



LIVEGUARD ADVANCED

ESET LiveGuard Advanced – 제품 컨셉



행위 기반 탐지

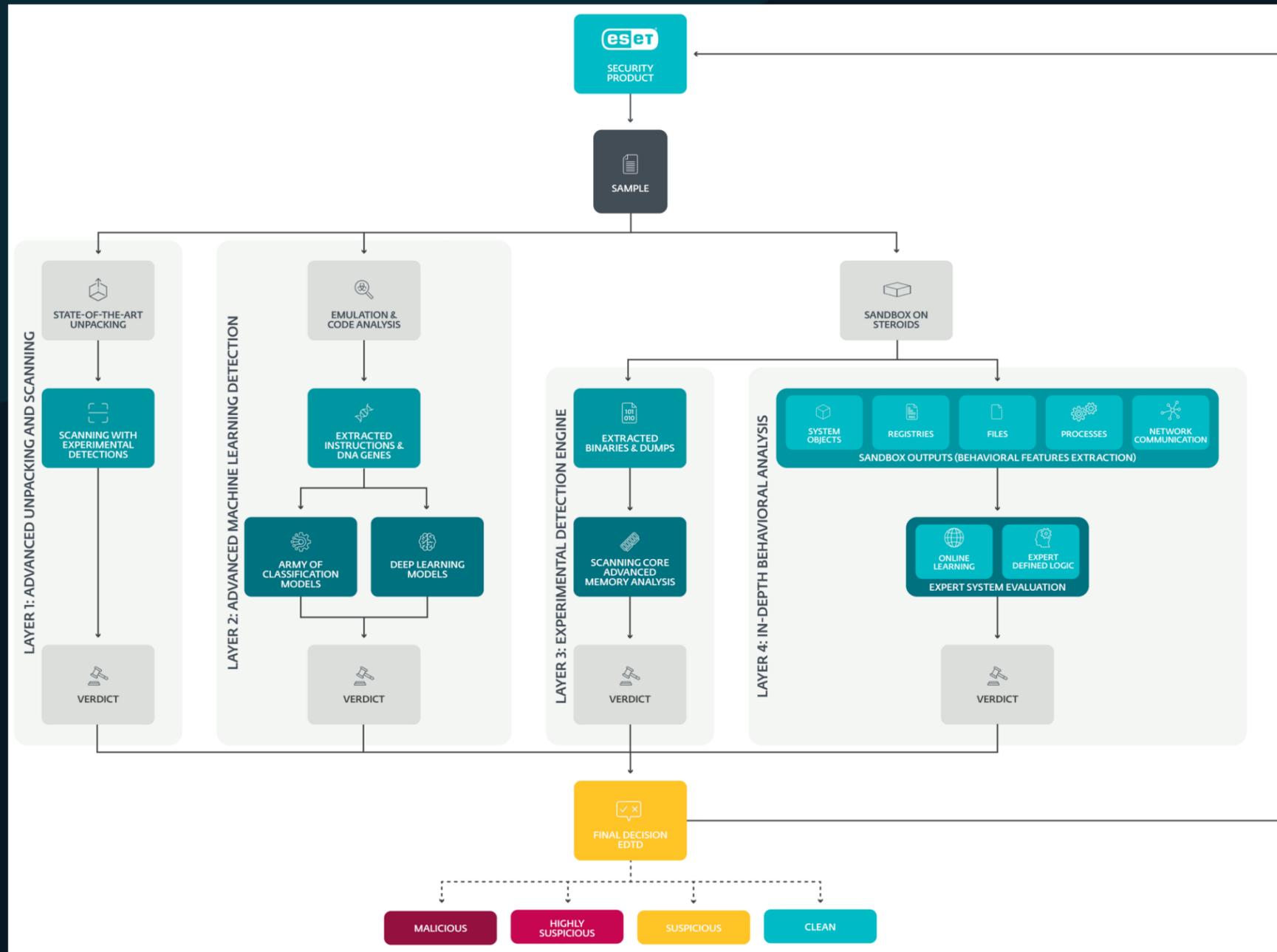


제로데이 위협 탐지



클라우드 샌드박스

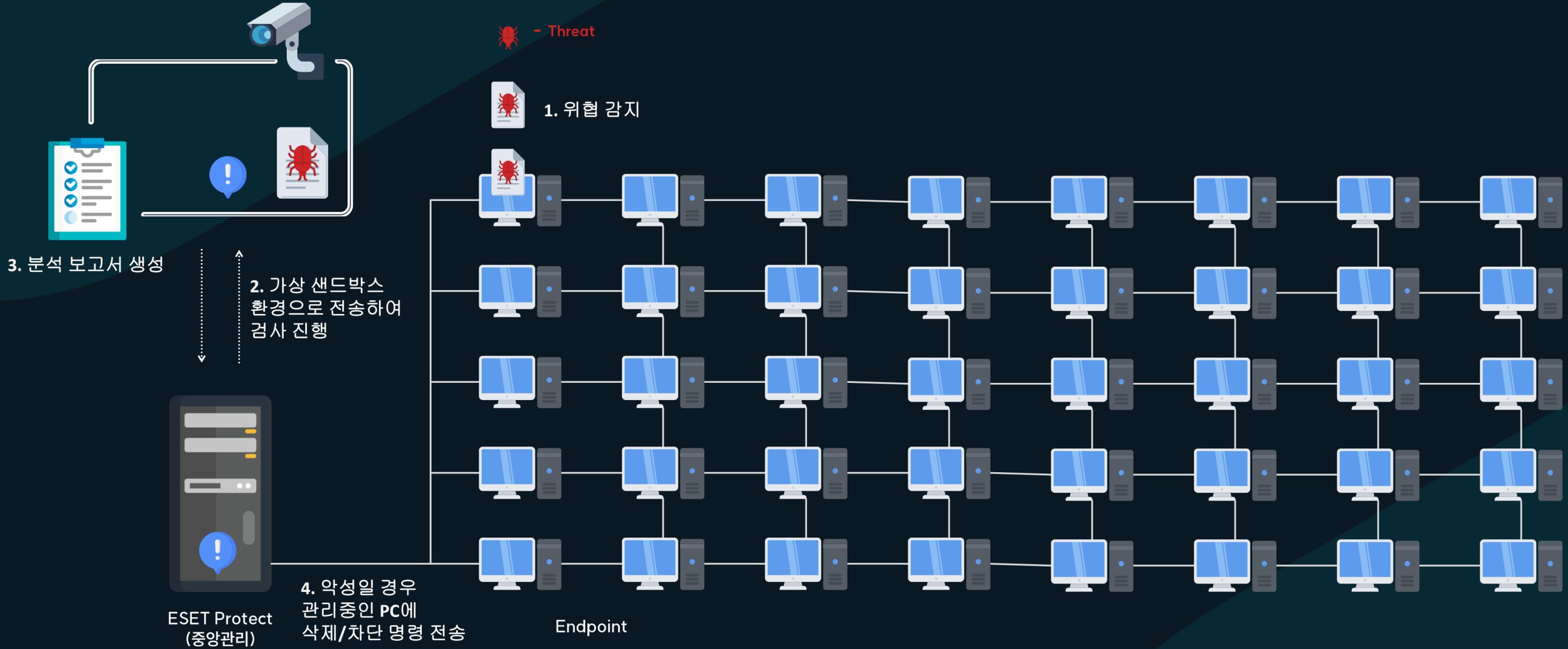
ESET LiveGuard Advanced – 분석 과정



아직 악성으로 확인되지 않고 잠재적으로 악성코드를 포함할 수 있는 의심스러운 샘플을 자동으로 ESET Cloud에 전송하여 분석을 진행합니다.

- 고급 압축 해제 및 검사
- 고급 머신 러닝 탐지
- 실험적 탐지 엔진
- 상세 동작 분석

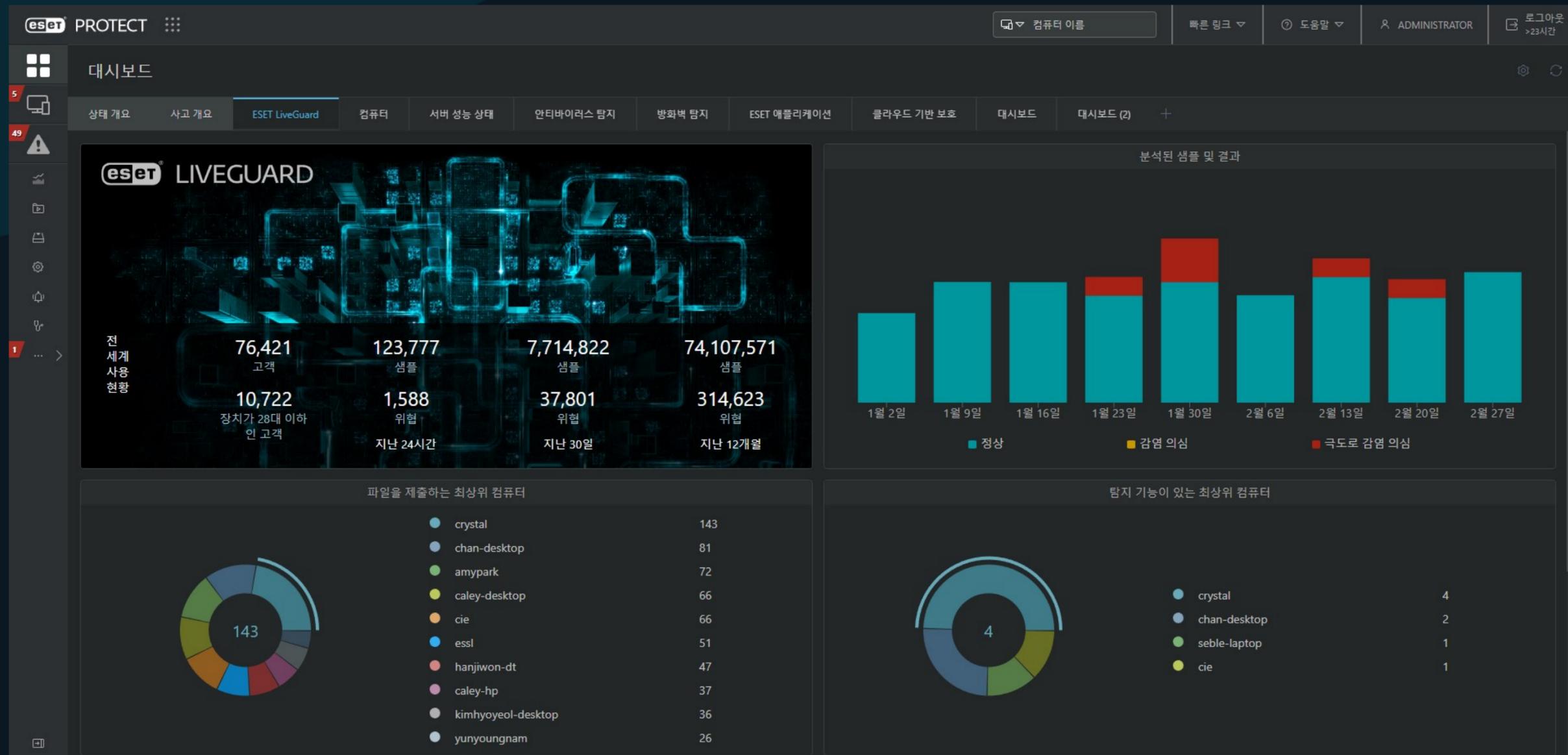
ESET LiveGuard Advanced - 동작 개요



ESET LiveGuard Advanced - 대시보드

ESET LiveGuard Advanced는 ESET PROTECT 중앙관리콘솔에서 전세계 샘플 분석 현황을 확인할 수 있습니다.

더불어 사내의 알려지지 않은 의심 파일 통계 또한 상세히 보여줍니다.



ESET LiveGuard Advanced – 동작 분석 보고서

악의적

SHA-1 **58A5F134F41B09659924245FEC93E9AD7FB42C1D**
범주 실행 파일

분석된 동작

 **맬웨어가 실행되지 않고 탐지됨**
샘플이 실행되지 않고 악의적인 것으로 검색되었습니다.

악의적 원인
ESET 검사 엔진을 통해 실행 없이 맬웨어가 검색되었습니다.

일반적 원인
정상적인 애플리케이션은 이러한 통신을 수행하지 않습니다.

× 샘플이 자체적으로 제거되었습니다	동작이 탐지되지 않음
× 안티바이러스 상호 작용	동작이 탐지되지 않음
× 감염 의심 암호화 작업	동작이 탐지되지 않음
× 바로 가기 키 등록	동작이 탐지되지 않음
× 부트 영역 수정	동작이 탐지되지 않음

× 머신 러닝 탐지	동작이 탐지되지 않음
× Fileless 위협	동작이 탐지되지 않음
× 권한 상승	동작이 탐지되지 않음
× Windows 폴더에 파일이 생성됨	동작이 탐지되지 않음



ESET LiveGuard Advanced – 상세 정보 확인

< 뒤로 제출된 파일 > file:///D:/9f...c939c3e11.exe - 파일 상세 정보

악성

상태	⚠️ 악성
상태	🕒 마침
마지막으로 처리한 날짜	2021년 8월 18일 15:53:30
전송한 날짜	2021년 8월 18일 15:53:27
동작	동작 보기

file:///D:/9f51...9bc939c3e11.exe

컴퓨터	[redacted]
사용자	[redacted]
사유	자동
보낸 곳	Dynamic Threat Defense
해시	58A5F134F41B09659924245FEC93E9AD7FB42C1D

분석

상태	<div style="width: 100%;"><div style="width: 100%;"></div></div> ⚠️ 악성
상태	🕒 마침
전송한 날짜	2021년 8월 18일 15:53:27
마지막으로 처리한 날짜	2021년 8월 18일 15:53:30

사유	자동
보낸 곳	Dynamic Threat Defense
해시	58A5F134F41B09659924245FEC93E9AD7FB42C1D
파일명	file:///D:/9f517d980426714b74fa59bc939c3e11.exe
크기	196KB (201 216 bytes)
종류	실행 파일

[닫기](#) [동작 보기](#) [제외 생성](#)

분석

상태	<div style="width: 100%;"><div style="width: 100%;"></div></div> ⚠️ 악성
상태	🕒 마침
전송한 날짜	2021년 8월 18일 15:53:27
마지막으로 처리한 날짜	2021년 8월 18일 15:53:30

악성

상태	⚠️ 악성
상태	🕒 마침
마지막으로 처리한 날짜	2021년 8월 18일 15:53:30
전송한 날짜	2021년 8월 18일 15:53:27
동작	동작 보기

file:///D:/9f51...9bc939c3e11.exe

컴퓨터	[redacted]
사용자	[redacted]
사유	자동
보낸 곳	Dynamic Threat Defense
해시	58A5F134F41B09659924245FEC93E9AD7FB42C1D

ESET LiveGuard Advanced – 도입 사례 (1)

soulbrain

솔브레인

S社 백신 사용 중 다수 PC에서 랜섬웨어 감염 사례 확인



표적 공격의 대상이 되어 회사 내부에서만 실행되는 맬웨어가 유포됨

(표적 공격에 의한 맬웨어는 샘플 분석이 불가능하므로 어떠한 맬웨어도 탐지할 수 없으며, 의심 파일의 존재 여부를 확인하는 것 또한 매우 어려움)



LiveGuard Advanced의 경우 모든 파일을 Cloud Sandbox에서 분석하므로 전산담당자가 의심 파일 유입을 따로 확인할 필요가 없으며, 분석 결과는 5분 내외에 모든 Endpoint에 실시간 전달되므로 파일기반의 제로데이 공격에 매우 효과적임.



고객사 도입 이후 랜섬웨어 피해 없음.

ESET LiveGuard Advanced – 도입 사례 (2)



엘오티베쿰

다수 PC에서 랜섬웨어 감염 사례 확인



제로데이 공격에 의한 것으로 확인되어 ESET LiveGuard 제품 도입을 권고함.

일반 백신의 경우 시그니처 DB에 등록되기 이전의 시점을 노리고 공격하는 제로데이 공격에는 취약함.



LiveGuard Advanced는 의심스러운 파일을 Cloud Sandbox 환경에서 실제로 구동시켜 파일이 악성인지 양성인지 판단하기 때문에 시그니처 DB에 등록되지 않은 악성 파일들도 탐지가 가능함.(제로데이 공격 방어)



고객사 도입 이후 랜섬웨어 피해 없음.

감사합니다.

Address : 서울시 송파구 송파대로 167, A동 521. 522호(문정동. 문정역 테라타워1)

Tel : 1899-8352 | Fax : 02-402-8352

영업 문의 : sales@estc.co.kr

웹 사이트 : <https://eset.estc.co.kr/>