HBGary
Detecting Tomorrow's Threats Today
Part of ManTech International Corporation

ACTIVE DEFENSE
Powered by Digital DNA™

HBGray Active Defense 제품 소개 및 기능 시연

INSEC security

HBGary
Detecting Tomorrow's Threats Today
A subsidiary of ManTech International Corporation

김 종 광 원장 masterkey@insec.co.kr

[악성코드 ?]

INSEC security

김 종 광 원장 masterkey@insec.co.kr

※ 악성코드의 정의

- 컴퓨터에 악영향을 끼쳐 정상적인 동작을 방해하도록 만들어진 프로그램
- 80년대 중반부터 시스템 파괴 형 바이러스, 웜, 트로이목마 등이 성행 하였으며 점차 시간이 지남에 따라 시스템 파괴형에서 사용자 개인 정보 유출 유형의 악성코드가 성행하게 됨
- 윈도우, 리눅스, 유닉스 운영체제 환경에 맞는 다양한 악성코드들이 존재
- 악성코드 차단을 위해 기업 내부에서 안티 바이러스, IPS, IDS 등을 사용하여 차단

김 종 광 원장 masterkey@insec.co.kr

※ 악성코드 차단 / 대응 기술

악성코드 실시간 탐지
(Anti-Virus)

악성 트래픽 / 패킷 차단
(IDS, IPS, UTM)

김 종 광 원장 masterkey@insec.co.kr

※ 현 악성코드 대응 방안의 한계점

➢ 기업 내부에서 사용되는 대부분의 악성코드 대응 장비들은 패턴 매칭 기술을 사용하여 악성코드를 탐지

패턴 매칭(Signicture Machine)

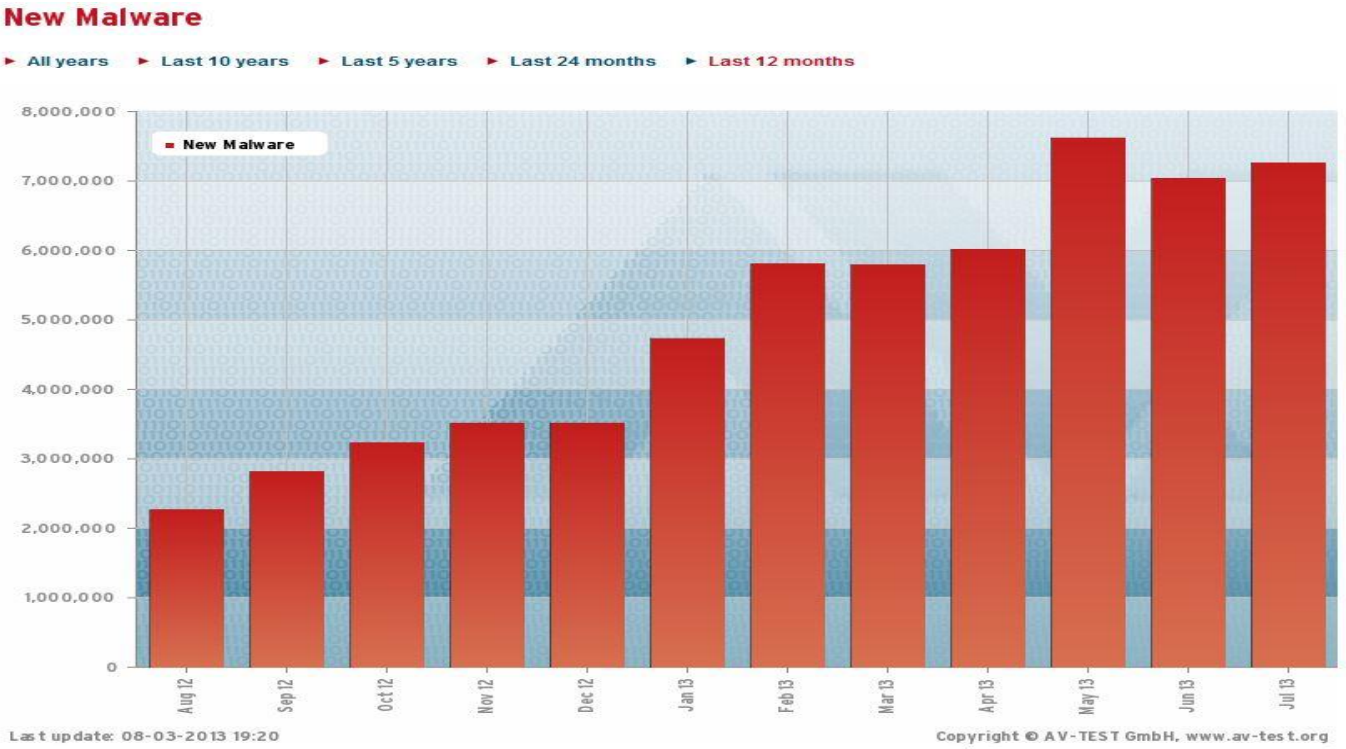
(Anti-Virus, IDS, IPS, UTM)

✓ 이미 알려지거나 분석 된 악성코드의 정보를 데이터베이스화 하여 악성코드를 탐지하는 방식

✓ 주로 해시 값, 특정 위치의 바이너리 코드를 등록

※ 현 악성코드 대응 방안의 한계점

➢ 전 세계적으로 하루에 새롭게 생성되는 악성코드는 약 평균 60만개 이상



※ 현 악성코드 대응 방안의 한계점

- 하루에 안티 바이러스가 패턴 데이터베이스를 업데이트하는 평균 패턴 갯수 ?
- 악성코드를 유포하는 제작자들은 소스 코드가 존재하기 때문에 소스 일부분을 수정하여 쉽게 변종을 제작할 수 있음 (안티 바이러스 회피 !!!)
- Resource Modification, Code Patch, PE Header Modification, File Joining 패키징 등 패턴 기반을 우회할 수 있는 다양한 기술들이 존재

김 종 광 원장 masterkey@insec.co.kr

[Active Defense 주요 기능]

INSEC security

김 종 광 원장 masterkey@insec.co.kr

※ Active Defense 주요 기능

- 에이전트 기반으로 동작되며 시스템에 감염 된 악성코드를 행위 기반 기술로 탐지하여 안티 바이러스들이 탐지하지 못하는 Unknown Malware, APT 공격을 탐지

- 실시간으로 에이전트의 메모리를 모니터링하여 메모리 내의 악성 코드를 탐지

- Active Defense 의 주요 기술 중 Digital DNA 을 이용하여 실행 중인 프로세스를 대상으로 행위 분석을 통해 악성코드를 탐지

김 종 광 원장 masterkey@insec.co.kr

※ Active Defense가 필요한 이유?

- 신종 / 변종 악성코드는 패턴 기반 탐지로는 한계점이 존재! 그러면 어떻게 탐지할 것인가?
- 악성코드로 감염 된 의심되는 시스템에서 어떻게 악성코드를 찾아낼 것인가?
- 패킹 / 난독화 된 악성코드는 어떻게 분석을 수행 할 것인가?
- 루트킷을 적용 한 악성코드를 어떻게 탐지 할 것인가?
- 악성코드가 감염 된 경로 및 시간 분석을 확인하고 싶을 때
- 자사 내의 수 많은 시스템들의 악성코드를 어떻게 찾아 낼 것인가?

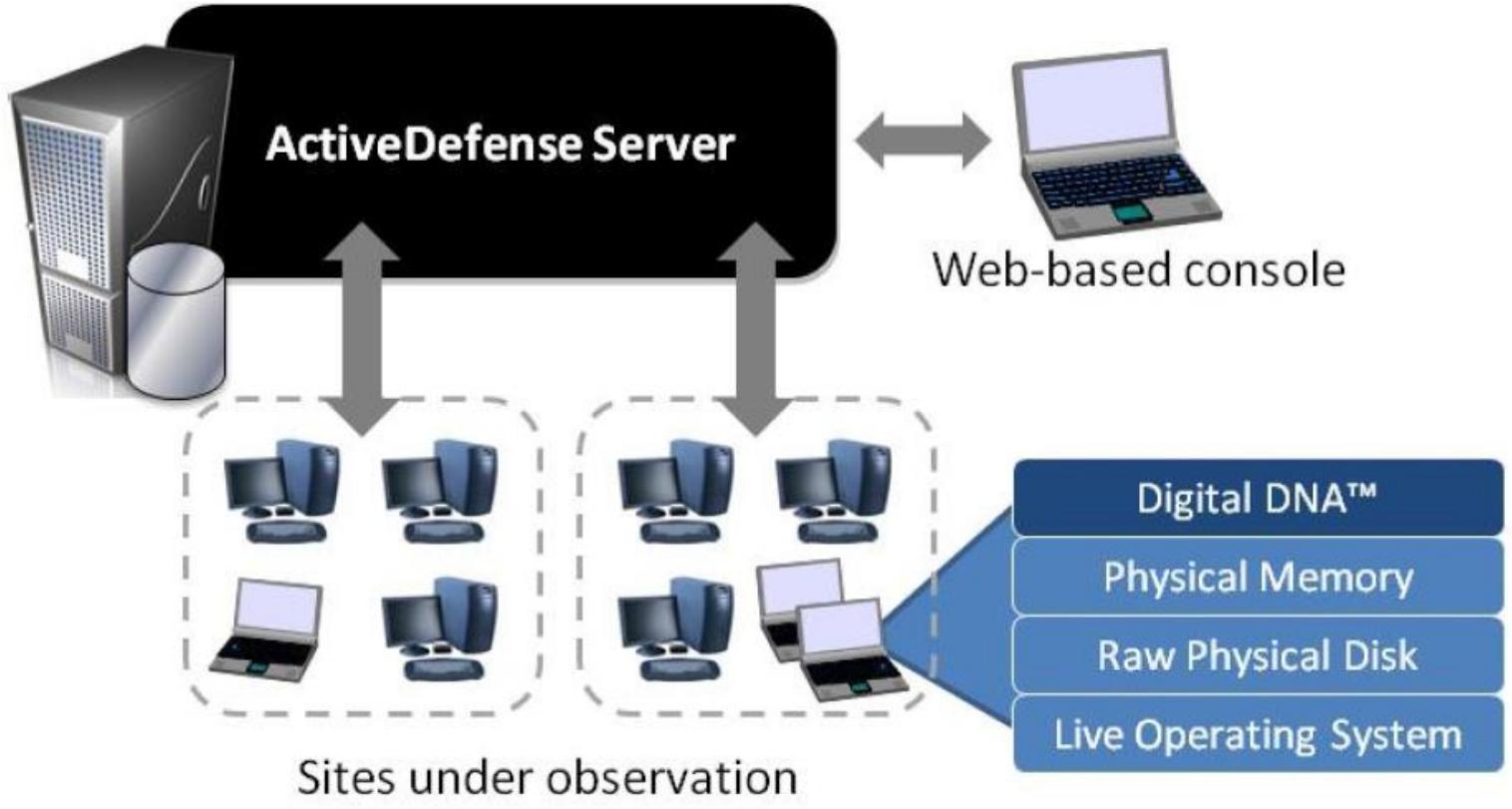
김 종 광 원장 masterkey@insec.co.kr

※ Active Defense 주요 기능

- 실시간 메모리 분석을 통한 악성코드 탐지
- 실행 프로세스 정보 분석
- 원격 메모리 덤프 및 분석 기능
- 타임 라인 분석을 통한 시간 대 별 악성코드 동작 판별
- Incident Analysis 기능 제공(파일 다운로드, 프로세스 분석, 매칭 파일 분석)
- Rootkit & RAT 탐지
- 프로세스 스트링 분석 기능

김 종 광 원장 masterkey@insec.co.kr

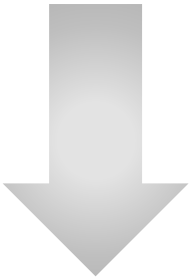
※ Active Defense 동작 방식



※ Active Defense 중앙 관리 인터페이스

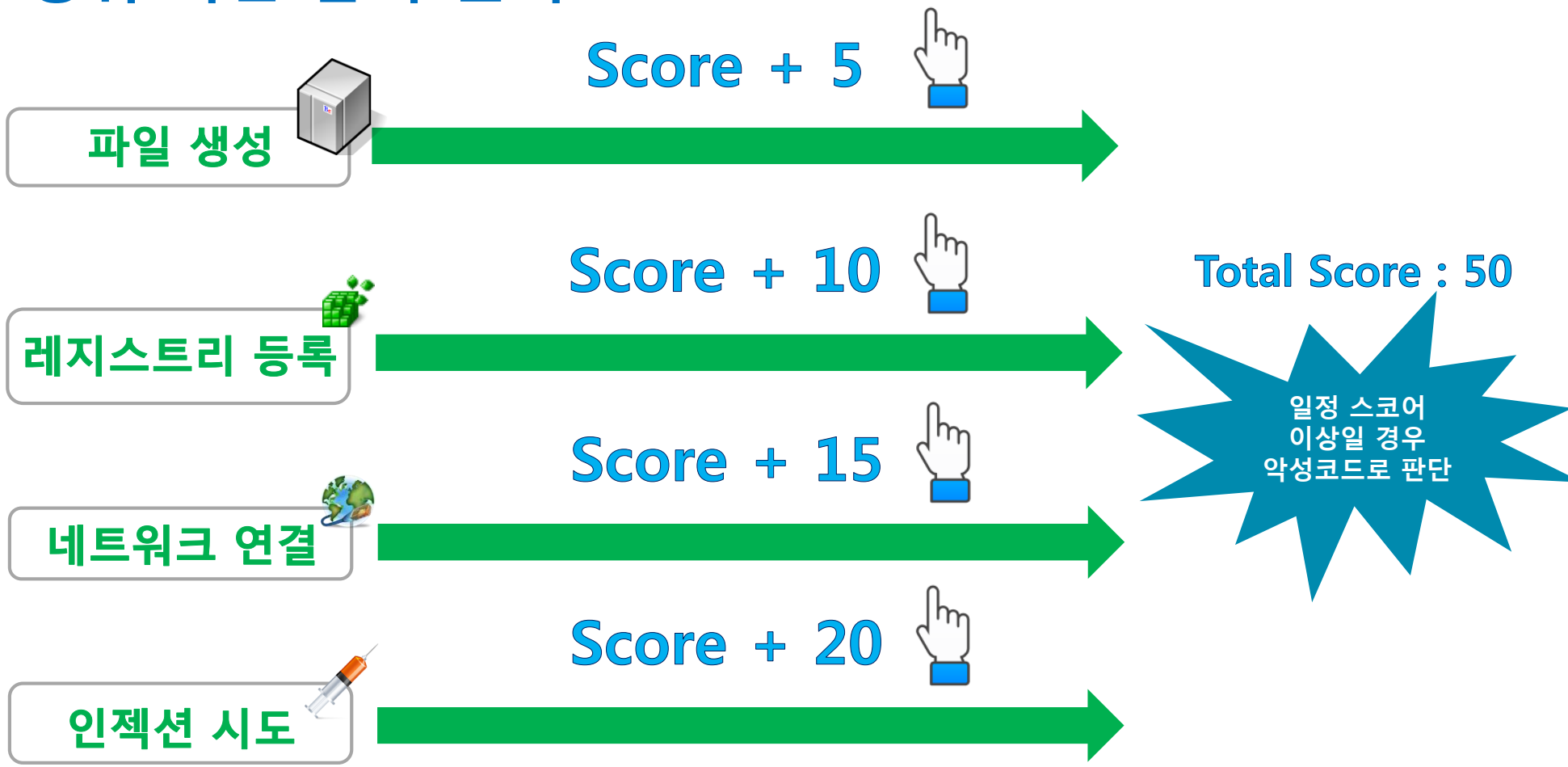
※ Active Defense 핵심 기능

행위 기반 탐지
(Behavior Detection)



패킹, 난독화가 적용 된 악성코드 탐지
신종, 변종 악성코드에 대한 빠른 대응

※ 행위 기반 탐지 원리


파일 생성
Score + 5
레지스트리 등록
Score + 10
네트워크 연결
Score + 15
인젝션 시도
Score + 20
Total Score : 50
일정 스코어
이상일 경우
악성코드로 판단

※ Digital DNA

DIGITAL DNA™
Advanced Detection For Faster, More Targeted Incident Response

- 기존 보안 솔루션들의 악성코드 탐지 방식에서 벗어나 모듈의 행위를 통해 악성코드를 판별하는 특허 기술(행위 분석 패턴)

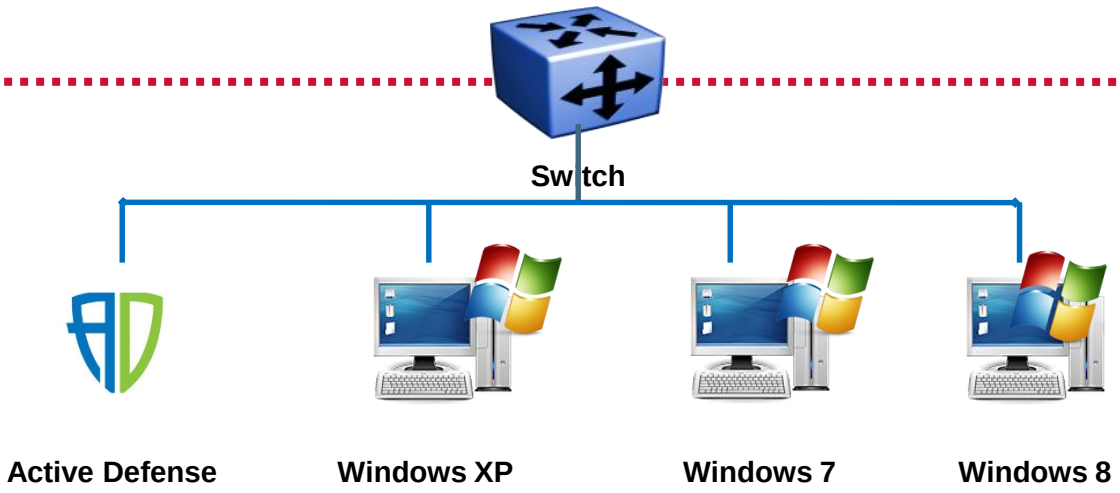
- 안티 바이러스들이 탐지하지 못하는 Unknown Malware 및 APT 형 악성코드를 행위 기반으로 탐지하여 빠른 대응이 가능

Digital DNA Sequence	Name	Process Name	Size	Severity	Weight
0F 16 30 04 2D 97 0F ...	memorymod-code-0x00150000-0x00151000	IEXPLORE.EXE	4096		71.8
0F 16 30 04 2D 97 0F ...	memorymod-code-0x01100000-0x01101000	explorer.exe	4096		71.8
00 B4 EE 0F 20 22 00 ...	memorymod-code-0x00160000-0x00161000	IEXPLORE.EXE	4096		49.4
0F 20 22 00 66 09 00 ...	memorymod-code-0x01530000-0x01531000	explorer.exe	4096		43.5
00 B4 0B 02 38 CD 00 ...	izarccm.dll	explorer.exe	688128		7.7
02 00 B1 00 DE FC 01 ...	dxg.sys	System	73728		7.0
02 00 B1 02 3C 02 01 ...	win32k.sys	System	1839104		6.4

김 종 광 원장 masterkey@insec.co.kr

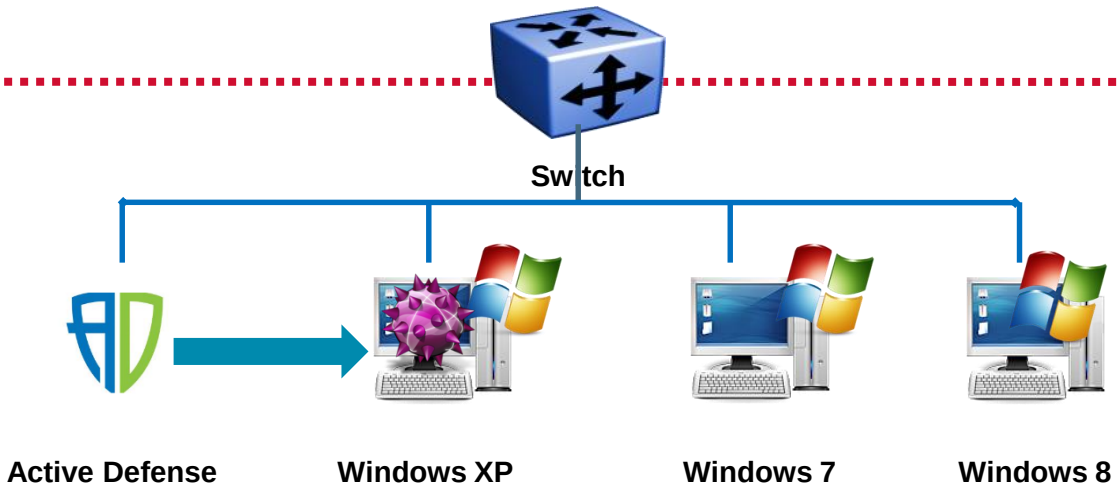
[기능 시연 구성도]

※ 기능 시연 구성도



※ 기능 시연 구성도

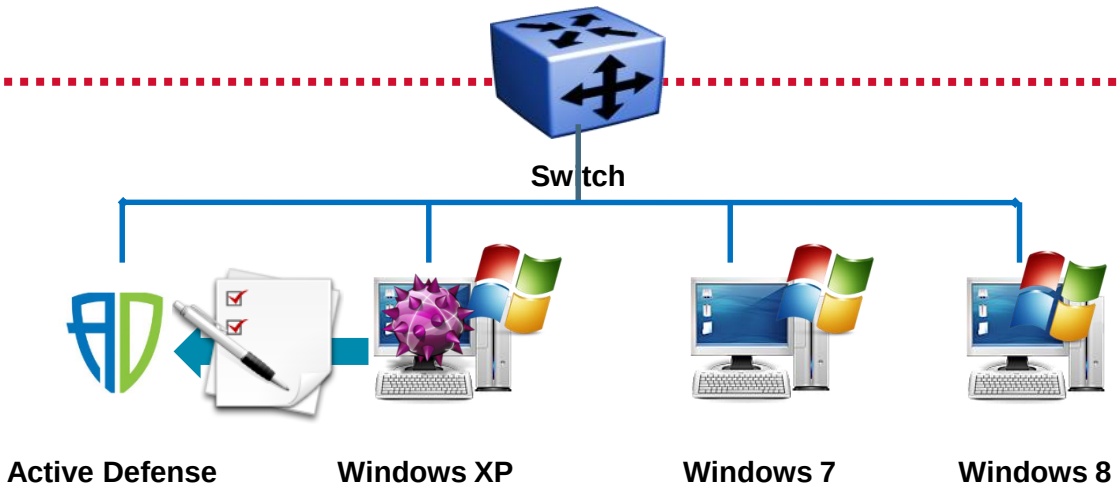
➢ 악성 코드가 감염 된 에이전트 시스템을 대상으로 스캔 수행 후 악성코드 탐지 시연



실시간 메모리 분석 수행

※ 기능 시연 구성도

➢ **Incident Analysis 기능을 활용한 악성코드 행위 추가 분석 시연**



※ 기능 시연 구성도

➢ 원격 메모리 덤프 기능을 이용하여 추가 악성코드 분석