

호스트 보안 : 기업용 클라우드 소프트웨어 솔루션 업체

Host 환경의 취약점을 점검/탐지하여 통합 모니터링 및 관리

PainPoint

- 환경
 - 리눅스 기반 AWS EC2/ECS 도입, 8천대의 EC2 운영 중
 - 1700여개의 FedRAMP/PCI 컴플라이언스 준수
- 직면 과제
 - 다양한 호스트용 툴의 확산 (OS Query, Rapid7, Axonious 등)
 - 현재 툴은 클라우드 네이티브가 아니며 CSPM, 컨테이너 등을 수용하지 못함
 - SOC 업무 증가

Solutions

- **클라우드 네이티브 보안 솔루션을 통한 호스트 보안**
 - 에이전트를 줄이고 Prisma Cloud의 호스트 보안과 통합
 - 프로세스, 파일 및 네트워크 모니터링을 통해 알려진 위협에 대한 IDS 탐지를 호스트 보안으로 변환
 - 주요 애플리케이션 (MySQL, Postgres 및 Ruby)을 보호하기 위한 사용자 지정 규칙을 통합하여 SOC에 대한 부하를 줄이고 알려진 위협 벡터를 방지

