IGLOO

SPiDER TM on Cloud

클라우드 환경에 최적화된 보안 정보 및 이벤트 관리(SIEM) 솔루션

Background

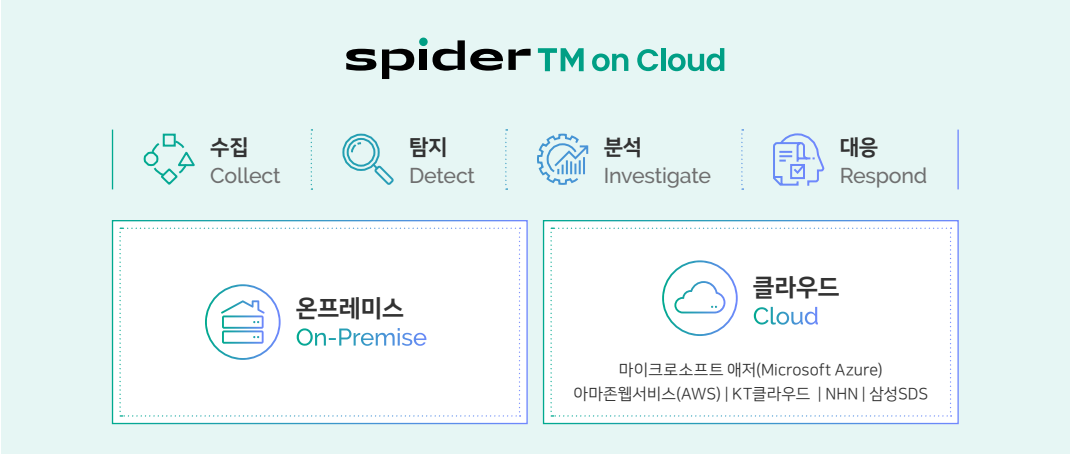
온프레미스, 멀티·하이브리드 클라우드 환경을 아우르는 보안 가시성 확보 필요

전 세계적으로 많은 조직의 IT 인프라가 클라우드 중심으로 빠르게 전환되면서, 클라우드는 디지털 전환을 성공적으로 안착시키기 위한 필수 조건이자 비즈니스 혁신을 주도하는 핵심 인프라로 떠올랐습니다. 그동안 온프레미스 환경에서 사용되던 보안 솔루션과 정책은 클라우드 환경을 보호하는 데 한계가 있습니다. 클라우드 보안의 핵심 기능을 갖춘, 클라우드 환경에 최적화된 보안 솔루션이 필요한 시점입니다.

Overview

SPiDER TM on Cloud는 클라우드 환경에 최적화된 보안 정보 및 이벤트 관리(SIEM) 솔루션입니다.

업계 선도의 검색 기능과 상관 분석 기술, 빅데이터 활용 역량을 토대로, 온프레미스 환경과 단일 및 멀티 클라우드 환경의 각종 위협 요소를 보다 쉽고 빠르게 탐지, 분석, 대응함으로써, 조직의 보안성을 높은 수준으로 유지할 수 있습니다. 사용자는 SPiDER TM on Cloud를 통해 솔루션 도입 및 관리의 부담을 해소하면서 온프레미스와 클라우드를 아우르는 폭넓은 가시성을 확보할 수 있게 됩니다.



Why SPiDER TM on Cloud

01 클라우드 최적화

클라우드 환경에 최적화된 형태로 설계되어 수분 안에 배포가 가능하며, 서비스 장애에 대비한 가용성을 보장합니다. 또한 클라우드에서 발생되는 보안 서비스 로그 및 이벤트의 연동을 지원하고, 구축형 뿐만 아니라 SaaS형 등 구독 모델에 기반해 별도의 설치 과정 없이 손쉽게 사용하고 관리할 수 있는 유연한 운영이 가능합니다.

02 완벽한 가시성

에이전트(Agent), 시스로그 (Syslog), 클라우드 연계 API 등 다양한 방식으로 클라우드 보안 서비스에서 생성된 보안 이벤트 및 로그를 실시간으로 수집·저장·연계 분석할 수 있습니다. 조직에서 일어나는 모든 IT 활동에 대한 최초 탐지부터 분석, 대응까지 일원화된 보안관제 환경을 제공합니다.

03 고도화된 위협 탐지

최신 보안 위협과 공격 기법에 대한 핵심 정보를 제공하는 IGLOO CTI(Cyber Threat Intelligence)와의 연계를 통해 오탐을 최소화하고, 발생 가능한 위협을 선제적으로 탐지하면서 사전 대응 체계를 구축합니다.

04 차별화된 보안 전문성

20년 이상의 보안 경험과 노하우, 역량을 토대로 보안 업무에 최적화된 프로세스 및 기능을 제공합니다. 검증된 룰 및 침해 사고 처리 프로세스 적용으로 안전하고 효율적인 클라우드 환경 운영을 지원합니다.

Features

01 빅데이터 로그 처리 지원

· 모든 종류의 로그와 보안 이벤트를 수집 및 분석

02 실시간 분석 및 시나리오 기반 상관분석 지원

· 인메모리(In-Memory) 기반의 분석 엔진 탑재를 통한 실시간 분석 수행
· 경보 이벤트에 대한 시나리오 기반 상관분석 수행

03 고도화된 보안위협 대응체계 지원

· 실시간 모니터링 및 다양한 분석 기능 제공

실시간 모니터링 > 경보 상세 분석 > 페이로드(Payload) 분석 > 시간대(Time Line) 분석 > 통계 분석 > 로그 추적 분석

· 다년간의 보안관제 노하우가 적용된 체계화된 침해사고 프로세스 제공

침해사고 접수 > 침해사고 이관 > 침해사고 대응 > 침해사고 종결 및 이력 관리

04 자동화된 침해대응 및 차단 기능 지원

· 관제 인력 숙련도와 상관없는 표준화된 대응 및 효율적인 보안관제 운영 지원

05 직관적인 시각화 기술이 적용된 통합 대시보드 지원

· 사용자 정의 대시보드 지원
· 시각화를 위한 다양한 컴포넌트 지원 (3D 세계지도, 3D 지구본 등)
· 여러 시스템과의 유연한 연동 지원
  - 서로 다른 제품 간 데이터셋, 위젯 등을 조합하여 대시보드 생성 가능
  - 다양한 데이터 소스 연동을 통한 새로운 데이터 표현 가능

Benefits

SPiDER TM on Cloud는 클라우드 환경에 최적화된 형태로 설계되어 복잡해지는 IT 및 보안 환경에 대한 완벽한 가시성을 제공합니다. 조직은 솔루션 도입 및 관리의 부담을 최소화하면서 비즈니스 환경 전반에 걸친 체계화된 보안관제 환경을 마련하고, 효율적이고 안정적인 IT 인프라 운영을 위한 기반을 확보할 수 있습니다.

- 온프레미스 및 클라우드를 아우르는 가시성 확보
- 비즈니스 환경 전반에 걸친 통합된 보안 인사이트 확보
- 신속한 위협 탐지 및 체계화된 대응으로 보안관리 체계 고도화
- 관리 업무 간소화에 따른 운영 효율성 극대화

» **안정적인 클라우드 환경 운영** » **성공적인 디지털 전환 실현**

1999년 보안 벤처 기업으로 시작한 이글루코퍼레이션은 국내 최초 보안 정보 및 이벤트 관리(SIEM) 솔루션을 시작으로 수많은 정보보호 핵심 중추 기관과 기업에 보안 솔루션 및 서비스를 제공하며 정보보안 시장의 성장을 이끌어왔습니다. 또한, 디지털 전환 시대 흐름에 맞는 꾸준한 기술 고도화 및 미래 기술 준비를 통해 사업 영역을 확장해 나가며 보안을 넘어 인공지능, 클라우드, 빅데이터 분야를 아우르는 종합 IT 기업으로 성장했습니다. 이글루코퍼레이션은 세계의 고객에게 고유의 보안과 데이터 역량에 기반한 최적의 솔루션, 서비스를 제공하며 급변하는 비즈니스 환경에 최적화된 혁신적인 디지털 경험을 선사하는 기업으로 나아가고자 합니다.

서울특별시 송파구 정의로8길 7 한스빌딩 6층 | TEL 02-3452-8814 | FAX 02-3452-8815 | www.igloo.co.kr

IGLOO