



레거시·가상화·클라우드·컨테이너 환경까지 아우르는

AI 통합 관제 솔루션 Polestar 10

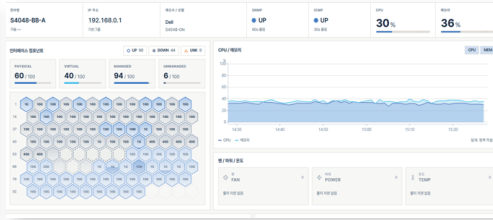
서비스 모니터링 (SMS)

등록부터 실시간 자원, 프로세스, 하드웨어, 컨테이너까지 서버의 모든 계층을 하나의 운영 흐름으로 관리합니다.



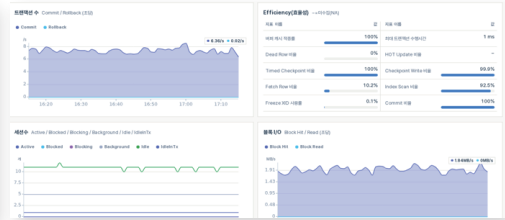
네트워크 모니터링(NMS)

장비 상태부터 인터페이스, 경로, 트래픽까지 하나의 장비 상세 화면에서 확인하고, 장애 시점을 Snapshot으로 분석합니다.



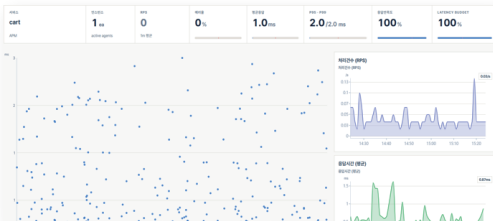
Database 모니터링(DPM)

Oracle부터 오픈소스, NoSQL 등 다양한 DB를 세션, Lock, Wait, SQL 실행계획까지 심도 있게 분석합니다.



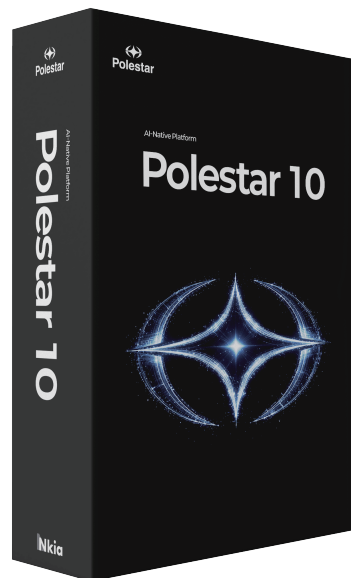
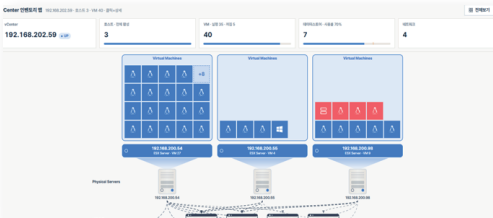
애플리케이션 모니터링(APM)

Java/Node.js/Go/Python과 OpenTelemetry를 수용하는 분산 트레이스로 서비스 품질 저하를 코드 DB 호출까지 추적합니다.



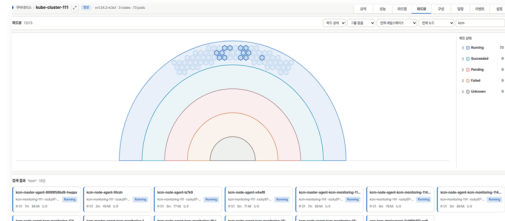
가상 머신 모니터링(VMM)

vCenter-AHV-OpenStack의 서로 다른 자산 구조를 공통으로 관제하고, Host-VM을 하이퍼바이저 관점에서 분석합니다.



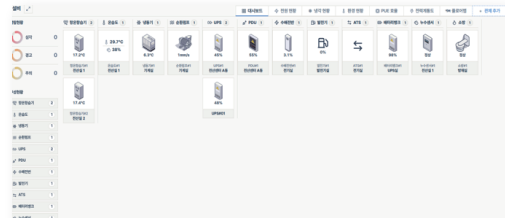
Kubernetes 모니터링(KCM)

Kubernetes/OpenShift/EKS/AKS/GKE의 Node-Namespace-Workload-Pod-Service를 하나의 계층과 운영 경험으로 관리합니다.



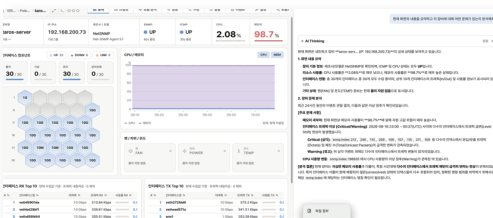
설비 관리 시스템 모니터링(FMS)

전원·냉각·환경·공간을 IT 인프라의 배경이 아니라 서비스 가용성에 영향을 주는 관제 도메인으로 다룹니다.



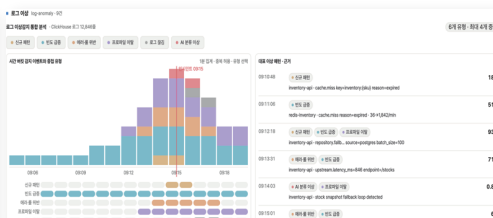
LLM 기반 AI 어시스턴스

LLM 기술을 활용한 요약, 정보 검색 기능으로 사용자 편의성과 업무 효율성을 높이고, 문제 해결 시간을 단축하며, 신속한 의사결정을 지원합니다.



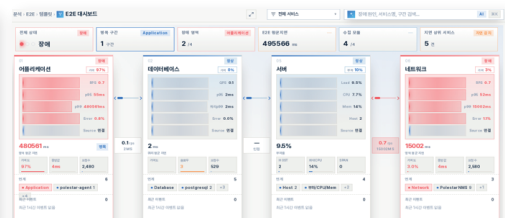
AI 기반 데이터 해석

AI 기반으로 다양한 소스의 이벤트와 데이터를 시각화하고, 로그 파서를 통해 복잡한 로그를 구조화하여 분석 편의성을 높입니다.



End-to-End 분석

다양한 서비스 상태를 한 화면에서 확인하여 실시간으로 이상 알림과 대시보드를 통해 이상 발생 시 즉각적인 대응이 가능합니다.

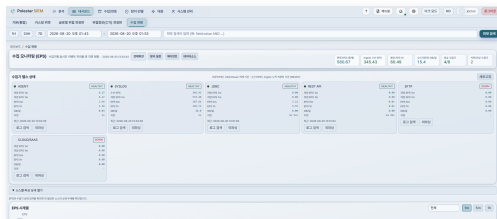


탐지에서 대응까지, 하나로 완성하는

지능형 보안관제 솔루션 Polestar SIEM

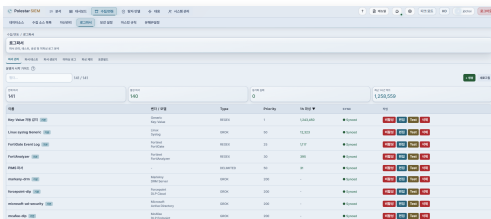
수집 현황 모니터링

유연한 확장을 지원하며 다양한 환경에서도 수집을 지원하며 수집 지연 시 즉시 확인 가능합니다.



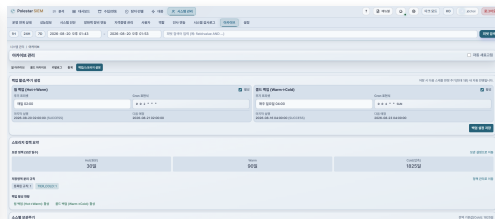
사용자 정의 파서

사용자 정의 파서를 통해 신규 시스템을 신속하게 연계하고, 조직 환경에 맞는 로그 분석과 검색, 통계 및 탐지 정책을 유연하게 적용할 수 있습니다.



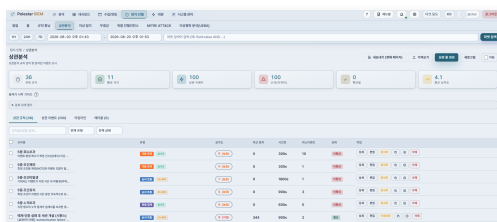
원본로그 정책

법적 요구사항 및 규정에 따른 원본 로그별 보관주기 설정하고 원본로그 백업 주기를 설정합니다.



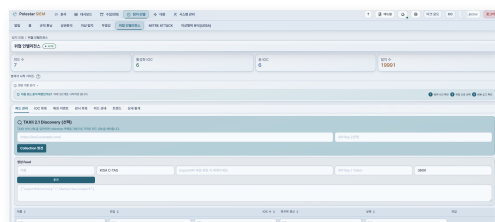
상관 분석

조건 및 규칙을 기반으로 회수초과, 누적초과, 조건유지, 조건제외, 조건 미발생 유형을 조합하여 복합 상관분석을 지원합니다.



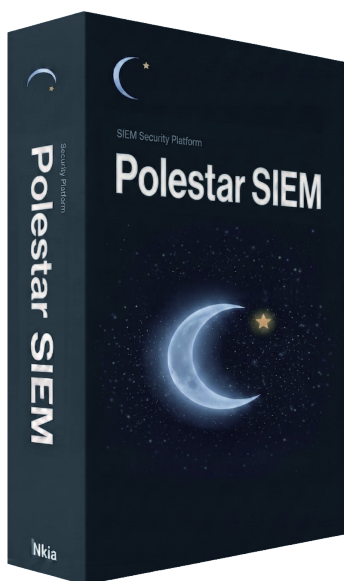
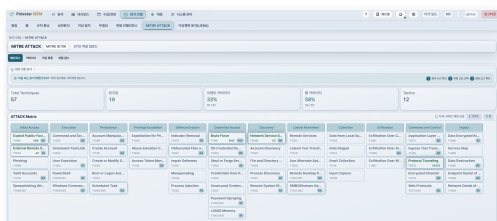
위협 인텔리전스 연동

외부 위협 인텔리전스(금융보안원, KISA, VirusTotal, AbuseDB 등) 정보를 수집하고, IOC와 로그/알람의 상관분석 지원합니다.



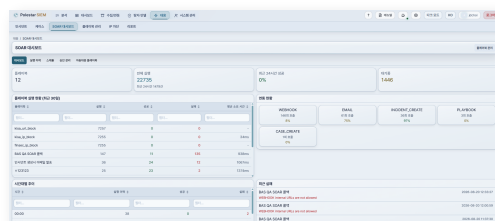
MITRE ATT&CK 자동 매핑

STIX 지식베이스를 활용하여 룰, 이벤트 및 엔티티를 MITRE ATT&CK 프레임워크에 자동 매핑하고, ATT&CK 커버리지 분석을 지원합니다.



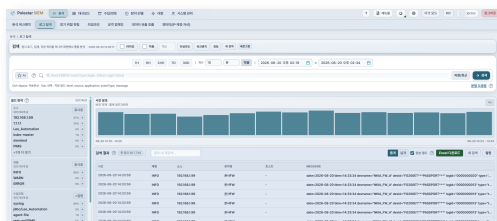
SOAR 자동 대응

전반복적인 보안 대응 절차를 자동화하고, 신속한 위협 대응을 통해 MTTR 단축을 지원합니다.



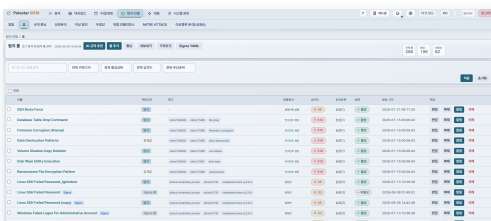
자연어 검색과 이벤트 요약

AI 기반 자연어 검색과 보안 이벤트 요약 기능을 통해 복잡한 로그 분석 과정을 단순화하고, 보안 담당자의 신속한 위협 분석 및 대응을 지원합니다.



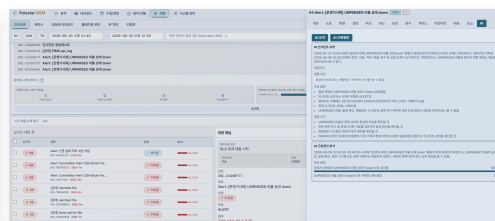
AI 탐지 룰 추천

로그 샘플과 기존 룰을 분석해 누락된 탐지 시나리오의 탐지률을 AI가 추천하는 기능을 제공합니다.



AI 인시던트 요약 및 근본원인 분석

인시던트의 연관 알람-증적-타임라인을 AI가 종합해 핵심 경위와 권장 조치를 자동 요약하는 기능을 제공합니다.



정보시스템 안정성 관리체계 제도화 및 시행

2026.04 행정기관 및 공공기관 정보시스템 안정성 고시

정보시스템 등급에 따른 체계적 운영 및 관리

정보시스템 장애 발생 시 신속한 장애 대응 및 복구

장애 재발방지와 지속적 개선을 위한 사후관리 체계 확립

재해복구 및 백업체계 구축·운영을 통한 정보시스템 안정성·신뢰성 제고

- 정보시스템 등급 구분 및 운영·관리 기준 적용
- 표준화된 대응체계를 통해 복구시간 단축
- 근본원인 분석을 통해 유사 장애 재발 방지
- 이력·결과를 반영하여 지속적 개선 체계 마련
- 백업 및 재해복구 체계 구축
- 정기백업·복구훈련을 통한 서비스 연속성 확보

“해야 할 일이 너무 많습니다”

표준운영절차

적용 대상

- A1~A3 등급 : 절차 및 운영 시스템 도입 의무
- 범정부 정보시스템 : 8개 표준운영절차 적용 및 시스템 의무화
- 응용프로그램 관리 : 9개 표준운영절차 적용 및 시스템 의무화

내용

- 예방 : 요청관리, 구성관리, 변경관리, 이벤트관리, 서비스수준관리, 배포관리, 테스트관리, 형상관리, 연계관리, 운영상태관리
- 대응 : 장애관리, 백업관리
- 사후관리 : 문제관리

예방점검체계

- A1~A3 등급 : 8개 분야 점검 의무화
- A4 등급 : 3개 분야 점검 의무 및 4개 분야 점검 권고

- 일상점검 : 상태점검, 서비스점검, 유효성점검
- 특별점검 : 오프라인점검, 이중화점검, 성능점검, 업무집중기간 점검
- 구조진단

“예상되는 문제점, 어떻게 해결하시겠습니까”

표준운영절차

무엇을 준비하고
어떻게 대응해야 할까요?

인력부족

표준운영절차 담당자,
ITSM 시스템 담당자,
예방점검 담당자는
누가 말습니까?

시간부족

언제 그 많은 점검항목을
수작업으로 점검하고,
절차를 관리합니까?

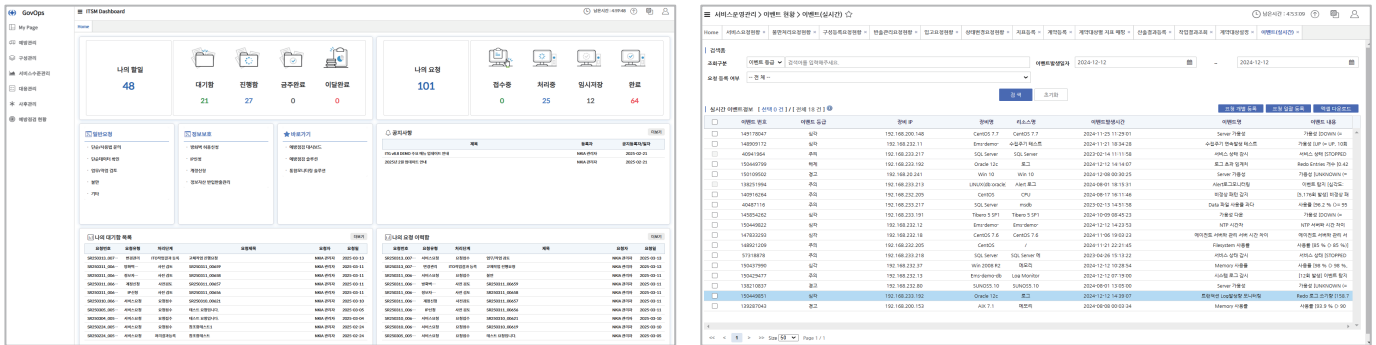
예산부족

필요한 컨설팅 또는 자문,
시스템 도입 비용과
운영비용은 어떡합니까?

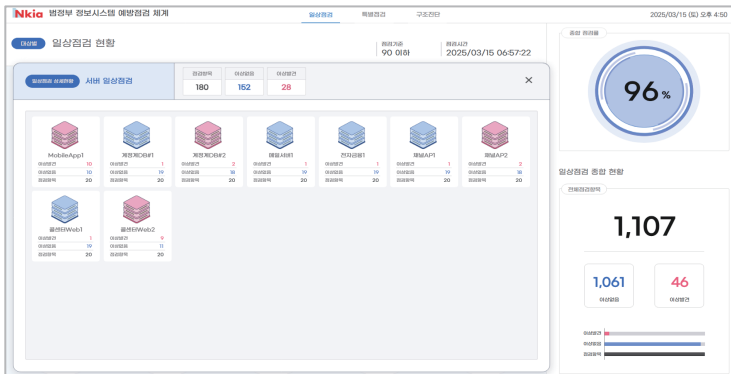
Polestar GovOps

표준운영절차 · 예방점검 체계 확립

예방 · 대응 · 사후관리 운영절차 표준화



예방점검체계 자동화



“Polestar GovOps를 도입하면 이렇게 달라집니다!”

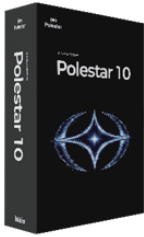
Before

- 표준화 및 체계화 되지 않은 절차
- 점검과 결과보고에 많은 시간 투입
- 시스템별 개별 기준으로 운영 및 관리

After

- 현장 중심의 표준운영절차 정착
- 자동화로 운영업무 효율화
- 정보시스템 중심의 운영

솔루션 라인업



Polestar 10



Polestar ITSM
Polestar ITAM



Polestar Dashboard
Polestar DOMS



Polestar SIEM

주요 레퍼런스

공공 기관 · 지자체



금융 기업



민간 기업

