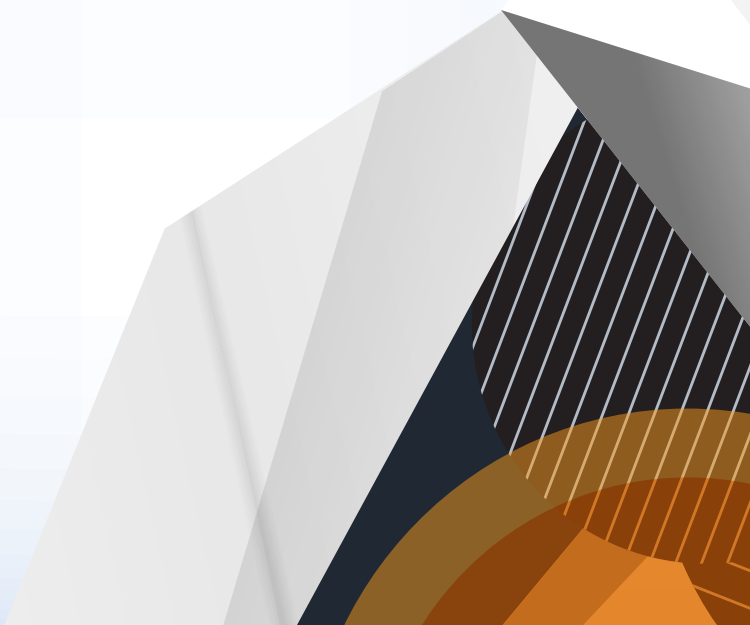
백서

보안 운영 제어

모든 회사가 이용할 수 있는 통합 보안 솔루션 제공

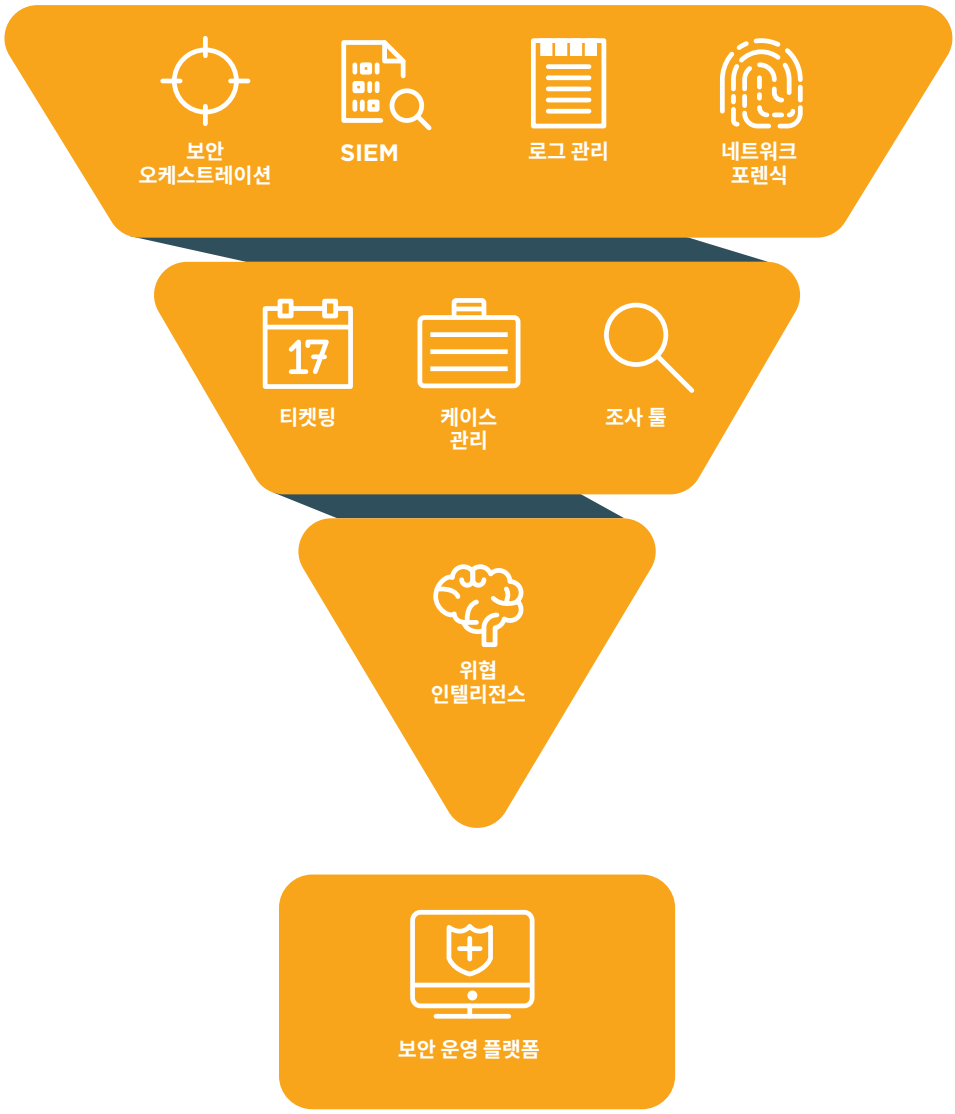


보안 운영에 대한 새로운 사고방식

매일 새로운 위협이 등장하는 환경에 대응하여 기업들은 보안력 강화를 위해 갈수록 많은 비용과 노력을 투자하고 있습니다. 이 같은 투자를 하는 이유는 단순합니다. 어떤 조직이든 규모에 관계없이 정보, 돈, 파괴 행위 중 하나라도 공격자가 노리는 것을 가지고 있다면 공격의 표적이 되기 때문입니다. 특히 리소스가 한정된 회사에게는 효과적인 보안 에코시스템을 구축하는 것이 큰 부담이 될 수 있습니다. 이러한 회사들은 대기업과 동일한 수준의 위험에 노출되어 있지만, 투자자금과 인적 자본의 수준은 그에 미치지 못합니다.

재정적인 한계는 둘째로 치더라도, 어플라이언스를 새로 구매하거나 서비스에 가입하는 것만으로는 기업들이 필요로 하는 개선 효과를 실현하는 것은 어렵습니다. 오히려 포인트 제품을 추가하면 복잡성이 가중되고, 인력이 더 필요하게 되며, 오류가 발생하기 쉬운 수작업이 늘어납니다. 설상 가상으로 새로운 보안 시스템이 제대로 구현되지 않는다면 위험에 더 많이 노출될 수도 있습니다. 놀라운 점은 새롭게 출시되는 보안 제품들 역시 이렇게 절실하고 잘 알려진 고객의 필요를 빠르게 해결해 주지 못하고 있다는 점입니다.

다행이도, 보다 종합적인 사이버 보안 접근 방식이 새로 등장하고 있습니다.



보안 운영 플랫폼

운영상의 문제에 대한 혁신적인 대응책 중 하나는 바로 보안 운영 플랫폼입니다. 이 같은 플랫폼은 보안 운영 센터(SOC)의 관제 센터와 같은 역할을 합니다. 이는 보안 운영을 통합하고 자동화하여 보안 팀이 위협을 더 신속하게 저지하는 동시에 운영 비용을 절감하도록 설계되었습니다. 하지만 그 안에 포함되어 있는 솔루션은 각기 다릅니다.

예를 들어 SIEM(보안 정보 및 이벤트 관리) 솔루션은 한정적인 전술적 이점만 제공하면서 보안 운영 콘솔로서 다시 자리잡으려 하고 있습니다. 그러나 이러한 솔루션은 상황 분석 또는 자동화 없이 대량의 경보를 취합하므로 SOC 분석가에게 더 큰 문제를 야기합니다.

본 백서에서는 보안 플랫폼의 필수 기능을 살펴보고 보안 벤더를 선정할 때 고려해야 할 점을 몇 가지 제시합니다. 그 어떠한 혁신적인 기술이 등장하더라도, CISO는 최상의 기술, 프로세스, 인적 자본을 보유하고 있어야 합니다. 보안 운영 플랫폼의 이점은 기업이 일관된 보안 운영 경험을 갖추게 하는 것입니다. 이 같은 이점은 미래에 컴퓨터 네트워크가 훨씬 효율적이고 단순하며 그 결과 더 안전해질 것임을 예고합니다.

가시성

가시성이란 공격이 미치는 영향을 탐지하고 경고하고 평가하는 조직의 능력을 말합니다. 여기에는 조직이 직면한 위협에 대한 가시성뿐 아니라 그 중 가장 큰 위험이 어떠한 것인지까지 파악하는 능력이 포함됩니다. 효과적인 보안에는 가시성이 필수입니다. 인프라에 맹점이 있으면 중대한 문제로 이어질 수 있기 때문입니다.

사이버 위협 환경이 진화함에 따라 네트워크에서 새로운 가시성의 허점이 나타날 수 있습니다. 일례로, 오늘날의 조직에게는 벤더 연결 지점, 자회사 조직 및 기타 과거에는 존재하지 않았던 상호 연결 네트워크에 대한 가시성이 필요합니다.

클라우드 인프라의 사용이 급증하면서 새로운 취약점과 가시성의 허점도 나타나고 있습니다. 사용자 인증 및 구성 관리를 중앙 집중식으로 유지하기가 어려운 공용 클라우드를 사용하여 중요 비즈니스 작업을 실행하고 기밀 데이터를 저장하는 조직의 경우 데이터 보안을 적용하기가 더욱 어렵습니다.

가시성을 개선하려면 신속하게 보안 침해를 파악하고, 취약점을 사전에 식별하고, 공격자를 예측하기 위해 보안 데이터를 중앙 집중화 및 취합하는 보안 운영 플랫폼이 필요합니다.

침해가 발생한 사실을 신속하게 파악

조직들은 공격을 완벽하게 예방하기 원하며, 이는 당연한 이치입니다. 하지만 사이버 공격자들이 기술적, 사회 공학적 취약점을 악용하는 능력이 갈수록 지능화되는 만큼, 보안 침해를 100% 예방하기는 사실상 불가능합니다. 따라서 우리가 생각해야 할 문제는 이러한 보안 침해가 얼마나 오래 지속될 것인가입니다. 침해가 발견되기까지 소요되는 글로벌 평균 공격 체류 시간은 99일로, 범죄자들이 민감한 정보를 빼내는 것은 물론이고 보안 침해의 증거까지 없애기에도 충분한 시간입니다.[1]

따라서 공격에 사용된 악성코드를 파악하고, 노출 정도와 피해를 평가하고, 그러한 정보를 다시 전반적인 보안 운영 기능에 적용할 수 있도록, 신속한 탐지로 예방을 증진하는 보안 운영 플랫폼이 필요합니다. 침해가 1분간 지속될 때마다 수백 또는 수천 달러의 비용이 발생하는 오늘날, 보안 운영 플랫폼은 몇 시간이나 며칠이 아니라 몇 분 안에 보안 침해를 탐지해낼 수 있어야 합니다.

대량의 경보 분석

우리에게는 방대한 양의 경보 노이즈 사이에서 실제 위협을 식별해내는 능력이 필요합니다. 평균적으로 한 조직에서 발생하는 17,000건의 악성코드 경보 중에 19%만 신뢰할 수 있는 것으로 간주되고 있으며, 그 중 4%만 조사 대상이 됩니다. 잘못된 경보는 번거로울 뿐만 아니라 비용도 발생시킵니다. 조직이 부정확하고 오류가 있는 인텔리전스에 대응하느라 허비하는 시간을 비용으로 환산하면 매년 평균 127만 달러에 달합니다.[2]

적절한 상황 정보가 없는 경우 보안 분석가는 정보에 근거하여 경보를 판단하기 어렵습니다. 효과적인 보안 운영 플랫폼은 위협을 노출시키고 분석하며 경보의 검증 작업을 자동화하여 오탐을 제거합니다. 또한 보안 팀이 대량 경보 속에 숨어 있는 위협의 우선 순위를 정해 신속하게 대응할 수 있게 해 줍니다.

공격자의 행동 파악 및 예측

기존의 시그니처 기반 제품은 지난 몇 년간 효용성이 급격하게 낮아졌습니다. 이는 공격자가 시그니처 기반 탐지 방식을 무력화하도록 악성코드를 변조할 수 있는 능력을 갖추었음을 시사합니다. 또한 공격자가 악성코드를 이용하던 수법에서 유출된 인증 정보를 이용하는 수법과 악성코드와 전혀 관련이 없는 수법으로 옮겨가고 있음을 의미합니다.[3]

효과적인 보안 운영 플랫폼은 이전에 관찰된 적이 없는 위협을 인식할 수 있어야 합니다. 또한 공격자의 행동을 모델링하여 미래의 행동을 파악하는 정교한 분석 방식을 적용해야 합니다. 이 같은 방식으로 행동을 코드화함으로써 분석, 인텔리전스 및 현장의 실제 경험이 유기적으로 작용하도록 해야 합니다. 머신 러닝과 사용자 행동 분석(UBA) 이상의 기능을 제공하는 솔루션이 필요한 이유가 바로 여기에 있습니다. 즉, 솔루션은 분석가가 위협의 우선 순위를 정하고, 위협을 격리하며, 적절한 복구 전술을 선택하는 데 도움을 주어야 합니다.

1 FireEye (2017). M-Trends 2017: A View from the Front Lines.
2 Ponemon Institute (January 2015). The Cost of Malware Containment.
3 Joshua Goldfarb (October 26, 2016). 20 Endpoint Security Questions You Never Thought to Ask.

대응

사이버 공격에 대한 보도 건수가 사상 최대에 이르고 있습니다. 최근에는 보안 업계에서 일하지 않는 사람도 침해 이후의 대응이 사전에 예방하고 보호하는 것만큼이나 중요하다는 사실을 잘 알고 있습니다. 양질의 경보, 우선 순위가 잘 정해진 작업 대기열, 정확한 분석, 원활한 케이스 관리 등으로 효율적이고 효과적인 프로세스를 구현할 수 있습니다. 일반적인 회사에 있어 워크플로우의 원활한 작동은 우선 순위가 그리 높지 않을 것이라고 생각할 수도 있지만, 데이터는 다르게 나타납니다. 작년에 기업들이 지능형 공격을 격리하고 복구하는 데에만 평균 82일이 소요되었습니다.[4]

이 같은 대응 실태를 개선하기 위해서는 모든 보안 운영을 통합하고, 인텔리전스로 대응을 강화하고, 케이스 관리 기능을 제공하며, 직원의 효율성을 높이는 보안 운영 플랫폼이 필요합니다.

보안 운영의 모든 부분을 통합

바람직한 플랫폼은 보안 팀이 경보를 신속한 대응으로 전환하기까지 소요되는 시간을 단축합니다. 일반적으로 대응 속도는 보안 팀이 경보를 얼마나 신속하게 분석하는지에 따라 좌우됩니다. 그러나 상황 정보와 상관 관계를 활용하지 않은 상태로 여러 소스에서 경보를 받는다면, 로그 소스의 가치는 거의 없는 것이나 마찬가지입니다. 따라서 로그 소스를 결합하고 거기에 위협 인텔리전스와 분석을 더해 새로운 위협을 가시화하여 대응 속도를 촉진하는 플랫폼이 효과적일 것입니다. 이렇게 구축될 경우, 플랫폼은 단순히 그 구성 요소의 기능을 취합한 것보다 훨씬 큰 효과를 제공합니다.

인텔리전스로 대응 강화

신뢰성과 충실도가 높은 인텔리전스는 성숙한 보안 운영 역량의 중요한 요소입니다. 하지만 운영 환경에 직접적으로 적용할 수 없는 인텔리전스는 도움이 되지 않습니다. 다시 말해, 조직을 방어하는 데 간편하게 활용할 수 없다면 인텔리전스는 아무 소용이 없습니다. 보안 플랫폼의 인텔리전스가 항상 상황정보와 상관 관계에 대한 정보를 포함하고, 조직과 조직이 직면한 보안 침해에 구체적으로 적용할 수 있으며, 이상적으로는 팀이 조사를 지원할 추가 정보를 필요로 할 때 온디맨드 방식으로 사용할 수 있어야 하는 이유가 여기에 있습니다.

케이스 관리 기능 제공

탐지의 경우, SOC 팀의 개별 실무자에게 의존하는 경우가 많은데, 조사와 오케스트레이션에는 일반적으로 여러 팀원이 참여하여 배정된 작업을 수행하고, 보고서를 작성하고, 민감한 정보를 공유합니다. 그러나 유감스럽게도, 기존 프로젝트 관리 및 통신 툴은 SOC 팀의 이러한 활동을 조율하기에 전혀 적합하지 않습니다. 좋은 보안 운영 플랫폼은 작업을 배정 및 추적하고, 작업 대기열을 관리하며, 효율적인 해결을 위해 지식의 교환을 증진할 수 있는 간편한 툴을 팀에 제공할 수 있어야 합니다.

직원 리소스의 효율성을 증진 또는 강화

위협이 진화하면서 조직들은 앞다투어 사이버 보안 인력 확보에 나서고 있지만 공급이 수요를 따라가지 못하고 있습니다. 미국에만 아직 209,000개 이상의 사이버 보안 일자리가 주인을 찾지 못하고 남아 있고, 지난 5년간 채용 공고가 74% 증가했습니다.[5] 조직에서 연중 무휴로 보안을 운영하려고 해도, 예산 부족으로 보안 팀의 인력을 적절하게 확보할 수 없습니다. 대부분 조직의 현재 리소스 보유 실태를 감안할 때, 분석가가 기존 보안 시스템의 경보를 처리하도록 하는 것은 시간이나 예산의 낭비입니다. 이러한 수작업 프로세스는 비효율적이고 오류가 발생하기 쉬우며, 보안 운영 플랫폼이 그러한 반복적이고 시간이 많이 소요되는 작업을 자동화하지 못하면 조직의 보안 태세와 직원의 참여에 있어서 더 큰 위험이 발생하게 됩니다.

총 소유 비용(TCO)

사이버 보안 업계에서 총 소유 비용(TCO)만큼 중요하게 다루는 주제는 없습니다. 기업들은 가격을 기준으로 제품을 서로 비교하기를 좋아하기 때문입니다. 서로 분야가 전혀 다른 제품을 비교한다 해도 이 같은 관행이 잘못되었다고 할 수는 없습니다. 사이버 보안에 예산을 투자하면 다른 비즈니스 우선 과제에 지출할 예산이 그만큼 줄어드는 것이므로 조직에서는 그에 따라 신중하게 우선 순위를 평가해야 하기 때문입니다.

가치 있는 자산을 보호하는 것이 앞으로도 기초적인 운영 지출 항목이 될 것임을 감안할 때, 지금까지와 다소 다른 방식으로 TCO에 접근한다면 사이버 보안에 대해 더 포괄적이고 전략적인 논의를 증진할 수 있습니다. 이를 통하여 보안 운영 플랫폼의 비용과 편익을 보다 포괄적으로 파악할 수 있습니다.

금전적 비용

하드웨어 및 소프트웨어, 구독 및 업그레이드, 설치 및 유지보수와 관련된 비용 - 일반적으로 이러한 비용들을 가장 확실하게 검토합니다. 표면적으로는 명확해 보이지만, 이러한 비용은 기능이 비슷한 여러 솔루션이나 과도한 유지보수, 잦은 업데이트, 더 긴 다운타임이 필요한 분산된 포인트 제품과 같이 인프라 내에 존재하는 불필요한 중복과 비효율성을 제대로 반영하지 못합니다.

효과적인 보안 운영 플랫폼은 네트워크, 엔드포인트 및 이메일 보호, SIEM, 오케스트레이션, 로그 관리, 포렌식 등 다양한 기능을 통합합니다. 또한 기존 포인트 제품을 통합하거나 처리하는 옵션을 제공함으로써 비용의 타당성을 확보하는 데 도움을 주어야 합니다.

4 Ponemon Institute(2016년 3월). "The State of Malware Detection and Prevention(악성코드 탐지 및 예방 실태)."
5 Ariha Setalvad(2015년 3월 31일). "Demand to fill cybersecurity jobs booming(폭발적으로 늘어나는 사이버 보안 인력 수요)."

운영 비용

조직이 어플라이언스를 구매하거나 서비스에 가입하는 것으로 비용 지출이 끝나는 것이 아닙니다. 최고의 보안 인재를 확보 및 채용하고, 제품에 대한 교육을 실시하며, 지속적인 운영을 지원하는 데 시간과 예산을 배정해야 하기 때문에, 그에 따른 추가적인 운영 비용이 발생합니다. 대부분의 회사에게 이러한 비용은 재무 비용과 마찬가지로 불가피합니다.

시간이 곧 운영 비용인 만큼, 조직은 어디에 시간을 할애할지 신중하게 결정해야 합니다. 보안 플랫폼을 평가할 때 기업은 다음과 같이 해야 합니다.

- 직원에게 서로 연동되지 않은 수많은 포인트 제품에 대해 교육하는 시간과 비용을 절감하거나 없앨 수 있도록 포괄적인 기능을 제공하는 제품 모색
- 경보로 인한 피로를 최소화하고 실제 위협을 신속하게 탐지하는 고급 탐지 기능에 투자
- 보안팀이 부가가치가 가장 큰 작업에 시간을 할애할 수 있도록 오케스트레이션 및 조사 기능 강화

자동화는 경보 검증과 같은 반복적인 수작업 프로세스를 최소화해 줍니다. 보안 전문가가 업무 시간의 80%를 이 같은 작업에 할애하는 경우가 허다하며, 이로 인해 피로를 많이 느끼고 이직을 결심하는 경우도 많습니다. 보안 운영 플랫폼은 이 같은 작업을 자동화하여 보안 전문가가 위협을 탐지하고, 위협을 방어하며, 위협이 발생한 경우 대응 및 해결하는 등 훨씬 중요한 작업에 집중할 수 있게 해줍니다.

일반적인 인력 감소 문제에 대처하려면, 보안 운영 플랫폼이 보안 팀의 활동을 코드화 및 자동화하여 회사가 베스트 프랙티스를 유지하도록 해야 합니다.

마지막으로, 보안 서비스의 연속성도 운영 비용을 발생시키는 주요 요인 중 하나입니다. 우수한 보안 인력이 이탈하지 않게 하는 것은 인력을 유치하는 것만큼이나 어렵습니다. 채용은 일반적으로 예측할 수 있지만 인력의 이탈은 예측할 수 없으며, 이러한 이탈은 모든 보안 노력의 연속성을 위태롭게 합니다. 보안 플랫폼은 직원 이동을 최소한으로 유지할 수 있도록 역량과 수준에 맞는 올바른 작업, 지식 및 툴을 그 구성원에게 제공해야 합니다.

표 1. 보안 운영 플랫폼: 중요 기능 체크리스트

가시성 향상	
몇 분 안에 보안 침해 식별	✓
중요한 경보 취합 및 우선 순위 지정	✓
공격자 행동 예측	✓
신속한 대응	
전체 인프라를 단일 콘솔로 통합	✓
인텔리전스로 대응 강화	✓
케이스 관리 기능 제공	✓
비용 최적화	
재정 투자 효율화	✓
직원 효율성 향상	✓
서비스 연속성 보장	✓

맺음말

보안 운영 플랫폼은 여러 조직에 수많은 이점을 제공합니다. 구매 결정과 마찬가지로, 조직은 벤더가 제안하는 솔루션의 실제 기능을 완벽하게 파악할 수 있도록 명확히 확인시켜 줄 것을 요구해야 합니다. 이는 대규모의 엔터프라이즈급 예산을 보유하지 못한 조직도 성숙한 보안 태세를 갖출 수 있는 방법입니다.

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울 특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

FireEye, Inc. 소개
FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.

FIREEYE™