IDG
STRATEGIC
MARKETING SERVICES

IBM

IDG Summary | SOAR

“보안, 사고 대응에 초점을 맞춘다” SOAR의 효과와 도입 선택 기준

“완벽한 보안이란 없다.” 모두가 인정하는 사실이지만, 정작 보안 사고에 제대로 대응하는 조직은 소수에 불과하다. 조직의 보안 담당자는 진화하는 공격과 까다로운 컴플라이언스, 보안 인력 부족, 복잡해지는 운영 환경 등 많은 보안 과제로 인해 그 스트레스는 더 가중되고 있다. 이를 해결하고자 등장한 것이 바로 SOAR(Security Orchestration, Automation and Response)이다. SOAR는 다양한 보안 위협에 대한 대응 프로세스를 자동화하고 조율해 SOC(Security Operation Center) 직원의 단조롭고 반복적인 업무를 효과적으로 줄이고, 각종 보안 이벤트를 빠르고 정확하게 대응할 수 있게 도와주는 새로운 보안 패러다임이다. SOAR의 의미와 효과, 그리고 이를 도입하는 데 준비해야 할 것들이 무엇인지 알아보자.

“보안, 사고 대응에 초점을 맞춘다” SOAR의 효과와 도입 선택 기준

김승준 | 한국IBM 보안사업부 실장

일반적으로 사이버보안의 프레임은 크게 예방(Prevention), 탐지(Detection), 대응(Response)으로 나눌 수 있다. 지금까지 조직은 엔드포인트 보안, 네트워크 보안 등 보호 부문에 투자를 집중해왔다. 하지만 지난 십수 년 동안 하루가 멀다하고 발생하는 보안 사고를 통해 전세계는 사이버 공격을 예방하려는 노력만으로는 보안 위협으로부터 벗어날 수 없다는 것을 알게 됐다.

또한 기존에 투자했던 보안 솔루션이 생성하는 로그 데이터나 이벤트가 많아지면서, 기업은 시스템 로그 및 보안 이벤트를 중앙으로 모으고 분석하여 위협을 탐지할 수 있는 SIEM(Security Information and Event Management)을 도입했다. 이런 노력으로 인해 ‘2017 M-트렌드 보고서’에 따르면, 사이버침해 탐지 시간은 2015년 평균 146일에서 2016년 평균 99일로 감소했다. 최근에는 탐지 시간을 더 줄이고 정확성을 높이기 위해서 인공지능과 머신러닝 기술을 이용한 탐지 솔루션들을 이용하고 있다.

전세계 3,600명 이상의 보안 및 IT 전문가를 대상으로 포네몬 연구소와 IBM이 조사한 ‘2019년 기업 사이버공격 대응 실태’ 보고서에 따르면, 조직 가운데 절반 이상이 사이버보안 사고에 적절하게 대응할 수 있는 역량을 갖추지 못한 것으로 밝혀졌다. 응답자 가운데 77%는 조직 전반에 걸친 사이버보안 사고 대응 계획(CSIRP)을 보유하지 않았다고 답했다. 대응 계획을 갖추고 있다고 답한 23%에서도 절반 이상(54%)은 정기적인 테스트를 실시하고 있지 않다고 답했다. 더불어, EU의 일반개인정보보호법(GDPR)이 시행된 지 1년이 다 된 시점에도 불구하고 46%의 조직이 규정을 완벽하게 준수하지 못하고 있다.

한편 조직의 57%가 사이버 공격을 확인하고 대응하기까지 걸리는 시간이 증가하고 있다라고 응답했으며, 60%가 넘는 조직이 보안 사고의 피해와 심각성이 점점 더 커지고 있다고 우려했다.

사고 대응에 대한 SOC의 고민

보안 사고는 발생한다는 것을 전제로 해야 한다는 주장은 이제 모두가 인정하고 있지만, 보안 이벤트나 사고에 제대로 대응하는 조직은 소수에 불과하다. 2019년 포네몬의 한 보고서에 따르면, 전사적으로 적용되는 사이버보안 사고 대응 계획을 갖추고 있다고 응답한 조직 중에서도 업데이트 기간이 정해져 있지 않은 조직이 42%, 1년에 한번 검토하는 조직이 34%였다. 조직에서 사고 대응이 제

대로 이뤄지지 않는 이유는 무엇일까?

우선 조직의 77%가 보안 전문가를 고용하고 유지하는데 어려움을 겪고 있다. 보통 SOC(Security Operation Center)에서 숙련된 보안 인력은 고용하기가 힘들고, 막상 고용했다 하더라도 유지하기가 어렵다. 사이버시크(CyberSeek)에 따르면, 약 2만 개의 사이버보안 관련 일자리가 충원되지 못한 상태다.

두 번째, 지속적으로 계속 증가하는 공격 빈도와 위험성이다. 지난 한해 동안 악성코드 감염은 더욱 심해졌다. 응답자의 60%는 지난 한해 동안 악성코드 감염의 심각성이 증가했다고 밝혔다. 보안 직원은 악성코드 경고에 대응하는데 소요되는 시간의 2/3가 오탐을 추적하는데 낭비했다. 이는 매주 평균 395시간으로 시간당 매주 평균 2만 5,000달러, 매년 127만 달러의 비용을 낭비하는 것으로 추산된다.

세 번째, 지난해 5월에 시행된 GDPR은 국내 기업이라도 유럽 고객을 보유하고 있거나 유럽 지역에 인력을 운영하고 있다면 GDPR 규제에 대응해야 한다. 현재 국내 기업은 GDPR 시행 전후로 컨설팅을 받고 있지만 내부 데이터 유출이나 개인정보 유출 사고가 발생할 경우, 72시간 내에 보고를 하거나 적합한 사고 대응을 위한 문서화된 사고 대응 프로세스를 제대로 갖추지 못하고 있다. 한편 익스피리언(Experian)과 포네몬(Ponemon) 보고서에 따르면, 자체 데이터 침해 대응 계획의 효과가 "매우 높다"고 답했다.

네 번째, 복잡해지는 SOC 운영 환경이다. SOC는 평균 75개 이상의 보안 툴을 사용하고 있는데, 이를 제대로 제어하기란 쉽지 않다. 예를 들어, 20명이 운영하는 SOC 팀의 경우, 관리자와 선임을 제외하면 15명이 남는다. 이를 주야간(3교대)으로 나누면, 결국 5~7명이 75개 툴을 운영해야 하는 상황이 된다.

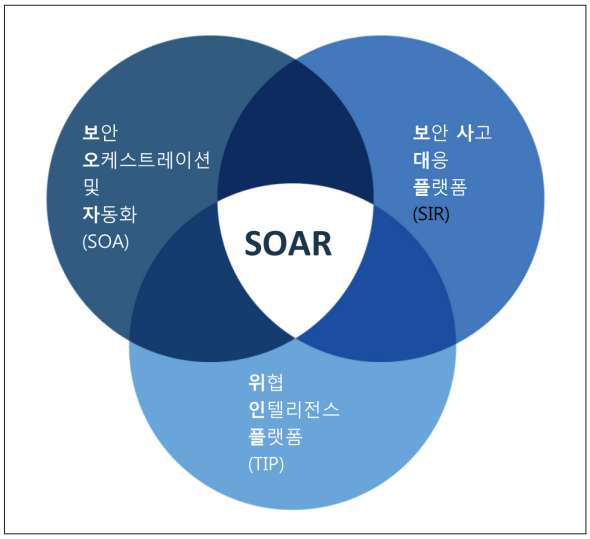
해가 지날수록 보안 이벤트의 양과 심각도, 그리고 처리 시간이 증가하고 있으며, 사고 발생 시 기업에 미치는 영향 또한 높아지고 있다. 최근 SOC가 겪는 고민은 다음과 같이 6가지로 정리된다.

- 보안 사고유형 별 표준화된 대응 프로세스 부재
- 업무에 대한 성과관리 어려움
- 사고 대응 업무에 대한 데이터 공유 어려움
- 보안 사고 대응 시 외부 및 내부 협업 프로세스 부재
- 보안 인력 확보의 어려움과 인력 부재 시 업무 처리에 대한 이슈 발생(지연 또는 단절)
- 복잡한 컴플라이언스 대응의 어려움

SOAR = SOA+SIRP+TIP

보안 위협을 사전에 예방하고 탐지하는 노력만으로는 위협으로부터 벗어날 수 없음을 인지하면서 등장한 것이 바로 보안 운영 자동화 및 대응(Security Orchestration, Automation and Response, SOAR)이다. 2017년 가트너는 "기술 인력, 전문성, 예산 부족과 더불어 적대적 위협 발생이 증가하고 있는 현 과제를 해결하기 위해 조직은 SOAR 기술을 검토하고 있다"고 밝혔다.

그림 1 | SOAR의 3대 필수 기능



출처: 가트너

SOAR는 다양한 보안 위협에 대한 대응 프로세스를 자동화해 낮은 수준의 보안 이벤트는 사람의 도움없이 처리하고, 보안 사고 발생시 표준화된 업무 프로세스에 따라 직원이 쉽게 대응할 수 있게 도와주는 보안 솔루션이다. 가트너는 SOAR를 통해 사람(People), 기술(Technology) 그리고 프로세스(Process)를 조율하고 자동화함으로써 조직에서 사고 대응 효율성과 일관성을 개선하고자 한다. SOAR는 보안 오케스트레이션 및 자동화(Security Orchestration and Automation, SOA), 보안 사고 대응 플랫폼(Security Incident Response Platform, SIRP), 위협 인텔리전스 플랫폼(Threat Intelligence Platform, TIP)의 세 가지 보안 대응 영역을 제공한다.

SOA(Security Orchestration and Automation) 영역은 보안 대응팀의 단조롭고 반복적인 업무를 파악하고 그 업무에 소요되는 시간을 줄여준다. 이는 툴 간 워크플로우를 자동화시키는 영역으로, SOAR의 핵심 기능이라 할 수 있다. SIRP(Security Incident Response Platforms) 영역은 툴 간 자동화가 아니라 프로세스의 자동화다. 보안 사고가 발생하면 사고 유형별로 내부 보안 사고 대응 정책에 의해 미리 정해진 프로세스에 따라 어떤 업무를 할 것인지, 해당 업무가 누구에게 할당되고 SLA에 의해 언제까지 마무리해야 하는지 관리해주는 것이다. TIP(Threat Intelligence Platforms)은 조직에서 발생하는 보안 위협의 분석 업무를 지원하기 위해 여러 소스의 위협 데이터를 실시간으로 수집, 상관 분석해 제공한다. 분석된 위협 정보 데이터를 기업의 기존 보안시스템이나 대응 솔루션과 연계해 위협 요소를 제공함으로써 보안 인력의 사전 대응력을 높여준다.

ESG 조사에 따르면, 1,000명 이상 기업의 19%가 이미 SOAR를 위한 기술을 광범위하게 도입하고 있다. 39%의 기업이 제한적으로 추가하고 26%는 이 기술을 추가하는 프로젝트에 참여하고 있으며, 13%는 가까운 미래에 구현하거나 관심을 갖게 될 것이라고 응답했다. 가트너는 2020년까지 5명 이상의 보안 전문가를 보유한 보안 조직 가운데 15%가 SOAR를 채택할 것으로 예측했다.

OODA 방법론을 기반으로 한 IBM의 리질리언트 SOAR 플랫폼

IBM의 리질리언트 SOAR 플랫폼(Resilient SOAR Platform)은 가트너의 SOAR 핵심 요소 3가지를 모두 갖춰 SOC에서 특정 이벤트나 사이버보안 사고가 확인되면 정확하고 빠르게 처리, 대응할 수 있는 환경을 제공한다. 2016년 리질리언트 시스템을 인수한 IBM은 현재 SOAR 분야에서 30개국 300곳 이상의 고객을 보유하고 있다.

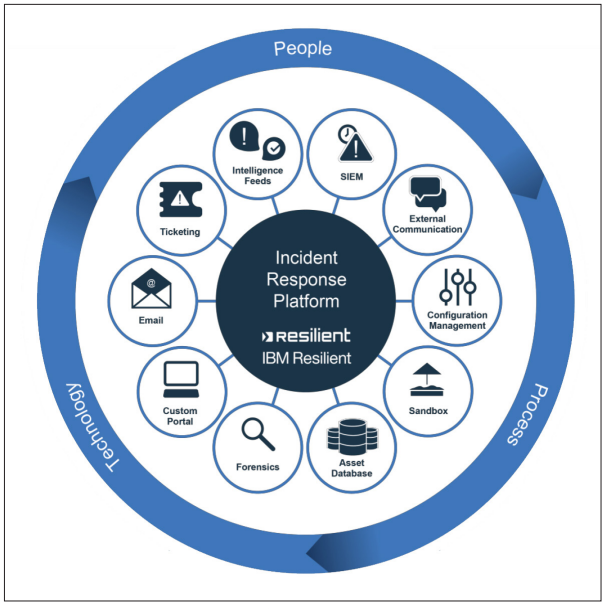
IBM 리질리언트 SOAR 플랫폼은 최근 혁신을 통해 조직을 역동적이고 빠른 대응 프로그램을 작성하는 데 필요한 도구를 보유하고 있다. OODA(Observe,

Orient, Decide, and Act) 루프 방법론을 기반으로 한 이 플랫폼은 분석가가 사고 대응 프로세스를 좀 더 빠르고 정확하게 처리할 수 있도록 도와준다. 또한 100가지가 넘는 보안 툴과 통합할 수 있어 기존 보안 환경과 사고 대응 프로세스와 연결하는 중앙 허브를 형성한다. 리질리언트 SOAR 플랫폼의 오케스트레이션 기능은 다음과 같다.

- 동적 플레이북(Dynamic playbooks): 복잡한 공격에 대응하는 데 필요한 민첩성과 정교함을 제공한다. 동적 플레이북은 사고 상황을 실시간으로 자동 대응하고 분석가가 사고를 접하기 전에 반복적인 초기 단계가 완료되도록 한다.
- 시각적 워크플로우(Visual workflows): 복잡 다난한 워크플로우를 시각적으로 보여줌으로써 분석가가 사고 대응을 잘 조율할 수 있도록 도와준다.
- 사고 시각화(Incident visualization): 조직 환경에서 발생한 보안 이벤트(사고) 사이의 관계 또는 IoC(Indicators of Compromise) 등을 시각적으로 표시한다.
- 타이머(Timers): 팀이 시기 적절한 대응을 보장하고 병목 현상을 식별하며 SLA를 준수할 수 있도록 워크플로우에서 시간 기반의 규칙을 적용한다.
- 아티팩트 워크플로우(Artifact workflows): 툴 간 자동화 워크플로우를 구현하는 동시에 사람 중심의 작업 및 승인을 허용한다.
- 작업 및 스크립트(Tasks and scripts): 워크플로우에서 스크립팅 기능을 추가해 플랫폼 내 자동화를 가능케 한다.

사례 관리(Case Management)와 SOA가 함께 진행되어야 제대로 된 사고 대응을 할 수 있는데, 툴 간 자동화에만 초점을 맞췄을 때에는 유연성이 상당히 떨어진다. 예를 들어, 사이버보안 사고 발생시 특정 보안 솔루션에서 로그를 분석하고 특정 IP를 뽑아내 이를 추가적으로 분석하고 최종적으로 방화벽을 차단하라는 워크플로우를 만들었다. 만약 이 IP가 잘못 탐지된 IP라면 중간에 해당 IP에 대해 사람이 한번 더 분석하고 판단한 다음, 방화벽에서 자동으로 막을지, 워크플로우 중간에서 끊을 지에 대해 판단해야 한다.

그림 2 | IBM 리질리언트 SOAR 플랫폼



전형적인 SOA 솔루션은 사람의 판단이 들어가는 부분이 없으며 기존에 만들어진 워크플로우를 통해 진행된다. SOAR에서 가장 중요한 요소는 자동화다. 하지만 가트너에 따르면, 자동화는 오케스트레이션의 일부분이며 같은 의미로 사용될 수는 없다. 즉, 지능형 오케스트레이션 기술은 툴 간의 자동화 프로세스를 이용해서 보안 사고를 처리할 수 있어야 하지만, 중요한 업무처리 단계에서는 의사 결정에 필요한 정보와 정황을 분석가에게 제공해 올바른 방향을 제시할 수 있도록 해야 한다.

사람, 기술, 프로세스를 하나로 만드는 SOAR 효과

SOAR 도입의 가장 큰 효과는 사람, 기술, 프로세스를 하나로 만드는 것이다. 다양한 경험을 갖춘 숙련 보안 직원만 알고 있는 지식을 신입 직원도 따라 할 수 있도록 반복 가능한 프로세스로 정리, 체계화한 것이다. 이를 통해 조직은 개인 직원에 대한 의존도를 낮추고 보안 기술 과제 측면에서 가장 중요한 신입 분석가를 교육하는 데 필요한 시간을 단축해 실무 처리에 대한 일관성을 높일 수 있다.

– 전사적 도입 효과

SOAR 도입 효과를 전사적으로 본다면, 100가지가 넘는 다양한 보안 기술을 통합함으로써 복잡한 공격에 대응하고 기존 보안 투자의 비즈니스 가치를 입증하며 전체 보안 스택에 대한 ROI를 높일 수 있다. 또한 SOC관리자나 기존 보안 툴과 대응 업무 프로세스를 통합하고 자동화해 SOC 생산성을 높이고 그 업무 성과를 측정할 수 있다. SLA에 준하게 업무를 시행하고 엔지니어가 올바른 기술을 사용해 업무를 수행할 수 있도록 한다. 이와 함께 필요한 대응 장비 선별 및 룰 적용 업무를 자동화해 신입 엔지니어도 정교한 위협을 관리하고 다양한 툴 속에서 헤매지 않고 조사 및 대응에 집중할 수 있도록 한다. 뿐만 아니라 최신 규제에 즉각적으로 대응하는 글로벌 규정 및 대응 계획에 대한 지식 기반을 제공해, 개인 정보 침해 규제 및 의무 이행의 복잡성을 제거함으로써 개인 정보 대응 관리를 간소화한다.

– 실무 측면에서의 효과

실무 측면에서는 플레이 북을 통해 사고 유형별 최적의 대응 프로세스를 생성하고 업무 필요 담당자에게 개별 업무 가이드를 자동으로 할당한다. 예를 들어,

표 | SOAR의 효과

Action	Before Resilient IRP	With Resilient IRP
SIEM, EDR 또는 NGFW를 통해 이벤트 수동생성	5 min	10 sec
영향을 받는 자산 확인 - CMDB / AD / IAM	5-10 min	10 sec
위협 인텔리전스 피드에 대한 IOC 확인	5 min	10 sec
앞에서 발생한 보안 사고 데이터의 상관 관계 분석	10-20 min	instant
수동 데이터 조사 - 엔드 포인트, 외부 네트워크, VPN 로그, DNS 레코드, 네트워크 인프라 및 엔드 포인트 포렌직에서 이상행위 내역 추출	30-55 min	30 sec
보안사고 업무 추적 – 보안 사고 대응주기 전반에 걸쳐 상세한 메모 및 작업 유지 필요	N/A	instant
감사 추적 및 로깅 유지 - 감독기관에서 인정하는 사건 대응 감사 기록 제출 필요	N/A	instant
보안 사고 상황보고 및 관리에 대한 **가시성 제공** 필요	N/A	instant
Total	**85 min**	**1 min**

랜섬웨어 사고가 발생한 경우, 기업마다 기본적으로 대응 프로세스의 각 단계가 명확하게 정리되어 있다. 계획 단계에서 프로세스가 문서화되고 구체화되면 사고 대응팀은 사고를 즉시 해결하기 위해 각 단계에서 취해야 할 조치를 정확히 알 수 있다. 사고 대응 프로세스를 설계하고 공식화하는 과정에는 필연적으로 사람이 개입된다. 그런데 이 조치에 대해 SOC 직원 모두가 숙련자는 아니다. 전반적인 업무 프로세스는 노련한 엔지니어에게 국한되어 있고, 이러한 정보의 공유도 쉽지 않은 것이 현실이다. 이를 문서화했다고 하더라도 정작 사고가 발생했을 때 찾아보고 업무에 반영하기 어렵다. 플레이 북은 직원 자신이 어떤 업무 프로세스를 거쳐야 하는지 리질리언트 시스템을 통해 확인할 수 있으며, 로그인하면 어떤 업무를 해야 하는지 업무별로 가이드를 받을 수 있다.

또한 SOAR는 서드파티 보안 솔루션 연동을 통해 위협정보에 대해 분석하고, 정형화된 사고에 대해 자동으로 대응해 불필요한 업무 리소스 낭비를 최소화한다. 이는 SOC 직원이 단조롭고 반복적으로 수행하는데 걸리는 업무 시간을 현저히 줄여 업무량에 대한 스트레스를 낮추고 사고 대응에 효율적으로 시간을 할애할 수 있도록 돕는다.

컴플라이언스와 관련된 보안 사고 유형에 대해 필요한 대응 프로세스를 생성하고 자동으로 역할을 할당한다. 사고 대응 업무 프로세스를 생성할 때 컴플라이언스에 준하게 업무 프로세스를 생성했다면, 대응업무 또한 규정에 위배되지 않고 자연스럽게 컴플라이언스를 준수하면서 업무를 처리할 수 있게 된다.

이후 보안 사고에 대한 히스토리 통합 관리를 통해 향후 유사 공격에 대한 빠르고 정확한 대응을 할 수 있으며 사고 대응 팀 운영을 통한 자동화된 보고라인 생성과 자동 적용을 기대할 수 있다.

– 관리자 측면에서의 효과

SAOR을 통해 관리자는 조직 내 전체 보안 사고에 대한 과거/현재 사고 대응 현황을 빠르게 파악할 수 있다. 또한 사고 대응 프로세스 최적화를 통해 내부 보안 기술을 상향 평준화시킬 수 있으며, 보안 자원 활용 현황을 수치화해 업무성과 측정과 ROI를 파악할 수 있다. 이와 함께 분산된 보고 시스템을 일원화해 사고 대응 업무 시 혼란을 최소화하고 보안 사고 대응을 위한 타 부서와의 협업 환경을 구축할 수 있다.

SOAR 도입을 위한 준비와 솔루션 고려 사항

SOAR를 도입하기 전에 조직이 준비해야 할 것은 두 가지로 볼 수 있다.

우선 기본적인 사고 대응 프로세스가 정의되어야 한다. 보안 사고 발생시, 어떻게 할 것인지 미리 정해놔야 한다는 것이다. 예를 들어, SOC가 랜섬웨어의 감염을 탐지했을 때나 SQL 인젝션 공격을 탐지했을 때, 어떤 조치를 취하고 대응할 것인지 사전에 업무 프로세스를 수립해야 한다.

두 번째, 정의된 업무 프로세스 가운데 자동화시킬 수 있는 부분을 찾아야 한다. 보안 사고가 발생하면 사전 정의한 업무 프로세스대로 이행하게 되는데, 이

가운데 특정 보안 솔루션과 연계하는 작업이 있다. 예를 들어, 샌드박스(Sandbox)를 통해 악성코드의 유입여부를 확인하거나, LDAP(Lightweight Directory Access Protocol)에서 감염된 단말의 사용자가 누구인지 확인하거나, 관계자에게 이메일을 보내는 등 여러 가지 업무가 있는데, 업무 프로세스 성격에 따라 해당 업무가 사람에게 맡겨지느냐, 툴간 자동화된 프로세스에 맡겨지느냐가 정해진다. 해당 업무 중 자동화 기술이 적용될 부분을 확인해야 한다.

최근 SOAR가 떠오르면서 많은 보안업체가 관련 솔루션을 확보하고 시장 공략에 나섰다. 많은 업체가 사고 대응 범위 내에서 특정 분야를 지원하는 툴을 제공하고 있지만, 가트너가 주창하는 세 가지 필수 대응 영역과 이 영역의 완벽한 조합을 제공하는 업체는 거의 없다. 따라서 조직은 SOAR를 도입하기 전 다음과 같은 질문 사항을 통해 보안업체를 평가할 필요가 있다.

1. 사고 대응 플랫폼에서 사람, 기술 그리고 프로세스를 통합해 다양한 사고 유형에 대한 유연한 대응이 가능한가
2. 자동화를 통해 좀 더 신속하고 효과적인 사고 대응을 지원하는가
3. 사고 대응 플랫폼의 효과를 추적하고 측정할 수 있는 시스템을 제공하는가
4. 보안 사고에서 법무팀, HR, 마케팅 또는 임원진의 개입이 필요한 경우, 이들에게 사고에 대해 설명하고 업무를 공유할 수 있는 기반 시스템이 있는가
5. 기존 보안 및 IT 툴과 통합되는가
6. 팀에서 사람의 개입이 필요한 업무와 자동화를 결합한 사고 대응 워크플로우를 구축할 수 있는가
7. 상황에 맞는 관련 위협 인텔리전스를 활용하는가
8. 업데이트나 커스터마이즈가 신속하고 쉽게 이뤄지는가
9. 조직 간 협업을 지원하는가
10. 플랫폼에 개인정보보호 규정 및 데이터 침해 통보 워크플로우가 포함되어 있는가
11. 공급업체가 비즈니스파트너로서 가치를 제공하는가, 신뢰할 만한 실적이 있는가

지금도 많은 조직의 임직원은 절대로 보안 사고가 발생해서는 안 된다고 생각한다. 하지만 이는 희망사항일 뿐, 어떤 기업이라도 보안 사고를 100% 막을 순 없다. 이제 조직의 보안 전략은 사고가 발생한다는 전제를 기반으로 수립해야 하며, 그래서 SOAR 도입은 필연적이다.