EDR 솔루션 개발 프로젝트

EDR 사업본부 / 컨설팅팀

강서일 부장

Smart Security & Service
NICSTECH

EDR 솔루션 개발 방향성 및 목표

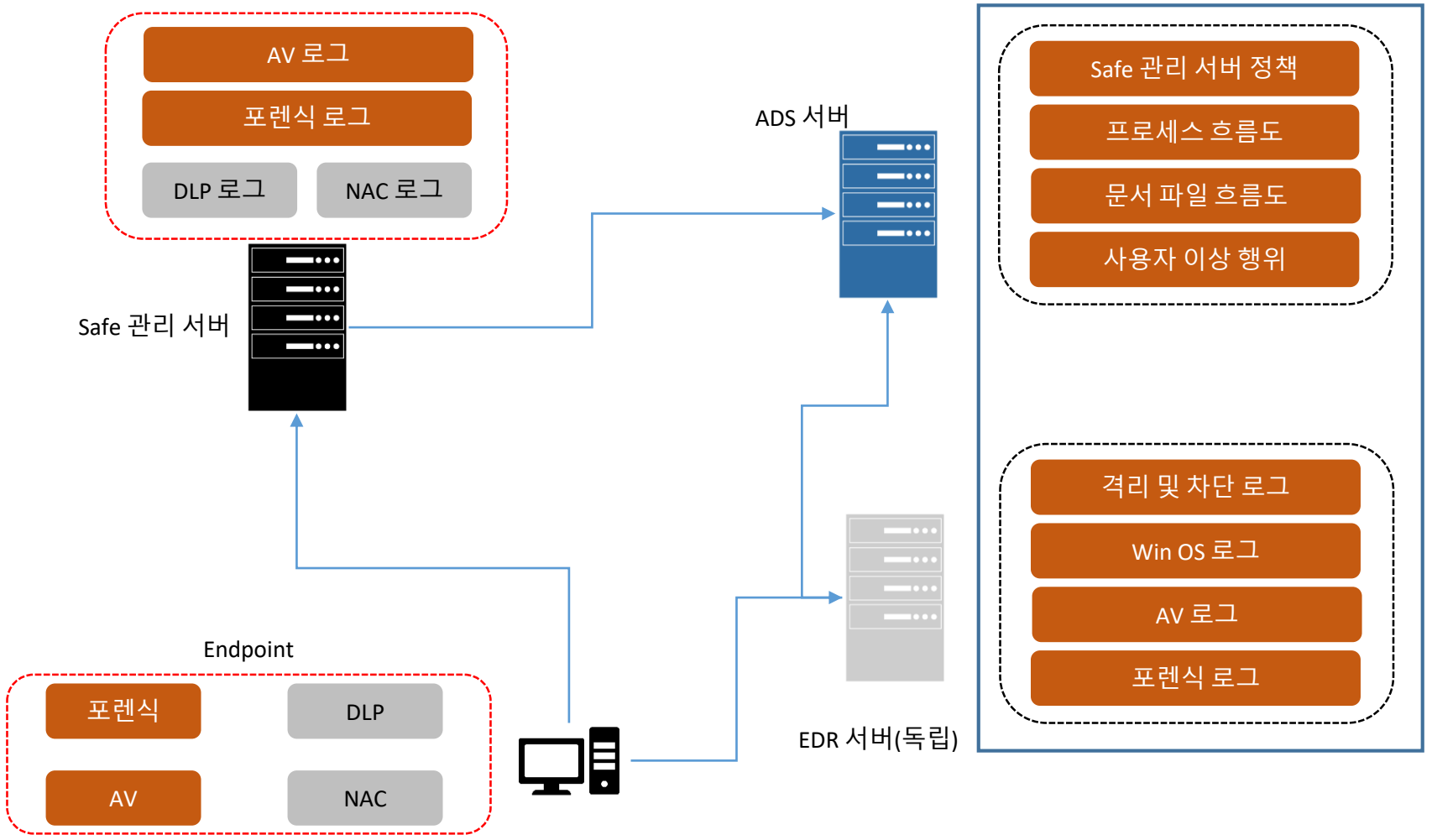
- 목표
  - 2018년 EDR 솔루션 출시
  - 2018년 상반기 내 POC 버전 출시
  - 고객사 EDR 솔루션 제안 및 판매

- 방향성
  - 기존 제품(Safe 시리즈)와 연동 혹은 업그레이드로 운영
  - 신규 고객이 도입 시 독립적인 솔루션으로 운영
  - EDR의 백신 업체와 경쟁 방안으로는 연동
  - 닉스테크의 EDR은 DLP 기반으로 장점 특화
  - 외산 솔루션과 차별성을 제공

EDR 솔루션 개발 구성도

: 보유 기술

: 미 보유 기술

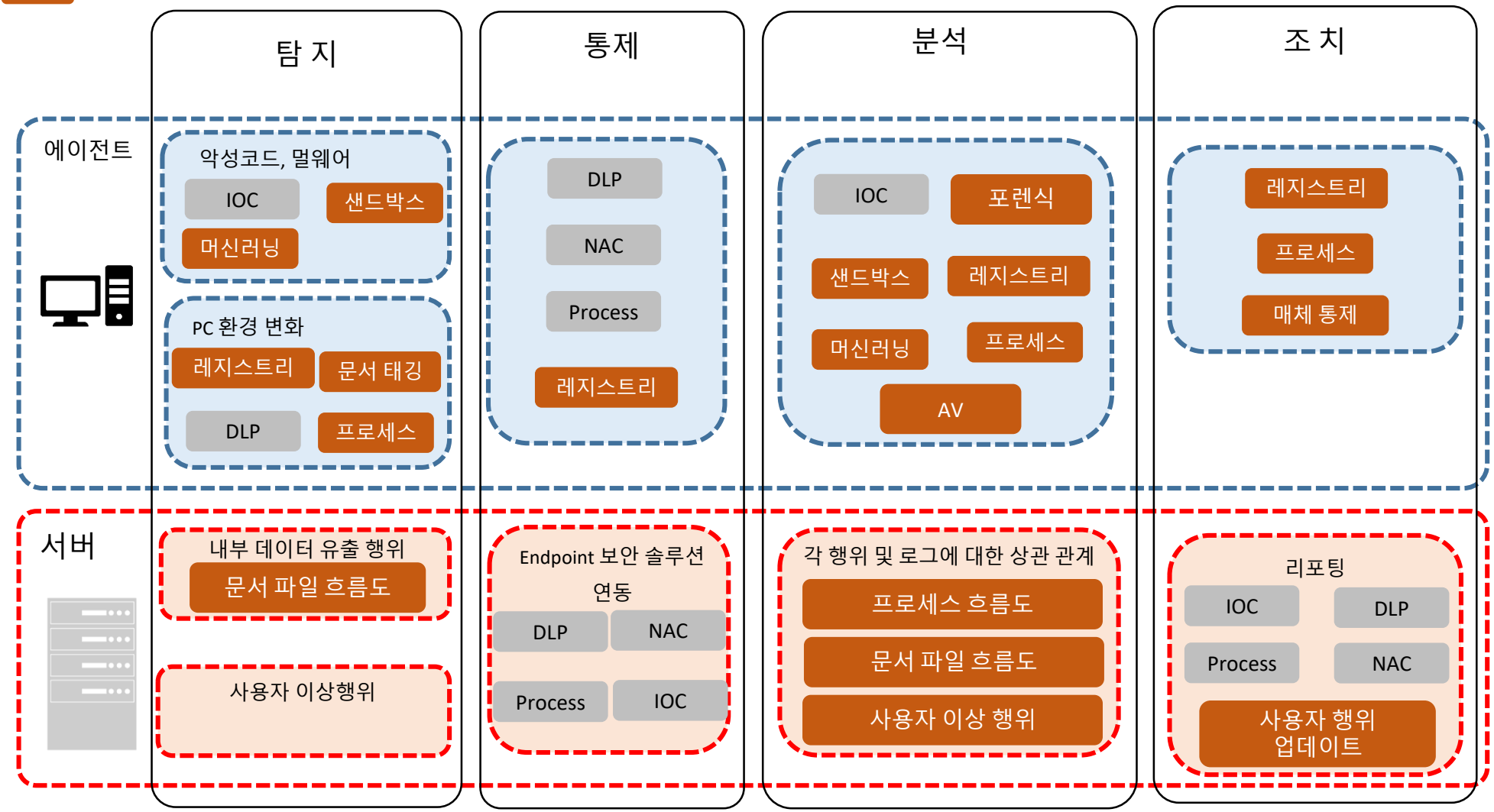


EDR 솔루션 개발 기능(요약)

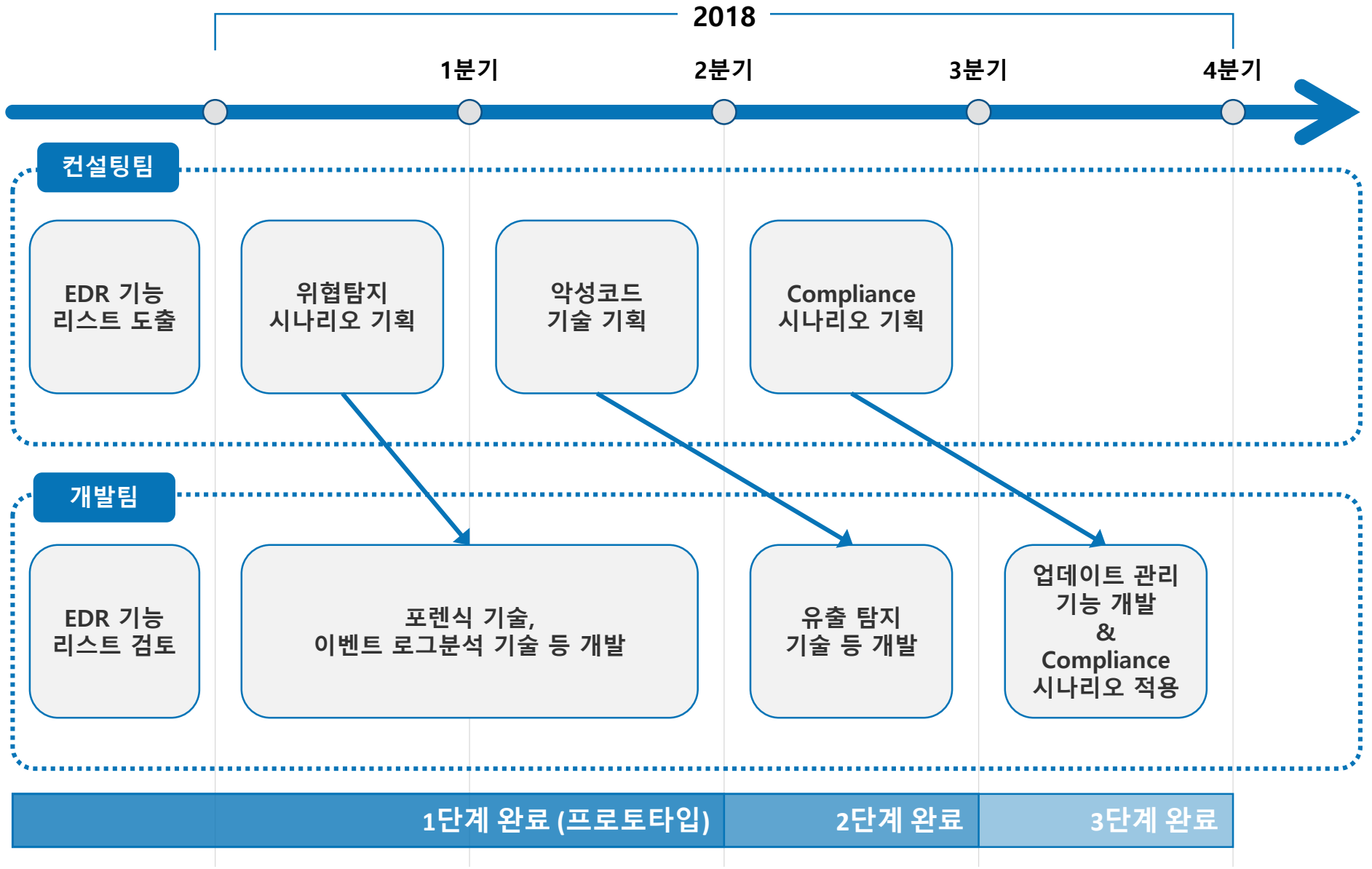
: 보유 기술

: 미 보유 기술

*** 기능 상세 내용은 엑셀 파일을 참고 하시기 바랍니다.**



EDR 솔루션 개발 일정 (요약)



EDR 솔루션 개발 일정 (상세)

EDR 제품기획				
분류	내용	우선순위	완료일정	부서
초안기획	EDR 기능리스트 산출		11/13 (1차)	컨설팅
EDR 기능리스트 검토			11/20 (1차)	기술연구소
EDR 탐지룰 기획	위협탐지 시나리오 기획 - 내부정보 유출행위 위협 정의 - 단말의 환경변화에 따른 보안 위협 정의		1사분기	컨설팅
악성코드 기술 기획	기존 악성코드 기술 조사		2사분기	컨설팅
	업체 조사 및 기술검토		2사분기	컨설팅
	보고서 작성		2사분기	컨설팅
컴플라이언스 조사	국내 컴플라이언스 조사		3사분기	컨설팅
	보안시나리오 화		3사분기	컨설팅
EDR 상세설계 및 개발 (Windows, MAC 지원)	**포렌식 기술 (레지스트리, 프로세스, 문서태깅 등)**	1	2사분기	기술연구소
	프로세스 흐름 모니터링 기술	1	2사분기	기술연구소
	문서파일 흐름 모니터링 기술	1	2사분기	기술연구소
	Windows OS 이벤트로그 분석 기술	1	2사분기	기술연구소
	자산에 대한 가시성 확보	1	2사분기	기술연구소
	내부정보 데이터 유출행위 탐지 기술	2	3사분기	기술연구소
	사용자 이상행위 탐지 기술	2	3사분기	기술연구소
	레지스트리 원복 기술	2	3사분기	기술연구소
	엔드포인트 보안솔루션 정책 연동 (DLP, NAC, Process, IOC 등)	2	3사분기	기술연구소
	IOC 업데이트 관리 (모델)	3	4사분기	기술연구소
	내부정보 데이터 유출행위 관리 (모델)	3	4사분기	기술연구소
	사용자 이상행위 관리 (모델)	3	4사분기	기술연구소
옵션(특화)	악성코드 및 멀웨어 진단 (2단계 필수)	2	3사분기	기술연구소
	국내 컴플라이언스 준수 현황 진단 (인더스트리 별)	3	4사분기	기술연구소
마일스톤				기술연구소
품질테스트				기술연구소
POC (프로토타입)				기술연구소

- 기술연구소와 미팅을 통해 일정 및 개발 내용이 변경될 수 있음
- 완료 일정만 명시할 뿐 투입 M/M는 기술연구소에서 산정 필요