Kaspersky Industrial Cybersecurity Conference

Новости и планы KICS

Стрелков Андрей,
старший менеджер по продукту

kaspersky

Содержание

3. Платформа KICS

9. KICS for Networks

19. KICS for Nodes

28. Планы на 2023

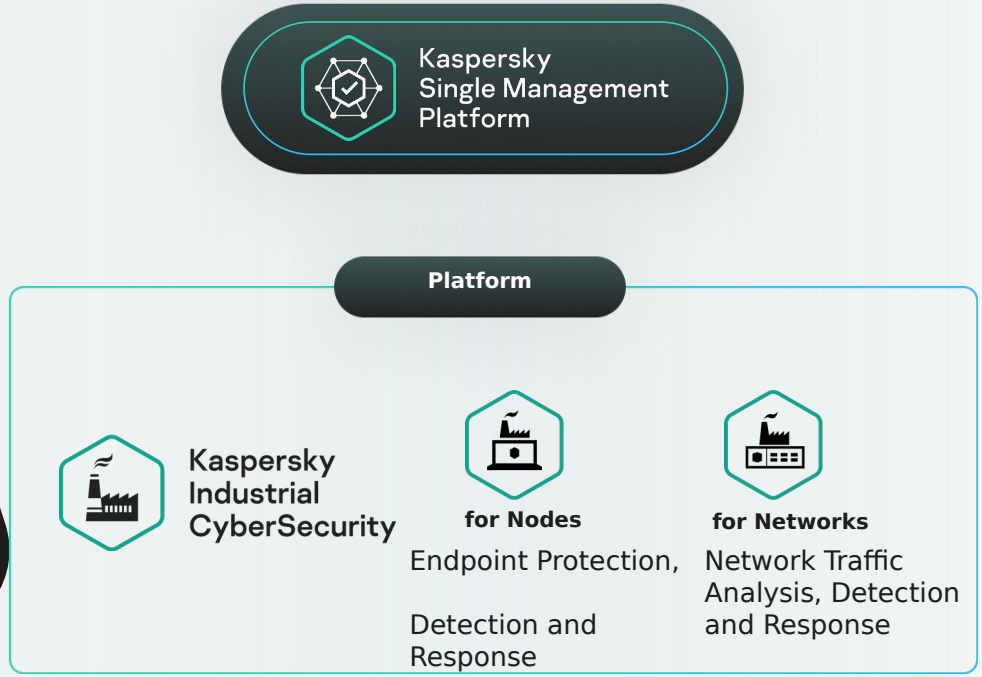
32. Еще Интересное

Платформа KICS

Обновления
продуктовой линейки,
2022

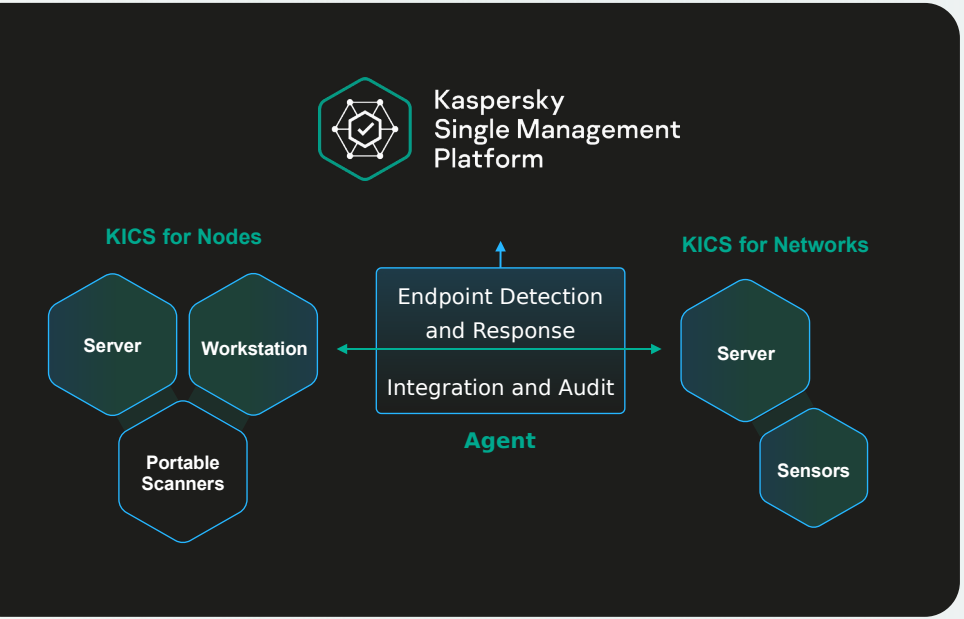
Решение для защиты индустриальных сред

Много-функциональная платформа для защиты промышленных сред



Архитектура платформы

Kaspersky Industrial CyberSecurity



Детектирование и реагирование в сети

Анализ сетевого трафика от сетевых и узловых сенсоров для обнаружения угроз и аномалий тех процесса.

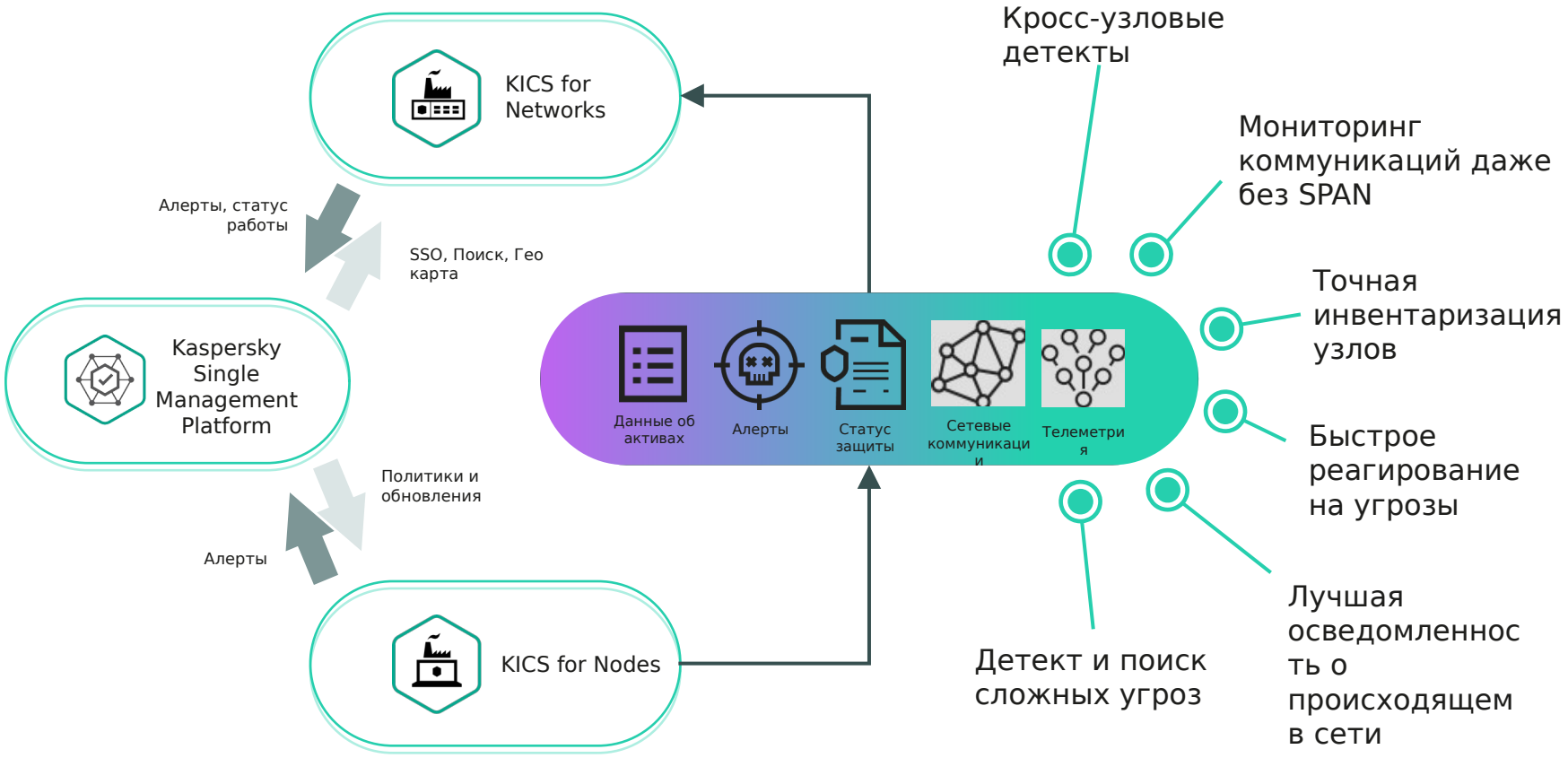
Управление активами и рисками

Пассивный и активный анализ активов и выявление уязвимостей. Ситуационная осведомленность и отчетность.

Детектирование, реагирование и аудит на узлах

АВ, контроль устройств и приложений, аудит безопасности. Расследование угроз и реагирование с KICS EDR

Нативный индустриальный XDR: возможности платформы



Обогащение событий KICS for Networks

Данные о программе и пользователе

Communications Front End - IEC 870-5-104 Slave (2.22.13)

Поставщик продукта	Siemens AG, PTD EA
Имя продукта	RC-PCSW-CFE
Версия продукта	2.22.13
Путь к файлу	C:\Program Files AM\PAS PQS\CFE
Операционная система	Microsoft Windov
Адрес взаимодействв...	172.17.0.220:240
Является сервером	Нет
Имя пользователя	SicamPAS\PASRu
Тип учётной	Не администрат

QTester104.exe

Путь к файлу	C:\qtester104-v2.1\bin\QTester104.exe
Операционная система	Microsoft Windows Server 2012 R2 Standard
Адрес взаимодействв...	172.17.0.220:2404
Является сервером	Нет
Подпись	Недействительная
Md5	5cd3a5e9d8291c6deb037dfe47b110ac
Sha256	a0fffa2d4a91787e5b5e58f1c43858953945 bdc379ddfa1767f3345333848b5f

Устройства

Знаем с какого устройства была аномальная коммуникация

Приложение

Знаем какое приложение является источником

Пользователь

Знаем от имени какого пользователя запущено приложение

Обогащение события NIC в KICS for Networks

Events | Export | Customize table | Update table

83 New events | 0 Events in progress

Scores 0 → 10 | Technologies DPI NIC IDS CC EXT AM EPP | Period Last 48 hours | Default filter

Last seen	Title	Score	Source	Destination	Proto...	Techn...
2022-09-09 13:46:10.464	Attempt to run an unauthorized or untrusted appli...	8.6	192.168.55.235	192.168.55.235	TCP	EPP
2022-09-09 13:46:10.306	Prohibited file operation in the specified monitorin...	8.6	192.168.0.200	192.168.0.200	TCP	EPP
2022-09-09 13:46:10.305	Prohibited file operation in the specified monitorin...	8.6	192.168.0.200	192.168.0.200	TCP	EPP
2022-09-09 13:46:07.299	Prohibited file operation in the specified monitorin...	8.6	192.168.0.200	192.168.0.200	TCP	EPP
2022-09-09 13:45:58.655	Unauthorized network interaction detected (ARP)	6.6			ARP	NIC
2022-09-09 13:45:58.655	Unauthorized network interaction detected (ARP)	6.6			ARP	NIC
2022-09-08 14:47:30.240	**Attempted network interactions with IP address ...**	9.6	10.65.92.144	142.250.150.94	IP	EXT
2022-09-08 14:48:03.530	Unauthorized network interaction detected (T...	6.6	10.65.92.144:56221	142.250.150.94:80	TCP	NIC
2022-09-08 14:47:48.479	Unauthorized network interaction detected (T...	6.6	10.65.92.144:56211	142.250.150.94:80	TCP	NIC
2022-09-08 14:47:30.240	Unauthorized network interaction detected (H...	6.6	10.65.92.144:56205	142.250.150.94:443	HTTPS	NIC

Unauthorized network interaction detected (HTTPS)

Score 6.6

2022-09-08 14:47:30.240 – 2022-09-08 14:48:56.272

Data on program and user

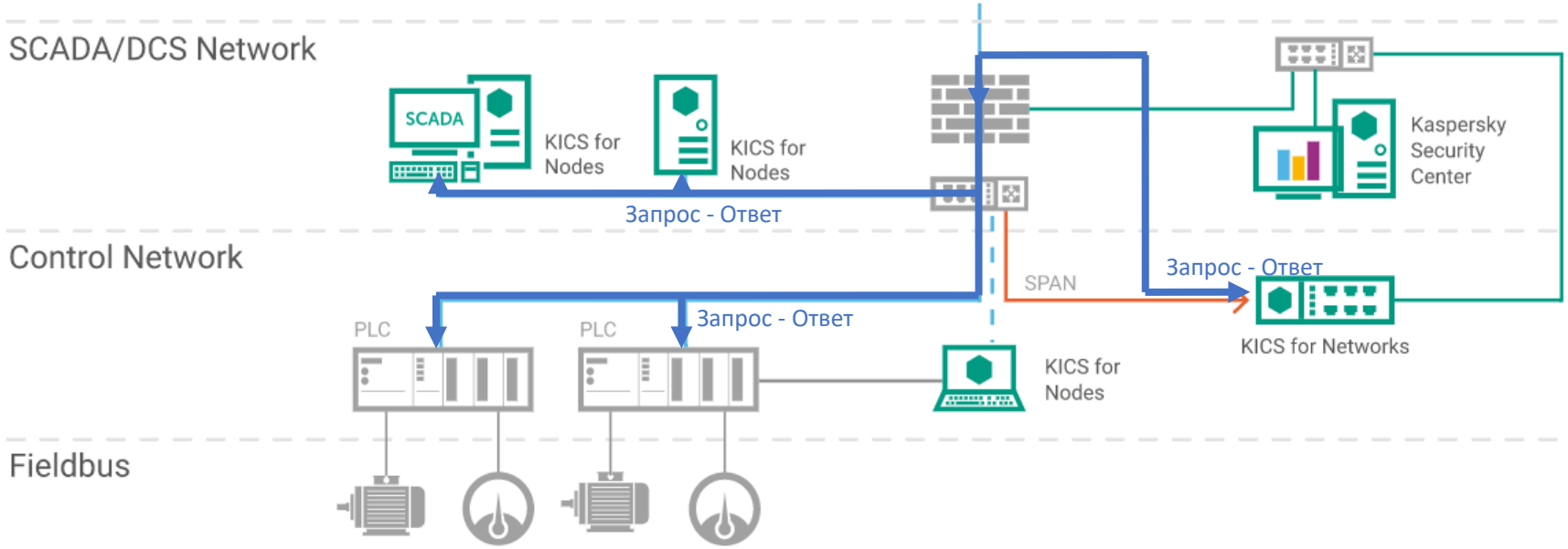
Google Installer (1.3.35.451)

Product vendor	Google LLC
Product name	Google Update
Product version	1.3.35.451
Path to file	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
Operating system	Microsoft Windows Server 2012 R2 Standard
Communication address	142.250.150.94:443
Is a server	Yes
User name	ENERGOSTEND-KSC12\ENERGOSTEND-KSC$
User account type	Not administrator
Signature	Valid
Md5	0bca3f16dd527b4150648ec1e36cb22a

KICS for Networks

Обновления
продуктовой линейки,
2022

Активный опрос для промышленных сред



+

- Не нужно ждать
- Точные данные
- Безопасные методы
- Анализ рисков

-

- Инвазивный метод опроса
- Требует тестирования
- Полу-автоматический
- Нужен доступ к

Активный опрос: преимущества

АРМ

Серверы

Сетевые устройства

Контроллеры

Modbus
S7comm (TCP)
S7comm (Ethernet)
CIP
Profinet-DCP
MMS
Beckhoff (TCP/UDP)
DNP3

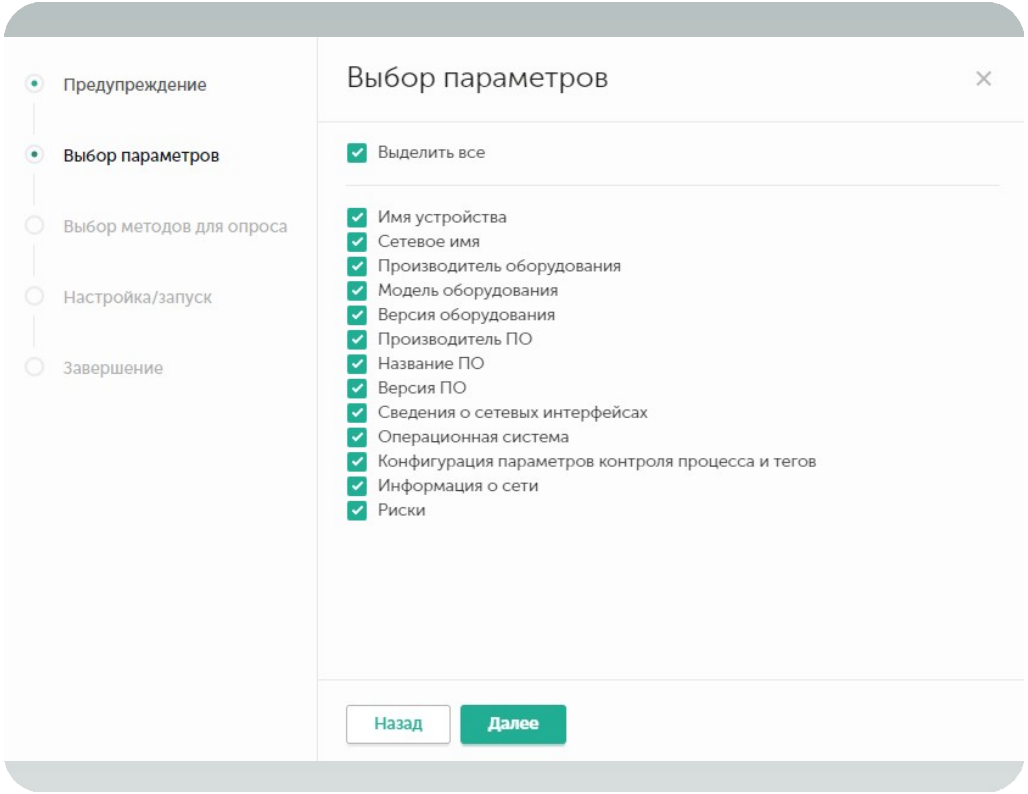
SNMP v1,2,3
SSH
WMI
WinRM (HTTP)
WinRM (HTTPS)
SMB
ARP

Только поддерживаемые стандартные протоколы и порты. Нет сканирования портов.

Авто-определение методов опроса по категории устройства.

Опросы удаленных сегментов сети с сенсоров или Linux-узлов. Модуль опроса – подключаемый коннектор.

Активный опрос: возможности

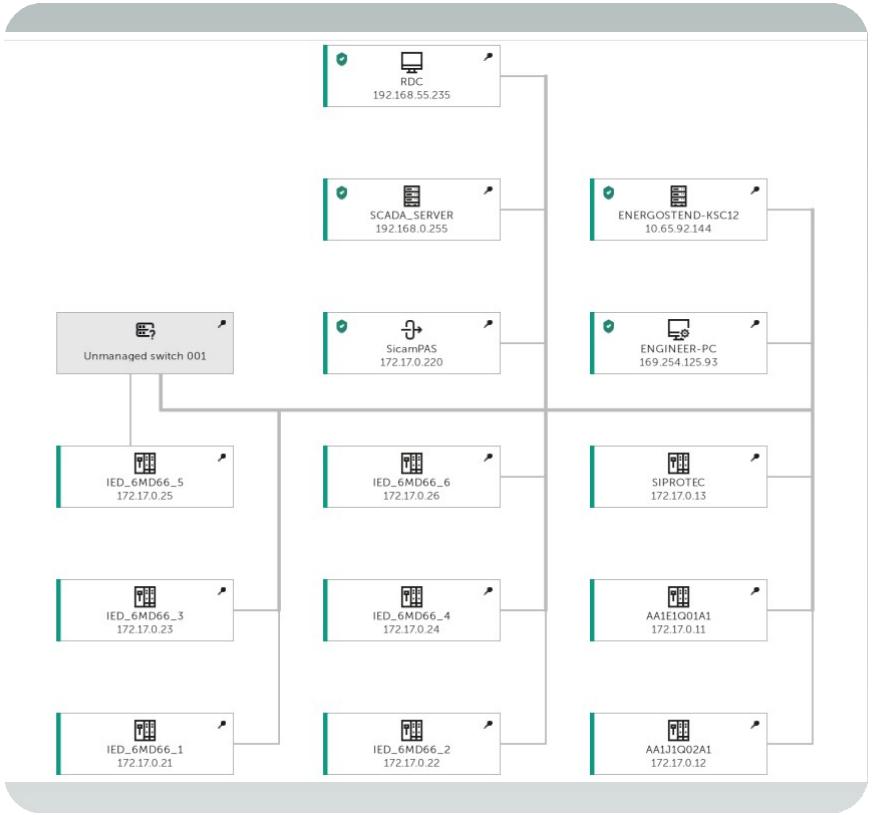


Инвентаризация
Определение множества атрибутов устройств разом

Физические подключения
Построение топологической карты сетевых подключений

Риски
Определение рисков и проблем конфигурации

Топологическая карта сети



Карта физических подключений с ортогональными линками и шинами данных

Позволяет точно определить к какому порту коммутатора подключено устройство

Строится автоматически за счет активного опроса узлов и сетевого оборудования, есть ручное редактирование

Анализ рисков в инфраструктуре для плановой работы по усилению ИБ

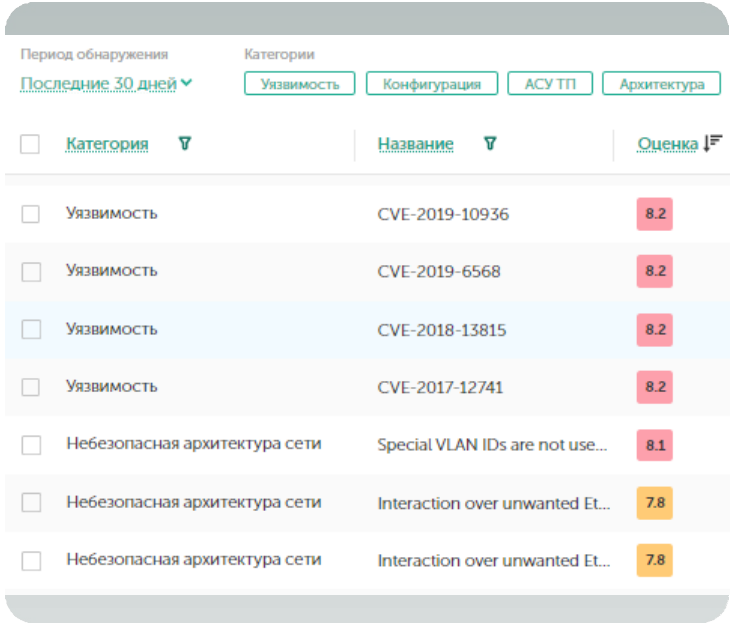
Имя	Адресная инфор...	Категор...	Знач...	Риски
SIMATIC S7-1500	Несколько значений	Коммутатор	Высокая	CVE-2020-15782 CVE-2017-12741 ...
Mx80 Ethernet: CPU	Несколько значений	Коммутатор	Средняя	Небезопасная архитектура сети
OS-PC	Несколько значений	Рабочая станция	Средняя	Небезопасная архитектура сети
WIN7_PAS_CC	00:50:56:8a:41:6f; 192...	Рабочая станция	Средняя	Небезопасная архитектура сети
ES1	00:50:56:8a:76:47; 192...	Рабочая станция	Средняя	Небезопасная архитектура сети
OS-PC (2)	00:0e:04:03:09:92; 192...	Рабочая станция	Средняя	Проблемы конфигурации ...
WIN-2GRCNFRCFPC (2)	00:50:56:ba:1f:90; 10....	Рабочая станция	Средняя	Небезопасная архитектура сети
WIN-2GRCNFRCFPC	192.168.2.212	Рабочая станция	Средняя	Проблемы конфигурации ...

- Уязвимая сетевая архитектура
- Слабые настройки безопасности
- Устаревшие, уязвимые, нежелательные, незашифрованные протоколы
- Аномалии в сетевых протоколах
- Устаревшая ОС
- Неавторизованные устройства

Ситуационная осведомленность

Самое важное на дашборде

10-ти балльная шкала оценки критичности событий и рисков

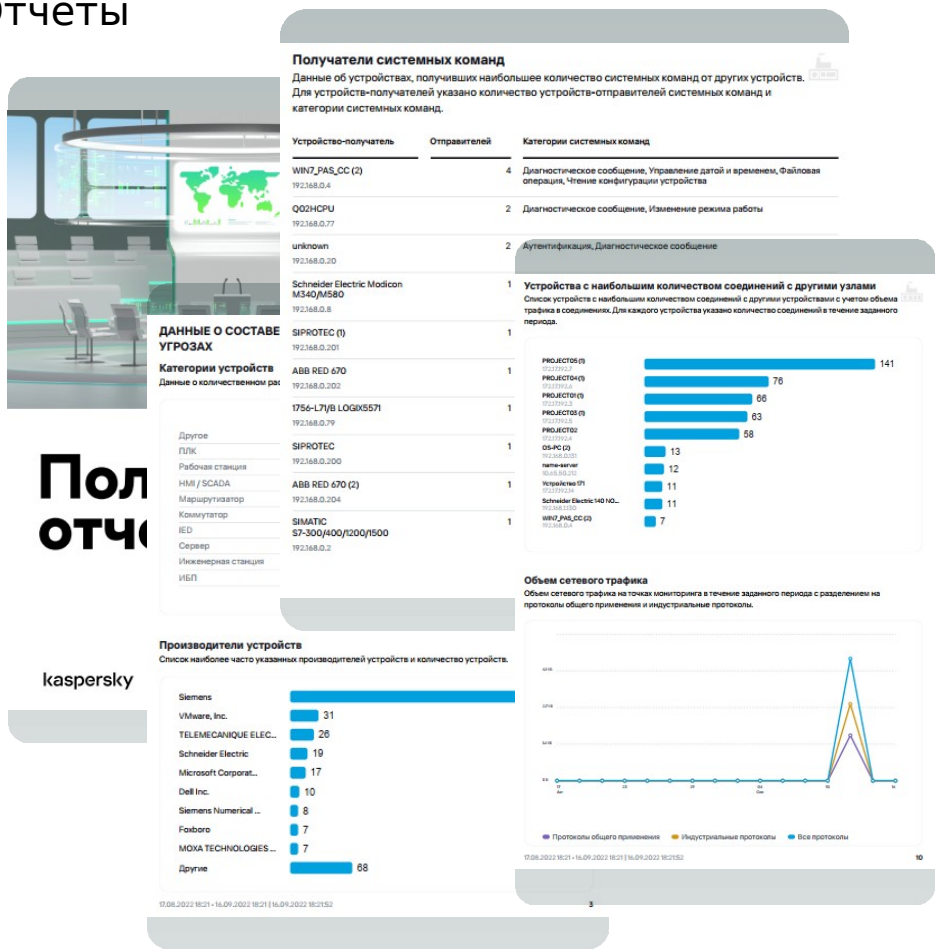


Гранулярные оценки
Легче приоритезировать более критичные события

Динамический скоринг
Учитывается значимость актива, его сетевые подключения и уязвимости

Гибкость
Настраиваемые базовые оценки рисков

Отчеты



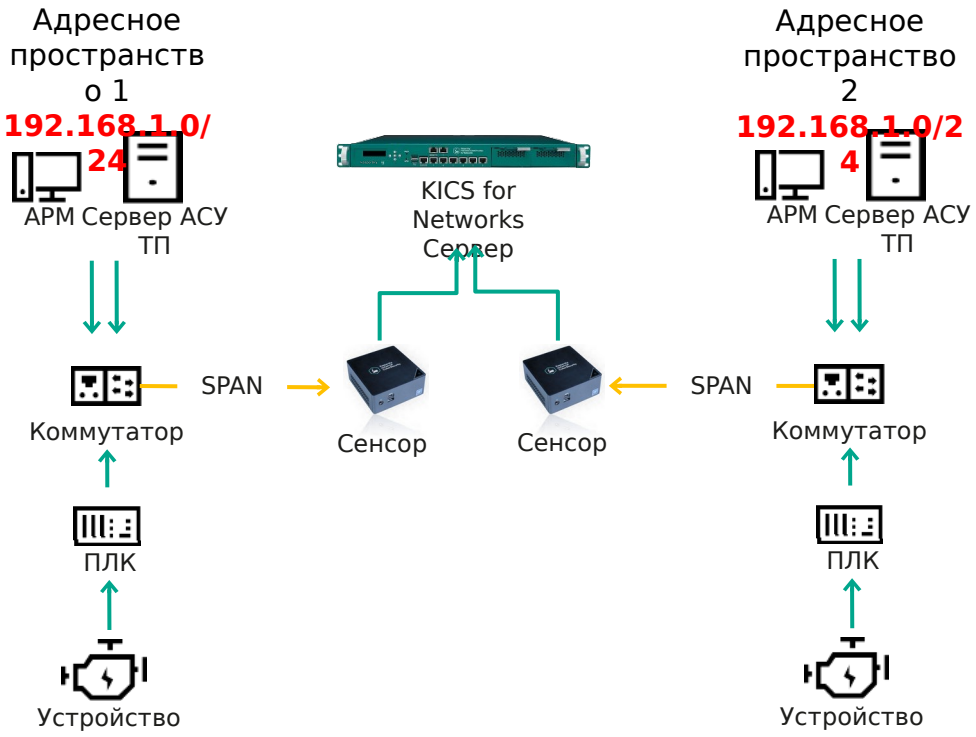
Отчеты в pdf формате
Несколько шаблонов отчетов

Отчеты строятся за произвольный период времени

Можно настроить генерацию по расписанию и отправку по почте

Поддержка сегментов сети с одинаковой адресацией

АП позволяют мониторить устройства с одинаковыми IP и/или MAC адресами



Обновления индустриального DPI в цифрах

Распознавание 7 новых OT протоколов и более 10 IT
Доработки для 10 уже поддержанных протоколов: обучение, системные команды, индустриальные конфигурации

Статистическое обучение тегам для Modbus и S7Comm

Импорт из файлов проектов для 8 новых АСУ ТП

2 новых модели ПЛК
Пассивный PLC Checker для 2х протоколов

… и многое другое в Онлайн доке

KICS for Nodes

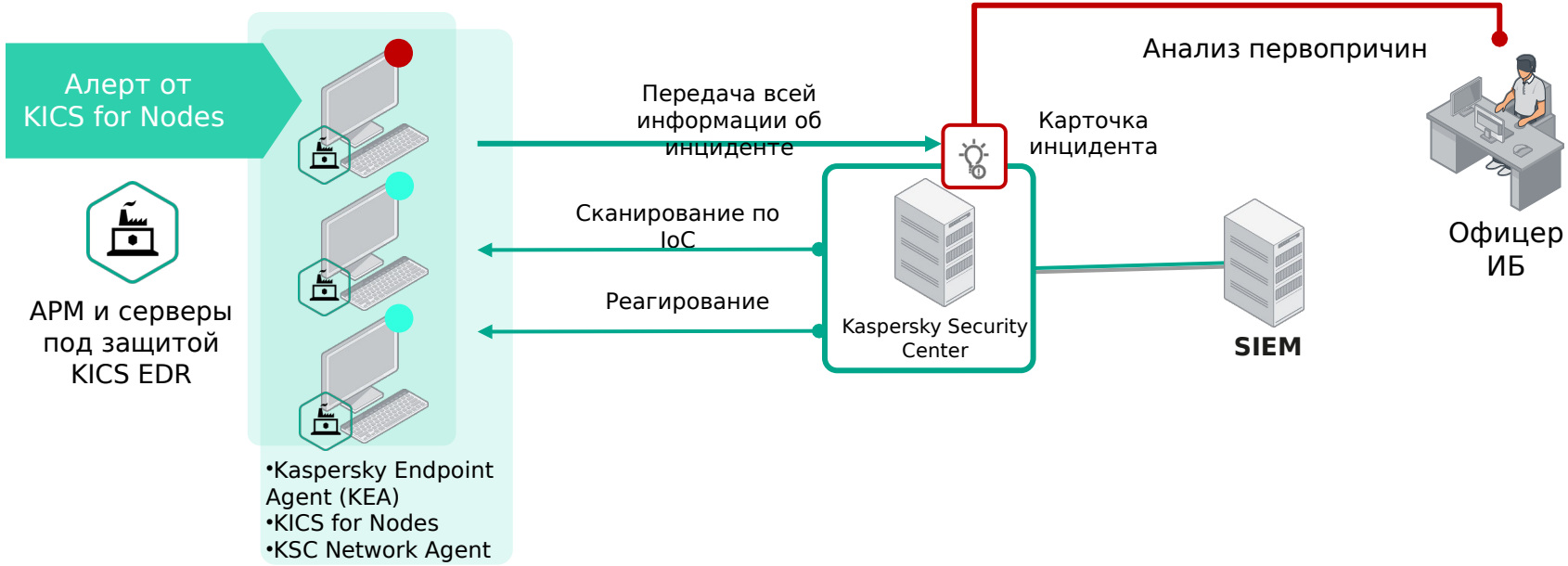
Обновления
продуктовой линейки,
2022

KICS Endpoint Detection and Response

Преимущества:

- Вся необходимая информация об инциденте
- Снижение времени реагирования на инциденты
- Богатый набор инструментов для реагирования, но все решения принимает оператор
- Не влияет на работу АСУ ТП, не генерирует трафик. Совместим с устаревшими ОС

Архитектура KICS EDR



Аудит безопасности

Преимущества:

- Автоматизированный аудит на базе единого агента
- Не влияет на технологический процесс
- Групповые задачи и централизованное управление
- Детализированные отчеты
- База данных уязвимостей АСУ ТП от ICS Cert
- Открытый стандарт OVAL. Поддержка БДУ, АЛТЭКС-СОФТ и любого другого контента в OVAL

Отчеты аудита KICS for Nodes

oval:ru.altx-soft.win:def:26242	High	**Минимальная длина пароля** Этот параметр безопасности определяет минимальное количество знаков, которое должно содержаться в пароле пользователя. **Ссылка на источник:** **Снижение рисков:** **Источник:** GPO:Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей *Эталонное значение:* ***8 знаков*** ***Этот параметр безопасности определяет минимальное количество знаков, которое должно содержаться в пароле пользователя. Можно установить значение от 1 до 14 знаков, либо 0 знаков, если пароль не требуется. По умолчанию: 7 - на контроллерах домена. 0 - на автономных серверах. Примечание. По умолчанию компьютеры-члены домена используют конфигурацию своих контроллеров домена.***
oval:ru.altx-soft.win:def:26243	High	**Минимальный срок действия пароля** Этот параметр безопасности определяет период времени (в днях), в течение которого пользователь должен использовать пароль, прежде чем его можно будет изменить. **Ссылка на источник:** **Снижение рисков:** **Источник:** GPO:Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей *Эталонное значение:* ***1 день*** ***Этот параметр безопасности определяет период времени (в днях), в течение которого пользователь должен использовать пароль, прежде чем его можно будет изменить. Можно установить значение от 1 до 998 дней либо разрешить изменять пароль сразу, установив значение 0 дней. Значение минимального срока действия пароля должно быть меньше значения максимального срока действия пароля, за исключением значения максимального срока, равного 0 дней, означающего, что срок действия пароля никогда не истечет. Если значение максимального срока действия пароля равно 0, то минимальный срок действия пароля может принимать любые значения в диапазоне от 0 до 998 дней. Установите значение минимального срока действия пароля больше 0, чтобы включить ведение журнала паролей. Без установки минимального срока действия пароля пользователь может изменять пароли повторно, пока не получит свой старый предпочитаемый пароль. Значение по умолчанию установлено вопреки этой рекомендации, поэтому администратор может назначить пользователю пароль, а затем потребовать сменить его при входе пользователя в систему. Если для журнала паролей установлено значение 0, пользователю не нужно выбирать новый пароль. По этой причине значение для журнала паролей по умолчанию равно 1. По умолчанию: 1 - на контроллерах домена. 0 - на автономных серверах. Примечание. По умолчанию компьютеры-члены домена используют конфигурацию своих контроллеров домена.***
soft.win:def:74003		

База уязвимостей АСУ ТП от Kaspersky ICS Cert

Уникальный контент для автоматизированного поиска уязвимостей с большим покрытием:

Вендоры: Siemens, Schneider Electric, Yokogawa, Emerson, ABB и другие

АСУ ТП:

WinCC OA
STEP7
SIMATIC WinCC
SIMATIC PCS 7
DeltaV
TIA Portal
ProSafe RS
ClearSCADA
Wonderware Intouch
CENTUM VP
Freelance и другие

Уязвимости имеют рекомендации по митигации как от вендоров АСУ ТП, так и от экспертов ICS Cert

Высокое качество контента. Контент пишется на базе анализа собственных стендов с настоящим ПО

Исправляем ошибки и неточности в данных из сторонних источников

Уязвимости с мерами митигации от ICS Cert

TLP: AMBER

Kaspersky ICS CERT kaspersky

Vulnerability Analysis: Yokogawa Centum VP DCS. Hard-coded credentials

Version: 1.0 (30.05.2022)

Analysis of known vulnerability data for inaccuracies and mistakes to help avoid incorrect vulnerability and risk assessments and ineffective mitigation and offer applicable and actionable recommendations

Executive Summary

A hard-coded credentials vulnerability that could lead to remote code execution by an unauthenticated attacker exists in the Yokogawa CENTUM VP DCS.

We rate the vulnerability as Critical against the initial assessment by Yokogawa.

Mitigating this vulnerability should be the highest priority.

CVE-2022-21194	Use of Hard-coded Credentials CVSSv3.0 **7.1 High** (Yokogawa) CVSSv3.1 **9.8 Critical** (Kaspersky ICS CERT)
Affected products	Yokogawa Centum VP DCS

Mitigations

Kaspersky ICS CERT recommendations

Primary Change the default password of the OS account `CTM_PROCESS` on all workstations by following these steps:

1. Choose a long and unique mixed character password that cannot be easily guessed or cracked (only one password for all workstations!)
2. Logon with administrator rights
3. Insert the CENTUM VP software media
4. Find and execute the following file in the command prompt with "-p" parameter: `<CENTUM VP Drive>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateCentumProcess.exe -p (new CTM_PROCESS password)`

⚠ Ensure that all workstations are using the same new password!

We also advise to change `OFFUSER` password using the Windows user management tools. This password must also be the same on all workstations.

For more information about the list of the predefined user accounts in CENTUM VP and how to change their passwords refer to the CENTUM VP Security Guide

Primary To avoid reconfiguring the entire system with a new password, set up the border firewall (or a similar network traffic control solution) to allow only authorized parties to send traffic to the affected workstations.

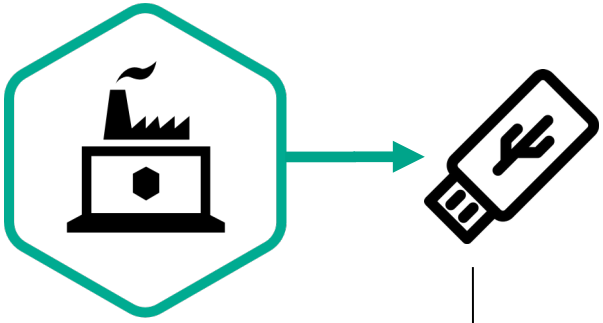
General Regularly update the operating system on the workstations with the affected system

Vendor recommendations*

General Yokogawa strongly recommends all customers to establish and maintain a full security program, not only for the vulnerability identified in this YSAR. Security program components are: Patch updates, Anti-virus, Backup and recovery, zoning, hardening, whitelisting, firewall, etc. Yokogawa can assist in setting up and running the security program continuously. For considering the most effective risk mitigation plan, as a starting point, Yokogawa can perform a security risk assessment.

* https://web-material3.yokogawa.com/1/32094/files/YSAR-22-0001-E.pdf

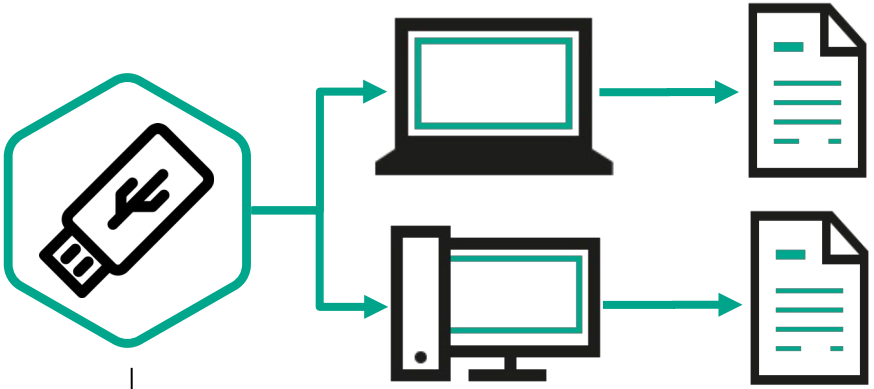
KICS for Nodes Portable Scanner



Стандартный

KICS for Nodes. Проходим Визард для создания портативной версии.

Подходит любая флешка. Нужна лицензия на Portable Scanner.



Портативный сканер KICS for Nodes. Защищен от копирования. Сканирование запускается из CLI.

Сканируем узел с запретом на установку ПО или изолированный узел.

Отчет о сканировани и

Еще новые возможности Nodes

Монитор реестра

Мониторинг и блокирование изменения ключей и значений реестра для выбранной области мониторинга

Модульная установка

Возможность установки компонентов продукта без обязательной установки антивирусного модуля и антивирусных баз

AMSI сканер

AMSI-защита позволяет разрешать или запрещать исполнение опасных и предположительно опасных скриптов

Планы на 2023

Обновления
продуктовой линейки,
2022

KICS for Networks

Q1 2023

4.0.1

- Поддержка Astra 1.7
- Выполнение требований для сертификации ФСТЭК и ФСБ
- [Предварительно] Расширение кол-ва точек мониторинга для одного сервера

Q3 2023

4.1

- **Система централизованного аудита для промышленных сетей** на базе KICS for Networks
- **Развитие XDR-функционала**
  Детальные карточки ассетов и инцидентов с цепочками атаки, реагирование из Networks
- Контроль оборудования на узлах
- Определение категории и роли узла по телеметрии с Nodes
- Гранулярное обучение для сенсоров и точек мониторинга
- Возможность выпуска патчей для продукта
- Обновления DPI
- [Предварительно] Новые схемы лицензирования
- [Предварительно] Виртуальный апплаенс

KICS for Nodes Windows

Q1 2023

KEA

- Интеграция с KEDR Expert: использование KICS for Nodes в качестве сенсора к экспертному EDR
- Поддержка XCCDF фидов для аудита от Altx-soft
- Расширение сетевой телеметрии для отправки в Networks

Q3 2023

3.2

- Сертификация ФСТЭК, ФСБ
- Поддержка централизованной системы аудита на базе Networks
- Легкий KICS for Nodes: новая лицензия без анти-вируса
- Развитие интеграции с KICS for Networks:
  - Контроль оборудования
  - Определение роли узла
  - Расширение сетевой телеметрии для отправки в Networks

KICS for Nodes Linux

[Предварительно] June 2024

1.5

- Сертификация ФСТЭК, ФСБ
- Поддержка Байкал
- Поддержка централизованной системы аудита на базе Networks
- Развитие интеграции с KICS for Networks:
  - Контроль оборудования
  - Определение роли узла

На что еще обратить внимание

KICS + MDR

Непрерывный поиск, обнаружение и устранение угроз от лучшего ИБ вендора

KICS + KUMA

Полноценный XDR. Конвергенция IT и OT сред

KICS + SD-WAN

Легкое подключение удаленных площадок с мониторингом ИБ

Спасибо!

Стрелков Андрей

Старший менеджер по продукту

kaspersky