INSEC security

EnCase Endpoint Investigator 제품 소개 자료

2017년

CONTENT

CONTENT

포렌식 개요 / 기업활동과 정보보안

Forensic의 개요

Computer Forensic 이란 무엇인가?

- ✓ "**법정의**", "**변론에 적합한**"
- ✓ **컴퓨터 범죄**에 대한 법적 **증거자료**가 **법적 증거물**로서 제출될 수 있도록 **증거물**을 **수집, 복사, 분석, 제출**하는 일련의 행위

포렌식 개요 / 기업활동과 정보보안

Forensic의 개요

Computer Forensic 이란 무엇인가?

- ✓ 컴퓨터 부정행위를 빠른 시간 안에 정확하게 찾아냄
- ✓ 행위에 이용된 **증거 확보**를 통한 **법적 대응**을 가능하게 함
- ✓ **컴퓨터 범죄를 지속적으로 감소** 시킴

포렌식 개요 / 기업활동과 정보보안

Forensic의 개요

Computer Forensic 의 유형

- ✓ 디스크 (Disk Forensics)
- ✓ 네트워크 (Network Forensics)
- ✓ 전자우편 (E-mail Forensics)
- ✓ 인터넷 또는 웹 (Internet or www Forensics)
- ✓ 휴대 정보기기 (Mobile device Forensics)
- ✓ 데이터 베이스 (Database Forensics)

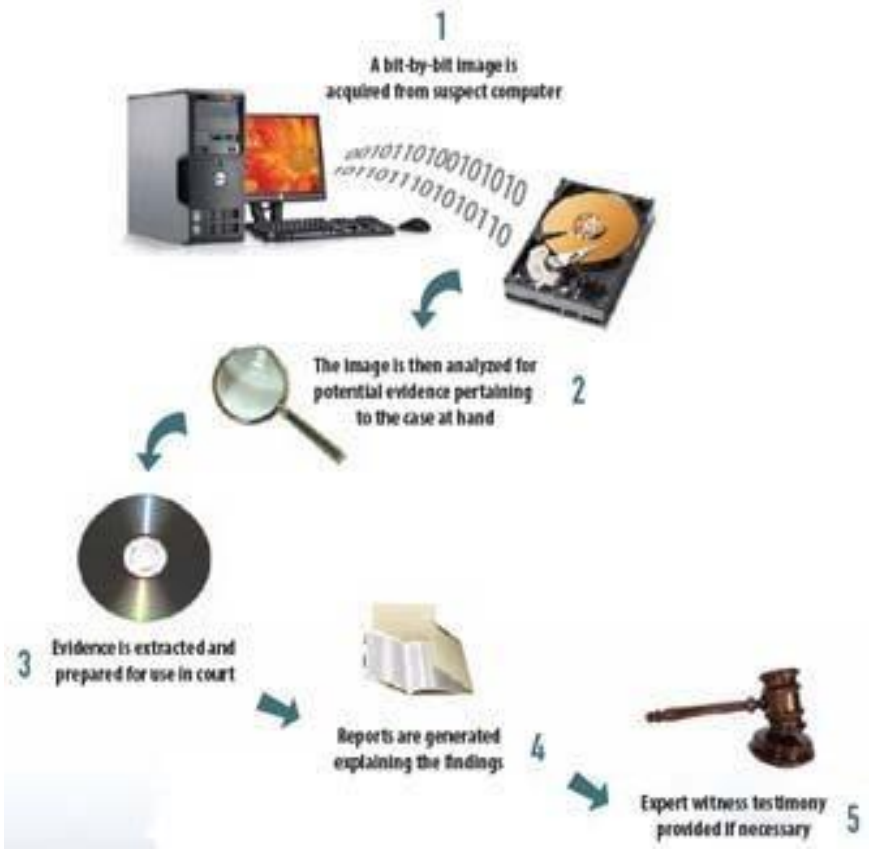
포렌식 개요 / 기업활동과 정보보안

Forensic의 개요

Computer Forensic 의 기술

✓ 디지털 증거물 분석

- ➢ 디스크의 내용이 변경되는 것을 방지(디스크 쓰기 방지)
  - Write Protector
- ➢ 디스크이미지 파일을 비트스트림으로 복제
  - EnCase에서 Evidence Acquire기능(자체 파일 포멧)
- ➢ 증거물에 대해서 해쉬를 계산한 후 원래의 계산 값과 비교하여 내용이 변경되지 않았음을 보장하는 메시지 다이제스트 기술
  - MD5 – 128bit message digest
  - SHA – 160bit message digest



포렌식 개요 / 기업활동과 정보보안

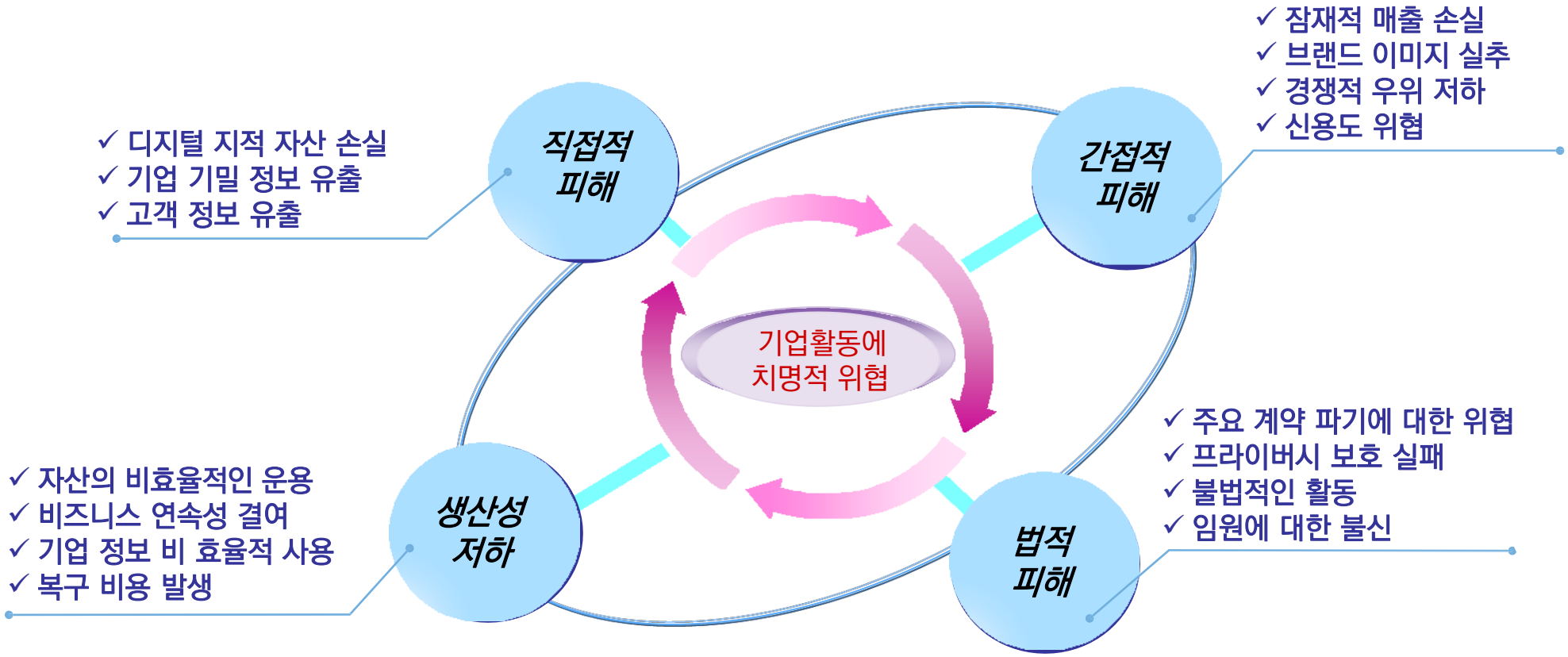
Forensic의 개요

Computer Forensic 의 기술

- ✓ 디지털 증거물 분석
  - ➢ 디렉토리, 파일목록 열람
  - ➢ 로그 분석
  - ➢ 프로세스 분석
  - ➢ 검색
  - ➢ 열람 프로그램 호출
  - ➢ 해시 분석
  - ➢ 시그니처 분석
  - ➢ 시계열 분석
  - ➢ 삭제된 파일 복구
  - ➢ 삭제된 전자우편 복구
  - ➢ 암호화된 파일 복호화 및 패스워드 크랙
  - ➢ 증거물 저장 및 관리
  - ➢ 보고서 작성 및 생성

기업활동과 정보보안 개요

정보보안 침해로 인한 기업의 위험



기업활동과 정보보안 개요 (계속)

기업활동에 있어서 IT Compliance 필요성

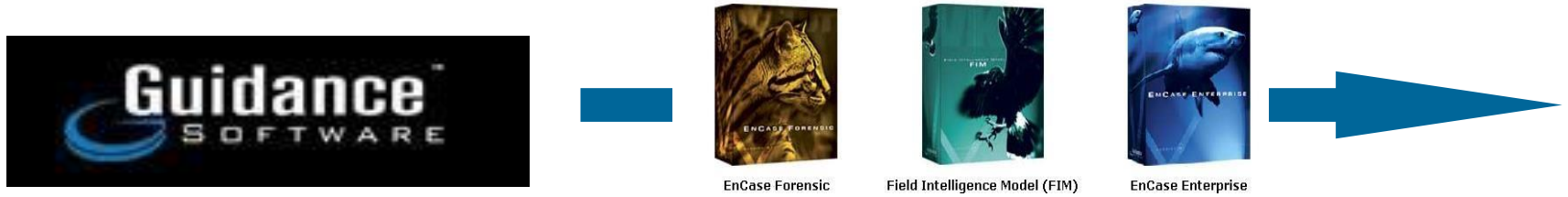
✓ IT Compliance는 기업의 리스크 관리 및 투명성 강화를 위해 해당기업에 대해서 정부나 관련기관들이 강제사항으로 규제하는 각종 규제법안의 요건들을 만족 시킬 수 있도록 기업의 IT 측면에서 이를 준비하고 관련 시스템을 재정비하는 것을 의미.

✓ 규제법안의 시초는 1988년 7월 국제결제은행내의 바젤 위원회에서 금융기관들의 각종 리스크 증대에 대처하고자 자기자본규제에 대한 기준을 설정한 바젤I이 시초이며, 현재는 그 기준을 강화한 바젤II가 준비되고 있다.

✓ 국내의 규제로는 정통부가 주요기업을 대상으로 고시한 "전산망 안전 신뢰성 기준"과 금융 정보화 추진분과위원회에서 마련한 " 금융정보망 안전대책 강화방안"등이 있다.

GuidanceSoftware사 소개

1. GuidanceSoftware사 소개



- 1997년에 설립된 **Guidance Software**는 전 세계적으로 컴퓨터 **조사용 솔루션 업계의 리더**로 인정받고 있습니다.
- **Guidance Software**사의 **EnCase®** 솔루션은 **기업, 정부 및 법 집행 기관으로 하여금 데이터의 과학 수사적 무결성을 유지**하는 동시에 모든 유형의 컴퓨터 조사를 효율적으로 수행하고 eDiscovery 요청을 신속하게 처리하며 **디지털 증거와 관련된 내부 조사를 빠르고 철저하게 수행**할 수 있도록 해주는, 법 진행 기관과 기업 조사 모두를 위한 토대를 제공합니다.
- 2만 명 이상의 조사관이 **EnCase Software**를 사용하고 있으며 매년 5천 명 이상의 조사관들이 **Guidance Software**의 과학 수사 방법론 교육에 참여하고 있습니다.
- 전세계의 수많은 법원이 인증한 **EnCase Software**는 **eWEEK, SC Magazine, Network Computing 및 기타 매체**로부터 **최고의 보안소프트웨어로 인정** 받고 있습니다.

Encase 제품 소개

1. 제품 소개

✓ Network에 접속되어 있는 Server 및 PC들을 대상으로 침해사고 대응 및 내부 통제를 할 수 있는 기업 전용 **"보안 감시 및 통제 솔루션"**

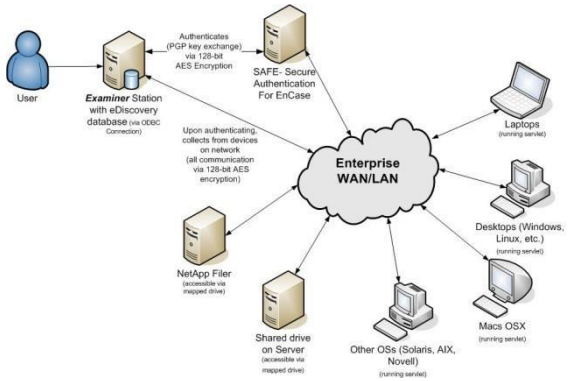
✓ 기업 내/외부 컴퓨터 보안 관련 사고에 즉시 대응, 보안 사고에 대한 정보를 수집, 분석, 증거 자료 확보 및 사전 감사 절차를 체계화 할 수 있는 **"통합 보안 평가 관리 체계"**을 제공

Encase 제품 소개(계속)

1. 제품 소개 (계속)

EnCase 기능

1. Encase 지원 OS
   - Windows FAT12(Floppy), FAT16, FAT32, NTFS
   - Macintosh HFS, HFS+
   - Linux EXT 2/3, Reiser
   - BSD FFS(FreeBSD's Fast File System 2 (FFS2) aka FreeBSD's UFS2)
   - Novell Netware v5.1 sp8, v6.0 sp5, v6.5
   - IBM's Journaling File System (jfs and JFS) and AIX LVM8
   - TiVo, including TiVo Series One and TiVo Series Two
   - CDFS, Joliet, DVD, UDF and ISO 9660
   - Palm
   - Sun Solaris UFS and HP-UX (vxfs) (COMING NEXT)



EnCase Endpoint Investigator 서비스 개요

Encase Software는 컴퓨터와 관련된 보안 침해사고에 실시간으로 대응하며 조사(감사)에 필요한 정보의 수집, 분석 및 증거 자료확보를 위한 ***Infrastructure***를 제공함으로써 효율적인 **"통합 보안 관리 체계"**를 지원합니다.

보안 침해사고 실시간 대응	부정행위 탐지 및 방어	디지털 문서 조사/감사
✓ IDS와 통합하여 내부/외부 사고에 적합한 대응 ✓ 정보감사와 디지털 자산 보호 ✓ **ZERO-DAY** 공격 대응	✓ 내부 통제 관리 ✓ 내부 정책 및 규정 통합 관리	✓ Timestamp을 통한 **디지털 문서의History관리** ✓ 고객 정보/내부 **기밀문서에 대한 통제 및 Tracking** ✓ 법정 소송 사건지원

EnCase Endpoint Investigator 서비스 개요

1. Encase Endpoint Investigator *일반 기능*

Non-Stop Operation 과학 수사솔루션

➢ **중요한 조직의 서버운용을 중단 없이 과학수사**

- 업무 중단 없는조사.

- 시스템의 휘발성 및 정적 데이터 분석.

- 방해 없이 대상서버, PC, 작업그룹을조사

완벽한 컴퓨터 과학 수사솔루션

➢ **휘발성 데이터에 실행중인 데이터를 빠르고 손쉽게 분류**

- Application, Open Port, File, Live window Registry.
- RAM에 상주한 모든 Program.

EnCase Endpoint Investigator 서비스 개요

1. Encase Endpoint Investigator *일반 기능(계속)*

현장 조사용 종합 솔루션

- 대상 네트워크 및 인프라와 무관한 정보검색.
- **시스템을 악용하는 행위** 또는 **삭제 시도**에 관계없이 정보검색.
- 복잡한 조사 작업의 자동화를 위한 맞춤형 Script 기능.
- - 포괄적인 조사를 신속히수행.

Encase Enterprise 제품 군 기능 요약

- 즉각적인 Preview 및 수집
- **비 간섭적인 휘발성 데이터 및 정적 데이타 수집 및 분석.**
- Time-Stamping 적용
- **Root Kit(Hacker Defender,..)**파악.
- 각종 다양한 플랫폼 / 파일 시스템 지원.

EnCase Endpoint Investigator 서비스 개요

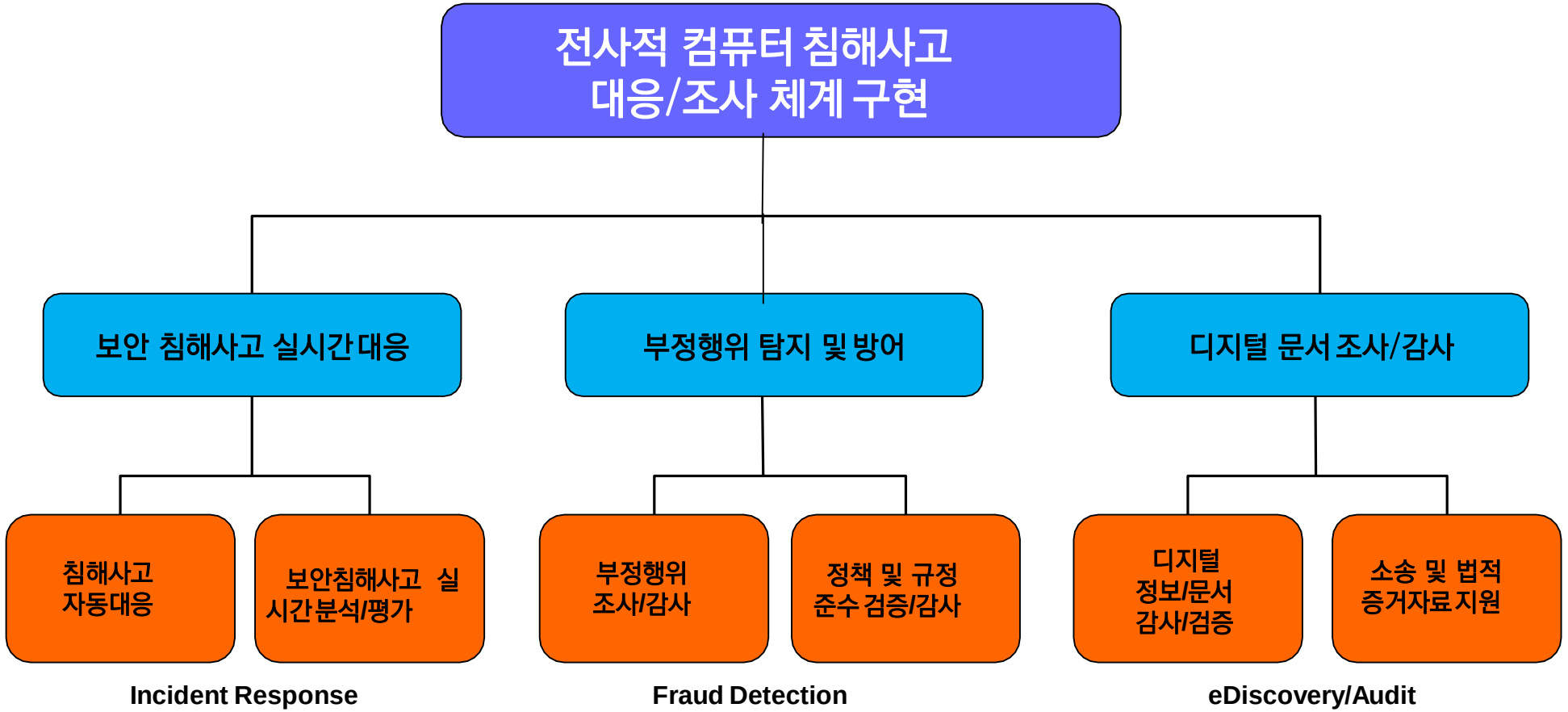
1. Encase Endpoint Investigator *일반 기능(계속)*

Encase Endpoint Investigator 제품 군 기능요약(계속)

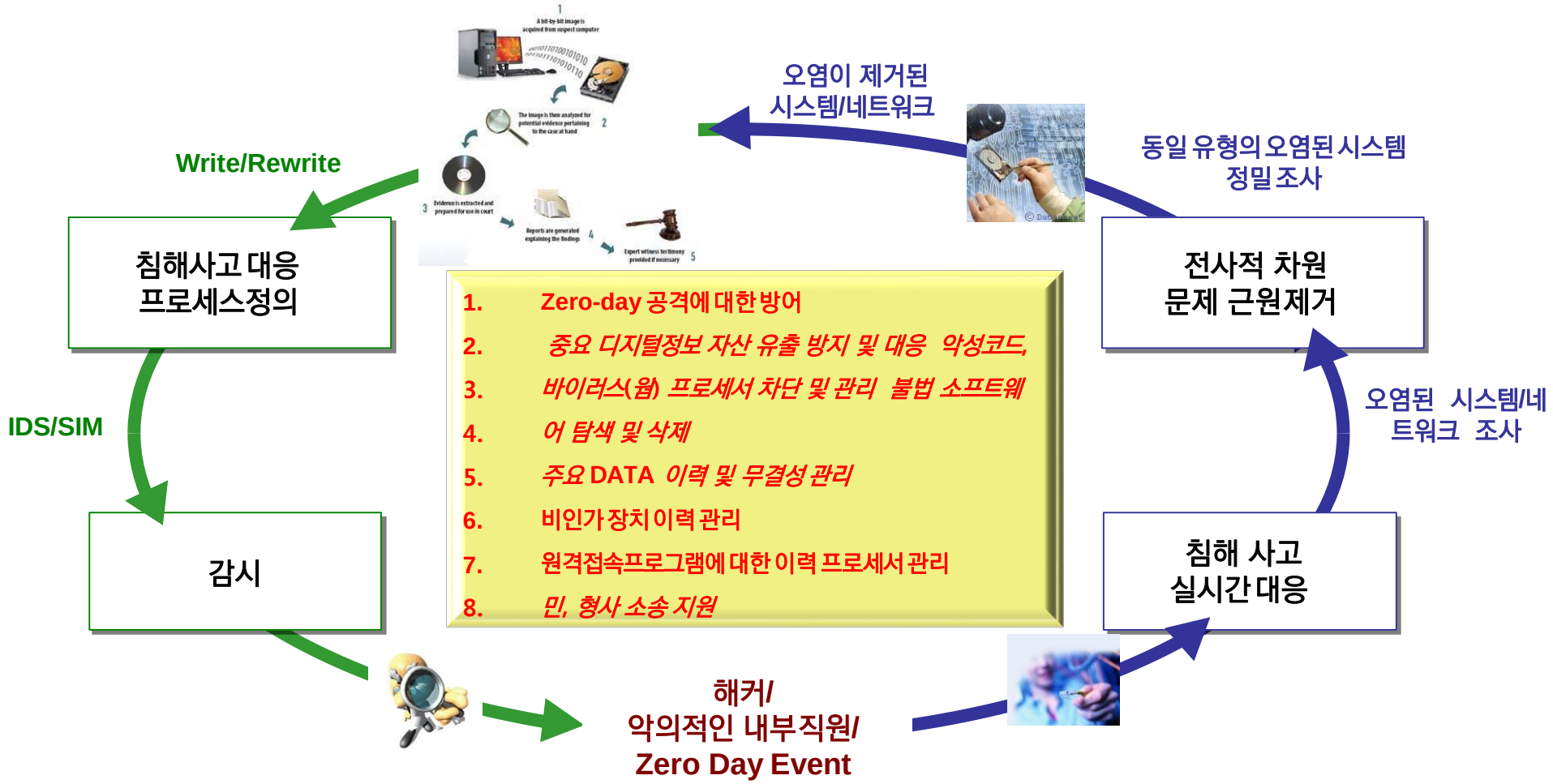
- 즉각적인 Preview 및 수집
- **비 간섭적인 휘발성 데이터 및 정적 데이타 수집 및 분석.**
- Time-Stamping 적용
- **Root Kit(Hacker Defender,..)**파악.
- 각종 다양한 플랫폼 / 파일 시스템 지원.

EnCase Endpoint Investigator 서비스 개요

1. Encase Endpoint Investigator 서비스

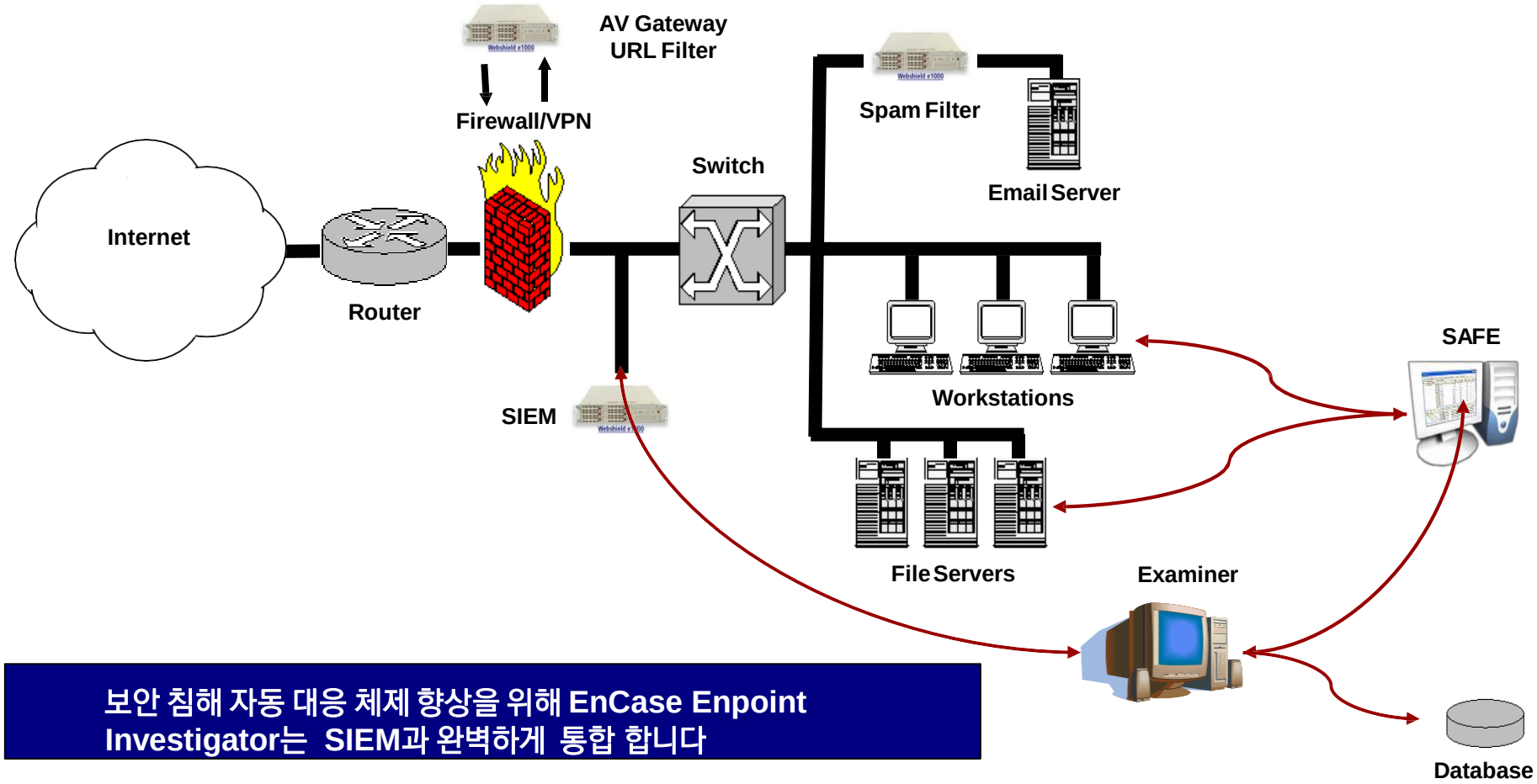


EnCase Endpoint Investigator 서비스 필요성 / 대응프로세스



EnCase Endpoint Investigator 구성

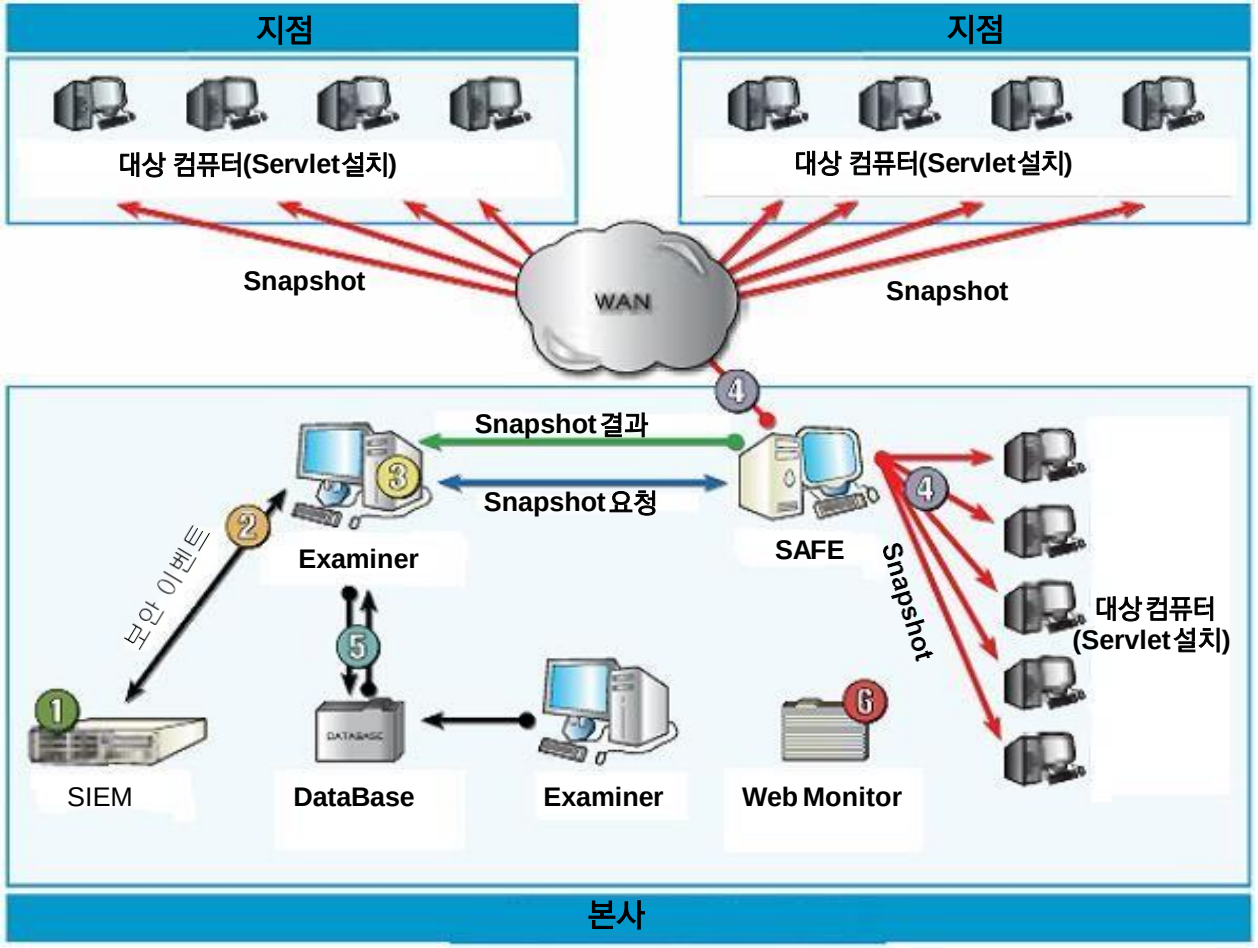
1. Encase Endpoint Investigator 보안 침해 자동사고 대응 및 원인분석



보안 침해 자동 대응 체제 향상을 위해 EnCase Enpoint Investigator는 SIEM과 완벽하게 통합 합니다

EnCase Endpoint Investigator 구성

1. Encase Endpoint Investigator 보안 침해 자동사고 대응 및 원인분석(계속)



① Network 이벤트 탐지를 위한 SIEM솔루션 과 연계, 연동

② EnCase는 주기적으로 SIEM 과 통신함

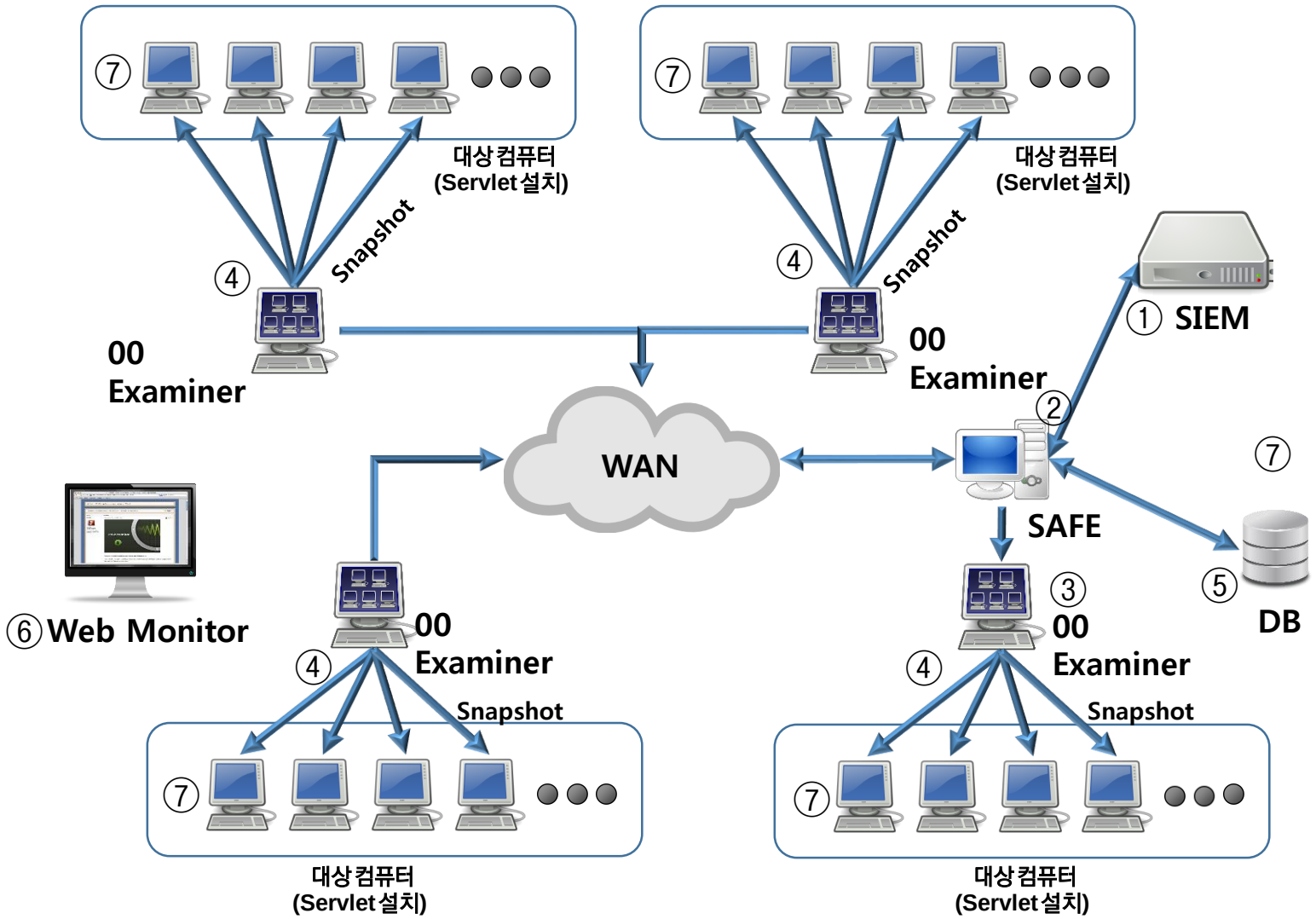
③ 특정조건 이벤트 발생시 Snapshot 준비

④ EnCase는 자동적으로 해당 컴퓨터에 Snapshot을 실시함

⑤ Snapshot 결과와 SIEM 이벤트는 DB에 저장됨

⑥ Web Interface를 통한 실시간 결과 분석 및보고

EnCase Endpoint Investigator 구성



① Network 이벤트 탐지를 위한 IDS/IPS

② EnCase는 주기적으로 SIEM 과 통신함

③ 특정조건 이벤트 발생시 Snapshot 준비

④ EnCase는 자동적으로 해당 컴퓨터에 Snapshot을 실시함

⑤ Snapshot 결과와 SIEM 이벤트는 DB에 저장됨

⑥ Web Interface를 통한 실시간 결과 분석 및보고

⑦ 전체 지점에서 사용 가능한 Node 수가 2000 Node 이므로 각 지점은 500여개의 자산을 순차적으로 Servlet 관리

EnCase Endpoint Investigator 구성

1. Encase Endpoint investigator 보안 침해 사고 자동 대응 및 원인분석(계속)

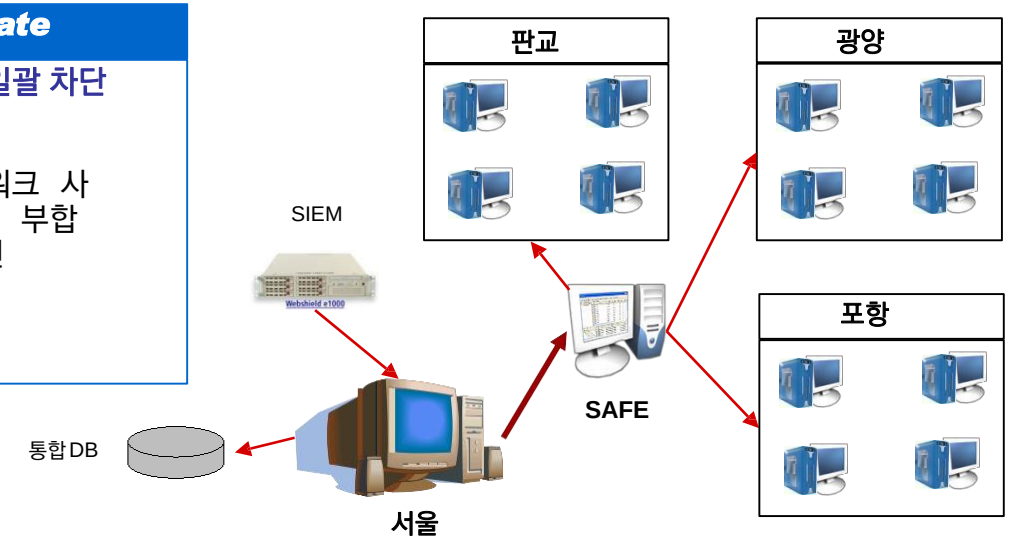
Trigger
- 네트워크 모의조사
- 새로운 Virus발견

Review Procedures
- 검색 유형
- Script 내용
- 검색 대상

SCAN
- 네트워크 일부 혹은 전반에 걸친 Script 실행
- 중요대상 노드 자동 점검

Analyze
- 검색 결과 분석
- 네트워크 기반과연계된 데이터 비교

Remediate
- 악성Process 일괄 차단
- 취약 PC 보완
- 검사결과와 네트워크 사용현황이 정책에 부합하는지 여부 확인



EnCase Endpoint Investigator 구성

1. Encase Endpoint investigator *보안 침해 사고 자동 대응 및 원인분석(계속)*

Trigger
- IDS/IPS 경고
- 보안 이벤트

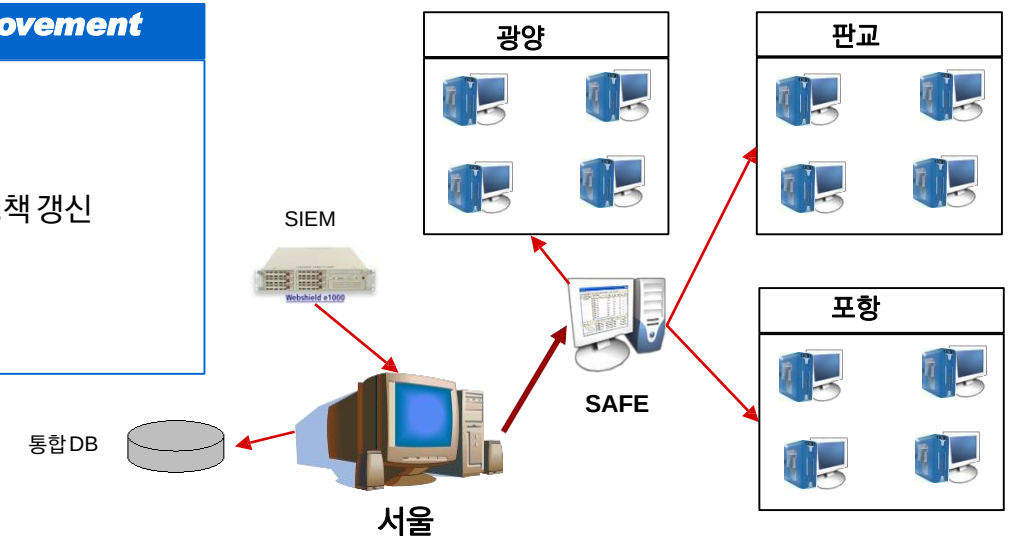
First Level Response
- 실시간 자동 Snapshot 확보(통합DB에 저장)

사전 정책에 의한 대응

Second Level Response
- IDS/IPS 경보에 의해 확보된 휘발성 데이터 검사
- EE를 이용, 해당 노드 조사
- 기존 Profile과 상이한 부분 확인

Remediate
- 감염 확인 노드 치료 (예, 악성파일/프로세스 제거)
- 사고 대응 완료
- 평가

Process Improvement
- 사고 내역 확인
- 소요시간 측정
- 취약점 확인
- 대응절차 및 보안정책 갱신



EnCase Endpoint Investigator 의 차별성

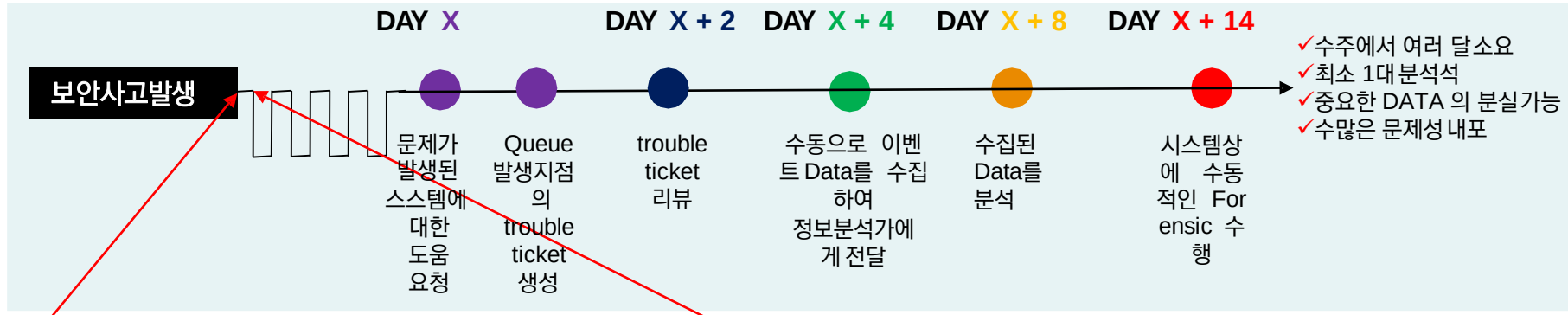
1. Encase Endpoint Investigator 비교

Depth Of Analysis	Encase’ Products	일반적인 조사툴
러닝 프로세스 탐지(Detect Running Processes)	O	O
히든 프로세스탐지(Detect Hidden Processes)	O	X
리네임 프로세스 나 드라이버 탐지 (Detect Renamed Processes or Dirvers)	O	X
러닝 서비스탐지(Detect Running Services)	O	O
악의적으로 삽입된Dll’s 탐지(Detect Malicious Injected Dlls)	O	X
루트키트 탐지(Detect Rootkits)	O	X
현재 로근온 된 사용자 식별(Identify Current Logged-on User)	O	O
자동실행된 레지스트리 키 열거(Enumerate Autostart Registry Keys)	O	X
히든 포트탐지(Detect Hidden Ports)	O	X
히든 레지스트리 키 나열(Identify Hidden Registry Keys)	O	X
상세한 리포팅제공(Provide Detailed Reporting)	O	X
머신 프로파일링(Machine Profiling)	O	X

EnCase Endpoint Investigator 의 차별성

2. Encase Endpoint investigator 의 대응 방법 비교

전통적인 자동대응 방법



EnCase Endpoint Investigator 도입 효과

1. Encase Endpoint Investigator 일반적 도입 효과

✓ **디지털자산 보호**

- **악성 프로세서검색 및 차단**
  - VIRUS, ROOT KIT, PROCESSOR 관리
- **소프트웨어 관리**
  - SERVER 및 PC의 소프트웨어 관리
- **DATA 무결성 관리**
  - 특허 관련 자료의 창출 이력관리
- **원격 접속 차단 및 감지**
  - HACKER 및 비 인가자의 접속 차단
- **비인가 장치의 접속 감지 및 확인**
  - USB, CD/DVD-RW, 등
- **출입통제**
  - 외부인력에 대한 디지털이력 확인
- **문서복구**
- **개인정보 / 중요 정보 유출**

✓ **기업내 정책 지원**

- **내부 사용자 설정**
- **불법소프트웨어 설치**
- **파이내셜 및 마아케팅자료 유출 방지**
- **퇴사자 DATA 관리**
- **법정 소송사건 지원**
- **산업스파이에 의한 유출사건 대응**

EnCase Endpoint Investigator 도입 효과

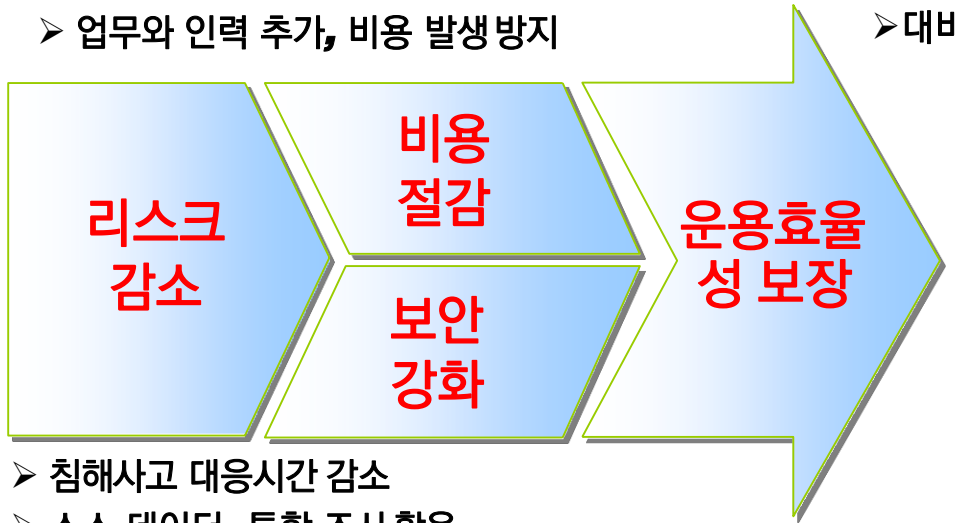
2. Encase Endpoint Investigator 구축 활용 및 예제

	Server	시스템 A	시스템 B
관리 대상	MEMORY	MEMORY	MEMORY
	DISK	DISK	P
데이터 관리	O	O	P
문서복구	O	O	P
비 인가통신수단 접속	O	O	O
원격 접속	O	O	O
프로세서관리	O	O	O
소프트웨어 관리	O	O	O
악성프로세서 검색 및 차단	O	O	O
중요정보유출	O	O	P
방문자 PC 관리	O	O	P

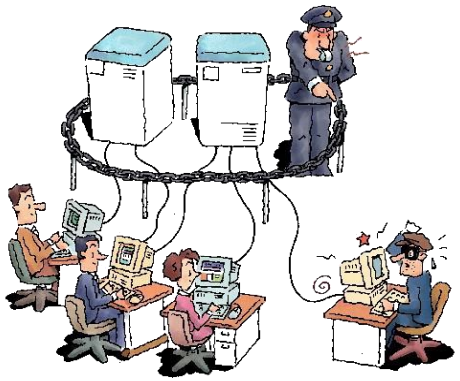
EnCase Endpoint Investigator 기대 효과

- 기밀정보 유출 방지
- 비정상행위 탐지 및 트래픽 분석
- 이메일, 키워드 등 유사성 분석
- 부적절한 정보교환 및 유출 방지

- 네트워크 트래픽 저장과 분석 자동화
- 업무와 인력 추가, 비용 발생 방지



- 보안 침해사고 / 기밀정보 유출 방지
- 대비 체제 확립



- 침해사고 대응시간 감소
- 소스 데이터 통합 조사 활용

- 네트워크 자원의 오남용방지, 생산성 강화.

- Zero Day 사건들에 즉시 대응가능
- 다운 타임 없이 컴퓨터 보안 사건에 대한 분석을 원격으로 수행 가능
- 네트워크 침입 사건의 철저한 원인분석
- 모든 사고에 대해 네트워크 포렌식 조사

EnCase Endpoint Investigator Reference