kaspersky

Эволюция бизнеса KICS в 2020

Георгий Шебулдаев
Head of Growth Center

Kaspersky Industrial Cybersecurity Conference 2020

KICS сегодня – это:

1000

Заказов

на продукты и сервисы

120

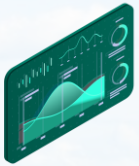
Промышленных сетей

Под защитой KICS for Networks

220

Клиентов

По всему миру



33,000

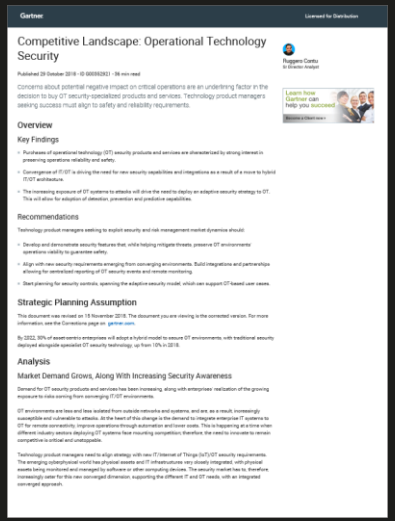
Эндпойнтов

Под защитой KICS for Nodes

Gartner признает KICS в 4х из 5ти доменах промышленной ИБ

- ✓ OT Endpoint Security
- ✓ OT Network Monitoring and Visibility
- ✓ Anomaly Detection, Incident Response and Reporting
- ✓ OT Security Service

Покрытие шире, чем у любого другого вендора



Gartner

Licensed for Distribution

Competitive Landscape: Operational Technology Security

Ruggero Contu
Sr Director Analyst

Learn how Gartner can help you succeed.

Overview

Key Findings

Recommendations

Strategic Planning Assumption

Analysis

Market Demand Grows, Along With Increasing Security Awareness

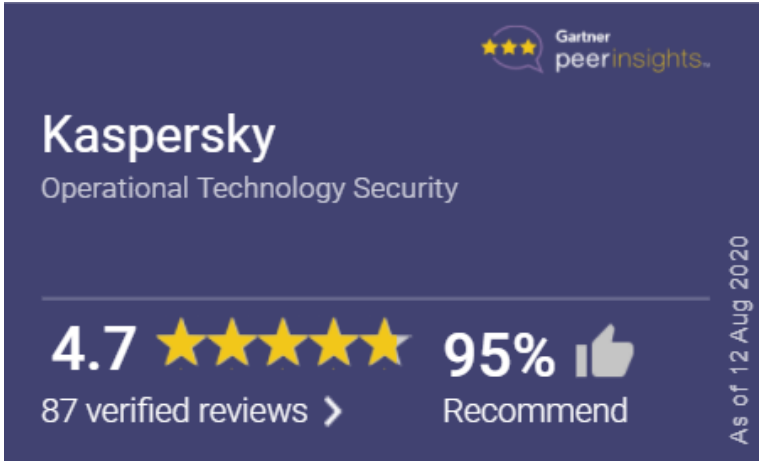
KICS отмечен наибольшим числом “5-star” обзоров

Топ 3 причин покупки KICS по мнению клиентов:

1. Внедрение инноваций
2. Соблюдение требований регулятора и оценка рисков
3. Управление затратами

Топ 3 качества KICS, повлиявших на решение о покупке:

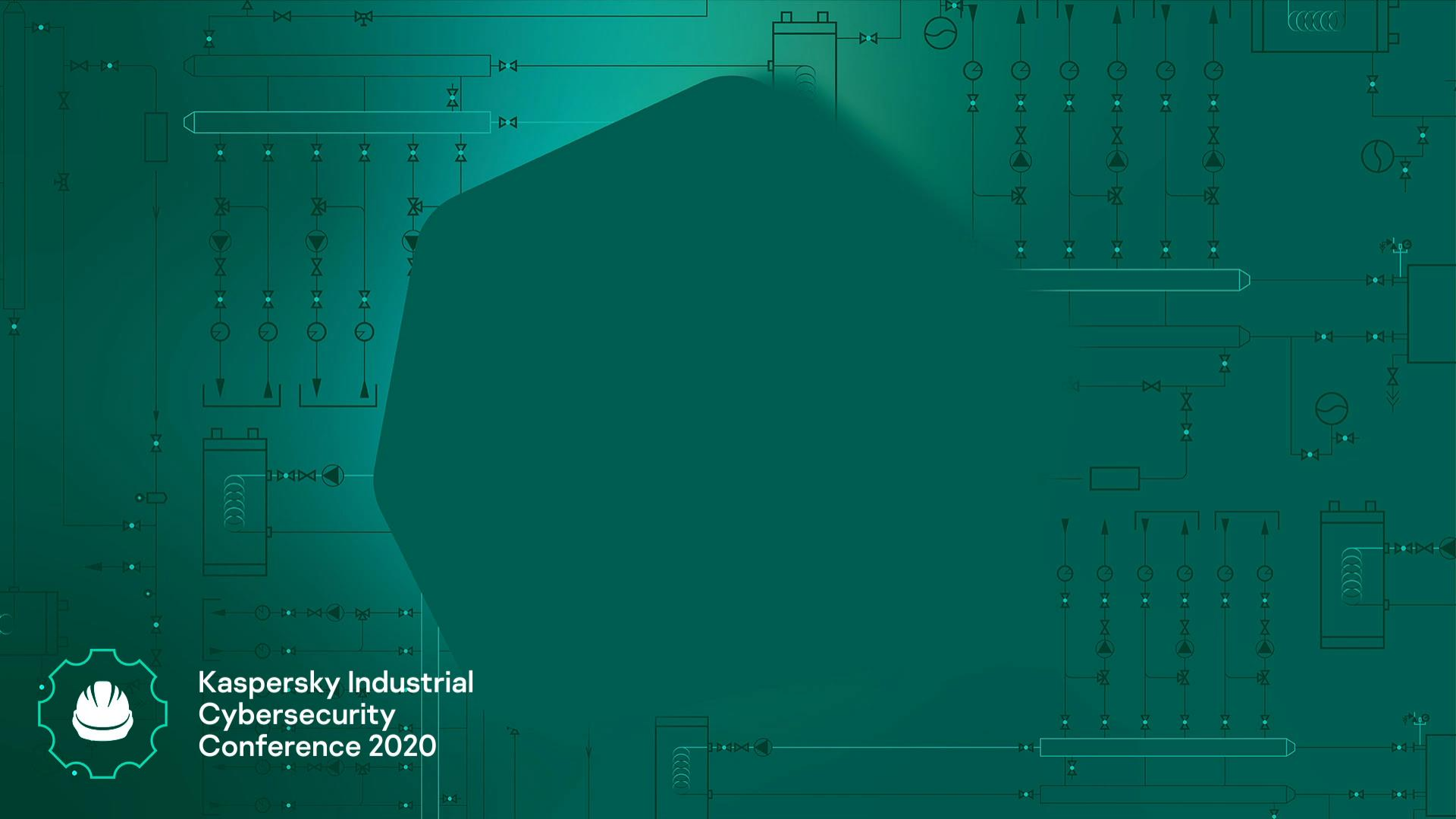
1. Роадмап продукта и видение будущего
2. Функционал и быстродействие продукта
3. Сильная сервисная поддержка



Больше деталей:
https://www.gartner.com/reviews/market/operational-technology-security

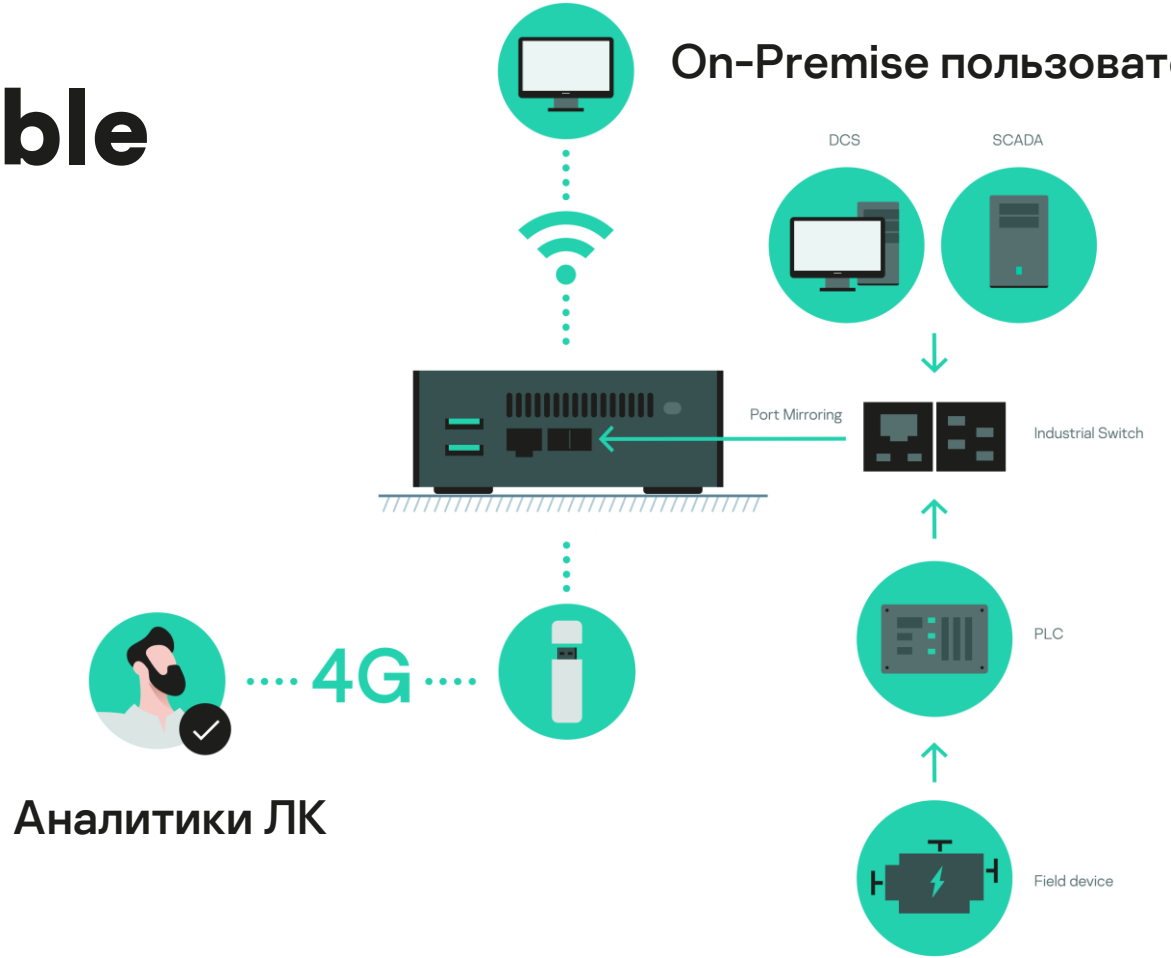
*As of 12th Aug 2020, Kaspersky has an overall rating of 4.7 out of 5 in the Operational Technology Security Market based on 84 reviews, with a total of 62 5-star reviews. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences, and do not represent the views of Gartner or its affiliates.

Новые функции KICS


Kaspersky Industrial
Cybersecurity
Conference 2020

KICS Portable

KICS Portable



KICS Portable – Пример отчета

109

Cell area

Issues in main industrial process network with PLCs can directly impact automation process by altering or disrupting production.

91

Industrial zone and cell area

Compromise of management systems of industrial process might lead to loss of operations control and visibility of automation process.

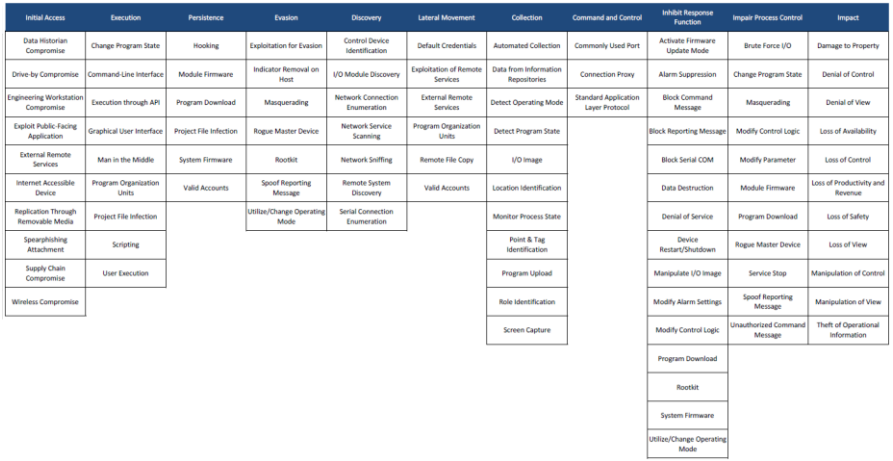
2

External networks

Potentially adversary can get access to some systems or networks from Internet.

2021 – Первые испытания решений по мониторингу безопасности сетей АСУ ТП на основе базы техник атакующих MITRE ATT&CK for ICS

Kaspersky Industrial CyberSecurity for Networks один из пяти участников.



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

- Armis
- CyberX, a Microsoft company
- Dragos
- The Institute for Information Industry
- Kaspersky

https://medium.com/mitre-engenuity/announcing-the-att-ck-evaluations-for-ics-fall-2020-cohort-19fb6a1df164

Жизненный цикл разработки **KICS for Networks** сертифицирован на IEC 62443 Part 4-1

Стандарт **МЭК 62443-4-1:2018** Безопасность для систем управления и промышленной автоматики: требования к жизненному циклу безопасной разработки продукта

KICS for Networks первый продукт в мире в своей категории прошел сертификацию на уровень зрелости процессов безопасной разработки **ML-3** (ML-4 максимальный)

- Большая степень уверенности в безопасности продукта
- Вероятность уязвимостей максимально снижена
- Лучшие практики программирования
- Всестороннее тестирования и документирование

TÜV AUSTRIA

CERTIFICATE

Certification according to IEC 62443
Security for industrial automation and control systems
Part 4-1: Secure product development lifecycle requirements (IEC 62443-4-1:2018)

In accordance with TÜV AUSTRIA SERVICES procedures, it is hereby certified that

Kaspersky Lab JSC
Leningradskoe sh. 39A bld.2
125212 Moscow
Russian Federation

applies a secure product development lifecycle in line with the above standard **at a maturity level of 3** for the following scope

Kaspersky Industrial Cybersecurity for Networks

Based on inspection report: AU-20042706
Initial certification 2020-09-01
Valid until 2023-08-31

Certification Body
at TÜV AUSTRIA SERVICES GMBH Vienna, 2020-09-01

This certification was conducted in accordance with TÜV AUSTRIA SERVICES auditing and certification procedures and is subject to regular surveillance audits.

TÜV AUSTRIA SERVICES GMBH Deutschstraße 10 A-1230 Wien www.tuv.at

ZERTIFIKAT | CERTIFICATE | CERTIFICAT | CERTIFICADO | СЕРТИФИКАТ | 证书 | 認證

Программа сотрудничества с исследовательскими лабораториями и университетами

Профиль партнёров

ВУЗы, исследовательские департаменты промышленных компаний, центры мониторинга (SOC), центры реагирования на инциденты (CERT and CSIRT), и другие организации у которых есть лаборатории/стенды АСУ ТП и которые проводят исследования и обучение специалистов

Выгоды

- Бесплатные лицензии на продукты для заданных целей
  - **KICS for Nodes** – Industrial Endpoint Protection
  - **KICS for Networks** – Industrial Network Anomaly Detection
  - **MLAD** – Process Variables Anomaly Detection
- Экспертная поддержка при создании лабораторной среды, развёртывании и наладке наших инструментов, помощь в моделировании сценариев атак, интеграции решений в процессы SOC, и разработке правил детектирования и корреляции

Наши цели

- Вклад в повышение квалификации профессионалов
- Доступ к разным промышленным процессам для лучшей их защиты
- Обратная связь на наши технологии для их совершенствования
- Возможности демонстраций совместных успехов профессиональному и академическому сообществу по кибербезопасности и промышленной автоматизации

kaspersky

Спасибо Вам!

Kaspersky Industrial Cybersecurity Conference 2020