엔드포인트 보안

질문	파이어아이 답변
PC가 아닌 탭이나 핸드폰과 같은 모바일 단말기를 통하여 재택 업무를 수행할 경우, 이에 대해서도 대응이 가능한지 궁금합니다.	FireEye의 제품으로 모바일 단말에 대한 직접적인 통제나 보호는 어렵습니다만, 재택시 모바일 단말 등으로 업무를 보는 이메일, 내부시스템업무처리로 볼 때 VPN으로 사용되거나 SaaS 형태로의 업무를 보실 것 같습니다. 이런 경우 VPN의 오남용 및 이상사용형태, SaaS의 인증 이슈, 접근 행동 등에 대한 이력 등을 XDR 형태로 인텔리전스와 관련 행위 이벤트 로그 등을 통해서 위협으로부터의 보호가 이루어질 수 있을 것 같습니다. 또한 컨설팅 서비스를 통해서 구성된 보안아키텍처나 프레임이 적절한지 여부 등을 확인해 드릴 수 있습니다.
일부 직원이 재택근무 시 MAC OS를 사용하는데 신규 파이어아이 기능이 동일하게 적용되나요?	네, FireEye는 MVX 샌드박스 엔진 및 엔드포인트 솔루션 등에 Mac OS / Linux를 적용하고 있어서 동일하게 보호받을 수 있습니다. 참고로 저희도 업무에 Mac을 사용하고 있습니다.
안녕하세요. 파이어아이의 이메일보안과 엔드포인트 보안이 클라우드에서 민간이 아닌 공공기관의 국정원 cc인증을 대체할 수있나요, 파이어아이의 보유 인증을 무엇을 취득했는지 궁금해요.	파이어아이 솔루션은 국정원 보한적합성 평가를 받았으며, 기존 버전의 솔루션은 CC인증 또한 취득했으며 지금 설명 드리고 있는 신규 OS 버전에 대한 CC인증은 진행하고 있습니다.
파이어아이 장비가 사용되는 사이트는 중대형 사이트일거라 많은 클라우드 환경이나 타기종 장비들이 많을텐데 솔루션간 충돌에 대한 예외처리에 대해 대응이 가능할까요?	솔루션간 충돌의 경우, Endpoints Agent 설치시에만 발생이 되면 예외 처리가 가능합니다. 기타 장비들 간에 충돌 이슈는 없으며 탐지된 이벤트 또는 특정 트래픽/파일 등에 대한 예외 처리는 가능합니다.
현재 회사 내에서 end-point 및 서버 측면에서 Risk를 진단하고 평가를 해 볼수 있는 서비스나 Tool이 있는지요?	FireEye에서 작년에 인수한 Verodin에서 해당 기능을 제공합니다. 담당 영업분께 요청하시면 자료 보내드리도록 하겠습니다.
재택근무에 의한 사용자 감염과 이로 인한 클라우드와 VPN 등으로 감염된 파일 전송을 파이어아이에서는 어떻게 방어하게 되는지 궁금합니다.엔드포인트 솔루션을 통해 방어하게 되는지요?	재택근무자의 경우, 앤드포인트 솔루션을 통하여 방어를 지원합니다.
기존에 알려지지 않은 악성코드나 멀웨어의 경우에 사전에 탐지하여 대응을 하여야 하는데 파이어아이는 어떤 방식으로 지원을 하여 주시는지 답변 부탁드립니다.	어떤 악성코드라도 필수적으로 OS 에서 수행해야 하는 작업들이 있습니다. 파이어아이는 시그니처 기반의 분석 외에도 머신러닝, 행위분석,IoC 탐지 엔진을 지원하며, 추가로 방금 설명드린 모듈을 통해 탐지 및 차단기능을 강화할 수 있습니다.
일부 집중관리를 해야 하는 부분에 Fire eye 의 end-point tool를 V3와 일부 병행운영을 할 수 있는지요. 이 경우 각 Tool간의 충돌 등의 문제가 없는지요 ?	툴간의 충돌은 상호 예외처리를 통해 충분히 회피 가능한 부분입니다.
코로나 시대 보안경계가 기업을 넘어 원격 근무자가 위치한 장소까지 확대되고 있는데 원격 근무자들이 사용하고 있는 디바이스 및 홈 네트워크를 보호할 수 있는 방안이 있을까요 ?	지금 진행하고 있는 세션의 내용으로 보입니다. 파이어아이의 HX를 통해 end-point 보안을 진행하여 코로나 시대의 원격 근무자를 보호해야 될 것으로 생각 됩니다.
엔드포인트보안을 위해 클라이언트 에이전트가 설치되는 형태인가요? 다른 보안 프로그램과 충돌이 발생하는 경우는 없는지요?	네 맞습니다. 엔드포인트에 에이전트가 설치되는 방식이며, 말씀주신 것처럼 다른 보안시스템과의 상호간 예외처리 설정이 필요합니다. 다수의 고객사를 통해서 국내솔루션 등과의 처리방식 및 동작 검증이 되어있습니다.
코로나19로 인해 재택근무가 기업 업무유형의 하나로 자리 잡을 듯 싶은데요... 엔드포인트의 경우 VDI로 가상화PC를 사용해도 로컬PC로 유통되는 업무 자료나 VDI자체 취약점 노출로 인한 보안사고가 우려 됩니다. 혹시 파이어아이 제품군은 VDI나 클라우드 취약점에 대한 보안 관리를 어떻게 체계적으로 하고 있는지 궁금합니다.	말씀주신 것처럼 클라우드 자체 취약점에 대한 부분으로 보안사고가 우려되는 상황입니다. 파이어아이는 레거시 솔루션 뿐만 아니라 맨디언트 컨설팅을 전문으로 하고 있는 기업입니다. 클라우드 영역에 대한 위협 조사 및 취약성에 대한 컨설팅 지원이 가능하며 보안관리 체계에 대한 도출을 지원 드릴 수 있겠습니다. 자세한 내용은 별도 연락 주시면 상세히 설명 드릴 수 있도록 하겠습니다.
EDR 관련하여 궁금한 점이 있습니다. 1) 악성 파일 탐지 시 가상 환경에서 실행 및 분석 가능한가요? 만약 가능하다면 모든 악성 행위 탐지 시 작동하는건지 아니면 위험도 높은 악성행위 시 동작하는지 로직이 궁금합니다. 2) 가상 환경에서 실행 가능한 타 솔루션들도 많은데 파이어아이만의 장점이 어떤것인지 궁금합니다. 3) HX만 도입 시 상세 정보를 알 수 없고 Helix에서 확인 가능하다고 하는데 HX와 Helix 지원 범위를 알고 싶습니다.	드릴 수 있는 답변 내용이 많아서 간략하게만 말씀드리면 사용자환경에서의 샌드박스/가상환경은 없습니다만 Exploit Guard를 통해 행위기반으로 탐지하는 엔진이 있습니다. 샌드박스 분석기법은 파이어아이가 원천사라고 보셔도 무방하며 그렇기에 엄청난 노하우가 있습니다. 그리고 HX와 Helix는 HX의 내용을 Helix가 포괄한다고 이해해주시면 좋을 것 같습니다. 따로 자세하게 추가 설명 드릴 수 있으면 좋을 것 같습니다.
EDR(Endpoint Detection and Response) 솔루션 시장은 춘추전국 시대라 할정도로 치열하던데... 파이어아이의 가장 큰 특장점은 무엇인지요?	실제 사용중인 고객분의 의견을 빌어 말씀 드리면, 국산 제품과 외산 제품의 가장 큰 차이는 파일 베이스의 조사인지 타임라인 베이스의 조사 지원이지로 갈리게 되고, 글로벌 제품 중 파이어아이 제품의 장점은 사용자의 높은 분석 자유도에 있다고 말씀 드릴수 있겠습니다. 물론 조사의 기능을 제외하고 탐지를 위한 시그니처, 머신러닝, 행위분석 엔진도 특장점이라고 말씀 드릴 수 있겠습니다. EDR시장은 말씀주신 것처럼 많은 제품이 존재합니다. FireEye Endpoint는 EDR시장을 위해 런칭된 솔루션이기도 하며, 이전 Mandiant 컨설턴트들이 침해사고 조사의 도구로 사용되던 MIR이라는 솔루션을 기업화 한 솔루션이 HX입니다. 다른 시스템처럼 시장이 형성되어 탄생된 솔루션이 아닌만큼 깊은 분석과 조사를 쉽고 빠르게 할수 있는 경험에 의한 장점이 있으며, 이에 더해서 침해사고의 경험을 통한 위협인텔리전스가 현실성이 있음이 큰 장점이라고 보실수 있습니다.
최근에 있었던 해외 반도체 제조회사의 감염사고에서는 USB를 통한 감염이었는데... 이러한 사용자 USB 사용으로의 감염에 대해서는 어떤 대응기능을 제공할 수 있나요?	FireEye EDR(HX)를 통하여 USB를 통하여 악성 파일이 유입 또는 실행시에 탐지/차단하는 기능을 제공합니다.
EDR 사용시 랜섬웨어도 예방되는지요?	EDR에 Detection 기능(AV, 머신러닝, 행위기반 엔진)을 통하여 랜섬웨어 예정을 제공합니다.

네트워크 보안

질문	파이어아이 답변
단일 구성 시 NX 장비에 H/W 또는 전원 다운 등에 문제를 발생 시 Bypass 기능이 있는지요?	NX 장비에서는 HW Bypass 기능을 제공하고 있습니다.
ICAP 통신 분석이 가능한 것으로 나오는데... 별도 Proxy 장비가 아닌 차세대방화벽(팔로알토) 의 Proxy(SSL복호화) 기능과도 연동이 되나요?	네, 세부적으로는 추가확인을 하면 좋을것 같으나 기본적으로 ICAP을 지원한다면 사용가능하십니다.
SSL Over SSH나 DNS Over SSH와 같은 방식으로 유입되거나, 통신을 하는 악성코드의 경우 탐지가 가능한가요?	Endpoint Agent 설치시 탐지가 가능하며, 네트워크 구간의 장비에서는 탐지를 제공하지 못합니다.
난독화된 웹쉘이나 스크립트에 대해서도 지연없이 필터링이 되는건가요?	예, 당연히 난독화 되었어도 지연없이 필터링 지원합니다.
vNX를 온프라미스 환경에서 사용할 경우 vmware esx 환경에 설치하는 경우 라이센스는 어떻게 되는지요?	라이센스의 경우 트래픽별로 vNX 제품이 달라지게 됩니다. 자세한 부분은 담당 영업쪽으로 문의 주시면 자세한 설명 드리도록 하겠습니다.
예전 APT 침입대비로 NX장비 도입을 검토했을땐 암호화된 패킷(SSL)에 대한 대응이 불가능 했는데 지금은 가능해 졌을까요?	암호화된 패킷에 대한 기능지원은 가능하나, 해당 작업은 솔루션의 부하가 많이 들어가는 작업입니다. 이러한 기능은 타 벤더 또한 유사한 상황으로 복호화 장비를 상단에 두고 운영하시는 것을 권고 드리고 있습니다.
기존 레거시 영역에 NX / EX. 사용 중인데, 여기서 탐지 또는 적용된 정책을 Public Cloud 환경에 구축된 서비스 내 장비 셋팅하여 정책 연동이 가능 한가요?	가능합니다. 기존 레거지 장비를 Sensor Mode로 변경하여 Cloud VX로 연동하실 수 있습니다.
웹쉘탐지는 저희가 쓰고 있는 - NX 7400 에서도 동작되고 - 추가 구매한 VX5500 에서도 동작 되는거죠? VX5500과 vNX 센서를 연동해서 웹쉘탐지 가능한거죠?	웹 쉘 탐지 기능은 CentOS가 Intel 기반 H/W에서만 동작을 하기 때문에 NX 7400은 제공되지 않습니다. 다만 Smart Vision 기능으로는 사용이 가능합니다. 추가로 구매하신 VX 5500에서는 vNX 센서를 통하여 사용 가능합니다.
현재 ICAP과 proxy 연동된 레퍼런스가 얼마나 되나요?	해당 기능이 나온지 오래 되지 않았기 때문에 현재는 삼성 해외망 쪽에 테스트 완료되어 적용 예정입니다.
vNX 서비스를 AWS 내에 구성 시 VPC를 분리하여 Transit Gateway로 구성하는 예를 봤는데, 그렇다면 다른 계정이나 다른 VPC의 Network Traffic 도 분석 및 보안 정책 적용이 가능할 것으로 보입니다. 가능한가요?	교차계정 연동을 통해서 A 계정에서 발생하고 있고 있는 로그를 B 계정에서 확인 할 수 있을 겁니다. 교차계정 연동을 한다면 얼마든지 가능할 것으로 보입니다.
ICAP 연동 시 대용량 망에서 충분한 부하 테스트를 수행하셨나요? 분석 지연에 따른 인터넷 속도 저하가 우려됩니다.	ICAP 연동을 통한 NX 장비의 부하도 없으며 인터넷 속도 저하가 없습니다(실제 그냥 받을때와 ICAP으로 사용자가 받을때의 속도 차이가 1초 이내임). 실제 ICAP을 연동해 주는 Proxy 장비의 경우 ICAP을 포함한 Sizing을 제공하는 것으로 알고 있습니다.
언택트 이슈로 재택근무도 많은 시점으로 사내망/사외망 구별없이 PROXY, DLP, Malware 관제 등의 클라우드 서비스형 솔루션은 없을까요?	FireEye 에서는 iBoss + NX 서비스를 제공하고 있으며 iBoss를 통하여 Proxy, DLP 기능을 같이 받으실 수 있습니다.
재택근무 중인 직원 단말기에 기존에 이미 위협이 되는 소프트웨어가 있는 경우 이런 소프트웨어를 차단하거나 사용하지 못하도록 하거나 삭제할 수 있는 제품이 있나요?	이전에는 FireEye MTP라는 Mobile Threat Protection 솔루션이 있었으나 현재는 제공되지 않으며, 해당 엔진의 기능을 네트워크 솔루션에 적용하여 통해 Network를 통한 모바일 악성 트랜젝션을 탐지/대응 하고 있습니다만 말씀주셨던 직접적인 통제방안과는 차이가 있습니다.
트래픽별로 vNX 제품이 달라진다는게 무슨 의미인지여?	NXS 1500V (50Mbps) ~ NSX 6500V(1Gbps) 트래픽별로 vNX 모델이 다릅니다.

이메일 보안

질문	파이어아이 답변
파이어아이 솔루션으로 URL에 인증 피싱사이트 링크가 없는지 검사하는 능동적인 URL 방어 기능이 있나요? 그리고 메일 전달후 활성화되는 URL을 탐지하고 대응할 수 있는 솔루션이 있나요?	파이어아이 이메일 시큐리티 솔루션은, 메일 본문 및 첨부파일에 들어있는 URL에 대한 전수검사를 수행합니다. 이미 등록되어 있는 알려진 악성 URL은 즉시 대응을 하고 알려지지 않은 URL은 글로벌 엔진에서 한 번 더 검사해 누수되는 URL 없도록 대응합니다.
파이어아이 제품 중 나이지리아스캠 공격을 예방하거나 대응할 수 있는 솔루션이 있나요?	파이어아이 이메일 시큐리티 솔루션에 대한 다음 세션에서 소개 드릴 예정인데, 파이어아이 EX는 스캠 공격에 대한 대응도 가능합니다.
이메일 솔루션을 도입할 경우 고객사 운영인력의 역할과 파이어아이 관제센터의 R&R은 어떻게 나뉘게 되는지요?	파이어아이는 관제센터를 운영하지 않습니다. 다만, 파이어아이 이메일 시큐리티 솔루션은 자동화된 대응을 하기 때문에, 고객사 운영인력은 일부 대응이 필요한 메일에 대해서만 추가적인 확인 및 대응을 하시면 됩니다. FireEye 이메일 솔루션은 On-prem 서버형태와 ETP라는 SaaS 형태의 서비스를 제공하고 있으며, 해당 서비스에 대한 관제운영 서비스와 같은 서비스는 함께 제공하지 않고 있습니다.
이메일 공격에서 첨부 파일이나 위변조된 링크에 대한 위협에 대한 탐지는 어떤 방식으로 가능한 것인지 설명 부탁드립니다.	첨부파일의 경우 EX 자체 가상머신에서 분석을 통하여 탐지하며, 링크의 경우 Cloud 와 연동을 통하여 실제 로그인 화면시 테스트 계정을 입력하여 해당 접속 URL과 로그인 정보를 보내는 값과 동일한지 비교하게 됩니다. 메일 남겨 주시면 좀 더 자세한 설명 드리도록 하겠습니다.
이메일 수신시, 스팸메일을 거르는 식으로 많은 보안절차를 거치며 안정적으로 운영하려 하는데... 보안이 강화될수록 중요 고객사로부터의 메일이 차단되는 등 불편함이 비례하여 증가하는 경향이 있습니다. 이러한 불편해소와 안전을 둘다 해소할 유용한 관리 방안은 무엇일까요?	단일 솔루션에서 제어를 하면 아무래도 과오탐 및 차단 이슈가 발생 할 수 있습니다. 확실한 스팸만 스팸필터로 걸러내고, 그 외 APT 공격을 위한 악성 메일은 전문 솔루션으로 대응하는 병행 전략으로 가는것이 좋을 것 같습니다.
AI 베이스가 아닌 상태에서 위협 인지 및 대응의 자동화 라는 것이라면 어떤 방식인지요? 사전 정의 시나리오 방식, 프로파일링 방식... 이런 것을 의미하는지요?	예 맞습니다.
이메일 보안과 관련한 IOC 정보(발신자주소, 제목 등)를 제공하여 장비에 자동 등록되는 기능이 있을까요?	이메일 보안장비에서 탐지된 악성코드 정보에 대하여 자동으로 IOC를 생성하여 FireEye EDR(HX)로 등록되는 기능을 제공하고 있습니다. 발신자주소, 제목을 IOC로 제공하지는 않습니다.
이메일과 피싱 사이트 등의 공격에 ICAP를 연동해서 운영하기 위한 시스템 구성을 어떻게 하는 것이 좋은지 궁금합니다.	해당 파이어아이 솔루션은 Email APT 솔루션으로 icap 연동이 필요하지 않으며, 피싱사이트의 경우 FireEye 별도 클라우드(FAUDE)를 통하여 검사를 수행합니다.
이메일이나 or 모바일에 대응이 가능한지…	이메일의 경우, 이메일 APT 장비를 통하여 대응이 가능합니다. 모바일의 경우에는 제공되지 않으며 해당 모바일 사용자의 트래픽이 NX를 통과하는 경우 모바일 트래픽에 대한 콜백 알려진 공격등을 탐지/대응 합니다.
이메일을 통해 피싱 URL이 가장 많이 유포되는 것으로 아는데, 피싱 URL에 대해 추가 보완한점이 있나요? 특히, 피싱 URL의 경우 로그인 계정 정보 입력 유도 사이트의 경우 EX에서	피싱의 경우, FireEye Advance Url Defense(FAUD)에서 탐지하며 로그인 유도 사이트의 경우, 해당 FAUD 클라우드에서 실제 로그인 정보를 입력하여 해당 값이 업로드 되는 것과 실제 접속 URL과 비교하여 탐지를 합니다.
EX에서 이메일 첨부파일중에 암호화된 것이 있으면 본문에 비밀번호가 있는 경우에만 풀어서 검사하는 것으로 알고 있는데요. 이런 첨부파일 공격을 막을수가 있나요?	비밀번호가 없다면, 누구도 첨부된 압축파일은 해제 할 수 없기 때문에 비밀번호가 메일에 동봉되어야 해제 가능합니다.
브랜드사칭 공격인 경우, 알려진 유명한 브랜드에 대한 방어만 가능한 것인가요? 사칭 공격인지 판단하는 기준은 무엇인가요?	실제 입력되는 값과 유명 브랜드 주소와 같은지 확인하여 방어를 제공합니다.
url기반공격은 ssl인증기법으론 해결이 안되나요?	SSL 인증 기법으로는 해결이 되지 않습니다. 예로 최근 URL 공격은 단축 URL, 네이버/다음 대용량 메일 링크를 통하여 공격을 하기 때문입니다.
정상적인 URL에서 악성 URL에 시간이 변한 뒤 변경된다면 파이어아이에서 사용자가 향후 변경된 악성 URL에 접근하는 것을 실시간으로 차단하도록 하는 URL 정보 업데이트가 어떤 프로세스로 진행되는지 궁금합니다.	FireEye Cloud(FireEye Advance Defense Engine)에서 유입된 URL에 대하여 주기적으로 재검사를 수행합니다. 따라서 정상이었다가 나중에 악성으로 동작을 하는 경우, retro active 이벤트를 발생합니다.
개인정보 검출 출력물 보안 메일보안 내부개인정보시스템 과다오남용 점검 등 개인정보 유출을 예방할수 있는 통합 모니터링을 할수 있는 파이어 아이 시스템 혹은 서비스 가 있는지 궁금 합니다	개인정보유출 관련 솔루션은 제공하지 않습니다.
Impersonation Attack 방지를 위한 Active Directory Sync를 ETP에서도 지원하나요? Anti-Spam 현재 미사용 인데, 해당 기능을 사용할 수 있나요?,	ETP에서 O365와 연동을 통해서 제공하고 있습니다.
실제 공격받고 피해가 발생한 SCAM공격건이 있습니다. Impersonation 기능을 좀더 진보시키면 SCAM 공격도 대응이 가능할 것 같은데 혹시 SCAM 공격 대비를 위해 EX장비의 대응 계획이 있을까요?	EX 장비에서는 여기 세션에서 설명드리지 못한 Supply Chain Impersonation protection 기능이 있습니다. 담당 영업분을 통하여 요청해주시면 관련 자료 보내드리도록 하겠습니다.
impersonation 공격에 대한 예방차원에서 자체적으로 모의공격 훈련시에도 예외적용이 가능한가요?	예외 적용시에는 Impersonation에 대한 분석을 제공하지는 않습니다.
이전 세션에서 이메일 수신 이후이더라도 악성으로 판단된 경우 Alert을 준다고 하셨는데, Alert 이후 해당 파일의 추적 관리를 지원할 수 있는 방법이나 솔루션이 있을까요?	Retro Alert 기능을 통하여 이후 악성으로 판단된 경우, 해당 사용자에서 악성메일이라는 안내 메일을 보내주는 기능을 제공합니다. 혹 사용자가 해당 파일을 실행한 경우에는 FireEye EDR 솔루션을 통하여 추적 관리를 제공합니다.
이메일이 종종 탈취되어 스팸메일로 도용되어 피해를 보고 있습니다. FireEye에서 이메일 탈취 대응 방안도 있는지 궁금 합니다.	이 메일 탈취 대응 방안은 가지고 있지 않습니다. 다만 해당 이메일 주소를 이용한 사칭 공격, 피싱공격에 대하여 FireEye 이메일 솔루션(EX)에서 대응을 해드리고 있습니다.
코로나 확산 후 특정 회사나 개인 상대로 '스피어피싱'이 증가되고 있는데 이러한 악성코드를 사전에 방지할 수 있는지요? 재택근무로 인터넷사용량도 지속적으로 늘어나고 있어 새로운 앱 활용도 늘어나는데 해킹에 대한 안전장치가 필요함에 대한 대책, 특장점은 무엇인가요?	스피어피싱의 경우 FireEye 이메일 솔루션(EX)에서 대응을 제공하고 있으며, 재택근무의 경우에는 FireEye Endpoint 솔루션(HX)을 통하여 대응이 가능합니다. 대표적인 특장점으로는 위협 인텔리 전스를 통하여 IOC를 지속적으로 받을 수 있으며, 탐지 엔진이 우수합니다. 자세한 정보는 https://www.fireeye.kr/company/press-releases/2019/fire-eye-endpoint-security-leads-mitre-att-ck-evaluation.html 통하여 확인하실 수 있습니다.

SIEM (Helix)

질문	파이어아이 답변
helix 같은 경우 서버에 대한 로그 관리 및 검색 기능도 지원되나요?	네 안녕하세요? Helix는 3rd party 솔루션도 연동을 지원합니다. 서버의 어떤 로그인지는 모르겠지만 현재 Helix에서 자동으로 연동되지 않는다고 한다면 Helix 전문 조직에서 파싱을 지원해 드릴 수 있습니다.

클라우드 보안 (Cloudvisory)

질문	파이어아이 답변
요즘은 클라우드 환경에 회사의 시스템을 구성 하는 추세 인데, FireEye 솔루션은 AWS, Azure 환경에서 Co-work 해서 구축 및 연동한 사례가 있는지요?	국내보다는 해외에서 클라우드를 더 활성화돼서 많이 쓰기 때문에, 해외 레퍼런스가 많이 있습니다. 파이어아이는 클라우드에 대한 지원을 점차 강화하고 있으면 매 분기 로드맵에도 지원계획이 추가되고 있습니다. 자세한 내용은 연락 주시면 별도 자리를 빌어 설명드릴 수 있도록 하겠습니다.
Software 방식으로 사용 시, 사용량의 규모에 따라 Pricing 정책이 있는지요? 소규모로 테스트 하다가 전체 확산 등을 고려 할 수도 있기 때문입니다.	라이센스 정책은 사용량에 따라 책정되기 때문에 충분히 지원 가능합니다만 세부적인 내용은 연락 주시면, 자세히 설명 드리겠습니다.
Cloudvisory의 지능형의 의미가 무엇인가요? AI가 적용되어 있다는 의미인가요?	AI가 적용되어 있지는 않으나, 위협에 대해 인지하고 대응하는 방식이 자동화 되어 있다는 의미로 해석하면 좋을 것 같습니다.
파이어아이는 물리 장비 말고 소프트웨어도 지원되나요?	클라우드보안제품의 경우는 소프트웨어형태인 SaaS 타입으로 준비 되어 있습니다. 예를들면 이메일 보안 솔루션인 Ex의 클라우드 버전인 ETP 같은 경우도 SaaS일 수 있구요. 파이어아이의 SIEM인 Helix 같은 경우도 SaaS 제품으로 볼수 있습니다.
정부기관업무망내부망 망분리되어있는데 클라우드 사용사례가있나요?	망 분리가 되어 있으신 고객의 경우, 내부 데이터가 외부로 가는 것을 원하지 않기 때문에 클라우드와 연동하신 사례는 없습니다. 다만 FireEye FX(파일 분석 솔루션)과 연동한 사례는 많이 있습니다.

FireEye General

질문	파이어아이 답변
막상 솔루션을 도입해도 운영 직원의 미숙으로 관리에 어려움이 따를텐데 교육은 어떤식으로 진행되나요?	일반적으로 장비 운영 교육은 파트너사를 통해서 지원을 해 드리며, 신규 기능 설명 같은 경우, 담당 지사 엔지니어 분이 진행해 드립니다. 운영을 하면서 특별히 설정하는 것이 없기 때문에 대부분 고객 분들이 어려워 하지는 않습니다.
파이어아이의 특장점인 공격하는 해커들의 테크닉과 툴을 99% 이상 탐지해내는 기능이 경쟁사와 차별화되는 경이로운 점으로 알고 있는데, 어떠한 원리를 이용하여 그렇게 철저히 해내는지 구체적으로 궁금합니다!	글로벌 위협정보/침해조사 정보/실제 가상머신에서 분석된 결과 등이 FireEye 클라우드에 있으며, Fireeye 솔루션에는 자체 가상머신에서 분석을 수행하기 때문에 탐지률이 경쟁사보다 우수합니다.