EnCase 포렌식부터 EDR까지, 진단에서 추적에 이르는 토탈 가시성 확보!

May 18

OpenText Korea 정택준 위원

opentext™

opentext™

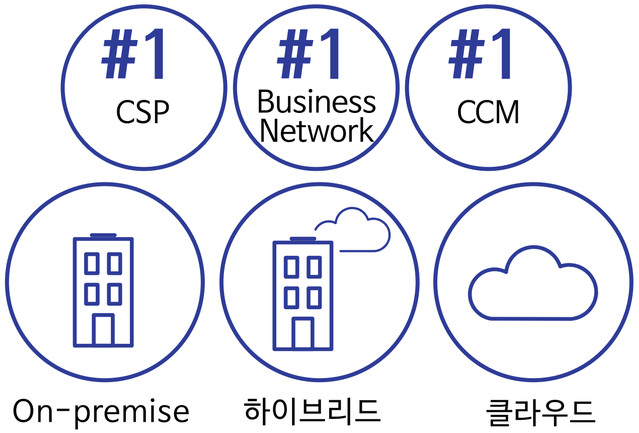
NASDAQ, TSX: OTEX
A TSX-60 Company

OpenText는 기업 소프트웨어 및 클라우드 솔루션을 위한 EIM 업계의 선두주자로서,
조직 내외부의 다양한 정보를 원활히 연결하여 똑똑하게 일할 수 있는 환경 조성을 지원합니다.

#1

EIM

클라우드 및 On-premise



$2.9 B
FY19 매출

13,100+
임직원

100M
사용자

120,000
고객사

80%
포춘 1000대 기업

60M
Secured IDs

29년
혁신의 시간

1,250+
파트너

40M
안전한 엔드포인트

104개
전 세계 오피스

35개
국가

3 Exabyte
관리 중인 데이터

OpenText 인수 기업*

- Year Founded — 1991
- NIRV Center / NirvCentre — 1995
- InfoDesign — 1995
- SoftCore — 1995
- Network Software Group (NSG) — 1996
- Information Dimensions — 1997
- LAVA Systems — 1998
- Bluebird Systems — 1999
- BRS/Search Query Server — 1999
- Open Image — 2000
- Centrinity — 2002
- Artesia — 2003
- IXOS Software — 2003
- Vista Plus — 2004
- BitFlash — 2004
- Hummingbird — 2006
- eMotion — 2007
- Spicer Corp — 2008
- Captaris — 2008
- Nstein — 2009
- Burntsand — 2010
- New Generation Consultants — 2010
- StreamServe — 2010
- Easylink — 2012
- GXS — 2014
- Acquired Select CEM and CCM Assets from HP — 2015
- ANXeBusiness, LLC. (ANX) — 2016
- Recommind — 2016
- Liaison — 2017
- Hightail — 2018
- Odesta — 1995
- Intunix — 1995
- Internet Anywhere — 1995
- Campbell Services — 1997
- Microstar Software — 1999
- PSSoftware Solutions — 1999
- TierTwo Systems — 1999
- Base4 — 2001
- Gauss Interprise — 2003
- Eloquent — 2003
- Corechange — 2003
- SER Solutions Software, Austria — 2003
- SER eGoverment Deutschland — 2003
- EDC Solutions — 2003
- Optura — 2005
- Momentum Systems — 2007
- Vignette — 2009
- Vizible — 2009
- Metastorm — 2011
- weComm — 2011
- Global 360 — 2011
- Operitel — 2011
- MESSAGEmanager Solutions — 2011
- Resonate KT — 2013
- ICCM Solutions — 2013
- Cordys — 2013
- Informative Graphics Corporation (IGC) — 2015
- Actuate — 2015
- Daegis — 2015
- Acquired Dell EMC's Enterprise Content Division — 2017
- Covisint — 2017
- Guidance Software — 2017
- Catalyst — 2019
- Carbonite — 2019

(*) Calendar year 기준으로 작성된 타임라인입니다.

OpenText 보안 포트폴리오

Train | Block | Protect | Backup | Recover

WEBROOT®
an opentext™ company

- Security Awareness Training
- BrightCloud Threat Intelligence
- DNS Protection
- Business Endpoint Security

opentext™

- Core Share
- Core Signature

GUIDANCE SOFTWARE
an opentext™ company

- EnCase Security
- EnCase Forensic
- Tableau

CARBONITE®
an opentext™ company

- O365 Backup
- Server Backup
- Recover
- Availability

OpenText 보안 제품군

시장을 선도하는 포렌식 및 보안 솔루션

eDiscovery

전자 증거 개시를 위한 증거물의 보존, 수집, 검토 및 생산에 이르기까지 필수적인 EDRM 기능을 제공하는 솔루션

- EnCase eDiscovery

디지털 포렌식

수사 기관과 일반 기업에서의 조사를 위해 포렌식 기반의 증거물 수집 및 분석 기능을 제공하는 솔루션

- EnCase Endpoint Investigator
- EnCase Forensic
- EnCase Mobile Investigator
- Tableau

Endpoint Detection & Response(EDR)

사이버 위협 탐지, 사고 대응 및 대상 시스템의 격리/치료 기능을 제공하는 솔루션

- EnCase Endpoint Security

모든 EnCase 제품군을 PC에서 하나의 Agent로 관리 가능하며, 전 세계 약 4천만대 이상 PC에 Agent 설치 후 운영

EnCase Forensic

Software Utilities

단순 하드웨어 뿐만 아니라, 하드웨어의 가치를 확장하기 위한 소프트웨어

Forensic Bridges

휴대성을 강조한 디지털 미디어에 대한 안정적인 하드웨어 기반 쓰기 방지 기능(Write-Blocker)

Forensic Imagers

현장 또는 분석실에서 저장매체의 증거자료를 획득할 수 있는 고속 복제 및 이미징 장비

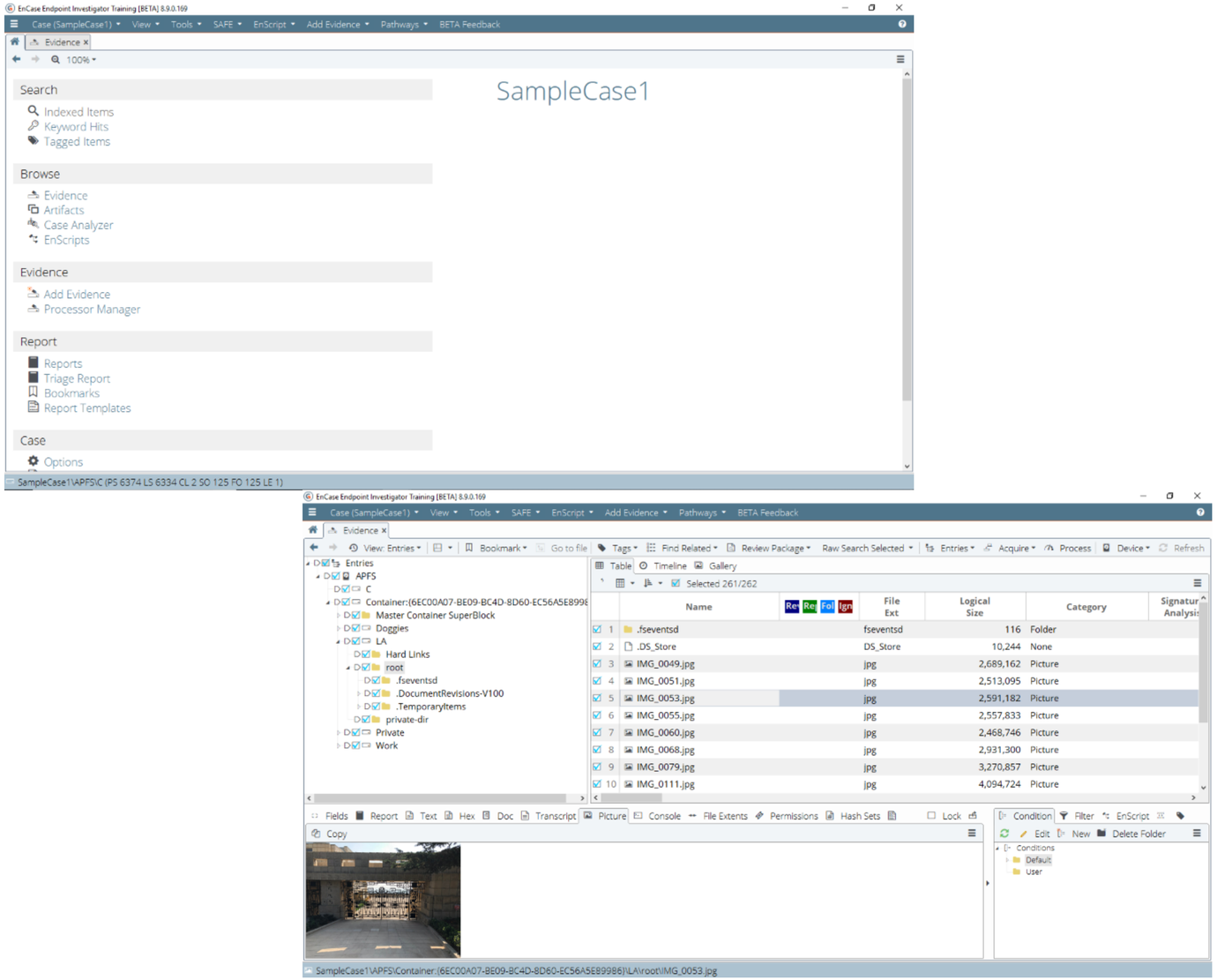
Password Recovery

Passware와 EnCase가 협력하여 암호 복구를 위한 Brute-Force 공격을 향상시킨 맞춤형 하드웨어

Accessories

다양한 저장 매체 유형들로부터 증거를 수집할 수 있도록 맞춤 설계된 어댑터와 케이블

EnCase Endpoint Investigator



- **주요 기능**
  - **비 접속 Endpoint로부터의 정보 수집:**

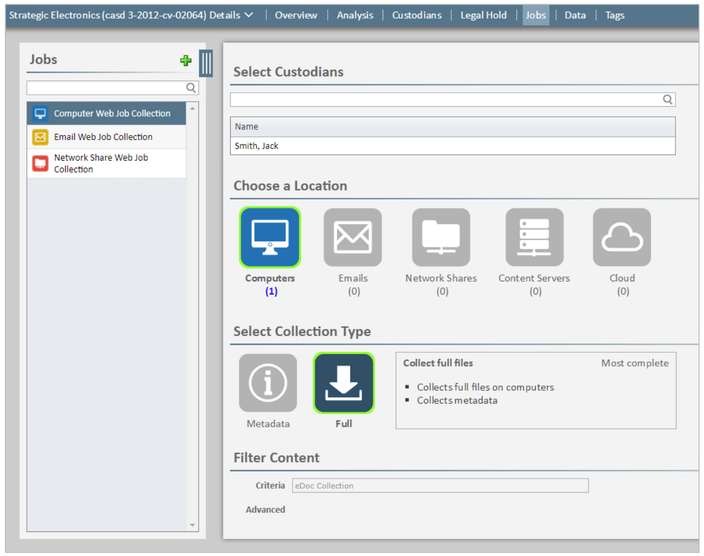
    EnCase Enhanced Agent를 활용하여 조사를 진행하는 담당자는 직원이 네트워크에 연결되어 있거나 접속되어 있지 않더라도, 대상 Endpoint 에서 관련 정보를 검색하고 수집할 수 있음
  - **다양한 장치와 광범위한 OS 지원:**

    Microsoft® Windows®, Linux®, Apple® Mac® 및 UNIX® 등의 광범위한 운영체제를 지원하고 있고, 26,000개가 넘는 모바일 프로파일을 수집하고, 전자 메일, 문자 메시지, 브라우저 증거물 등 주요 데이터들을 분석할 수 있음
  - **지역에 관계 없이 원격 접속 및 수집:**

    Endpoint 자산이 전 세계 어디에 존재하더라도, 담당자가 원격으로 접속하여 증거물을 수집하고 분석할 수 있음
  - **법적으로 채택 가능한 증거물 수집:**

    증거물을 원격으로 수집하였다고 하더라도, 전세계 법원에서 인정하고 입증된 EnCase Evidence File(LEF) 형식으로 증거물을 저장

EnCase eDiscovery



EnCase eDiscovery의 Agent는 7개의 운영체제를 지원하고, VM머신 혹은 일반 머신을 지원하며, 원격으로 배포가 가능

- **주요 기능**
  - **수집:**

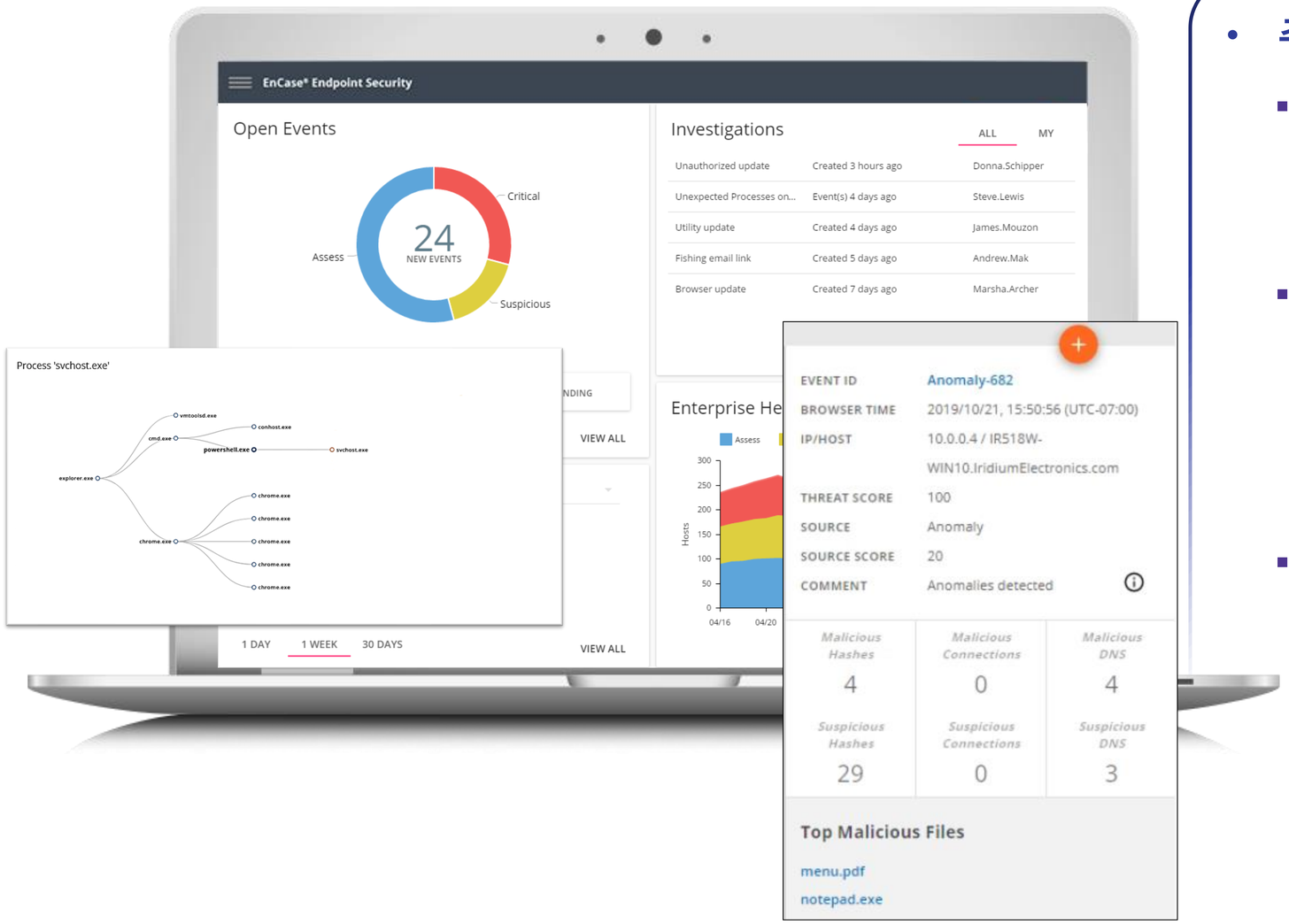
    일상 업무에 방해 없이 수 십만의 Endpoint으로부터 증거물 수집하고, 다양한 시스템(이메일, 네트워크 공유 폴더, 클라우드 등)으로부터 수집 가능
  - **프로세싱과 컬링:**

    완전히 자동화된 통합 도구로 다양한 유형의 증거물들의 중복 제거 및 식별 가능
  - **증거물 보존:**

    전세계 법원에서 인정하고 입증된 EnCase Evidence File(LEF) 형식으로 증거물 저장

더욱 완벽하게 EDRM을 커버하기 위해, 증거물들에 대한 검토와 분석 그리고 생산 기능 향상시킬 수 있는 Recommind의 Axcelerate와 Catalyst의 Insight를 통합하는 작업을 진행 중에 있음

EnCase Endpoint Security



- **주요 기능**
  - **Advanced 위협 탐지:**

    Endpoint들의 실시간 감시 기능, MITRE ATT&CK 기반의 기본 악성 행위 룰 셋 제공 및 업체의 보안 정책에 부합하는 별도의 자체 악성 행위 룰 작성 가능
  - **가시성 확보 및 경고 알림 선별:**

    SIEM, IPS/IDS 등의 솔루션들과 연결되어 Webroot의 BrightCloud에서 제공하는 위협 평판 점수 및 정보를 바탕으로 경고에 대한 가시성을 확보하고, 동적 분석(샌드박스) 서비스를 통하여 0-day 대응을 위한 정보를 제공
  - **적극적인 대응:**

    의심 대상 Endpoint에 대한 격리가 가능하고, 포렌식 수준의 조사를 통해 공격에 대한 식별 및 Actionable 정보를 제공함으로써, 사용자가 직접 비정상 행위에 대한 탐지 룰 제작 및 적용 가능

EDR(Endpoint Detection & Response) 소개

디지털 위협의 증가

52%의 공격
2017년, 발생한 전체 공격 중 File-less 공격 빈도
– SC Media

$864억
2017년, 집행된 InfoSec에 대한 비용
– Gartner

60억
2022년까지 인터넷 이용자
– Cybersecurity Ventures

$6조
2021년까지 사이버 공격에 의해 연간 발생할 피해
– Cybersecurity Ventures

1만 5천건 이상의 유출 사고
2017년, 1만 7천 4백만 기록 유출
– ITRC

EPP-EDR

예방이 무엇보다 중요하지만 EPP만으로는 효율적이지 못함

Attacks on your organization

Tens of thousands attacks daily

EPP
(AV replacement) may block **up to 99%** of attacks

An estimated **1%** may get through

EDR
(Endpoint detection & response) **necessary** for breach remediation

Organizations spend **$12B annually** on prevention

Successful attacks cost $500B annually
Ponemon institute 2016

- IRS — inside USB job
- Ashley Madison — mass extortion
- Yahoo! — millions of user credentials
- Scottrade — millions of records
- FDIC — Chinese hackers
- Your organization

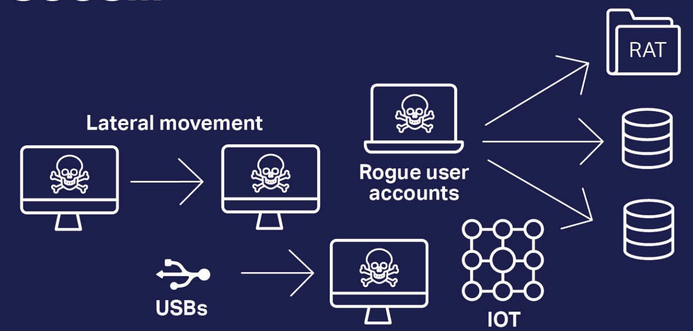
Visibility is a critical gap

organizations report little to no visibility in:

- 87% Kernel-level visibility
- 86% Cloud repositories
- 81% Anomalous behavior
- 78% IOCs

SANS survey 2016

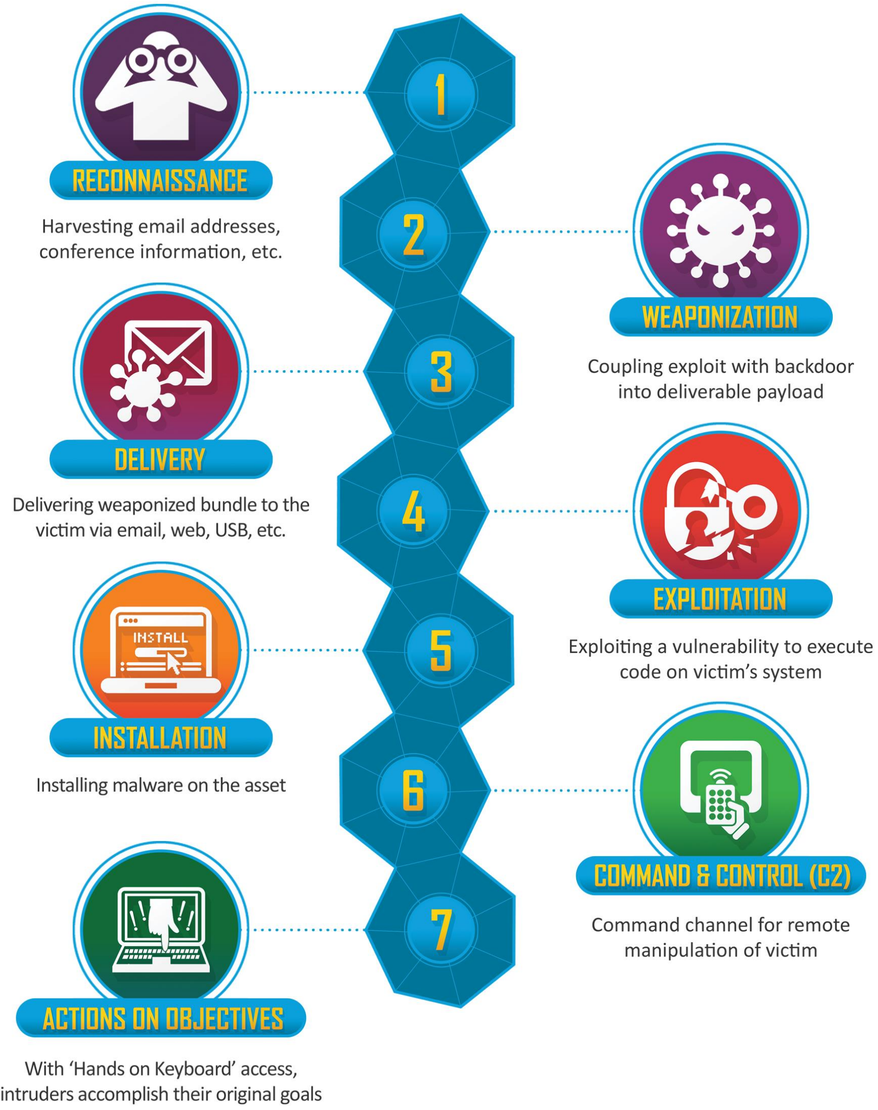
Only opentext™ | EnCase® sees...



- Detect unknown threat
- Forensically sound
- Surgical remediation

EDR은 사이버 보안의 완성을 위한 필수 솔루션

Cyber Kill Chain



정찰	• 공격 목표와 대상을 조사, 식별하고 선정
무기화	• 자동화 도구 등을 이용, 공격을 위한 악성 코드 제작
유포	• 대상 시스템에 악성 코드를 전달
취약점	• 악성 코드의 작동 촉발
설치	• 대상 시스템에 악성 코드를 설치
원격 제어	• 대상 시스템 원격 조작하기 위한 채널 구축
목적 달성	• 정보 수집, 시스템 파괴 등의 목적 달성

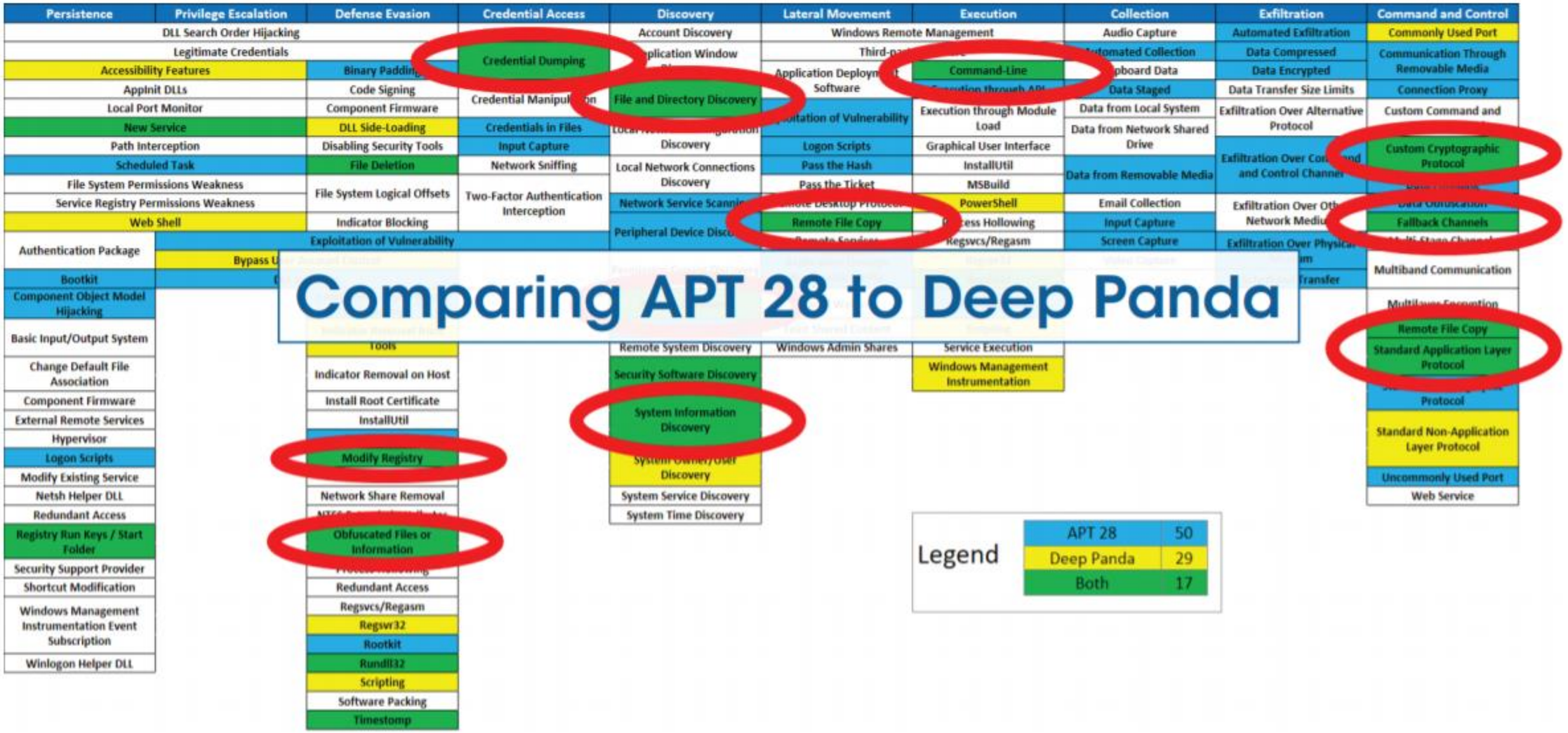
MITRE | ATT&CK™

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking

Enterprise ATT&CK
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

MITRE | ATT&CK™



MITRE | ATT&CK™

MITRE | ATT&CK®

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search

The sub-techniques beta is now live! Read the release blog post for more info.

GROUPS

- Overview
- admin@338
- APT1
- APT12
- APT16
- APT17
- APT18
- APT19
- APT28
- APT29
- APT3
- APT30
- APT32
- APT33
- APT37

Home > Groups > Kimsuky

Kimsuky

Kimsuky is a North Korean-based threat group that has been active since at least September 2013. The group focuses on targeting Korean think tank as well as DPRK/nuclear-related targets. The group was attributed as the actor behind the Korea Hydro & Nuclear Power Co. compromise.[1][2]

ID: G0094
Associated Groups: Velvet Chollima
Version: 1.0
Created: 26 August 2019
Last Modified: 07 October 2019

Associated Group Descriptions

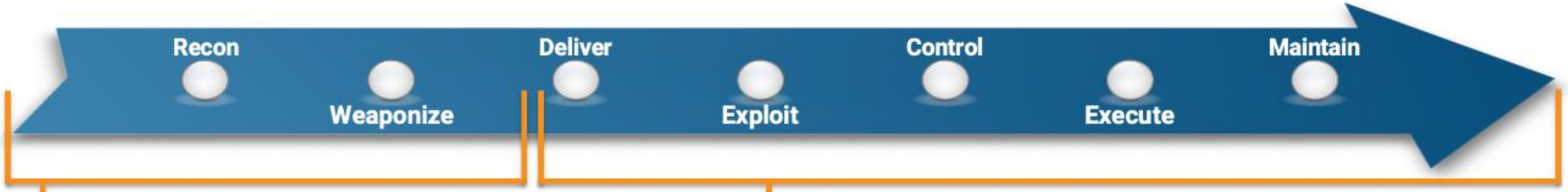
Name	Description
Velvet Chollima	[3]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID	Name	Use

Cyber Kill Chain과 MITRE ATT&CK 관계



PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

ATT&CK for Enterprise

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

MITRE ATT&CK

MITRE | ATT&CK™

사이버 위협

사이버 위협을 식별하기 위해서는 장시간의 추적을 통한 정보가 필요하며, 전문 지식이 있는 보안 전문가가 조사하고 대응해야 함

??

MITRE ATT&CK

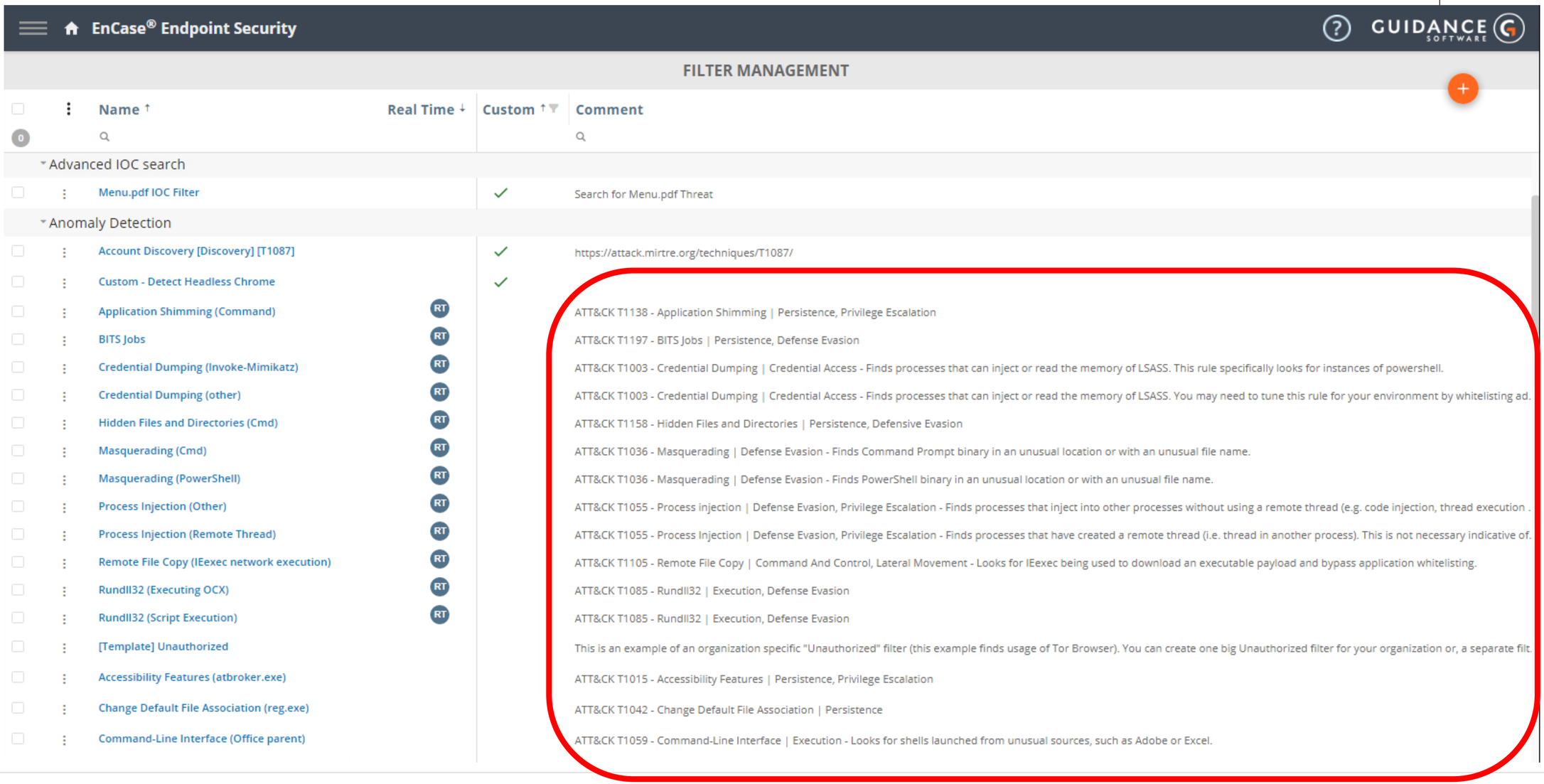
공격자의 TTP(전술, 기법 및 절차)를 명확하게 함으로써, 공격에 대응할 수 있는 방어 수단과 맵핑 시킴

EnCase™를 통한 공통의 결과를 도출

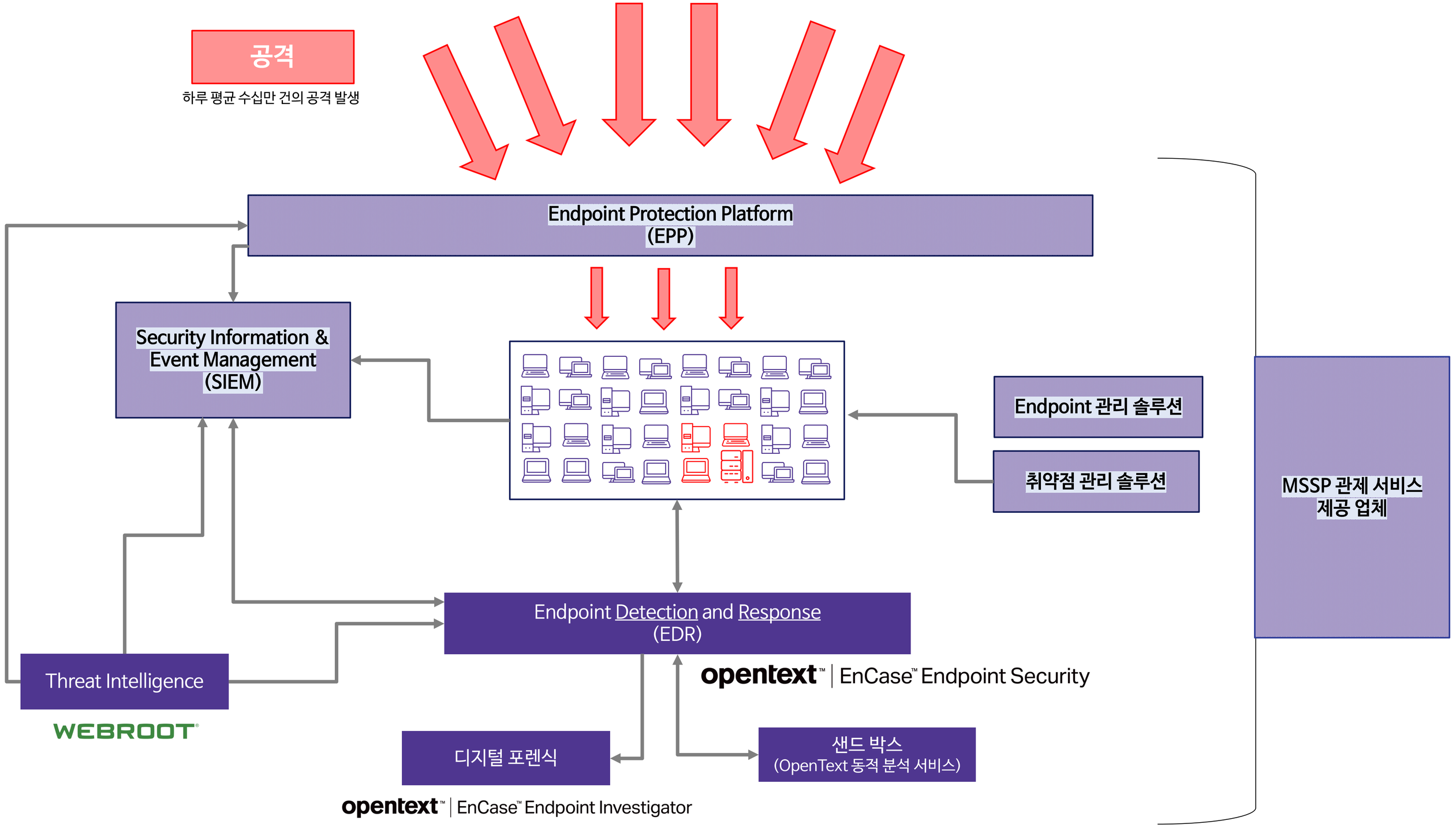
명확한 위협 정보 제공을 통해 보안 담당자들이 다음 단계로 넘어갈 수 있도록 함

MITRE ATT&CK

MITRE | ATT&CK™

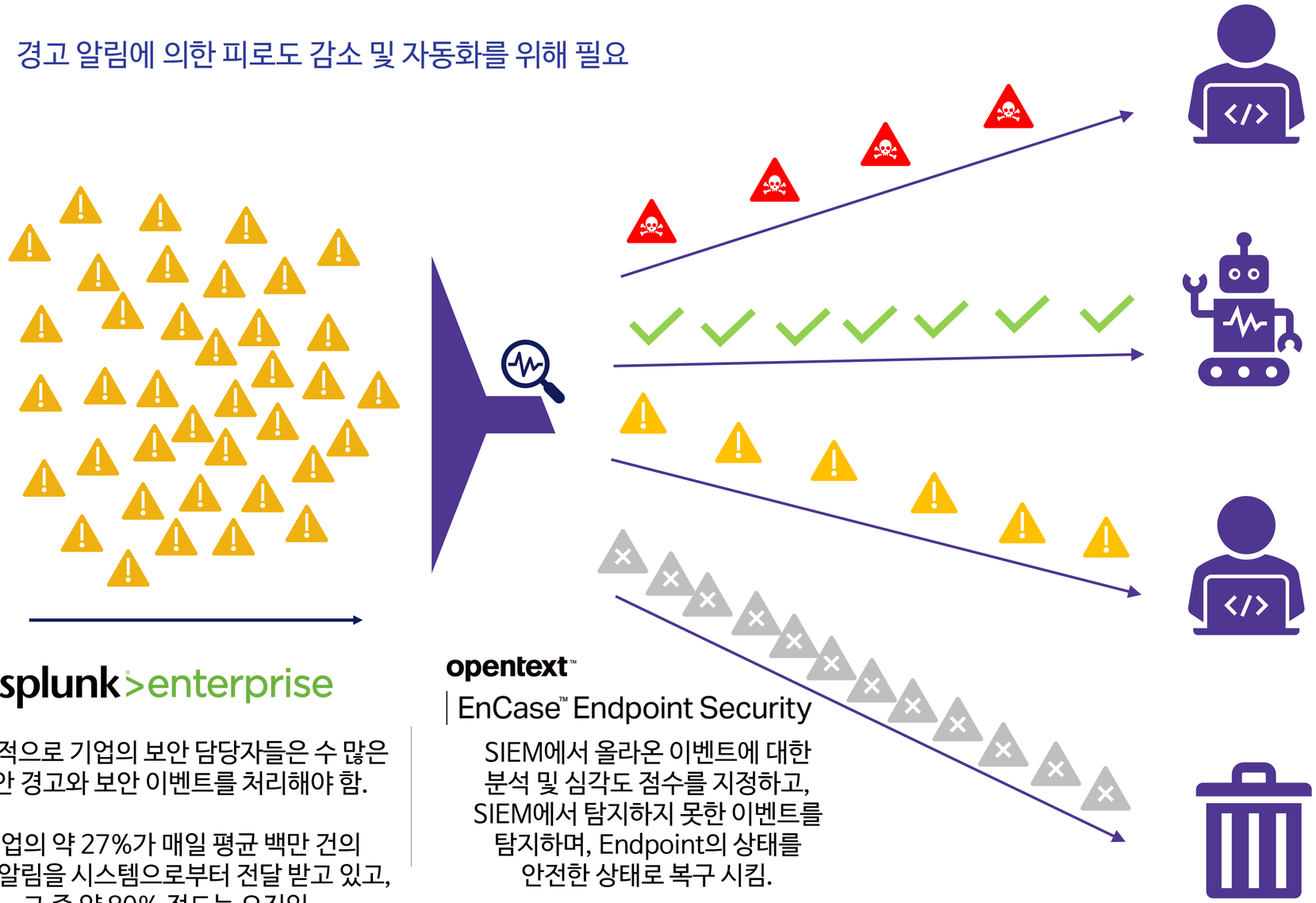


EnCase Endpoint Security 소개


공격
하루 평균 수십만 건의 공격 발생
Endpoint Protection Platform
(EPP)
Security Information &
Event Management
(SIEM)
Endpoint 관리 솔루션
취약점 관리 솔루션
MSSP 관제 서비스
제공 업체
Endpoint Detection and Response
(EDR)
opentext™ | EnCase™ Endpoint Security
Threat Intelligence
WEBROOT
디지털 포렌식
샌드 박스
(OpenText 동적 분석 서비스)
opentext™ | EnCase™ Endpoint Investigator

이벤트 관리 및 경고 알림 선별

경고 알림에 의한 피로도 감소 및 자동화를 위해 필요



splunk>enterprise

일반적으로 기업의 보안 담당자들은 수 많은 보안 경고와 보안 이벤트를 처리해야 함.

기업의 약 27%가 매일 평균 백만 건의 경고 알림을 시스템으로부터 전달 받고 있고, 그 중 약 80% 정도는 오진임.

opentext™

| EnCase™ Endpoint Security

SIEM에서 올라온 이벤트에 대한 분석 및 심각도 점수를 지정하고, SIEM에서 탐지하지 못한 이벤트를 탐지하며, Endpoint의 상태를 안전한 상태로 복구 시킴.

2/3단계의 보안 분석가 및 SOC 요원

전문가의 판단이 필요한 위협에 대해 완벽히 조사하고 해결 합니다. 전문가들은 오진 경보로 인한 시간 낭비를 감소 시키고 실제 위협에 대한 조사를 진행할 수 있습니다.

대응 자동화

일반적으로 알려진 위협 및 취약점에 대해서는 3단계 보안 담당자에 의해 미리 설정된 정책 및 예외 규칙에 따라 자동으로 대응 합니다.

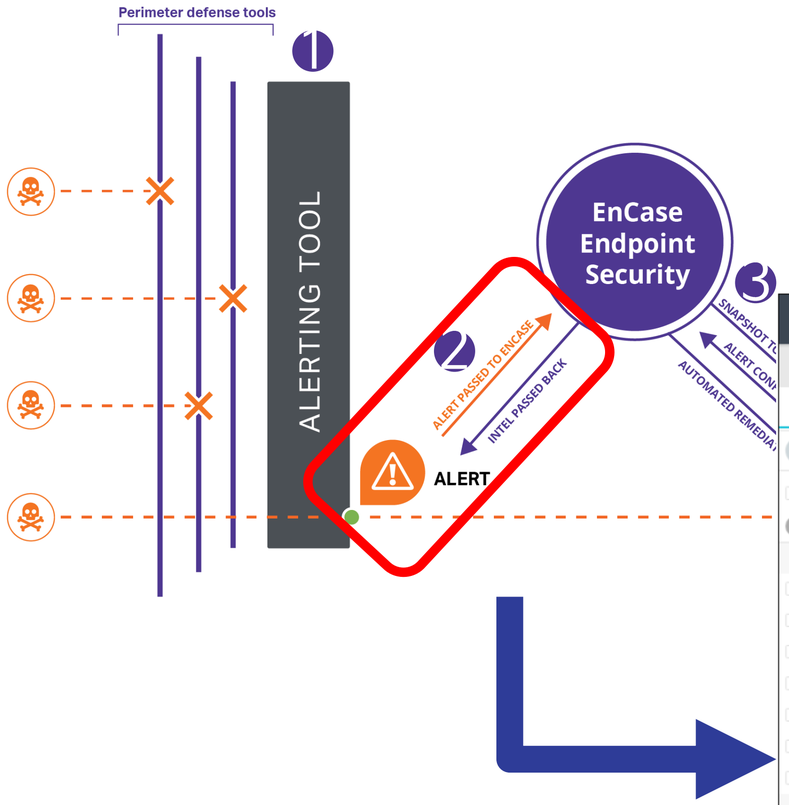
1단계 보안 담당자

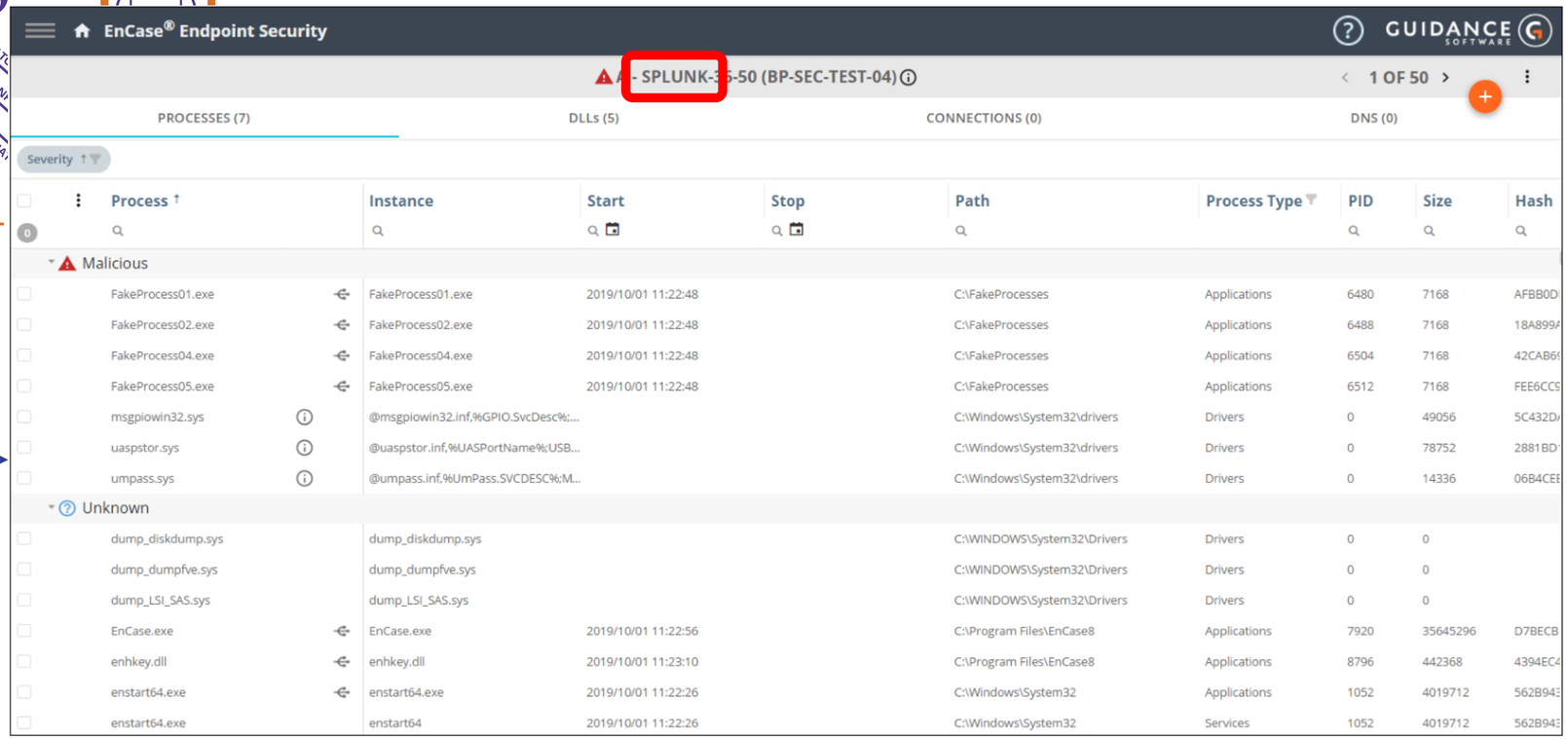
1단계 보안 담당자들은 간단한 이벤트 및 알림 선별 작업을 수행하고, Advanced 위협에 대해서는 2/3단계 보안 담당자에게 Escalation 시킵니다. 주니어 레벨의 분석가들은 위협을 격리시키고, 복잡한 선별 작업은 3단계 보안 담당자에게 전달할 수 있습니다.

오진 경보 감소

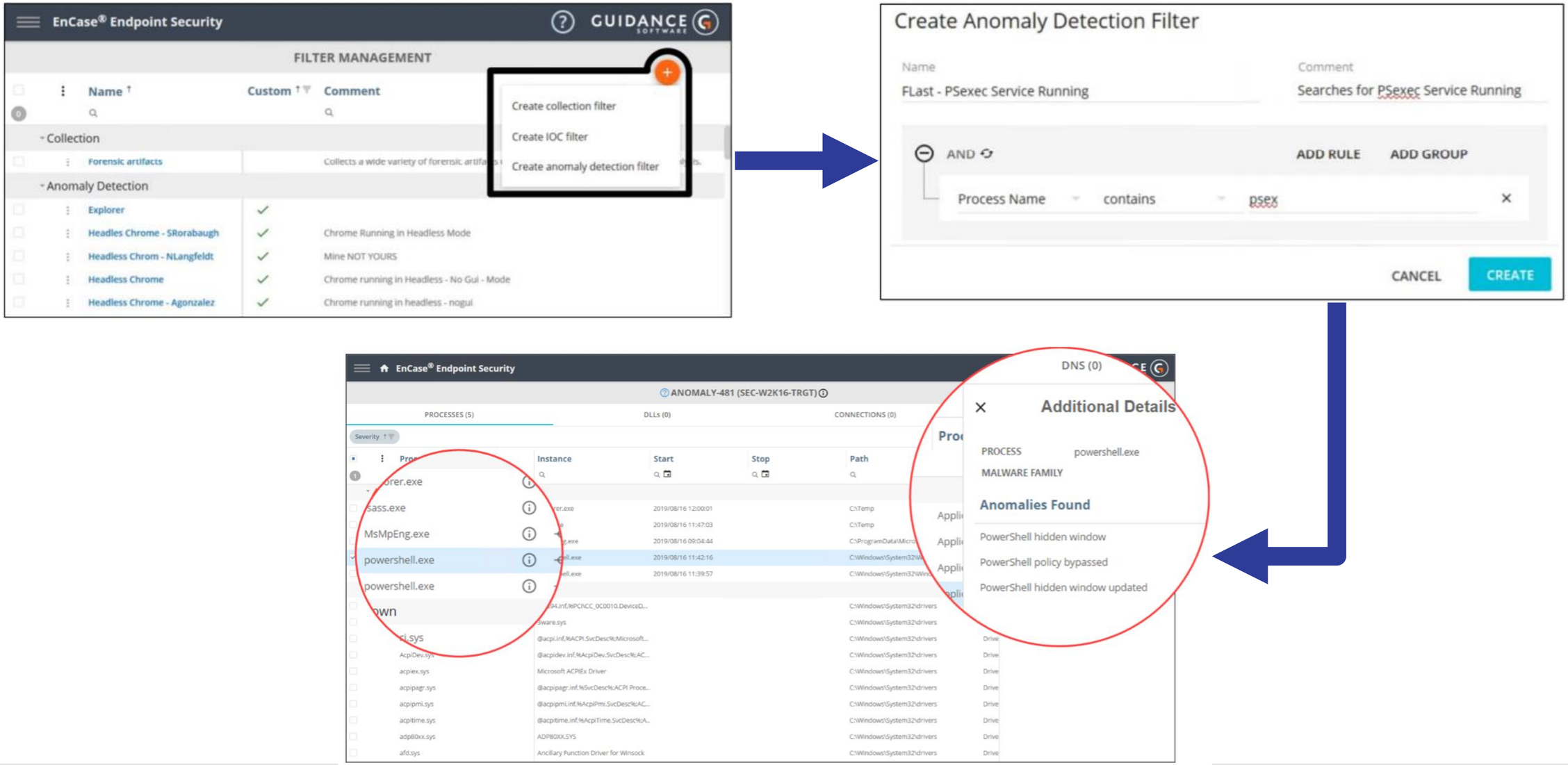
혼란을 방지하고 경고 알림에 대한 피로도를 줄여 줍니다.

가시성 확보

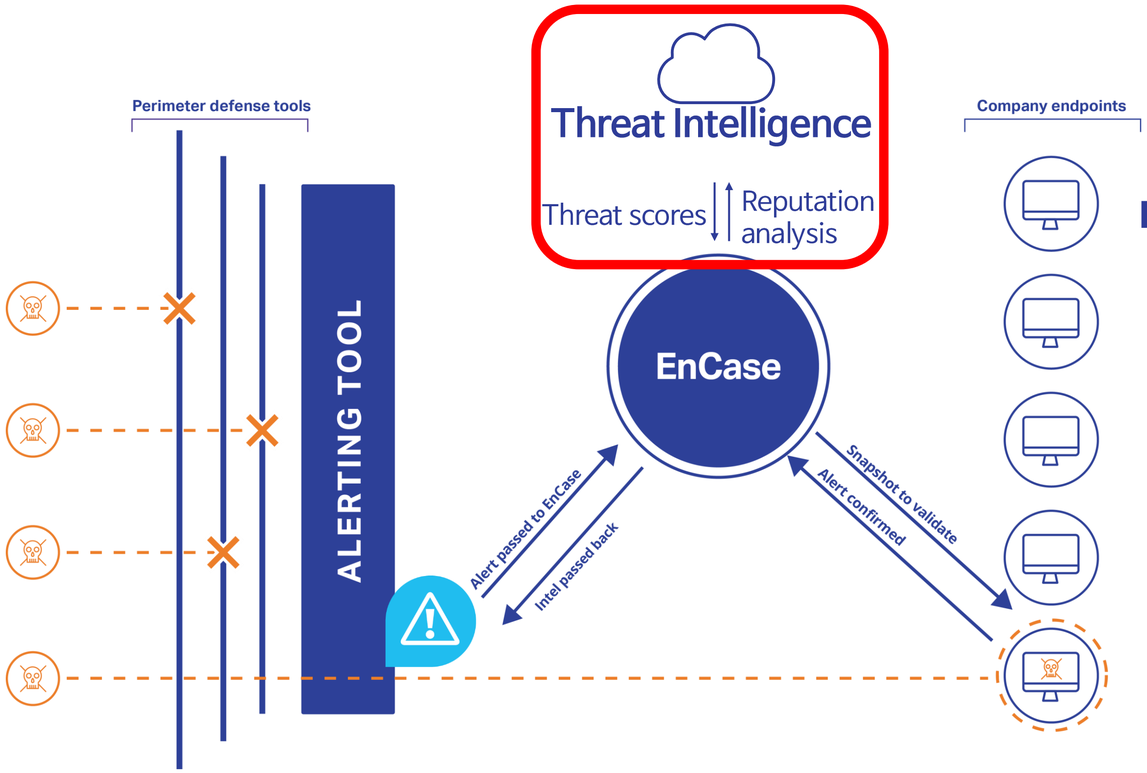




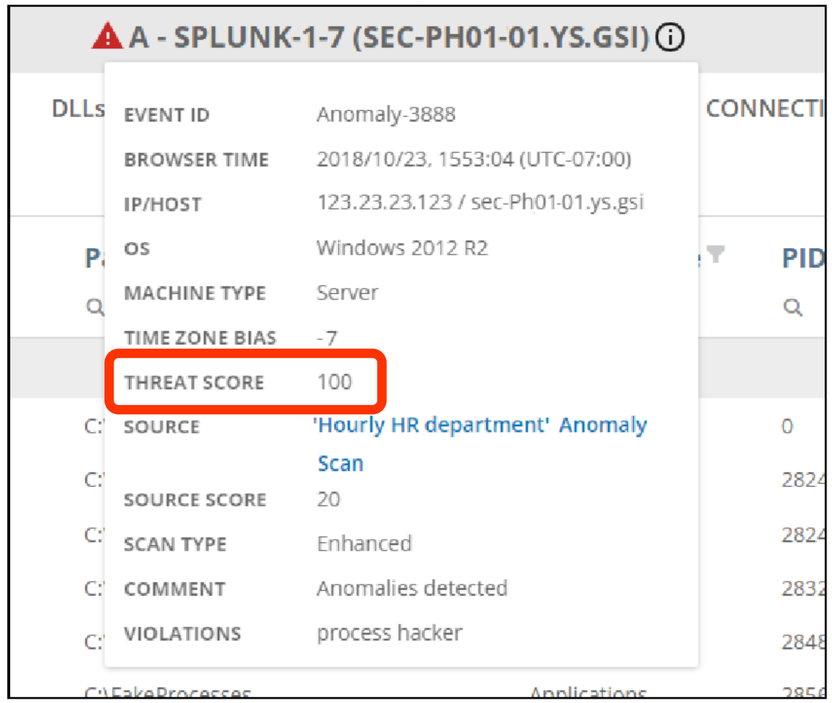
비정상 행위 탐지



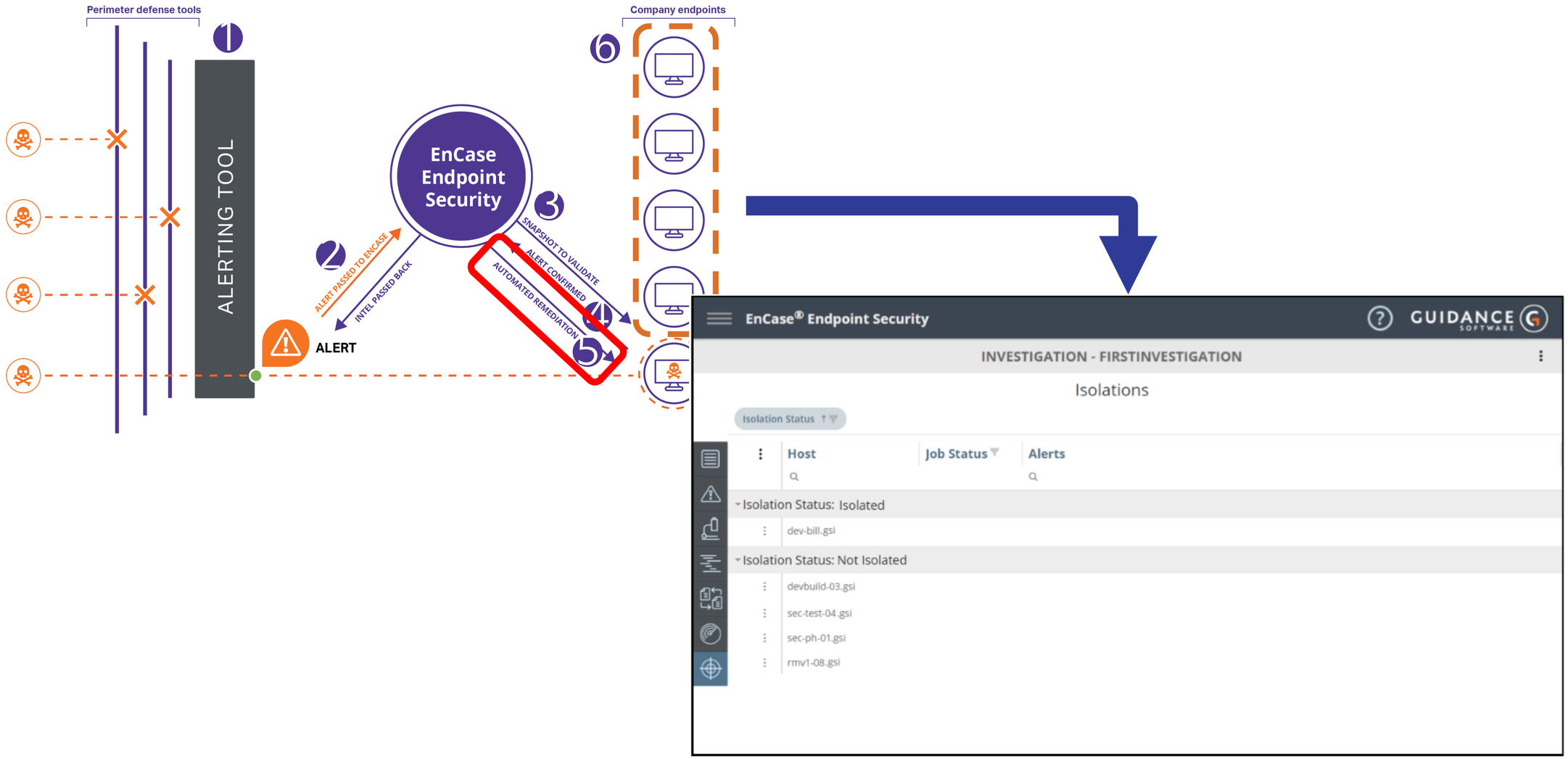
Threat Intelligence



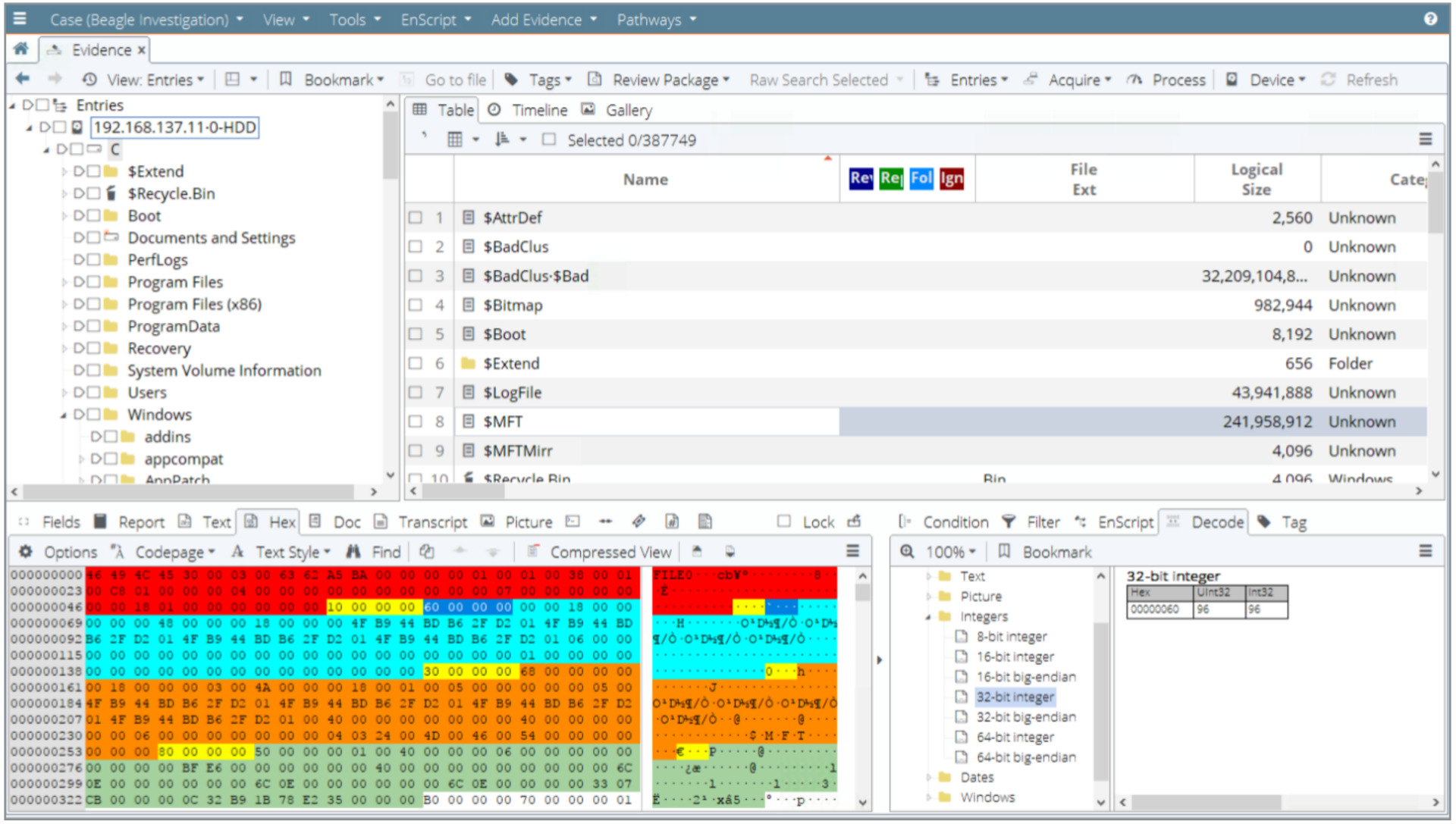
WEBROOT®
an opentext™ company



격리 및 치료

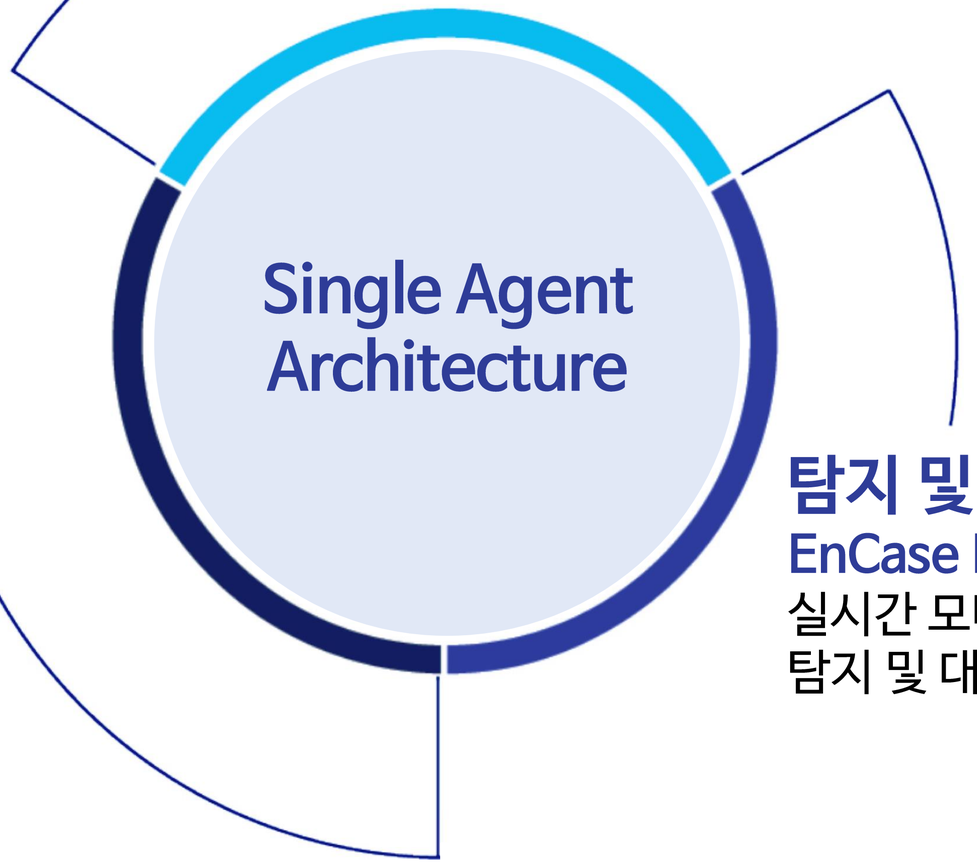


포렌식 기반의 조사



단일 Agent 사용

법적 보존
EnCase eDiscovery
사건 대상자를 중심으로 수집한 법적 증거물에 대한 보존



조사
EnCase Endpoint Investigator
심층적인 포렌식 기능으로 사건 및 컴플라이언스 문제 분석

탐지 및 대응
EnCase Endpoint Security
실시간 모니터링을 통한 위협에 대한 탐지 및 대응

컨텐츠 보안

opentext™ | Security

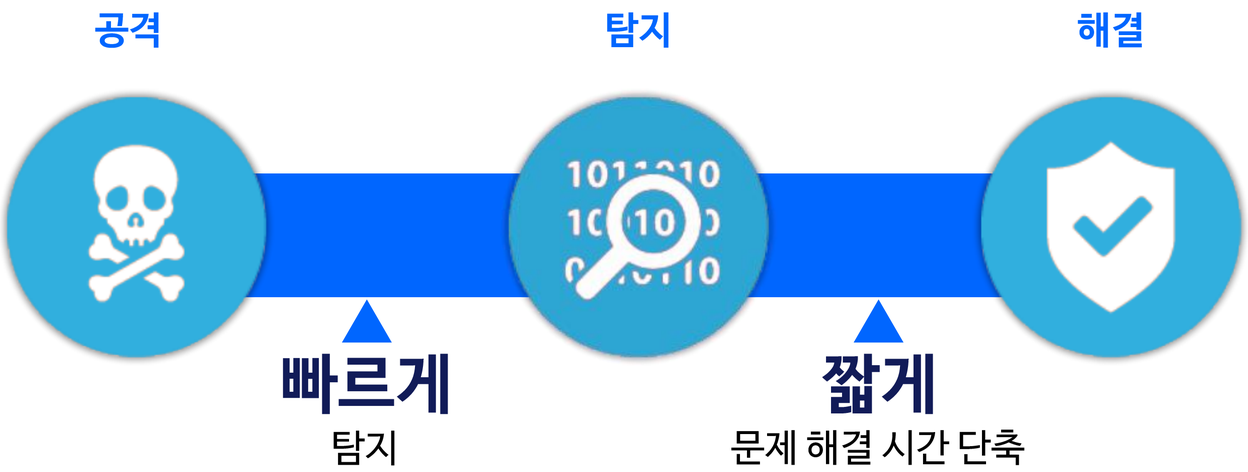
EnCase™의 컨텐츠 보안은
Cyber Kill Chain의 마지막
단계인 “목적 달성”에서 공격자가
어떤 컨텐츠를 유출하는지
가시화 시켜 줍니다.

이 단계에서 정보 보안 팀은
문서화된 민감 정보가
유출되는 것을 막을 수 있습니다.

opentext™ | EnCase™ Endpoint Security

Reveille SEE. KNOW. PROTECT.

EnCase Endpoint Security



평균 탐지 및 대응 시간 단축

Endpoint으로부터 광범위한 정보 수집과 실시간 모니터링 기능

- 규칙 및 정책에 맞게 **행위 기반 탐지** 제공
- **MITRE ATT&CK**을 기반으로 한 이상 행위 탐지
- **SANS "Find Evil"** 기반의 이상 행위 탐지
- **사용자 정의 기반**의 비정상 행위 탐지 룰 반영 가능
- **클라우드** 및 **컨텐츠 저장소**에서도 탐지가 가능

opentext™

온디멘드 웨비나 다시 보기

https://resources.opentext.com/security_webinar_kr

Contact

Phone 02-2185-1054

Mail krmarketing@opentext.com

twitter.com/opentext

facebook.com/opentext

linkedin.com/company/opentext

Opentext.com