솔루션 개요

보안 운영팀의 신속한 인시던트 대응을 가능하게 하는 FortiSOAR

종합 요약

각종 위협이 점점 진화하고 새로운 디지털 혁신이 출현하면서 네트워크 공격 면은 점점 더 넓어지고 있습니다. 대다수의 기업에서는 이러한 변화의 속도에 맞추기 위해 포인트 솔루션을 추가합니다. 이렇게 보안이 더 복잡해지면 수많은 문제가 발생하게 됩니다. 관리할 벤더가 너무 많거나, 조사할 위협 경고가 너무 많아지기도 하고 수동 프로세스가 많아 대응 시간이 느려지기도 하며 매일 늘어나는 작업 부하를 관리할 숙련된 인력이 부족한 경우도 있습니다. 또한 이러한 복잡성 때문에 보안팀에서 자사의 다양한 난관에 적합한 최적의 솔루션을 파악하기가 어렵습니다.

보안 아키텍처에 보안 오케스트레이션, 자동화 및 대응(SOAR) 기능을 더하면 이러한 부담을 덜 수 있습니다. FortiSOAR는 보안팀이 맞춤 자동 프레임워크를 만들도록 지원합니다. 이 프레임워크에 기업의 보안 도구를 모두 통합하지만, 알림 피로(alert fatigue)를 없애고 컨텍스트 전환을 줄입니다. 이렇게 하면 보안 관제팀에서 보안 프로세스에 적응할 뿐만 아니라 자사 상황에 맞게 최적화까지 할 수 있습니다.

위협 경고 피로와 통합되지 않은 보안으로 인한 위험

요즘 보안 애널리스트는 매일 접하는 보안 위협 경고의 수가 워낙 많아 과중한 부담에 시달리고 있습니다. 보안 인프라가 점점 더 복잡하고 파편화되었다는 점(여러 벤더가 제공하는 포인트 제품이 너무 많음)이 문제의 주된 이유입니다. 최근 엔터프라이즈에서는 새롭게 출현하는 위협, 새로운 위험 노출 지점과 속도를 맞추기 위해 평균 47종의 보안 솔루션과 기술을 구현하고 있습니다.[1]

위협 경고의 양 자체가 문제의 큰 부분을 차지하지만, 출처가 다양한 경고를 추적하고 조사해 수정하려 시도하려면 보안 운영 센터(SOC)의 수동 인력을 대량 투입해야 합니다. 이처럼 비효율적인 프로세스는 결국 인시던트 대응 프로세스의 속도를 느리게 만듭니다. 현재 한 건의 침해 사례를 파악하여 차단하는 데 소요되는 시간은 평균 279일입니다.[2]

이와 동시에 기업에서는 보안 운영에 관하여 전 세계적인 사이버 보안 기술 부족 문제로 곤란을 겪고 있습니다. 현재 전체의 거의 2/3(65%)에 달하는 기업에서 효율적인 보안 운영을 유지하기 위해 필요한 전문 기술을 갖춘 인력이 부족한 상황입니다.[3] 이처럼 서로 교차되는 여러 요인이 작용하여 침해 시도가 탐지되지 않을 확률이 한층 더 높아집니다.

작년 한 해 동안 수명 주기가 200일 미만인 침해 건은 수명 주기가 200일을 넘는 침해 건에 비해 처리 비용이 122만 달러 적게 들었습니다 (평균, 각각 334만 달러 대 456만 달러). 이 차이를 백분율로 환산하면 37%나 됩니다.[6]

SOAR 시장은 SOC팀의 수요가 워낙 막대하여 2019년부터 2024년까지 CAGR이 15.6% 상승해 약 18억 달러 규모에 달할 것으로 전망됩니다.[7]

SOAR 솔루션은 보안팀이 무수히 많은 보안 도구를 통합하는 데 도움이 되며, 별개의 구성요소가 방어를 위해 협조하며 서로 통신하고 함께 작용할 수 있습니다. 이 때문에 네트워크 가시성이 향상될 뿐만 아니라 사이버 보안과 관련된 위협경고 수를 줄이고 좀 더 전략적인 경고를 얻을 수 있습니다.[4] 구체적으로 설명하자면 SOAR는 보안 운영팀에서 사람이 직접 감독할 필요가 없는, 지루하고 반복적인 워크플로 요소를 자동화하는 동시에 담당자의 권한은 그대로 유지하도록 도와줍니다. 가장 좋은 SOAR 솔루션은 위협을 보강하고 컨텍스트와의 관련성을 파악하여 애널리스트가 위험의 심각도, 민감도 또는 위협의 목표가 되는 비즈니스 부서의 중요도 등에 따라 사례를 신속하게 분류하는 데 유익한 역할을 합니다.[5]

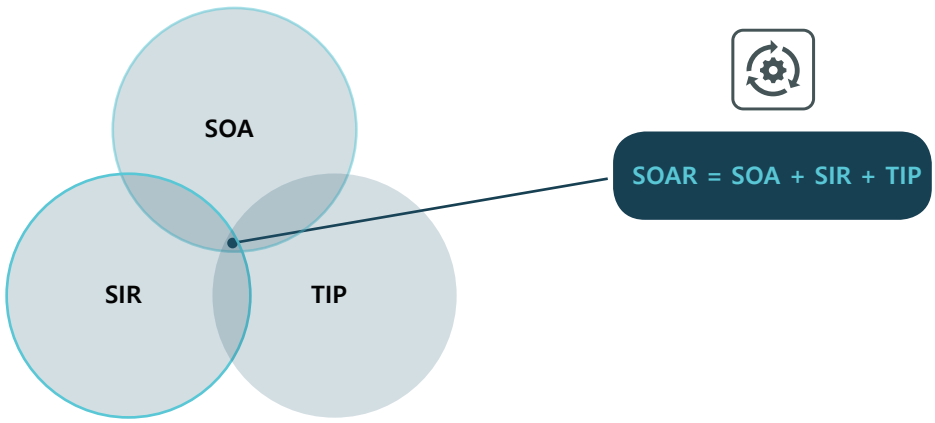

그림 1: SOAR는 제때 위협을 식별하여 완화하기 위해 필요한 세 가지 주요 기능을 모아놓은 솔루션입니다.

FortiSOAR로 보안의 통합과 대응의 자동화

FortiSOAR는 보안팀이 광범위한 보안 제품으로부터 제공되는 위협 경고를 취합하여 보강할 역량을 제공합니다. 잘 정의된 환경설정을 활용해 오케스트레이션과 관리가 간소화되므로, 시간이 오래 걸리는 수동 워크플로를 없앨 수 있습니다.

그림 2는 FortiSOAR가 SOC 팀에서 최대 98%나 인시던트 대응 시간을 단축하는 데 어떤 면에서 유익한지 나타냅니다. 비효율적이고 오류가 발생하기 쉬운 수동 단계는 최장 15시간이나 걸릴 수 있는데, FortiSOAR는 총 20분(평균)이면 완료되는 자동 프로세스를 제공합니다.

인시던트 대응 시간: 수동 대 FortiSOAR 비교

단계	수동	FortiSOAR
아티팩트를 보강하여 IOC 식별	46~60분	3분
SIEM에서 받은 이벤트 분류 수행	20분	1분
데토네이션 엔진에 압축(Zip) 파일 제출	1~6시간	1분
영향을 입은 디바이스 분리	10분	1분
인시던트 분석, 생성 및 주석 달기	60분	5분
방화벽(예: FortiGate)에서 IOC 차단	45분~2시간	2분
수정 및 인시던트 대응	60분~6시간	5분
인시던트 요약 보고서를 작성하여 보내기	2~3시간	2분
총합	**4.5~15시간**	**20분**

그림 2: FortiSOAR는 SOC 팀에서 인시던트 대응 시간을 단축하는 데 도움이 됩니다.[8]

FortiSOAR는 통합된 포티넷 보안 패브릭 아키텍처의 일부분으로서 여러 가지 보안 도구를 단 하나로 통일합니다. 이를 통해 FortiSOAR는 레벨이 낮은 Tier-1 위협 경고 프로세스를 대부분 자동화하여 팀의 작업 부하를 덜어줌으로써 SOC 애널리스트가 좀 더 중요한 작업에 집중할 수 있게 됩니다. 다음 네 가지 핵심 사용 사례는 과도한 업무 부담에 시달리는 SOC 팀을 위해 FortiSOAR가 즉각적으로 제공할 수 있는 가치를 나타냅니다.

사용 사례 1: 통일된 SOC 워크벤치

FortiSOAR는 벤더를 가리지 않는 SOAR 제품으로서 서로 다른 포인트 보안 솔루션을 단 하나의 중앙 집중식 오케스트레이션 시스템에 통합하여 복잡한 SOC를 간소화해줍니다. 이러한 시스템은 사실상 어떤 환경에도 배포할 수 있습니다. 여기에는 300여 가지 기성품(바로 사용 가능한) 커넥터가 포함되어 있습니다. 따라서 SOC 팀에서는 다른 벤더에서 제공한 기존 보안 솔루션과 FortiSOAR를 함께 운영할 수 있으며, 기업 전체에 걸쳐 중앙 집중식 가시성과 제어 권한을 제공하는 동시에 위협 경고 정보를 수집할 수 있습니다. 이렇게 통합하면 보안 파편화 현상을 막을 수 있고 보안 운영 프로세스가 간소화되며 기존 도구의 사용 수명을 늘려 ROI(투자수익)를 극대화하는 데에도 도움이 됩니다. FortiSOAR는 보안팀이 보안 프로세스 전체를 중앙에 집중하고 현재 보유한 도구에 모두 대응할 수 있도록 지원하여 결과적으로 전보다 더욱 빠른 실시간 대응을 보장합니다.

사용 사례 2: 자동 위협 경고 분류

인시던트 대응 프로세스가 시간을 오래 잡아먹는 탓에, 애널리스트가 수신되는 위협 경고의 속도를 따라잡기가 점점 더 어려워지고 있습니다. FortiSOAR는 이러한 경고를 한 곳에 집계하면서 추가적인 컨텍스트로 보강하여 해결까지 걸리는 시간을 단축합니다. 또한 "오탐지" 경고 수를 줄여주고 지능형 관리 기능도 다양하게 제공하여 조사를 정의, 감독하고 속도를 빠르게 하는 데에도 도움이 됩니다. FortiSOAR는 위협 경고 수집, 심각도에 따른 우선순위 지정, 작업 할당 및 서브루틴 등과 같은 단순한 SOC 작업을 간소화합니다. 또한 분류, 보강, 조사 및 수정과 같은 복잡한 E2E(exchange-to-exchange) 작업도 자동화하여 보안 프로세스 전체에 걸친 경고의 상관관계를 자동으로 정립해 하나의 인시던트로 정리함으로써 보안 프로세스를 응집력 있는 중앙 집중식으로 바꿔줍니다.

이처럼 정교한 통합 및 자동화 기능을 활용하면 위협 경고 피로와 관련된 흔한 부담 중 대다수를 없앨 수 있습니다. 따라서 SOC 애널리스트는 위협 헌팅(threat hunting)과 같은 업무에 집중하면서 작업 부하는 줄이고, 침해 위협에 노출되는 기간을 줄일 수 있습니다.

사용 사례 3: SOC를 증강하여 인시던트 대응 속도 가속

수많은 수동 워크플로가 존재함으로 인해 위협 조사에 차질이 빚어지고, 해결까지 걸리는 시간이 늘어나면서 사람이 직접 감독하고 그로 인한 오류가 발생할 위험이 커집니다. 이런 상황에 처한 기업은 단순히 운영 업무가 비효율적으로 처리되는 것에 그치지 않고, 한층 커진 침해 위험에 노출됩니다. 이에 대한 처리 방안으로 FortiSOAR를 활용해 SOC를 증강하면 FortiAnalyzer의 로깅 및 보고 자동화 기능과 FortiSIEM 보안 정보 및 이벤트 관리(SIEM) 솔루션 등의 이점을 확대 적용할 수 있습니다. 이렇게 하면 모든 SOC 프로세스가 강력하게 오케스트레이션 및 자동화되며 전반적인 보안 상태가 개선됩니다.

보안팀에서는 기업의 요구사항에 따라 모든 작업, 변경 또는 업데이트를 자동화하여 효율성을 증강할 수 있습니다. FortiSOAR는 작업 하나만 자동화하는 것이 아니라, SOC 전체를 증강하여 전반적인 보안을 개선합니다.

FortiSOAR는 고유한 사용자 지정이 가능합니다. 보안팀에서 각종 대응과 서브루틴을 얼마든지 자동화할 수 있습니다. 일반적으로 임계값 조건을 설정하여 이 조건에 부합하면 FortiSOAR가 오프라인으로 즉시 ID를 입수하여 이를 기본 제공되는 환경설정과 커넥터에서 활용해 최적의 인시던트 대응을 달성하도록 합니다.

사용 사례 4: 한정된 SOC 팀 리소스의 부담 덜기

FortiSOAR는 자동화된 워크플로를 통해 보안 운영과 프로세스를 간소화함으로써 보안 인시던트 대응과 관련하여 발생하는 직원 시간과 비용을 절약합니다. 위협 환경이 계속 발전하고 보안 디바이스가 급증하면서 SOC 효율성을 증강하면 네트워크 보안에 드는 총소유비용(T-CO)을 대폭 절약할 수 있습니다.

FortiSOAR가 보안 직원의 부담을 덜어주는 한 가지 방법으로 SOC팀이 도구의 프로토콜과 자동 보안 대응을 각자의 SOC 프레임워크 및 요구사항에 맞게 사용자 지정할 수 있도록 지원합니다. 이렇게 하면 대응 과정 중에 필요한 수동 작업량이 최소한으로 줄어들어 팀의 전반적인 작업 부하가 확실히 줄어듭니다.

FortiSOAR는 간편한 도입을 위해 바로 사용 가능한 드래그앤드롭 환경설정 옵션을 제공하여 즉시 구성할 수 있으며, 바로 효과를 볼 수 있습니다. FortiSOAR는 SOC팀이 내부적인 지식을 유지, 관리하는 데에도 도움이 됩니다. 직원이 기업을 퇴사하더라도 그 직원이 가지고 있던 워크플로, 인사이트 정보와 경험을 통해 얻은 데이터는 시스템 내에 문서로 기록되어 있으므로 온전히 유지됩니다.

발전된 SOC를 위한 강력한 솔루션

SOC는 자동화 레벨에 따라 크게 세 가지로 분류할 수 있습니다(그림 3 참조). 인력 수준과 기업 구조가 달라 각 레벨의 SOC에는 특징적으로 서로 다른 여러 가지 문제가 수반됩니다. 포티넷 보안 패브릭은 각 자동화 레벨에 뒤따르는 문제에 고유하지만 통합된 세 가지 제품을 제공하여 해결책을 제시합니다. 그 세 가지란 FortiAnalyzer 로깅 및 보고, FortiSIEM 보안 정보 및 이벤트 관리, 그리고 FortiSOAR입니다.

98%

FortiSOAR로 단축할 수 있는 인시던트 대응 시간[9]

FortiSOAR의 강력한 기능이 가장 진가를 발휘하는 곳은 SOC 자동화 레벨 3입니다. 레벨 3은 노련한 보안팀(애널리스트가 5명 이상), 잘 정의된 보안 프로세스 및 상당한 규모의 보안으로 정의됩니다.

FortiSOAR는 포티넷 보안 패브릭과 멀티벤더 환경 전체에 걸쳐 보안 프로세스를 완벽하게 오케스트레이션하고 자동화해야 하는 엔터프라이즈 팀에 맞게 고안되어 있습니다. FortiAnalyzer와 FortiSIEM의 기능을 기본 토대로 좀 더 종합적인 워크플로 자동화와 오케스트레이션을 추가하고, AI 지원 경고 우선순위 지정은 물론 데이터 수집과 대응 조율을 위한 더 많은 기본 제공 커넥터를 제공합니다. 또한 FortiSOAR는 SOAR와 비슷한 분석 또는 전용 제품을 여러 개 사용해온 SOC에도 매우 효과적입니다. 이런 SOC는 SOAR에 맞는 수준의 성숙도를 갖추고 있을 가능성이 높고, FortiSOAR는 효과적이고 효율적인 업그레이드를 제공합니다.

FortiSOAR: SOC 자동화 수준

- SOC 효율성을 간소화하고 인시던트 대응 속도 가속

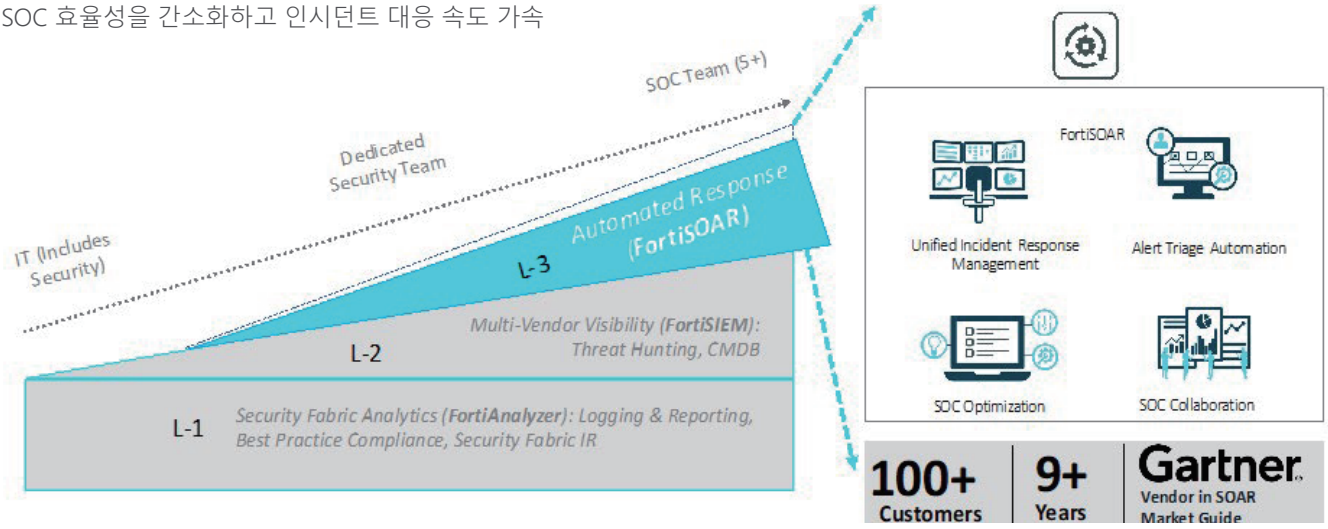

그림 3: FortiSOAR는 최고 수준의 SOC 자동화를 위해 고안되었습니다.

위험, 리소스 및 결과 관리

보안 운영팀은 앞으로도 점점 더 확장되는 공격 면, 그리고 리소스 부족이라는 압박에 시달리며 점점 더 커져가는 위험 노출도에 속도를 맞추기 위해 애써야 합니다. 모든 기능을 제공하는 효과적인 SOAR 솔루션이 있으면 성숙한 SOC 팀에서 이러한 난제를 해결하면서 그와 동시에 자사의 기업 보안 프로세스를 강화, 최적화하고 보강할 수도 있습니다.

FortiSOAR는 민첩하고 사용자 지정 가능한 솔루션을 제공하여 보안 운영팀이 점점 더 진화하는 위협 환경에 신속하게 적응하며 대응책을 적용하는 데 도움이 됩니다. FortiSOAR의 자동화 및 오케스트레이션 기능을 활용하여 인시던트 대응 프로세스를 전반적으로 한 단계 발전시킬 수도 있습니다. 그러면 기업에서는 보안을 간소화하고 위협 경고 피로를 없애며 대응 시간을 단축하고 한정된 SOC 팀 리소스에 가해지는 부담을 덜면서 팀 작업능률을 극대화하는 등 다양한 성과를 얻을 수 있습니다.

또한 FortiSOAR는 사용자 기반, 예측 가능한 라이선싱 모델을 통해 간소화된 라이선싱을 제공합니다. 이 때문에 FortiSOAR의 효율성은 활용하면서도 정해진 예산을 넘기지 않을 수 있으며, 처리하는 인시던트의 양과는 무관하게 어느 팀이나 똑같이 얻을 수 있습니다. FortiSOAR는 본질적으로 확장 가능한 아키텍처를 가지고 있으므로 성장 중인 엔터프라이즈 조직에 고도의 가용성을 제공하여 성장 중이거나 분산된 기업 조직 전체에 걸쳐 솔루션을 확장하면서도 규모에 맞춰 배포 및 관리하는 데 필요한 리소스에는 영향을 미치지 않습니다.

FortiSOAR는 단독형 SOAR 제품

- 기업을 위해 여러 출처에서 데이터를 수집하여 기업이 정보를 이해하도록 돕고 보안 프로세스를 최적화하는 동시에 자동 대응 기능 제공

SOC 관리

- 엔터프라이즈 사례 관리
- 역할 기반 액세스

오케스트레이션과 자동화

- 환경설정
- 커넥터/통합

사례 관리

- 인시던트 대응을 위한 OOB 모듈, 취약성 및 위협 관리
- 나만의 모듈 구축(예: GDPR, Legal)
- 상황별 가시화

간소화된 대응

- 비주얼 플레이북 디자이너
- 자동 작업을 위한 커넥터 300여 개
- 실제 사용 사례에서 가져온 참조 콘텐츠

멀티테넌트

- 분산형/연합형 아키텍처
- 데이터 및 환경설정에 대한 액세스 제어

그림 4: FortiSOAR는 엔터프라이즈 보안 아키텍처에 꼭 필요한 주요 기능을 제공하는 중요한 제품을 모아놓았습니다.

[1] "전체 엔터프라이즈의 53%는 자사 보안 도구가 제대로 작동하는지 몰라(53% of enterprises have no idea if their security tools are working)," Help Net Security, 2019년 7월 31일.

[2] "2019년도 데이터 침해 비용 보고서(2019 Cost of a Data Breach Report)," Ponemon Institute and IBM Security, 2019.

[3] "튼튼한 사이버 보안 팀의 구축 및 성장을 위한 전략(Strategies for Building and Growing Strong Cybersecurity Teams): (ISC)2 Cybersecurity Workforce Study, 2019," (ISC)2, 2019.

[4] Muhammad Omar Khan, "대규모 사이버 보안 침해를 막기 위해 SOAR가 전도유망한 이유(Why SOAR is a Good Bet For Fighting Mega Cyber Security Breaches)" Entrepreneur, May 23, 2019.

[5] Cian Walker, "SOAR:보안 관제의 두 번째 대표 무기(SOAR: The Second Arm of Security Operations)" Security Intelligence, 2019년 4월 9일.

[6] "2019년도 데이터 침해 비용 보고서(2019 Cost of a Data Breach Report)," Ponemon Institute and IBM Security, 2019.

[7] "SOAR 세계 시장 현황, 2024년까지의 전망(Security Orchestration Automation & Response (SOAR) World Markets, Outlook to 2024):오탐지 알림이 많을수록 유리한 시장 기회를 의미(The High Number of False Security Alerts Presents Lucrative Market Opportunities)," Research and Markets, 2019년 11월 5일.

[8] 포티넷 내부 계산치.

[9] 위와 같은 책(자료).