CARBON BLACK
ARM YOUR ENDPOINTS

INSEC security

Carbon Black Enterprise

제품 소개 자료

2016

㈜인섹시큐리티

Copyright INSEC Co.,Ldt. All Rights Reserved.

최근 악성코드 동향

TeslaCrypt 변종 – 파일 확장자를 ‘mp3’로 바꾸는 랜섬웨어

파일 확장자 `mp3`로 바꾸는 랜섬웨어 등장… 이중 프로세스로 탐지 우회

[AD] [3/23] 지능형 서비스로봇 기술,시장 최신분석 및 적용사례와 상용화 세미나

파일 확장자를 ‘.mp3’로 바꾸는 랜섬웨어가 국내에 등장했다. 지난해 유포돼 확장자를 ‘.micro’로 변경하는 테슬라크립트(TeslaCrypt) 변종이다. 이중 프로세스로 동작으로 보안제품에 적용된 행위기반 탐지 일부 기능을 회피한다. 올 들어 랜섬웨어 피해가 다소 줄었지만 다양한 변종이 등장해 주의가 요구된다.

<파일 확장자를 ‘.mp3’로 바꾸는 랜섬웨어가 등장했다.ⓒ게티이미지뱅크>

보안 업계에 따르면 확장자를 mp3로 바꾸는 랜섬웨어는 설 연휴 직후인 지난 11일경부터 국내피해사례가 보고됐다. 온라인 커뮤니티와 네이버 지식인 서비스 등에도 관련 문의가 올라왔다.

Copyright INSEC Co.,Ldt. All Rights Reserved.

최근 악성코드 동향

KeRanger – 3일 동안 잠복 후 데이터를 암호화하여 금전을 요구하는 랜섬웨어

Copyright INSEC Co.,Ldt. All Rights Reserved.

최근 악성코드 동향

Locky – 기본적으로 파일을 암호화하고, 네트워크에 공유된 데이터까지 암호화를 수행하는 랜섬웨어

또 새 랜섬웨어! 단일 시스템뿐 아니라 네트워크도 침입

입력날짜 : 2016-02-19 11:55 스크랩 프린트하기 목록

좋아요 63 트윗

최근 랜섬웨어의 트렌드 : 파일이름 바꾸기, 네트워크 넘나들기
랜섬웨어 해커들에 돈을 주는 건 공격자들을 후원하는 꼴

[보안뉴스 문가용] 이제 귀에 못이 박힐 정도로 지겨울 수 있지만, 어쩔 수 없다. 새로운 랜섬웨어가 또 다시 등장했다. 이번에 등장한 랜섬웨어의 이름은 록키(Locky)로 이를 처음 발견한 건 영국의 보안 전문가인 케빈 뷰몬트(Kevin Beaumont)다. 그에 따르면 록키 랜섬웨어는 1시간의 4000대의 기기를 감염시키는 속도로 퍼져가는 중이라고 한다.

▲ 말 그대로 우후죽순 피어나는 랜섬웨어들

Copyright INSEC Co.,Ldt. All Rights Reserved.

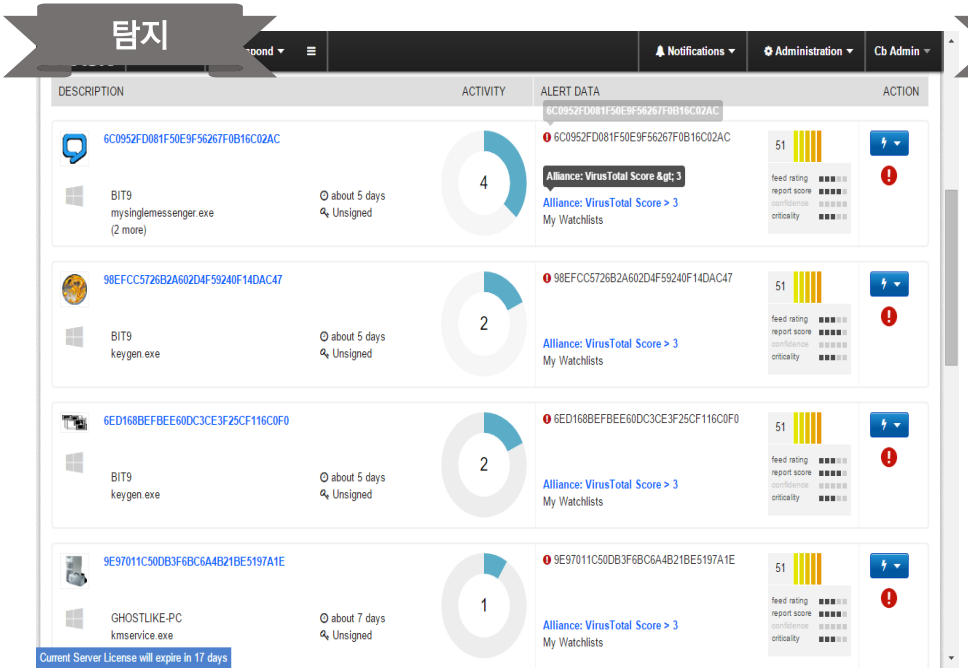
Instructions

Carbon Black Enterprise Response

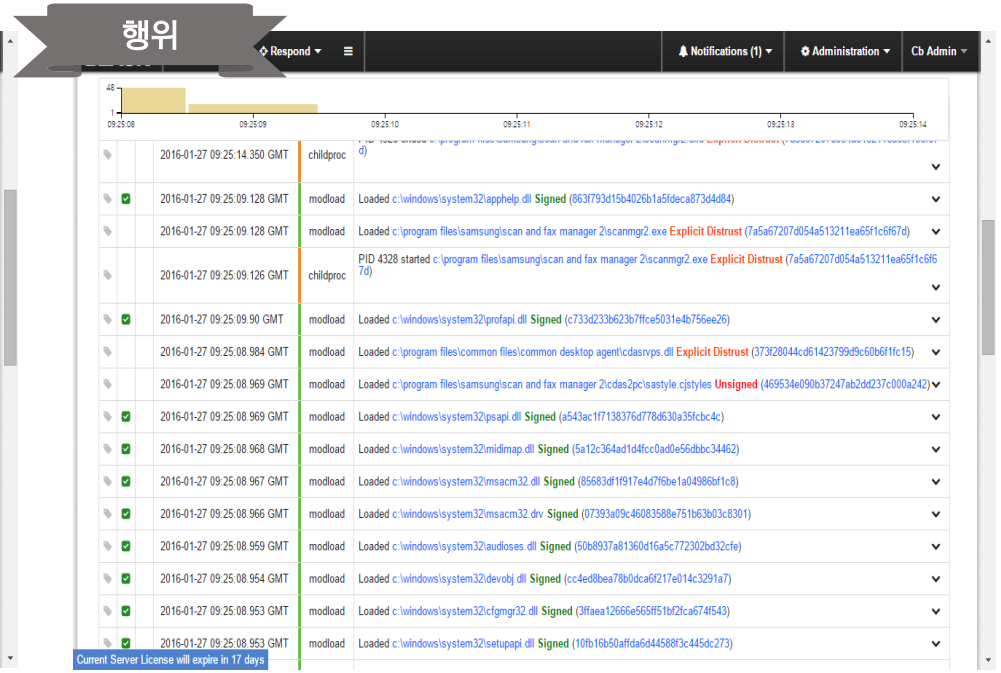
최신 사이버 위협 및 악성코드 탐지 / 실시간 침해사고 대응 솔루션

Carbon Black은 Carbon Black 전용 에이전트를 통하여 엔드포인트에서 일어나는 모든 프로세스의 행위를 모니터링 및 추적하여 사이버 위협 또는 악성코드를 실시간으로 탐지하고, 신속하게 대응 가능한 솔루션 입니다.

탐지



행위



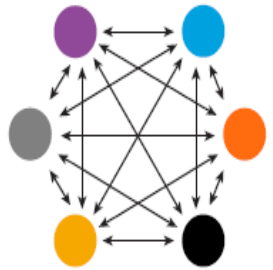
Copyright INSEC Co.,Ldt. All Rights Reserved.

Why Use?

Why you need Carbon Black ?

최근 보안 동향은 사이버 위협 및 악성코드 사전 차단과 사후 분석/탐지

Carbon Black은 실시간으로 발생되는 사이버 위협과 악성코드를 탐지하고 차단이 가능합니다.



Real Time

다양한 운영체제의
프로세스를 실시간으로 모니터링
및 추적, 기록
(Windows, Linux, Mac 지원)

Containment

악성 프로세스 탐지 시
버튼 하나로 확산 방지를 위해
위협 탐지 호스트 네트워크 차단

Alliance

다양한 글로벌 보안 업체와
위협 정보 공유 체계를 구축하여
Threat Intelligence 제공

Copyright INSEC Co.,Ldt. All Rights Reserved.

Feature (1)

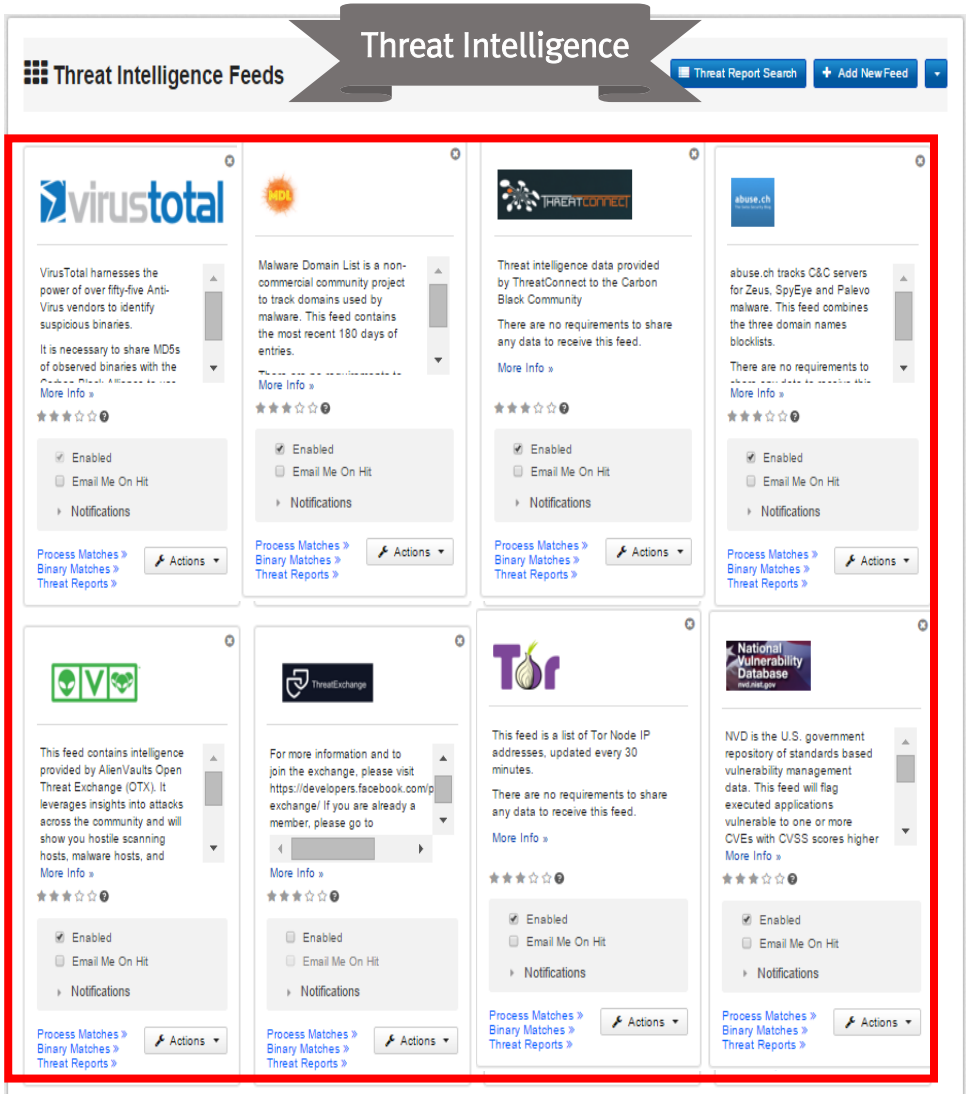
Threat Intelligence

Carbon Black에서 제공하는 악성코드 및
사이버 위협 정보 공유 연합

Carbon Black은 글로벌 보안업체들과 전략적 파트너십을 체결하여
최신 악성코드 및 위협들을 탐지하고 차단하는데 필요한
Threat Intelligence 서비스를 제공하고 있습니다.

주요 Alliance 구성원

VirusTotal, MDL, THREATCONNECT, abuse.ch,
AlienVaults, ThreatExcahnge, Tor, NVD 등



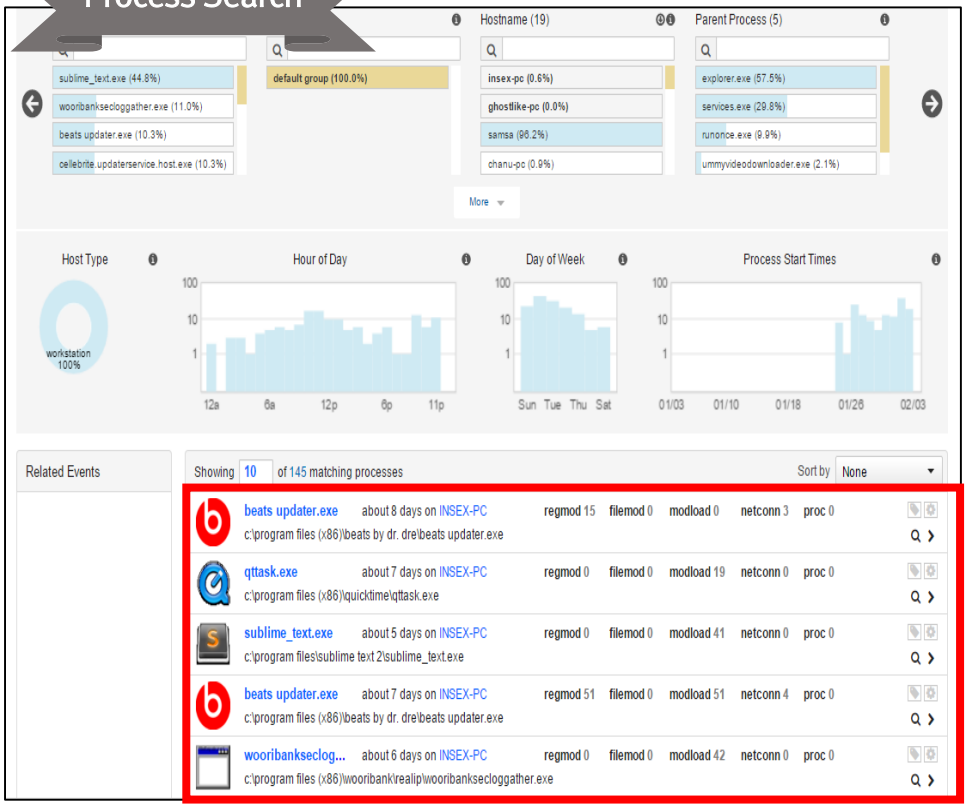
Copyright INSEC Co.,Ldt. All Rights Reserved.

Feature (2)

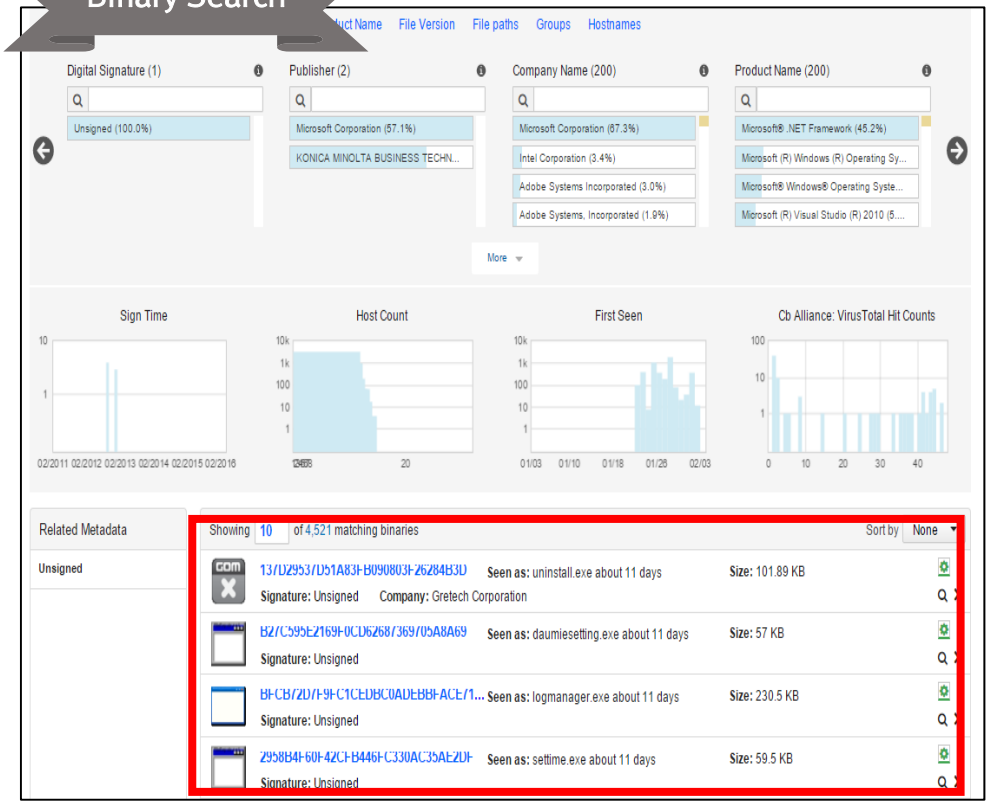
Endpoint Monitoring

지속적으로 모니터링하고 행위를 기록하여 침해사고 분석 시 필요한 아티팩트 정보를 제공합니다

Process Search



Binary Search



Copyright INSEC Co.,Ldt. All Rights Reserved.

Feature (3)

Process Analysis

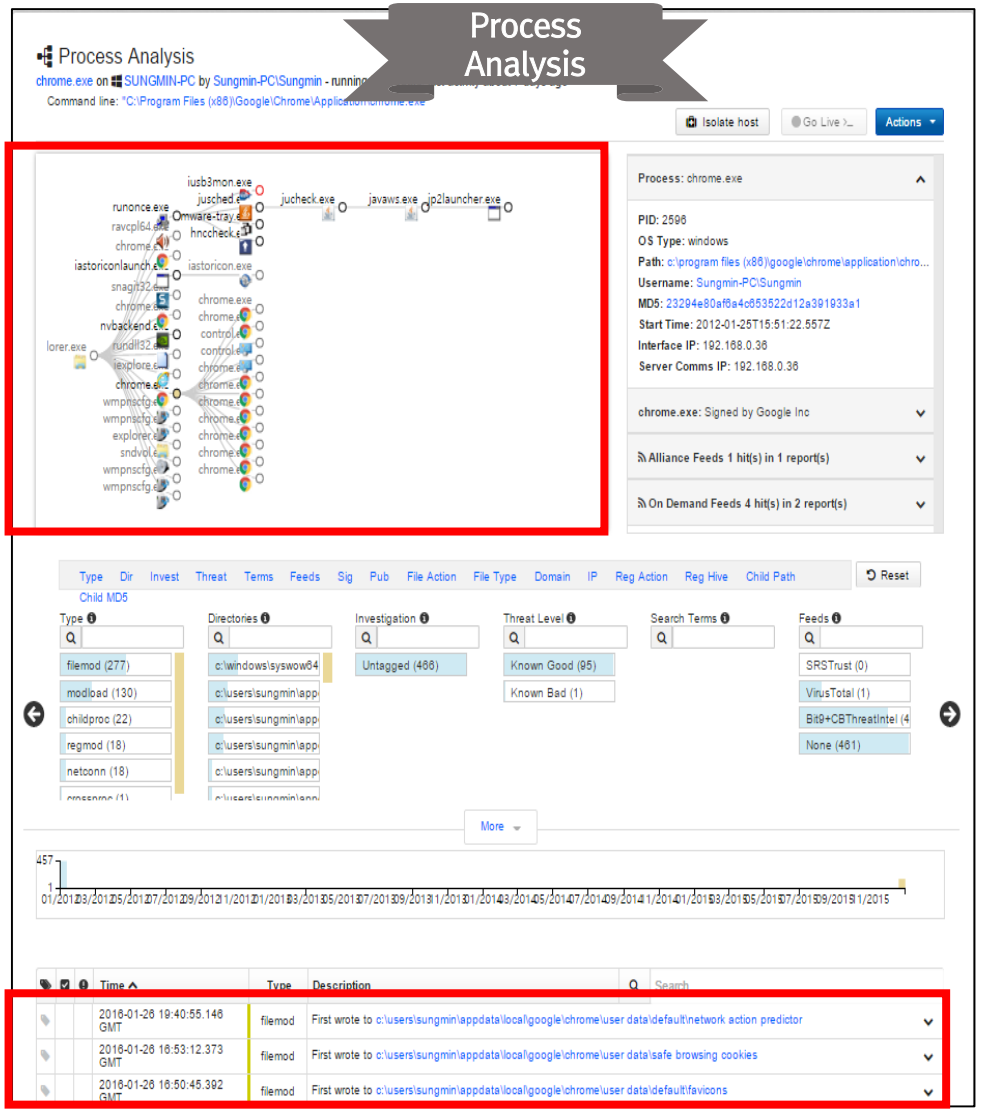
– 프로세스 트리 및 동작 흐름 확인

프로세스 트리로 부모 프로세스와 자식 프로세스를 확인 할 수 있으며, 해당 프로세스의 Threat Intelligence 와의 Match를 통해 악성 프로세스 정보 확인 가능

프로세스 활동 로그

Filemod, Regmod, Modload, netconn, block등 다양한 기준으로 활동 로그를 분류하여 상세한 프로세스 활동 기록 분석 가능

각 활동 로그 및 프로세스를 위협 정보 공유 연합인 Threat Intelligence의 정보와의 Match를 통해 악성 행위 판별 가능



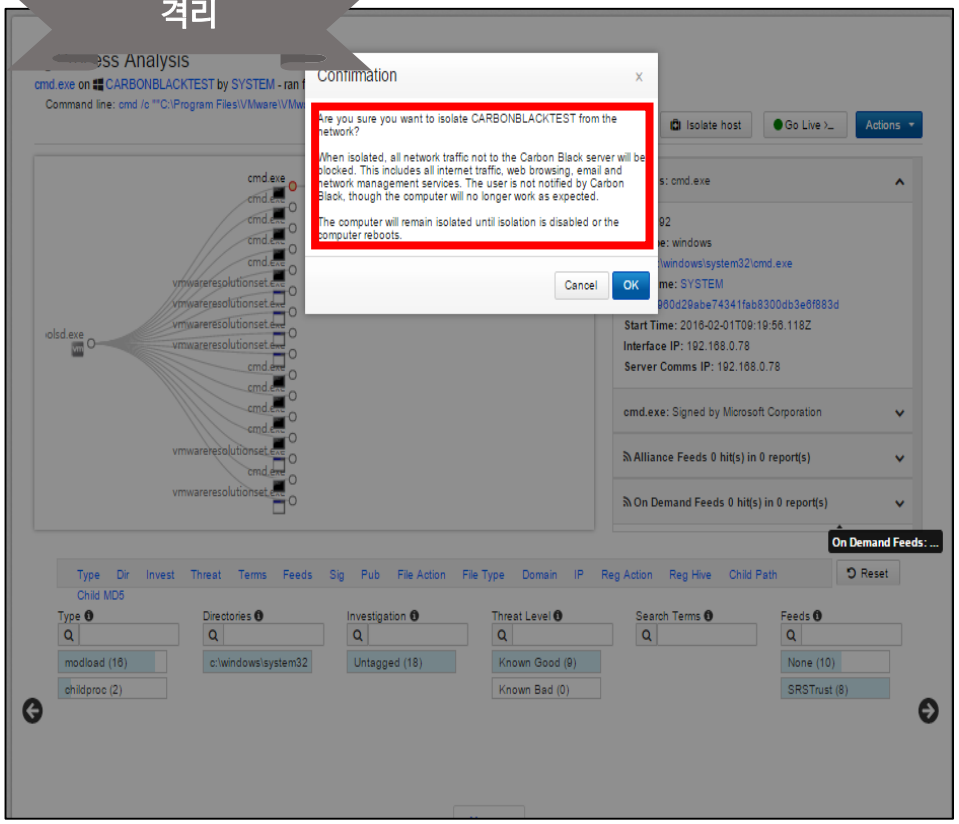
Copyright INSEC Co.,Ldt. All Rights Reserved.

Feature (4)

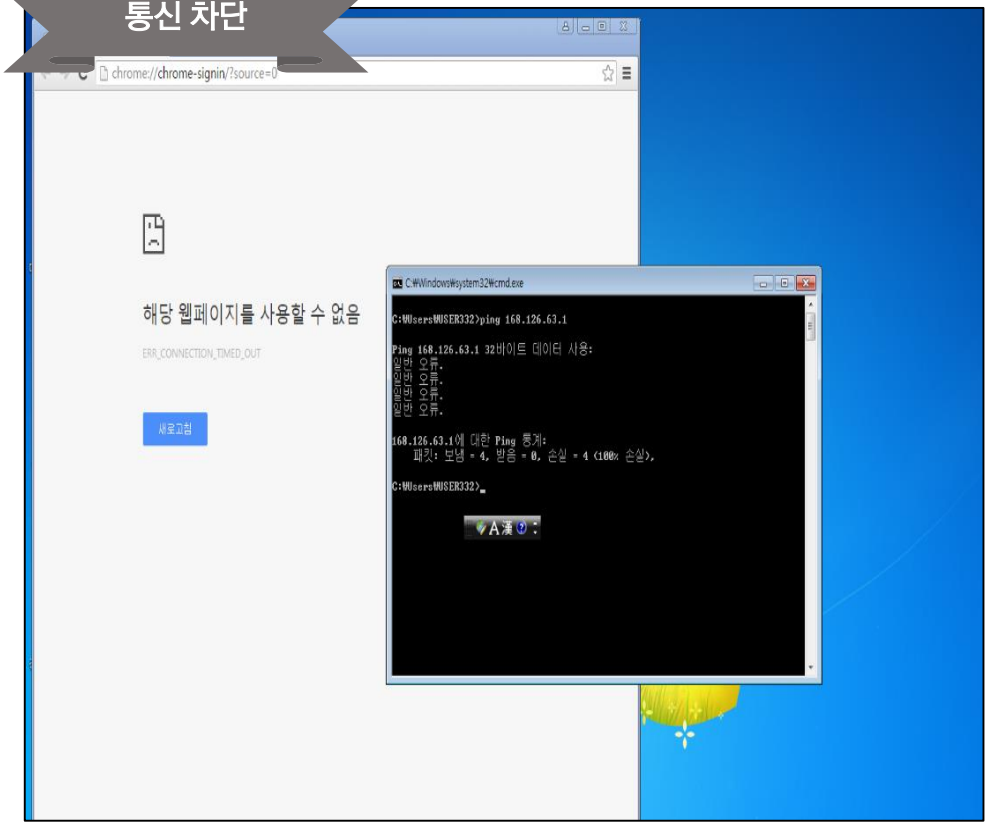
Isolate [호스트 네트워크 격리 기능]

격리 기능으로 카본블랙 서버와의 통신을 제외한 모든 네트워크 통신을 차단합니다

격리



통신 차단

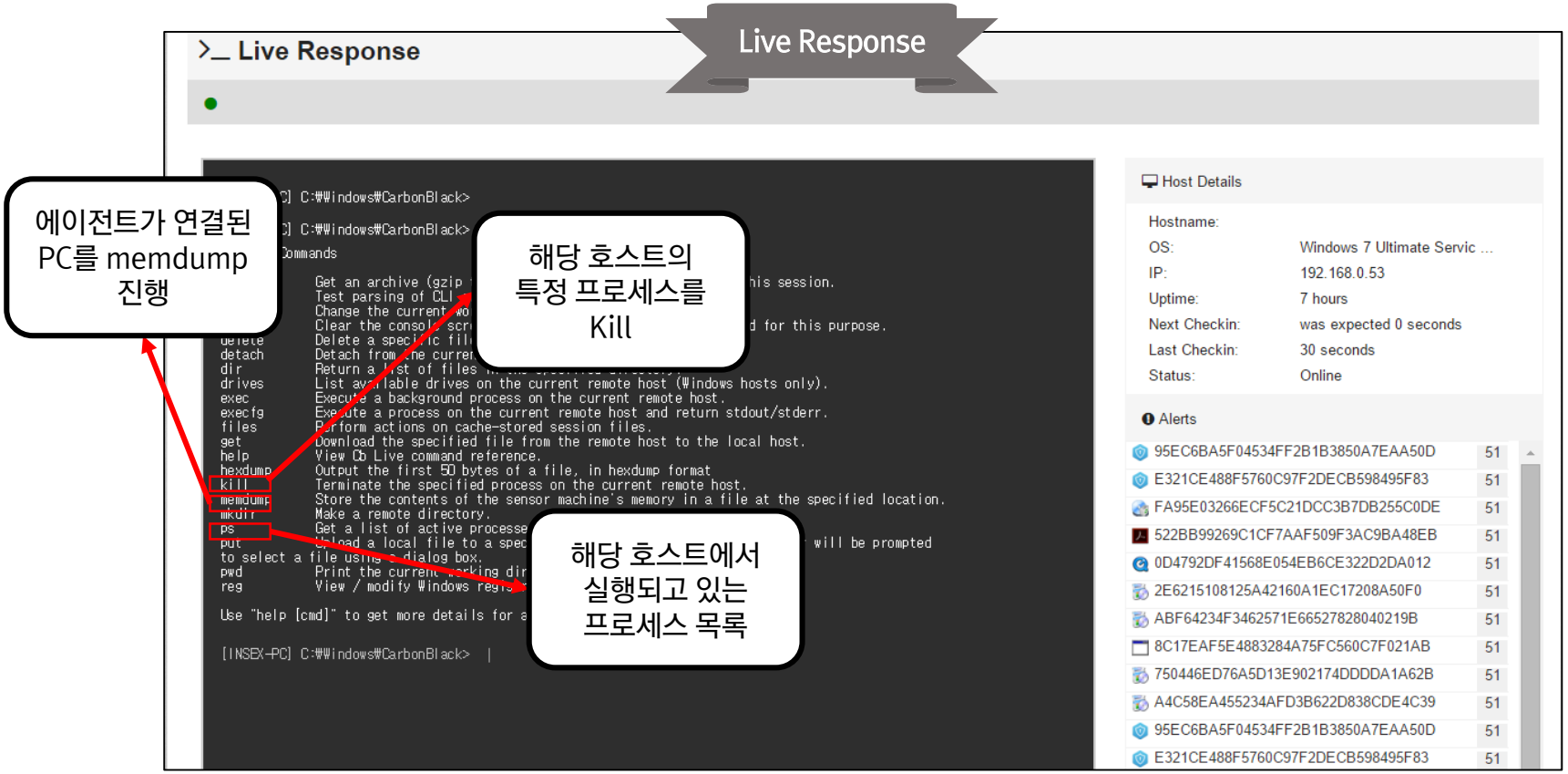


Copyright INSEC Co.,Ldt. All Rights Reserved.

Feature (5)

Live Response

엔드포인트 위협 검사, 치료, 상세 분석 및 악성 프로세스 종료를 위한 Command Line



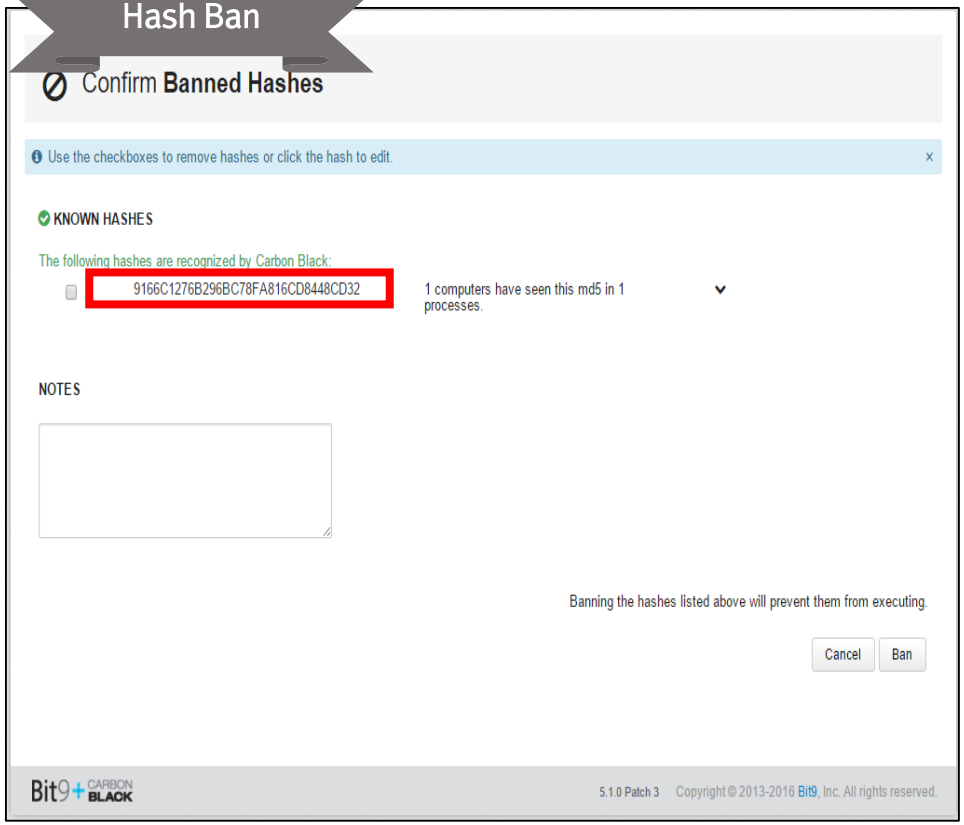
Copyright INSEC Co.,Ldt. All Rights Reserved.

Feature (6)

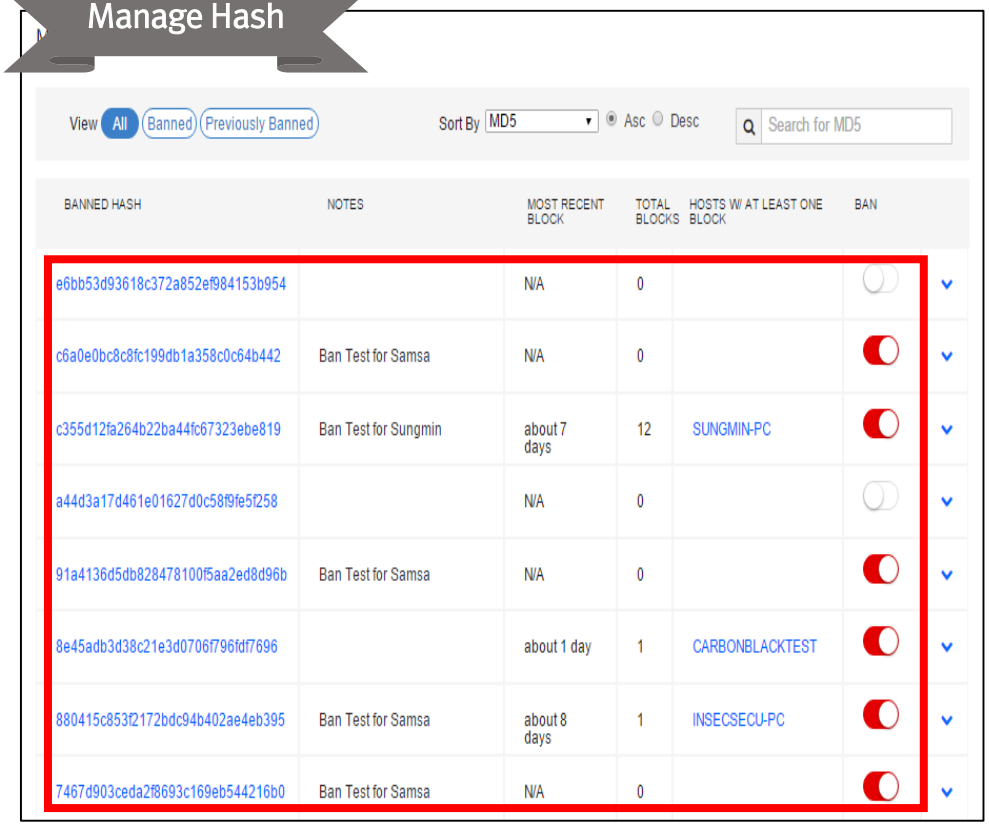
Easy Hash Ban

Hash 차단 기능으로 동일 Hash값을 가진 프로세스를 모든 호스트에서 실행 차단합니다

Hash Ban



Manage Hash



Copyright INSEC Co.,Ldt. All Rights Reserved.

CARBON BLACK
ARM YOUR ENDPOINTS

INSEC security

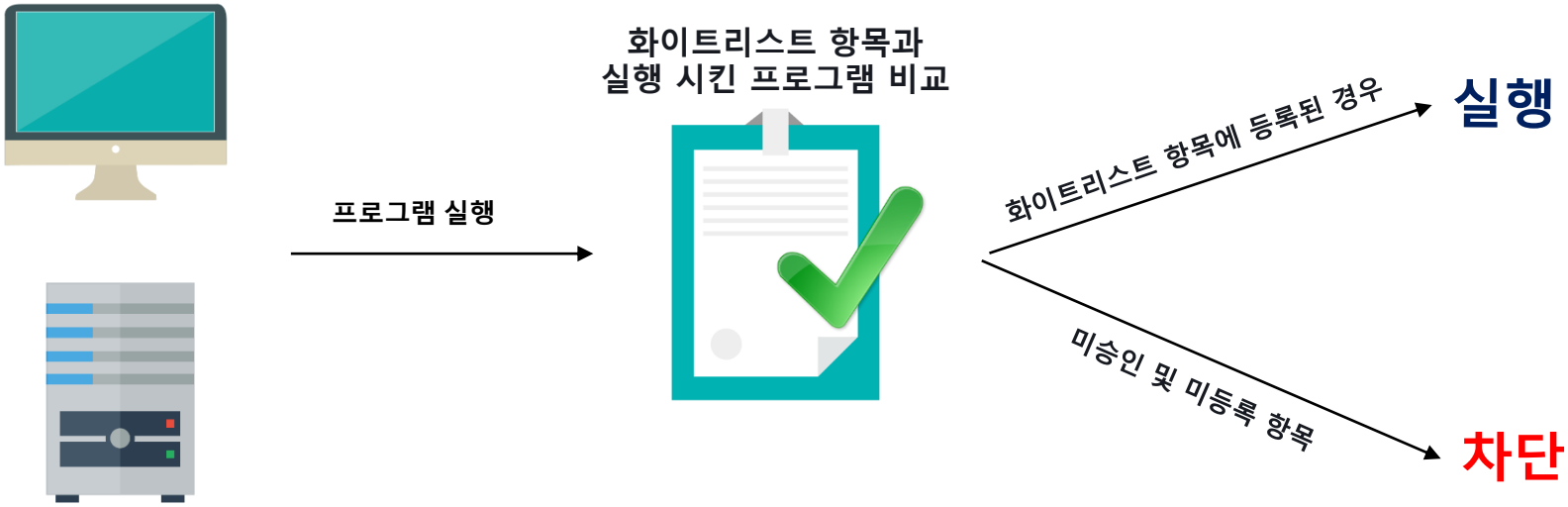
BUT,

사전 차단 어려움

Copyright INSEC Co.,Ldt. All Rights Reserved.

화이트리스트(WhiteList) 란?

화이트 리스트(WhiteList)란 리스트에 등록된 프로세스들만 동작하도록 하고 리스트에 없는 프로그램은 실행을 거부하는 방식을 말합니다.



Copyright INSEC Co.,Ldt. All Rights Reserved.

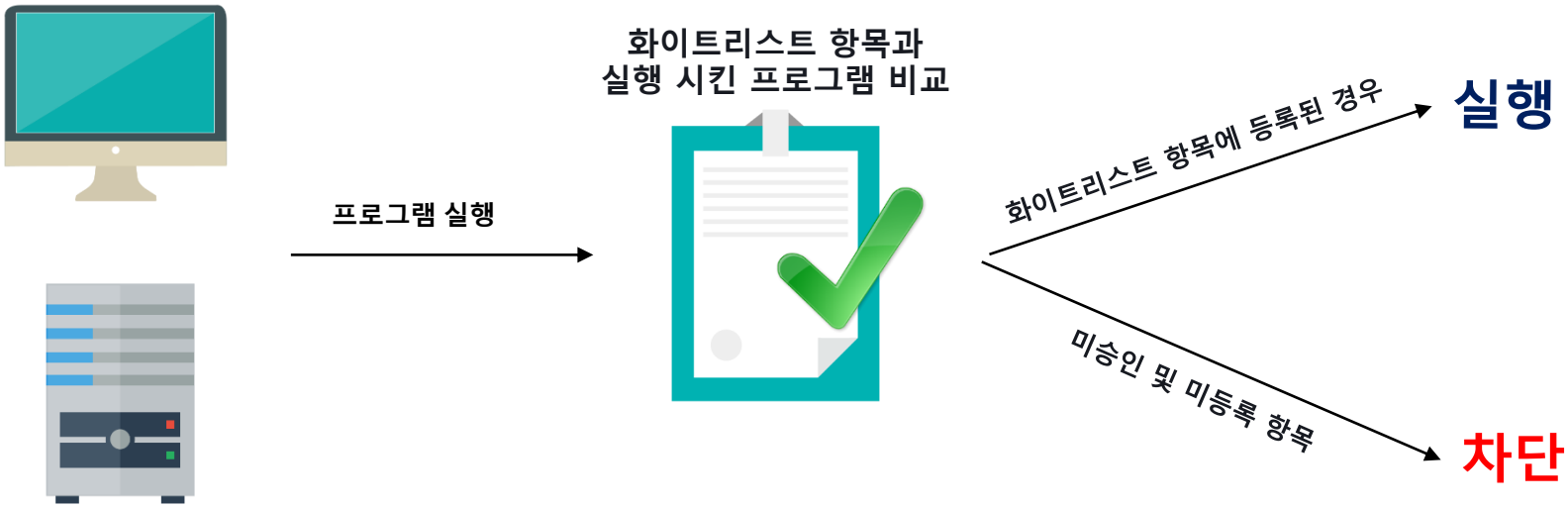
CarbonBlack Enterprise Protection 소개

사용자의 PC, 서버 등에서 실행되는 응용프로그램 및 운영체제의 파일의 Hash 값을 화이트리스트 목록으로 생성한 뒤, 목록에 없는 파일의 실행을 차단합니다.

Copyright INSEC Co.,Ldt. All Rights Reserved.

화이트리스트(WhiteList) 기반의 보안 솔루션

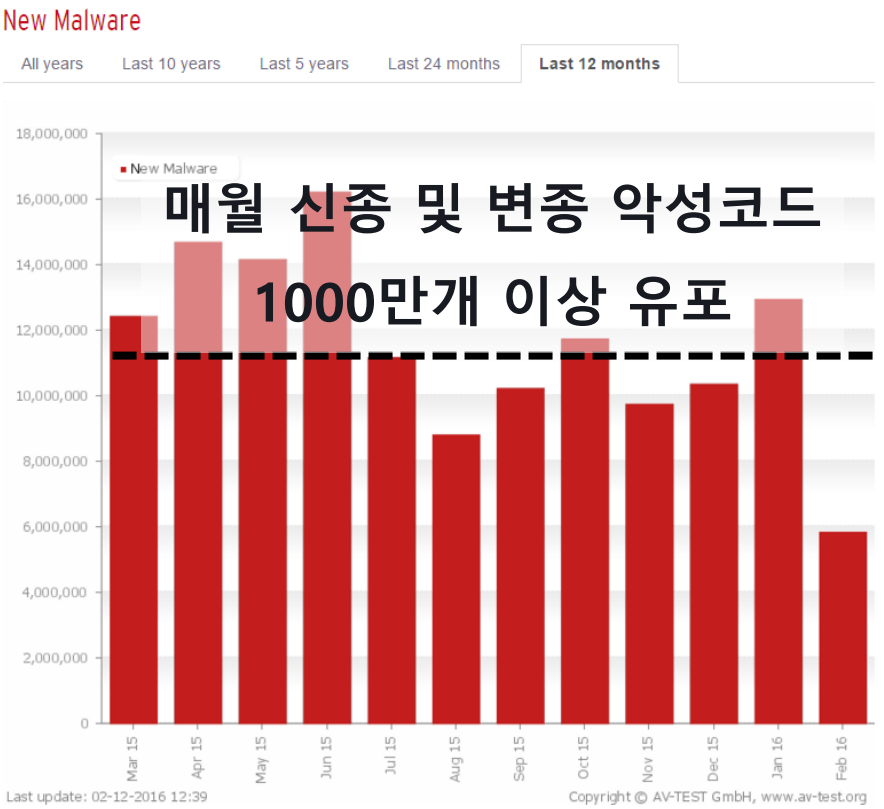
화이트 리스트란 등록 된 프로세스들만 실행을 허용하고 리스트에 없는 프로그램은 실행을 거부하는 방식을 말합니다.



Copyright INSEC Co.,Ldt. All Rights Reserved.

WhiteList 방식의 필요성

현재 전 세계 유포 된 악성코드 누적 양은 5억 개 정도이며 매달 새로운 악성코드가 약 1000 만개 이상 유포되고 있습니다.



Copyright INSEC Co.,Ldt. All Rights Reserved.

WhiteList VS BlackList

Protection 같은 경우는 화이트리스트 방식, 일반적으로 알고 있는 AV 엔진들이 블랙리스트 방식입니다.

WhiteList 방식과 BlackList 방식의 비교표

WhiteList	구분	BlackList
사전 예방	처리 방식	사후처리
허용된 프로세스만 사용	실행 범위	모든 프로그램 허용
제한적 환경	편의성	범용적 환경
변경 없음	엔진 사이즈	지속적인 증가
낮음	리소스 점유율	높음
높음	보안 수준	낮음
필요없음	업데이트/패치	주기적 필요

Copyright INSEC Co.,Ldt. All Rights Reserved.

WhiteList 방식의 필요성

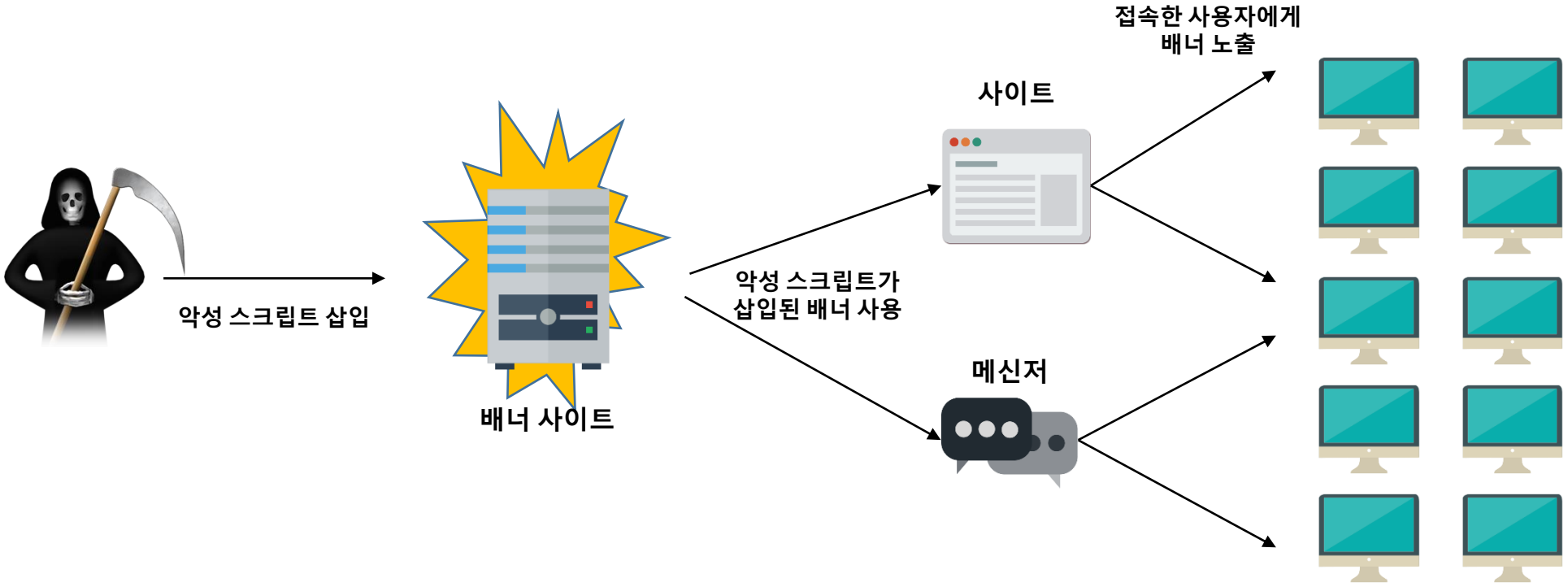
WhiteList 방식의 CarbonBlack Enterprise Protection을 사용하면 랜섬웨어를 예방할 수 있습니다.

사전에 랜섬웨어 실행을 차단함으로써 감염으로부터 예방할 수 있습니다.

Copyright INSEC Co.,Ldt. All Rights Reserved.

WhiteList 방식의 필요성

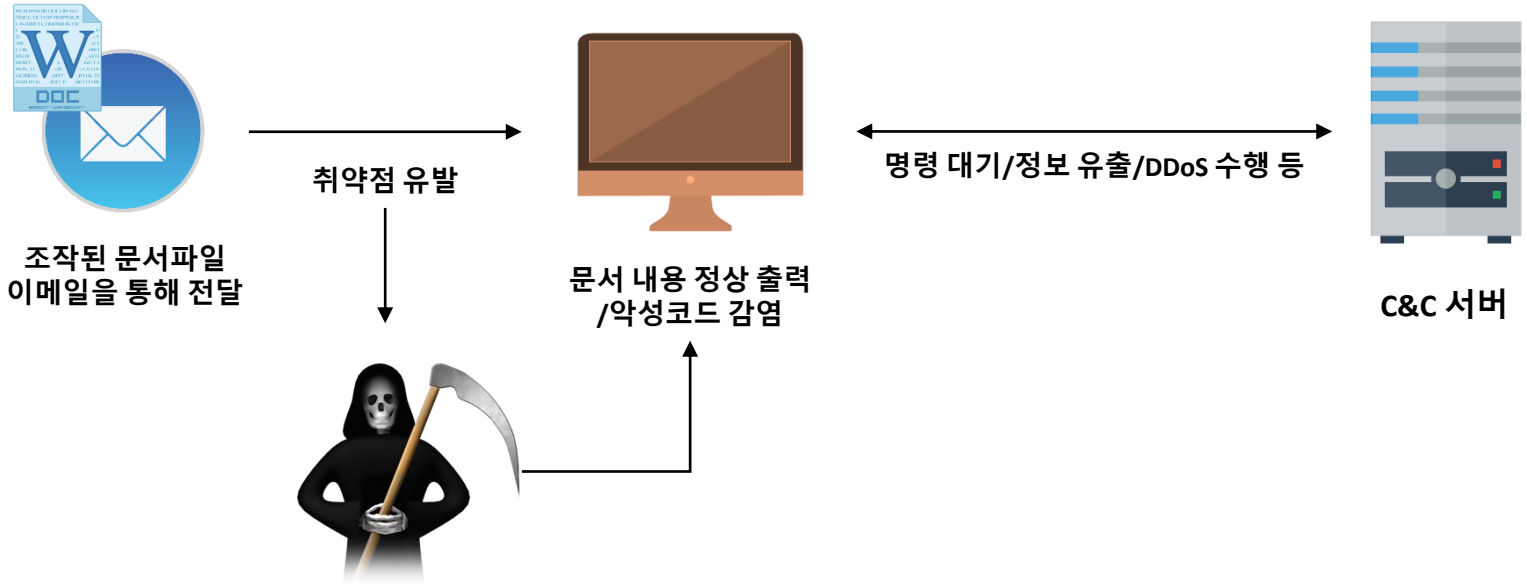
웹 사이트를 통한 악성코드 경유 및 유포 감염



Copyright INSEC Co.,Ldt. All Rights Reserved.

WhiteList 방식의 필요성

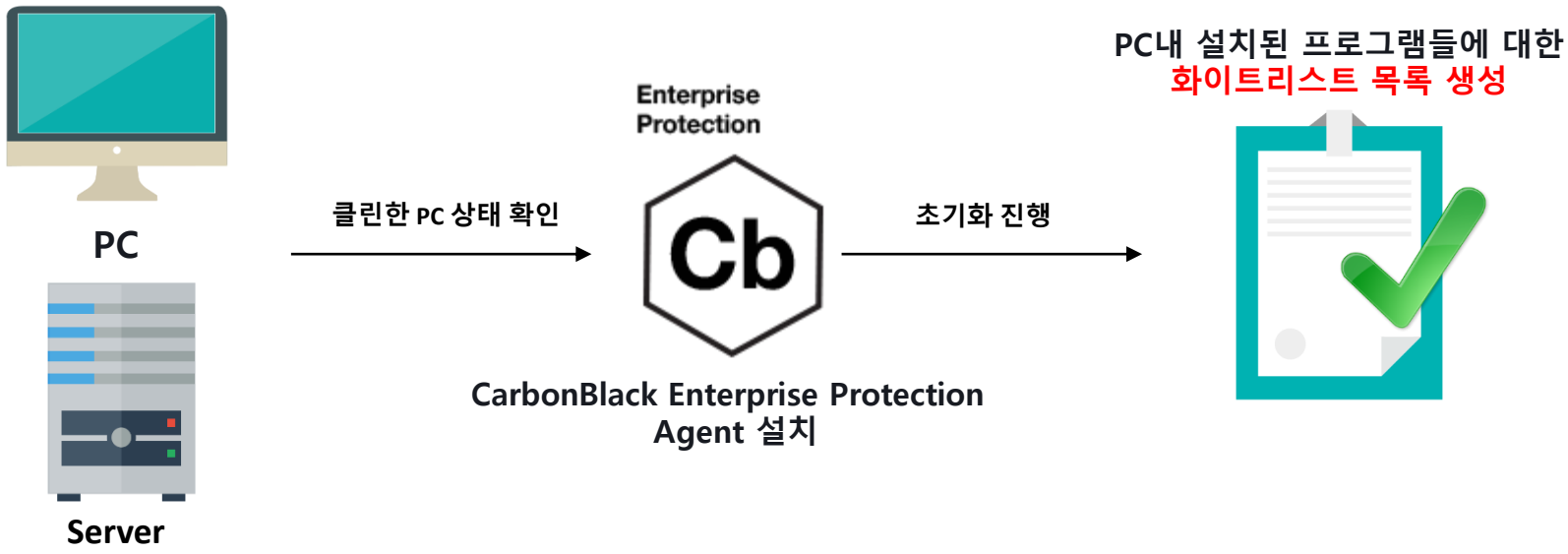
이메일 전파를 통한 악성코드 감염



Copyright INSEC Co.,Ldt. All Rights Reserved.

CarbonBlack Enterprise Protection 동작방식

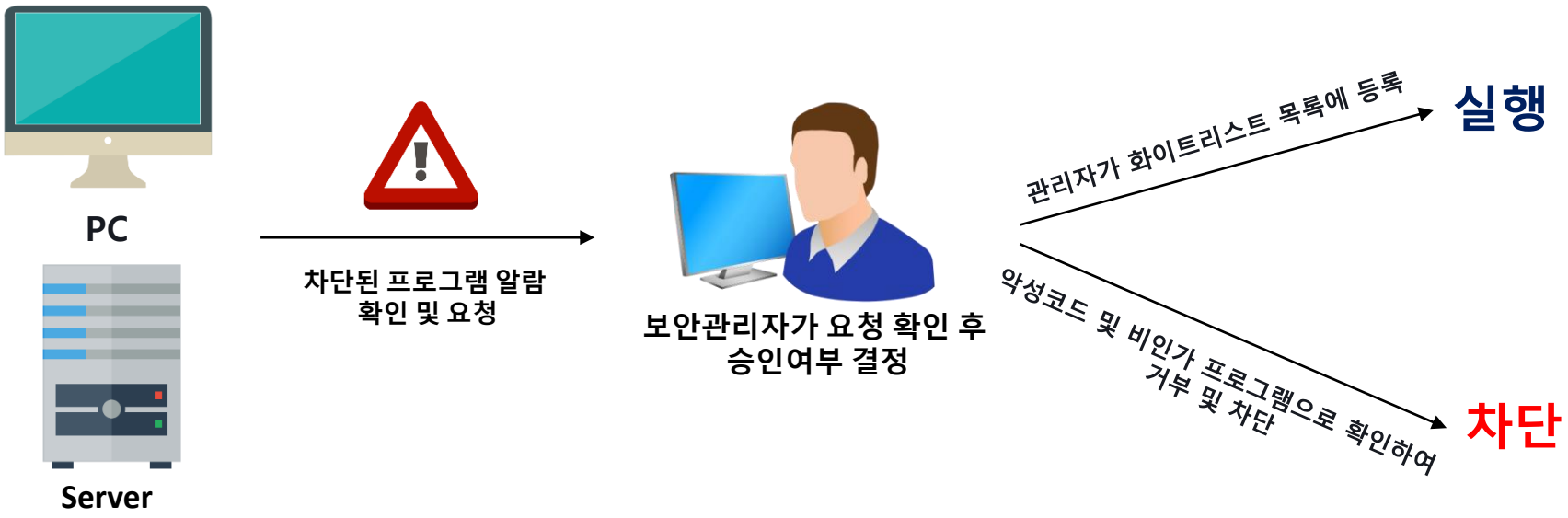
사용자 PC를 신뢰할 수 있는 상태로 만든 뒤, Protection Agent를 설치합니다.
이후 초기화 과정을 통해 설치 된 프로그램 및 정책을 포함하여 화이트리스트로 생성합니다.



Copyright INSEC Co.,Ldt. All Rights Reserved.

CarbonBlack Enterprise Protection 동작방식

Protection에 의해 차단된 항목에 대해서 관리자에게 요청하게 되면 요청 내역이 관리자에게 전달이 되고 관리자는 해당 내역을 확인하여 승인/차단을 결정할 수 있습니다.



Copyright INSEC Co.,Ldt. All Rights Reserved.

CarbonBlack Enterprise Protection 동작방식

회사 정책에 따른 승인된 소프트웨어만 허용 함으로서 최신 APT 공격, 스피어 피싱, Zero-day 공격을 차단

레지스트리, 프로세스, 시스템 파일 등에 대한 불법적인 접근을 막기 위한 실시간 모니터링 및 제어, 통제

Parity Knowledge 서비스를 이용 소프트웨어의 위험성을 식별하고, 개인저장 장치에 내부 데이터 접근 내역 추적 가능

Copyright INSEC Co.,Ldt. All Rights Reserved.

CarbonBlack Enterprise Protection 의 특징

1. 화이트리스트 방식으로 운영됩니다.
2. 등록된 자산들의 모든 행위에 대해서 모니터링이 가능합니다.
3. 정책을 레벨을 설정하고, 설정된 정책을 그룹별, 개인별로 구분하여 적용할 수 있습니다.
4. 인터넷이 단절된 상태에서도 오프라인 정책을 적용할 수 있습니다
5. 앤드포인트에서 설치 된 에이전트를 강제로 삭제할 수 없습니다.
6. 이동형 저장매체에 대해서 접근 제한 및 차단할 수 있습니다.
7. 뛰어난 확장성을 바탕으로 타 AV 엔진들과 연동하여 사용할 수 있습니다.
8. 정책을 설정할 때 로컬, 글로벌 단위로 구분하여 적용할 수 있습니다.
9. 적은 리소스 소요로 에이젼트로 설치된 자산들이 운영 되는데 있어서 영향이 전혀 없습니다.

Copyright INSEC Co.,Ldt. All Rights Reserved.

Peristalsis

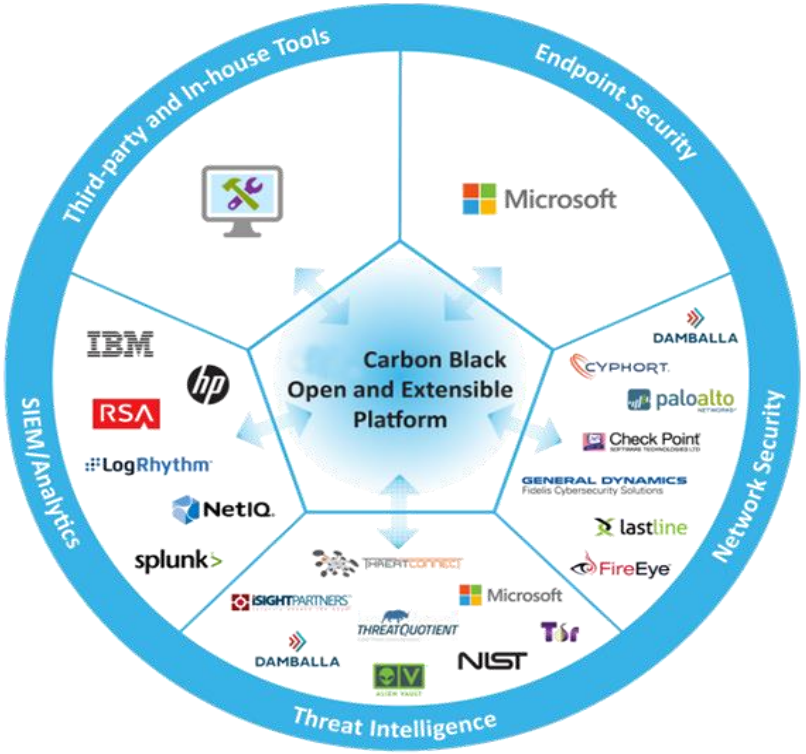
- 다양한 보안 솔루션 연동 및 확장 가능한 제품

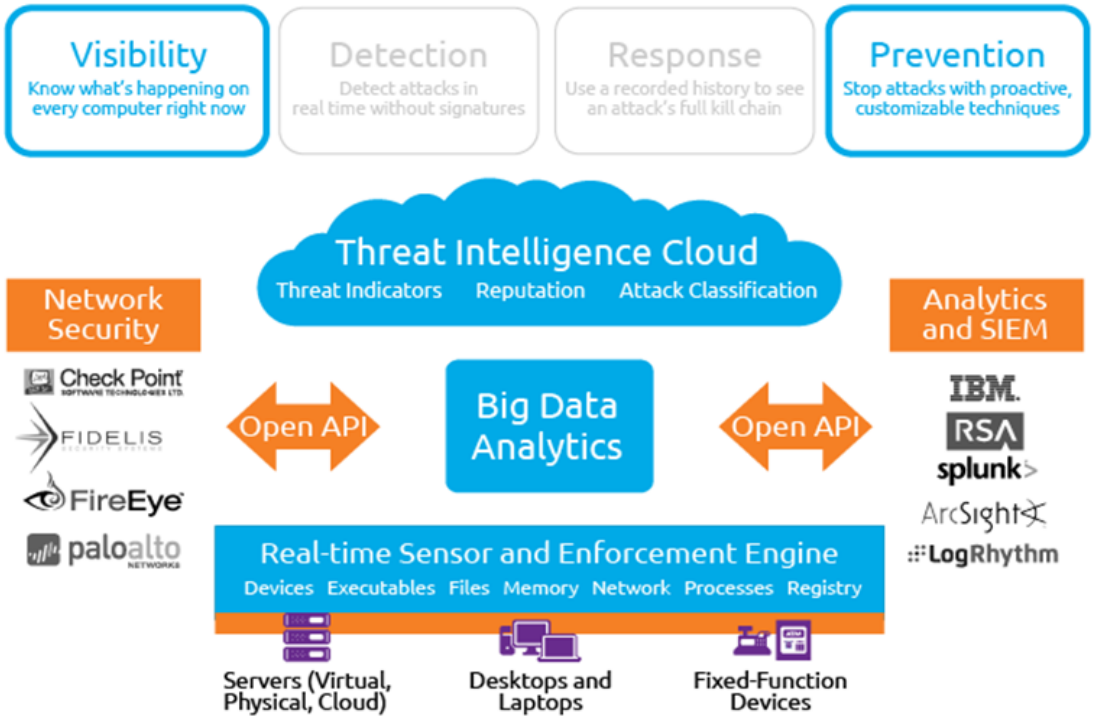
Copyright INSEC Co.,Ldt. All Rights Reserved.

Peristalsis (2)

다양한 보안 솔루션 연동 및 확장 가능한 제품

Carbon Black은 아래와 같은 솔루션(Network Security, Endpoint Security, SEIM / Analytics, Threat Intelligence, Third-party and In-house Tool)과 연동을 할 수 있습니다.





Copyright INSEC Co.,Ldt. All Rights Reserved.

Reseller

INSEC security

INSEC Security

Solution Business Department, INSEC Security
[Education & Products Sales]
www.bit9korea.co.kr / www.totalsecurity.com
서울시 금천구 가산디지털1로 128 STX-V-TOWER 5층 505호
Tel : + 82-2-863-5687 | Fax : + 82-2-862-5687 |

Contact

Sales Director, INSEC Security, 신영섭 이사 | **kidari@insec.co.kr** | Tel : 010-4145-6800
Technical Engineer, INSEC Security, 채준혁 대리 | **david@insec.co.kr** | Tel : 010-2031-4456

Copyright INSEC Co.,Ldt. All Rights Reserved.