ESET LIVEGUARD ADVANCED

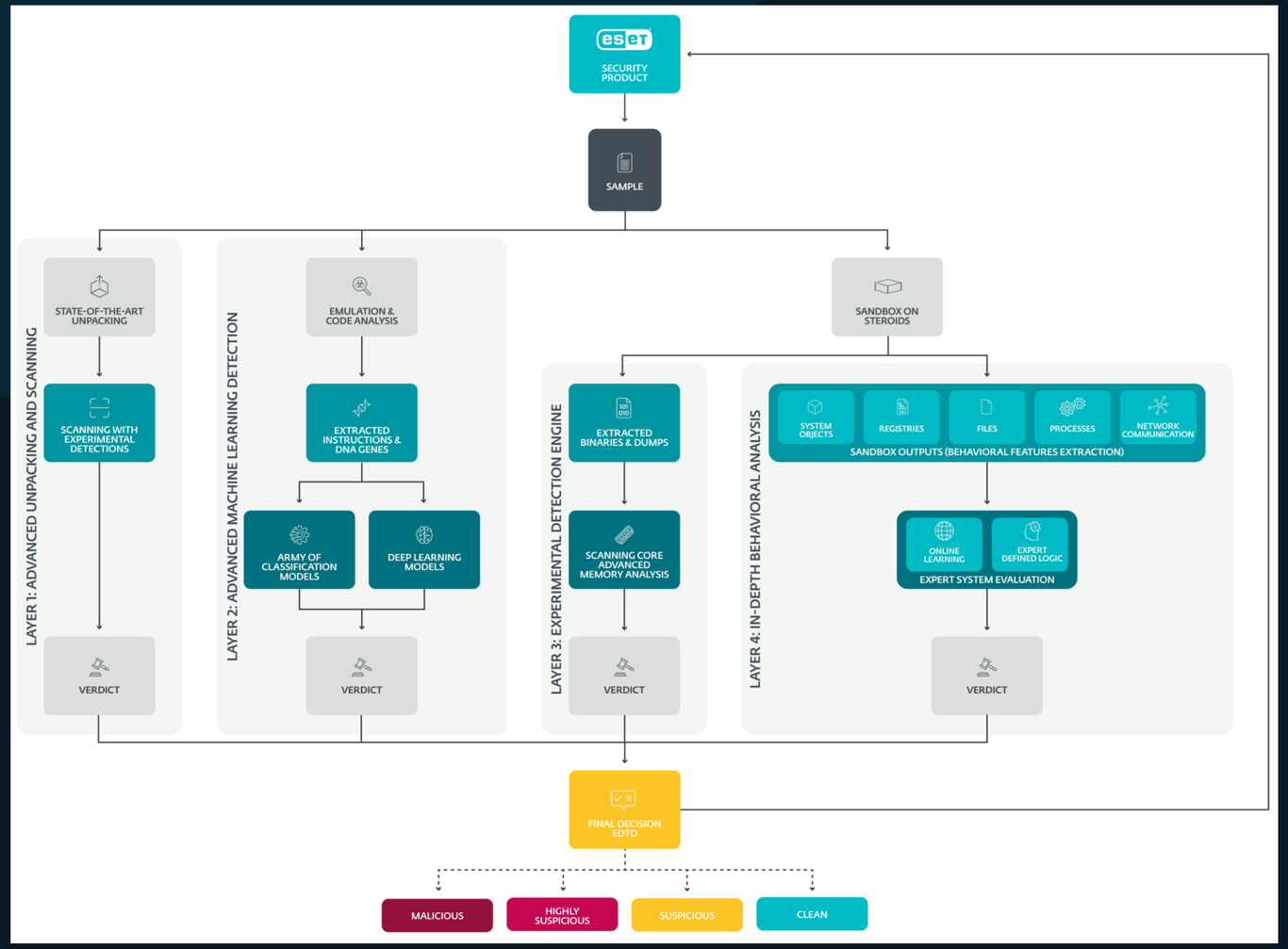
ESET LiveGuard Advanced – 제품 컨셉

행위 기반 탐지

제로데이 위협 탐지

클라우드 샌드박스

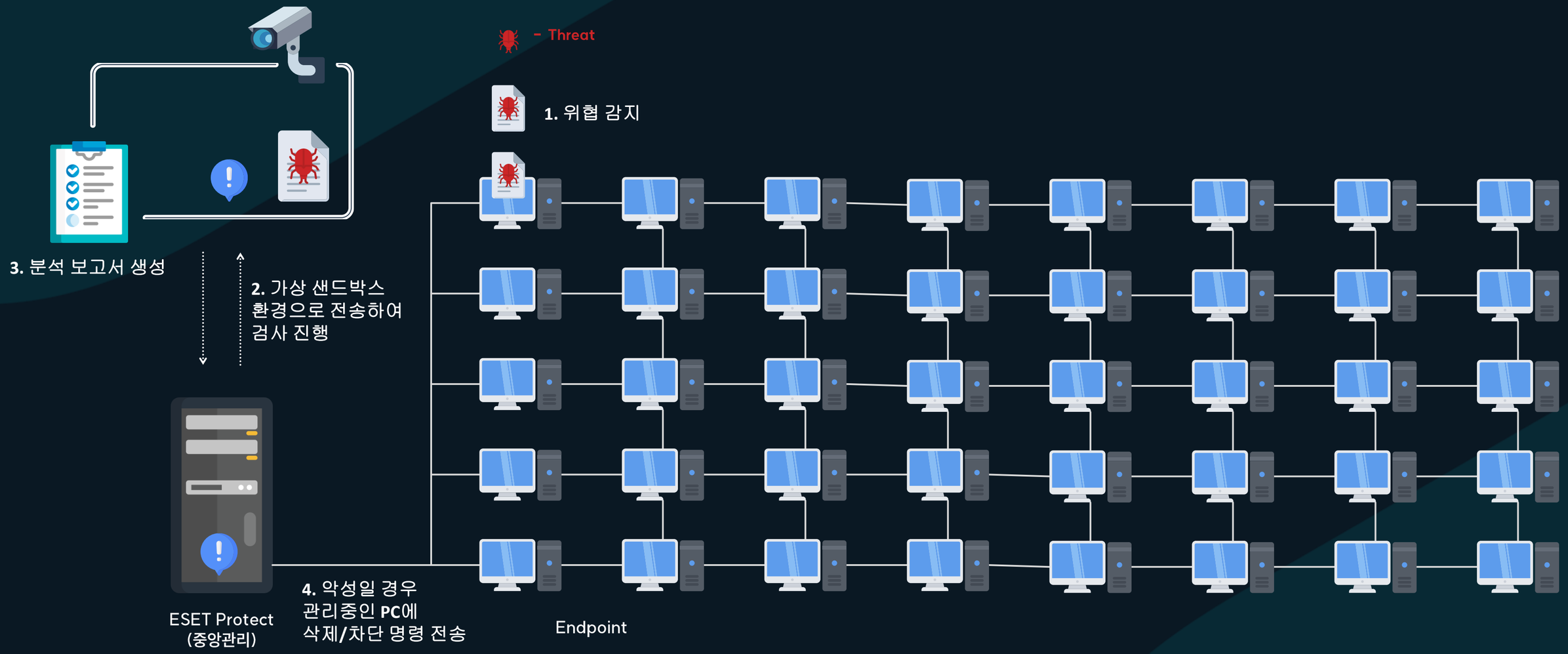
ESET LiveGuard Advanced – 분석 과정



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

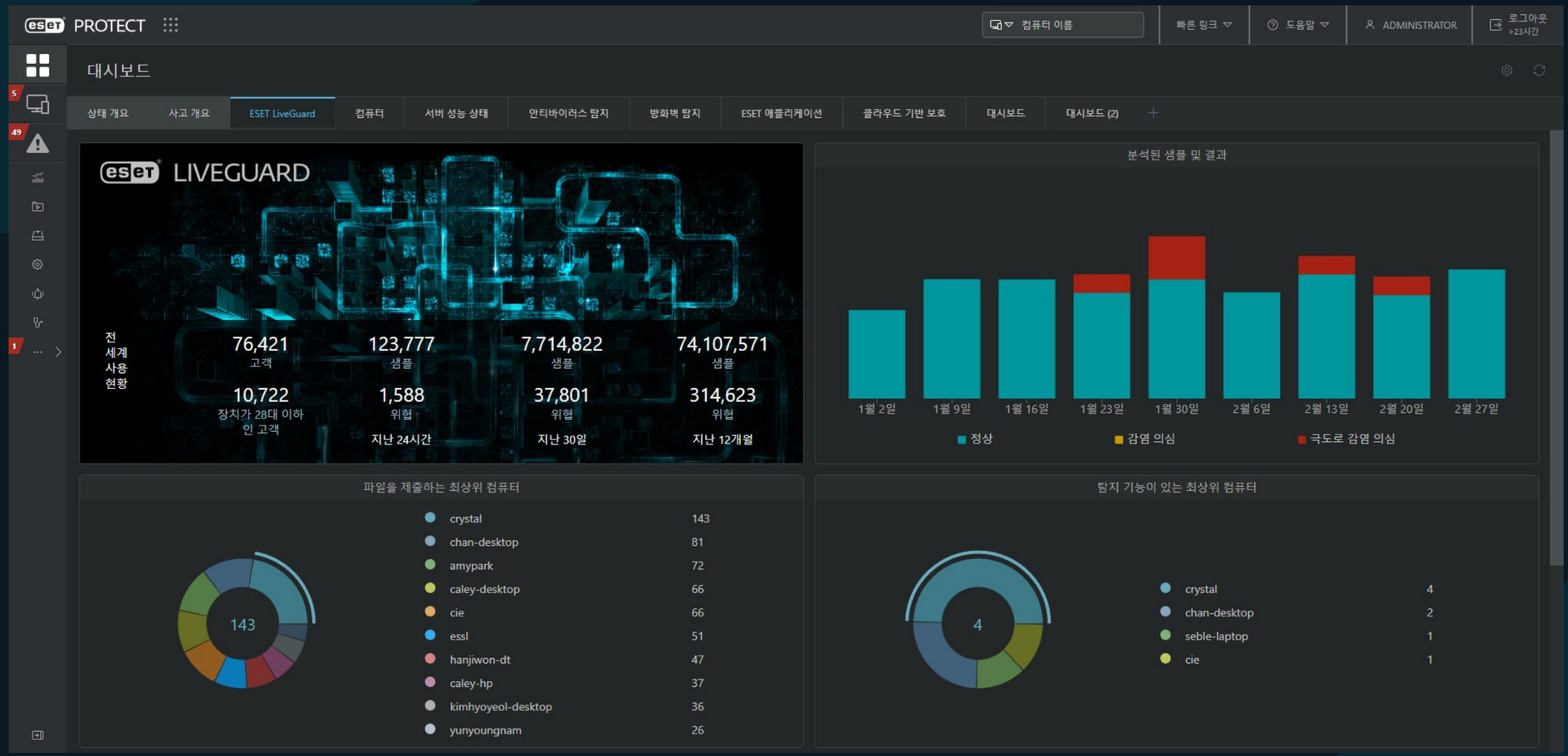
ESET LiveGuard Advanced – 동작 개요



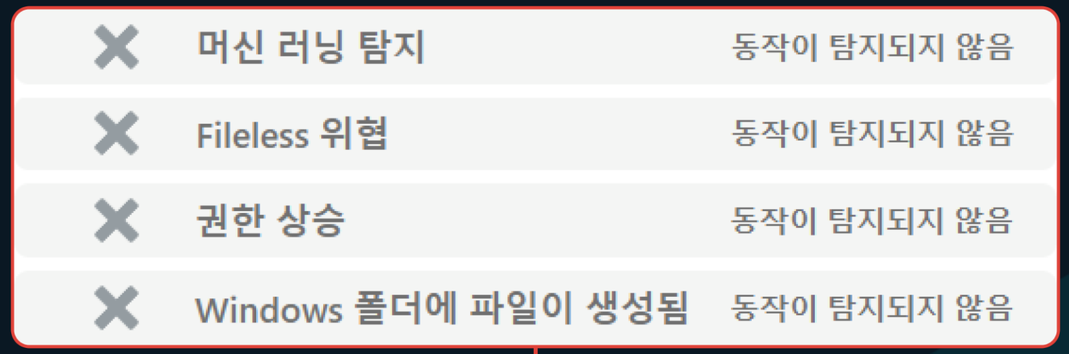
ESET LiveGuard Advanced - 대시보드

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

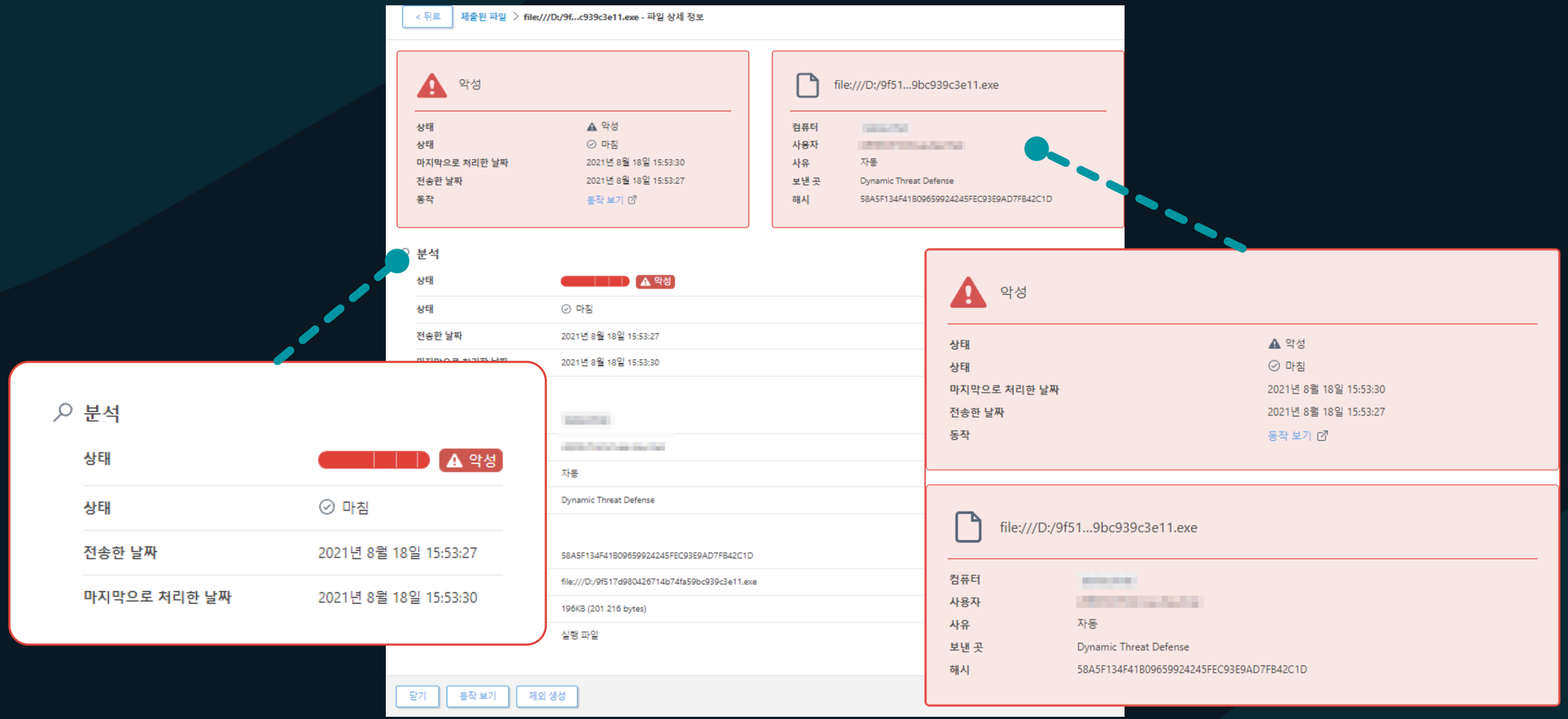
더불어 사내의 알려지지 않은 의심 파일 통계 또한 상세히 보여줍니다.



ESET LiveGuard Advanced – 동작 분석 보고서



ESET LiveGuard Advanced – 상세 정보 확인



ESET LiveGuard Advanced – 도입 사례 (1)

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)

엘오티베큠

다수 PC에서 랜섬웨어 감염 사례 확인

↓

제로데이 공격에 의한 것으로 확인되어 ESET LiveGuard 제품 도입을 권고함.

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

↓

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

↓

고객사 도입 이후 랜섬웨어 피해 없음.

감사합니다.

Address : 서울시 송파구 송파대로 **167, A**동 **521. 522**호(문정동. 문정역 테라타워**1**)

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

영업 문의 : **sales@estc.co.kr**

웹 사이트 : **https://eset.estc.co.kr/**

Digital Security
Progress. Protected.