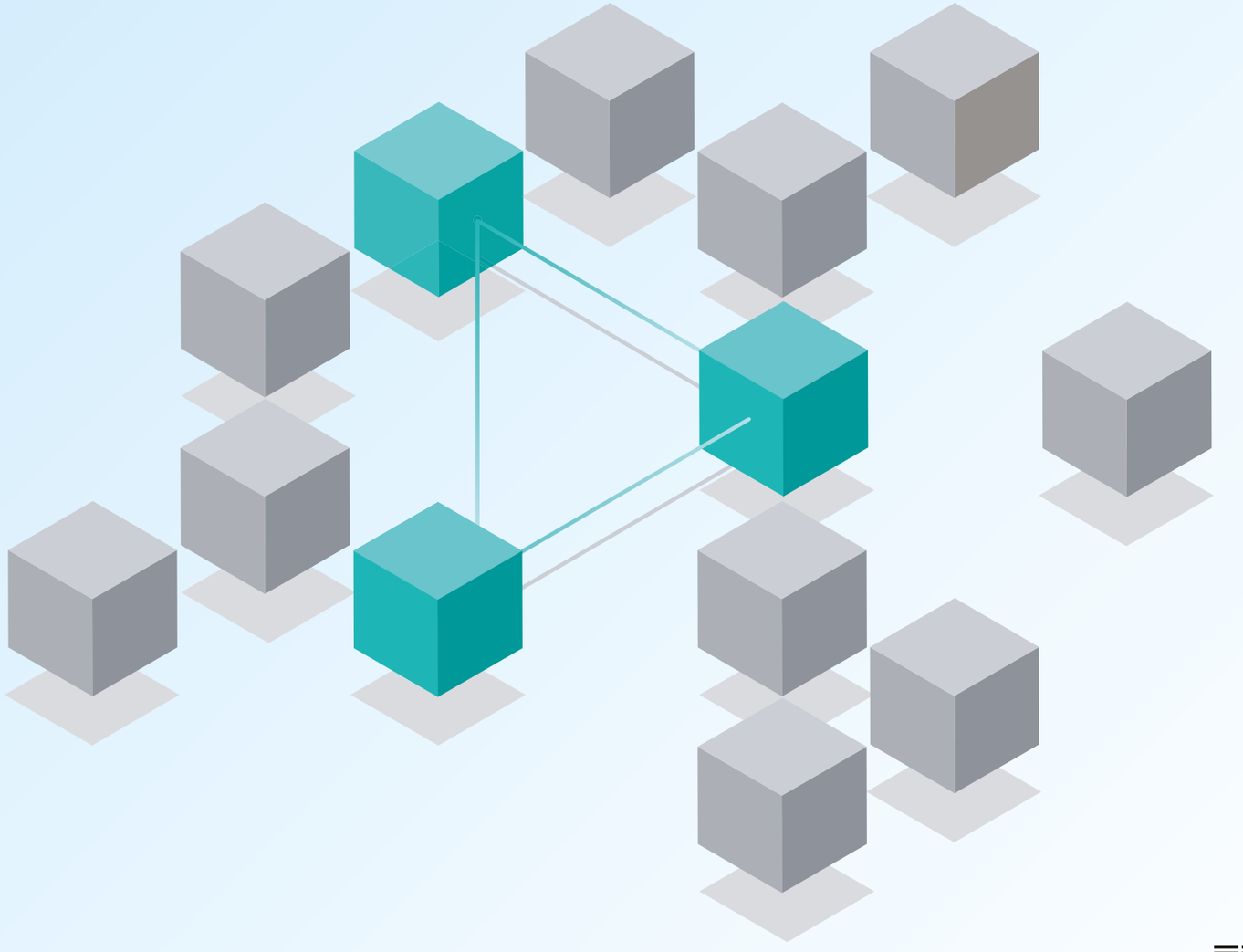
EDR 구매자 가이드

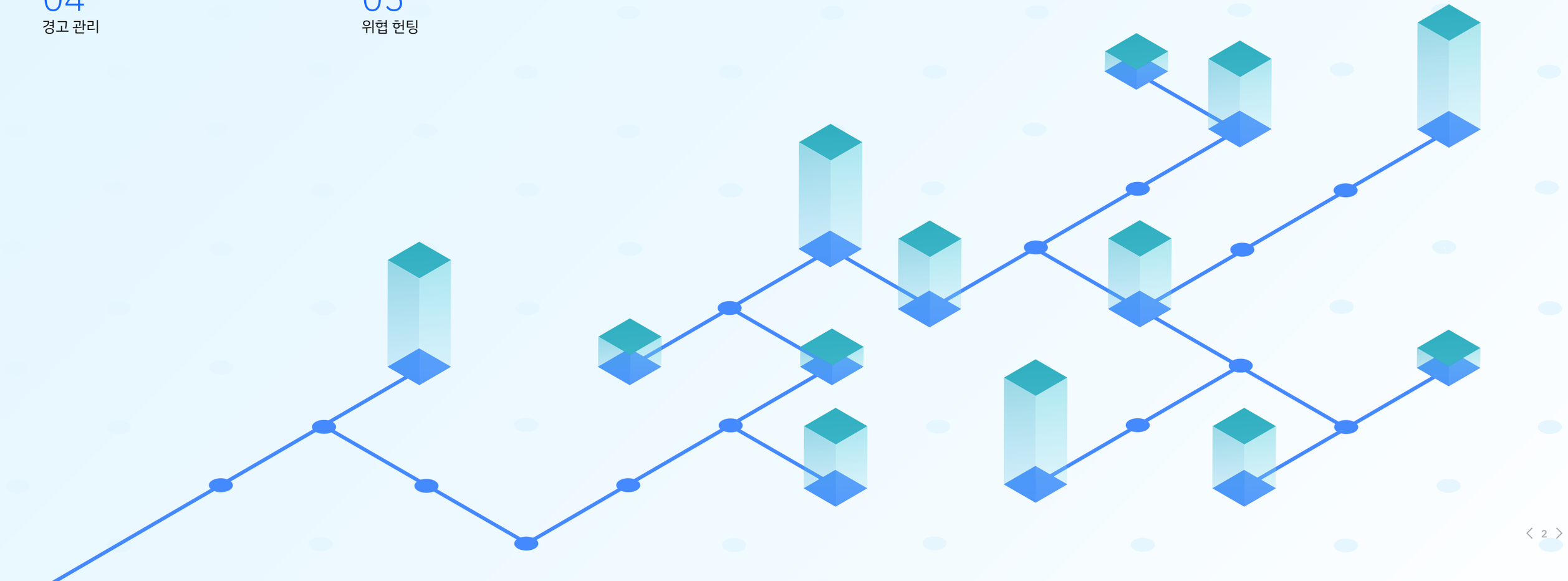
비즈니스에 가장 적합한 엔드포인트 탐지 및 대응 솔루션을 선택하는 방법



REAQTA
an IBM Company

IBM

목차



01
소개

EDR이란 무엇이며 왜 필요할까요?

최근 몇 년 사이 엔드포인트와 데이터가 크게 확산되고 그에 따른 상호 연결성이 증가함과 동시에, 공격자들의 악성 활동 또한 급격하게 늘어나고 있습니다. 이러한 요인들은 크고 작은 모든 조직의 비즈니스 연속성에 심각한 위협을 가합니다. 점점 더 많은 기업이 사이버 범죄에서부터 국가 주도 공격까지 다양한 악성 공격으로 큰 피해를 겪고 있는 것이 현실입니다.

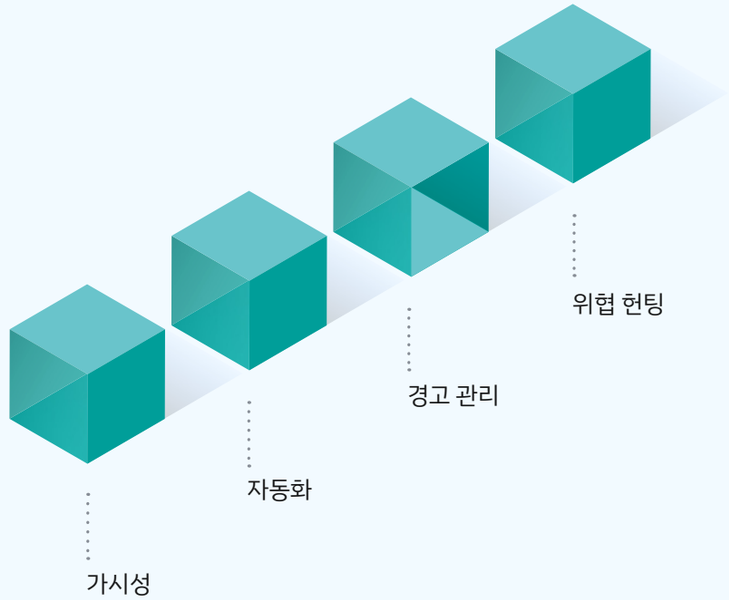
기존의 보안 솔루션은 이미 알려진 위협에 대처하는 방식으로는 작동하지만, 대개 잘 알려지지 않은 고도화된 공격 기술에는 취약하며 시스템 자산에 대한 가시성도 제공하지 않습니다. 이는 해당 시스템 보안 상 주요 장애 요소 중 하나로 꼽힙니다. 엔드포인트 보안 기술 전문가의 도움을 받는 것은 보통 대규모 조직이나 자금이 가장 풍부한 조직에서나 가능한 방법입니다. 많은 공격이 다수의 이동하는 영역에서 빠른 속도로 발생하고 있는 현실 속에서, 담당 인력이 기존의 엔드포인트 보안 솔루션에 의지하는 것만으로는 이러한 위협을 따라잡기 힘든 상황에 이르게 되었습니다.

엔드포인트 탐지 및 대응(EDR) 솔루션은 사전 예방 차원에서 자동으로 악성 소프트웨어를 차단하고 격리함과 동시에, 이러한 문제 상황을 확실히 처리할 수 있는 툴을 보안 팀에 제공합니다. 최신 EDR은 분석 워크로드를 늘리거나 고도로 숙련된 보안 전문가의 도움을 받지 않아도 랜섬웨어 또는 파일리스 공격과 같이 급증하고 있는 자동화된 지능형 위협을 효과적으로 완화하여 비즈니스 연속성을 보장할 수 있습니다.

다음과 같은 문제 상황을 겪고 계시나요?

- 기존 솔루션의 실패
- 제한된 가시성
- 전문 인력 부족
- 경고 피로
- 비활성 위협

다음 장에서는 효과적인 최신 EDR을 구성하는 4가지 핵심 요소에 대해 알아봅니다.



02

엔드포인트 전반의 완전한 가시성

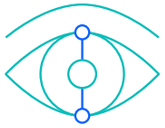
엔드포인트 보안에서 주된 장애 요소 중 하나는 바로 가시성 부족입니다. 따라서 최신 EDR 솔루션은 실행 중인 애플리케이션과 프로세스에 대한 완전하고 심층적인 가시성을 제공해야 합니다.

위협이 발생하면, 공격 단계가 진행됨에 따라 해당 위협 행위에 대한 실시간 경고를 MITRE ATT&CK 매핑과 같은 그래픽 스토리라인과 함께 자동 생성해야 합니다. 이를 통해 분석가는 현재 상황에 대한 완전한 가시성과 이해를 얻게 됩니다.

대다수 엔드포인트 보안 소프트웨어 솔루션은 운영 시스템 내부에서 작동하므로, 엔드포인트 에이전트에 대한 경계가 생성됩니다. 이는 에이전트의 가시성과 기능을 제한하는 동시에 컴퓨터 리소스를 더 많이 소비합니다. 하이퍼바이저 계층에서 작동하며 설계 상 탐지될 수 없는 에이전트를 보유하는 경우 리소스 사용을 최소화할 뿐만 아니라 뛰어난 가시성을 제공하여, 공격자에게 노출되지 않은 상태에서 모든 프로세스 행위를 모니터링할 수 있습니다.

고려 사항

- 완전한 엔드포인트 가시성
- 실시간 경고
- 스토리라인 생성
- 충돌 없는 에이전트
- 통합된 워크플로우



고려해야 할 질문

→ 귀사의 보안 솔루션은 완전하고 깊은 가시성을 현재 실행 중인 애플리케이션 및 프로세스에 제공하나요?

→ 공격 단계가 진행됨에 따라, 귀사의 솔루션은 유의미한 실시간 정보를 제공하여 해당 위협을 파악하는 데 도움을 주나요?

→ 데이터 유출 탐지 및 경고 기능뿐만 아니라, 귀사의 보안 관제 서비스 공급자(MSSP)는 엔드투엔드 대응 및 교정 기능을 제공하나요?

03
자동화 · 편의성

2022년을 기점으로 고도화된 위협과 공격 표면이 증가할 것으로 예상되는 가운데, 대다수 조직은 사이버 범죄에 미리 대처하는 데 큰 어려움을 겪고 있습니다. 최신 EDR은 스마트 자동화를 통해 워크로드가 증가하는 것을 완화함과 동시에, 숙련된 보안 전문가의 도움이 크게 필요하지 않을 만큼의 편의성을 갖추고 있어야 합니다.

구매자 입장에서 EDR의 진가를 가장 빠르게 느낄 수 있는 핵심 요소는 바로 자동화 및 편의성입니다. AI 자동화 기능은 대량 작업을 알고리즘으로 처리하여 인력의 개입을 최소화합니다. 이러한 AI 알고리즘을 통해 소프트웨어를 더욱 간편하게 활용할 수 있으며, 오랜 시간 활성화할 필요 없이 담당 팀에서 신속하게 작동시킬 수 있습니다.

공격이 발생하면, 대응 시간이 가장 중요합니다. 고도의 지능형 위협이 인프라에 피해를 일으키기 전에 이를 제거하려면 반드시 조사 시간을 1분 미만으로 유지해야 합니다.

구매자는 자율 작동이 가능할 뿐만 아니라 자동 탐지 및 대응 기능을 제공하는 EDR을 선택해야 합니다. 이는 공격 진행에 대한 실시간 상황을 분석가에게 전달하고, 유도 교정 기능으로 신속하게 정상 업무로 복귀할 수 있게 합니다.

고려 사항
- 자율 탐지
- 유도 교정
- 에이전트 분석
- 빠른 대응 시간
- 편의성

고려해야 할 질문

→ EDR 운영에 반드시 고급 기술이 필요한가요?

→ 분석 워크로드를 낮추기 위해, EDR은 자율 작동 기능을 제공하나요?

→ 대응 시간을 고려할 때, 위협 분석은 클라우드에서 진행돼야 할까요, 아니면 에이전트에서 진행돼야 할까요?

→ 만일 클라우드에서 위협 분석이 이루어진다면, 인터넷 연결이 안 되는 곳에서는 어떻게 되나요?

04
경고 관리

기존 안티바이러스(AV) 솔루션과 비교할 때 EDR의 핵심 차별점은, AV가 단지 탐지 가능한 특성에 의존한다는 점과 반드시 해당 위협에 대한 지식이 있어야만 이를 차단할 수 있다는 점인데 반해, EDR은 행위적 접근 방식을 활용하여 엔드포인트에서의 행위 방식에 따라 악성 소프트웨어 및 기타 잠재적인 위협을 식별합니다. 또한 AV와 달리 EDR은 본질적으로 가벼운 솔루션으로 업데이트가 자주 필요하지 않습니다.

AI 기술이 적용된 최신 EDR은 높은 정확도와 충실도를 갖춘 신속한 탐지 기능으로 경고량 및 분석 워크로드를 최소 수준으로 유지합니다. 구매자는 해당 EDR에 적용된 AI 및 머신 러닝 기술에 대한 정보도 반드시 살펴봐야 합니다. 사전 학습된 모델 및 분석에 의지하여 탐지하는 AI 엔진과 비교하면, EDR은 초기 학습 모델을 사용하여 각 엔드포인트의 정상 행위를 파악합니다. 따라서 정상 행위 대비 편차 발생 시 더욱 정확한 탐지 및 경고 능력을 발휘할 수 있습니다.

분석가의 경고 피로를 완화하고 대응 시간을 단축하려면, 최신 EDR은 분석가의 상시 경고 처리 관련 의사 결정을 학습하여 이를 자율 적용할 수 있는 강력한 AI 주도형 경고 관리 시스템을 갖추고 있어야 합니다. 완전 자동화된 AI 주도형 경고 관리 시스템을 배포하는 것은 경고 피로를 해소하고 담당 인력의 이탈을 완화하며 시스템 제어 능력을 회복하는 데 가장 핵심적인 역할을 합니다.

고려 사항
- 고충실도 경고
- AI 모델 활용
- 경고 피로 방지
- 자동화된 경고 관리

고려해야 할 질문

→ 귀사의 솔루션은 자동으로 경고를 처리/종료하는 기능을 제공하나요?

→ 귀사의 솔루션은 분석 시간을 단축해 주나요?

→ 귀사의 솔루션은 오탐율을 낮춰주나요?

→ 담당자가 퇴사할 경우, 관련 인프라에 대한 지식을 어떻게 유지할 수 있나요?

05
위협 헌팅

위협 헌팅은 최신 EDR 솔루션에서 매우 중요한 기능이며 위협 없는 청정 시스템 환경을 유지하는 데 필수입니다. 위협 헌팅으로 새로운 위협이 시스템 환경에 진입하였는지 신속하게 확인하고 취약점을 파악할 수 있습니다. 비활성 위협은 데이터 마이닝을 통해 검색하고 제거할 수 있습니다. 이러한 위협은 당장 눈에 띄지는 않지만 수개월 또는 수년 동안 시스템 환경에 잠복하여 공격자에게 이용될 수 있습니다.

인메모리 및 파일리스 위협은 본질적으로 추적이 어려울 뿐만 아니라 대규모 인프라 내에서 이동하기 때문에, 공격자가 각기 다른 변이를 사용하는 경우 추적하기가 훨씬 어려워집니다. 최신 EDR은 헌팅 작업을 자동화하고 기타 인시던트와 유사한 수준의 행위 및 기능을 공유하는 위협을 보안 팀이 자동으로 헌팅할 수 있도록 데이터 마이닝을 활용하며, 해당 결과를 단 몇 초 만에 제공할 수 있어야 합니다.

위협 헌팅에서 유연성은 매우 중요합니다. 구매자는 즉시 배포할 수 있도록 사전 구축된 대규모 탐지 플레이북 라이브러리를 제공할 뿐만 아니라 스크립팅 지식이 없어도 조직의 보안 요구사항을 반영한 특정 시나리오에 따라 손쉽게 사용자 정의 플레이북을 생성할 수 있는 EDR을 선택해야 합니다.

위협 헌팅은 사막에서 바늘을 찾는 것에 비유되곤 합니다. EDR 검색은 특정 헌팅 매개변수를 드릴다운 방식으로 분석하고 해당 매개변수를 포괄적 또는 배타적 방식으로 조합하여, 종합적이면서도 세분화된 결과를 실시간으로 제공해야 합니다. 분석 시간을 절약하고 더욱 실질적인 도움을 제공하려면, 검색 결과를 이해하기 쉬운 그래픽 유저 인터페이스(GUI)로 표시해야 합니다. 이에 따라 분석가는 언제든지 모든 엔드포인트에서 모든 이벤트를 직관적으로 쉽게 검색할 수 있습니다.

고려 사항
- 비활성 위협 검색
- 자동화된 헌팅
- 사용자 정의 플레이북 생성
- 스크립팅 불필요
- 데이터 마이닝
- 실시간 기능
- 그래픽 개요

고려해야 할 질문

→ 사용자는 맞춤형 탐지 전략과 플레이북을 구축할 수 있나요?

→ 위협 헌팅 시나리오를 자동화할 수 있나요?

→ 빠른 선별 목적에 맞게 위협 헌팅에 관한 그래픽 개요를 제공하나요?

→ 플레이북을 생성하는 데 스크립팅 지식이 반드시 필요한가요?

다음 단계

IBM Security ReaQta에 대해 더 자세히 알아보고 데모를 요청하세요.

(07326) 서울특별시 영등포구 국제금융로 10
서울국제금융센터(3IFC)

미국에서 제작
2022년 4월