 위협의 대응을 위한 고객이 구매 가능한 최적의 비용으로 도입이 가능 합니다.
12	이종원	새로운 악성코드가 생기면 주기적으로 대응하는 보안프로그램이 생기는 건가요?	센티넬원 최충성	새로운 악성코드가 생기더라도 갖고 있는 행위 자체를 탐지하는 기능을 지원하기 때문에 새로운 악성코드에 대응할 수 있습니다.
13	허노정	공격과 방어에 모두 AI가 활용될 수 있을 것 같습니다. 각 측면에서 어떤 식의 발전이 이루어질지 궁금합니다. AI를 이용한 방어의 측면에서 보완할 수 있는 점이 있다면 무엇일지요?	박정수	공격이 지능화, 다양화, 고도화되면서 많은 사람과 시간이 필요하게 되는데 이 부분을 AI로 자동화하면서 효율화할 수 있을 것으로 기대됩니다.
14	이형준	Rogue & Ranger는 일종의 Visibility 관련 서비스인가요?	센티넬원 최충성	내부 네트워크의 기본적인 자산정보를 확인 할 수 있는 기능입니다.
15	방극민	악성코드나 신종 변종 위협에 대해서는 어떤 강점을 지니고 있는지 설명 부탁드립니다	센티넬원 최충성	변종되더라도 악성 행위 자체는 달라지지 않습니다. 행위 자체를 탐지하는 기능을 보유하고 있기 때문에 새로운 보안 위협에 대해서도 대응이 가능합니다.
16	손정환	SentinelOne이 효과를 발휘하는 분야나 기업은 어디가 있는가요	센티넬원 유세종	모든 분야에서 효과적이라고 생각 합니다. 특히 재택근무 때문에 PC가 외부 인터넷에 많이 연결된 기업에는 효과적이라 생각합니다.
17	이형준	ActiveEDR 은 Forensic srevice와 비슷하다고 보아도 되죠?	센티넬원 유세종	ActiveEDR은 EDR이라고 보실 수 있습니다. EPP기능에서 위협을 분석 가능한 EDR기능을 무상으로 제공 합니다. EDR 기능과의 차이점은 정상 파일의 대한 로그는 제공하지 합니다.
18	김수열	새로운 위협정보 업데이트 방법과 주기는? 사용자가 업데이트 주기조정 가능한가요?	센티넬원 최충성	SentinelOne은 SaaS 방식으로 동작하므로 위협정보 업데이트는 자동으로 진행됩니다. 에이전트의 업데이트 주기는 별도로 지정이 가능합니다.
19	전영진	질문을 잘못 드려서 내용을 정정합니다. 지금 박정수 이사님께서 소개해주시고 계신 제품은 Singularity Core인가요? Singularity Control에도 해당되는 내용인지 궁금합니다.	박정수	저희 라이센스는 Core, Control, Complete으로 구성되어 있습니다. Core는 악성코드 대응/복구, Control는 Core 기능 및 방화벽/매체제어, Complete은 정상 파일도 로깅하는 EDR까지 포함된 라이센스입니다. 에이전트는 모두 동일하구요. 라이센스별 기능만 차이가 있습니다.
20	김건호	sentinelone 보안 스토리라인이 이벤트발생 시 리포트형식에 리포팅 시스템이 있는 지 궁금합니다	센티넬원 최충성	리포트 형식의 분석 정보를 확인 및 출력이 가능합니다.
21	한주호	안녕하세요 작년에 비공식적으로 많은 회사들이 AD(Active Directory)서버를 헤커에게 탈취당해 곤란을 겪었습니다 이에 대한 보완은 어떻게 해야 할가요	센티넬원 최충성	서버를 탈취하는 행위 자체는 Mitre Att&ck에서 제시하는 Framework로 진행됩니다. 해당 행위 기반으로 탐지 및 차단 기능을 보유하고 있기 때문에 해당 공격에 대응할 수 있습니다.
22	김홍준	센티넬원과 같은 동종의 제품중에 시장점유는 얼마나 되나요?		
23	윤성원	이미 네트웍과 클라우드에서 제공하는 보안 솔루션이 있다면 또 굳이 새로운 솔루션 XDR 등과 같은 어떻게 보면 중복된 기능을 가지것을 도입하는 거은 낭비가 아닌가요? 그리고 네트웍의 분서을 실시간으로 모니터링 하는 곳에서는 벌써 많은 투자가 이루어져 있는데 이곳에서 그럼 센티넬원의 차별화된 기능은 무엇인가요?	센티넬원 최충성	네트워크 기반의 솔루션은 Device 내에서 이루어지는 행위 자체를 탐지할 수는 없습니다. EDR은 Endpoint 기반으로 프로세스 및 행위 자체를 모두 탐지할 수 있으므로 중복된 기능이라고 볼 수 없으며, 다른 영역의 보안 체계 입니다.
24	정광진	위협정보를 외부에서 지속적으로 업데이트를 할텐데요, 인터넷이 차단된 내부 업무망에서의 위협정보 업데이트는 어떤 방법(중계 등)으로 제공될까요?	센티넬원 최충성	On-Premise 형태의 구축도 가능합니다. 단, HASH값 기반의 Reputation 업데이트 기능은 지원하지 않으나, 악성행위에 대한 탐지가 가능하기 때문에 별도의 업데이트가 필요하지 않습니다.
25	정진희	SentinelOne 대응기술중에 Rogue & Ranger가 사내 네트워크에 있는 에이전트 미설치 단말에 대한 점검이 가능하다고 하셨는데 재택근무나 외부 환경에서 근무하는 직원의 에이전트 미설치 단말에 대한 대응 기술도 있는 것인지 문의드립니다.	센티넬원 최충성	Rogue & Ranger 기능은 동일네트워크 기준에 Agent가 지정된 개수 이상이어야만 동작할 수 있도록 설정이 가능합니다. 일부 자산정보를 확인하기 위한 기능으로 미설치 단말에 대한 보안대응 기능은 아닙니다.
26	김기수	행위기반이면 파일을 가상환경에서 돌려보고 판단하는 건가요?	센티넬원 유세종	센티넬원은 샌드박스와 같이 가상환경에서 분석하지 않고, 센티넬원 에이전트가 설치되어 있는 PC 환경에서 행위를 모니터링하면서 위협의 되는 것에 대한 탐지 및 차단을 제공 합니다.
27	한용운	agent 가 계속 실행되면서 리소스 사용량이 꽤 될거 같은데, 평균 리소스 사용량이 어느정도 되나요?	센티넬원 최충성	Disk Full Scan 을 제외하고 약 1~3% 미만의 리소스 점유율을 갖고 있습니다.
28	윤성원	센티넬원의 가장 큰 장점이 온프레미스, 클라우드, 하이브리드 환경에서 구축이 가능한 것인데이 3가지환경에서 센티넬원 솔루션의 차이점은 무엇인지 궁금하고 백도어, 제로데이 어택 등 잠재적인 보안 공격에 대한 대응은 어떤환경에서 가장 이상적인가요?	센티넬원 유세종	환경의 장점은 고객사 환경에 따라 차이가 있다고 생각합니다. 금융사 처럼 패쇄망에서 운영이 필요한 고객한테는 온프레미스로 구성이 가능하며, 패쇄망이 아닌 고객에는 클라우드를 권장 드립니다. 클라우드의 장점은 관리 콘솔이 자동 업데이트가 되며, 위협 탐지를 위해 파일 평판 서비스를 이용하실 수 있습니다. 또한 재택근무인 경우 일반적으로 보안솔루션은 온프레미스 환경이라면 PC에 새로운 위협을 탐지 및 분석이 어렵습니다. 클라우드 구성이라면 사내/사외에서 PC에 보안을 완벽히 도와드릴 수 있습니다.
29	이형준	오탐이 False negative인가요?	센티넬원 최충성	미탐이 False negative 입니다.
30	이호승	# 현상황 해커가 Cobalt Strike로 저희 서버에 쉘코드를 삽입했고 내부 서버들과 becon 통신을 하면서 서버들이 원격제어를 당했고 최종 어떤 정보가 유출되었는지 알지 못하는 상황입니다. 서버포렌식을해서 Cobalt Strike becon 통신흔적만 찾았습니다. # 궁금한점 1. 만약 센티널원이 있었다면 탐지가 가능했을지 2. 가능한경우 어떤기능을 통해 이러한 APT공격을 탐지할 수 있는지 3. 유출된데이터는 어떤 것인지 포렉식이 가능한지	센티넬원 최충성	탐지가 가능합니다. 관련된 행위와 스크립트 등이 어떠한 경로와 어떠한 커멘드로 실행 됐는지 까지 모두 모니터링이 가능하고 어떠한 데이터를 네트워크를 통해 유출이 됐는지도 함께 확인이 가능합니다.
31	임지현	악성코드 탐지에 인공지능을 활용하려면 학습데이터가 충분히 축적되야 제대로 된 탐지능력이 생길텐데요, 학습 데이터 소스는 어떻게 확보하고, 업데이트 하는지요?	센티넬원 최충성	비지도 학습데이터는 Mitre Att&ck에서 정의한 Framework를 모두 지원하고 있으며 SaaS 형태의 서비스이기 때문에 AI를 통한 학습한 데이터가 자동으로 업데이트 합니다.
32	지정호	새로운 위험에 대한 가시성과 탐지를 높이기 위한 AI 학습 데이터의 양과 질 관리는 어떻게 지원되는지요?학습에 의한 새로운 위험 탐지 능력은 어느 정도 되는 것으로 보시는지요?	센티넬원 최충성	악성 행위의 학습 데이터는 Mitre ATT&CK Framework에서 정의한 모든 행위를 기반으로 합니다. 추가로 AI에서 학습한 데이터를 기반으로 새로운 위협에 대한 대응이 가능합니다.
33	윤성원	셉티넬원의 관리자료 접근시 MFA가 지원하는지 궁금하고 망이 분리된 경우 agent는 각각 설치해야 하는지요 아님 단일 에이젠트로 운영이 가능한지 궁금합니다.	센티넬원 최충성	Agent는 Device 단위로 제공됩니다.
34	전영진	시그니처를 사용하는 백신 소프트웨어는 시그니처 정보 업데이트를 주기적으로 받아야 하는데 SentinelOne은 시그니처를 아예 사용 안하고 시스템을 보호하는 체계이니까 업데이트의 빈도가 낮을 것 같습니다. 일반적으로 업데이트 주기가 어느 정도 되고 있나요?	센티넬원 최충성	SaaS 기반으로 동작하기 때문에 자동 업데이트가 됩니다.
35	김형욱	본사에서 센티널원 에이전트를 깔았는데, 해당 에이전트가 어느정도까지 매니지하고 있는지 궁금합니다.	센티넬원 최충성	모든 프로세스 및 어플리케이션을 제어할 수 있습니다.
36	이형준	PowerShell 공격 이전의 Shell process의 fork 부터 로그를 알 수 있나요?	박정수	가능합니다.
37	한용운	policy 설정을 할 수 있고 inventory기능도 어느정도 있는거 같은데 AD를 대체할 수 있을까요?	센티넬원 최충성	AD를 대체할 수는 없습니다.
38	문태진	랜섬웨어가 걸린 데이터를 제공되는 포렌식 기능을 통해 데이터를 복구하는 성공율은 어느정도인가요? 그리고 포렌식을 통해 어떤 정보 수준까지 침임이나 변경에 대한 내용 들을 알수 있는지요?(예: 침입일, 변경유형 기술, 데이터 전송 유무 등) 그리고 이러한 포렌식 기능을 통해 바로 해당 공격을 바로 신고까지 하는 경로까지 연결시켜줄수 잇는지요? 국내 사례중에 제공되는 포렌식 기능을 이용해서 성공적인 운영사례가 있다면 어떤 사례가 있을까요?	박정수	랜섬웨어 데이터 복구는 대부분 가능합니다. 신고는 현재 지원하지 않습니다. 현재 운영 중인 모든 고객사에서 악성코드 발생 시 차단 및 감염경로 추적에 활용되고 있습니다. 말씀하신 기능들은 모두 지원 가능합니다.
39	문주웅	행위 기반 탐지 엔진은 각 공격기법별 상세 정보를 제공해 줍니다 기업 담당자가 악성코드를 효과적으로 탐지하는 시스템을 구축하는 방법에 대해서 설명해 주세요 그리고 VSS를 효율적으로 활용하는 방법에 대해서 설명해 주세요	박정수	시그니처 기반의 한계는 잘 이해하고 계시리라 생각됩니다. 샘플을 신고하고 패턴을 업데이트하는데 많은 시간이 소요되며 악성코드 공격 시 격리도 직접해야 하므로 많은 어려움이 있습니다. 현재 보안 솔루션에서 지원하지 않는 이슈들을 해결할 수 있는 보안 솔루션을 고려하는게 좋은 방법입니다. VSS는 백업은 아닙니다. 하지만, 랜섬웨어 및 악성코드 공격으로 인한 피해를 즉각 복구할 수 있는 방안으로 이해하시면 됩니다.
40	이형준	Rollback시 사용자에게 Rollback된 화일에 대한 Alert 등을 제공하나요?	센티넬원 최충성	어떠한 이벤트 때문에 동작을 했는지에 대한 Log를 확인할 수 습니다.
41	윤성원	어떤 좋은 보안솔루션도 완벽하지는 않기에 때로는 침해가 발생하는데 예를들어 AI기반 행위 탐지기능을 가지 센티넬원의 XDR이 관리자권한이 침입자에게 넘어갔을 때 치료 및 복구 등 대처는 어떻게 하는지 궁금합니다.	센티넬원 최충성	관리자 권한 탈취에 대한 사전 악성 행동들에 대한 탐지 및 차단이 동작합니다. 탈취 이후에도 네트워크 단절 및 복구 등 다양한 Action을 지원합니다.
42	이상원	1. Agent와 센티넬원 cloud측의 서버와의 통신은 TCP 443으로하는것인지요 ? 2. 센티넬원의 가격정책은 어떻게 되나요 ?	센티넬원 최충성	기본적으로 TCP 443을 사용합니다. 가격 정책은 별도 문의 부탁 드립니다.
43	김홍준	바이러스 공격이 아니더라도 임의로 스냅샷을 롤백할 수도 있는지 궁금합니다.	센티넬원 최충성	이벤트가 발생하여야 롤백할 수 있습니다.
44	윤성원	이사님께서 센티넬원이 Microsoft VSS를 활용한다고 하셨는데 악성코드가 동작하기 전에 VSS 데이터를 지운 경우에도 복구가 가능한가요? 아니면 VSS 데이터 삭제 방지 장치가 별도로 있는지요?	박정수	VSS가 없는 경우는 복구가 되지 않습니다. 대신 삭제 방지 기능을 지원합니다.
45	김민경	스크립트 및 메모리공격 등 악성코드가 HDD파일이 없는 Fileless형태의 공격을 AI기술로 탐지 분석 해결한다고 하셨는데, 랜섬웨어에 의한 데이타 피해는 어떻게 대처할 수 있는가요?	박정수	VSS기능을 활용한 Rollback 및 remediate을 통해 공격 전 상태로 복구할 수 있습니다.
46	한용운	현재 데모환경을 보니까 영문화면으로 되어 있는거 같은데 한글화가 되어 있지 않나요?	박정수	현재는 한글화는 되어 있지 않습니다.
47	윤성원	보안 위협을 AI 기반으로 예방 및 탐지, 대응, 격리, 치료까지 하는 것으로 아는데 AI 기반이므로 오탐에대한 예방은 어떻게 하는지 또 오탐의 비율이 시그니처 기반의 XDR과 비교시 어느정도 감소되는지 궁금합니다.	박정수	오탐은 해쉬, 폴더 기반, 사인너, 웹 브라우저 등 다양한 방식으로 예외처리할 수 있습니다. 통계 데이터는 없지만, 현재 도입된 고객사에서 이슈없이 잘 운영되고 있습니다.
48	김준석	랜섬웨어 발견시 데모에서처럼 시차를 두고 차단하는게 아니라 , 인지하자 마자 차단한다면 피해가 더 줄어들 것 같은데 그렇게 하지는 않는 이유가 있는지요?	박정수	데모이기 때문에 탐지모드로 해서 감염이 된 사례입니다. 실제 운영환경에서는 바로 차단됩니다.
49	김홍준	최근의 랜섬웨어는 파일을 암호화하는데서 벗어나 파일을 탈취하고 탈취한 파일들을 공개하겠다는 위협을 통해 금품을 갈취한다고 하는데요 이러한 행위에 대한 방어도 가능한지 궁금합니다.	박정수	랜섬웨어 및 최근 다양한 해킹 기법을 통해 내부 파일을 외부 탈취하고 있습니다. 이러한 행위들에 대한 행위기반으로 효율적으로 차단이 가능합니다. 시그니처의 경우 다양한 변종들에 대해 모든 패턴을 패턴으로 넣어야 하지만 모든 변종들이 실제로 하는 악성 행위는 동일하므로 효율적으로 대응 가능합니다.
50	윤성원	요즘은 데이터량이 기본이 TB인데 감염된 파일 용량이 1TB라고 하면 복구 시간이 얼마나 소요되는지요?	박정수	복구 시간은 늦어도 수분 내에 이루어 집니다.
51	이민수	SentinelOne의 고유기술중 스토리라인에 대해서 질문드립니다 C&C 통신을 효율적으로 하는 방법에 대해서 질문드립니다 그리고 레지스토리를 효과적으로 변경하는 방법에 대해서 질문드립니다	박정수	스토리라인은 AI에 의해 공격에 사용된 다양한 프로세스, 파일 등 연관된 정보들은 상관 분석하여 분석이 용이하도록 지원해 주는 기술입니다. 악성 행위에 대한 전문지식이 없더라도 스토리라인를 통해 쉽게 이해할 수 있습니다.
52	김명환	행위기반으로 탐지/차단 하신다고 말씀하셨는데, 비정상 행위 후 탐지/차단하면, 이미 피해를 본 상태일텐데요. 행위기반의 보안제품(센티넬원) 도입 시, 보호대상자원에 대해 실시간 사전 백업/스냅샵이 필수조건 인지요?	박정수	악성 행위 후 차단이 아닙니다. 악성 행위 수행 시 바로 차단됩니다. 스냅샷은 필수 조건은 아닙니다. 저희 에이전트 설치 시 자동으로 수행되므로 고객께서 따로 신경쓰실 필요는 없습니다.
53	이형준	백업본 삭제 뿐 아니라, 분석의 소스가 되는 Log의 삭제등이 일어난다면 문제가 있지 않을까요? 센티넬원은 로그를 WORM 매체등에 저장하나요? 그렇다고 해도 관리자 권한의 탈취가 일어났다면 로그를 Disable 시킬 수도 있을 것 같은데요.	박정수	에이전트관련 로그는 모두 로컬 디스크에 저장됩니다. 고객이 원하시는 경우 온프라미스 서버를 WORM매체에 구성해서 정보를 저장할 수는 있습니다. 로컬 디스크 저장된 정보는 모두 보호 기능을 통해 보호됩니다.
54	양성필	랜섬웨어에 의해 암호화된 값에 대한 복구가 가능한지요? 가능하다면 복구 방식은 어떻게 되며, 어느 선까지 복구가 가능한가요? 또 센티넬원 에이전트는 타 솔루션 대비 탐지 및 차단 측면에서 차별성이 있는지 궁금합니다.	박정수	랜섬웨어 감염 시 암호화된 파일을 복호화하는 것이 아니라, 공격 전 파일을 Snapshot기능으로 저장했다가 원래 상태로 복구시키는 기능을 제공합니다. 타 솔루션 대비 강점은 악성코드가 수행한 작업 내용을 저장 후 원래 상태로 remediate 및 rollback시키는 기능을 제공합니다.
55	문태진	방근 설명해 주신 스토리 라인이 포렌식 기능안에 포함된 기능인거 같은데 맞나요? 스토리 라인을 적용해서 복구한 국내 대표적인 사례가 있을까요?	박정수	포렌식 기능은 remote shell에서 제공합니다. 모든 고객사에서 악성코드 공격 시 remediate 및 rollback 기능을 통해 악성코드로 부터 보호받고 있습니다.
56	한승일	파일리스 공격에 대한 행위도 탐지가 되는지요?	박정수	특화된 엔진을 통해 차단 가능합니다.
57	문주웅	기업 담당자가 실행된 프로세스간 연관관계 분석을 효과적으로 하는 방법에 대해서 질문드립니다 그리고 악성 행위와 연관된 프로세스 분석 관련하여 효과적인 Mitre Attack 기준코드에 대해서 설명해 주세요	박정수	Stroyline이라는 특허 기술로 제공하고 있습니다. 발표를 보셨으면 아시겠지만 악성코드가 수행한 내용에 대한 분석 및 remediate/rollback을 제공합니다.https://www.youtube.com/channel/UCg_BAR4R0YqHZDyA-k8Q4xQ
58	손정환	Active EDR에서 Active는 기능면에서 어떤 특징을 가지고 있나요	박정수	Stroyline이라는 특허 기술로 제공하고 있습니다. 발표를 보셨으면 아시겠지만 악성코드가 수행한 내용에 대한 분석 및 remediate/rollback을 제공합니다.https://www.youtube.com/channel/UCg_BAR4R0YqHZDyA-k8Q4xQ
59	전영진	센티넬원 웹사이트의 내용에 The End of Data Loss라는 홍보 내용이 포함되어 있어 찾아보니 Singularity Control이 DRM 또는 DLP처럼 데이터 암호화 저장이 가능하고 DLP 기능을 포함하고 있는 것 같습니다. 오늘 소개해주신 EPDR 제품과 구분된 별도의 제품인지 궁금하고 만약 별도의 제품이라면 함께 운영하여 얻을 수 있는 특별한 장점에 대해 소개해주시면 고맙겠습니다.	박정수	DLP 기능을 제공하지 않습니다. The end of data loss는 랜섬웨어에 감염되어 복구할 수 없는 데이터 손실에 대한 보호를 제공하다고 이해하시면 됩니다.
60	한승일	버에 설치해서 사용하는 사례가 있는지요?	박정수	대부분의 고객사에서 윈도우 및 리눅스 서버에 운영 중입니다.
61	김홍준	헤르메스(Hermes)와 같이 웹사이트접속만으로도 랜섬웨어에 감염된다고하는데요 이러한 행위에 대한 방어도 가능한지 궁금합니다.	박정수	Anti-exploitation을 통해 방어 가능합니다.
62	윤성원	요즘은 파일리스 형태의 매그니베르 랜섬웨어가 발생하는데 파일리스 랜섬웨어도 방어가 가능한지 그리고 예방기능도 가지고 있는지요?	박정수	Anti-exploitation을 통해 방어 가능합니다.
63	박재범	랜섬웨어에 의한 암호화된 값들을 복구할 수 있다고 하지만, 만약에 솔루션도입후 랜섬웨어에 의한 피해가 생길 경우에 센티넬원의 보상정책이 따로 있나요?	박정수	보상 정책을 운영하고 있습니다.https://www.sentinelone.com/legal/ransomware-warranty/
64	이형준	사용자에 따라 정상행위와 악성행위의 기준이 다를 것 같은데요, 연구소에서 예산부분 자료를 수정하려한다면 이는 악성행위이겠지만, 경영지원에서 하는 행위라면 정상행위라는 거죠. 이처럼 Role 에 따른 행위의 분류, RBAC과 연계된 행위의 구분 및 Kill chain의 발동 조건 변경이 가능한가요?	박정수	악성 행위를 차단하는 것은 맞으나 말씀하신 것 처럼 프로파일을 통한 차단은 아닙니다. Mitre Att@ck에서 제공하는 TTP기준 차단으로 이해하시면 됩니다.
65	한승일	센티넬원은 인텔리전스를 자체 운영하는지요? 아니면 다른곳에서 DB를 제공 받는지요?	박정수	자체 인텔리전스를 운영하고 있으며, Vigilance라는 보안관제 서비스도 제공하고 있습니다.
66	공유원	지금 차단 방법에서, 격리/예방 시 오탐에 의한 수동 원복은 관리자페이지에서 즉시 가능한건가요.	박정수	지원합니다.
67	윤성원	센티넬원은 국내에서는 생소한 회사 인것 같은데요, 센티넬원을 NGAV(차세대백신)에 특화된 기업이라고 보면 되는건지요? 또 다른 사업 영역이 있는지요?	박정수	현재는 NGAV 기능인 EPP와 EDR을 단일 에이전트로 제공하고 있으며, 최근 Scalyr를 인수하여 XDR 영역까지 사업을 확대하고 있습니다.
68	이민수	기업 담당자가 Star Alert을 활용하여 Treat as a Threat와 Network Quarantine를 구별하는 원리와 방법에 대해서 질문드립니다 좋은 프로젝트 사례가 있으시면 소개해 주세요 그리고 SentinelOne에서 제공하시는 서비스에 대해서 설명해 주세요	박정수	Treat As a Threat은 탐지된 행위를 악성코드와 동일한 방식으로 처리하는 기능이고 Network Quarantine은 해당 행위 발생 시 네트워크으로 부터 엔드포인트를 격리하는 기능입니다. 기타 내용은 연락주시면 방문드리고 설명드리겠습니다.
69	이형준	Singularity XDR에서 의심스러운 행위가 실제 threat (True positive)로 확인된 경우, 그리고 이벤트가 발생하여 탐지된 결과가 Threat가 아닌 정상행위(False positive가 True negative)로 확정된 경우 얼마나 신속하게 이러한 Exception 등에 대한 Threat vector(Reputation)의 update나 action update에 반영할 수 있나요?	박정수	실시간입니다. 정책으로 입력이 바로 반영됩니다. 에이전트와 콘솔간 통신은 tcp 443포트로 항시 연결되어 있습니다.
70	이종원	공공기관에 납품하기위한 cc인증같은게 있나요?	박정수	현재 진행 중이며, 10월 중 완료예정입니다.
71	김홍준	설치가능 단말기중에 모바일기기 또는 산업용PDA도 포함되는지 궁금합니다.	박정수	모바일 기기는 올해 말 예정되어 있습니다.
72	전영진	클라우드 Only이 권장됨에도 불구하고 하이브리드로 구성하는 경우에는 어떤 장점을 얻을 수 있는지 궁금합니다.	박정수	고객사의 상황 또는 컴플라이언스 관점에서 구성하는 정도가 많고 비용적인 측면/관리적인 측면에서 고려하고 있습니다.
73	강한별	이미 공격자들은 Living Off the Land 방식으로 공격을 진행합니다. os에서 기본적으로 설치 또는 제공되는 리소스들을 사용한 공격은 어떠한 방식으로 탐지하는지요? 특정 행위를 연속적으로 분석했을 때 공격 시나리오 형태로 AI가 판단을 하면 이를 공격으로 인지하는 건가요?	박정수	지원가능합니다. 정상 파일이라고 하더라도 악성행위를 하는 경우 차단이 가능합니다. 다음 링크에서 데모를 보실 수 있습니다. https://www.youtube.com/channel/UCg_BAR4R0YqHZDyA-k8Q4xQ
74	김민경	End point에 Mac PC를 많이 있는데, 맬웨어 위협이 있는가요? 있다면 Mac이 실제로 어떻게 맬웨어에 감염되는지 사례를 알려주시고, SentinelOne은 Mac PC에 대한 보호도 가능한가요?	박정수	지원가능하고 현재 M1 칩셋도 지원합니다. 탐지 방식과 원리는 모든 OS에서 동일합니다.
75	김명환	센티넬원은 미국 EDR시장에서 강자라고 알고있어 문의드립니다^^ 머신러닝으로 학습한 인공지능 보안(센티넬원 제품)이 인간에 의해 수행된 것보다 2~3배 이상의 보안효과를 보여주는 것은 확실하겠지만, 잘못 사용되면 오히려 부작용이 나타날 수 있다고 보여집니다. 대표적인 예로, 성향적(Variance) 오류와 오버피팅(Overfitting) 오류를 들 수 있는데, 센티넬원에서는 이런 오류를 줄일 수 있는 방안이 있는지요?	박정수	말씀하신 오류를 잡기 위한 별도의 엔진 및 지도 학습 기능을 제공하고 있습니다.
76	윤성원	센티넬원은 샌디박스개념인가요? 실제로 엔드포인트에 설치되는 것인가요? AI기반이면 변화가 많을 것 같아 샌디박스가 더 유리할 것 같은데 어떤지 궁금합니다.	박정수	아닙니다. 살제 엔드 포인트에 설치되어 동작하는 에이전트 방식입니다.
77	문주웅	자율형 사이버 보안 관련해서는 SentinelOne이 우수하다고 생각합니다 SE Labs Awards에서 평가한 Best New Endpoint 이외의 강점에 대해서 설명해 주세요 그리고 현재 서비스에서 업데이트 예정이거나 개선해야 할 점에 대해서 설명해 주세요	박정수	https://selabs.uk/reports/annual-report-2020/ 상세 내용은 확인이 가능합니다.
78	방성현	윈도우 서버는 어떤 버전부터 서비스 제공이 가능한가요?	박정수	Microsoft에서 EOL되지 않은 OS는 지원 가능합니다. EOL된 OS도 예전 에이전트를 설치하여 운영하실 수 있으나 패치는 제공하지 않습니다.
79	이형준	탐지된 행위가 unknown이며, Learning sample의 수가 적을 경우, 그냥 outlier 처리가 되진 않을까요? Outlier를 Alert 처리하면 false positive 의 수가 너무 늘어나고, Outlier를 Alert 처리하지 않으면 false negative가 나오게 되는데, 이런 균형은 어떻게 잡고 계신가요?	박정수	학습이 완료된 엔진을 제공합니다. 엔드 포인트에서 프로파일 후 동작하는 방식이 아닙니다.
80	정진희	Rogue & Ranger 기능이 동일네트워크 기준에 Agent가 지정된 개수 이상이어야만 동작할 수 있도록 설정이 가능하다고 하는데 설명 부탁드립니다. 미설치 단말에 대한 보안대응 기능은 아닌 것인지요?	박정수	1대로 설정한 경우 모든 장소에서 검색을 수행하므로 10대 설정하면 회사가 아닌 경우 에이전트가 설치된 엔드 포인트가 10개가 될 수 없어 검색하지 않도록 하는 기능입니다.
81	김준석	클라우드버전으로 사용하려면 클라이언트측에 필요한 사항은 무엇인지요?	센티넬원 유세종	클라우드 메니저와의 통신을 위한 url,ip만 허용해 주시면 됩니다
82	이형준	AI의 특징은 학습한 것과 정확하지는 않지만 유사한 입력에 대해서도 동일한 action을 취한다는 것인데요, Threat에 대해서도 동일하게 작동할 수 있나요? 예를 들어 아직 본적 없는 threat이지만 기존에 학습한 Threat와 유사하게 행동한다면 이에 대한 warning이나 동일한 Threat kill chain을 발동하는 식으로요.	박정수	가능합니다. 방문드려 데모를 보여 드릴 수 있습니다.
83	양성필	SentinelOne은 북미에서는 잘 알려진 것 같은데, 국내에서는 어떤 적용 사례가 있는지요? 특히 금융권 구축 사례에 대해 소개 부탁 드립니다.	센티넬원 유세종	삼성sds에 25,000대 pc에 설치되어서 운영중입니다. 금융권 사례는 현재는 없으며 올해 도입을 하려는 고객들이 있습니다.
84	박재범	클라우드환경에서 악성코드 감염 전으로 복구하기위한 스토리지 네트워크에 부하로드에 영향을 주지는 않는지요?	센티넬원 유세종	복구는 센티넬원 설치되어 있는 pc에 백업을 진행하야, 네트워크 부하는 없습니다.
85	권창선	설치방식이 클라우드방식과 온프레미스 방식등이 있는데, 고객의 클라우드 자산의 정보보호하는 것은 아니지요? 즉 클라우드 워크로드 보안 솔루션과는 차이가 있는 것이지요?	박정수	저희 서버의 설치 방식입니다. 클라우드 환경을 보호하는 에이전트도 제공합니다.
86	권창선	기존의 EPP 솔루션의 바이러스 정보 업데이트 주기처럼 센티넬원의 바이러스 정보 업데이트 주기도 비슷하게 동작하나요?	박정수	아닙니다. 패턴 업데이트가 없습니다.
87	문태진	랜섬웨어가 걸린 데이터를 제공되는 포렌식 기능을 통해 데이터를 복구하는 성공율은 어느정도인가요? 그리고 포렌식을 통해 어떤 정보 수준까지 침임이나 변경에 대한 내용 들을 알수 있는지요?(예: 침입일, 변경유형 기술, 데이터 전송 유무 등) 그리고 이러한 포렌식 기능을 통해 바로 해당 공격을 바로 신고까지 하는 경로까지 연결시켜줄수 잇는지요? 국내 사례중에 제공되는 포렌식 기능을 이용해서 성공적인 운영사례가 있다면 어떤 사례가 있을까요?	센티넬원 최충성	Rollback 기능은 MS에서 제공하는 VSS 기반으로 동작합니다. 모든 프로세스 및 파일 수정/이동/삭제 모두 기록하고 있습니다.
88	전영진	답변 주셔서 고맙습니다. 말씀하시는 자동 업데이트는 제가 상상하는 업데이트와는 다를 것 같습니다. 제가 상상하는 업데이트는 시그너처를 사용하는 백신 소프트웨어의 경우에 나타나는 것과 같이 업데이트 진행시 시스템 부하가 증가하고 팝업창이 나타나기도 하는 과정인데 센티넬원 SaaS의 자동 업데이트 과정 중에는 이런 변화가 전혀 없어서 사용자는 업데이트가 이뤄지는지 아예 못느낄 수도 있을까요?	박정수	업데이트가 없습니다. 필요 시 에이전트 업데이트하시면 됩니다.