EDR 동향 및 윈스 연구 과제 방안

문서 이력

날짜	구분	내용	작성자
2017.05.11	초안	초안 작성	컨설팅팀 / 양다은 대리, 권혁재 과장, 김민규 차장, 강서일 부장

1. Endpoint 보안 동향

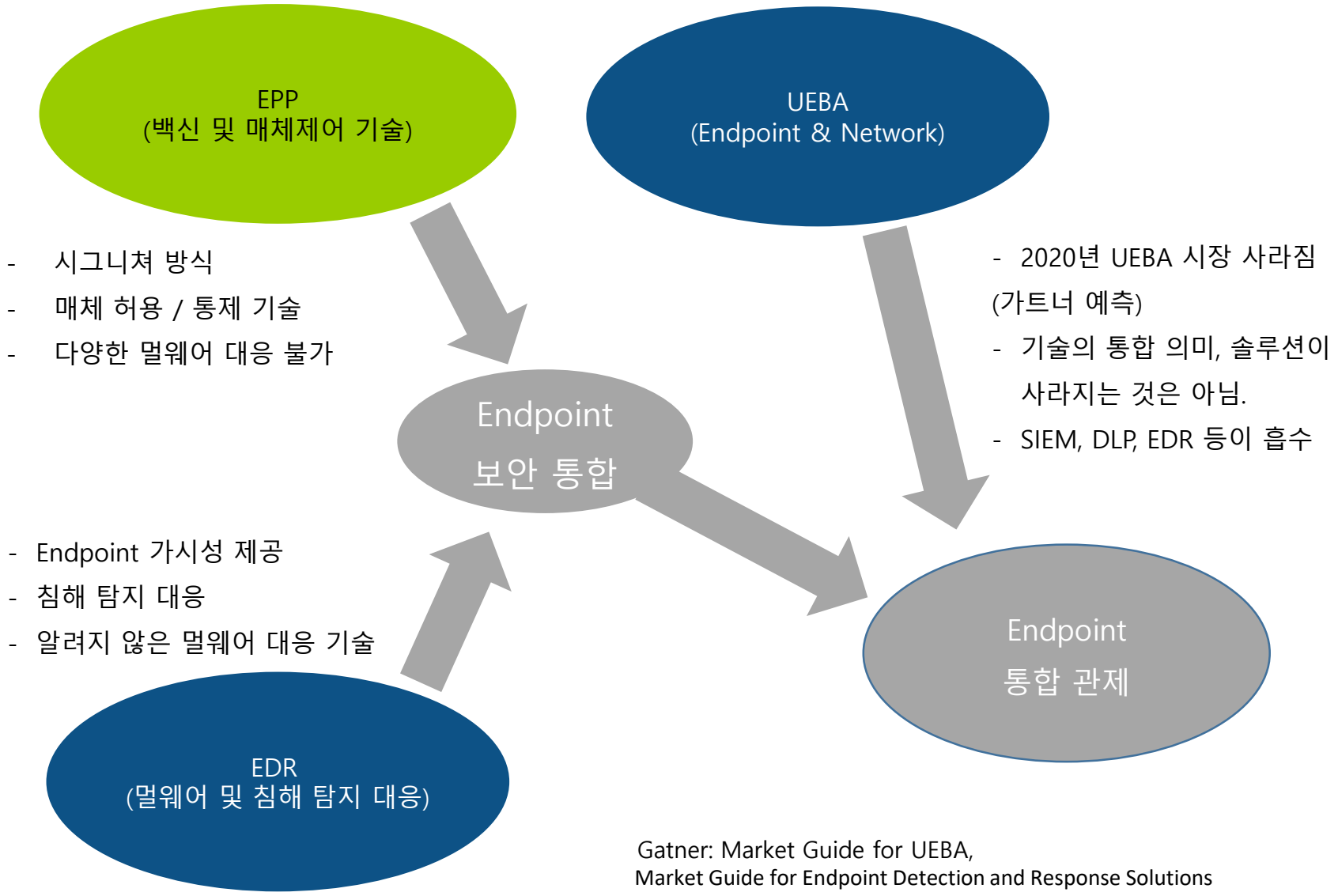
- EDR(Endpoint Detection & Response)
  - ➔ 멀웨어 공격에 대하여 샌드박스 및 시그니쳐 기반의 대응 한계
  - ➔ Endpoint에서 이상행위를 발견하여 분석하고 사후 대응 방안 모색

- UEBA(User & Entity Behavior Analytics)
  - ➔사용자나 단말의 행위 분석 기술
  - ➔분석으로 네트워크 통신, 어플리케이션 등 다양한 범위에 대한 내용 상관 분석
  - ➔ AI의 머신 러닝 기술 등을 활용으로 현재 각광 받고 있음.

- 국/내외 다양한 솔루션이 EDR로 이동하고 있음
  - ➔백신 업체는 시그니쳐 방식 및 머신러닝, 매체 제어를 통해서 이동
  - ➔네트워크 보안 솔루션은 에이전트 개발을 통해서 침해지표 및 멀웨어 탐지 방식 제공
  - ➔정통적인 매체 제어 보안 솔루션도 악성코드 탐지 기능 운영

<출처>
- Gartner Security Technology Trends 2016
- Endpoint Security Trends 2016 from Solutionreview.com

1. Endpoint 보안 동향



Gatner: Market Guide for UEBA,
Market Guide for Endpoint Detection and Response Solutions

2. 요구 기능

EDR

분류	기능	설명
침해사고 탐지	시스템 모니터링	• 시스템 레벨의 모든 행위 및 이벤트: File, Process, Registry, Memory, Network 등 • **사용자 행위 분석 (점점 추가되는 추세)** • 모든 행위 및 이벤트에 대해 실시간으로 높은 가시성 제공
	탐지	• **침해사고지표(IOC) 기반으로 위반, 이상 행위 탐지** • 일반적인 멀웨어 행위 뿐 아니라 메모리 공격, 권한 탈취 등에 대한 탐지
침해사고 기록과 조사	로깅	• 모니터링 하는 모든 엔드포인트의 이벤트를 기록하고, 타임라인 기능 반드시 제공 • 엔드포인트 혹은 로그들에 대한 자연어 검색 기능 (Top 5 벤더 지원)
	증거 자료수집	• 포렌식 수준의 증거자료 수집: 원본파일, 메모리/디스크/패킷 덤프 등
	가시성	• **침해사고 별 킬 체인에 따른 가시성 제공** • 대시보드, 로그 화면 등에서 드릴다운을 통한 상세 분석 정보 제공
침해사고 억제와 치료	격리	• 감염된 엔드포인트 격리
	치료	• **멀웨어 삭제, 변화 내용 롤백 등을 통한 치료**
기타	지원 OS	• Windows, Mac, Linux (Ubuntu, Redhat 등)
	머신러닝	• **머신러닝과 딥러닝을 통한 침해사고 등의 예측 (점점 추가되는 추세)**

UEBA

분류	기능	설명
데이터 분석	다양한 분석 지원	• 머신러닝 (필수) 뿐 아니라 룰과 프로파일링 분석 지원 • 비정형 데이터 (예. SNS 글)에 대한 분석 지원 (점점 추가되는 추세)
가시성 확보	데이터 표현과 시각화	• 드릴다운, 시계열, 트렌드 분석 및 리포트 기능 제공

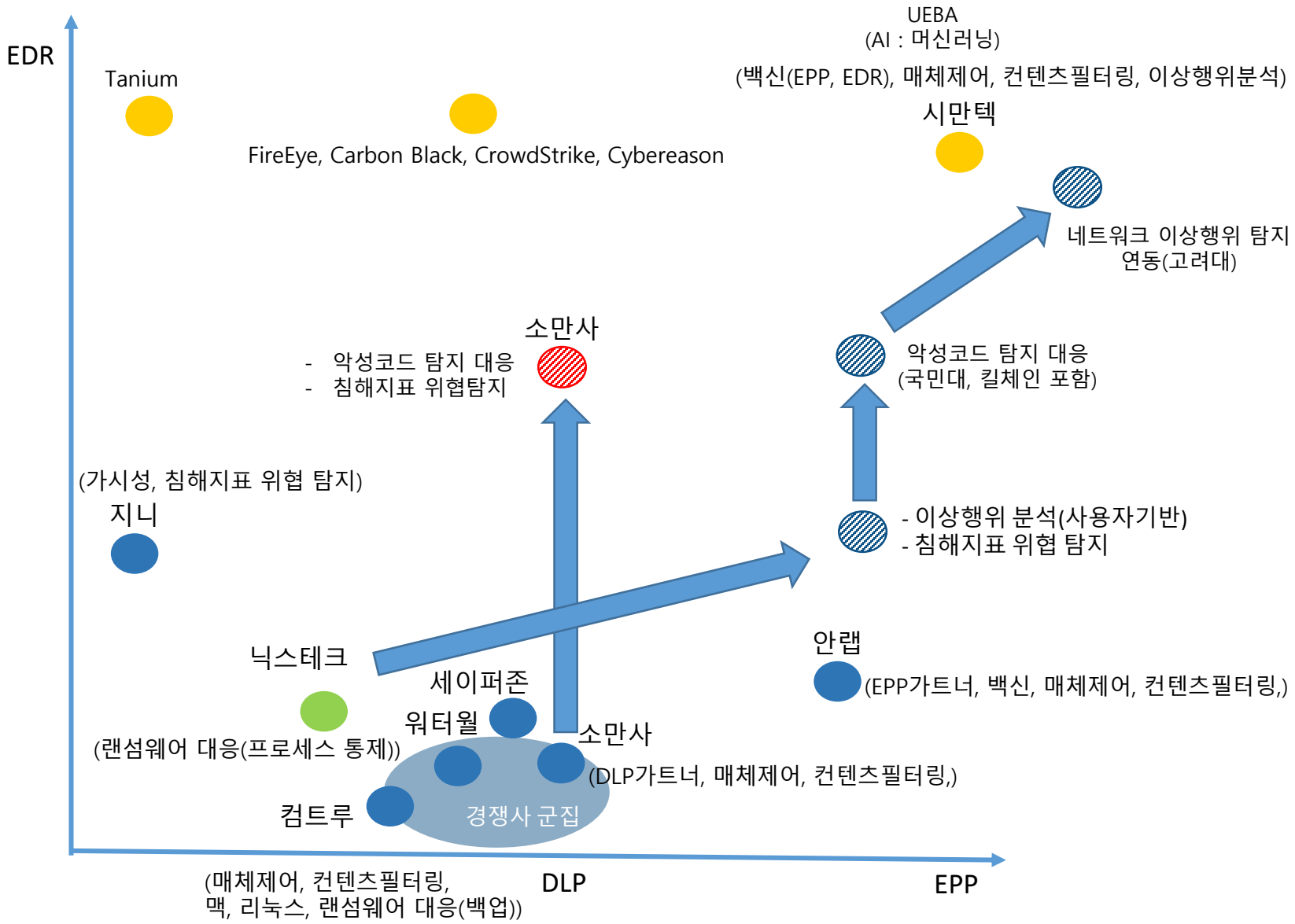
3. 연구 과제 개발 방향

1차년도	2차년도	
단말 보안장비의 STIX/TAXII 기반 프로토타입 구현	한국형 STIX/TAXII표준기능 고도화	• 침해사고지표(IOC) 기반으로 위반, 이상 행위 탐지
	정상 행위 기반 이상행위 탐지 (사용자 중심 내부 정보 유출)	• 사용자 행위 분석 (점점 추가되는 추세, UEBA)

확보 가능 기술

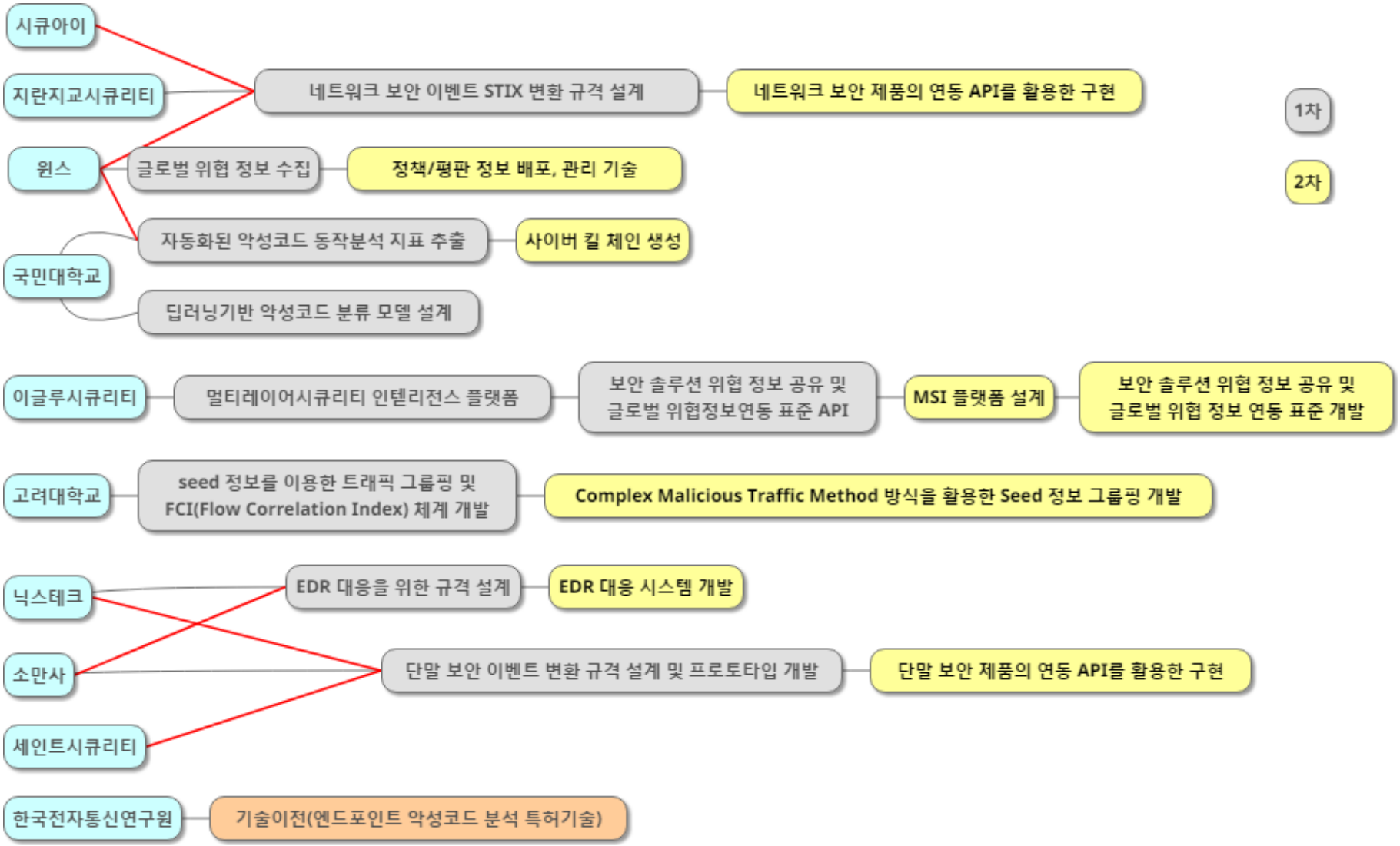
딥러닝 기반의 악성코드 분류모델 설계 및 구현 (국민대)	악성코드 그룹별 사이버 킬-체인 생성 (국민대, 윈스)	• 침해사고 별 킬 체인에 따른 가시성 제공
악성코드 동작 분석 지표 추출 (국민대)		• 머신러닝과 딥러닝을 통한 침해사고 등의 예측 (점점 추가되는 추세)
Seed기반의 이벤트 분석 알고리즘 개발 (고려대)	Seed기반의 비정상 행위 탐지/추적/예측/대응 기술 개발(고려대)	• 네트워크 이상행위 분석 대응

4. 기술 개발에 대한 의견


EDR
Tanium
FireEye, Carbon Black, CrowdStrike, Cybereason
UEBA
(AI : 머신러닝)
(백신(EPP, EDR), 매체제어, 컨텐츠필터링, 이상행위분석)
시만텍
네트워크 이상행위 탐지
연동(고려대)
소만사
- 악성코드 탐지 대응
- 침해지표 위협탐지
악성코드 탐지 대응
(국민대, 킬체인 포함)
(가시성, 침해지표 위협 탐지)
지니
- 이상행위 분석(사용자기반)
- 침해지표 위협 탐지
안랩
(EPP가트너, 백신, 매체제어, 컨텐츠필터링,)
닉스테크
세이퍼존
워터월
소만사
(DLP가트너, 매체제어, 컨텐츠필터링,)
(랜섬웨어 대응(프로세스 통제))
컴트루
경쟁사 군집
(매체제어, 컨텐츠필터링,
맥, 리눅스, 랜섬웨어 대응(백업))
DLP
EPP

별첨1. 과제 진행 (1,2 차)

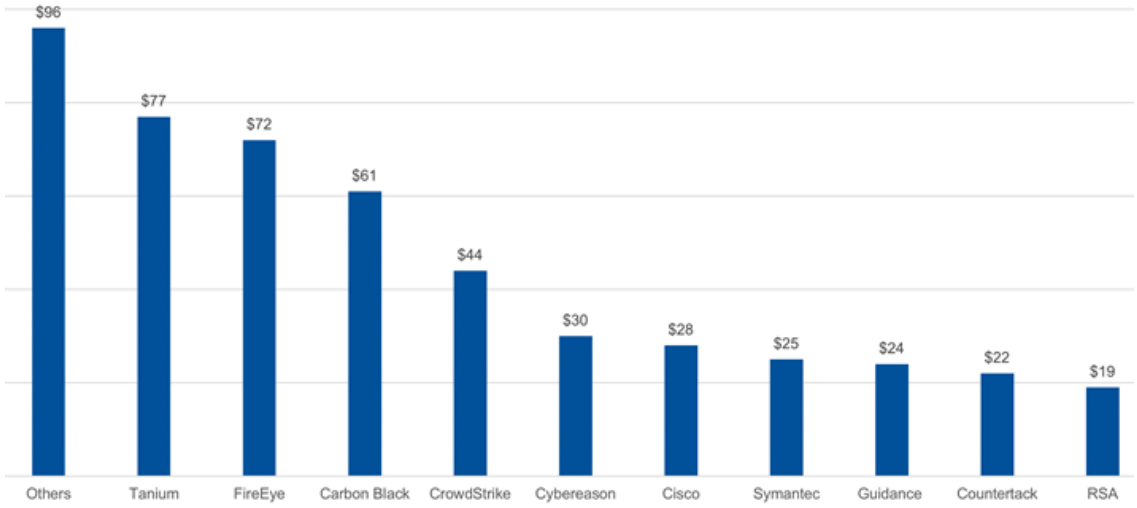
Security Analytics 기반의 이기종 보안 솔루션 위협 분석 및 대응 기술 개발



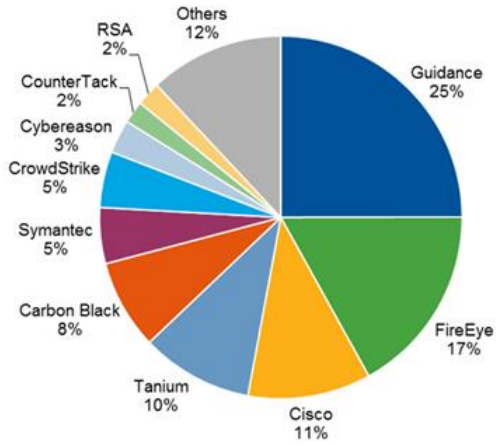
별첨2. 시장 규모

EDR

글로벌 시장규모: 2015Y $328M (약 3700억원) → 2016Y $623M (약 7000억원) 2배 성장



벤더 별 2016Y 매출



에이전트 설치 수에 따른 점유율
(전체: 약 4천만대)

출처: EDR Market Report, Gartner, 2017

UEBA

글로벌 시장규모: 2015Y $50M (약 550억원) → 2016Y $100M (약 1100억원) 2배 성장

2014	2015	2016	2017
$25M	$50M	$100M	$200M
약 275억원	약 550억원	약 1100억원	약 2200억원

출처: UEBA Market Post of Blog, Gartner, 2017