ETP(Endpoint Threat Platform)소개

엔드포인트 보안강화를 위한
행위기반 탐지분석 솔루션

SK infosec

I 개요

CounterTack 회사소개

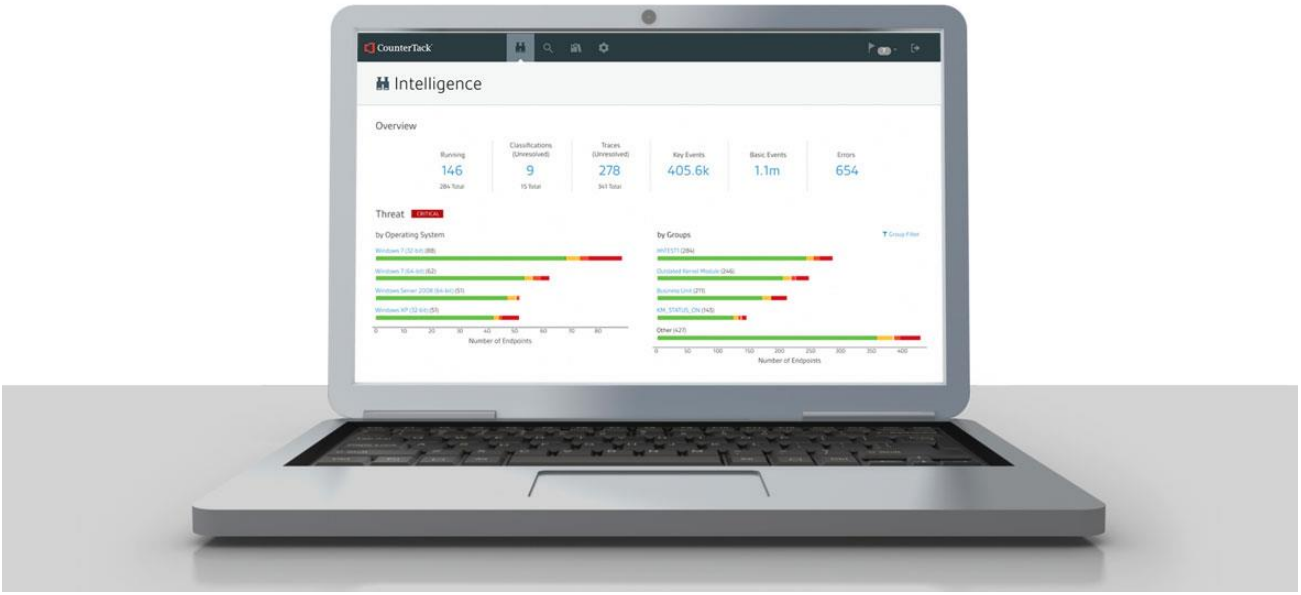
- 설립연도: 2011년 3월
- 본사 소재지 : 보스톤, 메사츄세츠
- 연구소 소재지 : 캘리포니아,산타모니카
- 아시아기술지원 소재지: 싱가포르, 로빈슨
- 주요 제품군 : Responder-Pro(메모리포렌식), Active-Defense(침해분석), ETP(단말APT)
- 경영진
  - Neal Creighton - CEO (GeoTrust)
  - Jim Bandanza - CRO/COO (RSA /EMC)
  - Alen Capalik - Founder / Chief Architect (Barclay Bank)
  - Michael Davis - CTO (McAfee)
  - Sean Bodmer - Chief Researcher (DoD, Federal Agency)
- 이사회
  - William J. Fallon - Chairman (US Military's Central Command)
  - Stuart McClure - Cylance CEO (McAfee, Foundstone)
  - Mark Hatfield - Fairhaven Capital

CounterTack
ENDPOINT SECURITY: AMPLIFIED

Gartner 2014 Cool Vendor

CRN
"Tech 10 Security Products: Advanced Threat Protection"

Bloor
ATP Technology (Champions category)



국내 침해사고 사례

"다수의 보안사고가 엔드포인트의 악성코드 감염으로 발생"

CounterTack

SK인포섹㈜

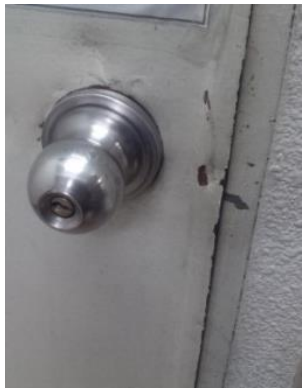
Anti-Virus 제품과 EDR(Endpoint Detection Response)제품의 차이?

"변형이 많은 시그니쳐 탐지가 아닌 공통적인 행위를 탐지"

Anti-Virus

VS

Endpoint Detection Response

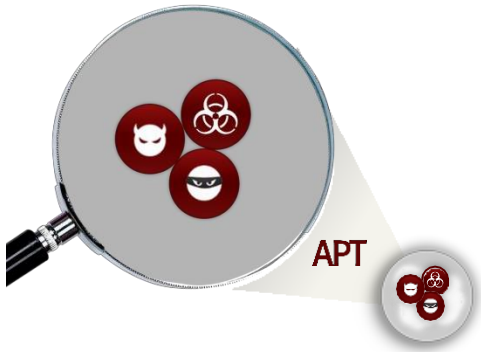


EDR은 AV의 대안이 아닌 강화

CounterTack

SK인포섹㈜

APT란 무엇이고, 대응방안은...?



APT(Advanced Persistence Threat)정의

특정 목적을 위해 특별한 형태와 방법으로 내부 시스템에 침투하여 자신을 은닉하고 목적이 달성될때까지 지속적인 활동이 가능한 실제적인 위협

APT 공격절차 – Cyber Kill Chain

① 정찰(Reconnaissance) ☞ ② 무기 제작(Weaponization) ☞ ③ 배달(Delivery) ☞ ④ 취약점 공격(Exploitation) ☞ ⑤ 설치(Installation) ☞ ⑥ 명령 및 제어(Command and Control) ☞ ⑦ 표적 대상 행동(Actions on objectives)

실제 악성코드가 동작되는 Delivery(APT Life Cycle) 단계 부터 탐지 및 대응이 이루어져야 함

CounterTack

SK인포섹㈜

Ⅱ 필요성 및 장점

SK 인포섹

ETP - 엔드포인트 랜섬웨어 및 APT 대응 솔루션

CounterTack®

Endpoint Threat Platform

알려지지 않은 악성 코드 탐지

- **행위기반 탐지진행으로 신종 및 변종 악성코드에 대한 추적이 가능**
- **커널기반의 모듈로서 엔드포인트의 부하 및 영향도 최소화**
- **악성코드의 루트킷이나 메모리패치 같은 은닉행위에 대한 가시성 확보**

탐지된 의심행위에 대한 명확한 분석과 신속한 대응

- **과탐 및 오탐을 줄이기 위한 다수의 분석모델을 종합적으로 판단**
  (Stateful Compromise Indicators + DigitalDNA + VirusTotal + IOC)
- **추적행위 전과정에 대한 도식화(RelationGraph) 사용**
- **악성코드의 실행중지, 추출 및 네트워크 자동격리 정책 운영**

●●● 추가적인 행위기반 엔드포인트 방어 대책 필요 ●●●

엔드포인트 백신을 통한 방어

- 악성파일의 샘플 확보가 필수
- 공격 분석이 되지 않으므로 변종에 의한 추가 공격시 선제적 차단 불가
- 백신엔진에 따른 과탐 및 오탐 사례 발생
- 후킹방식에 따른 엔드포인트의 부하 발생

네트워크 보안장비를 통한 방어

- 방화벽
  →단순 IP/PORT 차단에 기반
- IDS/IPS
  → 보안취약점 패턴방식으로 대량 수집로그에 대한 관리에 어려움
  → 코드압축 및 난독화를 공격시 탐지에 어려움
- 네트워크 APT
  → Sandbox 우회 및 회피기법 대응에 미비

보안운영정책을 통한 방어

- 망간 분리 운영
  → 업무 프로세스의 복잡성 및 리소스 증가
  → 잠입에 성공한 악성파일에 대한 조치불가
- 화이트리스트 정책 운영
  → 업무 가용성 및 신속성 저하
- 자동 패치 시스템 운영
  → 반복적인 무결성 검증과 배포관리가 필수

ETP만의 차별화된 기능

- ETP는 스냅샷 비교방식이 아닌 실시간 메모리 포렌식 기법을 기반으로 하고 있습니다
- 커널영역에 위치하여 중요정보를 보유한 장비의 시스템 성능저하 및 기존 보안솔루션과의 충돌 우려없이 정보를 수집합니다
- 수집된 단말 로그들은 빅데이터 분석 시스템으로 전송되며, 중앙에서 분석된 결과는 SIEM(CEF & LEEF)으로의 연계가 가능합니다

Kernel Module

엔드포인트(OS)에 설치
공격자는 발견할 수 없음
Temper-resistant, anti-evasion
시스템의 모든 행위 모니터링
실시간 데이터 수집 및 전송

Analysis Cluster

검증된 Big Data 기술 적용
수집된 위협에 대한 자동 분석
행위 분석에 기반한 탐지
기업 내 위협의 상관관계 분석
증거 자료의 안전한 관리 및 보전

Management Console

다양한 데이터 뷰 제공
강력한 검색 기능 제공
Dashboard option
- Intelligence, Endpoints, Behaviors, Search

Knowledge Library

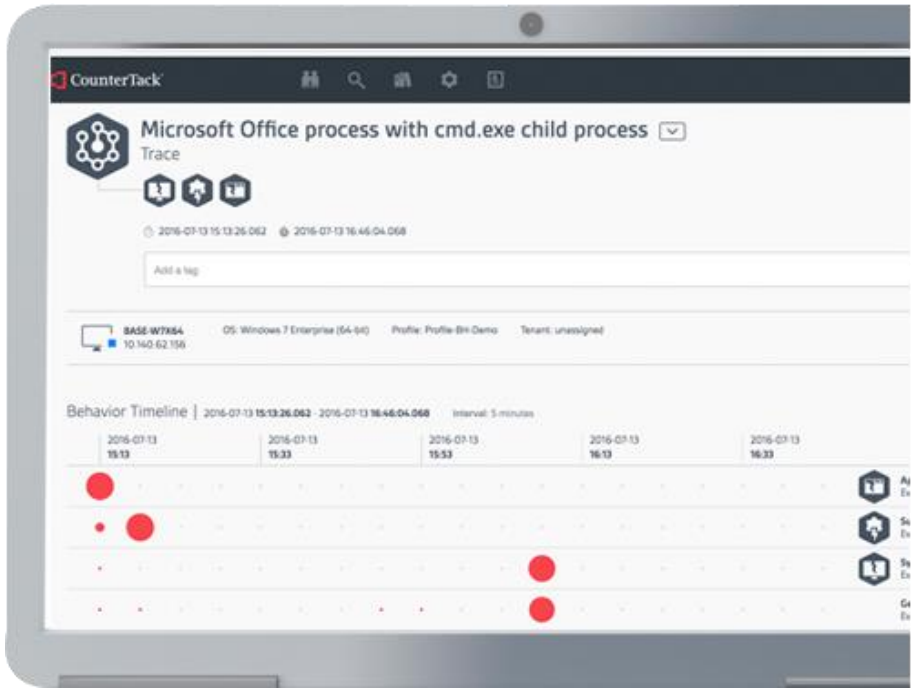
위협에 대한 자동 분류
다양한 탐지 Profiles 제공
사용자 정의 Basic connection
CyBOX, IOC 호환 및 지원

CyBOX(Cyber Observables eXpression): 사이버 운영 오브젝트 관련 표준
IOC(Indicators Of Compromised): 침해 지표

CounterTack

SK인포섹㈜

ETP 솔루션이 제공하는 '탐지–분석–조치–예방'의 보안사이클



❑ DETECT

- ❖ Stealth collection module에 기반하여 악성행위를 실시간으로 추적
- ❖ 특정 조건(Origin)에 맞는 행위 발생시 자동으로 상관 이벤트 수집

❑ ANALYZE

- ❖ 모든 행위를 Source / Action / Target으로 구별하여 분석
- ❖ File, Process, Thread, Registry, Network, Memory 정보확인
- ❖ 수집된 정보를 기반으로 위협요소의 가시성 확보를 통한 상세분석

❑ REMEDIATE

- ❖ 악성행위로 판별된 프로세스에 대한 차단 및 엔드포인트 격리
- ❖ 악성 프로세스의 실행 파일을 네트워크를 통해 수집

❑ RESIST

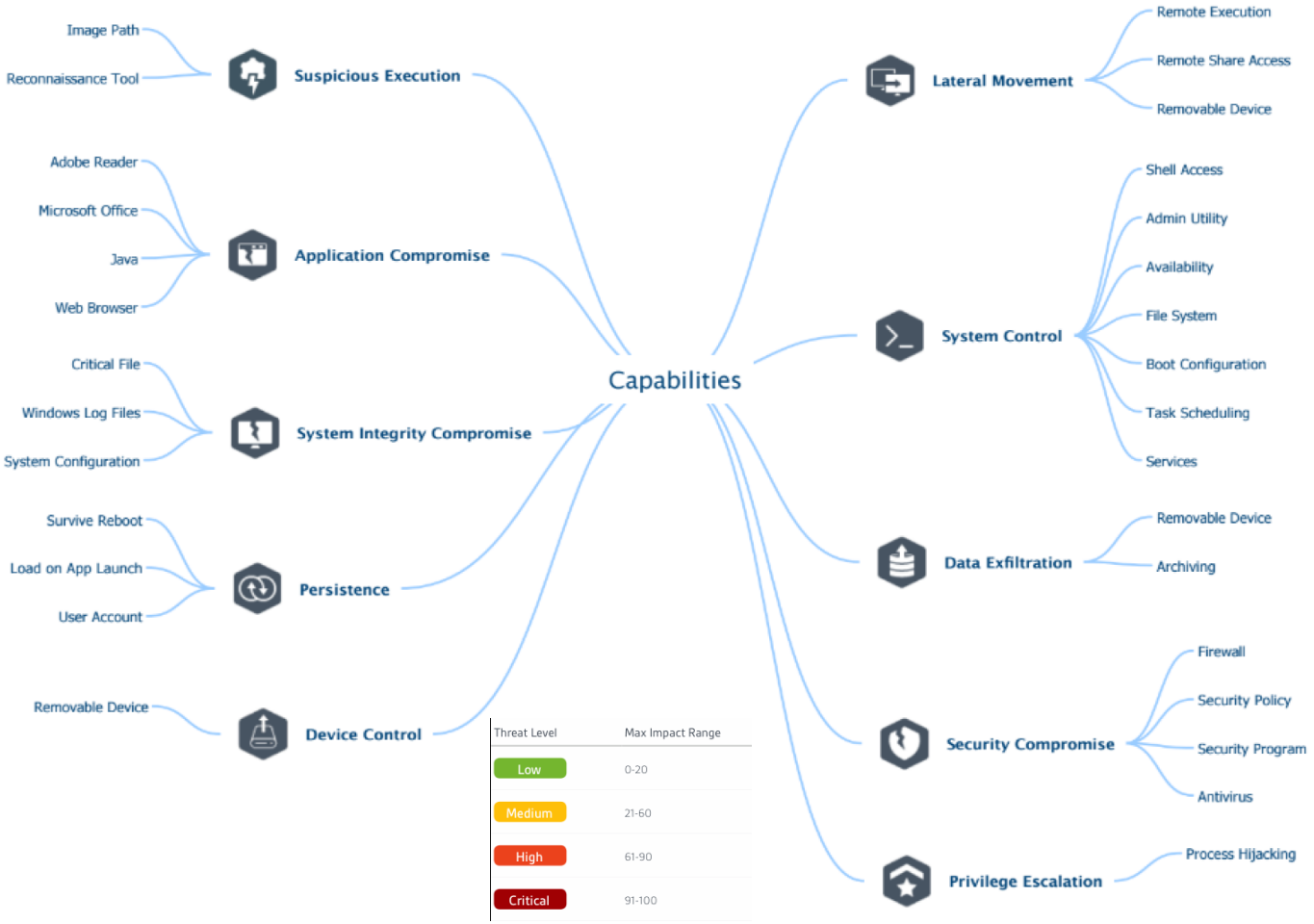
- ❖ 도출된 Resistance profile적용으로 자동 차단/격리정책 운영
- ❖ 분석된 새로운 악성행위는 탐지조건에 추가하여 변종에 대비

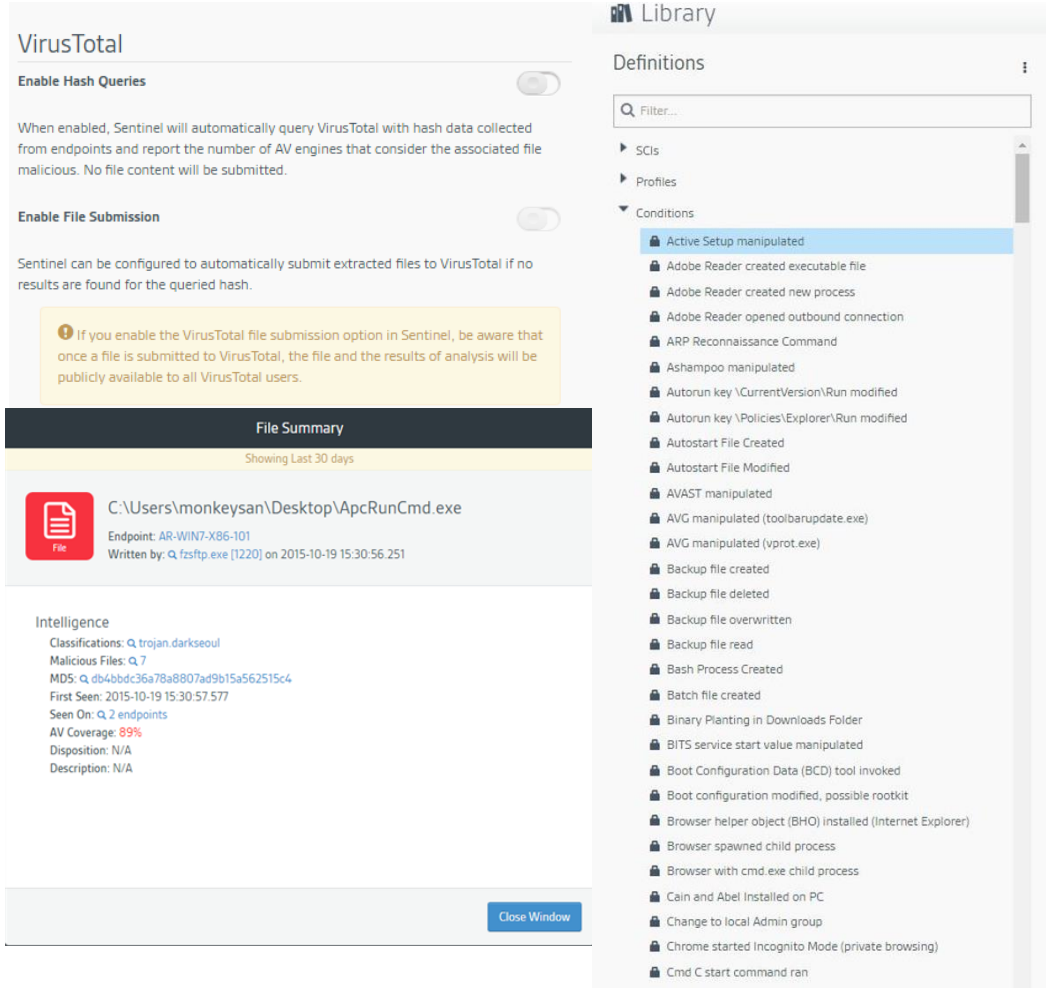
CounterTack

SK인포섹㈜

ETP의 위협행위 분류체계 (TAXONOMY)

- ❖ 엔드포인트의 행위이벤트에 대한 위협조건을 10가지로 카테고리화 하였으며, 세분화된 탐지조건으로 구성
- ❖ 이벤트에 대한 Impact score , 웹기반 백신(Virus Total)과의 연동을 통한 신속한 유해성 판단이 가능
- ❖ 침해정보(IOC)는 CybOX 표준을 이용하여 공유하거나 재사용이 가능



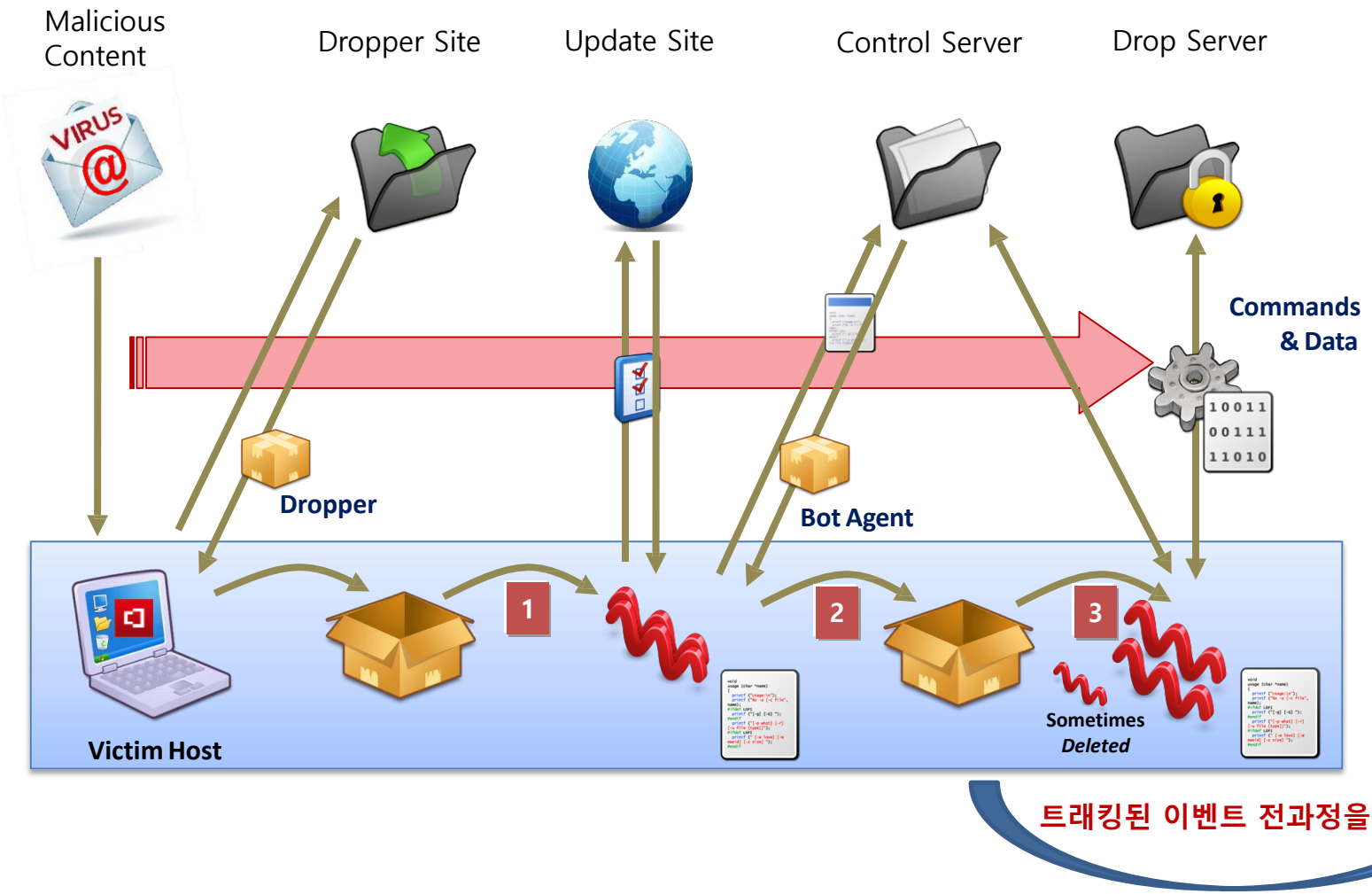


CounterTack

SK인포섹㈜

엔드포인트단 악성행위 탐지와 동시에 추적기능이 작동

❖ 엔드포인트단에서의 '초기감염→ 확산 → 제어권확보 → 정보유출'의 단계중 초기 감염단계 활동부터 탐지가 가능



1 2 백그라운드로 임의의 파일설치 행위 탐지

✓ Dropper나 Bot Agent가 설치되는 이벤트 발생시 악성행위로 간주하여 자동으로 트래킹 진행

3 MBR접근시도, 해쉬값변경등의 행위 탐지

✓ 악성코드 동작시 유해 행위에 해당되는 조건에 부합되는경우 자동으로 트래킹 진행

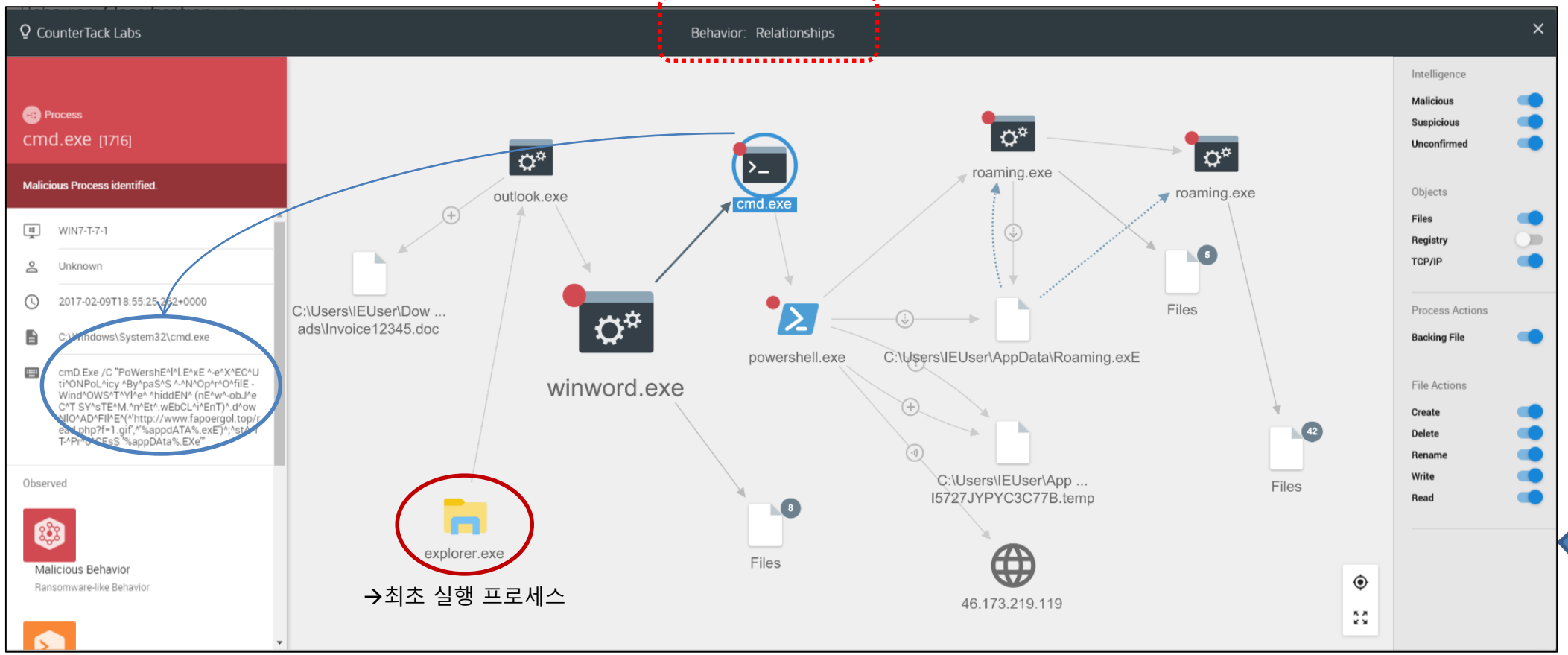
❖ 위협행위로 탐지시 연관행위 자동추적

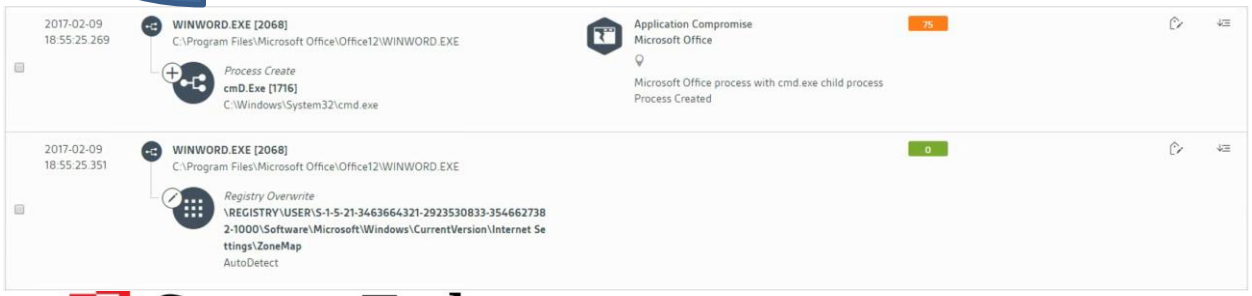
✓ 프로세스 이름 PID 및 프로세스 이미지 경로
✓ 삭제되거나 변경된 파일 및 레지스트리 정보
✓ 사용자 계정 및 사용자의 SID
✓ 전과정에 대한 Relation Graph제공

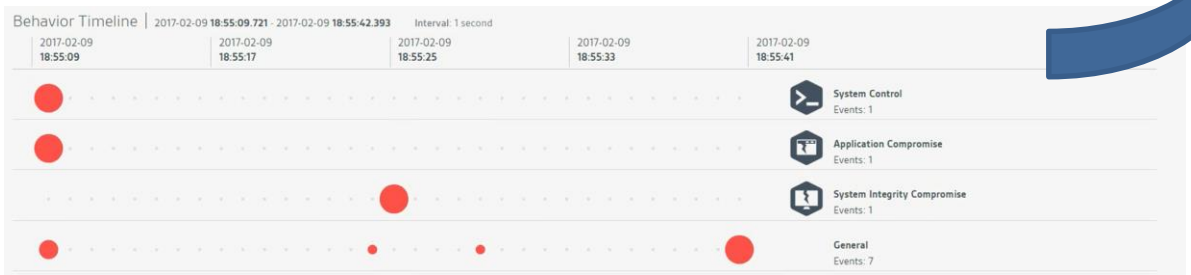
CounterTack

SK인포섹㈜

악성행위에 대한 단계별 시각화 기능으로 신속한 판단 및 대응이 가능





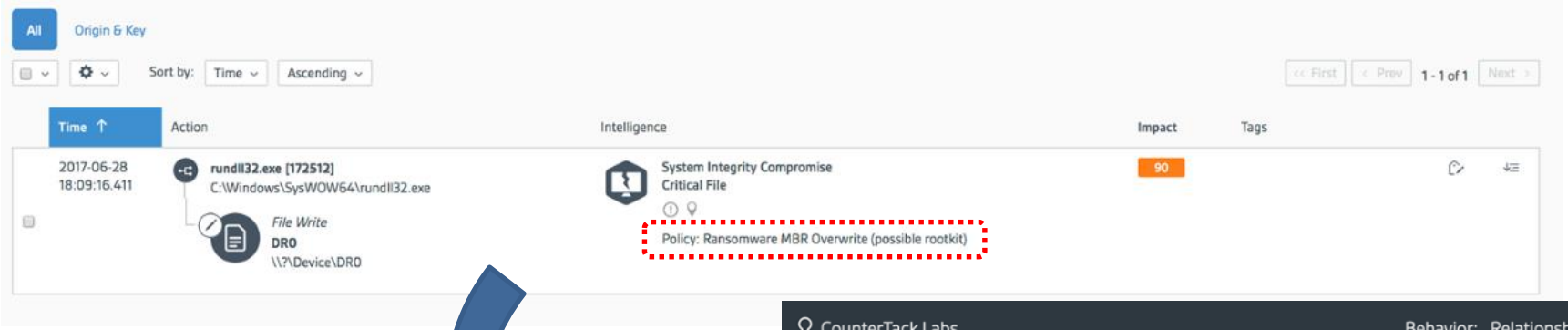


CounterTack

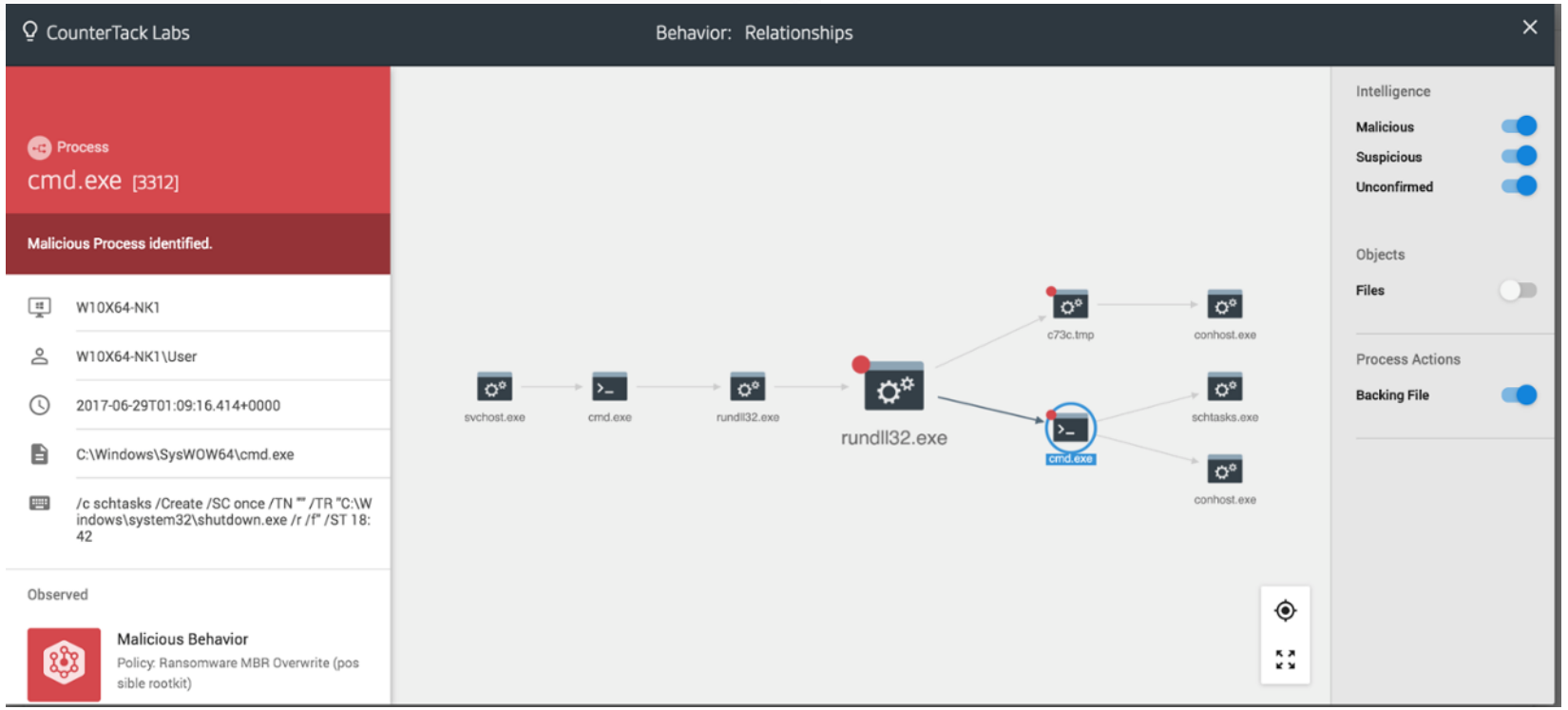
SK인포섹㈜

Ⅲ 고객사 침해사고 예시

CASE-1 백신이 나오지 않았던 랜썸웨어를 초기에 식별하여 차단



위협이벤트 탐지정책인
'랜썸웨어 MBR 덮어쓰기'
조건에 의해 탐지되어 분석된
랜썸웨어(NetPetya)



✓ **가시성을 통한 위협요소 판단근거**

① rundll32.exe 의한 MBR영역 이벤트 확인

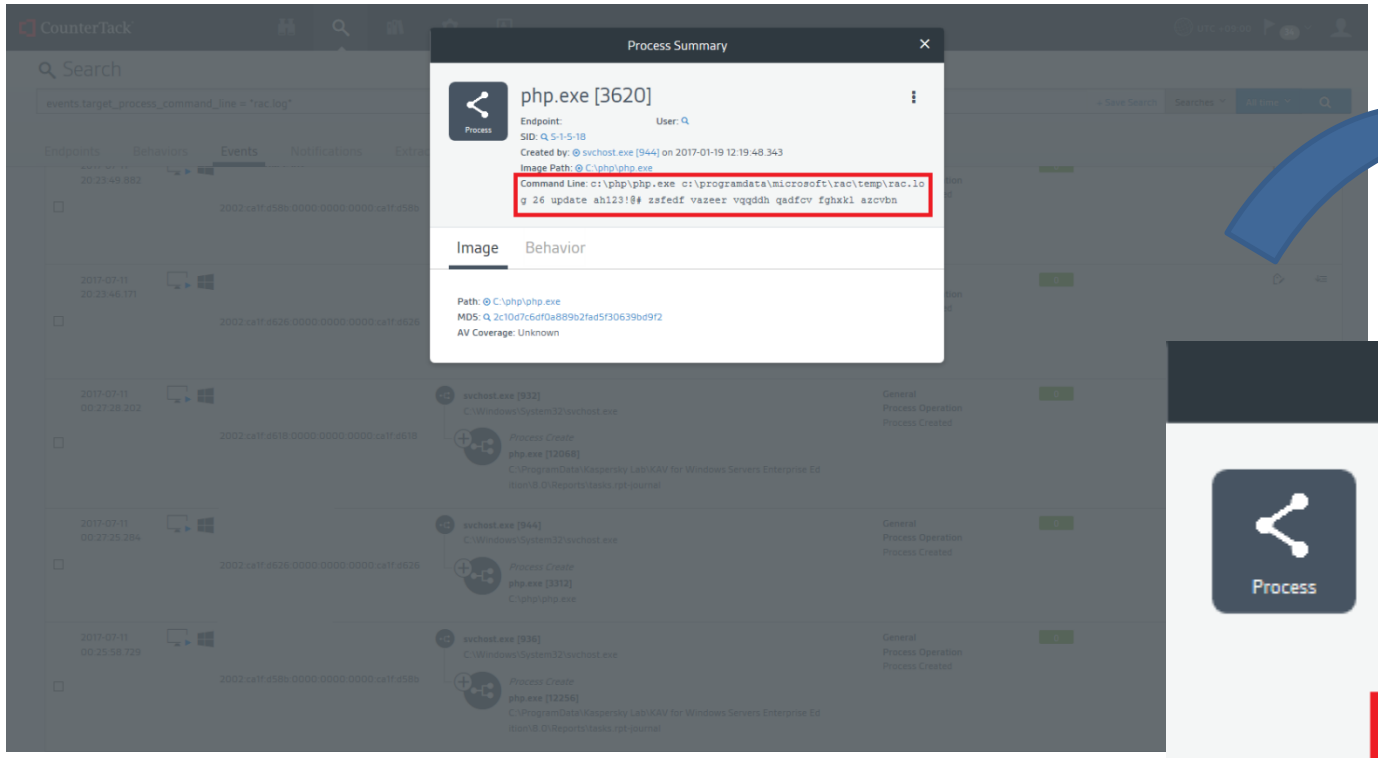
② 하위프로세스로 실행된 cmd.exe를 이용,
스케줄러에 시스템 강제종료 및 리부팅 명령 등록

③ c73c.tmp파일을 생성하여 반복복제

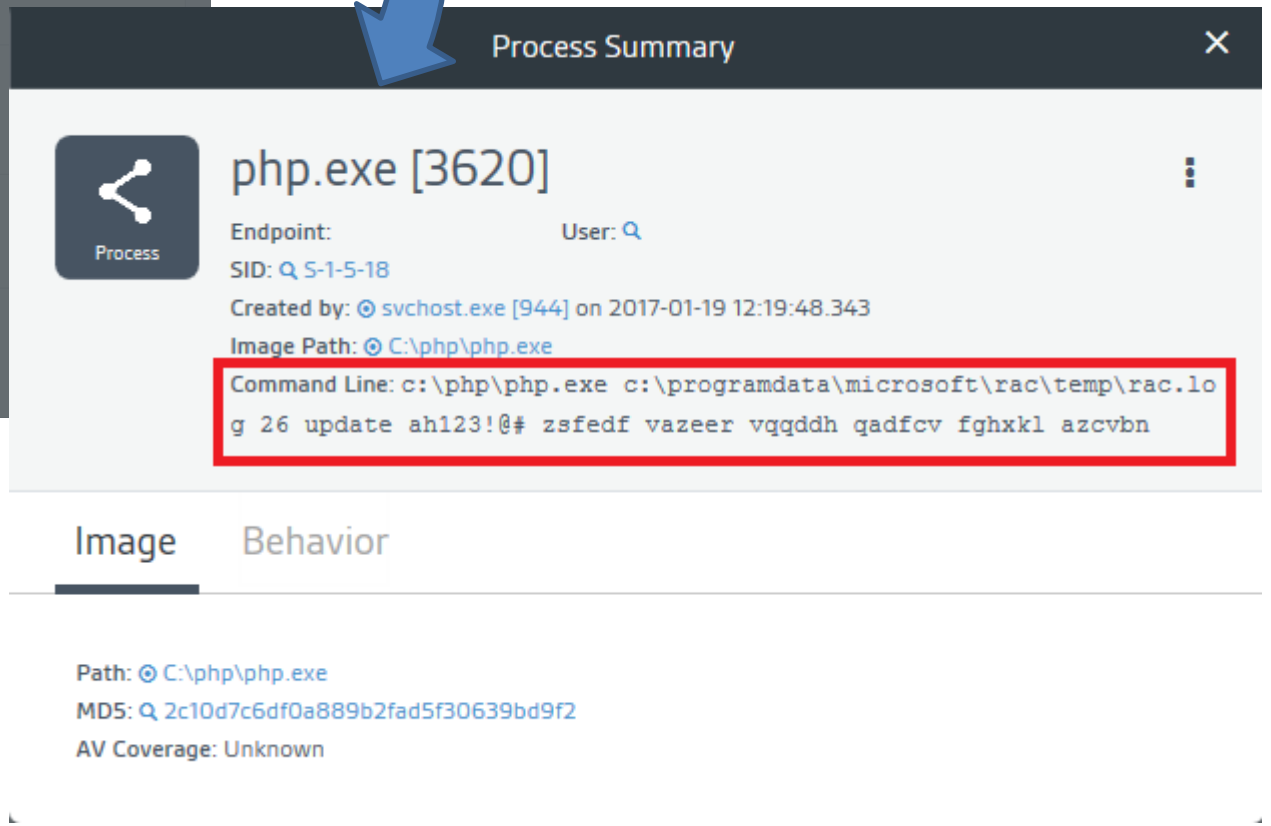
CounterTack

SK인포섹㈜

CASE-2 DB서버를 장악하여 내부정보를 변조한 해킹툴 적발



DB update 쿼리문이 포함된 php code가
실행되어 탐지된 화면



✓ **가시성을 통한 위협요소 판단근거**

① 커맨드명령에서 진행되는 Update 쿼리문을 탐지조건에 등록

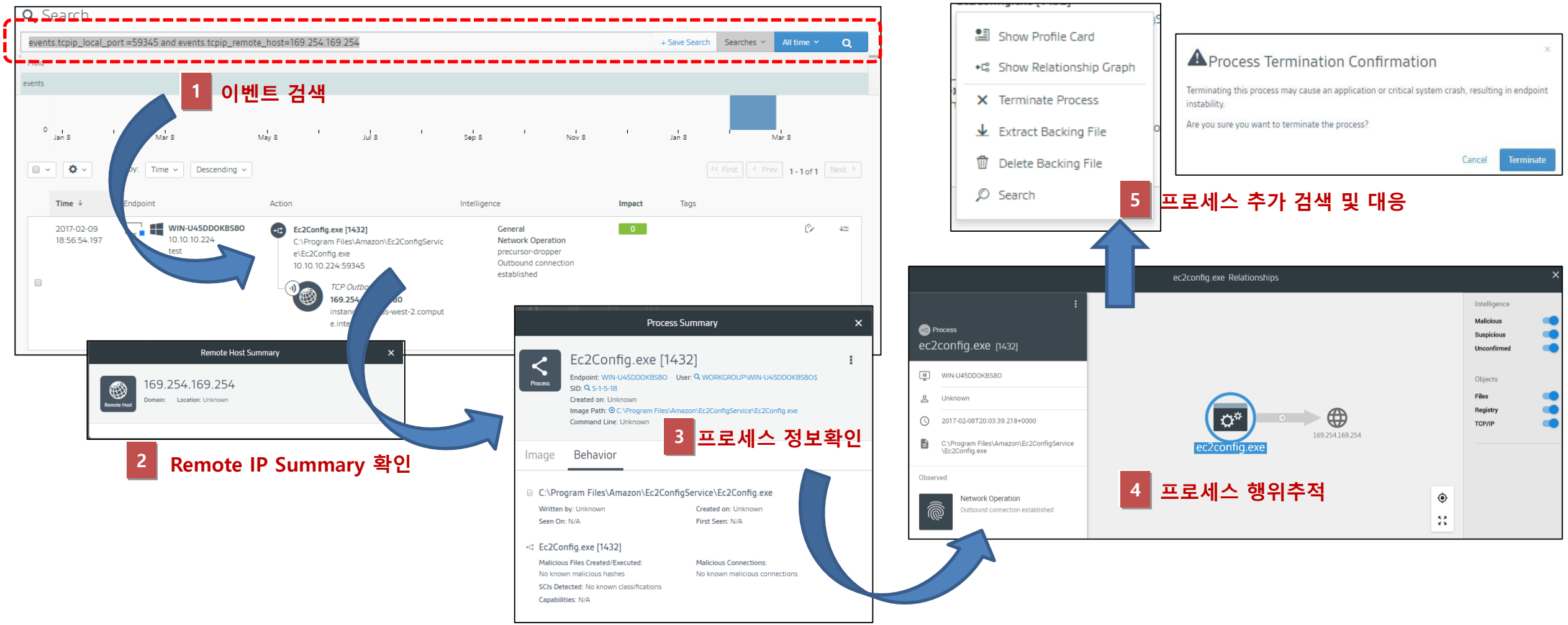
② 임의로 실행된 php.exe에 의한 update문 실행이벤트 기록 확인

CounterTack

SK인포섹㈜

CASE-3 외부 정보유출이 의심되는 엔드포인트를 검색하여 차단

❖ 검색조건에서 Local Port및 Remote IP를 지정하여 프로세스를 조회, 가시성을 통한 판단 및 대응



CounterTack

SK인포섹㈜

IV 하드웨어 및 소프트웨어 구성

SK 인포섹

대규모 데이터세트 분석에 적합한 Hadoop 기반의 엔진

❑ Big Data Analytics 기술 적용

- ❖ Hadoop 관련 전문 기술을 보유한 Cloudera Big Data 엔진 적용
- ❖ open source 사용으로 인한 TCO절감
- ❖ 대규모 데이터의 수집, 저장 및 운영에 대한 검증된 플랫폼 제공
- ❖ 강력한 검색을 기능을 통한 Enterprise threat correlation 지원
- ❖ Impala, HUE, HBASE 등의 내장된 Query를 사용

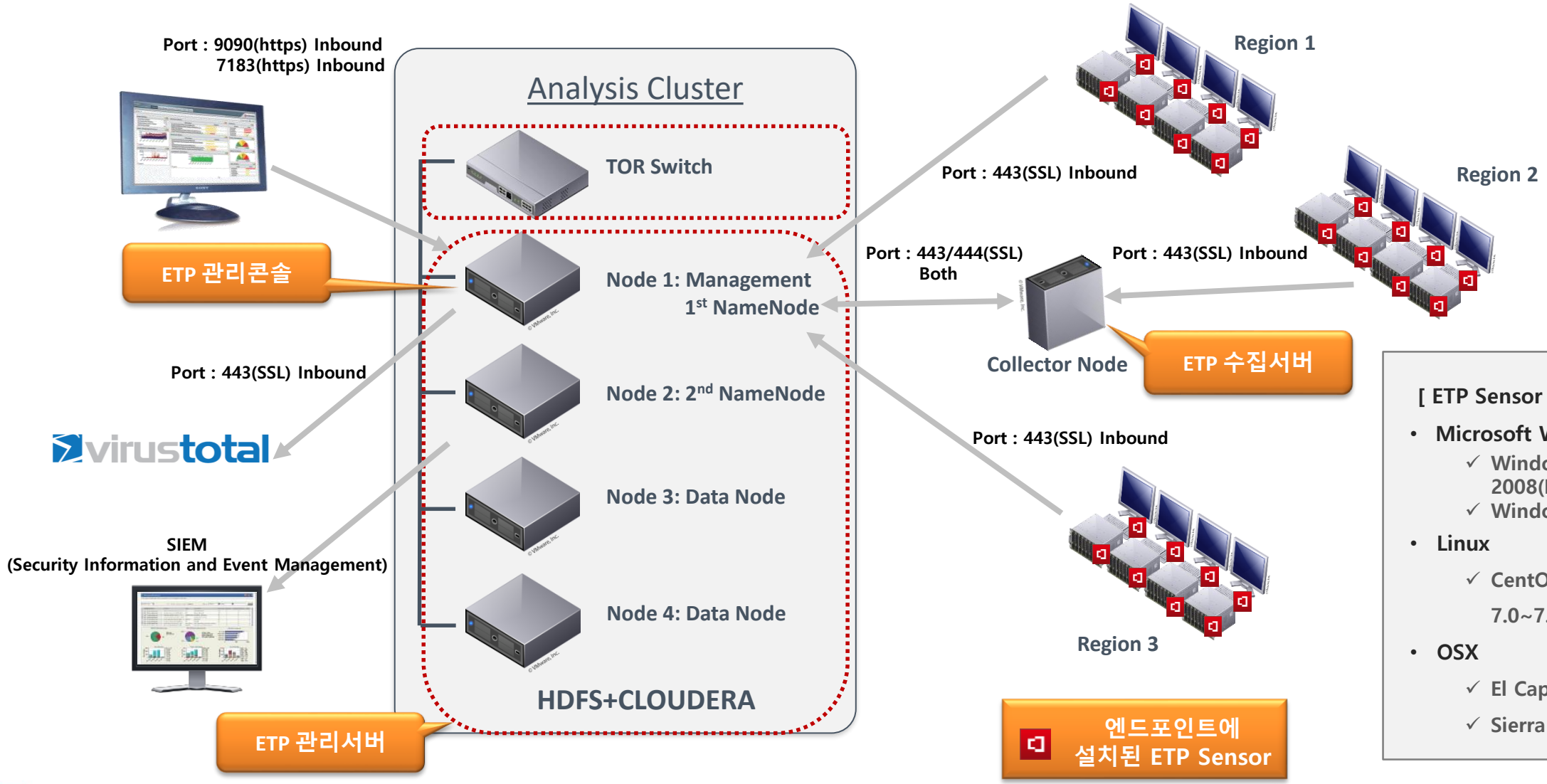
❑ 유연한 구축 확장성

- ❖ 기본 Cluster 당 최대 10,000 개의 Endpoint를 수용
- ❖ 데이터 노드의 추가 만으로 증가하는 엔드포인트 운영이 가능
- ❖ 다양한 네트워크 구성에 대응할 수 있는 유연한 아키텍쳐 제공
  (Multi-tier Flume configuration, DMZ configuration)

CounterTack

SK인포섹㈜

엔드포인트에 설치되는 센서, 독립망을 위한 수집서버, 정책설정을 위한 관리서버로 구성



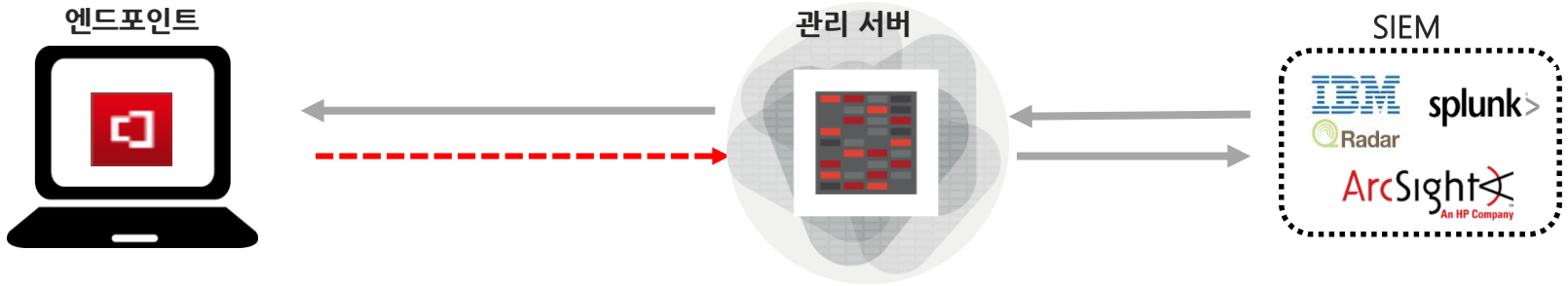
[ETP Sensor 설치가능 OS]

- Microsoft Windows
  - ✓ Windows Server 2008(R2), 2012(R2)
  - ✓ Windows 7/8.1/10
- Linux
  - ✓ CentOS/RHEL 6.8, 7.0~7.2
- OSX
  - ✓ El Capitan
  - ✓ Sierra

CounterTack

SK인포섹㈜

ETP는 정보수집을 위한 Conditions 및 Profiles, 분석을 위한 SCIs, Digital DNA 모듈로 구성



SENSOR 구성요소

수집 조건 (Conditions)

- File Activity
- Process Activity
- Network Activity
- Registry Activity

프로파일 (Profiles)

- 수집조건(Condition) 집합
- 에이전트의 이벤트 수집 룰

ETP 서버 구성요소

위협 분류 (SCIs)

CybOX

- 행위기반 위험분류체계
- IOC 추가 및 편집
  (Auto Remediation)

Virus Total

virustotal

- 실행파일 Hash 질의
- 실행 파일 전송

HashSet/IP

REST API

- Known Good Hash/IP
- Known Bad Hash/IP
  (Auto Remediation)

Digital DNA

- 메모리 분석을 통한
  위험예측 분석

CounterTack

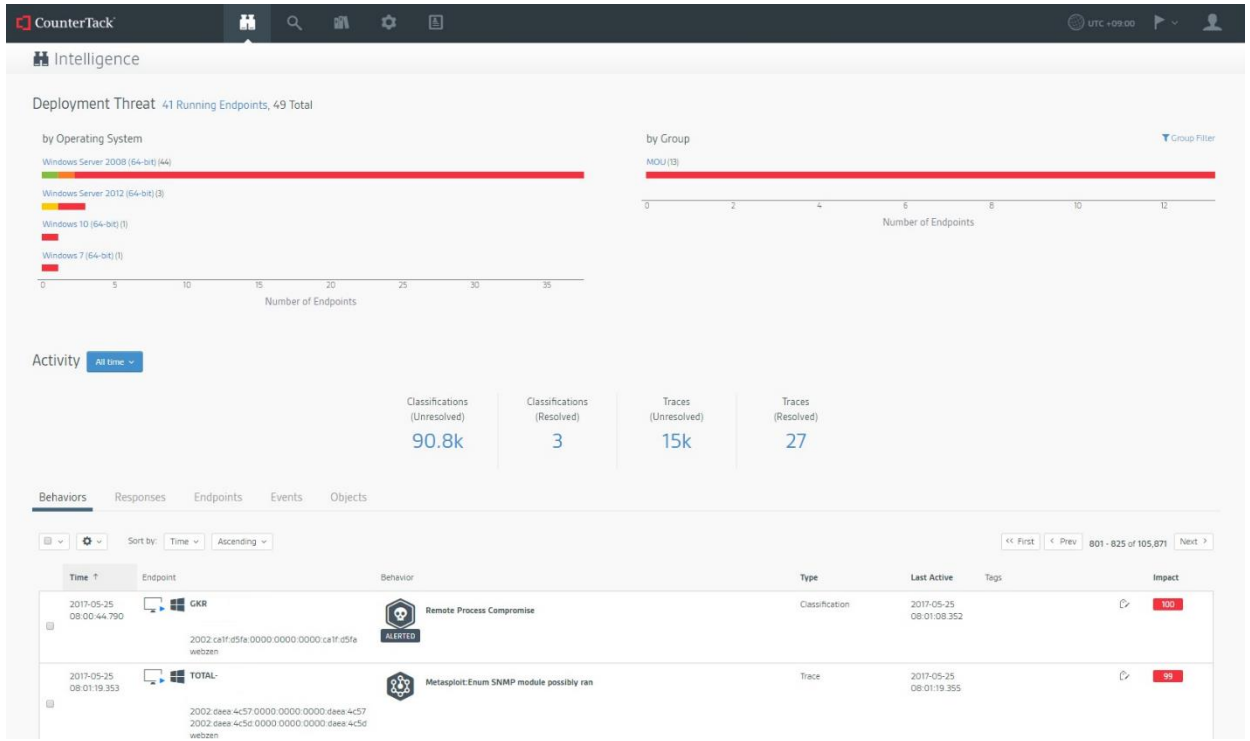
SK인포섹㈜

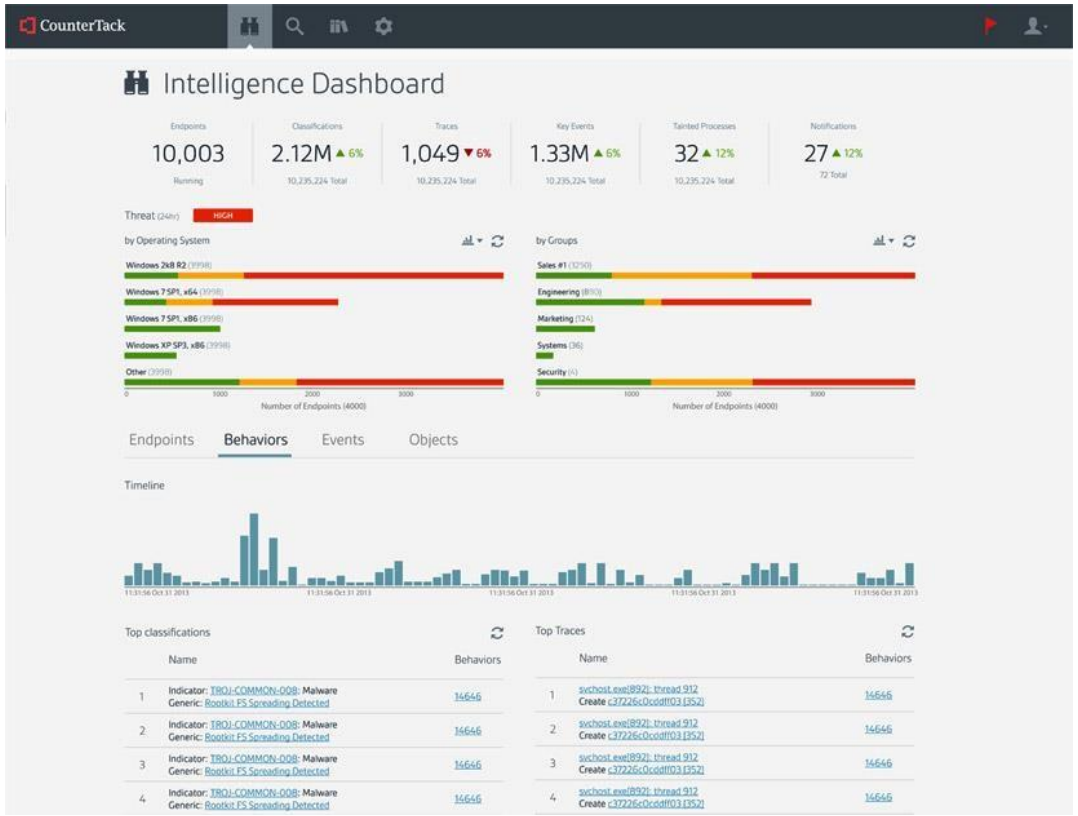
V 관리콘솔 화면

악성행위들에 대한 탐지결과 및 엔드포인트 현황의 실시간 확인

❑ Intelligence (Dashboard)

- 탐지대상인 Classification, Trace에 대한 실시간 정보 확인
- 엔드포인트의 OS 정보, Behaviors, Events에 대한 상세정보 실시간 확인
- 리포트 가공을 위한 파일추출 및 컨버팅 기능 제공
- 타임라인을 기반으로하여 특정시간에 발생한 이벤트 추적에 용이





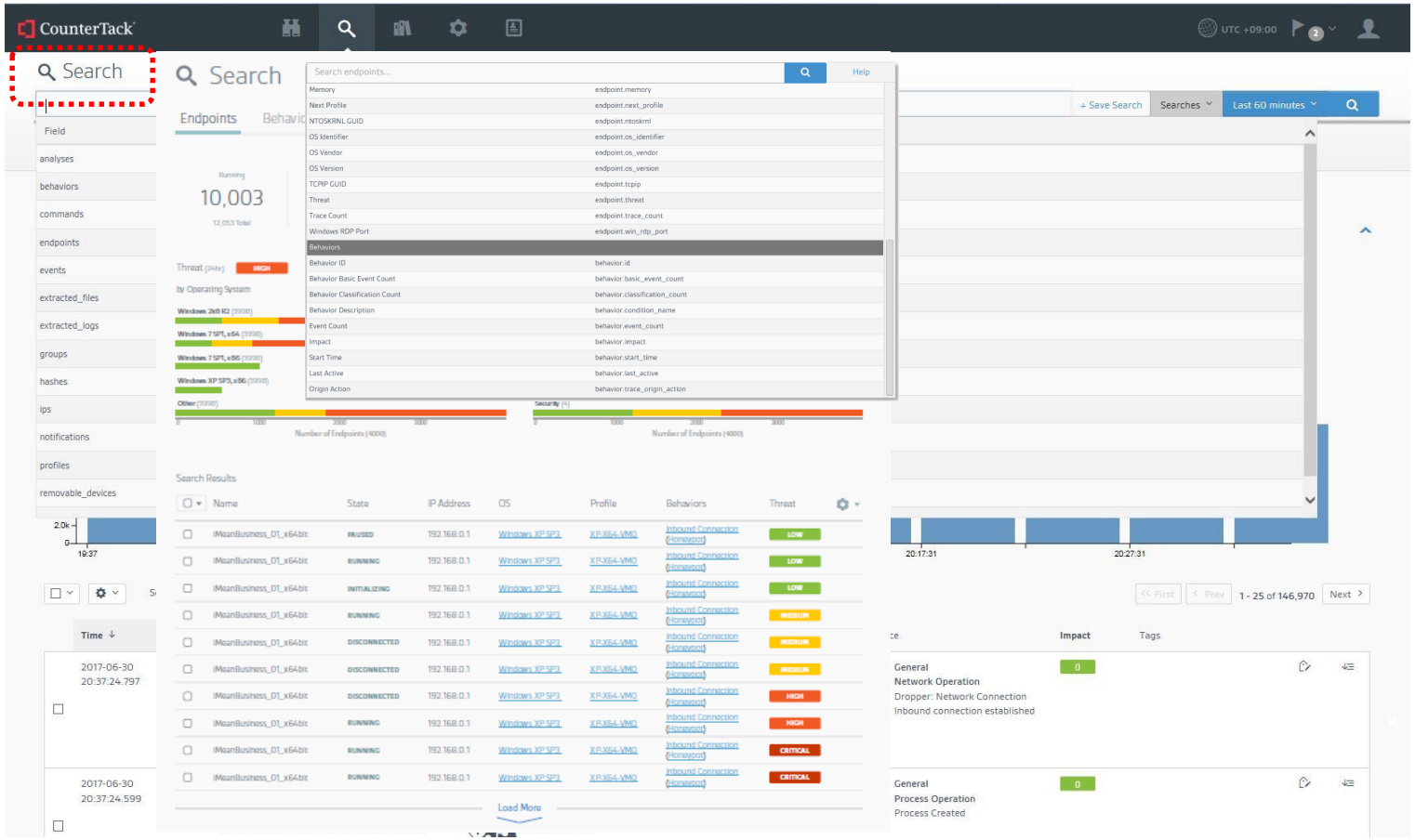
CounterTack

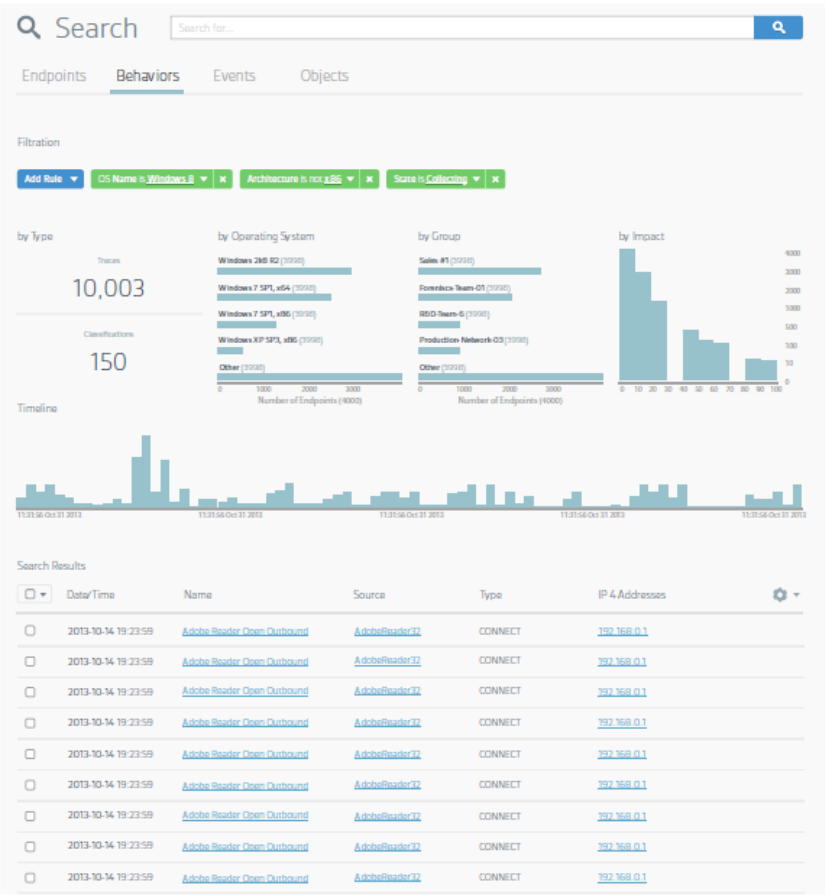
SK인포섹㈜

조건 검색결과에 따른 다양한 연관검색 기능 제공

❑ Search

- 분류조건에 따른 검색 및 예외 필터링 설정이 가능
- Events, Behavios, Profiles 등에 다양한 검색 기능 제공
- AND연산자 및 TimeLine 필터를 통한 상관관계 분석 가능





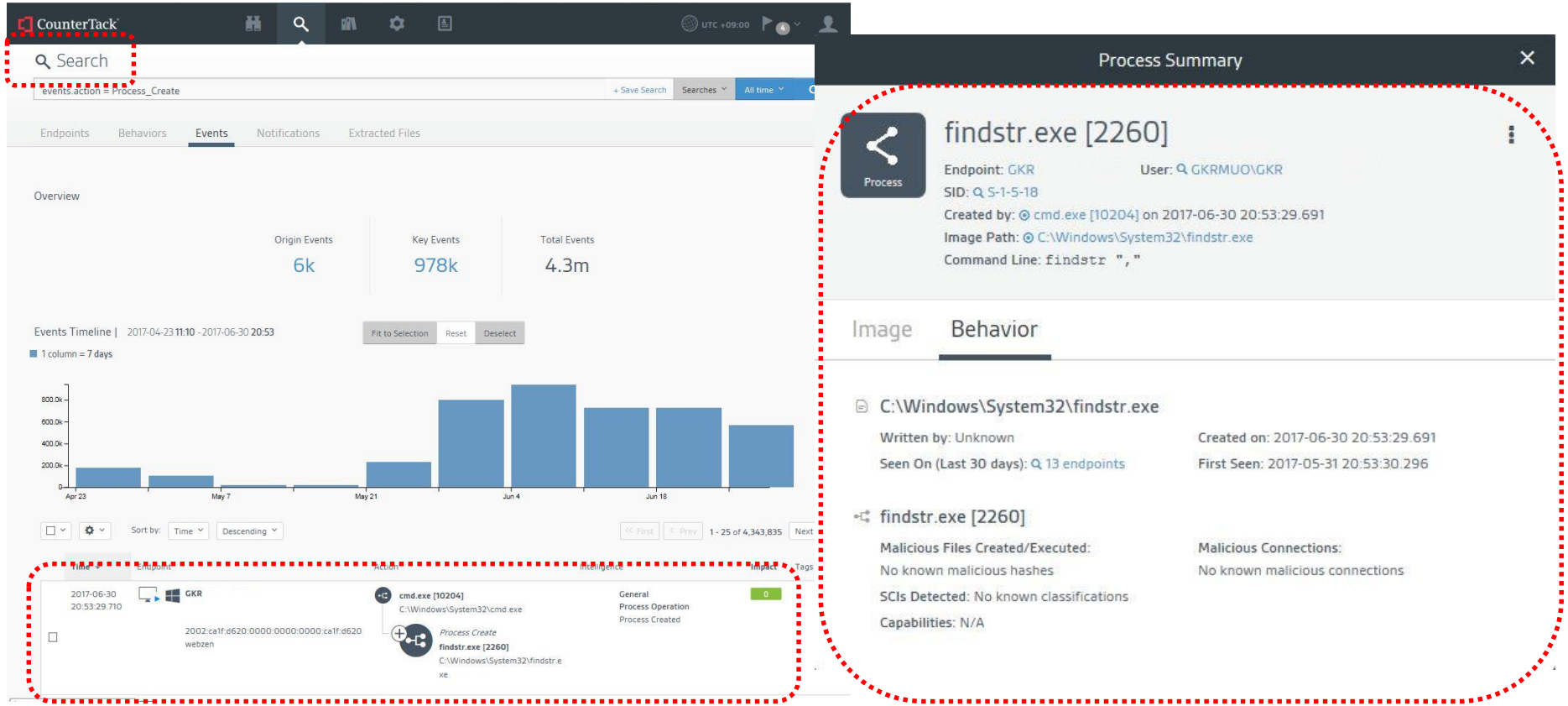
CounterTack

SK인포섹㈜

메모리 포렌식 기반 모듈 탑재로 악성코드에 대한 상세 분석 가능

❑ Search

- 특정 행위에 대한 상세 분석 결과 확인 가능
- Process, File, Network, Registry 등 행위에 대한 세부정보 제공
- 세부정보 확인을 통해 악성행위 여부 판단하여 네트워크 격리 등의 조치 가능



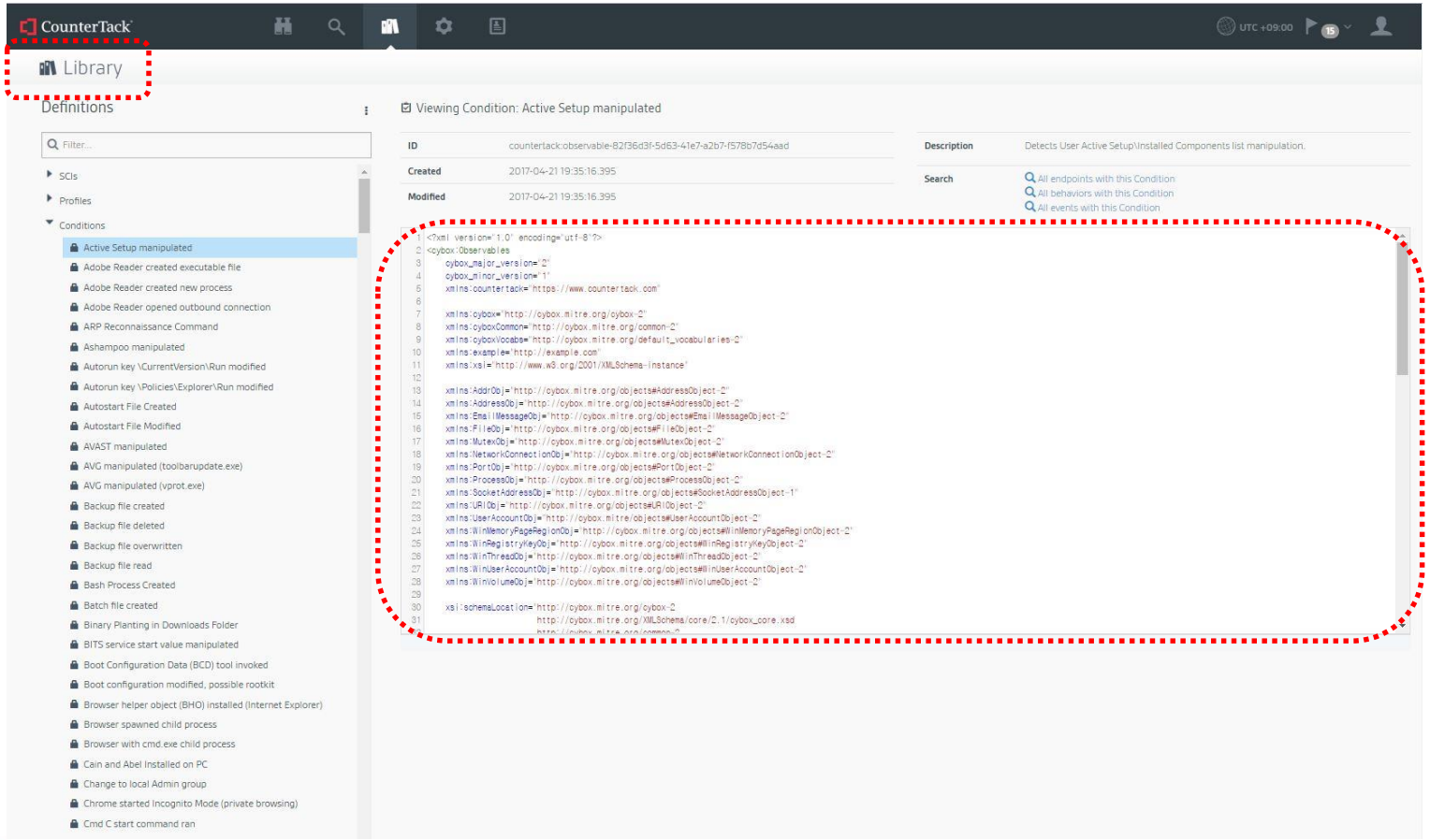
CounterTack

SK인포섹㈜

효율적인 수집분석을 위한 다양한 예외처리 및 정책 커스터마이징 가능

Library

- SCIs, Profiles, Conditions 등의 수집 및 분석 룰에 대한 편집이 가능 (Cybox 정규표현식 사용)
- 이벤트에 대한 예외처리 및 심화분석을 위한 레벨설정이 가능
- 알려진 위협에 대응하기 위한 다양한 Profile 및 Condition 기본 제공
- 위협 구분에 따른 자동 분류기능 제공



CounterTack

SK인포섹㈜

VI 레퍼런스

SK 인포섹

ETP 운영 및 관제 통합서비스 제공

- ❖ 고객사 엔드포인트 환경에 대한 보안컨설팅 및 사전조사
- ❖ 침해사고 분석을 위한 증거 데이터 확보
- ❖ 신속한 악성코드 판단 및 보안정책 적용
- ❖ 기존 보안시스템과 연계 운영을 통한 사고 대응 프로세스 강화

현황파악/환경설정	탐지 정책 최적화	악성코드 탐지/분석	악성코드 조치	보고/개선
• 고객 요구사항 분석 • 에이전트/분석서버 설치 & 연동 (장비 구축시) • 보안관제협의 – 연락/대응프로세스	• 스텔스 모드에서 악성 행위 정보 수집 • 탐지 정책 최적화 – 수집 정책, SCI, Bad Hash 등	• 행위 기반 이벤트 분석 – Process, File, Registry, Network • 분석 후 위협 판단 – SCI, VirusTotal, Auto Remediation, Bad hash IP	• 악성코드 유포 URL 및 C&C 차단 • 백신패턴 개발 요청 (고객사 백신 미탐지시) • 감염 PC에 대한 방역 가이드	• 침해위협발생보고서 • 정기보고서 • 악성코드 유포 URL 제공

ETP 운영 고객사

- 2015년부터 금융, 군수, 건설, 통신, IT분야 해외 레퍼런스 보유
- 2017년부터 국내 레퍼런스 보유

국내

kakao

SK 주식회사 C&C

WEBZEN

금융

WELLS FARGO

DBS

ZURICH

AIG

Deloitte.

citi

MAGNETAR CAPITAL

Close Brothers

jack henry Banking
A DIVISION OF JACK HENRY & ASSOCIATES INC®

Digital River

군수, 건설

BAE SYSTEMS

Battelle
The Business of Innovation

BECHTEL

accenture

SIEMENS

통신, IT

Bell

BT

Alcatel·Lucent

CISCO

Adobe

HARVARD

IQT
IN·Q·TEL