스폰서 발표 세션 | AWS를 위한 도커, 컨테이너 (이미지) 환경 보안 방안

양희선 부장, TrendMicro

AWS 내 보안 접근은 기존의 보안 적용 방식과 많은 차이점이 있습니다. AWS 환경에서는 도커 및 컨테이너를 사용하여 빠르게 서비스를 적용하고 커스터마이징 서비스가 이루어져 동시에 보안을 적용 적용함에 있어 많은 어려움이 있습니다. 호스트 OS 및 독립적인 컨테이너에 대한 많은 위협들이 있고 이러한 위협들을 빠르게 파악하는 동시에 해당 위협 요소를 제거 및 차단하는 방법이 필요합니다. 본 세션에서는 일련의 위협들로 부터 도커 컨테이너 및 컨테이너 (이미지)에 대한 보안 위협들을 알아보고 트렌드마이크로의 Deep Security 및 Smart Check를 통한 효율적인 보안 적용 방법에 대한 가이드를 제시합니다.

AWS + 도커 및 컨테이너 활용 서비스 인프라의 보안에 필요한 사항들

ㅇSW 변경 감지 : 업그레이드, 다운그레이드, 삭제 등

ㅇ속성 변경 사항에 대한 바이너리 모니터링

ㅇ프로세스 실행

ㅇ중요 파일

ㅇiptables

ㅇ주요 디렉토리 사용권한 등

Deep Security : 호스트 OS ~ 애플리케이션 단까지의 통합 보호

