조달청
Public Procurement Service

사이버리즌 EDR 조달청 디지털서비스몰 등록

글로벌 엔드포인트 솔루션 중 유일한 GS인증 1등급

두산디지털이노베이션은 사이버리즌 솔루션의 공공기관 도입을 위해
2022년 GS 인증 1등급을 획득했습니다.

조달청 디지털서비스몰에서 사이버리즌 EDR을 경험하실 수 있습니다.

디지털서비스몰 가기

*GS인증: 한국정보통신기술협회(TTA)가 기능적합성, 성능효율성, 호환성, 보안성 등 9가지 요소를 평가해 소프트웨어 품질을 증명해주는 국가 인증 제도

MITRE | ATT&CK™

2022-2023 2년 연속 마이터어택 테스트 최고 평가 솔루션

사이버리즌 EDR은 2023년 Turla의 정교한 공격 시뮬레이션 테스트에서 100%
역량을 입증했습니다.

- 100% 보호: 13개 공격 시퀀스 모두 발견 및 방어
- 100% 탐지: 유명 해커 단체인 Turla 19개 공격 단계 모두 탐지
- 100% 가시성: Windows와 Linux 시스템에서 143개의 테스트 공격 가시화
- 100% 실시간 탐지 : 모든 위협을 지연 탐지 없이 즉각적으로 감지
- 100% 즉시 사용 가능: 구성 변경 없이 즉시 사용이 가능한 완벽한 성능

영상으로 알아보기

DOOSAN

사이버보안 이제 두산디지털이노베이션에 물어보세요!

두산디지털이노베이션은 사이버리즌의 APAC 대표 파트너사로 사이버보안
컨설팅, PoC 및 구축, 기술 제공 뿐만 아니라 전문가 연동 및 고객사 대응
프로세스 수립을 지원합니다.

DDI에 문의하기

보안 담당자가 읽어보면 좋은
사이버보안 인사이트 리포트

DOOSAN ddi.marketing@doosan.com | www.doosandigitalinnovation.com | 두산디지털이노베이션

DOOSAN

두산디지털이노베이션

IT 보안부터 OT, xIoT 보안까지
모든 영역을 아우르는 사이버보안 전문가

두산디지털이노베이션

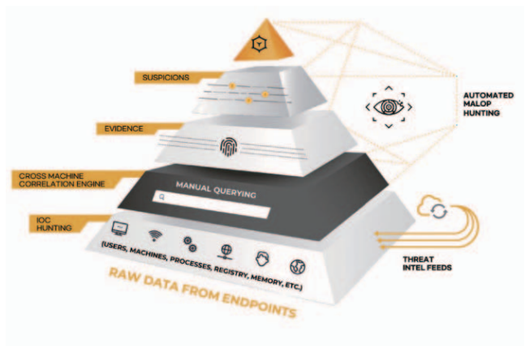
두산디지털이노베이션 | ddi.marketing@doosan.com | www.doosandigitalinnovation.com

DOOSAN cybereason

체계적인 방어부터 운영 최적화까지

사이버리즌(Cybereason)은 하나의 에이전트로 엔드포인트 보안 위협을 탐지 및 대응합니다

IT 보안



NGAV / EDR

*NGAV: Next-Generation Antivirus
*EDR: Endpoint Detection and Response

- ✓ SaaS(Cloud) 부터 On-Prem(구축형)까지 최고 수준의 보안 제공
- ✓ AI 기반 MalOp 엔진을 통해 방대한 데이터를 상관 분석하여 오탐을 제거해 공격 이벤트 감소
- ✓ 한눈에 탐지 가능한 가시성과 빠르고 정확한 탐지 및 대응

MDR

*MDR: Managed Detection and Response

- ✓ 4개의 글로벌 SOC
- ✓ 지능형 정오탐 분류
- ✓ 선제적 위협 차단
- ✓ EDR과 통합된 탐지 및 대응 서비스

IR / CA

*IR: Incident Response
*CA: Compromise Assessment

- ✓ DR과 결합된 IR
- ✓ TI팀과 숙련된 전문가의 완벽한 조치 (* TI: Threat Intelligence)
- ✓ 사고 상세 보고서
- ✓ 침해 진단 서비스(CA)

TAM

*TAM: Technical Account Management

- ✓ EDR 운영 최적화
- ✓ 교육, 지식공유, 점검, 설계, 기술지원
- ✓ 고객과 벤더 사이의 단일 창구

세계 최대 규모 글로벌 SOC(Security Operation Center)의 1-5-30 법칙

1 분 안에 탐지 하고 **5** 분 안에 분류하여 **30** 분 이내 조치합니다

- ▶ 24x7x365 보안 커버리지
- ▶ 업계 가장 빠른 탐지, 분류 및 조치
- ▶ 최고 수준의 보안 가시성, 신속성, 정확성을 제공
- ▶ 완벽한 매니지드 서비스로 EDR 운영 효율성 극대화

두산디지털이노베이션 | ddi.marketing@doosan.com | www.doosandigitalinnovation.com

DOOSAN CLAROTY

제조 기반 시설을 겨냥한 사이버 공격의 급증!

클래로티(Claroty)는 모든 사이버물리시스템(CPS)를 보호합니다

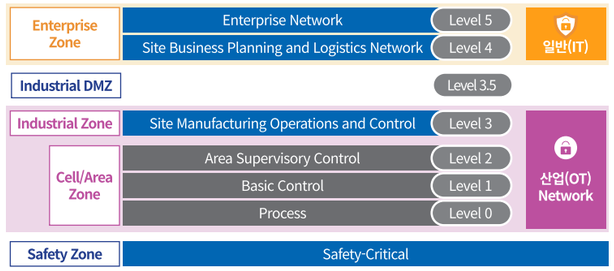
OT 보안

실시간 모니터링과 신속한 경고 알림

클래로티는 퍼듀모델(Purdue Model) 및 가상 영역(Virtual Zone) 기반으로 공격 확산을 막고 위협을 실시간 모니터링합니다.

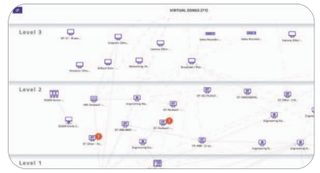
퍼듀모델로 네트워크를 6단계로 세분화해 액세스 위험을 최소화하고

전체 네트워크를 가상 영역으로 세분화해 이상 탐지 시 보안 담당자에게 실시간으로 경고를 보냅니다.



알려진 위협부터 비정상적 기능, 악의적인 행동 징후까지

고객의 OT/XIoT 자산에 최적화된 가시성을 제공해 보안 취약점(CVE)을 정확하게 식별합니다.



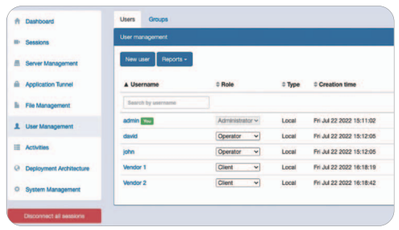
광범위한 가시성으로 네트워크를 자동 매핑 및 분류하고

사이버보안 사례와 자동 비교해 취약점을 정확하게 식별하고

5개 탐지엔진으로 오탐을 제거하고 실제 위협은 실시간으로 경고를 알립니다.

운영 환경에 영향 주지 않는 안정적이고 안전한 OT 원격 관리

OT 보안 표준 지침을 모두 충족하는 원격 관리 및 원격 제어로 잠재적 위협을 최소화합니다.



승인된 사용자만 원격 접속을 허용하며 역할 기반 액세스 제어로 제로트러스트 아키텍처를 구현합니다.

위협 경고 알림 발생 시 원격으로 직접 연결 해제가 가능하며 세션을 자동 녹화해 사후 대응 조치 및 조사에 활용합니다.

두산디지털이노베이션 | ddi.marketing@doosan.com | www.doosandigitalinnovation.com