Guidance SOFTWARE™

EnCase® Cybersecurity

The Global Leader in Digital Forensics Solution

사이버 위협 탐지 및 대응을 위한 솔루션

EnCase Cybersecurity

정보보안 감사, 내부감사, 부정조사, IT 감사

기업정보 유출 조사, 개인정보 검색 및 추출, 디지털포렌식을 위한 솔루션

인섹시큐리티

디지털 포렌식 | 악성코드 분석 및 대응 | 취약점 진단 및 모의해킹 | 정보보안 전문기업

제품 요약

EnCase Cybersecurity

INSEC security

1. 제품 요약

- 제품명 : **EnCase Cybersecurity**
- 제조사 : 가이던스 소프트웨어(**Guidance Software**)
- 제품개요 : **(개인/기업) 정보유출조사, 보안감사, 침해사고, 디지털포렌식**
  - 보안 감사, IT 감사
  - 내부감사, 부정조사, 회계비리, 횡령조사
  - 기업정보유출조사, 개인정보유출조사
  - 디지털 포렌식, 서버 포렌식, 네트워크 포렌식
  - APT 공격, 악성코드 탐지 및 분석 등 관련 침해사고 조사
  - 사이버해킹범죄수사

1. 제품 요약 [계속]

- **제품 특징 / 장점**
  - 대부분 운영체제(OS) 지원 [Windows, MAC, AIX, HP-UX, Linux, Solaris 등]
  - 가상화 운영체제 지원
  - **기업정보, 지적자산(IP)** 등 중요 데이터에 대한 검색, 추출 및 삭제 기능
  - **개인 정보(PII)** 등의 중요 데이터 검색, 추출 [강력한 개인 프라이버시 보호 기능]
    - 삭제 파티션 복구, 삭제 데이터 복구, 은닉 데이터 탐색 및 추출 기능
    - 삭제된 개인정보 파일 탐색 기능
    - 비 할당영역 까지 개인정보 검색 및 추출 기능
  - **기업정보 및 개인정보 유출 사전 탐지 / 사후 조사 등 각종 흔적에 대한 증거 분석 및 조사**
  - 키워드(Keyword) 및 다양한 조건식 정의 및 검색 수행
  - 멀티 시스템 원격 조사 수행, 휘발성 정보, 메모리 덤프 수집 및 분석
  - 자동화 작업 수행 [스케쥴링 및 리포팅] 기능
  - 필요시 에이전트 설치 및 구동, 낮은 리소스 점유율

1. 제품 요약 [계속]

- **기대효과**
  - **개인정보 및 기업정보 검색 / 추출**
  - **개인정보 및 기업정보 유출 조사**
  - 내부감사, 부정조사, 회계비리, 횡령
  - 컴플라이언스, 정보보안 감사, IT 감사, 개인정보 보호 / 관리 / 통제
  - **디지털 포렌식, 서버 포렌식, 네트워크 포렌식**
  - 신속한 침해대응 및 확산 방지
  - **APT 공격 및 신종/변종 악성코드 탐지 및 조사**

회사 소개

2. 회사소개

- 회사명 : **Guidance Software**
- 설립 : 1997년
- 본사 위치 : Pasadena, Califonica
- 주요 사업 내용
  - **Enterprise Software Business :**

    EnCase® Cybersecurity, EnCase® eDiscovery, EnCase® Analytics
  - **EnCase Forensic, EnCase Portable, Tableau Kits**
  - **Professional Services, Customer Service and Technical Support, Training** 외
- 임직원수 : 600명

2. 회사소개 [계속]

- **제조사 소개**

  EnCase는 **Common Criteria EAL2**, DIACAP, FIPS 140-2에 대한 인증을 받았습니다.

  가이던스 소프트웨어사는 미국 내에 현재 19개의 특허를 가지고 있으며, 14개의 특허 신청을 해 놓았습니다.

  - **Department of Defense Information Assurance Certification and Accreditation Process Certified (DIACAP)**
    - EnCase는 보안 요구사항들을 충족시키고 국방부 네트워크 내의 작동을 인증 받음으로써 미 국방부 (DoD)로부터 DIACAP 인증을 받음.
  - **Federal Information Processing Standard (FIPS) 140-2**
    - 무결성 입증(증거의 조작 여부 입증) 기능을 포함한 암호화 알고리즘 인증
  - **Common Criteria Evaluation Assurance Level (EAL) 2**
    - CC(Common Criteria) 보안 평가 완료 후 EAL 2 수여

2. 회사소개 [계속]

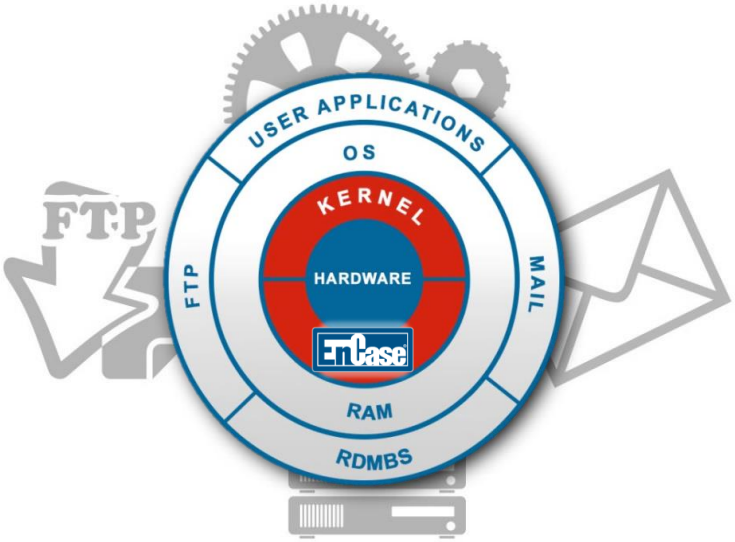
- **제안사 소개**

㈜인섹시큐리티는 GSI사의 국내 총판으로서 디지털 포렌식, 취약점 진단 및 모의해킹, 정보보안 분야의 대표기업으로 성장하기 위해 설립된 회사입니다. 기업정보 및 개인정보 관리 / 통제 / 유출 조사, 침해대응 분야에 포렌식 기술을 선도적으로 적용하고자 합니다.

- 회사명 : ㈜인섹시큐리티
- 설립 : 2005년
- 본사 위치 : 서울시 금천구 가산디지털1로 128
- 사업 분야 : 디지털 포렌식, 악성코드 분석, 취약점 진단 및 모의해킹 , 모바일 포렌식 등의 제품 판매 및 교육
- 주요 사업 내용 : EnCase 소프트웨어 판매
  - EnCase® Enterprise, EnCase® Cybersecurity, EnCase® eDiscovery, EnCase® Analytics
  - EnCase Forensic, EnCase Portable, EnCase Tableau Kit

중요 정보 및 악성코드 검색 / 탐지

[개인정보 | 기업정보 | 지적자산 | 악성코드]



3. 중요 정보 및 악성코드 검색 / 탐지

- **중요 정보 데이터에 대한 검색, 추출 및 삭제**
  - 기업정보, 개인정보, 지적자산 등 중요 데이터의 유출 방지를 위해서는 어디에 중요 정보들이 산재되어 있는가를 사전에 파악하는 것이 가장 중요합니다.
  - **EnCase Cybersecurity**는 개인정보, 기업정보, 지적 자산 및 각종 금융데이터의 완벽한 가시성을 확보하여 데이터 유출에 대한 위험을 사전에 제거할 수 있도록 합니다.
  - **EnCase Cybersecurity**는 정상 혹은 삭제 및 은닉된 형태의 주요 데이터를 가장 효과적이면서 포괄적으로 검색 가능토록 해줍니다.

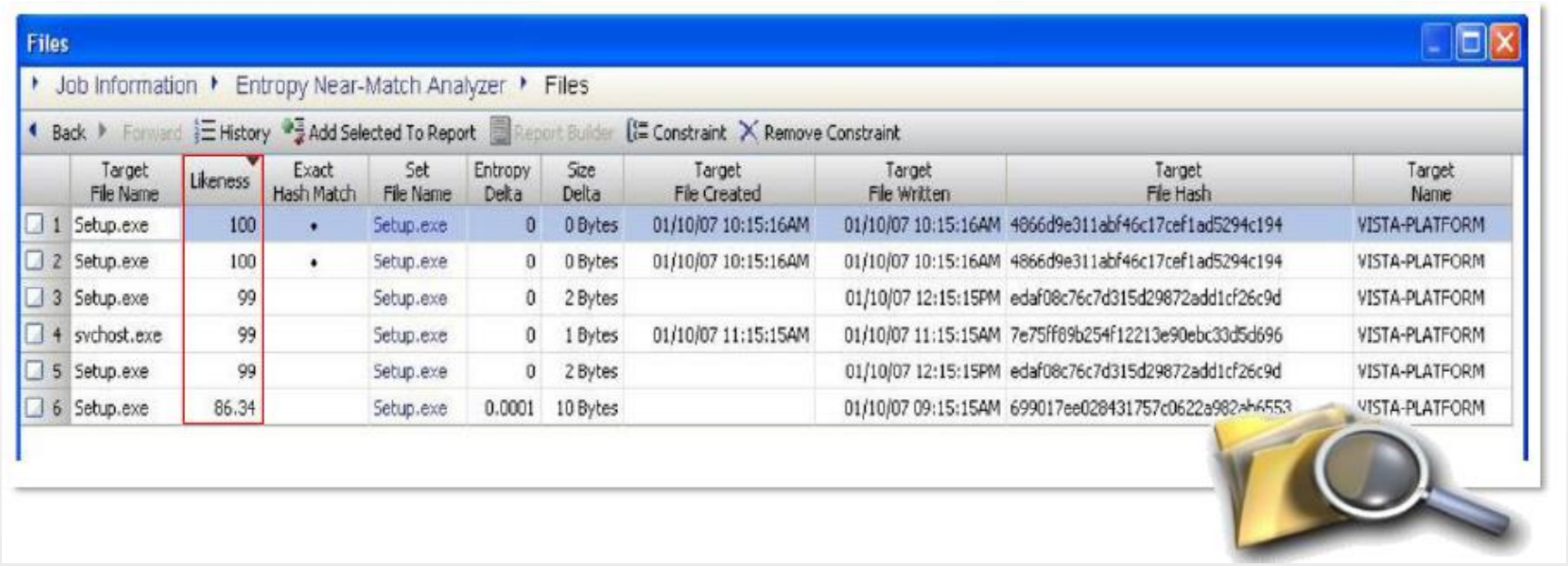
- **반복되는 정보유출 사고 방지를 위한 기준 제시**
  - **EnCase Cybersecurity**는 악성코드로 인한 정보유출 사고를 미연에 방지할 수 있습다.
  - **APT 악성코드, 신종/변종 악성코드를 탐지, 분석 및 차단할 수 있습니다.**
  - **EnCase Cybersecurity**는 반복적인 **개인정보 유출사고를 사전에 탐지 또는 방지할 수 있습니다**.

3. 중요 정보 및 악성코드 검색 / 탐지 [계속]

- **하드 디스크 및 메모리에 대한 철저한 검색 및 탐지**
  - **EnCase Cybersecurity**는 하드 디스크 및 메모리를 완벽하게 검색할 수 있습니다.
  - 삭제 파티션, 삭제 데이터, 비할당 영역에 대해서도 완벽한 검색 능력을 제공합니다.
    - 삭제된 데이터 검색
    - 비할당 영역 검색
    - 사용중인 데이터에 대한 분석
  - 주민등록번호, 신용카드번호 등 **개인정보(PII)**에 대한 다양한 패턴을 사전에 정의하여 주기적인 검색이 가능하도록 합니다.
    - 일정한 패턴을 가지기 어려운 중요한 데이터에 대해서도 다양하고 유연한 조합
    - 소스코드, 보안 분류된 문서, blueprints 등
    - 키워드 조합, Data 범위, 사용구문, 해시 값, Timeline 등

3. 중요 정보 및 악성코드 검색 / 탐지 [계속]

- **엔트로피(Entropy)를 통한 수정, 변조 등 은닉된 개인정보 및 중요 데이터 검색**
  - **원본 데이터를 변조시킨 은닉된 파일에 대한 유사도 비교 검색기능**을 제공합니다.
  - **Entropy Near Match** 기능을 통하여 **악의적으로 은닉되어 유출이 가능한 대량의 개인정보, 기업중요 정보, 지적 자산 등에 대한 검색, 탐지 및 삭제가 가능합니다.**



	Target File Name	Likeness	Exact Hash Match	Set File Name	Entropy Delta	Size Delta	Target File Created	Target File Written	Target File Hash	Target Name
1	Setup.exe	100	•	Setup.exe	0	0 Bytes	01/10/07 10:15:16AM	01/10/07 10:15:16AM	4866d9e311abf46c17cef1ad5294c194	VISTA-PLATFORM
2	Setup.exe	100	•	Setup.exe	0	0 Bytes	01/10/07 10:15:16AM	01/10/07 10:15:16AM	4866d9e311abf46c17cef1ad5294c194	VISTA-PLATFORM
3	Setup.exe	99		Setup.exe	0	2 Bytes		01/10/07 12:15:15PM	edaf08c76c7d315d29872add1cf26c9d	VISTA-PLATFORM
4	svchost.exe	99		Setup.exe	0	1 Bytes	01/10/07 11:15:15AM	01/10/07 11:15:15AM	7e75ff89b254f12213e90ebc33d5d696	VISTA-PLATFORM
5	Setup.exe	99		Setup.exe	0	2 Bytes		01/10/07 12:15:15PM	edaf08c76c7d315d29872add1cf26c9d	VISTA-PLATFORM
6	Setup.exe	86.34		Setup.exe	0.0001	10 Bytes		01/10/07 09:15:15AM	699017ee028431757c0622a982eb6553	VISTA-PLATFORM

3. 중요 정보 및 악성코드 검색 / 탐지 [계속]

- **신속한 조치 수행**
  - 검색과정에서 발견된 **허가되지 않은 개인정보, 기업정보, 지적자산** 등에 대하여 신속한 조치가 가능합니다.
    - 비 인가된 단말 또는 서버 등의 시스템에서 **개인정보, 기업정보 및 지적자산** 탐지시에 즉시 삭제 조치 수행
    - 기업 내부 사용자 PC에서 기타 중요 정보 탐지시 실시간 조치 가능
    - P-to-P 파일공유 프로그램에 대한 원격 삭제
    - **제로데이 공격, 신종/변종 악성코드** 등에 대한 탐지 및 즉각적인 원격 포렌식 기반의 침해대응 수행

Incident Response – 침해대응

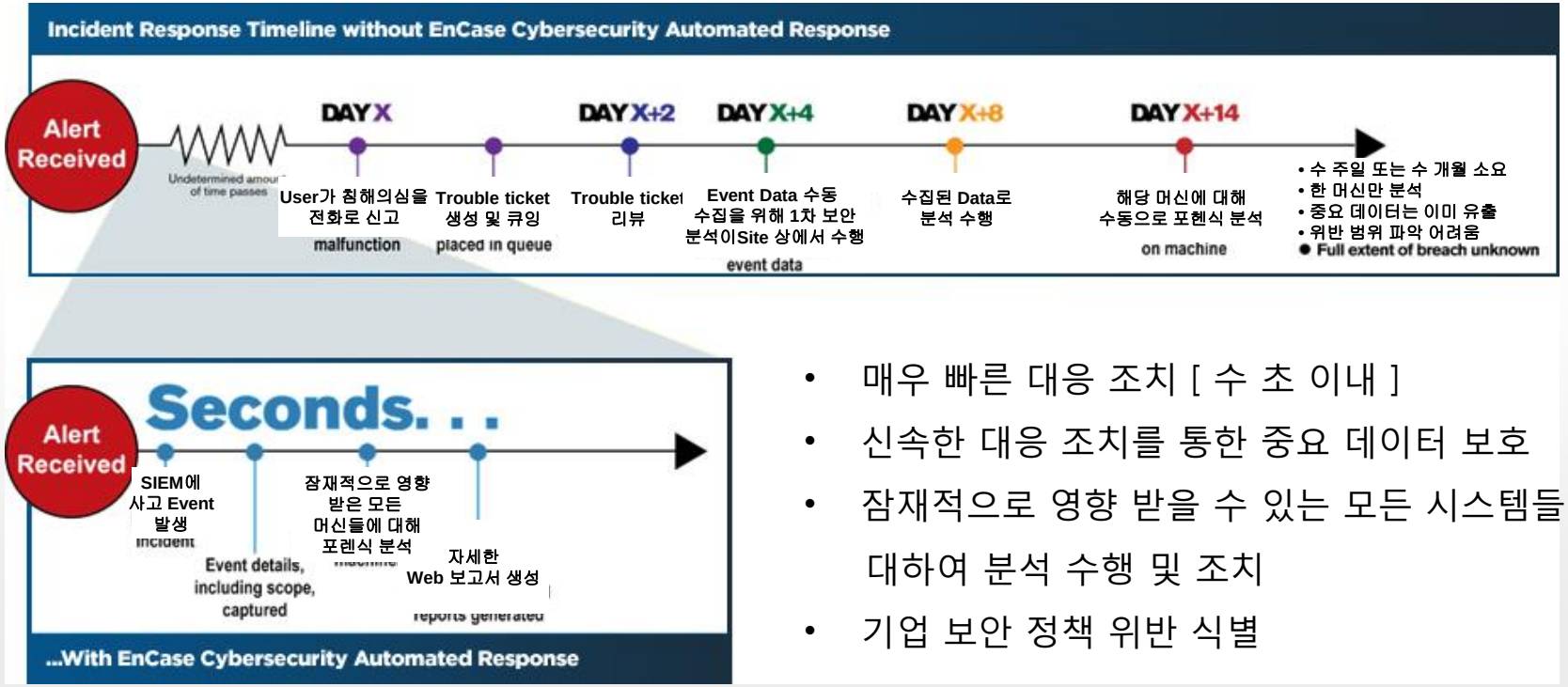
4. Incident Response [계속]

- **침해사고에 대한 분류, 조치, 자동화 대응**
  - **SIEM, ESM, IDS, IPS** 등의 시스템에서 수많은 경고(Alert) 이벤트들이 발생합니다.
  - 하지만 이러한 경고(Alert) 이벤트들은 공격의 범위와 어떠한 데이터가 공격받았는지 그리고 다음 공격대상이 무엇인지는 알려주지 못합니다.
  - **EnCase Cybersecurity**는 이러한 **경고(Alert) 이벤트들에 대하여 신속하고 자동화된 대응**이 가능하도록 합니다.
    - 기존 보안솔루션에서 탐지된 위협에 대한 실제적 확인
    - 위협의 근원지(source)와 침해 내용에 대한 평가
    - **개인 및 기업 정보유출 가능성 등 우선순위 선정 및 대응**
    - **개인정보, 기업정보 및 중요정보에 대한 즉각적인**

      삭제 및 와이핑(Wiping) 조치 수행

4. Incident Response [계속]

- **경고(Alert) 이벤트에 대한 신속한 대응 및 조치 [획기적인 대응 시간 단축]**
  - 경고 이벤트에 대한 대응체계로는 수일에서 수십 일의 오랜 시간이 소요됩니다.
  - **Encase Cybersecurity**는 이러한 대응시간을 **수분 또는 수십분 내로 신속한 대응이 가능**합니다.

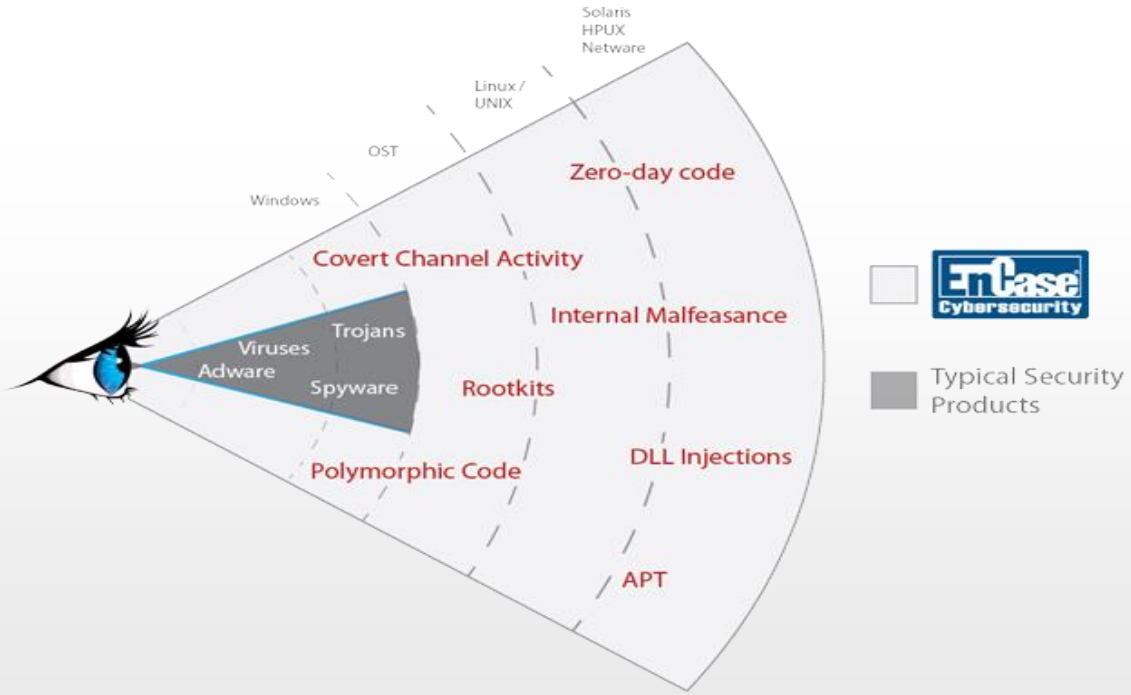


- 매우 빠른 대응 조치 [수 초 이내]
- 신속한 대응 조치를 통한 중요 데이터 보호
- 잠재적으로 영향 받을 수 있는 모든 시스템들에 대하여 분석 수행 및 조치
- 기업 보안 정책 위반 식별

4. Incident Response [계속]

- **사용자 PC 및 서버 시스템 등 엔드포인트(Endpoint)에 대한 가시성 확보**
  - 패턴 위주의 탐지방식 또는 Windows 운영체제에 한정된 솔루션과 달리,

    Encase Cybersecurity는 다양한 운영체제(OS)에 대한 지원이 가능합니다.
  - 사용자 PC 및 서버 시스템에 대한 제한 없는 엔드포인트에 대한 가시성을 확보해 줍니다.



Automated Response & Remediation

– 자동화 침해사고 대응 및 조치

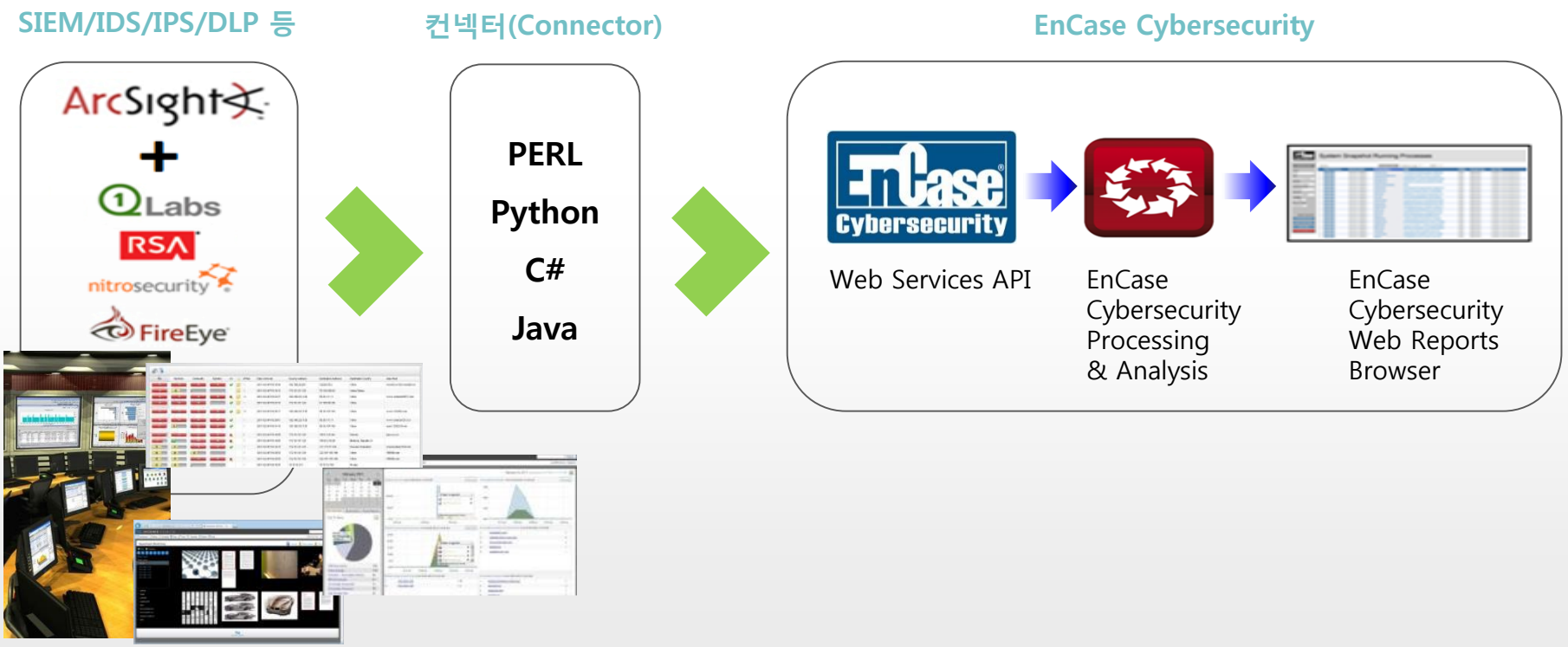
5. 자동화 침해사고 대응 및 조치

- **원격 포렌식**
  - **디스크 기반의 디지털포렌식 기술 수용, 파티션 복구, 삭제 데이터 복구 등 디스크 증거분석**
  - **다중 시스템에 대한 원격 네트워크 포렌식 조사 수행**
  - 보안정보이벤트관리(SIEM) 솔루션과 연동하여 자동화 포렌식 조사 수행

- **원격 포렌식 장점**
  - **시스템의 중단 없이** 분석이 가능하여 현업 업무 손실을 최소
  - **동시에 다수의 시스템에 대한 분석이** 가능하여 분석 업무의 효율성 증대
  - 업무 외 시간에도 스케줄링 된 분석이 가능하여 분석시간을 절감
  - 침해 행위에 대한 신속한 분석 가능
  - SIEM / ESM, FireEye 등 타 보안 솔루션과의 연동 구성 및 분석에 대한 유연성 제공
  - **HP ArcSight, Splunk, IBM QRader, RSA enVision, FireEye**와 연동하여 자동화 침해대응 구현

5. 자동화 침해사고 대응 및 조치 [계속]

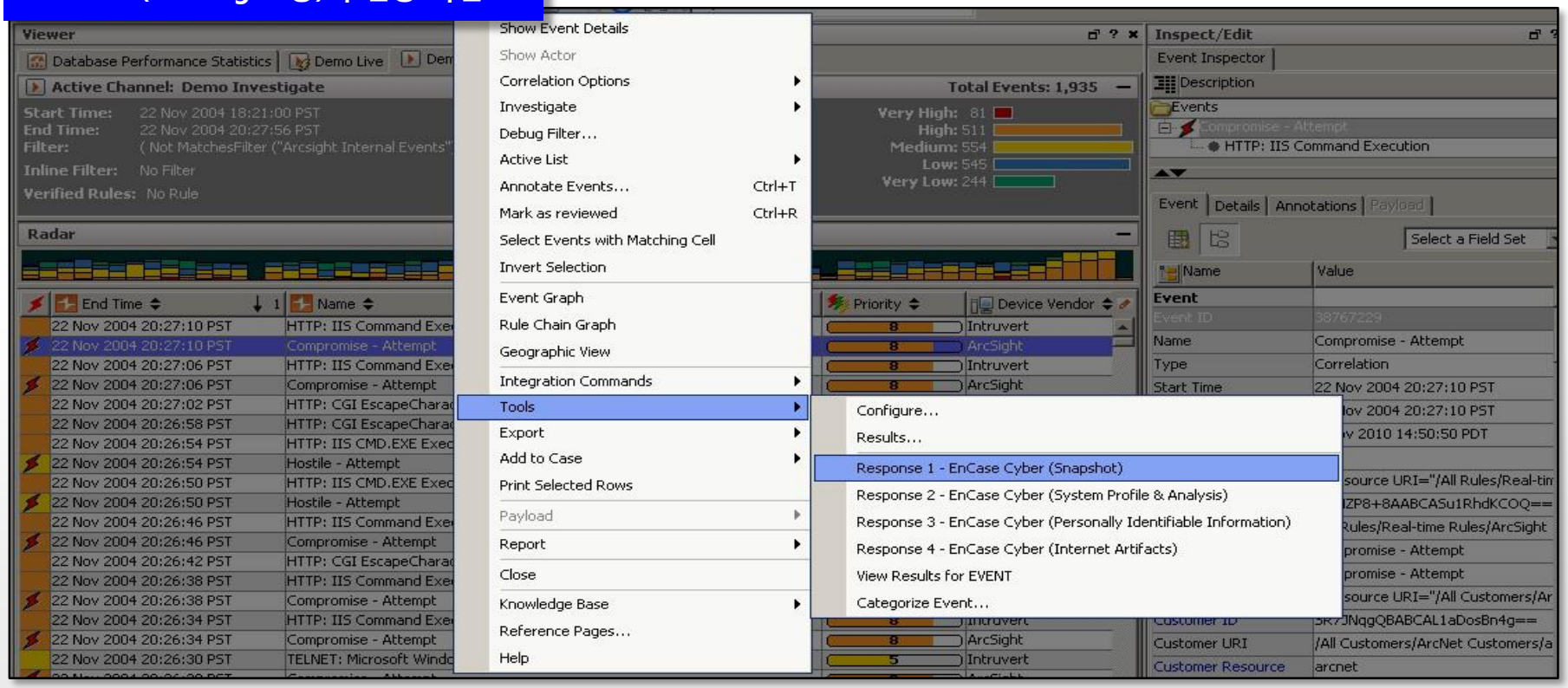
- **자동화 침해대응 기능**
  - **HP ArcSight, Splunk, IBM QRader, RSA enVision, FireEye** 등 탐지솔루션과 연동 구현



5. 자동화 침해사고 대응 및 조치 [계속]

- **HP ArchSight** 와의 연동 구성을 통한 자동화 분석 프로세스

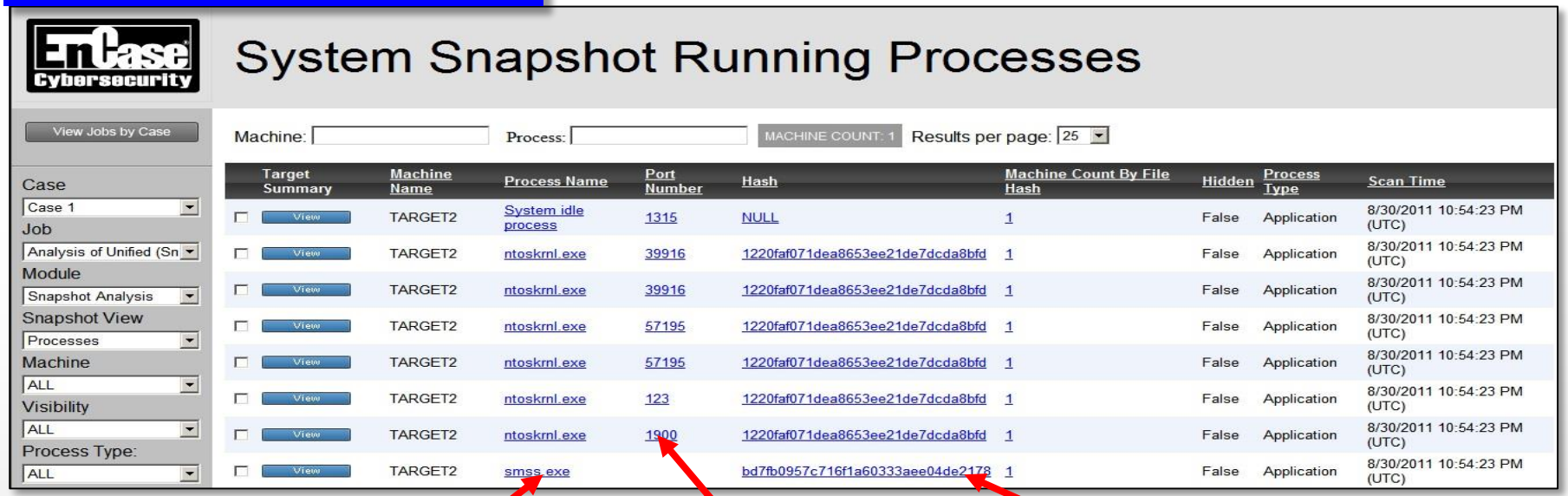
SIEM (ArchSight 등)과 연동 화면



5. 자동화 침해사고 대응 및 조치 [계속]

- **HP ArchSight** 와의 연동 구성을 통한 자동화 분석 프로세스

브라우저 기반 View 방법



실행 중인 프로세스 이름

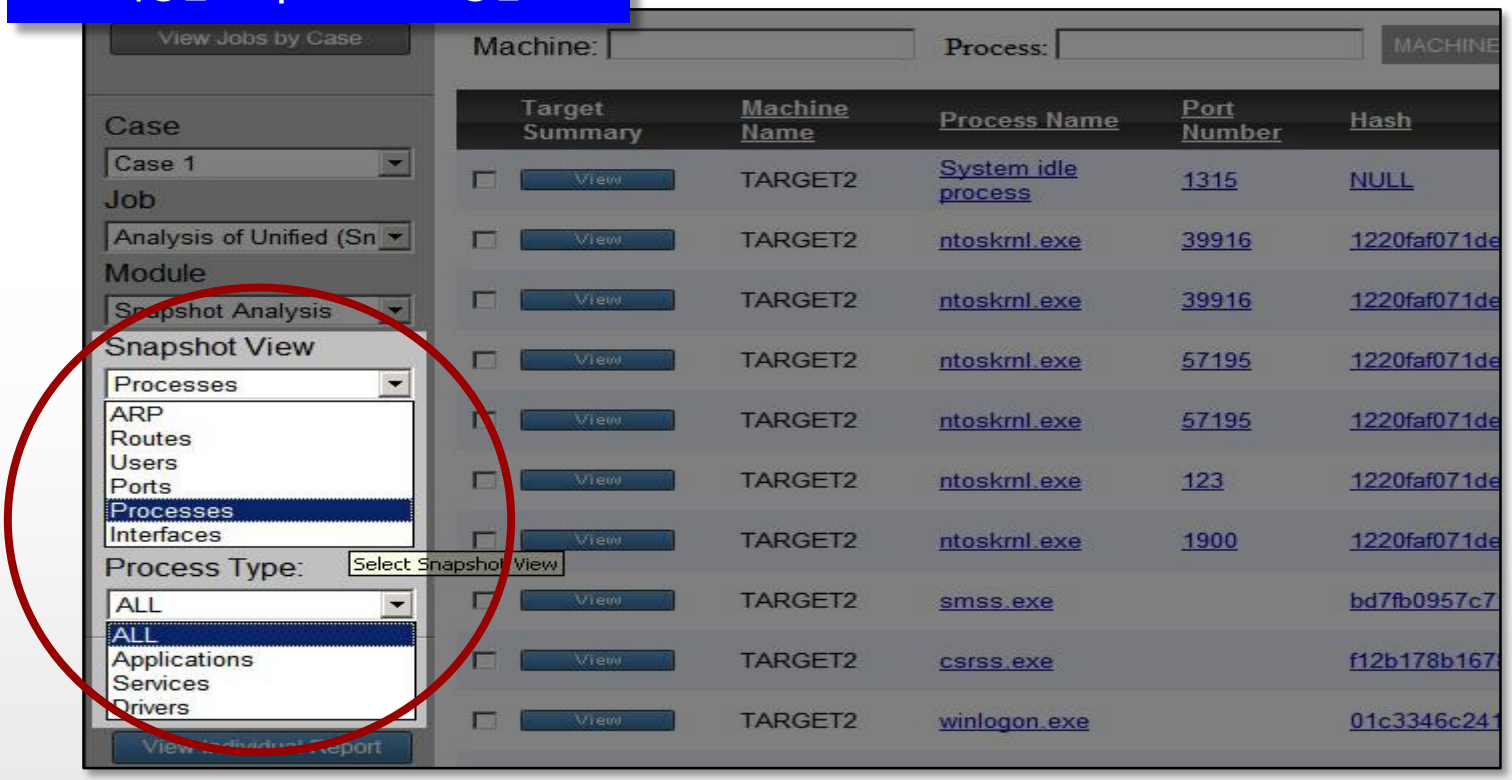
오픈 포트

프로세스 해시 값

5. 자동화 침해사고 대응 및 조치 [계속]

- **HP ArchSight** 와의 연동 구성을 통한 자동화 분석 프로세스

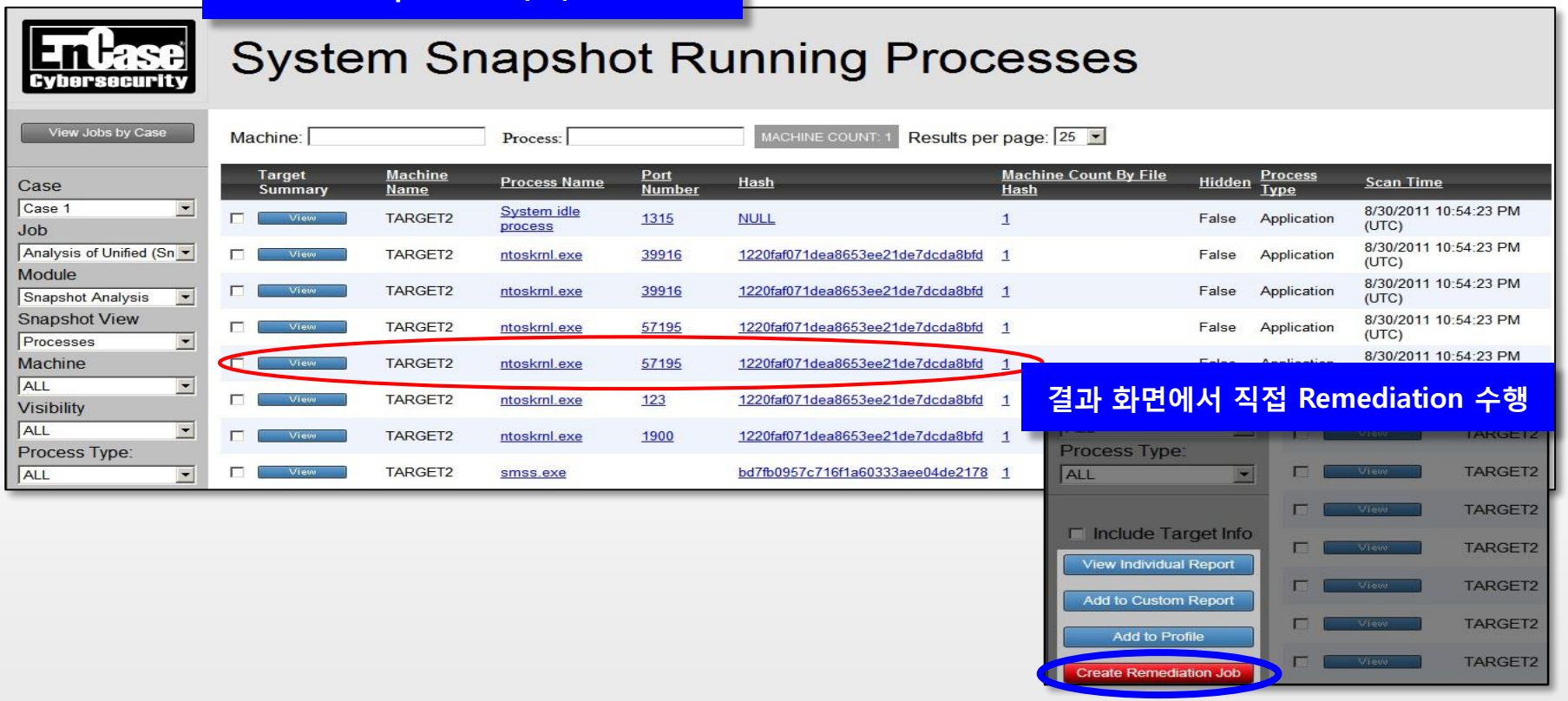
다양한 Snapshot View 방법



5. 자동화 침해사고 대응 및 조치 [계속]

- **HP ArchSight** 와의 연동 구성을 통한 자동화 분석 프로세스

Snapshot 결과 화면



Cybersecurity 제품소개

It's not if
you will be breached...

it's when

6. Cybersecurity 제품 소개

- **EnCase Cybersecurity**는 **사이버해킹범죄조사** 소프트웨어로서 **중요 정보 유출 사고 위험을 줄이고 악성코드 및 해킹 침해사고 대응의 복잡성, 비용, 시간 등을 줄이기 위해**, 스케줄링, **자동화 대응 조치**, 위협 레벨(Threat Level) 분석 및 **엔트로피(Entropy)** 기능들을 종합하여 설계되었습니다.

EnCase Cybersecurity

- 보안 감사 / IT 감사 / 부정거래조사 등
- 개인/기업 정보유출 조사
- 은닉된 위협 식별
- 침해사고 대응 및 복구
- 다중 시스템 / Network 침해 조사

- System Profiling 및 분석
- Malware Entropy Near-Match 분석
- 악성코드 및 프로세스 행위 분석
- 신속한 조사 및 증거수집
- 삭제 / 은닉 데이터 복구 및 탐지

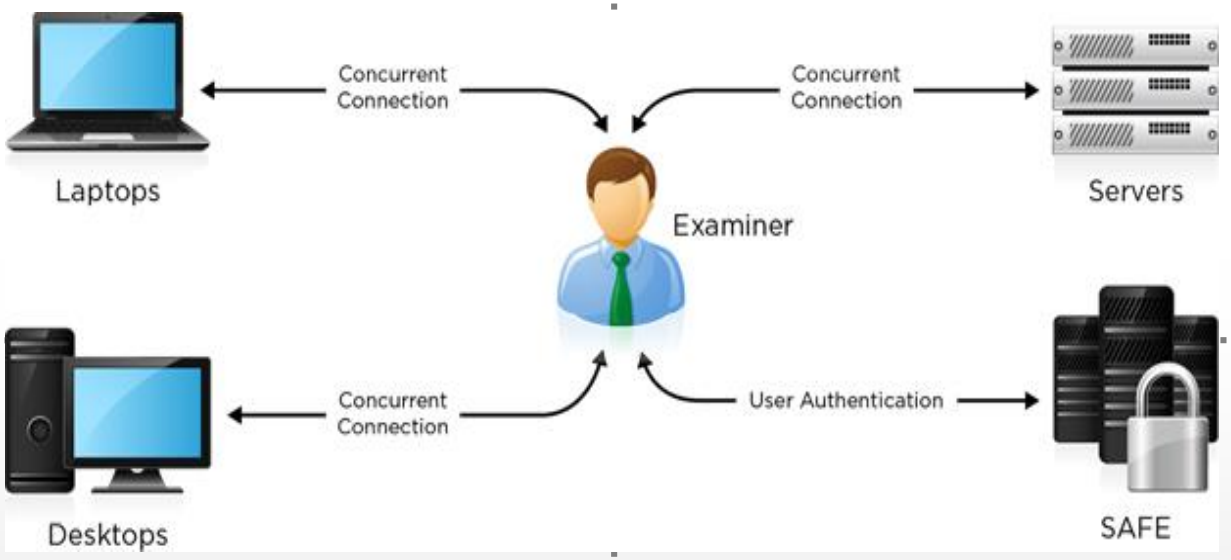
SAFE | **Examiner**

Servlet | **EnCase Enterprise**

6. Cybersecurity 제품 소개 [계속]

SAFE
[Secure Authentication For EnCase]

Servlet
[On Target Nodes]



Cybersecurity Examiner

EnCase Enterprise

6. Cybersecurity 제품 소개

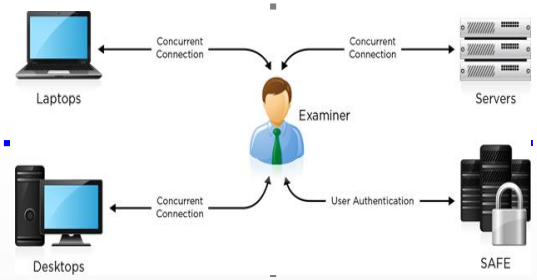
SAFE

- 사용자 계정**(Examiner)** 생성, 인증, 접근권한 **PKI** 인증, 보안 로그인을 제공
- 조사자**(Examiner)**와 서블릿**(Servlet)** 간의 통신 암호화 지원 **(128Bit AES**로 암호화된 테이터 스트림 사용**)**
- 타킷**(Target)** 시스템에 접근할 수 있는 사용자를 관제 및 통제

Servlet

- 필요시 또는 지속적으로 조사 대상 컴퓨터 또는 서버 시스템에 설치
- 기존 시스템 및 소프트웨어와 충돌 없이 설치 및 구동 **[Passive S/W Agent]**
- 통신 포트**(Port)**와 프로세스**(Process)** 이름 등은 사용환경에 맞게 설정 가능
- 조사자**(Examiner)**가 인증서버**(SAFE)**를 통한 인가된 명령을 내릴때까지 시스템에서 비활성화 상태

[다양한 운영체제 지원]
- Windows, AIX, OSX, Solaris HPUX, Linux등



- 조사자의 컴퓨터에 설치되어 침해대응, 조사 수행
- 조사자 **SAFE** 인증 후 권한을 부여 받은 후 대상 네트워크 노드 조사, 검색, 탐지 및 조치**(Remediation)** 업무 수행
  - 데이터 보안감사, 내부감사, 부정조사 모듈
  - **System Profiling & analysis module**
  - 엔트로피 분석기 **[Entropy Set Analyzer]**
  - 시스템 위협 레벨 모듈**[System Threat Level Module]**
  - 자동화 침해대응 모듈 **[EnCase Cybersecurity connector]**

Cybersecurity Examiner

- **Cybersecurity Examiner**와 컴퓨터간 가상 보안 접속
- 동시 연결**(Concurrent Connection)** 수는 동시에 분석할 수 있는 컴퓨터의 수량을 의미 **[** 구입 **License**에 따라 달라짐 **]**
- 복수 컴퓨터를 논리적 / 물리적 차원에서 개별적으로 분석, 검사, 검색, 탐지, 조치 수행
- 데이터를 수집하고 확보

EnCase Enterprise