CrowdStrike 솔루션

CROWDSTRIKE

워크로드 및 컨테이너 흔적 검색

퍼블릭 및 하이브리드 클라우드 흔적의 범위와 특성에 대한 가시성 제공

멀티 클라우드 워크로드 및 컨테이너 검색

CrowdStrike® 플랫폼에 필수적인 Falcon Discover™ for Cloud and Containers 를 사용하면 Amazon Web Services(AWS), Google Cloud Platform(GCP), Microsoft Azure 에서 실행되는 워크로드를 비롯하여 프라이빗/퍼블릭/하이브리드 클라우드에서 실행되는 컨테이너에 대한 가시성을 확보할 수 있습니다.

워크로드 검색

Falcon Discover for Cloud and Containers 는 기존의 AWS Elastic Compute Cloud(EC2) 인스턴스, GCP Compute Engine 인스턴스, Azure 가상 시스템을 열거합니다. 또한 통합 클라우드 워크로드 대시보드를 통해 멀티 클라우드 환경 전체에 대한 통합 정보를 표시합니다.

AWS, **GCP**, **Azure** 용 특정 대시보드를 통해 3 가지 퍼블릭 클라우드 각각에 대해 구성, 네트워킹, 보안 정보 관련 메타데이터 정보(Falcon 에이전트 적용 범위 포함)를 제공합니다. 이를 통해 CrowdStrike Falcon® 플랫폼으로 보호되지 않는 워크로드를 손쉽게 파악할 수 있습니다.

대시보드 구성요소를 추가하여 개별 워크로드에 대한 상세 보고를 표시할 수도 있습니다. 인스턴스 ID 를 클릭하기만 하면 단일 워크로드로 전환하여 태그, 네트워크 인터페이스, 저장 장치 등의 종합적 관련 정보를 확인할 수 있습니다.

대시보드에서 상세 디스플레이 및 필터로 신속하게 전환하는 드릴다운 기능을 통해 한눈에 확인 가능

주요 이점

클라우드 전체에서 클라우드 워크로드 및 컨테이너 흔적을 자동으로 검색

프라이빗/퍼블릭/하이브리드 클라우드 전체에 대한 통합 가시성

Falcon 플랫폼을 통해 보호되지 않는 워크로드 파악

공격 노출면 감소

잠재적 위험성이 있는 구성으로 실행되는 컨테이너 파악

CrowdStrike 솔루션

워크로드 및 컨테이너 흔적 검색 솔루션

컨테이너 검색

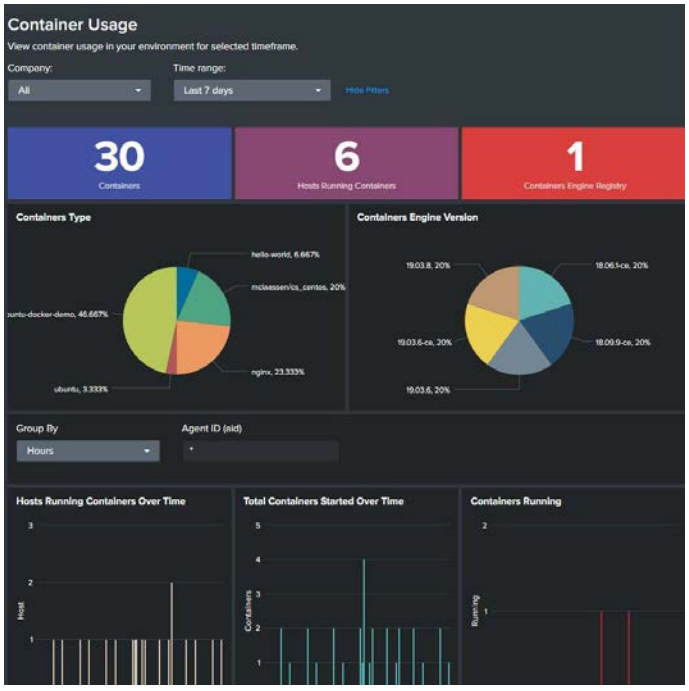
Falcon 플랫폼에서는 사용자 환경 내 컨테이너 사용에 대해 즉각적으로 확인할 수 있습니다. 즉, 세부 정보, 필터, 검색으로 빠르게 전환하는 드릴다운 기능을 통해 컨테이너 구축에 대한 분석 정보를 제공합니다.

컨테이너 사용: 컨테이너가 실행되는 호스트 수, 레지스트리 수, 컨테이너 유형, 엔진 버전 등, 사용자의 환경에서 사용되는 모든 컨테이너에 대한 가시성이 제공됩니다. 추세 그래프를 통해 실행되는 컨테이너 수, 컨테이너 가동 시간의 급증과 같은 이상 징후를 빠르게 파악할 수 있습니다.

호스트별 컨테이너: 호스트 속성을 검색하여 해당 호스트에서 실행되는 컨테이너 전체를 확인할 수 있습니다.

컨테이너 이미지: 사용된 이미지를 확인하고 취약한 이미지를 간편하게 검색할 수 있습니다.

컨테이너 구성: 침해를 표시할 수 있는 링크나 마운트 지점이 거의 없는 경우와 같이, 위험성이 존재하며 잘못 구성된 컨테이너를 신속하게 파악합니다. 탐지 건수가 가장 많은 호스트와 컨테이너를 확인할 수 있습니다. 권한 있는 컨테이너와 대화식 모드로 실행 중인 컨테이너를 비롯하여 루트 액세스를 통해 중단할 수 없거나 루트 액세스를 통해 실행되고 있는 컨테이너도 간편하게 모니터링할 수 있습니다.



대시보드에서 온프레미스 및 클라우드 구축을 포함하는 컨테이너 흔적을 간편하게 확인

지원되는 컨테이너

Falcon 은 Docker 와 같은 OCI(Open Container Initiative) 준수 컨테이너, 자체 관리형 Kubernetes 와 같은 오케스트레이션 플랫폼을 비롯하여 GKE(Google Kubernetes Engine), EKS(Amazon Elastic Kubernetes Service), ECS(Amazon Elastic Container Service), AKS(Azure Kubernetes Service), OpenShift 와 같은 호스팅된 오케스트레이션 플랫폼을 지원합니다.

CROWDSTRIKE 소개

세계적으로 손꼽히는 사이버 보안 업체 CrowdStrike® Inc.(Nasdaq: CRWD)는 처음부터 철저히 보안 침해를 차단하기 위해 설계된 엔드포인트 보안 플랫폼을 기반으로 클라우드 시대에 걸맞도록 보안의 개념을 새롭게 정립합니다. CrowdStrike Falcon® 플랫폼의 단일 경량 에이전트 아키텍처는 클라우드 스케일 AI(인공지능)을 활용하며 엔터프라이즈 환경 전반에서 실시간 보호 및 가시성을 제공하여 네트워크 연결 여부와 관계없이 모든 엔드포인트에서 공격을 방지합니다. 독자적인 CrowdStrike Threat Graph®를 기반으로 CrowdStrike Falcon 은 전 세계적으로 매주 3 조 건 이상 발생하는 엔드포인트 관련 이벤트에 대해 실시간으로 상관관계를 파악하여 세계 최고 수준의 보안 관련 데이터 플랫폼에 공급하고 있습니다.

차세대 AV

무료 체험 시작하기

자세히 알아보기: **www.crowdstrike.com**