INVESTIGATION ANALYSIS SYSTEM(IA 시리즈)

주요 기능

- **시각화 기능:** 생성하기 쉬운 맞춤형 대시보드를 통해 메타데이터 및 활동을 관찰 및 공유합니다.
- **신속한 응답:** 패킷 캡처 노드에 대한 애플리케이션 레벨의 중앙 집중식 와일드카드 쿼리 및 조사를 수행합니다.
- **강력한 검색:** HTTP, SMTP, POP3, IMAP, SSL, TLS, FTP 등의 프로토콜에서 인덱스된 메타데이터를 사용하여 검색을 가속화합니다.
- **워크플로우 효율성:** PCAP 파일을 보관하고 통합된 사례 관리를 통해 조사하는 동안 다른 분석가와 공유합니다.
- **SIEM 통합:** RESTful API를 통해 SIEM 플로우 및 메타데이터 인덱스에 연결합니다.
- **IOC 통합 및 전환:** FireEye Network Security, Email Security 및 Endpoint Security 제품 경보를 단일 워크벤치에 통합하고 IOC 간의 잠재적 상관관계를 드러내 더욱 심층적인 조사를 수행합니다.
- **보고서 자동생성:** 시간 간격 또는 이벤트 계수 한계점에 근거하여 보고서를 자동으로 예약하고 생성합니다.
- **한 번의 클릭으로 파일 복구:** 추가적인 분석을 위해 의심스러운 파일, 웹 페이지 및 이메일을 빠르고 안전하게 복구하고 분석을 위해 의심가는 페이로드를 FireEye Malware Analysis(AX 시리즈) 어플라이언스로 보냅니다.
- **확장 가능성** FireEye Investigation Analysis System(IA) 어플라이언스를 그룹화하여 메타데이터 저장 용량을 늘리고, 단일 관리 콘솔로부터 분산된 Network Forensics Platform 어플라이언스와 Investigation Analysis System 어플라이언스에 대한 검색 능력을 단일 관리 콘솔을 사용하여 확대합니다.

요약

최근 사이버 보안 침해 뉴스 보도에서 밝혀졌듯이, 보안 사고의 피해를 최소화하는 최선의 방법은 조기 탐지와 신속한 조사이고, 이를 위해서는 강력하고 빠른 포렌식 역량이 요구됩니다.

FireEye Investigation Analysis System(IA)은 사용하기 쉬운 분석 인터페이스가 포함된 중앙 집중식 워크벤치를 업계에서 가장 빠르고 손실이 없는 네트워크 데이터 캡처 및 검색 솔루션인 FireEye 기업 포렌식에 추가함으로써 숨겨진 위협을 밝혀내고 사고 대응을 가속화합니다. 고성능 패킷 캡처와 심층 분석을 통합하면 FireEye의 종합적인 위협 방어 및 탐지 역량을 강력하게 보완할 수 있습니다.

분석가들은 공격 전, 중, 후에 특정 네트워크 패킷 및 세션을 검토할 수 있습니다. 악성코드 다운로드 또는 콜백을 유발하는 이벤트를 재구성 및 시각화하는 기능을 갖춘다면 보안팀은 재발을 방지하기 위해 효과적이고 빠르게 대응할 수 있습니다. 또한 네트워크 내부에서 공격을 분산하는 데 일반적으로 사용되는 프로토콜을 해독하여 공격자 활동에 대한 가시성을 확장할 수 있습니다.

FireEye Investigation Analysis System(IA)은 단일 노드와 분산된 아키텍처에 대한 다수의 설정을 지원하여 메타데이터 취합, 쿼리, 분석의 대역폭과 성능을 최적화합니다.

역량

단일 조사 워크벤치: 심층 조사를 필요로 하는 경보를 신속하게 구분함으로써 조사 과정을 가속화하고 단일 워크벤치로부터 중앙 집중화된 기업 포렌식 조사를 통해 초점을 좁히십시오. 다음과 같은 위협에 관한 간단한 질문에 신속하게 답변할수록, 귀사의 조직, 고객 및 브랜드를 더 잘 보호할 수 있습니다: 공격자들이 어떻게 침입했습니까? 그들이 침입한 후에 어떤 일을 했습니까? 그들은 어디로 갔습니까? 그들은 이곳에 얼마 동안 있었습니까? 구체적으로, 공격자들이 무엇을 가져갔습니까?

보고서: FireEye Investigation Analysis System(IA)을 이용해서 시간 또는 정교한 계수 기반의 한계점에 근거한 보고서를 생성하십시오. 네트워크 내에서 발생하는 비정상 활동을 시각화하고 네트워크 이벤트를 모니터링하기 위해서 보고서 기능을 사용합니다.

시각화 및 정보 공유: 조사 중 귀중한 시간을 절약하고 숨겨진 위협을 검색합니다. 시각화와 최대 20Gbps의 속도로 패킷 데이터를 캡처하는 FireEye Network Forensics Platform을 결합하여 전례 없는 탐지 역량을 보유합니다. 끌어놓기 가젯과 아카이브를 사용하여 맞춤화된 대시보드를 생성하고, 통합된 사례 관리 기능을 사용하여 PCAP 파일을 다른 분석가와 공유하십시오.

인텔리전스 통합: FireEye iSIGHT 위협 인텔리전스 네트워크에서 IOC를 자동으로 다운로드하고 네트워크 내의 IOC 징후에 대한 과거 메타데이터를 분석하는 프로세스를 자동화합니다. 새 위협을 인식하기 전에 해당하는 위협에 대한 과거 데이터 검색을 수행합니다.

네트워크 전체에 걸친 중앙 집중적 가시성:
FireEye 기업 포렌식의 패킷 캡처에 대한 메타데이터를 취합하고, 중앙 대시보드에 분석 정보를 표시하여 사각지대를 제거하고 킬 체인의 엔드 투 엔드 뷰를 생성합니다. 이러한 전체적인 뷰를 사용하여 상황 정보를 제공하고 포괄적인 최적의 대응 방법을 개발합니다.

방대한 데이터 세트에 대한 초고속 쿼리: 쿼리 응답의 대기 시간을 절감하여 위협을 빠르게 해결합니다. 대량의 데이터 세트와 광범위한 프로토콜에 대해 초고속의 유연한 애플리케이션 레벨 검색을 지원합니다.

모델	총 온보드 스토리지	크기	전원/일반 작동 부하
IA 1000HN16	16TB	1U 랙 마운트 4.3 x 43.7 x 65.0cm (1.7" x 17.2" x 25.6") 20.9Kg(46lbs)	650W 고효율 (1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정 230-280W 일반
IA 2000HN48	48 TB	2U 랙 마운트 8.9x43.7x64.8cm (3.5"x17.2"x25.5") 23.6Kg(52lbs)	1280W 고효율 (1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정

FireEye에 대한 더 자세한 정보를 원하시면 다음의 웹사이트를 방문하십시오.
www.FireEye.com

FireEye, Inc. 소개

FireEye는 인텔리전스 기반 Security as a Service(서비스형 보안)의 선두주자입니다. FireEye는 고객사의 보안과 매끄럽게 연결된 확장성 있는 연장선으로 기능하면서, 고객사에 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스와 세계적으로 유명한 맨디언트의 컨설팅을 통합된 단일 플랫폼으로 제공합니다. 이러한 접근방식으로 FireEye는 사이버 공격 대비 예방 대응에 어려움을 겪는 조직들을 위해 사이버 보안의 복잡성과 부담을 덜어주고 있습니다. FireEye Forbes Global 2000 기업 중 940개 이상의 기업을 포함, 전세계 67개국에 걸쳐 5,000개 이상의 고객사를 보유하고 있습니다.

FireEye Korea |
서울특별시 강남구 테헤란로 534 글라스타워 20층 |
02.2092.6580 | korea.info@fireeye.com | www.fireeye.kr

www.FireEye.com

© 2017 FireEye, Inc. 저작권 소유. FireEye는 FireEye, Inc.의 등록상표입니다.
다른 모든 브랜드, 제품 또는 서비스 명칭은 해당 소유자의 상표 또는 서비스 마크입니다.
DS.PXS.KO-KR.032017