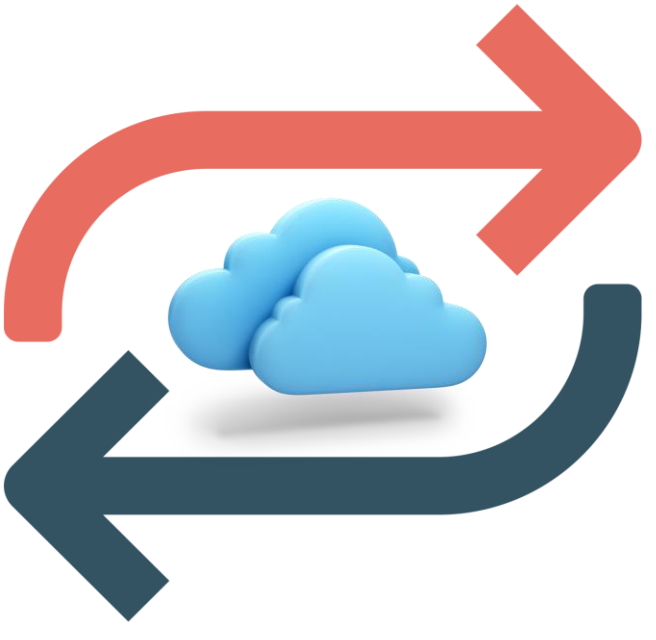
Ransomware Detection and Response 보안관제 서비스

Endpoint
EDR Agent 설치



A3Security의 RDR 보안관제 서비스는 EDR을 기반으로 한 MDR(Managed Detection and Response) 서비스입니다. 기존 전통적인 정보보안관제 서비스를 통하여 축적된 기술력을 바탕으로 하여 엔드포인트 보안을 책임지는 신규 서비스로 랜섬웨어에 대한 탐지와 대응을 전문으로 서비스를 제공합니다.

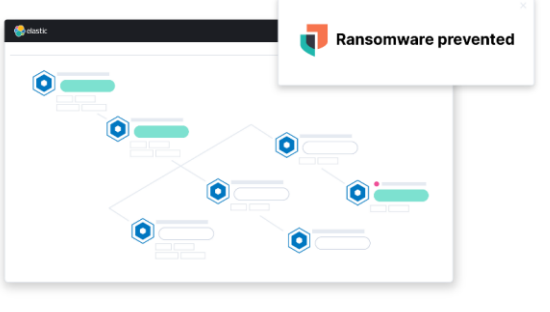
▪ 주요기능

● 24시간 365일 모니터링

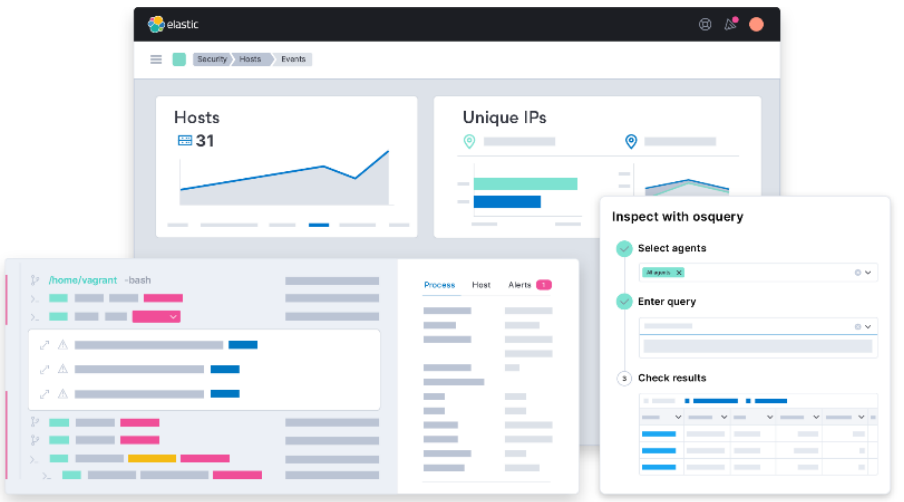
- 과학기술정보통신부 지정 정보보안관제 전문기업 지정
- 정보보안 전문가들의 24시간 365일 실시간 모니터링

● Ransomware Prevention

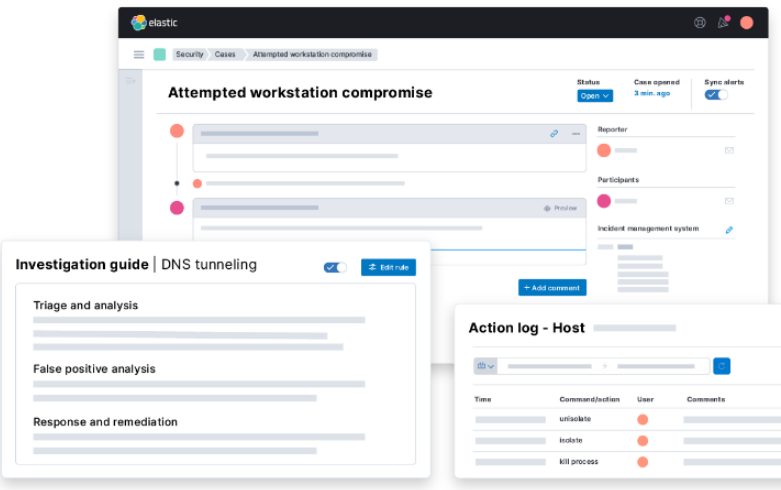
- 2020년에 랜섬웨어로 인한 피해가 20조 이상 발생한 것으로 추산되고 있으며, RaaS와 같이 산업화되어 광범위하게 위협이 확산되고 있는 상황입니다
- 행동 기반(Behavioral) 랜섬웨어 탐지 기능을 통해서 유사한 계열(Families)의 랜섬웨어들을 탐지하고 실행을 미연에 방지합니다.



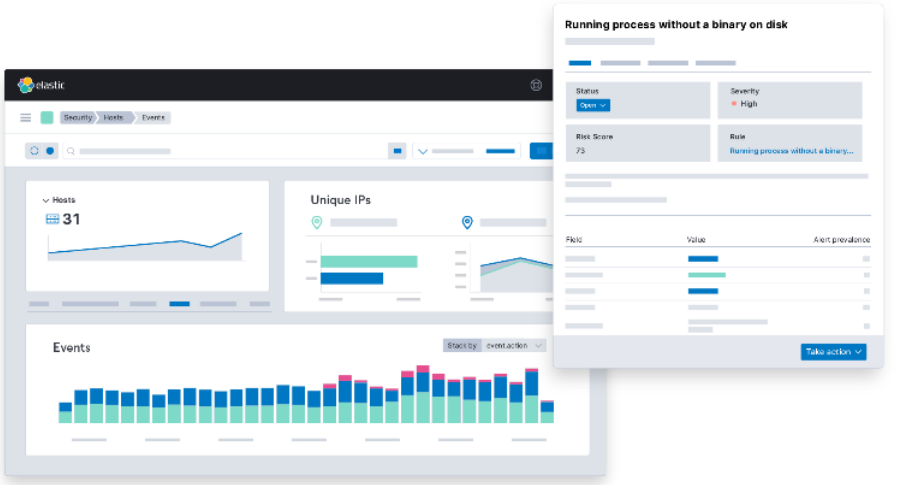
- **Malware Prevention**
  - Windows, macOS, Linux 시스템의 각종 Malware를 탐지하고 실행을 미연에 방지합니다
  - Machine learning 모델을 적용해서 복합적인 Malware에 대해서도 실행 전에 탐지하고 방어합니다



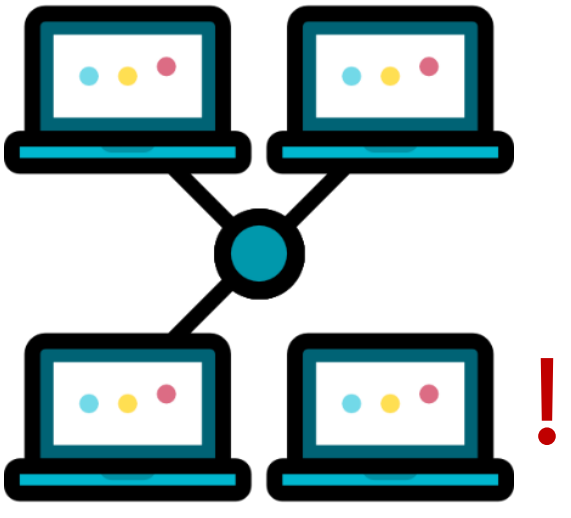
- **Memory Threat Protection**
  - Memory에서 바로 공격을 실행해서 파일 기반의 각종 탐지 기법을 우회하는 In Memory 공격들을 탐지하고 실행을 미연에 방지합니다
  - 탐지된 프로세스와 Thread를 자동으로 중지합니다



- **Malicious Behavior Protection**
  - 시스템 프로세스의 활동을 지속적으로 모니터링하여 악의적인 활동을 식별하고 해당하는 프로세스를 중지시켜서 해킹에 의한 피해를 미연에 방지합니다
  - Windows, macOS, Linux 호스트의 활동을 모니터링하여 Signature 기반으로 식별할 수 없는 복합적인 해킹 시도를 행동기반으로 탐지하고 방어합니다

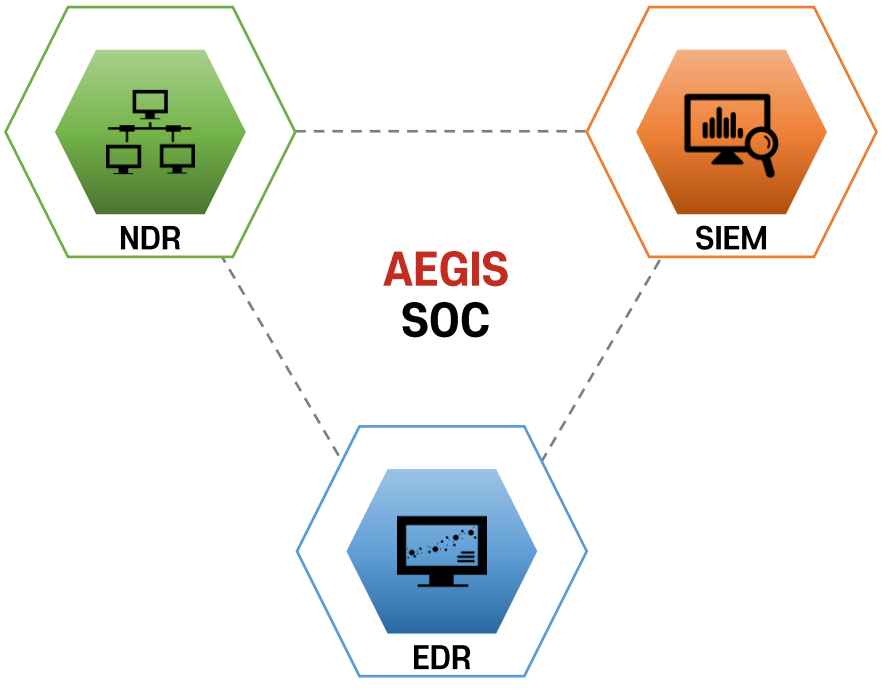


- **Host Isolation**
  - 원격에서 호스트를 격리하여 확산을 방지합니다



▪ Gartner SOC Visibility Triad 완성을 위한 시작

A3Security의 **RDR 보안관제 서비스** 도입으로 SIEM과 EDR을 완성하여,
Gartner가 제시한 SOC Visibility Triad를 완성해 나가시기를 바랍니다



▪ RDR 보안관제 서비스 도입 기대효과

- **랜섬웨어 탐지 및 차단**
  - RDR 보안관제 서비스는 시그니처 기반 방식 뿐만 아니라 행위 기반 탐지 및 휴리스틱 기술을 활용하여 알려지지 않은 랜섬웨어 변종과 새로운 위협을 식별할 수 있습니다.
    이를 통해 조기에 랜섬웨어 공격을 감지하고 차단할 수 있습니다

- **사전 예방 및 대응**
  - RDR 보안관제 서비스는 특정 행위 패턴과 이상 징후를 탐지하여 랜섬웨어 공격을 사전에 방지할 수 있습니다
  - 감지된 공격에 대해 AEGIS 팀이 실시간으로 대응 및 격리 조치를 취함으로써 랜섬웨어의 확산과 추가 피해를 최소화할 수 있습니다

- **인력 및 비용 절감**
  - RDR 보안관제 서비스는 귀사 보안 팀의 작업을 간소화하고 효율성을 높여줍니다.
    이를 통해 귀사 보안 팀은 더 중요한 작업에 집중할 수 있으며, 보안 위협으로 인한 업무 중단으로 인한 비용을 절감할 수 있습니다

- **보안 인사이트 제공**
  - RDR 보안관제 서비스는 보안 이벤트와 위협에 대한 상세한 정보와 분석 결과를 제공합니다.
    이를 통해 보안 팀은 조직의 보안 수준을 개선하고 약점을 보완할 수 있습니다

▪ 지원가능 OS

- **Windows, MacOS, Linux**

A3SECURITY
https://www.a3sc.co.kr
https://rdr.a3sc.co.kr

Head Office 서울특별시 영등포구 선유로9길 10(문래동6가, 문래 SK V1 center) 1710-11호
Security Operation Center 서울특별시 영등포구 선유로3길 10 하우스디비즈 1103호
Tel 02.2284.3388 **Fax 02.2284.3389**
aegis.sales@a3sc.co.kr

과학기술정보통신부 지정 정보보안관제 전문기업