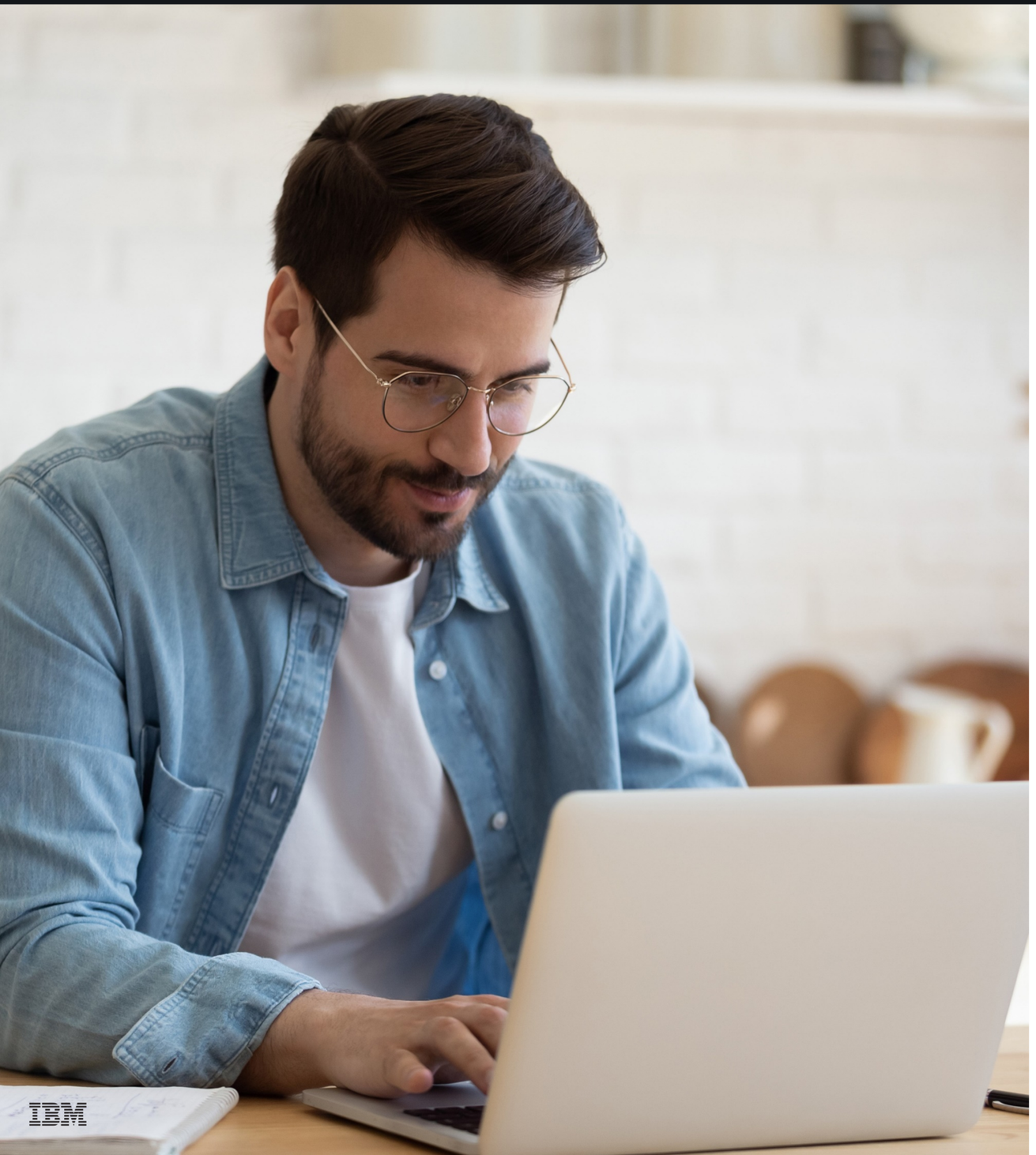
최적의 보안 플랫폼 채택 가이드

현명한 질문
최적의 해답



올바른 보안 플랫폼 선택

조직에 적합한 보안 플랫폼을 찾는 데에는 어려움이 따를 수 있습니다. 사이버 보안 분야에서 "플랫폼"이라는 용어가 남발되면서 불필요한 정보를 걸러내고 비즈니스를 위해 가장 현명한 선택을 하는 데 중요한 요인이 무엇인지 파악하기가 쉽지 않습니다. 지금 선택하는 플랫폼이 향후 몇 년간 조직의 보안 성숙도를 좌우할 기반이 될 수 있으므로 신중하게 선택해야 합니다.

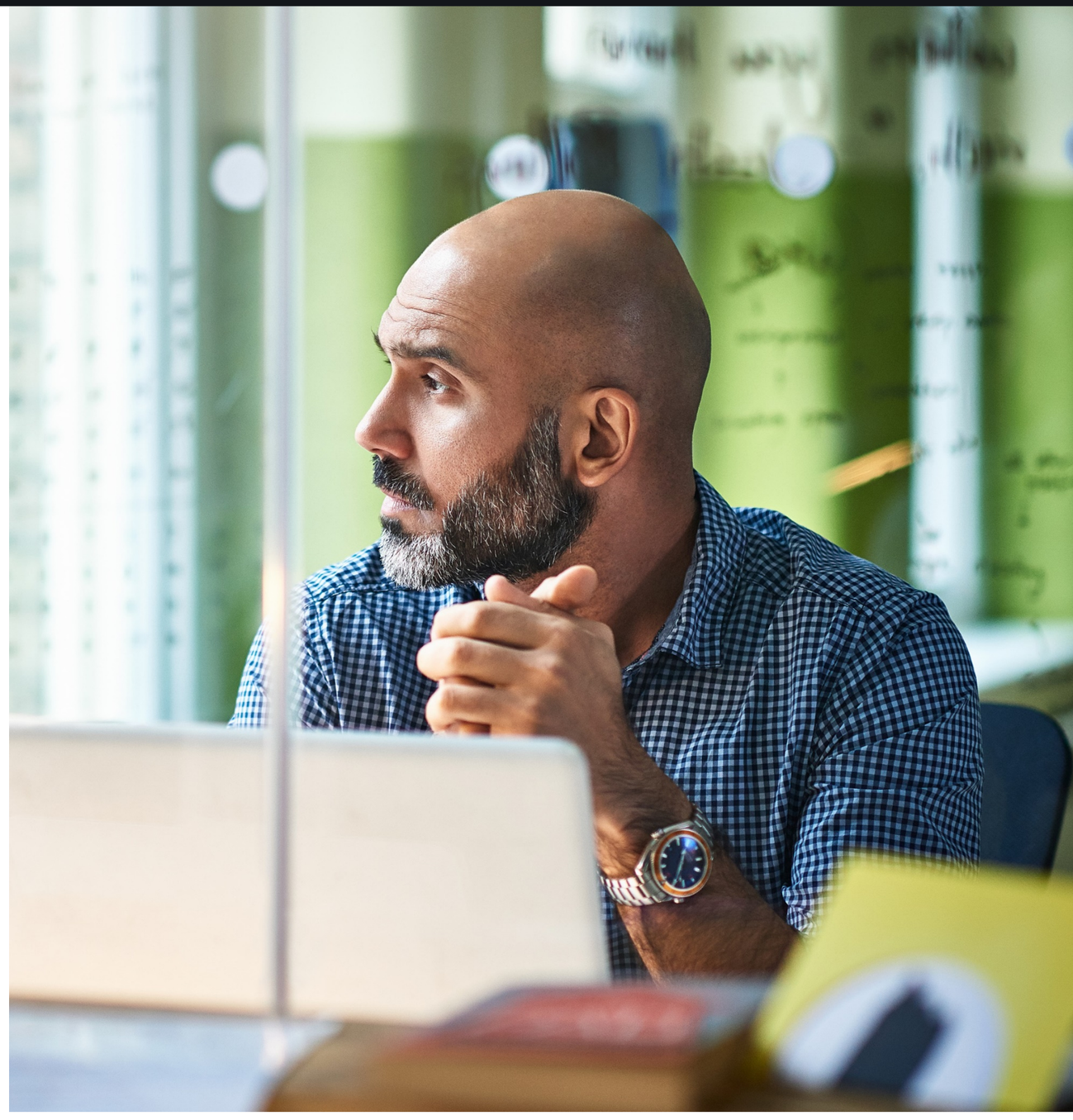
각 기업의 보안 팀은 다뤄야 할 데이터와 툴이 너무 많지만 리소스가 충분하지 않아 고전하고 있습니다. 이제는 다른 접근 방식으로 보안 데이터, 툴, 팀을 통합해야 합니다. 그리고 모든 요소를 한곳에 통합하여 진정한 통합형 보안 플랫폼의 이점을 누리는 것이 무엇보다 중요해졌습니다.

올바른 보안 플랫폼의 조건

현재와 미래에도 효과를 발휘할 거시적인 통합 사이버 보안 플랫폼을 찾으려면 다음 사항을 고려해야 합니다.

- 데이터 이동에 관한 고려사항
- 구축 옵션
- 필요한 다른 툴과의 연결
- 플랫폼의 개방성 및 적응력
- 오케스트레이션 및 자동화 기능
- 위협 인텔리전스 통합
- SOC 팀 간 연결
- 위험 관리 및 대시보드 기능
- 서비스 지원

다음 핵심 질문을 활용하여 보안 플랫폼 선택의 여러 옵션을 이해하고, 귀사에 가장 알맞은 플랫폼을 채택하십시오.



1. 진정한 가치를 누리려면 무조건 데이터를 옮겨야 할까요?

다수의 보안 플랫폼에서 모든 데이터를 해당 플랫폼으로 옮기는 것을 전제로 합니다. 모든 데이터가 한곳에 모이는 게 좋아 보이긴 하지만, 복잡해지고 막대한 비용이 들 수도 있습니다. 게다가 개인정보 보호 및 데이터 레지던시(data residency)와 관련된 중요한 문제도 해결해야 합니다.

비용과 복잡성을 고려한다면, 데이터를 기존 위치에 그대로 두고 플랫폼에서 데이터가 있는 쪽으로 연결하는 것이 나을 수 있습니다. 이 접근 방식은 기존 툴과의 시너지 효과를 통해 귀사가 지금까지 구축한 환경의 ROI를 극대화할 뿐만 아니라, 현재 각종 툴에 분산된 데이터를 중앙에서 통합적으로 모니터링하고 액세스하게 해줍니다.

2. 온프레미스, 퍼블릭 클라우드, 또는 프라이빗 클라우드에 구축할 수 있는 플랫폼입니까?

클라우드 기반 SaaS(Software as a Service) 솔루션의 형태로만 제공되는 보안 플랫폼이 많습니다. 귀사에 적합한 방식일 수도 있으나, 대개는 아직 100% 클라우드 솔루션을 도입할 준비가 되지 않아 유연한 하이브리드 멀티클라우드 아키텍처가 필요합니다. 많은 기업의 워크로드가 아직 온프레미스에 있으므로, 온프레미스, 퍼블릭 클라우드, 또는 프라이빗 클라우드에서 실행 가능하거나 SaaS 솔루션의 형태로 실행 가능하면서 유연성을 갖춘 보안 플랫폼이 진가를 발휘할 수 있습니다. 단 하나의 구축 옵션으로 선택 범위를 좁히기보다는 하이브리드 멀티클라우드 환경에 구축할 수 있는 유연한 아키텍처를 찾는 것이 좋습니다.

3. 플랫폼에서 타사 툴과의 연결 및 통합을 지원합니까?

현재 각 기업에서는 다양한 보안 툴을 사용하고 있으며, 이 모든 제품을 단일 벤더에서 공급했을 가능성은 낮습니다. 특정 벤더의 툴만 통합 가능하도록 제약을 둔 보안 플랫폼도 있습니다. 여러 벤더의 보안 툴을 사용하고 있다면, 다양한 보안/IT 툴과의 개방형 연결을 지원하는 플랫폼을 찾아야 합니다. 다음 조건을 갖춘 옵션을 선택하십시오.

- 대규모 파트너 에코시스템
- 개방형 SDK(Software Development Kit)
- 고객 맞춤형 연결을 추가하기 위한 지원 서비스

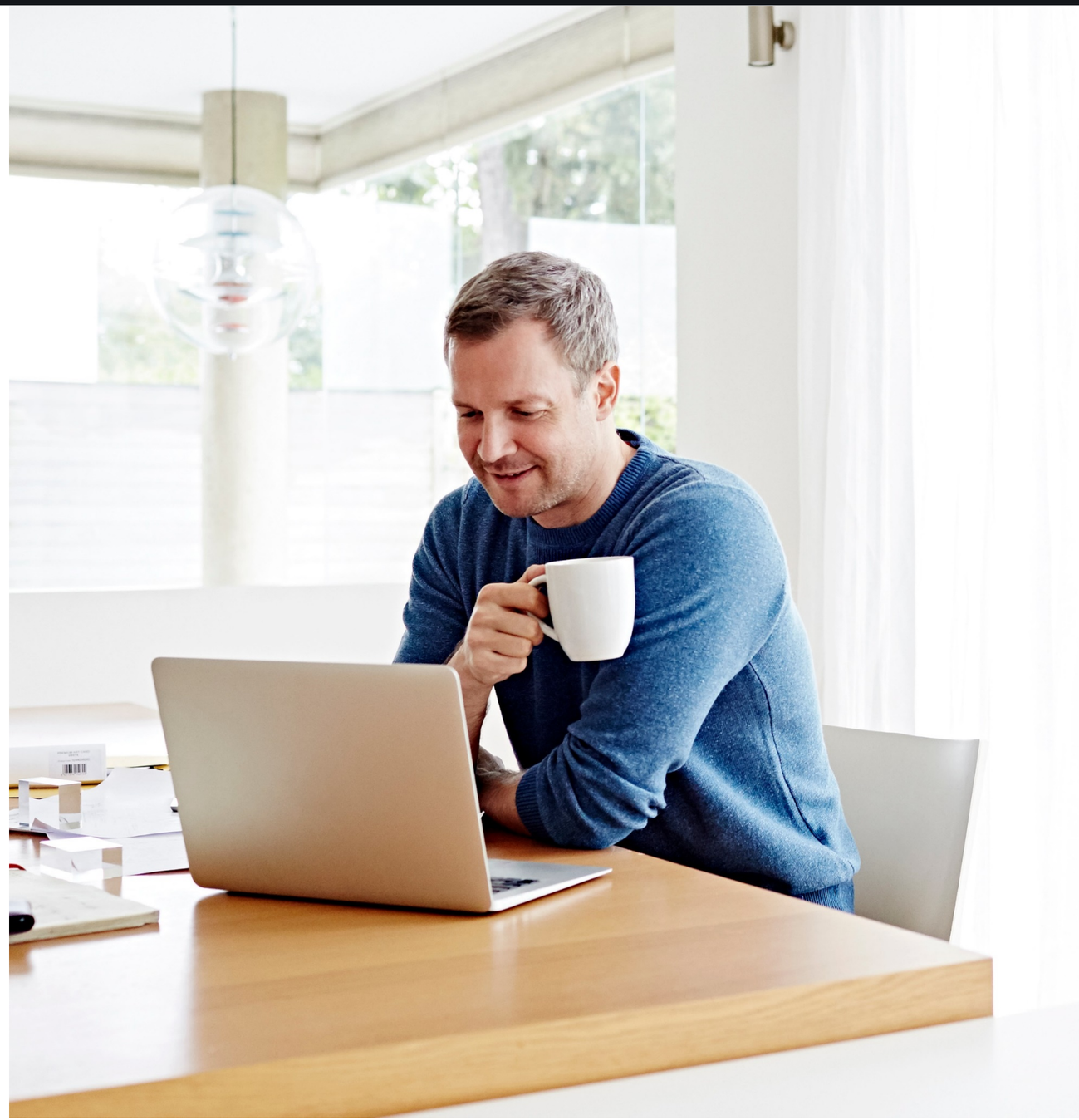
이러한 접근 방식은 해당 플랫폼이 기존 툴과 연동하는지 여부를 확인하는 데 유용하며, 기존 툴을 완전히 대체해야 하는 부담을 줄이는 데에도 도움이 됩니다.

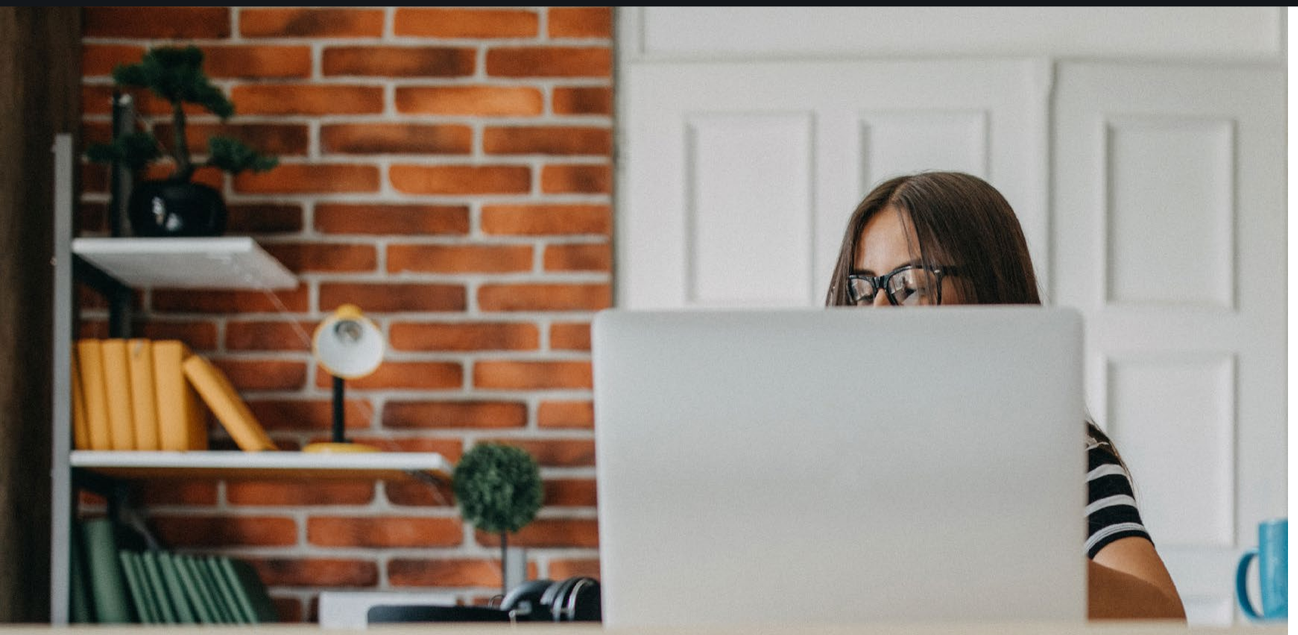
4. 보안 프로그램이 달라지면 플랫폼이 새롭게 적응합니까?

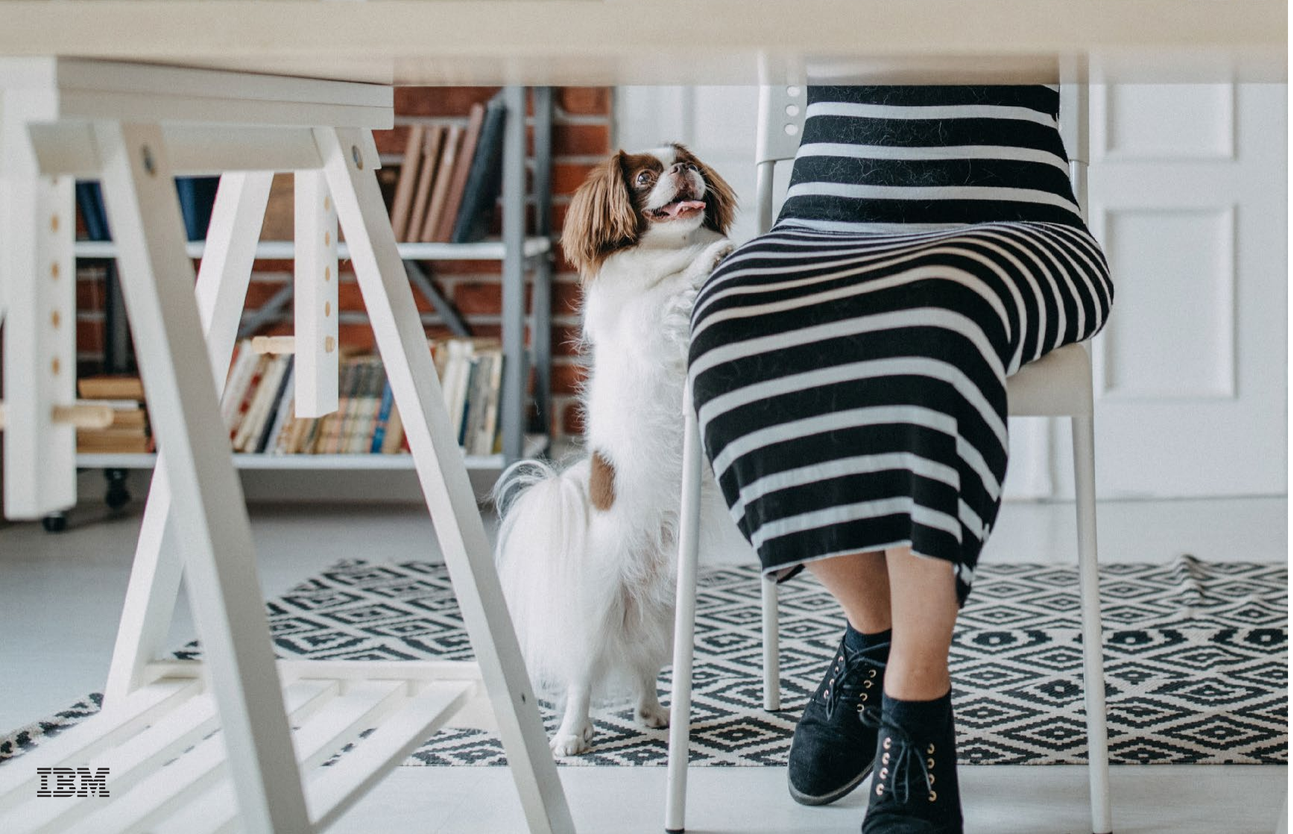
플랫폼을 선택할 때, 보안 프로그램의 변화를 제대로 지원할 만큼 개방적이고 유연한 플랫폼인지 여부가 중요한 기준이 되곤 합니다. 다음 조건을 갖추었는지 확인하십시오.

- 개방형 표준
- 오픈소스 기술
- 개방형 연결

개방형 플랫폼에서는 타사 툴과의 연결이 가능하고, 맞춤형 연결 및 개발이 지원됩니다. 이러한 접근 방식으로 벤더 종속 현상을 해소하고, 다양한 보안/IT 툴과의 상호 운용성을 증진할 수 있습니다.







5. 오케스트레이션, 자동화, 대응을 위한 코어 기능이 있습니까?

SOAR(Security Orchestration, Automation and Response) 솔루션을 플랫폼 자체인 것처럼 포지셔닝하는 경우가 종종 있습니다. 그러나 SOAR 기능이 따로 제공되기보다는 메인 보안 플랫폼에 기본 탑재될 때 훨씬 더 효과적일 수 있습니다. 보안 팀이 다양한 워크플로우 및 보안 활용 사례에서 더 효율적으로 일할 수 있도록 SOAR을 코어 기능으로 제공하는 보안 플랫폼을 찾으십시오. 지금까지는 위협 관리의 사고 대응 영역에 주력했던 SOAR이 더 포괄적인 플랫폼에 기본 탑재될 경우, 데이터 보안과 같은 다른 영역에도 효과를 발휘하면서 SOC(Security Operations Center) 팀과 데이터 보안 팀 간 협업을 촉진할 수 있습니다.

6. 위협 인텔리전스 통합을 어떻게 지원합니까?

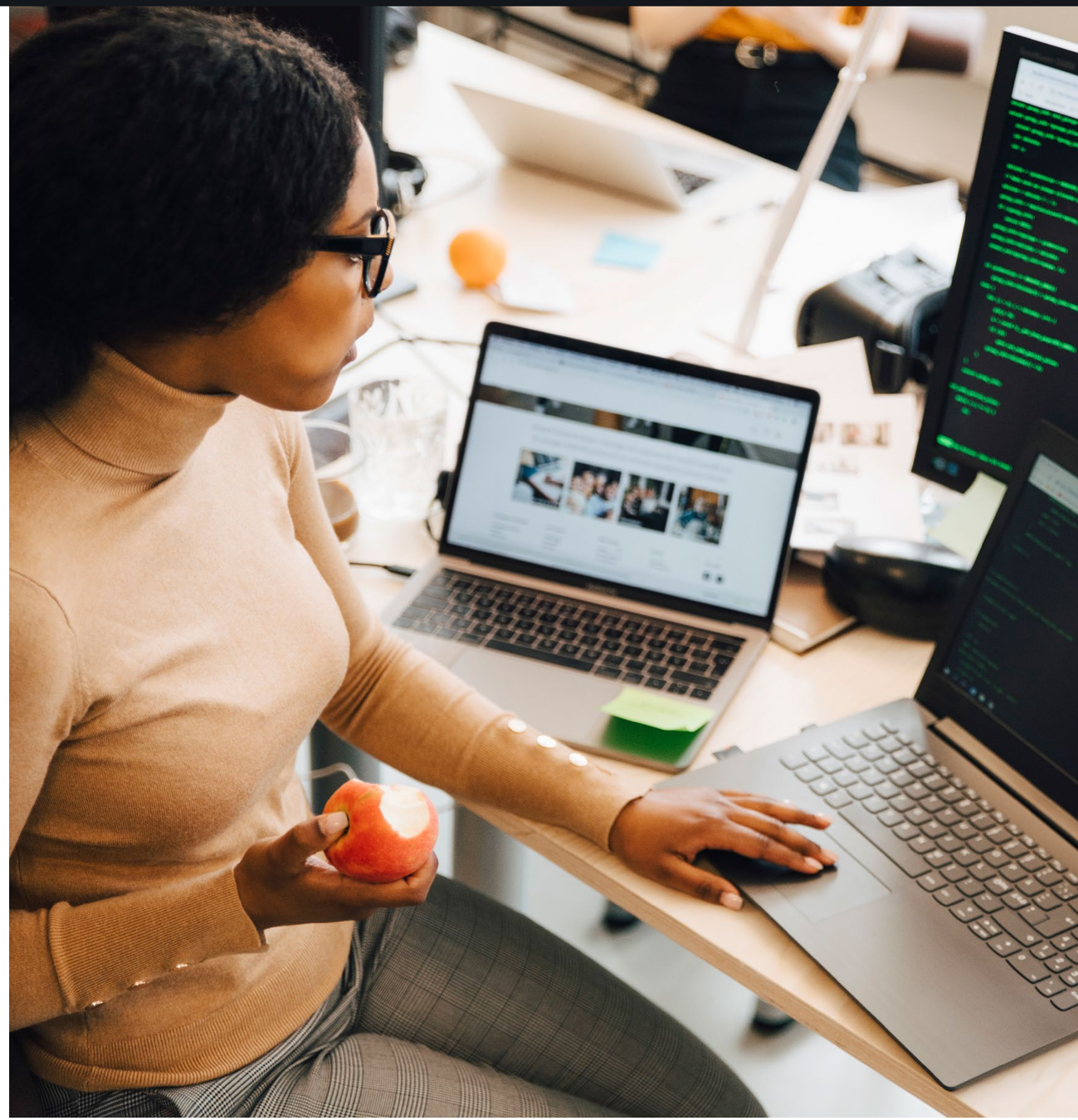
보안 분석가는 대개 다양한 위협 피드와 각종 제품을 사용하여 위협 인텔리전스를 철저히 탐색하고, 이를 조사 및 의사결정의 기반으로 삼곤 합니다. 해당 플랫폼에서 위협 인텔리전스 보고서를 제공하는지 여부를 확인하십시오. 이 인텔리전스가 다른 기능과 어떻게 통합되는지, 그리고 어떤 위협 인텔리전스 벤더를 지원하는지도 중요합니다. 보안 플랫폼에 위협 인텔리전스를 통합할 경우, 보안 분석가의 업무 부담이 줄어들 뿐만 아니라 더 신속하고 현명한 의사결정이 가능해집니다.

7. 이 플랫폼에서 각기 다른 팀끼리 연결할 수 있습니까?

대개 보안 플랫폼은 보안관제 및 보안관제 센터(Security Operations Center, SOC)에 집중합니다. 그러나, SOC 팀은 인시던트 조사 및 대응을 위해 데이터 보안 팀과 같은 다른 팀과 협업해야 할 때가 많습니다. 이러한 팀들이 보안 플랫폼에서 더 수월하게 협업하고 정보를 공유한다면, 보안 위협이나 보안 침해에 더 빠르고 효율적으로 대처할 수 있습니다. 보안 플랫폼을 평가할 때, 기존 SOC 기능에 머무르지 않고 더 거시적 관점에서 귀사의 보안 환경과 팀을 연결해 줄 플랫폼을 찾으십시오.

8. 플랫폼에서 위험 관리 및 대시보드 기능을 제공합니까?

보안 툴의 종류는 수십 가지에 달하므로, 보안 리더에게는 각 툴마다 발생할 수 있는 위험에 대한 이질적이고 주관적인 정의를 정리하는 것은 물론, 문제 해결의 우선순위를 정해야 한다는 것이 상당한 부담으로 작용할 수 있습니다. 회사의 위험 프로파일을 서둘러 효율적으로 최소화하려는 보안 경영진에게는 위험 데이터를 정규화하고, 상황과 연계하여 분석하며, 우선순위에 따른 처리를 지원하고, 전반적인 위험을 완화할 최상의 행동 방안을 결정하도록 도울 솔루션이 필요합니다. 보안 플랫폼에서 기본적인 위험 관리 기능을 제공하면서 보안 환경의 전 범위에서 위험 데이터를 수집하고 상황과 연계할 수 있어야 합니다.



9. 벤더가 소프트웨어와 함께 서비스도 제공합니까?

보안 플랫폼이 강력한 툴임은 분명하지만, 해당 기업 또는 보안 프로그램에 따라 부가적인 서비스가 필요해질 수 있습니다. 초기 단계에서 이루어지는, 보안 전략에 관한 자문이나 컨설팅, 가장 필요한 부분을 지원하는 하이브리드 모델, 종합 매니지드 보안 서비스 등입니다. 이러한 부가 보안 서비스도 제공하는 플랫폼 벤더를 선택하면, 더 용이하게 귀사의 보안 플랫폼에 서비스를 추가하고 통합할 수 있습니다.

보안 플랫폼에 대한 핵심적인 요구사항과 기대 이해

플랫폼 접근 방식은 보안 데이터, 툴, 팀을 효율화할 기회도 제공합니다. 그러나 선택할 수 있는 옵션이 많은 만큼, 어떤 보안 플랫폼이 귀사에 적합한지 판단하려면 다음과 같은 핵심 질문에 답할 수 있어야 합니다.

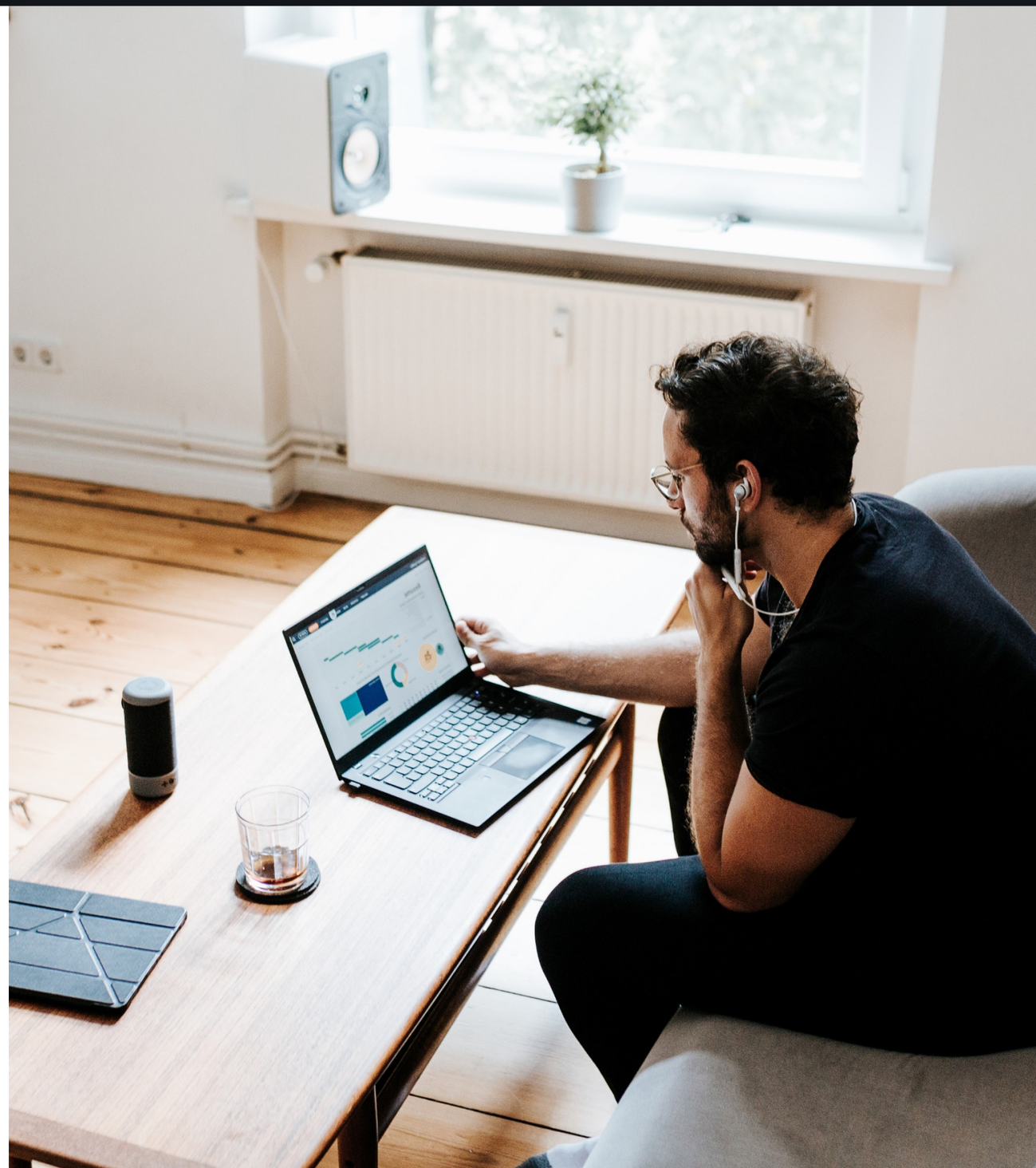
- 데이터를 현재 저장된 곳에 그대로 둘 수 있습니까?
- 구축된 환경에서 하이브리드 멀티클라우드 아키텍처를 지원합니까?
- 향후 다른 보안/IT 툴과의 개방형 통합 및 연결이 필요해질까요?
- 보안 프로그램이 달라지면 손쉽게 적응하고 조정할 수 있습니까?
- SOAR(Security Orchestration, Automation and Response) 기능이 귀사에 유용합니까?
- 어떻게 위협 인텔리전스를 통합합니까?
- 각기 다른 보안 팀을 어떤 방식으로 연결합니까?
- 위험 관리 및 대시보드 기능을 제공합니까?
- 벤더에서 소프트웨어와 함께 보안 서비스도 제공할 수 있습니까?

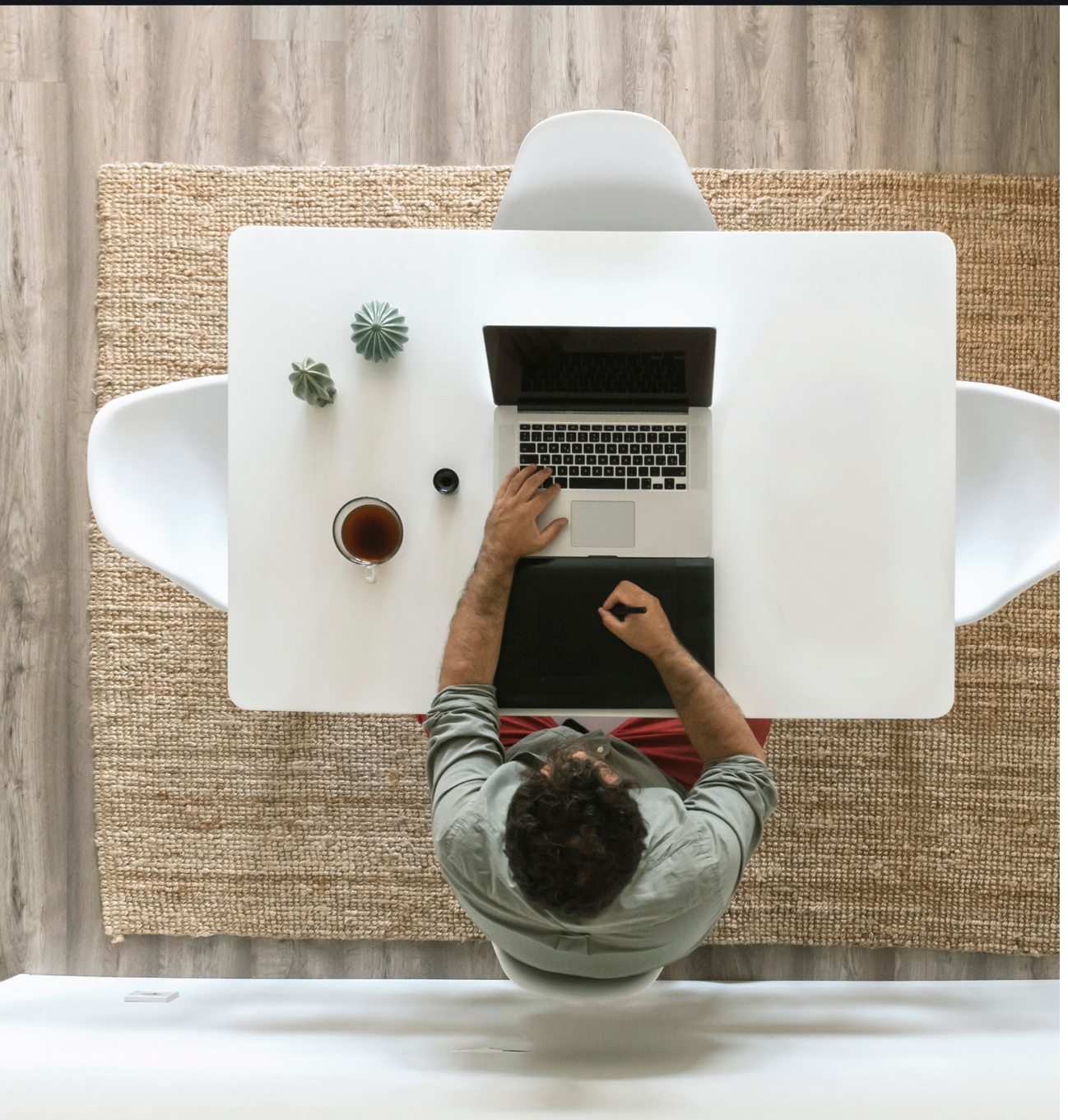
IBM Cloud Pak for Security: 개방형 멀티클라우드 플랫폼을 통한 보안 현대화

IBM Cloud Pak® for Security 개방형 통합 보안 플랫폼에서는 현재와 미래에 다양한 환경에서 발생하는 위험 및 위협을 심층 분석합니다. 데이터를 마이그레이션하지 않고도, 위협에 관한 정보를 찾거나 각종 활동을 조정하거나 대응을 자동화할 수 있습니다. 이 플랫폼은 사례 관리, 오케스트레이션, 자동화 기능으로 SOC 팀과 데이터 보안 팀의 소통과 협업을 지원합니다. 위협 관리 팀과 데이터 보안 팀이 공조하면서 더 강력한 가시성을 확보하고 신속하게 문제를 해결할 수 있습니다.

개방형 표준 및 혁신적인 IBM 기술을 기반으로 하는 IBM Cloud Pak for Security에서는 IBM 툴과 타사 툴을 활용하여 모든 클라우드 또는 온프레미스 로케이션을 대상으로 위협 지표를 탐색합니다. IBM은 OASIS Open Cybersecurity Alliance에 참여하여 IBM Cloud Pak for Security에 쓰인 기술을 오픈소스로 제공하고 수십여 개 회원사와 긴밀하게 공조하면서 상호 운용성을 강화하고 벤더 종속 현상을 줄이는 데 기여하고 있습니다.

IBM Cloud Pak for Security는 컨테이너 기반 소프트웨어이며, Red Hat® OpenShift® 엔터프라이즈 애플리케이션 플랫폼과 사전 통합된 형태로 제공됩니다. 이 통합 덕분에 온프레미스, 프라이빗 클라우드, 퍼블릭 클라우드 어디서나 실행 가능하므로, 고객은 원하는 위치에 구축할 수 있는 진정한 유연성의 이점을 누릴 수 있습니다.





IBM Cloud Pak for Security에 대한 자세한 정보

IBM Cloud Pak for Security 웹 페이지를 방문하세요. 숨어 있는 위협을 찾아내고, 위험 정보에 근거한 현명한 의사결정을 통해 보안 인시던트에 더 빨리 대처할 수 있는 방법을 알아보시기 바랍니다.

귀사의 팀을 효과적으로 지원할 전문가와 기술력이 필요하신가요? IBM Security 서비스와 함께 확실한 전략을 수립하고 보안 프로그램을 혁신하실 수 있습니다.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
2021년 1월