데이터시트

Endpoint Detection and Response Cloud

통합 엔드포인트 가시성 및 자동화된 보안 위협 추적

개요

탐지 - 환경에 속하지 않은 이상 요소 발견

- 기준 활동을 벗어나는 소프트웨어, 메모리, 사용자, 네트워크 이상 요소 탐지
- 타임라인 및 경로 분석을 통해 다단계 공격 탐지
- 프로세스 메모리 분석으로 메모리 기반 공격 규명

자동화 - 숙련된 조사 팀의 베스트 프랙티스 활용

- 자동화된 침해 사고 플레이북 규칙에 따라 숙련된 조사 팀의 베스트 프랙티스 및 분석 재현
- 자동화된 아티팩트 수집으로 엔드포인트 활동에 대한 심도 있는 가시성 확보
- 기본 제공된 플레이북을 활용하여 사이버 보안 기능 실행 및 전문적인 조사 방법 습득

시각화 - 방대한 양의 사이버 데이터에서 실행 가능한 결과 창출

- 시각적 링크 분석을 통해 관련 없는 데이터 유형 간에 상황에 따른 관계 발견
- 그래픽 알림을 활용하여 신속하게 침해 사고의 원인, 시점, 영향 파악
- 방대한 엔드포인트 텔레메트리를 대화형 그래픽으로 변환하여 중요한 활동 집중 조명

소개

보안 팀은 '눈에 띄지 않으면서' 최장 190일간 고객 환경에서 활동하는 정교한 공격에 맞서고 있습니다.[1] 공격자가 고객 환경 내에서 자유롭게 돌아다니기 위해 훔친 인증 정보를 사용하여 합법적인 사용자로 위장하는 등 은밀한 수법을 구사하는 경우가 늘고 있습니다. 제로데이 공격 발견 건수는 약간 줄어든 반면 취약점과 이를 노리는 악성 코드의 조합으로 구성된 기존의 공격 방식에서 벗어난 '자립형' 전술이 증가했습니다. 이러한 전술은 합법적인 툴을 사용하므로 탐지하기가 더 어렵습니다.[1]

기업은 이와 같이 기존의 탐지 기술을 우회하는 보안 위협을 찾아낼 수 있는 새로운 방식이 필요합니다. 또한 심층 조사를 수행할 만한 숙련된 인력을 확보하기가 어렵거나 많은 비용이 들 수 있습니다. 그러한 전문가를 보유했더라도 인재 이탈을 방지해야 하는 어려움도 있습니다.

EDR Cloud 개요

Symantec Endpoint Detection and Response(EDR) Cloud는 엔터프라이즈 환경 전반에서 심도 있는 엔드포인트 가시성을 제공하고 자동화된 방식으로 보안 위협을 추적하며 침해 사고에 대응합니다. Symantec EDR Cloud는 클라우드 기반 서비스로, 수분 내로 구축하여 사이버 공격에 대응할 강력한 보안을 실현할 수 있습니다. Symantec EDR Cloud는 수많은 경험을 보유한 보안 분석가의 기술력 및 베스트 프랙티스를 모든 조직에 적용할 수 있게 해주는 광범위한 규칙과 사용자 행위 분석을 통해 조사 팀의 생산성을 높이고 비용을 대폭 절약합니다.

보안 팀은 은밀한 보안 위협의 탐지를 지원하는 포렌식 분석 및 기본 제공 플레이북을 활용하면서 별도의 에이전트 구축 없이 원하는 대로 구성 가능할 수 있는 포인트 인 타임 검사 방식으로 신속하게 조사에 착수할 수 있습니다.

환경에 속하지 않은 이상 요소 발견

Symantec EDR Cloud는 소프트웨어, 메모리, 사용자, 네트워크 기준 활동을 통합적으로 모니터링하면서 이미 환경에 침투한 공격자를 간단하게 추적할 수 있도록 지원합니다. 공격자가 환경 내에서 활동 중이라면 해당 악성 코드 및 사용자 활동이 이상 요소로 나타납니다. Symantec EDR Cloud는 환경 전반에서 아래와 같은 이상 요소를 탐지합니다.

- **소프트웨어 이상 요소 - 특이한 소프트웨어, 일치하지 않은 빌드 버전, 패치가 적용되지 않았거나 오래된 운영 체제(OS) 릴리스가 있는 엔드포인트를 찾아냅니다.**
- **메모리 이상 요소 - 프로세스 메모리, 파일 및 OS 개체, 시스템 설정을 포렌식 분석하여 메모리에 상주하는 이상 요소를 탐지합니다.**
- **사용자 이상 요소 - 사용자 행위 분석을 통해 합법적인 사용자로 위장하고 비정상적인 활동을 수행하는 공격자를 찾아냅니다.**
- **네트워크 이상 요소 - 통계 분석을 통해 비정상적인 IP 주소를 식별하고 평판 조회로 데이터 유출과 관련된 IP 주소 및 도메인을 알아냅니다.**

또한 Symantec EDR Cloud에 포함된 여러 보안 위협 엔진은 파일, 사용자 계정, 네트워크 연결에 대해 리스크 점수를 부여합니다. 아래와 같은 탐지 기능도 제공합니다.

- **수백만 개의 정상 파일과 악성 파일을 활용하는 신경망 기반 머신 러닝**
- **고객 제공 및 타사 보안 위협 인텔리전스 소스**
- **레지스트리 변경 및 예약 작업을 조사하여 지속적 보안 위협 탐지**
- **복수의 악성 코드 차단 엔진**

숙련된 조사 팀의 베스트 프랙티스 활용

Symantec EDR Cloud는 보안 분석가의 복잡한 다단계 조사 워크플로우를 자동화하는 플레이북을 지원합니다. 기본 제공 플레이북을 통해 의심스러운 행위, 알려지지 않은 보안 위협, 측면 이동, 정책 위반을 신속하게 밝혀냅니다. 보안 팀은 플레이북을 참조하면서 전문적인 추적 및 조사 기법을 익힐 수 있습니다. 뿐만 아니라 조사 팀이 직접 플레이북을 작성하여 베스트 프랙티스를 자동화하고 특정 보안 위협 추적 시나리오를 문서화할 수 있습니다.

방대한 양의 사이버 데이터에서 실행 가능한 결과 창출

Symantec EDR Cloud는 강력한 시각화 기능을 제공합니다. 이 시스템은 시각적 링크 분석과 대화형 그래픽을 도입하여 보안 전문가가 컴퓨터 및 네트워크 데이터를 사용하고 연결하는 방식을 완전히 바꿔 놓았습니다.

시스템을 활용하는 분석을 통해 모든 연관 데이터와의 대규모 상호 작용이 가능합니다. 링크 분석을 통해 서로 다른 데이터 유형 간의 복잡한 관계를 포착하고 신속하게 개념적으로 연결합니다.

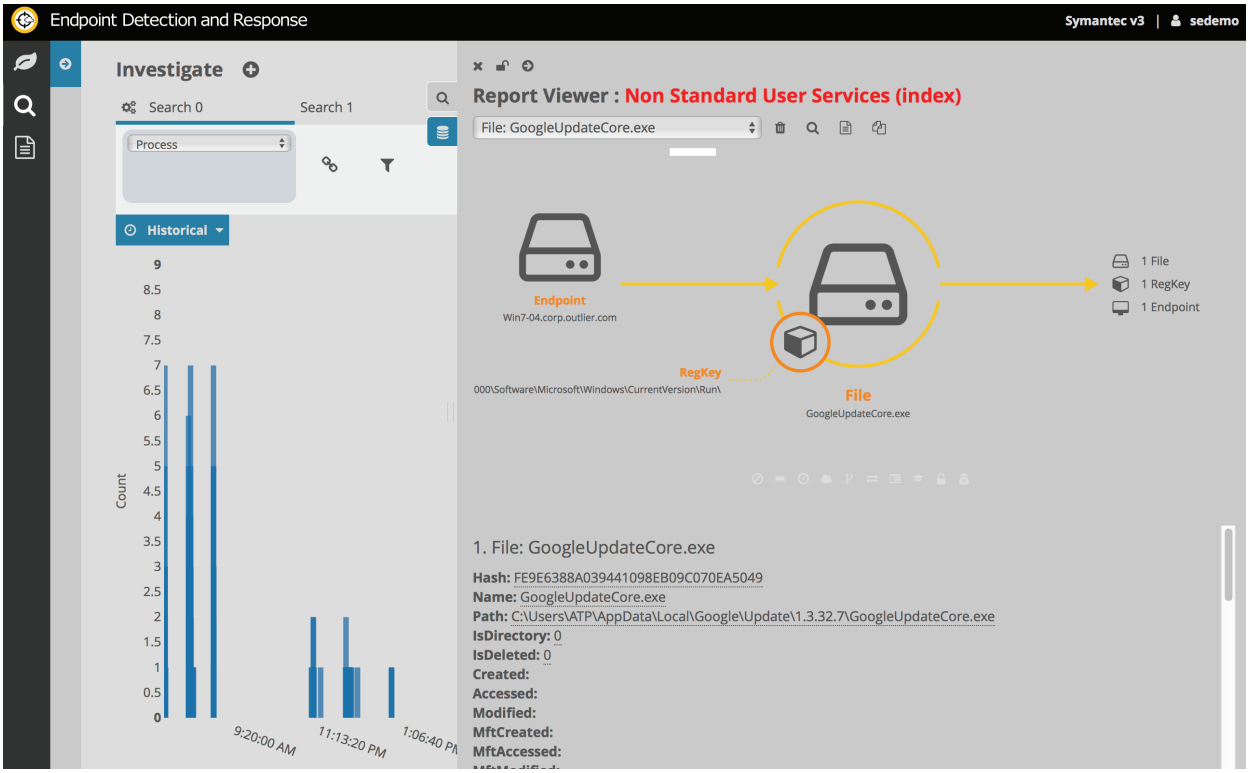
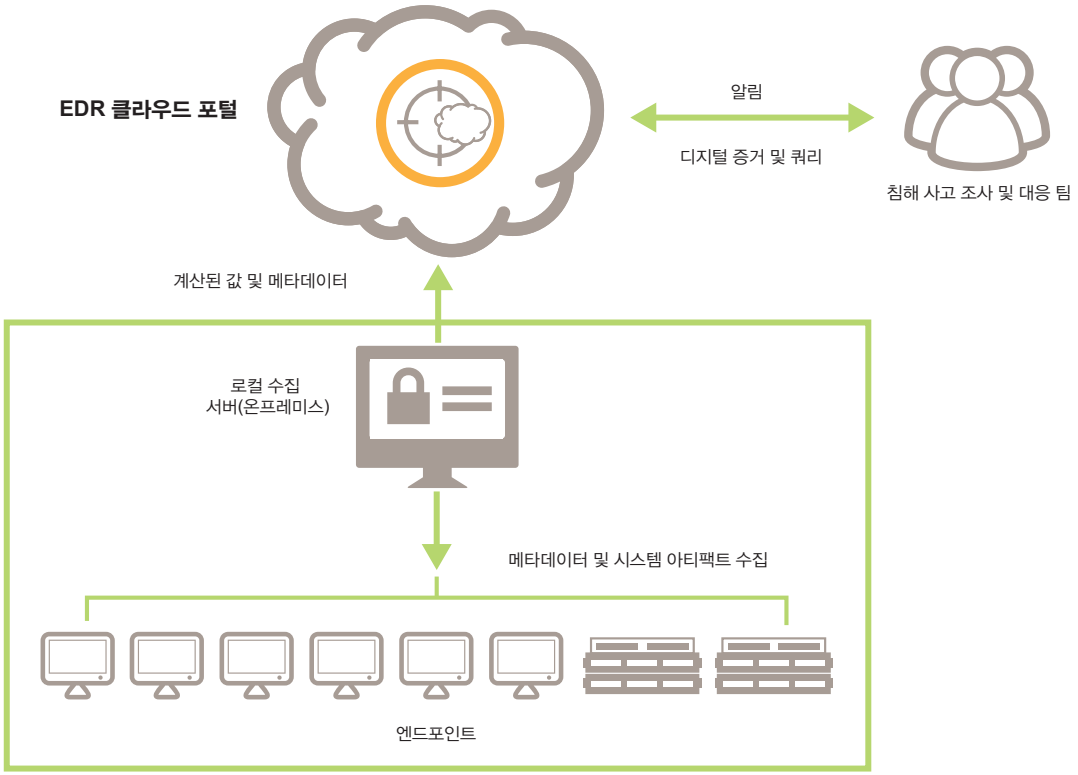


그림 1. Symantec EDR Cloud는 복잡한 사이버 데이터를 시각화하는 강력한 툴을 제공합니다.

작동 방식

아래 다이어그램에 나온 대로, Symantec EDR Cloud는 조사 전문가용 포털 및 하나 이상의 수집 서버로 구성됩니다. 포털은 조사 전문가용 인터페이스를 제공하며 보안 분석을 담당합니다. 이 솔루션은 엔드포인트로부터 데이터를 수집하고 탐지 목적으로 분석합니다. 또한 전사적 환경을 대상으로 쿼리를 수행하고 감염된 시스템을 치료하는 툴도 제공합니다.

Endpoint Detection and Response Cloud



온프레미스 서버는 중단 없이 여러 시스템으로부터 중요한 포렌식 분석 데이터를 수집합니다. 수집된 데이터에는 알 수 없는 파일, 프로세스 메타데이터, 프로그램, 서비스, 모듈, 파일, 자동 실행 프로그램, 사용자 행위, 네트워크 연결, 타임라인 등이 포함됩니다. 데이터 수집은 패시브 형태로 수행되고 60초 내에 실행되며 엔드유저 경험에는 전혀 영향을 미치지 않습니다.

요구 사항

브라우저 UI 요구 사항

버전 2.9는 Silverlight를 사용하므로 Microsoft Internet Explorer 11 이상이 필요합니다.

Version 3.0은 Mozilla Firefox 26 이상 및 Google Chrome 32 이상도 지원합니다.

수집 서버 요구 사항 - 데이터 볼트(Vault)

Windows 7 ~ Windows Server 2016

VMware, HyperV 가상 환경 지원

엔드포인트 요구 사항

Windows XP 이상

macOS Sierra, El Capitan, Yosemite

Redhat Linux 7.0 이상(32비트 및 64비트 버전)

CentOS, Mint, Cinnamon(32비트 및 64비트 버전)

참조:

1. 시만텍 인터넷 보안 위협 보고서(ISTR), 제22호

시만텍 소개

글로벌 사이버 보안 분야를 선도하는 시만텍은 기업, 정부 기관 및 개인의 중요한 데이터가 어디에 있든 안전하게 보호될 수 있도록 지원한다. 시만텍은 엔드포인트, 클라우드, 인프라 전반을 정교한 공격으로부터 방어할 수 있는 전략적인 통합 솔루션을 전 세계 기업과 기관에 제공하고 있다. 또한, 전 세계 5천만 이상의 개인사용자와 가정에서 시만텍 노턴 제품과 라이프록(LifeLock) 제품을 이용해 가정과 다양한 기기에서 디지털 라이프를 보호하고 있다. 시만텍은 세계 최대 규모의 민간 사이버 인텔리전스 네트워크를 통해 고도화된 지능형 위협을 탐지하고 고객들을 보호한다. 보다 자세한 정보는 시만텍 웹사이트(www.symantec.com/ko/kr)와 페이스북, 트위터, 링크드인을 통해 확인할 수 있다.

시만텍코리아 | 서울시 강남구 테헤란로 152강남파이낸스센터 28층 |
TEL: 02-3468-2000 | FAX: 02-3468-2001 | www.symantec.com/ko/kr

SYMC-DS-EDR_Cloud-KR-v1-bb