

<주요 Q&A>

CISO's Complexity, Containment and Other C-Words

Q1. 센티넬원이 어느 나라 제품인가요?

미국 제품이며, 삼성SDS에서 한국 총판을 담당하고 있습니다.

Q2. 센티넬원 EDR 솔루션의 주요 기능이 궁금합니다.

센티넬원 EDR 은 기존 백신으로는 제로데이, 랜섬웨어 같이 고도화 되는 공격의 방어에 대한 한계가 있어 이를 보완하기 위한 솔루션입니다.
인공지능(AI)기반으로 Endpoint 의 모든 위협을 탐지하고 방어하며, 사이트에 발생하는 잠재 위협에 대한 사냥기능(Threat Hunting)을 제공합니다.
또한 Endpoint 에 위협이 탐지되면 위협이 감염되기 이전 상태로 Clean-up 시키는 것은 물론, 랜섬웨어 감염 탐지 시 Rollback 을 지원하는 유일한 솔루션입니다.
또한, 클라우드 보안을 위한 CWPP Agent와 IoT 보안을 위한 가시성 확보 기능도 추가적으로 제공합니다.

Q3. 센티넬원은 Agent 방식으로 동작하나요?

맞습니다. EDR은 Agent 방식으로 Endpoint(PC 및 서버) 에 설치되어 Endpoint에 발생되는 이벤트를 모니터링 함으로써 위협을 탐지합니다.

지원환경

- Windows, Linux, MAC OS
- VM 및 컨테이너 (쿠버네티스) 환경
- Legacy Windows(windows XP 포함)