산업 기업의 포괄적인 보안을 위한 확장된 탐지 및 대응(XDR) 플랫폼

Kaspersky Industrial CyberSecurity

kaspersky BRING ON THE FUTURE

악성 코드 공격

2024년 1분기에는 피해 조직 또는 담당관을 통해 공식적으로 확인한 사이버 보안 사건이 총 30건이었으며, 이러한 사건의 64.5%를 제조 부문이 차지했습니다.

Kaspersky ICS CERT(2024년 6월)

자세히 보기

APT 공격의 주요 대상:

중요 인프라 소유주 및 운영사

석유, 가스, 화학, 에너지, 유틸리티 부문에서 전략적으로 중요한 조직은 운영에 차질이 생길 경우 잠재적으로 상당히 큰 규모의 피해를 입게 됩니다.

중요 제조업

금속 및 광산업, 농업, 글로벌 제조 산업을 비롯한 중요 제조업 분야 기업은 단일 공장에서 전국 또는 전 세계 규모에 이르기까지 상당한 사건 비용이 수반되는 고위험 운영을 수행합니다.

2024년 초반의 산업 기업 대상 APT 및 금융 부문 공격에 대해 자세한 내용 확인하기

자세히 보기

산업 위협 환경

산업 인프라 소유자 및 운영자가 마주하게 된 새로운 현실은 자동화 시스템에 대한 핵티비스트의 관심 증가, 높은 수준의 규제 요구사항, IT-OT 컨버전스, 산업 부문 사이버 공격의 다양성 증가를 비롯한 여러 요소로 이루어져 있습니다(2024년 1분기에 Kaspersky's 카스퍼스키 솔루션에서는 산업 자동화 시스템에서 10,865개의 악성 코드군에 속한 악성 코드를 차단했음).

디지털 기술의 확산은 일반적으로 좋은 일로 여겨지지만, 사이버 범죄로부터 OT 환경을 보호하는 데 이용되던 IT 환경과 OT 환경 간의 갭을 사라지게 만드는 단점도 있습니다. ICS 환경에 유입된 플래시 드라이브 하나가 기업의 핵심 비즈니스에 심각한 영향을 미칠 수도 있지만, 해킹 조직이 OT 네트워크에 침투하여 상당한 피해를 초래하거나 중요한 정보를 탈취할 수도 있습니다. 자동화 표준이 일반적 권장사항에서 법적 요건으로 발전한 데다가 모범사례 공유 및 위험 관리의 필요성도 증가하여, 산업 기업의 사이버 보안은 매우 어려운 과제가 되고 있습니다.

Kaspersky ICS CERT에서 사이버 공격이 가중될 것으로 전망하는 산업 분야:

석유, 가스, 화학

이 분야 기업의 주요 경쟁 요인인 탐사, 추출, 운송, 정제의 디지털화는 IIoT, 드론, 로봇의 통합과 5G, 블록체인, VR 솔루션의 배포를 이끌어 내며 공격 환경이 확장되는 계기가 되기도 합니다.

중요 제조업

이 분야의 기업은 비용 효율성을 개선하고자 첨단 기술 배포, 연결 확장, 클라우드 활용, IT-OT 컨버전스 시나리오 탐색을 진행하는데, 이러한 모든 활동이 새롭고 지속적으로 변화하는 위협에 대한 노출을 증가시키는 결과를 초래합니다.

광물, 금속, 광산업

필수 불가결하고 국가적으로도 중요한 제조업의 초석이 되는 이 산업은 비용 균형을 맞추면서도 자동화 및 디지털 기술을 도입해야 합니다. 핵티비스트와 잠재적 공격 조직 모두가 노리는 표적이라는 점을 감안하면 사이버 보안에 대해서는 적당히 타협할 수 없습니다.

전력, 전력망, 유틸리티

여전히 에너지 시설 대부분의 근간이 되는 기존 인프라를 유지하면서 에너지 전환을 추진하려면 디지털 및 신기술이 필수적입니다. 그러나 이는 매우 큰 위험이기도 해서 추가적인 사이버 보안 노력이 요구됩니다.

산업 시스템, 특히 ICS 및 SCADA에 대한 공격이 증가하고 있습니다. 한편, 산업 환경을 대상으로 하는 오늘날의 사이버 위협은 기존 솔루션에 대해 내성이 있는 것으로 보입니다. 이러한 상황에서 카스퍼스키는 해당 산업에 대한 포괄적인 접근 방식을 제공합니다. 고객 성공 사례, 위협 환경 분석 정보, 시나리오별 전용 제품은 카스퍼스키 웹사이트에서 확인할 수 있습니다.

산업 사이버 보안과 기업 사이버 보안 간에 겹쳐지는 요소에 대한 심층적인 지식과 광범위한 첨단 보안 기술 제공 능력을 갖춘 신뢰할 수 있는 파트너를 선택하는 것이 그 어느 때보다 중요합니다.

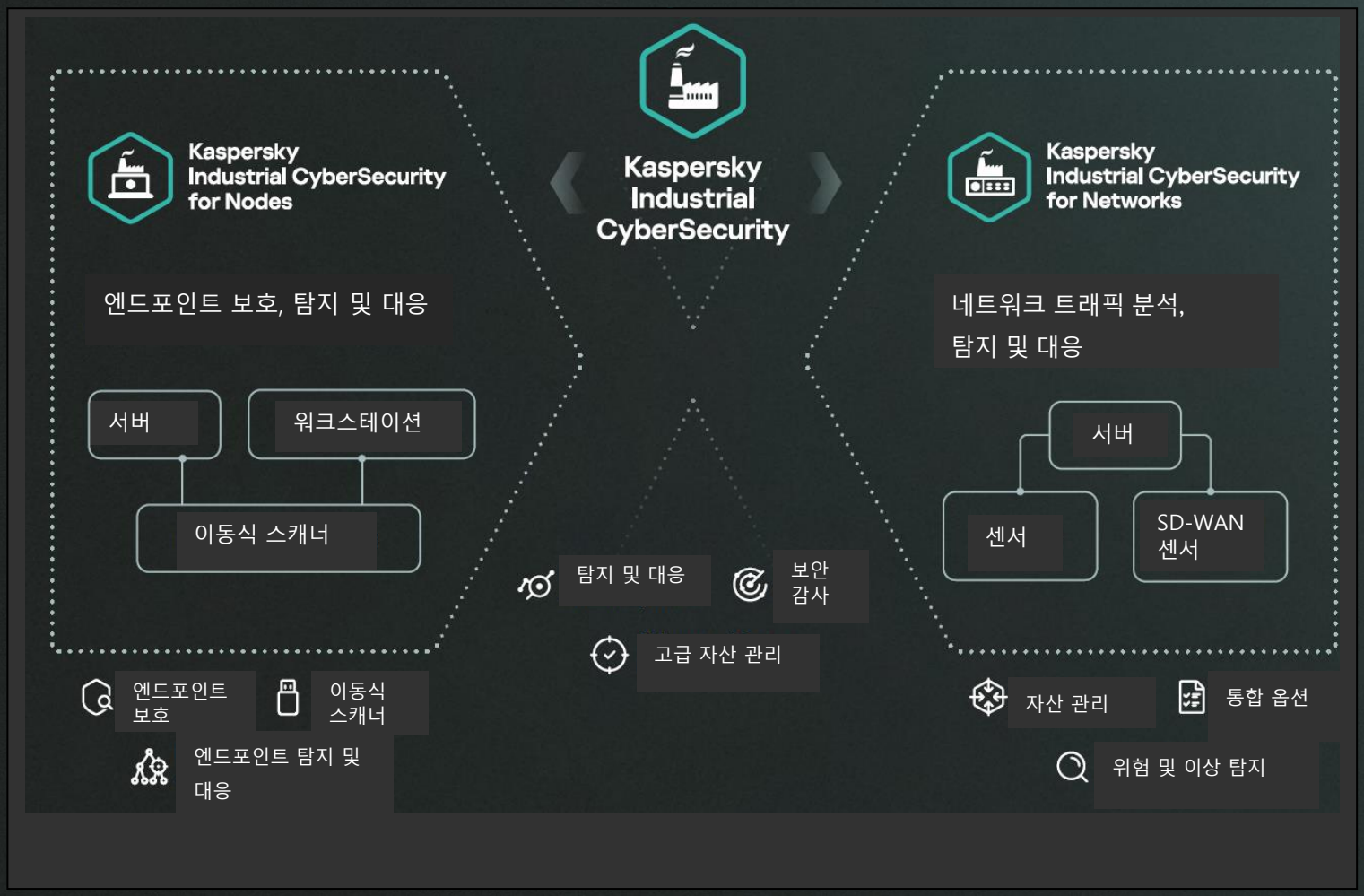
고급 ICS 보안 기술

사이버 범죄로부터 OT 환경을 보호하는 데 이용되던 IT 환경과 OT 환경 간 갭은 갈수록 줄어들고 있으며, 이로 인해 중요 인프라 보호를 위한 포괄적인 엔터프라이즈급 단일 벤더 보안 솔루션은 이제 사이버-물리적 시스템의 소유자 및 운영자에게 필수가 되었습니다. **Kaspersky Industrial CyberSecurity (KICS)** 네이티브 XDR 플랫폼은 KICS for Networks와 KICS for Nodes 구성요소로 이루어져 있으며 산업 자동화 시스템 및 네트워크를 보호합니다.

KICS for Networks는 트래픽 분석, 탐지 및 대응 제품으로, 산업 네트워크 모니터링, 침입 탐지 및 위험 관리 기능을 제공하는 동시에 산업 네트워크 노드의 취약점, 산업 표준 준수에 대한 중앙 집중식 감사 기능도 갖추고 있습니다. **KICS for Nodes**는 OVAL* 기반 규제 준수 감사 기능을 갖추어 산업 등급의 엔드포인트 보호, 탐지 및 대응 기능을 제공합니다. 이 모듈식 저영향 솔루션은 Linux, Windows, 레거시, 독립형 시스템 및 PLC와 함께 사용할 수 있습니다. 이동식 스캐너 버전은 설치할 필요 없이 독립형 시스템 및 계약업체 기기를 보호합니다.

이러한 구성요소가 결합되어 KICS XDR 플랫폼을 형성하며, 이는 중앙 집중식 자산 인벤토리, 위험 관리 및 감사 기능을 제공하고 사건, 분석 등에 대해 종학적인 그래프를 제시하는 단일 플랫폼을 통해 다양한 분산 인프라 전반에 걸쳐 보안 범위를 확장할 수 있습니다.

KICS XDR 플랫폼을 통해 사용자는 아직 트래픽 미러링을 사용할 수 없는 세그먼트에서도 네트워크 및 엔드포인트 수준의 연속 사건, 정확한 자산 매개변수, 네트워크 통신 및 토폴로지 맵 등, 상황과 맥락을 더 크고 광범위하게 파악할 수 있습니다.



* Open Vulnerability and Assessment Language (OVAL)

플랫폼 애플리케이션 개요

OT 및 IT 환경의 컨버전스

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

DMZ / GTW

IT 환경

OT 환경

운영자 워크스테이션

SCADA 서버

엔지니어 워크스테이션

ICS 게이트웨이

SPAN

네트워크 장비

베이 제어 유닛(BCU)

지능형 전자 장치(IED)

프로그래밍 논리 제어기(PLC)

릴레이 보호 및 안전 계측 시스템(SIS)

격리된 노드(KICS 이동식 스캐너를 사용하여 수동 확인)

물리적 수준

조기 이상 탐지 및 예측 분석

Kaspersky Machine Learning for Anomaly Detection(Kaspersky MLAD)은 신경망을 사용하여 광범위한 텔레메트리 데이터를 동시 모니터링하는 혁신적인 시스템입니다. 이 시스템은 고장 및 사고 방지를 위해 장비 결함 및 인적 오류를 탐지하고, 비정상적인 직원 행동 또는 장비 작동을 전문 공격 또는 사보타주 징후로 식별하며 이상 탐지 기능을 장비 상태 및 수명주기에 대한 예측 분석과 결합합니다.

자세히 보기

카스퍼스키 제품으로 보호

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

산업 네트워크 모니터링 및 트래픽 분석 솔루션. 자체 산업 프로토콜에 대한 DPI(심층 패킷 검사) 가능. 소프트웨어 또는 가상 어플라이언스로 제공.

KICS for Networks는 ICS의 이상 징후와 침입을 초기에 식별하고 네트워크 및 노드에서의 공격 전개 과정을 보여주며(EDR 킬 체인 및 텔레메트리) 산업 프로세스에 미치는 부정적 영향을 방지하기 위해 필요한 조치를 취하도록 지원합니다.

자산 관리

자산 검색
취약점 데이터베이스, 위험 우선순위 지정, 안전한 액티브 폴링으로 자산에 대한 분석 정보 확보

네트워크 가시성
최고의 가시성을 확보할 수 있도록 트래픽 모니터링, 토폴로지 맵 구성, 시간 경과에 따른 네트워크 보안 태세 추적

트래픽 분석 도구
네트워크 세션을 추적 및 분석하여 상세 트래픽 데이터의 내보내기 및 저장 가능

장점
- 산업 애플리케이션 및 프로토콜 전문 솔루션. 광범위한 OT 프로토콜, 기기, 네트워크 공격에 대해 바로 이용 가능한 지원 기본 제공 + 외부 프로젝트에서 가져오기 가능
- 사전 설정된 보안 감사 구성 규칙
- 손쉽게 사용할 수 있는 인터페이스와 맞춤형 보고서
- 분산 인프라 전반에 걸친 완벽한 위험 인식
- 다양한 소스(자체 네트워크 센서, SD-WAN 센서, 엔드포인트 센서, 이동식 프로브)에서 트래픽 샘플 수집

생태계 및 통합

생태계
다음 솔루션과의 통합 및 제품 간 통합 사이버 보안 접근 방식으로 카스퍼스키 생태계의 광범위한 기능을 활용할 수 있음

- Kaspersky NextXDR Expert
  자세히 보기
- Kaspersky IoT Secure Gateway (KISG)
  자세히 보기
- Kaspersky Machine Learning forAnomaly Detection (MLAD)
  자세히 보기
- Kaspersky Software-Defined Wide Area Network (SD-WAN)
  자세히 보기

단일 콘솔을 통해 생태계를 구성하는 모든 요소 관리

타사 제품 통합
다양한 외부 보안 도구 및 플랫폼과 원활한 호환 가능

위협 및 이상 탐지

침입 탐지
시그니처 기반 탐지 및 통계 엔진으로 무차별 대입 또는 스캔 시도를 탐지

네트워크 무결성 제어
시스템이 정상 네트워크 상호작용을 학습하여 이탈 시마다 경고

이상 탐지
기본 패킷 및 프로토콜 수준의 이상 징후 탐지. MLAD로 기능 강화 가능

산업 프로토콜 DPI
프로세스 및 C&C를 유지 관리하고 텔레메트리 데이터를 효율적으로 추적

이벤트 상관관계 분석
MITRE 분류 및 단일 킬 체인으로 보안 이벤트 연관성 파악

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

테스트 및 인증을 거친 산업 등급의 엔드포인트 보호, 탐지 및 대응 기능. 시스템에 미치는 영향이 적으며 호환성이 우수하고 안정적인 Linux, Windows, 독립형 시스템용 솔루션.

KICS for Nodes는 오늘날의 관리형 및 분산 디지털 자동화 시스템 내 모든 엔드포인트를 보호합니다. 이 솔루션은 텔레메트리를 수집하여 워크스테이션, 서버, 게이트웨이 및 기타 엔드포인트에서 사건의 진행 상황을 분명하고 상세한 시각적 표현으로 제시하므로, 자동화 시스템 관리자는 사건이 완전히 처리되었으며 다시 발생하지 않을 것을 확신할 수 있습니다.

엔드포인트 보호

실시간 위협 방지
이동식 드라이브 및 중요 영역에 대한 맞춤 온디맨드 검사를 통해 익스플로잇을 방지하고 파일을 보호

로컬 활동 제어
기기 및 Wi-Fi 제어 기능. 전체 로컬 활동 인식을 위한 PLC 프로젝트 무결성 확보.

네트워크 활동 제어
호스트 방화벽 관리 및 네트워크 세션 차단을 통해 네트워크 위협으로부터 안전하게 보호

시스템 모니터링
파일 무결성 검증, 레지스트리 접근 추적, 시스템 로그의 위협 탐지를 통해 OS 보안 확보

엔드포인트 탐지 및 대응

탐지
침해 지표(IoC) 검사, 포괄적인 모니터링 및 보고 기능

대응
실행 방지, 파일 격리/삭제, 프로세스 시작/종료, 네트워크 격리 등

Windows 노드
Linux 노드
이동식 스캐너
감사 에이전트

이동식 스캐너

악성 코드 스캐너
독립형 장비 및 산업 현장에 놓인 모든 컴퓨터에 대해 안티 맬웨어 검사

OVAL 스캔
수동 취약점 및 규제 준수 검사를 통해 독립형 시스템에 사이버 보안 정책 적용

패킷 캡처
네트워크 트래픽을 캡처 및 분석하여 격리된 인프라에 대해서도 탁월한 인식 기능 활용 가능

기본 자산 인벤토리
무설치 솔루션으로 하드웨어 및 소프트웨어에 대한 포괄적인 데이터 수집

장점

- 보호 대상 기기에 미치는 영향이 적고 리소스 소비를 조정할 수 있음
- 기존 OS 및 산업 자동화 벤더와의 호환성
- 기본 보안 구성 및 모든 유형의 위협으로부터 호스트를 보호하는 고급 옵션
- 모듈식 배포 및 비침투적 설정
- PLC 지원: Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4; Schneider Electric Modicon M340, M580; CODESYS V3 장치; Fastwel CPM723-01
- 유연한 라이센싱 옵션(1개월 ~ 5년)
- 가장 널리 사용되는 ICS에 대하여 검증된 효율적인 구성 사전 설정

- 게이트웨이
- 히스토리언 서버
- SCADA 서버
- 운영자 워크스테이션
- 임베디드 시스템
- 시스템 관리 워크스테이션
- 엔지니어링 워크스테이션

KICS 플랫폼의 다양한 활용

산업 현장 및 기업 세그먼트 전반에 걸친 통합 사이버 보안

네이티브 OT XDR

Kaspersky Industrial Cybersecurity의 핵심 구성요소인 KICS for Networks와 KICS for Nodes는 통일되고 결합도가 높은 경험을 지원하기 위해 카스퍼스키 생태계 내에서 원활하게 연동하도록 설계되었습니다. 함께 구매할 경우 유용한 제품 간 교차 기능이 추가로 제공되는 네이티브 XDR 플랫폼을 형성할 수 있습니다.

고급 자산 관리

엔드포인트 하드웨어 인벤토리

인프라 전반의 모든 연결된 기기에 대해 포괄적인 가시성을 확보하여 정확한 자산 추적이 가능하며 보안 관리 기능이 향상됨

애플리케이션, 사용자, 패치 인벤토리

사용 중인 환경 내의 소프트웨어 배포, 사용자 접근, 패치 상태에 대한 상세 분석 정보. 적절한 관리를 위해 데이터가 강화되고 잠재적 취약점은 감소.

엔드포인트 트래픽 모니터링

각 엔드포인트에서 데이터 흐름의 무중단 모니터링을 실시하여 비정상적 패턴이나 잠재적 위협을 신속하게 탐지하므로, 의심스러운 활동에 대한 신속한 대응 가능

보안 감사

취약점 검사

철저한 자산 검사를 통해 보안 취약점을 평가하고 위험 인식을 향상시키며 시기적절한 대응을 지원하고 전반적 보안 태세를 강화

규제 준수 감사

OVAL 및 XCCDF* 산업 표준 준수를 위한 에이전트 기반 감사 및 에이전트리스 감사. 완전한 기능을 갖춘 편집기, 중앙 집중식 보고서 데이터베이스, 노드 자격증명을 위한 보호 볼트(vault) 등.

구성 제어

안전한 자산 구성 지원, 보안 위험 관련 변경 추적, 하드웨어 및 소프트웨어 자산에 대한 기본 무결성 유지

탐지 및 대응

탐지

킬 체인을 포함한 호스트-네트워크 이벤트 상관관계 분석을 통해 위협 식별 기능 향상 및 간소화. 사건에 대해 심층적인 지식을 얻을 수 있도록 네트워크 경고 데이터 강화.

대응

실행 차단, 호스트 격리 및 파일 격리를 통한 강력한 위협 완화 기능 제공. 원활한 방화벽 통합으로 빠르고 효과적인 보안 사건 대응 능력이 더욱 향상됨.

개방형 OT XDR

상관관계 분석 엔진, 자동 대응 기능, 타사 커넥터를 통해 EDR 솔루션의 기능을 확장하고, Kaspersky XDR Core 솔루션으로 KICS 플랫폼을 강화하여 다음과 같은 장점을 활용할 수 있습니다.

- 정보 보안 이벤트(SIEM)의 포괄적인 모니터링 및 상관관계 분석, 다양한 시스템과의 통합
- 위협 인텔리전스 강화 및 관리

단일 IT-OT XDR

IT와 OT의 경계를 넘어 최고의 IT-OT 컨버전스 경험을 제공합니다. KICS 플랫폼을 Kaspersky Next XDR Expert 패키지와 결합하여 사용하면 최고 수준의 카스퍼스키 엔드포인트 보호 기능을 활용하고 다음과 같은 이점을 누릴 수 있습니다.

- Kaspersky Single Management Platform을 통한 단일 조사 그래프, 대응 계획서 및 사건 관리
- IT 인프라에 대한 복합 보호 기능(IT XDR)

산업용 XDR

Kaspersky Industrial CyberSecurity

자세히 보기

Kaspersky Single Management Platform

기업용 XDR

Kaspersky Next XDR Expert

자세히 보기

* Extensible Configuration Checklist Description Format (XCCDF)

27년에 걸친 세계 최고의 경험과 페타바이트 규모의 위협 데이터

ICS CERT

ICS CERT — 카스퍼스키 자체 글로벌 OT/IoT 보안 연구 부서

IT/OT 보안 업계에서 다수의 수상 및 성과로 입증된 전문성

다양한 자동화 벤더 솔루션과의 호환성에 대한 200여 종의 인증

입증된 기술 효과, 표준 및 요구사항의 준수

전 세계의 다양한 고객

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

자세히 보기

www.kaspersky.com

#kaspersky
#bringonthefuture