AKAMAI 데이터시트

API Security ShadowHunt

API Security ShadowHunt는 API 위협 탐지 분야에서 전문성을 갖고 있는 Akamia의 분석가와 함께 보안팀의 역량을 확장할 수 있는 매니지드 위협 탐색 서비스입니다. API Security ShadowHunt는 인력이 부족하거나 API 보안 전문 지식이 부족한 팀에 적합하며 리스크를 줄이는 데 도움이 되는 아웃소싱 솔루션입니다. 위협 탐지 전문가는 팀의 일원으로 API 트래픽에 숨어 있는 가장 은밀하고 난독화된 공격을 탐지하고 보고합니다.

API Security ShadowHunt의 작동 방식

ShadowHunt 작업은 API Security 플랫폼의 API 활동 데이터를 갖고 시작됩니다. 이 자동화된 애널리틱스는 행동 편차와 취약점 악용을 탐지하고, 머신 러닝 신호는 조사를 위해 ShadowHunt 분석가에게 전달됩니다. 여기서 인간의 전문성이 발휘되기 시작합니다.

분석가는 고객 API 자산에 익숙하기 때문에 활성 위협을 신속하게 탐지하고 ShadowHunt 알림을 생성해 전송합니다. 조사 결과에 모호한 부분이 있는 경우, 분석가는 ShadowHunt 구독자에게 연락해 확인합니다. 분석가와 API Security 연구 팀은 위협 인텔리전스 정보를 활용해 모든 서비스 고객에게 주기적으로 새로운 위협 보고서를 제공합니다.

API Security에 인간의 전문성 추가

API Security 플랫폼은 다음과 같은 포괄적인 API Security 기능을 제공합니다.

- **API 검색:** 광범위하고 지속적인 API 검색.
- **리스크 포스처:** API 리스크 이해.
- **행동 애널리틱스를 사용한 위협 탐지:** 빅 데이터, 클라우드 기반 애널리틱스 엔진이 시간 경과에 따른 모든 API 활동을 검사해 API 악용을 지속적으로 탐지합니다.
- **예방 및 대응:** 맞춤형 조건부 대응 플레이북으로 보안 및 API DevSecOps 프로세스를 강화합니다.
- **조사 및 위협 탐지:** 강력한 조사 기능을 통해 API 트래픽에 숨어 있는 위협을 찾아낼 수 있습니다.

위협 탐지는 API Security 플랫폼의 최신 기능 중 하나입니다. API Security ShadowHunt 서비스는 위협을 탐지하는 툴, 전문 지식 또는 시간이 부족한 고객을 위한 서비스입니다.

기업이 누릴 수 있는 혜택

- 전문가가 API 활동을 검토하므로 안심할 수 있습니다.
- API 데이터에 숨어 있는 더 많은 보안 위협을 탐지합니다.
- Akamai가 API 보안에 주력하기 때문에 내부 보안 인력의 업무 시간을 절감할 수 있습니다.
- 소프트웨어 개발 및 IT 운영에 필요한 유용한 인사이트를 확보합니다.
- 추가 조사를 통해 API 행동에 대한 가시성을 개선합니다.

API Security ShadowHunt 서비스는 다음을 제공합니다.

알림: *API 자산에 대한 위협을 알립니다.* API Security ShadowHunt 서비스의 가장 중요한 요소는 활성 인시던트가 확인되는 즉시 전송되는 알림입니다. 알림 내용:

- 인시던트 발견 사항 및 분석
- 인시던트와 관련된 위협 인텔리전스 요약
- 개선 권장 사항

위협 보고서: *조기에 API 보안 인텔리전스를 확보합니다.* API Security ShadowHunt 새로운 위협 보고서는 글로벌 위협 인텔리전스에 대한 접속, API Security 리서치팀의 의견, 지속적인 위협 탐지 활동을 기반으로 합니다. 새로운 위협 보고서에는 다음이 포함됩니다.

- 팀에서 파악한 새로운 API 취약점, 위협 또는 공격에 대한 세부 정보
- API 자산에 미치는 영향
- 필요에 따라 개선 권장 사항

월간 검토: *API 자산에 대한 완벽한 가시성.* ShadowHunt 월간 위협 보고서는 매월 첫째 주에 모든 API Security 고객에게 제공됩니다. 내용은 다음과 같습니다.

- 지난달에 전송된 ShadowHunt 알림 및 새로운 위협 보고서 요약
- API 자산 개요
- 지난 2개월 동안의 API 활동 비교
- API 업계의 보안 헤드라인

전문가에게 문의: 서비스 가입자는 알림 및 새로운 위협 보고서에 대해 API Security ShadowHunt 팀에 연락해 질문하고 논의할 수 있습니다.

API Security를 선택해야 하는 이유

API Security는 취약점과 API 악용으로부터 API를 보호하는 문제에 XDR(Extended Detection and Response) 원칙을 적용합니다. API 활동을 클라우드 기반 빅 데이터 환경으로 통합한 후에 복잡한 데이터 보강 및 정리를 진행하는 솔루션은 API Security가 유일합니다. 이 고유한 아키텍처는 지속적인 API 검색, 리스크 점수 매기기, 컨텍스트 인식 행동 애널리틱스를 통해 API 악용과 위협을 탐지하고 위협 탐지를 지원합니다. API Security 아키텍처에는 데이터 레이크로 향하는 모든 API 활동을 토큰화할 수 있는 개인정보 보호 설계가 포함되어 있습니다.

API를 보호하는 위협 탐지 전문 기술

API 배포의 증가는 기업의 IT 보안 부서에 부담을 줄 수 있습니다. 지금 API Security ShadowHunt 서비스로 보안 인력을 확장하세요.

전문가에게 문의하고 자세히 알아보세요.