Kaspersky Industrial Cyber Security (KICS)

HangRo Lee
hangro.lee@kaspersky.com
82-10-6397-7456

kaspersky

내용

산업 사이버 위협

As digital business blurs the digital and physical worlds, digital breaches result in physical damage.

디지털 비즈니스가 디지털 및 물리적 세계의 경계를 허물게 됨에 따라 디지털 침해는 물리적 피해를 초래합니다.

Gartner

ICS 대상 최근 주요 공격들 (2017-2020)

Cost of Norsk Hydro Cyber Attack Higher than Expected at Nearly $75 Million

July 24, 2019 by Gwladys Fouche

REUTERS

Aluminum producer Norsk Hydro has managed to ramp up operations at its Alunorte refinery in Brazil despite a cyber attack in March, the firm said on Tuesday, boosting its shares.

The Norwegian company's stock rose as much as 6% in early trade after it also reported a slightly

SECURITYWEEK NETWORK: Information Security News | Infosec Island | CISO Forum

SECURITYWEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe | 2019 CISO Forum, Presc

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Securit

Home > Cyberwarfare

Triton Malware Exploited Zero-Day in Schneider Electric Devices

By Eduard Kovacs on January 18, 2018

The recently discovered malware known as Triton and Trisis exploited a zero-day vulnerability in Schneider Electric's Triconex Safety Instrumented System (SIS) controllers in an attack aimed at a critical infrastructure organization.

The malware, designed to target industrial control systems (ICS), was discovered after it caused a shutdown at an organization in the Middle East. Both FireEye and Dragos published detailed reports on the threat.

Triton is designed to target Schneider Electric Triconex SIS devices, which are used to monitor the state of a process and restore it to a safe state or safely shut it down if parameters indicate a potentially dangerous situation. The malware uses the TriStation proprietary protocol to interact with SIS controllers, including read and write programs and functions.

Schneider initially believed that the malware had not leveraged any vulnerabilities in its product, but the company has now informed customers that Triton did in fact exploit a flaw in older versions of the Triconex Tricon system.

The company says the flaw affects only a small number of older versions and a patch will be released in the coming weeks. Schneider is also working on a tool - expected to

ITProPortal

News Best VPN Best Antivirus Guides Reviews Features Categories

What you need to know about the Petya and WannaCry cyber attacks

By Sam Reed August 07, 2017 Security

Financial losses, data breaches and reputational damage are just some of the ways a cyber-attack can hit an organisation hard.

Financial losses, data breaches and reputational damage are just some of the ways a cyber-attack can hit an organisation hard.

The Petya and WannaCry cyber-attacks in May and June are two of the biggest in history and impacted the finances of companies throughout the globe. A recent report by the insurers Lloyd's of London said a major cyber-attack has the potential to cost as much as a natural disaster.

WannaCry, which affected numerous organisations, including the NHS, spread to 150 countries and is estimated to have cost the global economy £6bn.

Petya caused problems with shipping and invoicing for Neurofen manufacturers Reckitt Benckiser, who are expecting to make losses of about £100m as a result of the attack. Some of the world's largest organisations including Cadburys and Oreo cookies manufacturer Mondelez were also affected by Petya.

A cyber-attack can also lead to a fine for a data breach - a prospect that will become even more real when the new General Data Protection Regulation is introduced in May 2018.

How WannaCry and Petya worked

To begin with, both attacks were referred to as ransomware attacks because they locked people out of their computers and demanded payment to let them back in.

Some cybersecurity experts now believe Petya was not a ransomware attack because it was incredibly difficult to pay the hackers. Ransomware attacks usually make it very easy to make payment. They sometimes even offer step by step guidance and a help centre.

Instead, they believe the malware which they are now calling NotPetya, was designed to spread damage rather than collect money. They have suggested the attack may have been disguised as ransomware to make it appear to be criminal led when it may have been state sponsored.

United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE

MIDDLE DISTRICT of LOUISIANA

U.S. Attorneys » Middle District of Louisiana » News

Department of Justice

U.S. Attorney's Office

Middle District of Louisiana

SHA

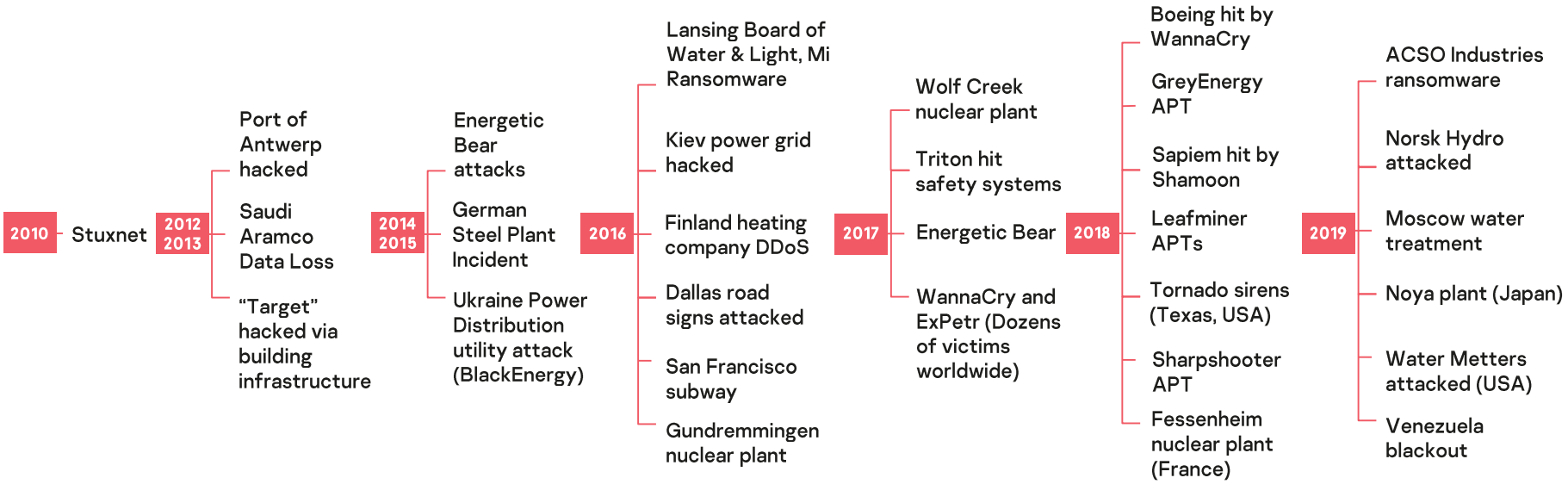
FOR IMMEDIATE RELEASE

Thursday, February 16, 2017

Former Systems Administrator Sentenced to Prison for Hacking into Industrial Facility Computer System

BATON ROUGE, LA – United States Attorney Walt Green announced today that BRIAN P. JOHNSON, age 44, of Baton Rouge, Louisiana, has been sentenced to serve thirty-four (34) months in federal prison, as a result of his conviction for hacking into the computer system of an industrial facility to disrupt and damage its operations, in violation of Title 18, United States Code, Section 1030(a)(5)(A). Chief U.S. District Judge Brian A. Jackson ordered JOHNSON to pay restitution to Georgia-Pacific in the amount of $1,134,828, pay a $100 special assessment to the United States, and

매년 발생하고 있는 매우 중요한 사회 기반 시설들 해킹 사례



어떻게 발생했는가? – BlackEnergy 예

스테이지 1 - 침입

피싱 이메일
+
BlackEnergy 악성코드
↓
VPN & 자격 증명 도용
Network & Host 발견

스테이지 2 – ICS 공격

악성 펌웨어 개발
SCADA 장악 (HMI/클라이언트)
↓
브레이커 열기 명령
↓
UPS 수정
펌웨어 업로드
Killdisk로 덮어쓰기
↓
정전

왜 일어나는가?

대기업 인프라스트럭쳐
인적 요소
공급망 공격

IT와 격리되지 않은 OT
OT 통신의 비가시성
취약한 OT 구성요소

https://www.kaspersky.com/resource-center/threats/blackenergy

랜싱 BWL, 미시간 2016

http://www.lansingstatejournal.com/story/news/local/2017/03/08/11-months-later-insurance-still-reviewing-bwl-cyber-attack/98847680/

도시 소유 유틸리티

피싱 공격

크립토 랜섬웨어

$25,000 몸값 요구

$2.4M 비용 / **$1.9M** 보험 청구

BWL 사이버 공격을 보험사가 리뷰하기 위해 11개월 이상을 사용했습니다.

산업 사이버 위협 동향

Kaspersky ICS CERT

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

최신 위협, 보안 사고 및 완화 전략에 대한 인텔리전스부터 사고 대응 및 조사 컨설팅과 서비스에 이르는 다양한 정보 서비스를 제공하는 특수 비상업적 프로젝트입니다.

KASPERSKY ICS CERT

Industrial Systems Emergency Response Team is a special Kaspersky project that will offer the wide range of information services, starting from the intelligence on the latest threats and security incidents with mitigation strategies and all the way up to incident response and investigation consultancy and services. In addition to the latest intelligence about threats and vulnerabilities, Kaspersky's Industrial CERT will share expertise on compliance. Being a non-commercial project, ICS CERT will share information and expertise to its members free of charge.

SERVICES | ALERTS | REPORTS | CONTACTS

ALERTS

Targeted attacks on industrial companies using Snake ransomware (updated)
17 June 2020

MORE ALERTS

EVENTS

Kaspersky conducts ICS digital forensics and incident response training course in China
30 January 2020

Applied industrial cybersecurity by Kaspersky at the Deggendorf Institute of Technology
25 November 2019

7th Kaspersky Industrial Cybersecurity Conference
01 November 2019

REPORTS

Steganography in attacks on industrial enterprises (updated)
17 June 2020

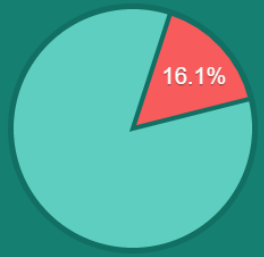
Overview of recommendations on organizing secure remote work for critical infrastructure and other facilities
30 April 2020

Threat landscape for industrial automation systems. 2019 Report at a glance
24 April 2020

Threat landscape for industrial automation systems. Vulnerabilities identified in 2019
24 April 2020

Threat landscape for industrial automation systems. APT attacks on industrial companies in 2019
24 April 2020

Percentage of industrial computers attacked, June 2020



Top countries by percentage of industrial computers attacked, June 2020

https://ics-cert.kaspersky.com/

연구 방법론

실시간 빅 데이터 기반
보고서에 제시된 통계 데이터는 카스퍼스키 제품에 의해 보호되는 약 200,000개 이상의 ICS 컴퓨터로부터 수신된 데이터입니다

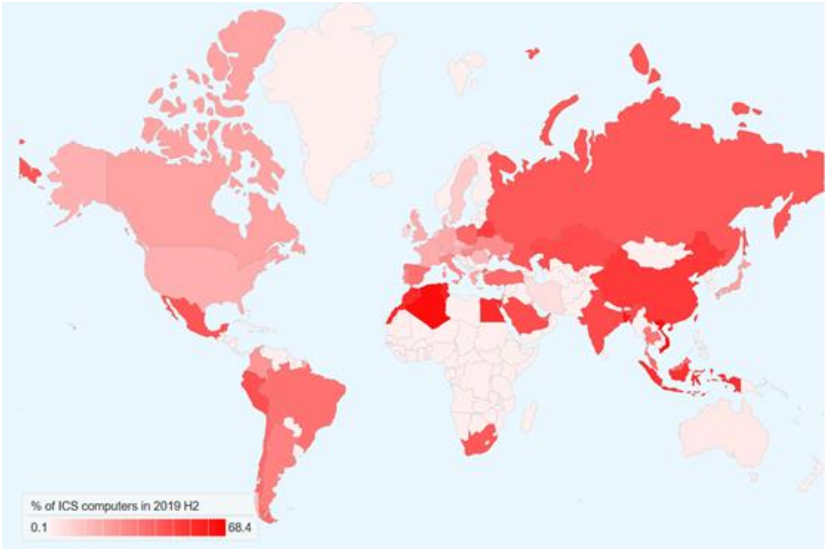
대표적인 ICS 구성요소
SCADA 서버, 히스토리안 서버, OPC, 운영자 및 엔지니어링용 워크스테이션, 랩탑, HMI, 관리 서버

목표 데이터
보고 기간동안 익명화된 정보 안에서 공격 당한 컴퓨터 수와 총 컴퓨터 수의 비율을 사용

Public:
https://ics-cert.kaspersky.com/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/

ICS 사이버 위협 동향: 지리학 기반

공격당한 ICS 컴퓨터의 지리학적 분포*, H2 2019
*악의적인 객체가 차단된 ICS 컴퓨터의 백분율



소스: Kaspersky ICS CERT 리포트 'Threat landscape for industrial automation systems H2 2019'

상위 리더

아프리카, **동남아시아** 및 **남아시아, 베트남 등이 악성 활동이 차단된 ICS 컴퓨터의 비율을 기준으로 상위 순위에 위치하였습니다.**

TOP 5에는 **알제리, 튀니지, 모로코 및 이집트가 포함됩니다.**

러시아에서는 **43.1%**의 ICS 컴퓨터에서 악의적인 객체가 차단되었습니다.

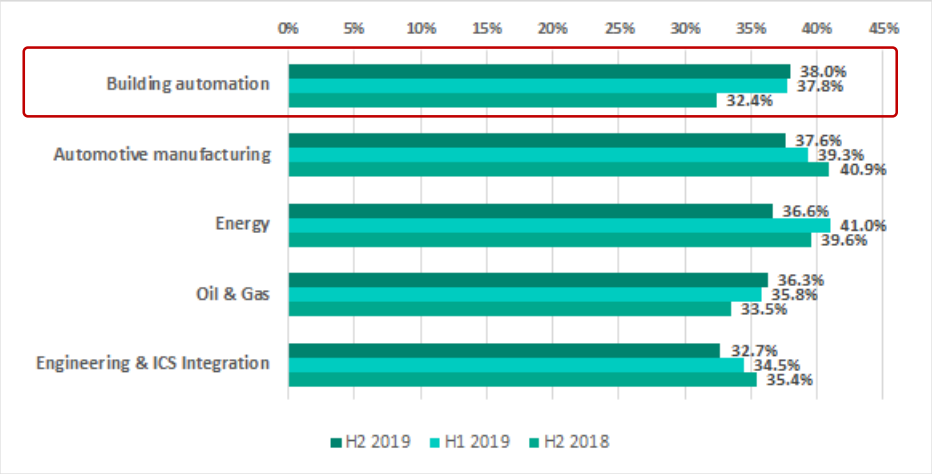
가장 안전한 나라

아일랜드 (7.3%), **스웨덴** (10.3%) 및 **덴마크** (11,6%)

특히 악의적인 활동이 차단된 ICS 컴퓨터의 비율은 6개월 연속 감소하고 있습니다.

ICS 사이버 위협 동향 : 산업

악의적인 객체가 차단된 ISC 컴퓨터의 백분율을 기준으로 나열한 산업 순위



소스: Kaspersky ICS CERT 리포트 'Threat landscape for industrial automation systems H2 2019'

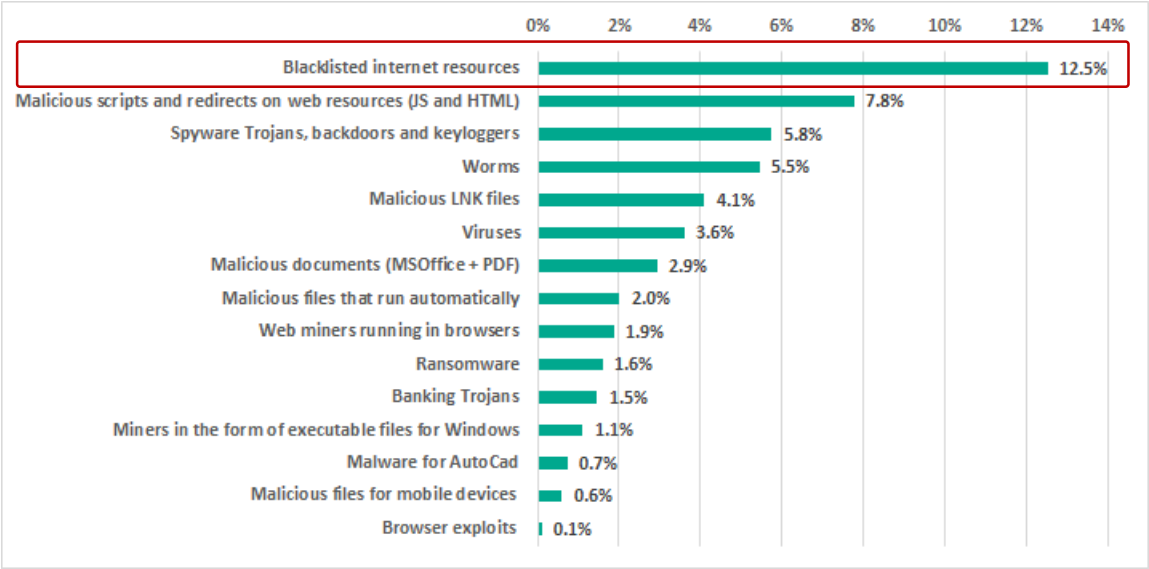
가장 많이 공격된 산업

공장 자동화 영역이 악의적인 객체가 차단된 ISC 컴퓨터 중 가장 높은 비율 (38%)을 차지했습니다.

공격 강도는 거의 동일하게 유지

H2 2019에 **ICS 컴퓨터의 39.2%**가 악성 객체를 차단했으며 H1 2019년에는 41,2 그리고 H2 2018년에는 40,8% 차단했습니다.

ICS 사이버 위협 동향 : 악성코드



소스: Kaspersky ICS CERT 리포트 'Threat landscape for industrial automation systems H2 2019'

ICS 컴퓨터가 일반적인 악성코드에 의해 공격당했습니다

블랙리스트에 있는 인터넷 리소스가 가장 빈번한 위협입니다.

피해자는 있지만 타겟은 아닙니다

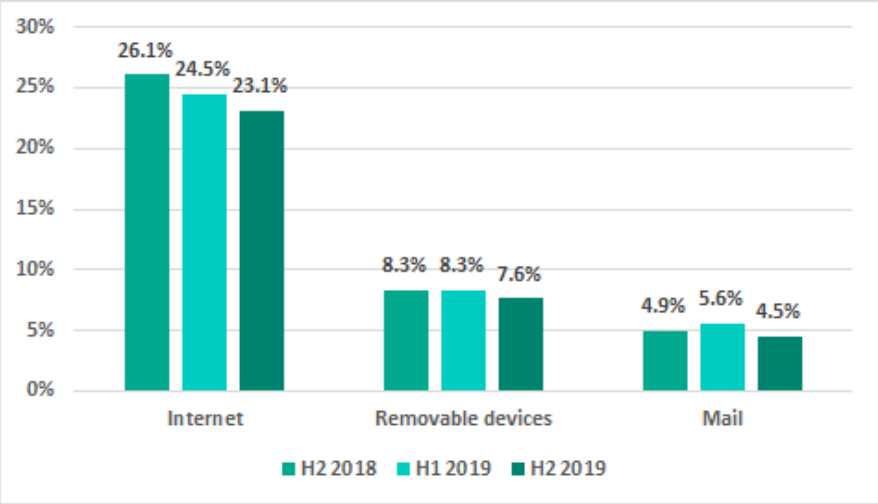
관찰된 위협의 특성은 심지어 가끔 감염이 발생한다는 것을 보여줍니다

낮은 레벨의 보호 수준

동기 부여된 해커가 침입할 수 있는 가능성이 높습니다

ICS 사이버 위협 동향 : 소스

ICS 컴퓨터에서 차단된 위협의 메인 소스*
* 서로 다른 소스의 악의적인 객체가 차단된 ICS 컴퓨터의 백분율



소스: Kaspersky ICS CERT 리포트 'Threat landscape for industrial automation systems H2 2019'

인터넷의 악성코드

OT 네트워크가 분리되어 있지 않음

웹에서 직접 연결 또는 회사 네트워크를 이용하여 연결 할 수 있음

이동식 저장 장치의 악성코드

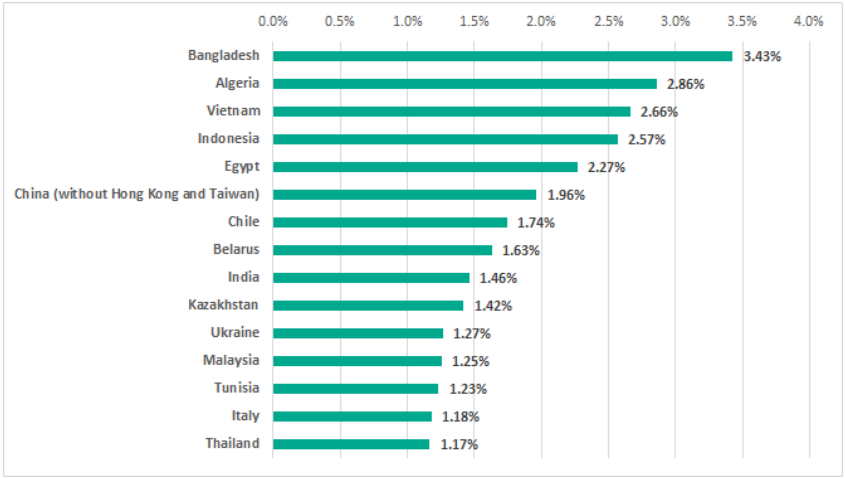
직원 및 외부 방문자가 가지고 있는 낮은 레벨의 사이버 보안 인식

이메일 클라이언트

피싱 캠페인에 사용

ICS 사이버 위협 동향 : 랜섬웨어

H2 2019에 랜섬웨어가 차단된 ICS 컴퓨터의 백분율 TOP 15



소스: Kaspersky ICS CERT 리포트 'Threat landscape for industrial automation systems H2 2019'

2019 H2 랜섬웨어 피해자

인도 쿠단쿨람 핵발전소
라인메탈 테크놀러지 그룹
에스파워 풍력 및 태양광 파워 설비
밥코, 바레인 국가 오일 회사
미쯔비시 전기

랜섬웨어 저항

2019년에 ICS 컴퓨터의 1.0%에서 랜섬웨어 감염 시도가 차단되었습니다.

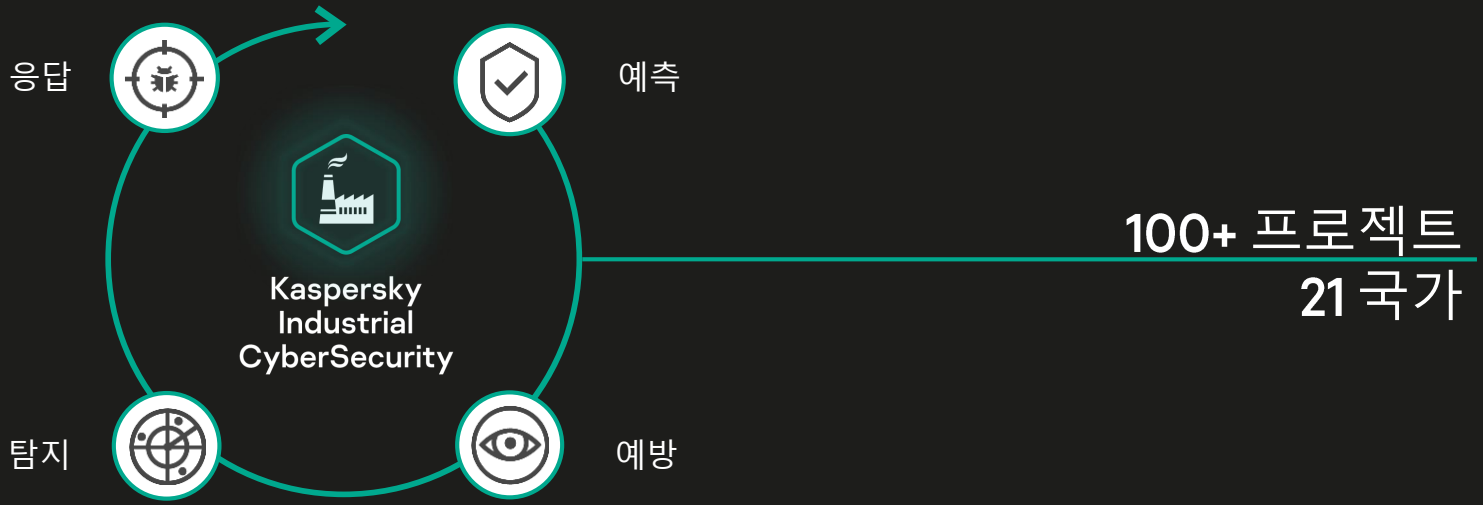
35%의 사용자가 WannaCry의 공격을 받았습니다. (2019년 랜섬웨어 공격을 받은 전체 사용자 중)

https://ics-cert.kaspersky.com/media/KASPERSKY_H22019_ICS_REPORT_FINAL_EN.pdf

포괄적인 제품 및 서비스 포트폴리오 제공

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity 제안



Kaspersky
Industrial
CyberSecurity

Gartner

카스퍼스키는 가트너의 Competitive Landscape For Operational Technology Security Report, 2020에 대표적인 벤더로 인정받았습니다.

KICS는 아래 4개의 범주를 제공하는 벤더로 인정받았습니다:

OT 엔드포인트 제안

OT 네트워크 모니터링 및 가시화
이상 징후 탐지, 사고 대응, 리포트

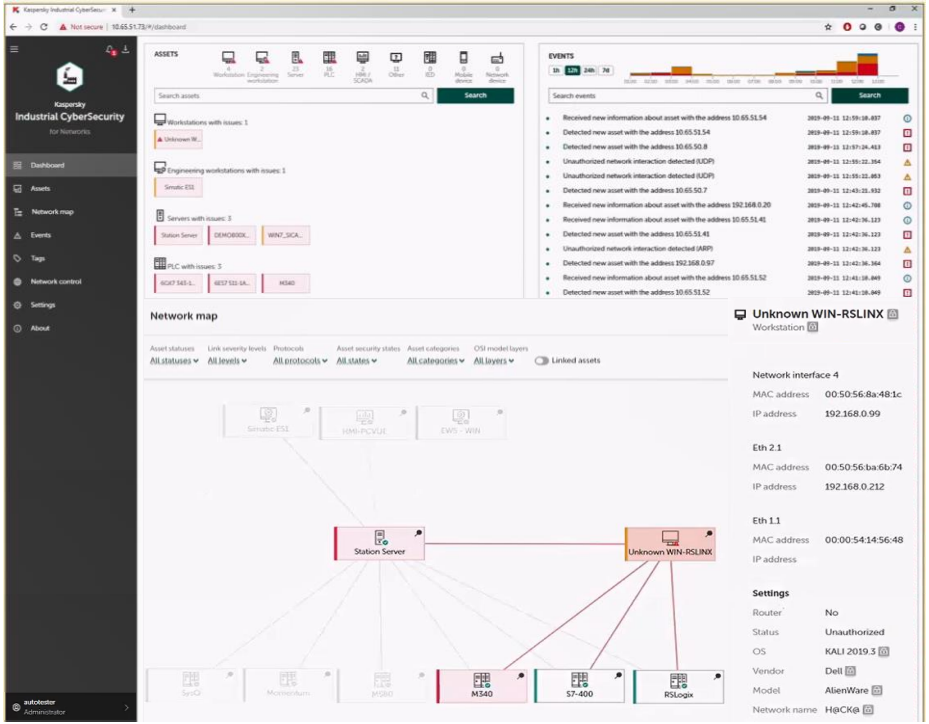
OT 보안 서비스

Competitive Landscape: Operational Technology Security, Ruggero Contu, 5 March 2020.

Kaspersky Industrial CyberSecurity 제안

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity 제품 포트폴리오



OT 침입 탐지

가장 낮은 수준의 APT를 탐지할 수 있습니다 (ICS 프로토콜 DPI (Deep Packed Inspection) 및 특정 시그니쳐)

자산 인벤토리

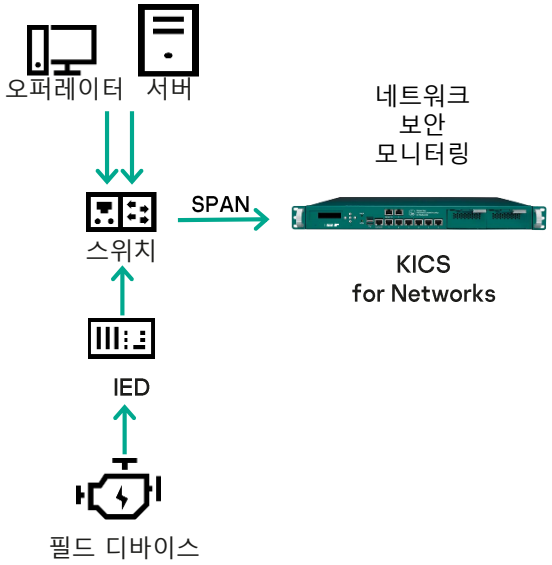
OT 구성 요소와 그 통신을 수동적으로 탐지합니다

OT 엔드포인트 보호

악성코드 방지, 화이트리스트 기반의 소프트웨어 및 디바이스, 기타 구성 요소 관리

KICS for Networks

KICS for Networks



소프트웨어 또는 가상 어플라이언스는 ICS 네트워크에 수동적으로 연결되며 다음과 같은 기술을 탑재했습니다:

자산 발견– 수동적인 OT 자산 식별 및 인벤토리 작성
딥 패킷 검사– 거의 실시간 기술 프로세스로 통신을 분석
네트워크 무결성 제어– 인증되지 않은 네트워크 호스트 및 흐름 감지
침입 탐지 시스템– 유해한 네트워크 동작의 징후를 경보
커맨드 제어– 산업 프로토콜의 커맨드를 검사
외부 시스템– 외부 탐지 기술과 API로 통합
이상 징후 탐지를 위한 머신 러닝 (MLAD) – 실시간 원격 및 과거 데이터 마이닝 (회귀 뉴럴 네트워크)를 통해 사이버 또는 물리적 위반을 검색

KICS for Networks:

Industrial Control Systems and Protocols support

Protocols

- ABB DMS
- ABB SPA-Bus
- Beckhoff
- CODESYS V3 Gateway
- Digsi4
- DNP3
- Ekra243 system protocol
- Emerson ControlWave Designer
- Emerson DeltaV
- EtherNet/IP
- FTP
- GE SRTP
- GOOSE
- IEC 60870-5-101
- IEC 60870-5-104
- Mitsubishi MELSEC System Q
- MMS
- Modbus TCP
- Moxa NPort Ia5000a system protocol
- Omron FINS
- OPC DA (DCE/RPC)
- OPC UA Binary
- ProsoftSystems DeviceDiscoveryProtocol
- Relematika BDUBus
- S7Comm over Industrial Ethernet
- S7Comm over TCP
- S7Comm Plus
- Sampled Values
- Schneider UMAS
- Yokogawa Vnet/IP

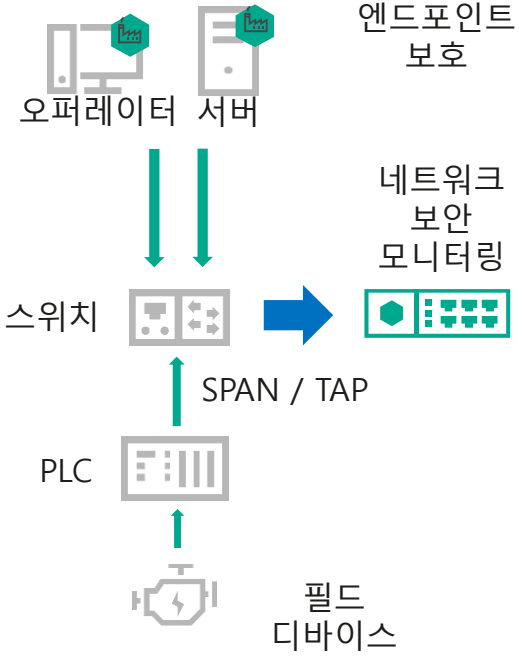
IT Protocols

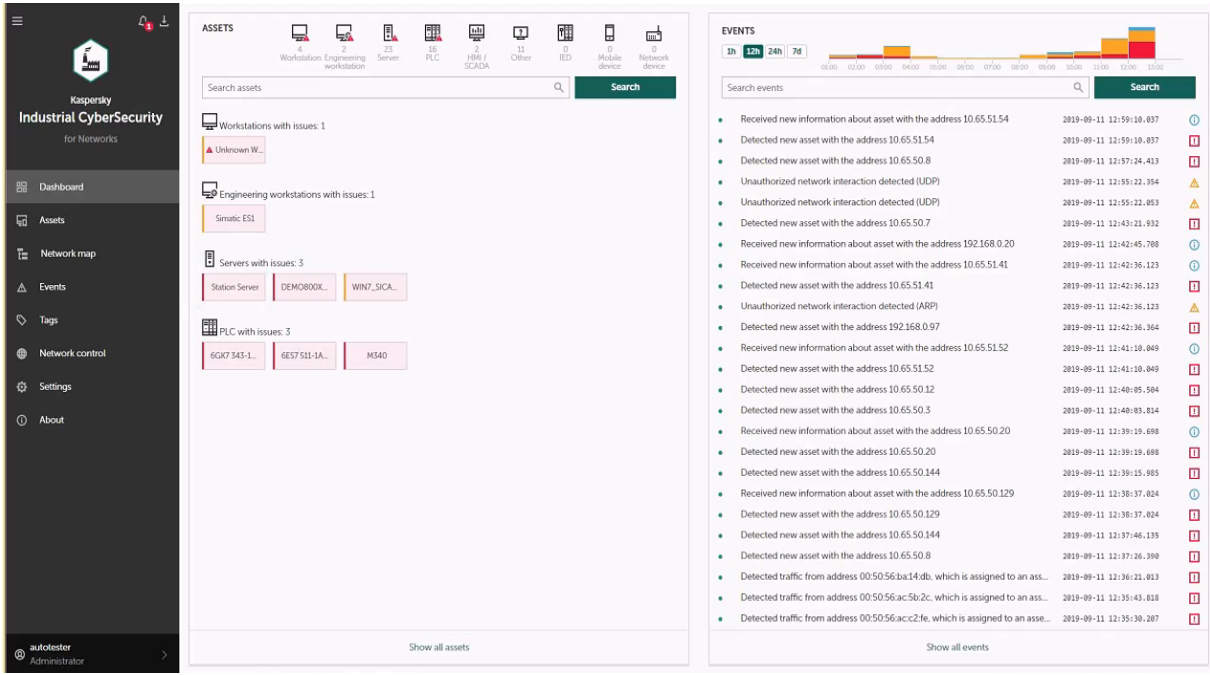
- Bittorrent
- BOOTP/DHCP
- DNS
- FTP
- HTTP
- ICMP
- IMAP
- IRC
- NetBIOS
- NTP
- POP3
- Radmin
- RDP
- Rlogin
- SMB
- SMTP
- SNMP TCP/UDP
- SSDP
- SSH
- Syslog
- Telnet
- TFTP
- Tor
- VNC

Vendors / Devices

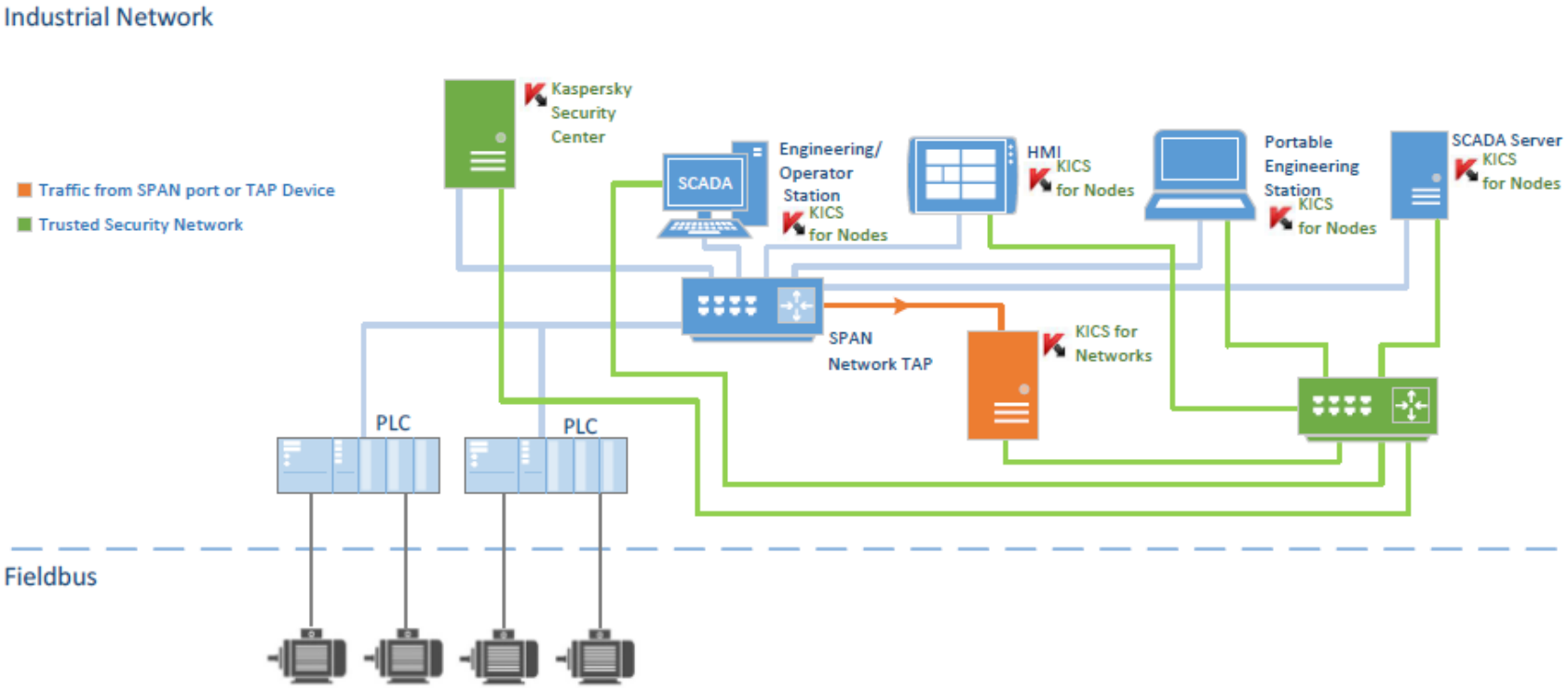
- ABB AC 700F
- ABB AC 800M
- ABB RED 670, REL 670, RET 670, REF 615
- ABB RTU 560
- Allen-Bradley CompactLogix Series
- Allen-Bradley ControlLogix Series
- Beckhoff Cx
- Devices with CODESYS V3
- Devices with DNP3
- Devices with IEC 60870-5-101
- Devices with IEC 60870-5-104
- Devices with IEC 61850-8-1: GOOSE, MMS
- Devices with IEC 61850-9-2: Sampled Values
- EKRA 200 Series
- EKRA BE2502
- EKRA BE2704
- Emerson ControlWave Micro 33
- Emerson DeltaV MD, MD Plus, MQ
- General Electric MULTILIN B30
- General Electric MULTILIN C60
- General Electric RX3i
- Mitsubishi System Q E71
- Moxa NPort Ia5000a
- Omron CJ2M
- ProsoftSystems Regul R500
- Relematika TOR 300
- Schneider Electric MiCOM P545
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580
- Schneider Electric Modicon Momentum
- Schneider Electric SEPAM S81 NPP
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- Siemens SIMATIC S7-200
- Siemens SIMATIC S7-300
- Siemens SIMATIC S7-400
- Siemens SIPROTEC 4 7SA52
- Siemens SIPROTEC 4 7SJ64
- Siemens SIPROTEC 4 7SS52
- Siemens SIPROTEC 4 7UM62
- Siemens SIPROTEC 4 7UT63
- Siemens SIPROTEC 5 7SJ86
- Siemens SIPROTEC 6MD66
- Yokogawa AFV10, AFV30, AFV40
- Yokogawa Centum VP
- Yokogawa PROSAFE-RS

KICS for Networks

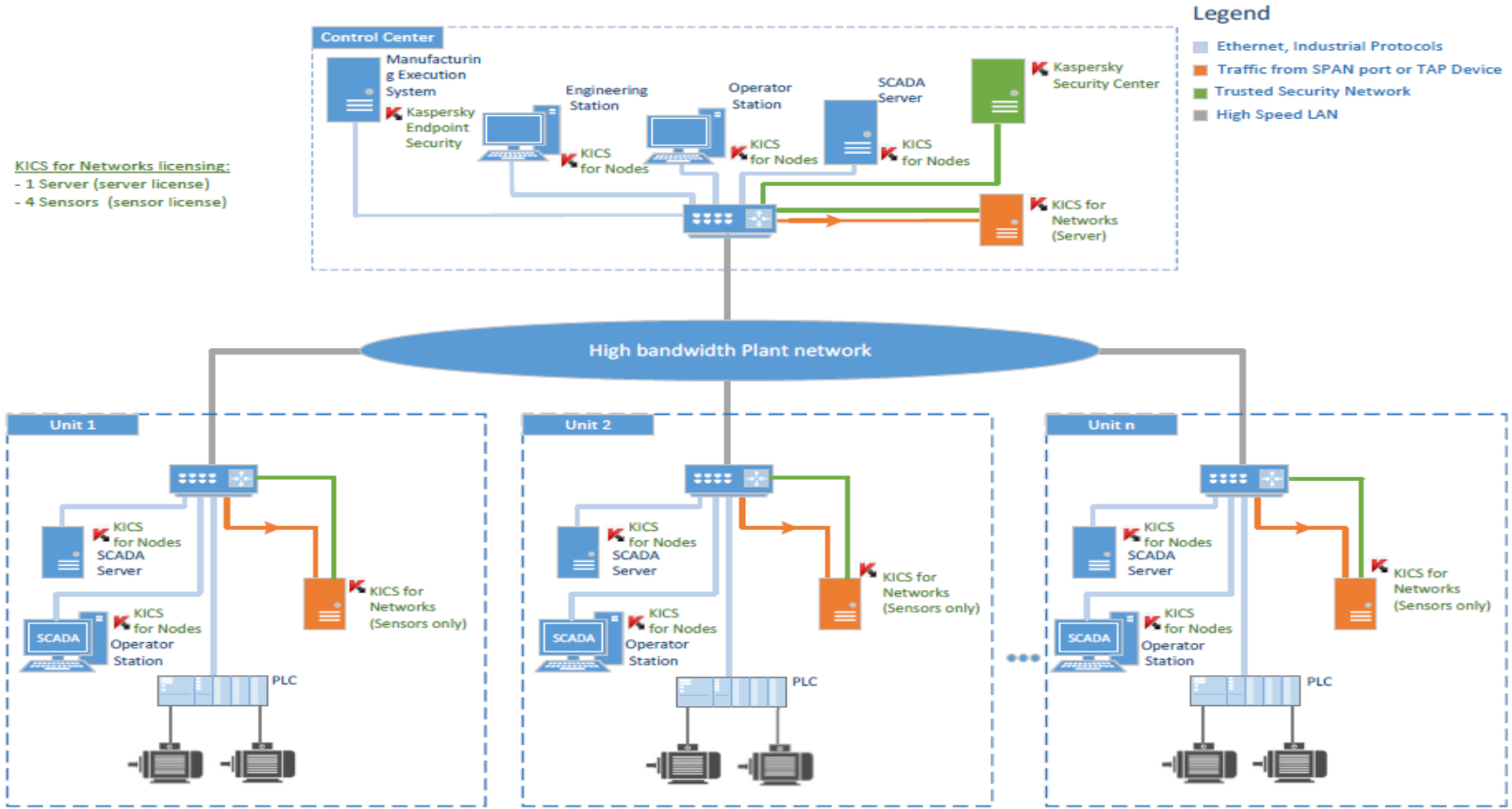




KICS for Networks – Deployment (Server)

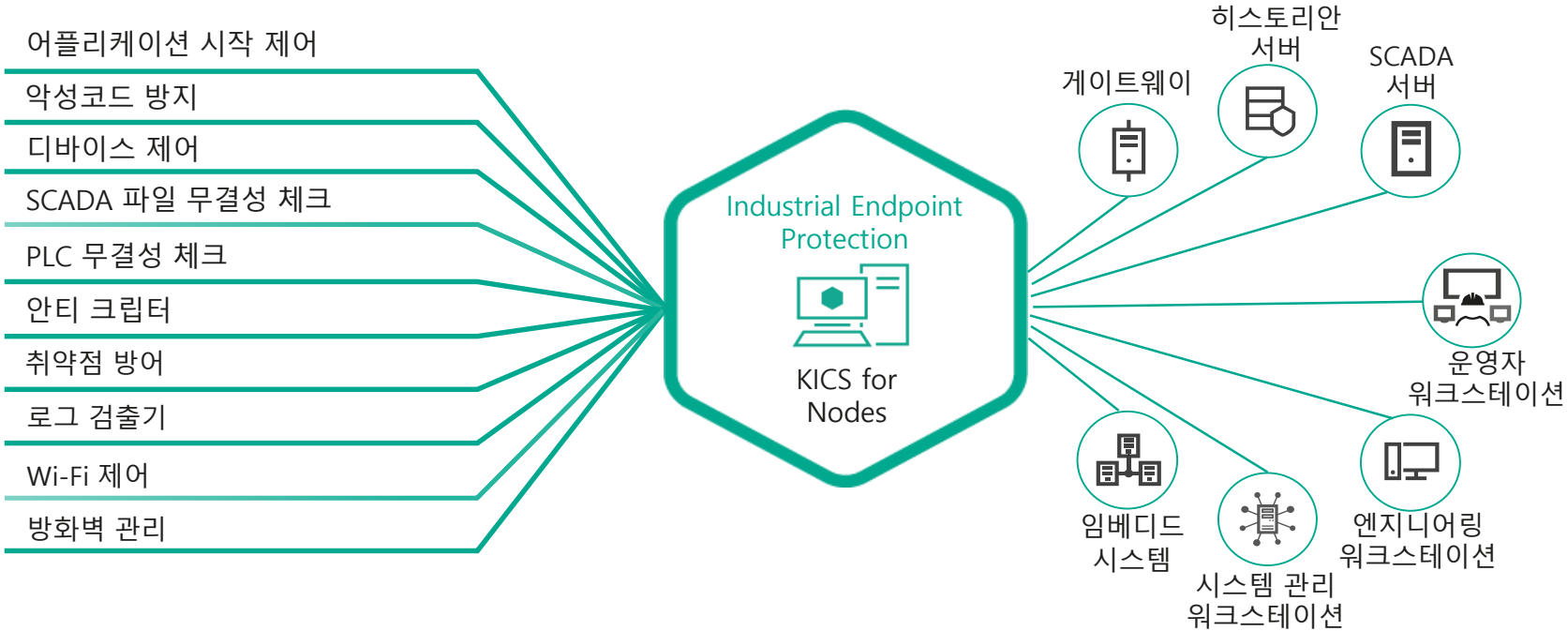


KICS for Networks – Deployment (Server + Sensors)



KICS for Nodes

KICS for Nodes



OT 및 ICS 전용으로 특별히 설계된 엔드포인트 보호 어플리케이션: 보호된 장치에 미치는 영향이 적고 호환성이 가장 높습니다.

SIEMENS Schneider Electric EMERSON YOKOGAWA PcVue Solutions ICONICS HollySys

KICS for Nodes – Supported Operating Systems

Workstation Edition:

- Windows XP Professional with SP2 and higher x86
- Windows Vista with SP2 x86/x64
- Windows 7 Professional x86/x64
- Windows 7 Enterprise / Ultimate x86/x64
- Windows 7 Professional with SP1 and higher x86/x64
- Windows 7 Enterprise / Ultimate with SP1 and higher x86/x64
- Windows 8 Pro x86/x64
- Windows 8 Enterprise x86/x64
- Windows 8.1 Pro x86/x64
- Windows 8.1 Enterprise x86/x64
- Windows 10 Pro x86/x64
- Windows 10 Enterprise x86/x64
- Windows 10 RS1/RS2/RS3/RS4/RS5/19H1

Server Edition:

- Windows Server 2003 Standard / Enterprise with SP2 and higher
- Windows Server 2008 Standard / Enterprise with SP1 and higher
- Windows Server 2008 R2 Standard / Enterprise
- Windows Server 2008 R2 Standard / Enterprise with SP1
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter x64
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter x64
- Windows Server 2016 / 2019

For embedded systems:

- Windows XP Embedded x86 (POS Ready)
- Windows Embedded Standard 7 x86/x64
- Windows Embedded 8.1 Industry Pro x86/x64
- Windows Embedded 8.0 Standard x86/x64
- Windows 10 IoT Enterprise x86/x64

KICS for Nodes – Supported Operating Systems

32-bit operating systems:

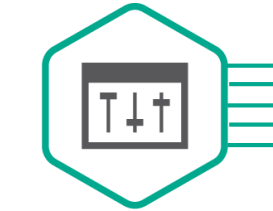
- Ubuntu 16.04 LTS and later
- Red Hat® Enterprise Linux® 6.7 and later
- CentOS 6.7 and later
- Debian GNU / Linux 9.4 and later
- Debian GNU / Linux 10
- Linux Mint 18.2 and later
- Linux Mint 19 and later
- Alt Linux SPT 8.0.0 Workstation
- Alt Linux SPT 8.0.0 Server
- Alt Linux 8.3 Workstation
- Alt Linux 8.3 Workstation K
- Alt Linux 8.3 Server
- Alt Linux 8.3 Education
- Alt Linux 9 Workstation
- Alt Linux 9 Education
- GosLinux 6.6
- Mageia 4

64-bit operating systems:

- Ubuntu 16.04 LTS and later
- Ubuntu 18.04 LTS and later
- Red Hat Enterprise Linux 6.7 and later
- Red Hat Enterprise Linux 7.2 and later
- Red Hat Enterprise Linux 8.0 and later
- CentOS 6.7 and later
- CentOS 7.2 and later
- CentOS 8.0 and later
- Debian GNU / Linux 9.4 and later
- Debian GNU / Linux 10.1 and later
- OracleLinux 7.3 and later
- OracleLinux 8 and later
- SUSE® Linux Enterprise Server 15 and later
- openSUSE® Leap 15 and later
- Alt Linux SPT 8.0.0 Workstation
- Alt Linux SPT 8.0.0 Server
- Alt Linux 8.3 Workstation
- Alt Linux 8.3 Workstation K
- Alt Linux 8.3 Server / Education
- Alt Linux 9 Workstation / Server
- Alt Linux 9 Education
- Amazon Linux AMI
- Linux Mint 18.2 and later
- Linux Mint 19 and later
- Astra Linux Special Edition 1.5
- Astra Linux Special Edition 1.6
- Astra Linux Common Edition Orel 2.12
- OS ROSA Cobalt 7.3 for client systems
- OS ROSA Cobalt 7.3 for server systems
- GosLinux 6.6
- GosLinux 7.2
- AlterOS 7.5 and later
- Pardus OS 19.1

Kaspersky Security Center

KSC (Kaspersky Security Center)



Kaspersky Security Center

시스템 관리

- 중앙화된 시스템 데이터 수집
- 중앙화된 소프트웨어 배포
- 취약점 탐지 및 패치 관리
- 확장된 클라이언트 관리 기능

SIEM 통합

- ArcSight, Splunk, QRadar
- Syslog 서버

정책 관리

- 중앙화된 정책 관리
- 리모트 작업 스케쥴링 및 실행

HMI 통합

MES 대시보드 통합

- 보안 상태 및 정보를 IEC 104 / OPC2.0 호환 호스트에 전달합니다.

리포트 및 알림

- 이벤트 로깅
- 대시보드 및 리포트
- SMS/이메일 알림

FORRESTER®

연구 읽기:
https://www.kaspersky.com/Forrester-TEI-for-KICS

Forrester의 연구는* Kaspersky Industrial CyberSecurity를 사용하는 회사가 ROI 368%를 기록하는 것을 보여줍니다.

도전 과제

높은 비용의 사이버 공격과 리스크가 증가
ICS를 전문적으로 보호할 필요성
사이버 보안에 해한 정부 요구 사항을 준수해야 할 필요성

주요 결과

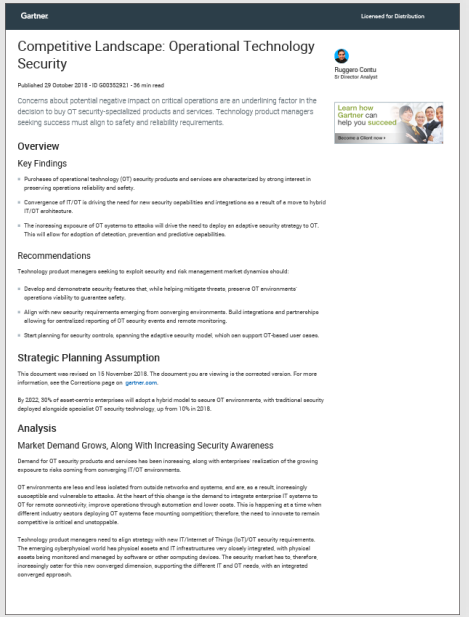
고객은 산업 시스템에 대한 더 나은 보호를 달성
경량화되어 있는 보안 솔루션은 생산 공정에 영향을 미치지 않음
간단한 설치 및 배포로 빠른 가치 실현

*The Total Economic Impact™ Of Kaspersky Industrial CyberSecurity is a commissioned study conducted by Forrester Consulting on behalf of Kaspersky Lab, April 2019.

Kaspersky Industrial CyberSecurity는 5개의 보안 역량중 4개의 영역에서 인정 받고 있습니다.

Gartner는 카스퍼스키를 다음과 같은 보안 기능을 제공하는 대표적인 벤더로 인정하고 있습니다 :

- ✓ OT 엔드포인트 보안
- ✓ OT 네트워크 모니터링 및 가시성
- ✓ 이상징후 탐지, 사고 분석, 리포트
- ✓ OT 보안 서비스



Gartner

Licensed for Distribution

Competitive Landscape: Operational Technology Security

Ruggero Contu
Sr Director Analyst

Published 29 October 2018 - ID G00352921 - 36 min read

Concerns about potential negative impact on critical operations are an underlining factor in the decision to buy OT security-specialized products and services. Technology product managers seeking success must align to safety and reliability requirements.

Learn how Gartner can help you succeed

Become a Client now >

Overview

Key Findings

- Purchases of operational technology (OT) security products and services are characterized by strong interest in preserving operations reliability and safety.
- Convergence of IT/OT is driving the need for new security capabilities and integrations as a result of a move to hybrid IT/OT architecture.
- The increasing exposure of OT systems to attacks will drive the need to deploy an adaptive security strategy to OT. This will allow for adoption of detection, prevention and predictive capabilities.

Recommendations

Technology product managers seeking to exploit security and risk management market dynamics should:

- Develop and demonstrate security features that, while helping mitigate threats, preserve OT environments' operations viability to guarantee safety.
- Align with new security requirements emerging from converging environments. Build integrations and partnerships allowing for centralized reporting of OT security events and remote monitoring.
- Start planning for security controls, spanning the adaptive security model, which can support OT-based user cases.

Strategic Planning Assumption

This document was revised on 15 November 2018. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

By 2022, 30% of asset-centric enterprises will adopt a hybrid model to secure OT environments, with traditional security deployed alongside specialist OT security technology, up from 10% in 2018.

Analysis

Market Demand Grows, Along With Increasing Security Awareness

Demand for OT security products and services has been increasing, along with enterprises' realization of the growing exposure to risks coming from converging IT/OT environments.

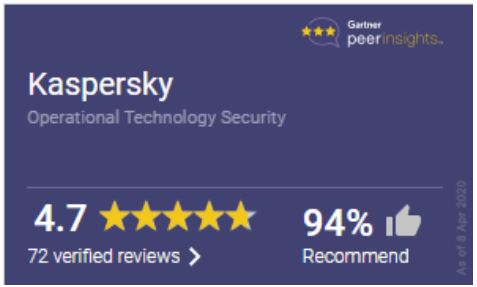
OT environments are less and less isolated from outside networks and systems, and are, as a result, increasingly susceptible and vulnerable to attacks. At the heart of this change is the demand to integrate enterprise IT systems to OT for remote connectivity, improve operations through automation and lower costs. This is happening at a time when different industry sectors deploying OT systems face mounting competition; therefore, the need to innovate to remain competitive is critical and unstoppable.

Technology product managers need to align strategy with new IT/Internet of Things (IoT)/OT security requirements. The emerging cyberphysical world has physical assets and IT infrastructures very closely integrated, with physical assets being monitored and managed by software or other computing devices. The security market has to, therefore, increasingly cater for this new converged dimension, supporting the different IT and OT needs, with an integrated converged approach.

Gartner®

Competitive Landscape: Operational Technology Security, Ruggero Contu, 29 October 2018.

Gartner Peer Insights: 카스퍼스키는 **OT** 보안 시장의 모든 벤더 중에서 전체적으로 가장 높은 점수를 받고 있습니다. *



*Kaspersky has an overall rating of 4.7 out of 5 in the Operational Technology Security market on Gartner Peer Insights, based on 80 ratings as of 6 May 2020 (among vendors with min 20 reviews)

"완전하고 안정적이며 견고한 솔루션입니다. 구현이 간편하며 SCADA와 호환됩니다."

★★★★★

(Customer review by firm size: <50M USD; Industry: Services; Role: CIO; Submitted: Dec 27, 2019)
Link to the review

"카스퍼스키의 전폭적인 지원 덕분에 **KICS**를 표준이 아닌 우리의 **SCADA**에 성공적으로 배포할 수 있었습니다."

★★★★★

(Customer review by firm size: 500M – 1B USD; Industry: Energy and Utilities; Role: Infrastructure and Operations; Submitted: Aug 23, 2019)
Link to the review

Read the customer reviews here: https://www.gartner.com/reviews/market/operational-technology-security/vendor/kaspersky

Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences, and do not represent the views of Gartner or its affiliates.

KICS 서비스

Kaspersky Industrial CyberSecurity 통합적 접근

Trainings and Awareness
OT의 사고 대응 및 분석을 위한 전문적인 교육
OT 스페셜리스트를 위한 기본 트레이닝

Assessment and other security services
침투 테스트
사이버 보안 평가
사이버 보안 성숙도 모델
APT 리포트
SOC 및 CERT 자문

Threat Intelligence
취약점 연구 및 악성 코드 데이터 베이스

Incident Response
사고 분석 및 포렌식 서비스
(리모트 및 온사이트)
대응 메뉴얼 준비 및 시뮬레이션

Kaspersky Industrial CyberSecurity **Trainings and Awareness**

ICS in Practice awareness training

온사이트 또는 온라인 기반의 인터랙티브한 교육 모듈 및 사이버 안전 게임
산업용 컴퓨터 시스템을 사용하는 직원 및 그들의 관리자용 교육
1-2 일, 10-20 수강생

ICS Penetration Testing for Professional

5 일, 최대 10명의 전문가

ICS Digital Forensics for Professional

4 일, 최대 10명의 전문가

Kaspersky Industrial CyberSecurity **Assessment and other security services**

외부 침투 테스트

black- or grey box
인터넷으로부터 회사 네트워크에 접근

내부 침투 테스트

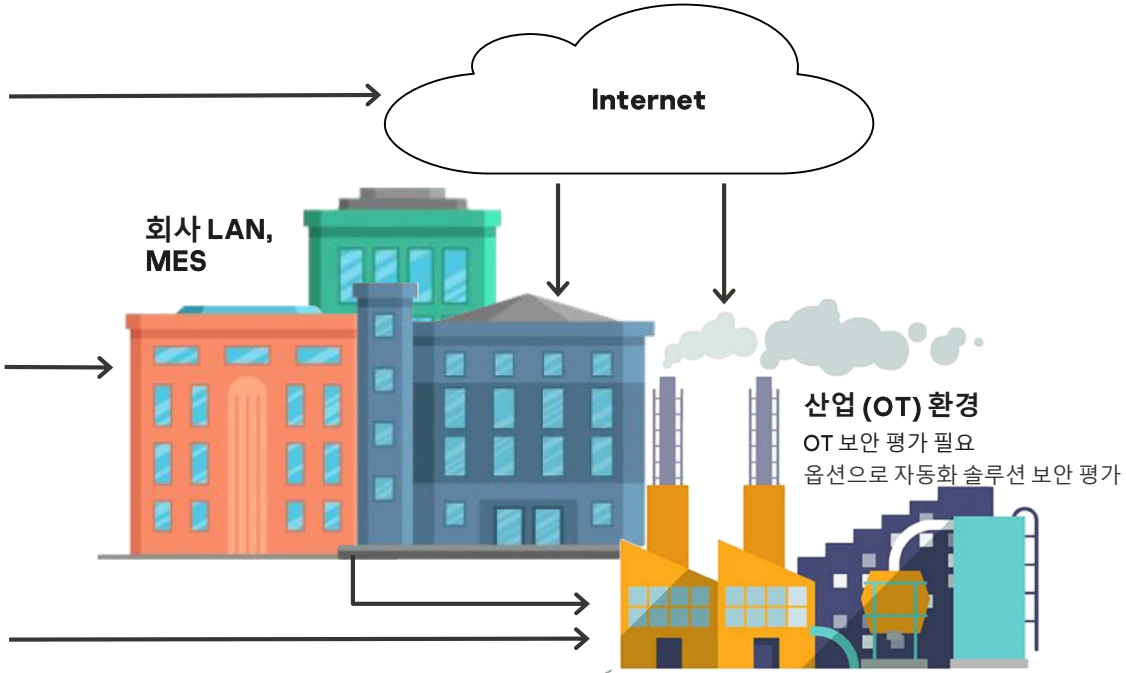
black- or grey box
회사로부터 산업 (OT) 네트워크에 도달

OT 보안 평가

white-box, interviews, audit
산업 (OT) 네트워크를 위한 인벤토리, 취약점, 추천

자동화 솔루션 보안 평가

white-box, 0-day vulnerabilities, configuration standards
보안 갭을 파악하고 사전 예방적 CTI를 구축하며 취약점을 보완합니다.



Kaspersky Industrial **Threat Intelligence**

ICS Vulnerabilities Database

Kaspersky®
Threat Intelligence

Available EoY 2020

대부분의 치명적인 취약점

대부분의 인기 있는 OT
디바이스 및 소프트웨어

전문가의 중요도 평가

조치 가능한 완화 권고 사항

네트워크 공격 시그니처 및
침해지표 **(IoCs)**

사람 및 기계가 읽을 수 있는 포맷

Kaspersky Industrial **Threat Intelligence (TI)**

TI Data feed

- ✓ Kaspersky Security Network (KSN)을 통해 ICS 컴퓨터에서 독점적으로 얻은 데이터를 기반으로 구축된 ICS 위협에 대한 고유 독점 데이터 베이스
- ✓ 1달에 100 000건의 기록, 매 24시간마다 업데이트
- ✓ HP ArcSight, IBM QRadar, Splunk, RSA, 기타 등의 타사 SIEM systems과 연결 가능

강점:

- ✓ **사고 대응 및 디지털 포렌식 절차 중 OT 네트워크 내의 악성 프로그램 감염 식별**
- ✓ **OT 네트워크 내부에서 발견된 위협 및 악성 프로그램에 대한 풍부한 데이터**

TI Report

- ✓ Kaspersky ICS CERT 연구에 기반하여 특정 고객이 필요로 하는 지역, 산업 및 보안 문제 매개변수와 매칭되는 전용 리포트
- ✓ 기술 스페셜리스트, 보안 연구원 및 개발자를 위한 선제적 행동 가능한 정보 포함

강점:

- ✓ **사내에서 많은 인력 리소스 소모 없이 위협 정보 수집, 처리 및 분석 가능**
- ✓ **ICS 사이버 보안 영역에서 의사 결정을 위한 정보 보유**

Kaspersky Incident Response

- 사건 조사
- 교정 계획 제공
- 향후 회피할 수 있는 권장 방법 제시

Incident Response Handbook

- 현재 고객 팀 및 도구들 평가
- 기존 사고 대응 절차를 분석 및 개선
- 고객 팀에게 시뮬레이션, 테스트, 교육 제공

Kaspersky **Incident Response** 절차

✓ **킥오프 콜**

콜 상담중에 프로젝트 코디네이터는 고객 담당자와 사건에 대한 세부사항을 논의하고 프로젝트 일정 (필요한 경우 출장)을 제안하며 추가 정보를 요청합니다

✓ **증거 모으기**

카스퍼스키가 온사이트 증거 수집

사고 대응을 제공하는 카스퍼스키 전문가들은 전 세계에 분포하고 있습니다. 그들은 고객의 사이트를 방문하여 사건과 관련된 모든 유형의 증거를 수집합니다

디지털 포렌식: 고객이 증거를 수집

이 경우 고객은 모든 증거를 수집하여 카스퍼스키와 공유합니다

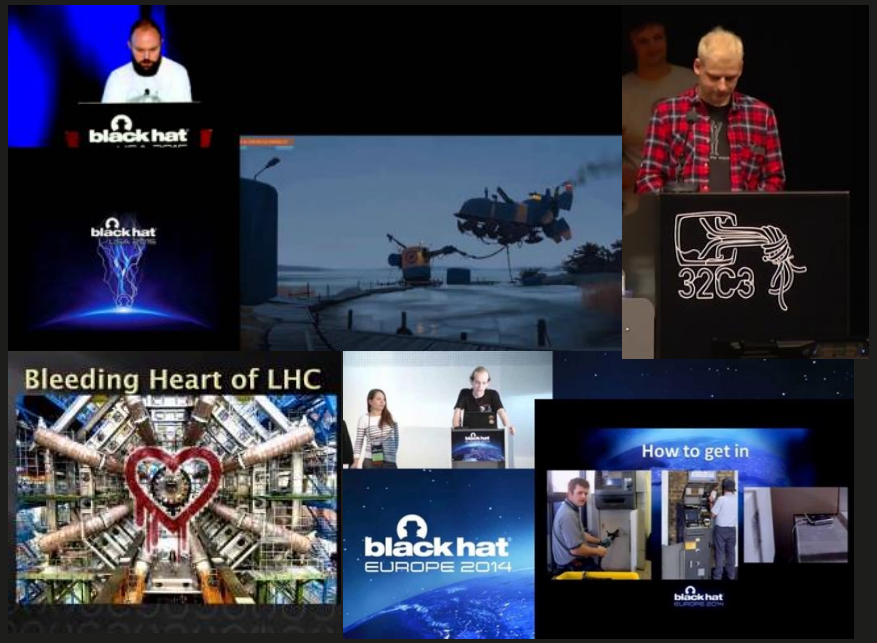
✓ **증거 분석**

✓ **완화 계획**

✓ **툴 기반의 네트워크 리소스 검색**

✓ **보고서 및 사고 대응 매뉴얼 작성**

Kaspersky 보안 서비스 팀



ORACLE SIEMENS Google

Microsoft CISCO SAP

전문가

취약점 연구원, 리버스 엔지니어링 및 어플리케이션 보안 전문가 보유

취약점 찾기

- 최신 엔터프라이즈 제품
- OT/ICS: SCADA/DCS/PLC/IED 및 기타
- 스마트/IoT 디바이스 및 플랫폼

유선 및 무선 통신 실험실

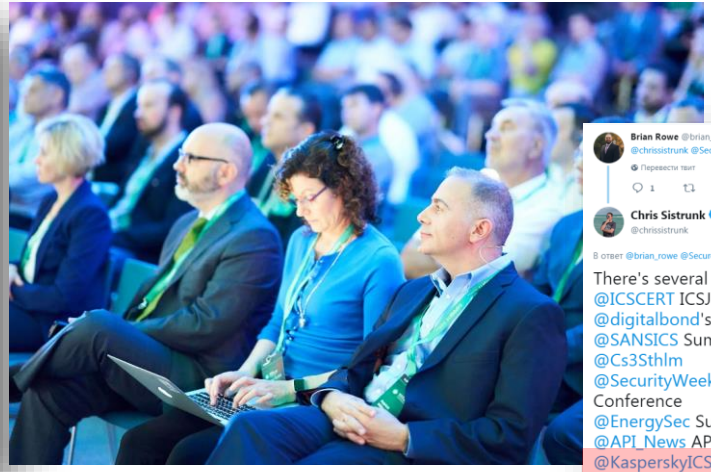
일반: 셀룰러, GNSS, Wi-Fi, Bluetooth, NFC 등.

독점적 표준의 리버스 엔지니어링 경험 보유

하드웨어 해킹 실험실

고급 신호 분석 및 맞춤형 공격 툴킷 개발 경험 보유

Kaspersky Industrial Cybersecurity Conference



https://ics.kaspersky.com/conference/

KICS 레퍼런스

AGC

“우리는 운영이 계속 진행되는 동안 구현할 수 있는 KICS를 제공하는 카스퍼스키와 협력하기로 결정했습니다. KICS 솔루션은 우리가 사용하는 제어 시스템 및 Tomorrow Connect와 호환이 가능한 시스템이기 때문입니다.”

Jan Houben, AGC Glass Germany GmbH의 공장 관리자

주요 자동차 생산자를 위한 유리 제조 업체

벤츠, BMW, 폭스바겐, 및 볼보등의 공급업체

기술적인 절차를 방해할 수 있는 모든 사이버 침해를 완화합니다.

보호

산업 네트워크를 최대한 제어할 수 있도록 허가되지 않은 장치 감지

화이트리스트 기반의 보호

운영 절차의 중단 없이 구현 가능

MosGaz

“우리는 이 공동 프로젝트가 긴밀하고 지속적인 협력을 위한 토대를 마련해 줄 것이라고 확신합니다. 우리는 MosGaz의 산업 제어 시스템을 보호하는 사이버 보안 시스템을 계속 현대화할 것입니다.”

– Alexandr Kuzin, MOSGAZ의 IT 부서 관리자

모스크바의 천연가스 유통업체

1865년 창업

연간 230억 입방미터의 천연가스 수송

7500 km에 달하는 가스 배포 네트워크

보호받는 산업 노드 및 네트워크

500개 이상의 천연 가스 배포 스테이션을 KICS for Network로 보호

- 총 600개의 지멘스 PLC
- 각 PLC 당 최대 20개의 밸브

KICS for Nodes로 7개의 클러스터로 중앙화된 SCADA 서버 보호

Alperia

“카스퍼스키 엔지니어와의 태스크 포스를 사내에서 이용할 수 있는 아이디어로 인해 우리의 상황에 맞게 맞춤 제작을 할 수 있었습니다. “ Sandro Moretti 원격 통신 부문 관리자

“이와 같은 케이스의 경우 우리는 전통적인 고객- 공급자 관계를 넘어 더 넓은 범위의 파트너십을 목표로 삼아야 한다고 확신합니다.“ Moretti 는 맺음말을 남겼습니다.

파워 생성기 및 분배기

280,000 사용자, 34 수력발전소, 6 지역 난방 발전소, over 8,600 킬로미터 이상의 전력 그리드 및 700개의 전기 충전 지점들이 이탈리아에 있습니다.

€1.3 M 매출

KICS for Nodes

" 현재 우리는 카스퍼스키 솔루션으로 약 40개가 넘는 서버를 보호하고 있습니다. " Morettiㄴ는 말했습니다. "전속력으로 달려온 6개월 남짓한 기간동안 우리는 점진적이고 완전한 안전을 만들어냈습니다. “

TANECO

"이 프로젝트는 이와 같은 솔루션이 산업 시설과 함께 성공적으로 사용될 수 있음을 보여줍니다. TANECO는 Kaspersky와의 산업 네트워크에 대한 보안 제공 협력을 더욱 확대할 계획입니다." Marat Gilmutdinov, 산업 제어 시스템 부문장, TANECO

오일 생산자

2005년에 설립된 Tatneft 그룹은 $150억 달러 규모

산업 제어 시스템(ICS)를 사용하여 경쟁사보다 기술 우위를 제공하고 생산 비용을 최소화

산업 인프라에서 기업 네트워크를 위해 원래 설계된 기술의 생산 자동화 및 사용 수준이 높아짐에 따라 회사는 사이버 공격의 위협에 노출

제조 프로세스의 연속성을 보호

이상 징후 및 무단 컨트롤러 재구성 시도 탐지

기술 프로세스를 모니터링하고 MLAD 기술로 정상 동과과의 공정 편차를 자동으로 감지

자동 조기 경고, 이상 징후 감지 및 편차 분석 도구 사용

TANECO

Wintershine

"자체 데이터를 시작으로 추후 외부 데이터 처리 가능성도 있는 다량의 데이터를 다루는 양식업에서는 기술 기반 접근 방식이 옳다고 생각하기 때문에 신회하고 의지할 수 있는 사이버 보안 솔루션이 반드시 필요합니다."
Dlrk Elchellberger, 박사, Wintershine

지속가능한 양식업으로 안전한 식품과 건강을 제공

싱가폴 최초의 부유식 스마트 양식장

통합 인공 지능 및 영상 분석 시스템을 통해 양식 어류의 건강 상태와 증가율 모니터링

최대 18톤의 어류를 수용할 수 있는 탱크 10대 보유

물 재활용 및 30% 이상의 에너지를 태양광으로 운영

KICS for Nodes

SCADA 서버, HMI, 엔지니어링 워크스테이션 보호

화이트리스트 기반의 보호

Siemens의 최신 OT 기술과 카스퍼스키의 사이버 안전 솔루션을 결합한 싱가포르의 업계 4.0 Siemens 솔루션 중 첫 번째 솔루션입니다.

Wintershine Teaming up With Nature

싱가폴 대학교의 SWaT 머신 러닝 테스트베드

SWaT 프로세스

P1: RAW 물 공급 및 저장장치
P2: 전처리
P3: 여과 (UF) 및 역세척
P4: 탈염소시스템
P5: 역삼투 (RO)
P6: RO 투과 전송, UF 역세척 및 청소

SWaT dataset

25 센서
26 액츄에이터

7 일간 정상 동작 컨디션
6 일간 34개의 공격

싱가폴 대학교의 SWaT 머신 러닝 테스트베드

Detected Attack

Kaspersky Machine Learning for Anomaly Detection

최첨단 머신 러닝 기술

데이터 기반 이상 징후 탐지

독립적인 이유 탐지

이상 징후 해석

예지보전

수동으로 규칙 생성 필요없음

추가적인 장비 필요없음(센서, 비파괴 제어 장비 등.)

https://ics.kaspersky.com/media/ics-conference-2018/Andrey-Lavrentyev-Protecting-ICS-Operational-Technologies-with-Machine-Learning-En.pdf

SWaT의 MLAD 결과

Attack #	Start Time	End Time	Attack Point	MLAD Detect	MLAD Interpret	MLAD Time	MLAD Interprettion
1	28/12/2015 10:29:14	10:44:53	MV-101	-			
2	28/12/2015 10:51:08	10:58:30	P-102	-			
3	28/12/2015 11:22:00	11:28:22	LIT-101	-			
4	28/12/2015 11:47:39	11:54:08	MV-504	-			
5	28/12/2015 11:58:20		No Physical Impact Attack				
6	28/12/2015 12:00:55	12:04:10	AIT-202	+	+	December 28, 2015 12:00:33	**AIT202**, PIT502, AIT502
7	28/12/2015 12:08:25	12:15:33	LIT-301	+	+	December 28, 2015 12:15:26	**LIT301**, P101, AIT202
8	28/12/2015 13:10:10	13:26:13	DPIT-301	+	+	December 28, 2015 13:09:52	**DPIT301**, FIT301,PIT502
9	28/12/2015 14:15:00		No Physical Impact Attack				
10	28/12/2015 14:16:20	14:19:00	FIT-401	+	+	December 28, 2015 14:16:04	**FIT401**, FIT502, LIT401
11	28/12/2015 14:19:00	14:28:20	FIT-401				
12	29/12/2015 11:10:40		No Physical Impact Attack				
13	29/12/2015 11:11:25	11:15:17	MV-304	+	+	December 29, 2015 11:10:59	**MV304**, PIT502, MV302
14	29/12/2015 11:35:40	11:42:50	Mv-303	-			
15	29/12/2015 11:52:01		No Physical Impact Attack				
16	29/12/2015 11:57:25	12:02:00	LIT-301	-			
				FP		December 29, 2015 14:33:53	MV101, FIT101, MV303
				FP		December 29, 2015 14:42:44	P602, MV301, MV303
17	29/12/2015 14:38:12	14:50:08	MV-303	-			
18	29/12/2015 18:08:55		No Physical Impact Attack				
19	29/12/2015 18:10:43	18:15:01	AIT-504	-			
20	29/12/2015 18:15:43	18:22:17	AIT-504	+	+	December 29, 2015 18:15:23	**AIT504**, FIT502, AIT402
21	29/12/2015 18:30:00	18:42:00	MV-101, LIT-101	+	+		
22	29/12/2015 22:55:18	23:03:00	UV-401, AIT-502, P-501	+	+	December 29, 2015 22:54:55	**UV401**, PIT502, AIT202, **AIT501**, P205
23	30/12/2015 01:42:34	01:54:10	P-602, DIT-301, MV-302	+	+	December 30, 2015 01:42:11	**MV302**, DPIT301,PIT502, AIT501
24	30/12/2015 09:51:08	09:56:28	P-203, P-205	+	+	December 30, 2015 09:51:34	**P203, P205**, P101
25	30/12/2015 10:01:50	10:12:01	LIT-401, P-401	+	+	December 30, 2015 10:11:46	**LIT401, MV101**, P302
26	30/12/2015 17:04:56	17:29:00	P-101, LIT-301	-			
27	31/12/2015 01:17:08	01:45:18	P-302, LIT-401	+	+	December 31, 2015 01:17:34	**LIT401, MV101**, AIT501
28	31/12/2015 01:45:19	11:15:27	P-302	-			
				FP		December 31, 2015 11:48:06	MV302,MV304, AIT501
				FP		December 31, 2015 11:48:20	AIT501, P302, AIT402
29	31/12/2015 15:32:00	15:34:00	P-201, P-203, P-205	-			
30	31/12/2015 15:47:40	16:07:10	LIT-101, P-101, MV-201	+	+	December 31, 2015 16:06:31	MV201, **LIT101**, MV304
				FP		December 31, 2015 22:05:43	MV304, LIT401, P302
31	31/12/2015 22:05:34	22:11:40	LIT-401	+	+	December 31, 2015 22:12:09	**LIT401**, LIT301,MV301
32	1/01/2016 10:36:00	10:46:00	LIT-301				
33	1/01/2016 14:21:12	14:28:35	LIT-101				
				FP		January 1, 2016 10:37:07	LIT301, MV201, AIT501
				FP		January 1, 2016 10:46:38	LIT301, MV201, LIT401
				FP		January 1, 2016 14:22:21	MV301, LIT101, P602
				FP		January 1, 2016 14:29:25	LIT101, AIT501, AIT402
34	1/01/2016 17:12:40	17:14:20	P-101	+	+	January 1, 2016 17:13:33	MV201, P203, FIT201, P205, **P101**
35	1/01/2016 17:18:56	17:26:56	P-101; P-102	+	+	January 1, 2016 17:19:59	MV201, **P101**,FIT101
36	1/01/2016 22:16:01	22:25:00	LIT-101	+	+	January 1, 2016 22:17:27	**LIT101**,AIT202,AIT402
37	2/01/2015 11:17:02	11:24:50	P-501, FIT-502	+	+	January 2, 2016 11:17:48	FIT504, PIT502, **FIT502**,
				FP		January 2, 2016 11:28:48	P602, MV303, MV304
38	2/01/2015 11:31:38	11:36:18	AIT-402, AIT-502	+	+	January 2, 2016 11:32:16	**AIT502, AIT402**, PIT502
39	2/01/2015 11:43:48	11:50:28	FIT-401, AIT-502	+	+	January 2, 2016 11:44:26	**FIT401**,AIT503,MV101
40	2/01/2015 11:51:42	11:56:38	FIT-401	+	-	January 2, 2016 11:52:19	P602, AIT503, P301
41	2/01/2015 13:13:02	13:40:56	LIT-301	+	+	January 2, 2016 13:41:15	**LIT301**, LIT401, AIT402

- 26 단일 스테이지 단일 포인트 공격
- 2 멀티 스테이지 단일 포인트 공격
- 4 단일 스테이지 멀티 포인트 공격
- 4 단일 스테이지 단일 포인트 공격

탐지된 공격
34번중 23번

탐지 안됨
9개의 작은 충격

올바른 해석
23번중 22번

오탐
연속된 공격으로 3번

새로운 이상징후
7개의 이상 징후

https://ics.kaspersky.com/media/ics-conference-2018/Andrey-Lavrentyev-Protecting-ICS-Operational-Technologies-with-Machine-Learning-En.pdf

Why Kaspersky

왜 카스퍼스키인가?

MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION

*kaspersky.com/top3

86
테스트 및 평가 참여

64
1위 횟수

81%
Top 3

사이버 보안이 개인과 기업 모두에 중요해짐에 따라, 공급 업체에 대한 신뢰는 필수적입니다. 카스퍼스키는 전 세계적으로 가정용 사용자와 기업 고객들에게 서비스를 제공하고 있으며 시장 신뢰를 무엇보다 중요하게 생각하고 있습니다.

2019년 카스퍼스키 제품은 86개 독립 테스트와 리뷰에 참여했으며 이중 1위 64회, TOP 3 선정 70회를 기록하였습니다.

*86 independent tests were completed by Kaspersky products in 2019 alongside 12 competitors. More than 100 vendors took part in the tests, but only those who participated in 35% or more of the tests had their results represented in the chart.

다양한 업종의 실제 고객으로부터 받은 2000건의 리뷰를 통해 2019년 Gartner Peer insight에서 고객이 선택한 엔드포인트 보안 플랫폼입니다.

* As of November 21, 2019
The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

카스퍼스키의 **글로벌 연구 및 분석 팀 (GReAT Team)**은
최첨단 사이버 위협을 지속적으로 탐색하고 대응합니다.

Kaspersky Industrial cybersecurity

KasperskyOS (Secure Operating System)
- Secure-by-design approach
- Proprietary lightweight microkernel and independent security engine.
- Cyber-Immunity

Authorized to Use CERT™
CERT is a mark owned by Carnegie Mellon University

Kaspersky ICS-CERT

Industrial Systems Emergency Response Team offering expert intelligence and consulting

Kaspersky Industrial CyberSecurity

PRODUCTS

Supported Industrial Endpoints:
- ✓ SCADA Servers
- ✓ SCADA Clients
- ✓ Human Machine Interfaces (HMI)
- ✓ Engineering Workstations
- ✓ Historians
- ✓ OPC Gateways

Industrial Endpoint Protection

KICS for Nodes

Endpoint protection capabilities:
- ✓ Application whitelisting
- ✓ Antimalware engine
- ✓ Device control
- ✓ File Integrity Monitoring
- ✓ Exploit Prevention
- ✓ Wireless access control
- ✓ Log Inspection
- ✓ PLC integrity checker
- ✓ Ransomware protection
- ✓ Firewall

Industrial Anomaly and Breach Detection

KICS for Networks

Network security capabilities:
- ✓ Network Visualization
- ✓ Network Activity Monitoring
- ✓ Asset Discovery
- ✓ Deep Packet Inspection
- ✓ Machine Learning for Anomaly Detection
- ✓ Remote Access Detection
- ✓ Malware Spreading Detection
- ✓ Event Correlation
- ✓ Safe Non-Invasive Mode
- ✓ SOC/SIEM Integration

Centralized security management

Kaspersky Security Center

Some of the supported devices & protocols

SIEMENS, Schneider Electric, OMRON, Rockwell Automation, MITSUBISHI ELECTRIC, EMERSON, ABB, CODESYS, YOKOGAWA

SERVICES

Training and awareness

- **Kaspersky® Security Awareness**
- **Kaspersky® Security Trainings**

Expert services and intelligence

- **Kaspersky® Security Assessment**
- **Kaspersky® Incident Response**
- **Kaspersky® Threat Intelligence**
- **Kaspersky® Managed Protection**

Awareness and training programs:
- Industrial Cybersecurity Awareness (1 day)
- Advanced Industrial Cybersecurity in Practice (1-2 days)
- ICS Digital Forensics for Professionals (4 days +)
- ICS Penetration Testing for Professionals (5 days)
- IoT vulnerability research and exploitation training (4 days)
- Capture the flag (CTF) competition
- Become a Trainer – Train the Trainer
- Kaspersky Interactive Protection Simulation (KIPS)

Expert services features:
- Penetration testing and threat modelling
- Secure network architecture and controls recommendations
- Emergency support to localize incident and digital forensics (available n demand or via subscription)
- ICS Adversary Update Reports (TTPs, targets, attribution)
- Vulnerability database and advisory

kaspersky

산업 사이버 보안에 대한 전략적인 접근

ics.kaspersky.com