API 검색에 대한 최종 가이드

목차

API 검색의 중요성

지금 API 보안을 시작하거나 전략을 더 강화하려는 기업이 기본적으로 실행해야 하는 단계는 바로 모든 API를 찾아 인벤토리로 구축하는 것입니다. 그 이유는 무엇일까요? 기업이 구축하는 모든 애플리케이션, 클라우드로 전환하는 모든 워크로드, 직원들이 협업에 사용하는 모든 툴에는 보이지 않는 곳에서 종종 민감한 데이터를 포함해 각종 데이터를 교환하는 API가 있습니다. 여기서 문제는 대부분의 기업, 특히 전체 인벤토리의 가치를 이해하는 기업조차도 이 API의 주요 부분을 실제로 볼 수 없다는 점입니다.

보이지 않으면 보호할 수도 없습니다.

기업이 점점 클라우드 중심적이고 디지털화됨에 따라 API의 범위와 규모, 복잡성도 증가하고 있습니다. API는 온프레미스에서 하이브리드 클라우드에 이르기까지 여러 환경에 분산되어 있는 경우가 많습니다. 여기에 API 생태계가 자체 네트워크와 클라우드를 훨씬 넘어 확장되어 있을 가능성이 높다는 점이 이를 더 복잡하게 만듭니다. API가 써드파티 및 개발자 생태계의 앱, 서비스, 시스템과 수없이 연결되어 있는 것을 생각해 보세요.

API의 범위와 규모, 복잡성이 증가함에 따라 다음에 대한 실시간 인사이트를 얻기 어렵습니다.

- 여러 사업부에서의 API 위치(대부분의 경우 사업부에 자체 개발자팀이 있음)
- API 설정 방법, API의 라우팅 위치, 적절한 인증 및 권한 제어가 존재하는지 여부
- API가 호출될 때 민감한 데이터를 반환하는지 여부와 해당 데이터에 접속할 수 있는 사람

특히 기업에 축적되는 API의 상당 부분이 관리되지 않고, 눈에 보이지 않으며, 보호되지 않는 경우가 많기 때문에 더욱 어렵습니다. 여기에는 API 게이트웨이 및 웹 애플리케이션 방화벽(WAF)과 같이 일반적으로 널리 사용되는 툴의 방어 체계에서 놓치고 있는 휴면, 섀도, 좀비 API가 포함됩니다. 물론 이러한 툴은 여러 이점과 기본적인 보호 기능을 제공하지만, 오늘날 API 위협 환경에는 보다 높은 수준의 가시성과 실시간 보안 그리고 전문적인 API 보안 솔루션이 제공할 수 있는 지속적인 테스트가 필요합니다.

모든 API를 검색할 수 있다면 각 API의 리스크 평가, 기업의 API 보안 체계 파악, 공격을 방지하는 실시간 보안 기능을 적용하기 위해 확보한 인사이트 사용 등 중요한 다음 단계를 위한 토대를 마련할 수 있습니다. 이 백서에서는 다음의 정보를 공유합니다.

- 보안팀이 특정 유형의 API를 파악하기 어려운 이유에 대한 인사이트
- 가시성을 확보하고 공격을 방지할 수 있는 API 검색 기능에 대한 세부 정보

API를 찾기 어려운 이유

운영팀이나 보안팀의 누구도 알지 못하는 관리되지 않는 API가 프로덕션에 존재하는 경우가 종종 있으며, 이로 인해 기업은 다양한 사이버 보안 리스크와 운영상의 어려움에 노출될 수 있습니다. 노출되었거나 잘못 설정된 API는 보안이 취약하고 광범위하게 존재하며 공격자가 쉽게 악용할 수 있습니다. 리스크 또한 높습니다. API에 대한 공격은 기업의 매출, 안정성 및 규제 컴플라이언스에 심각한 영향을 미칠 수 있습니다.

다음과 같은 네 가지 방식으로 악성 API가 발생할 수 있습니다.

1. API 바로 가기 및 프로세스 실패

적절한 사람에게 알리지 않았을 때 악성 API가 발생하기도 합니다. 예를 들어, LOB(Line of Business)팀은 IT팀에 알리지 않고 특정 요구사항에 대응하는 API를 생성할 수 있고, 개발자는 절차보다 실행에 더 관심을 가질 수도 있습니다. 합병으로 인해 '물려받은' API들도 자주 간과됩니다. 이러한 종류의 악성 API는 종종 섀도 API라고 합니다.

2. 이전 버전의 API

보안이 약하거나 알려진 취약점이 있는 이전 버전의 API가 제거되지 않고 남아 있는 경우가 많습니다. 소프트웨어가 업데이트되는 동안 이전 버전이 일정 기간 새 버전과 공존해야 할 수 있습니다. 하지만 실질적으로 API를 비활성화할 책임이 있는 담당자가 퇴사하거나, 인사이동이 있거나, 단순히 이전 버전을 중단하는 것을 잊어버리면 어떻게 될까요? API는 공식적으로 폐기되었지만 운영상의 실수로 계속 가동될 수 있습니다. 이러한 상황에서는 좀비 API가 발생합니다.

3. 상속된 API

합병 또는 인수로 인해 '상속'된 API 또한 자주 간과되어 섀도 API가 됩니다. 인벤토리가 있는 경우에는 까다롭고 복잡한 시스템 통합 과정에서 종종 유실됩니다. 소규모 기업은 API 자산이 방대하고 문서화되지 않는 경우가 많기 때문에 이러한 소규모 기업을 많이 인수하는 대기업은 특히 리스크에 직면하게 됩니다.

4. 상용 API

일부 상용 소프트웨어 패키지에는 다른 애플리케이션 및 외부 데이터 소스와 연결할 수 있는 API가 포함되어 있습니다. 이러한 API는 아무도 눈치채지 못하게 활성화될 수 있습니다.

API 검색이란?

API 검색은 기업이 API를 식별, 분류, 관리하고 리스크를 측정하는 데 도움이 되는 프로세스 및 기능입니다. API 검색을 올바르게 수행하면 기업은 다음과 같은 이점을 얻습니다.

- API 스프롤(적절한 문서화나 감독 없이 급격히 증가하는 API 누적) 감소 및 보안 체계 개선
- 기업의 현재 API 환경 이해 및 향후 개발에 대해 정보에 입각한 의사 결정 지원
- 권한이 부여된 사용자만 접속할 수 있도록 이러한 API에 대한 접속의 모니터링 및 관리

가시성을 높이고 리스크를 줄이는 주요 API 검색 기능

아무도 모르는 API가 생각보다 많습니다. 그러나 정확한 인벤토리가 없으면 기업은 다양한 리스크에 노출될 수 있습니다. API를 효과적으로 인벤토리화하려면 다음이 가능해야 합니다.

위치 파악

설정이나 종류에 관계없이 API를 찾아 인벤토리로 구축

탐지

휴면 및 좀비 API와 같은 관리되지 않는 API 탐지

식별

잊혀졌거나, 방치됐거나, 알려지지 않은 섀도 도메인 식별

제거

사각지대를 제거하고 잠재적인 공격 경로 발견

API 검색을 위한 새로운 솔루션을 평가할 때 다음 기능을 염두에 두어야 하며, 검색 툴은 이 모든 기능을 포함해야 합니다.

모든 API 유형에 대한 검색

API 검색 툴은 모든 설정이나 종류의 API에서 RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, gRPC 등 보유하고 있는 API를 식별할 수 있어야 합니다.

세분화된 API 인벤토리

API 검색 툴은 또한 인벤토리가 오래되지 않도록 자동으로 업데이트되는 인벤토리를 생성해야 하며, 모든 속성을 기반으로 API를 검색, 태그 지정, 필터링, 할당 및 내보낼 수 있는 기능을 제공해야 합니다.

교묘한 API 탐지

관리되지 않는 API는 기업의 API 보안 이니셔티브보다 앞서 있을 수 있습니다. 즉, API 스프롤의 오리진은 더 이상 기업에 존재하지 않는 개발자팀에서 시작되었을 수 있습니다. 이러한 API들은 일반적으로 소유권이 없으며 보이지 않거나 보안 제어가 없는 상태에서 작동합니다. 검색 툴은 이러한 API를 찾아낼 수 있어야 합니다.

섀도 API 도메인 검색

섀도 API 외에도 사용자가 전혀 모르는 API 도메인 이름, 즉 전체 섀도 도메인이 있을 수 있습니다. API 검색 툴은 보안 리스크를 초래할 수 있는 잊혀졌거나, 방치되거나, 알려지지 않은 섀도 도메인을 식별해야 합니다.

API 자동 스캐닝

스캐닝은 사각지대를 제거하고 다음과 같은 중요한 문제를 식별하는 데 필수적입니다.

- 유출된 API 키 및 인증정보
- API 코드 및 스키마 노출
- 인프라 설정 오류
- 문서, GitHub 리포지토리, Postman Workspaces 등의 취약점

이러한 문제점 및 기타 악용 가능한 인텔리전스 소스를 파악하면 사이버 범죄자들이 악용할 수 있는 잠재적인 공격 경로를 이해하는 데 도움이 될 수 있습니다.

필요한 통합 없음

API 검색 툴은 특별한 통합이나 소프트웨어 설치 없이 API 자산을 완전히 검색하고, 취약한 API 및 섀도 도메인을 찾을 수 있어야 합니다. 단순히 올바른 에이전트를 설치하지 않았거나 툴을 잘못 설정했기 때문에 발생하는 가시성 격차를 방지하는 것이 중요합니다.

제한된 맞춤형 개발

마지막으로, API 검색 툴은 트래픽 소스에 대한 맞춤형 개발을 할 필요가 없는 방식으로 설계되어야 합니다. 이러한 툴은 주요 인프라 구성요소를 위해 사전 구축된 통합 작업과 함께 제공되어야 합니다. 맞춤형 개발은 일반적으로 시간이 오래 걸리며, 소스 오리진이 변경되면 통합 작업을 다시 해야 할 가능성이 높기 때문에 이미 과부화된 IT 보안팀이 확장하기란 불가능합니다.

Akamai Security가 모든 API 검색을 지원하는 방법

포괄적이면서 지속적인 API 검색 기능을 통해 기업은 비즈니스에서 다음과 같은 이점을 얻을 수 있습니다.

- 전체 API 공격표면 파악
- API 인벤토리 및 문서 업데이트 비용 절감
- 규제 요건 및 내부 정책 컴플라이언스 개선

오늘날의 위협은 API 검색, 체계 관리, 위협 탐지 및 해결, 보안 테스트라는 4개의 주요 영역을 포괄하는 완전한 API 보안 솔루션을 필요로 합니다. Akamai API Security는 개발부터 프로덕션까지 전체 수명 주기 동안 API를 보호하는 4가지 필수 모듈을 모두 제공합니다. 파트너, 공급업체, 사용자에게 API를 노출하는 기업을 위해 구축된 Akamai의 API Security 솔루션은 API를 검색하고, 리스크 체계를 파악하며, 행동을 분석하며, 내부에 숨어 있는 위협을 차단합니다.

API 공격 방법, 일반적인 API 취약점 및 기업을 보호하는 방법에 대해 자세히 알아보세요.

맞춤 Akamai API Security 데모 일정을 예약하고 어떤 도움을 받을 수 있는지 알아보세요.

Akamai Security 소개

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 **akamai.com** 및 **akamai.com/blog**를 확인하거나 **X**(기존의 Twitter), **LinkedIn**에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 10월 발행.