Вебинар

Kaspersky ICS CERT: как избежать кибершторомов в 2023 году

kaspersky

Спикеры вебинара

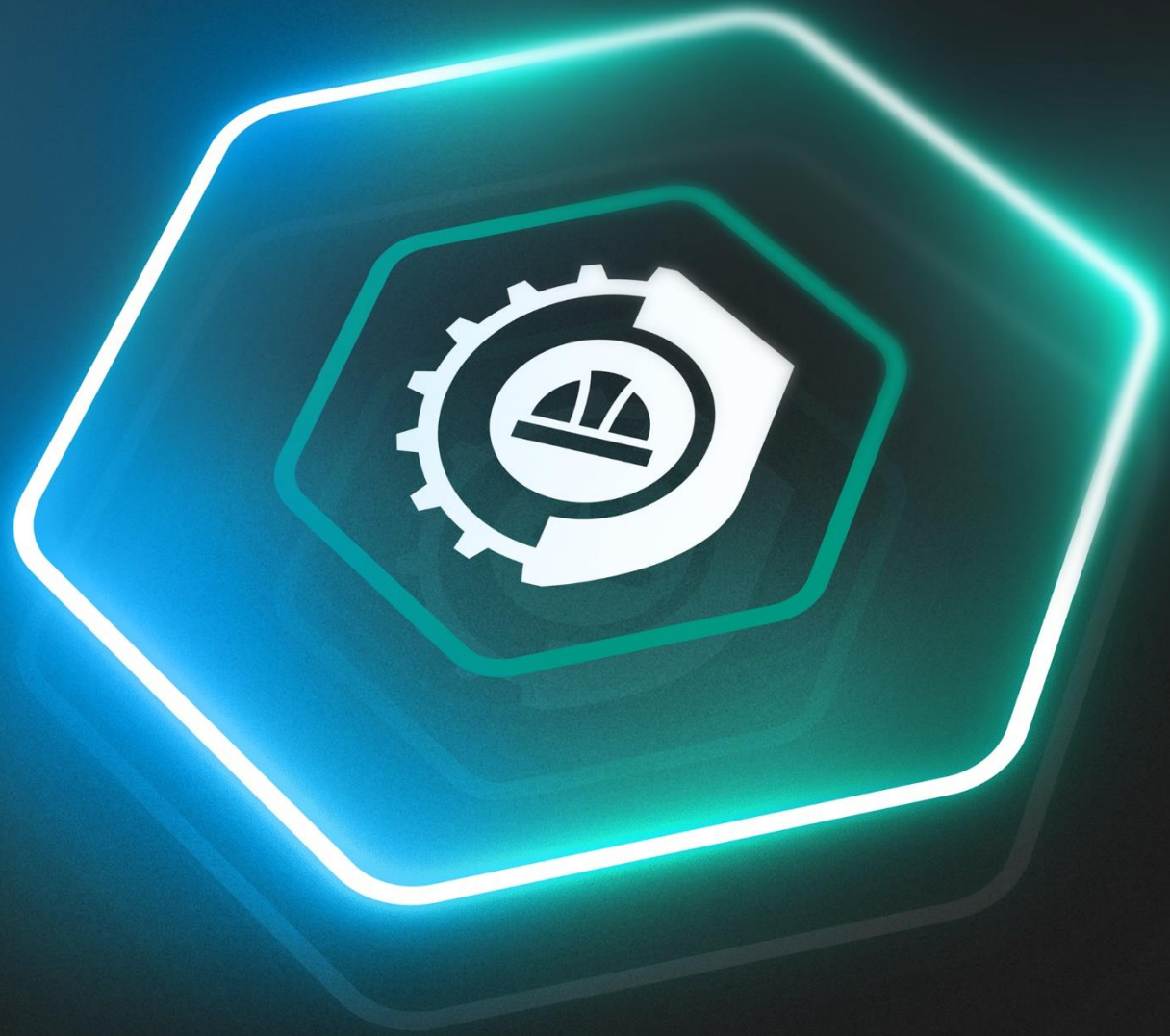
Михаил Березин

Руководитель отдела развития продуктов ICS CERT

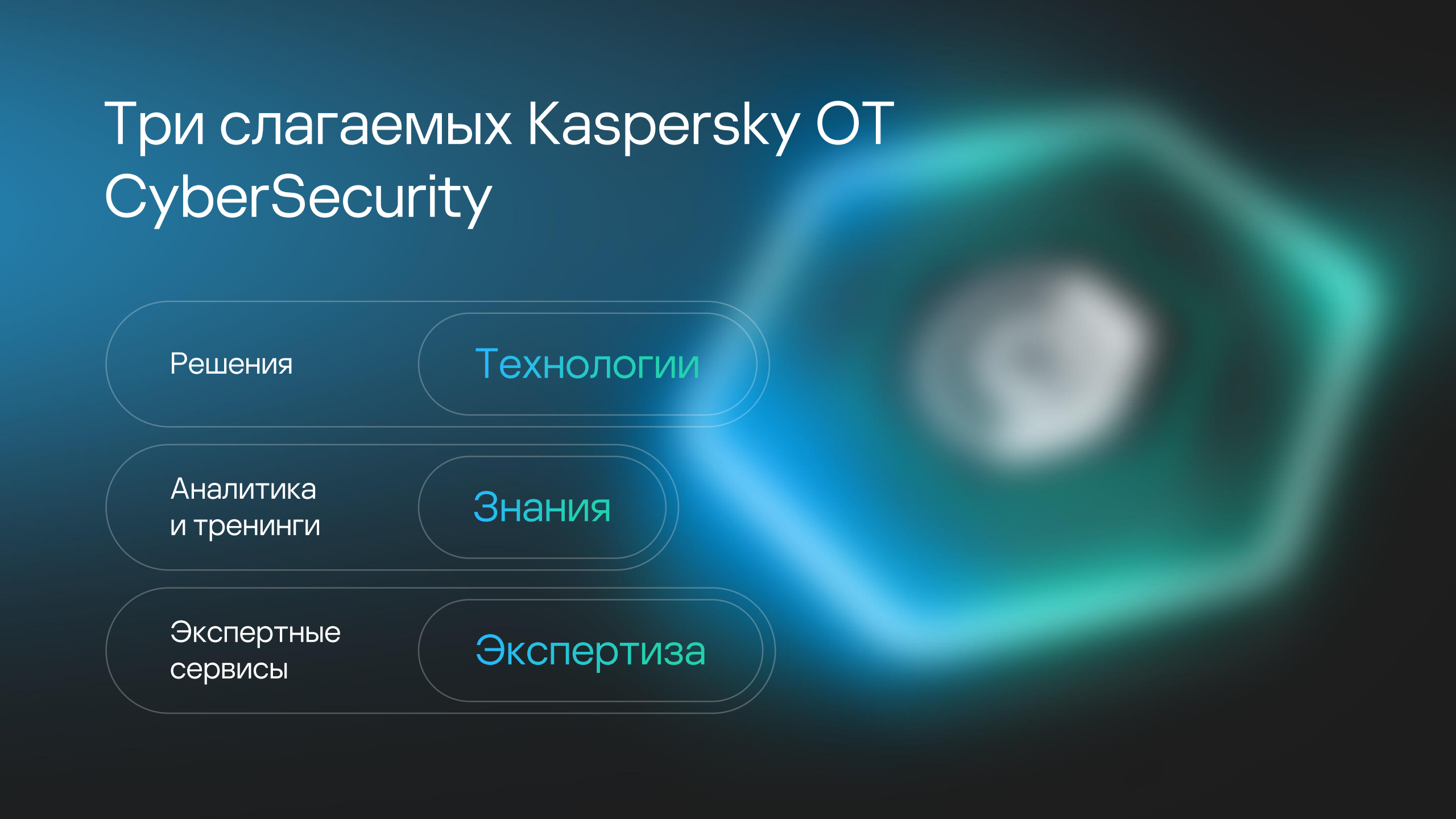
Андрей Бондюгин

Руководитель группы по сопровождению проектов защиты промышленных инфраструктур

Kaspersky OT CyberSecurity



Три слагаемых Kaspersky OT CyberSecurity



Единая концепция промышленной безопасности

Знания

Аналитика об угрозах

- Kaspersky ICS Threat Intelligence

Повышение осведомленности

- Kaspersky Security Awareness

Тренинги для специалистов

- Kaspersky ICS CERT Training

Достоверная аналитика угроз в АСУ ТП и специальные тренинги

Технологии

Основные

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Unified Monitoring and Analysis Platform

Фокусные

- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN
- Kaspersky Antidrone

Решения на базе KasperskyOS

- Kaspersky IoT Secure Gateway
- Kaspersky Secure Remote Workspace
- Kaspersky Automotive Secure Gateway

Полный арсенал защитных решений, протестированных вендорами АСУ ТП

Экспертиза

Анализ защищенности

- Kaspersky ICS Security Assessment

Управляемая защита

- Kaspersky Managed Detection and Response

Скорая помощь

- Kaspersky ICS CERT Incident Response
- Kaspersky Industrial Emergency Kit

Набор экспертных сервисов для комплексной промышленной кибербезопасности

Kaspersky OT CyberSecurity

Средство обнаружения и реагирования на сложные атаки

Единая концепция промышленной кибербезопасности

Технологии

Полный арсенал защитных решений, протестированных вендорами АСУ ТП

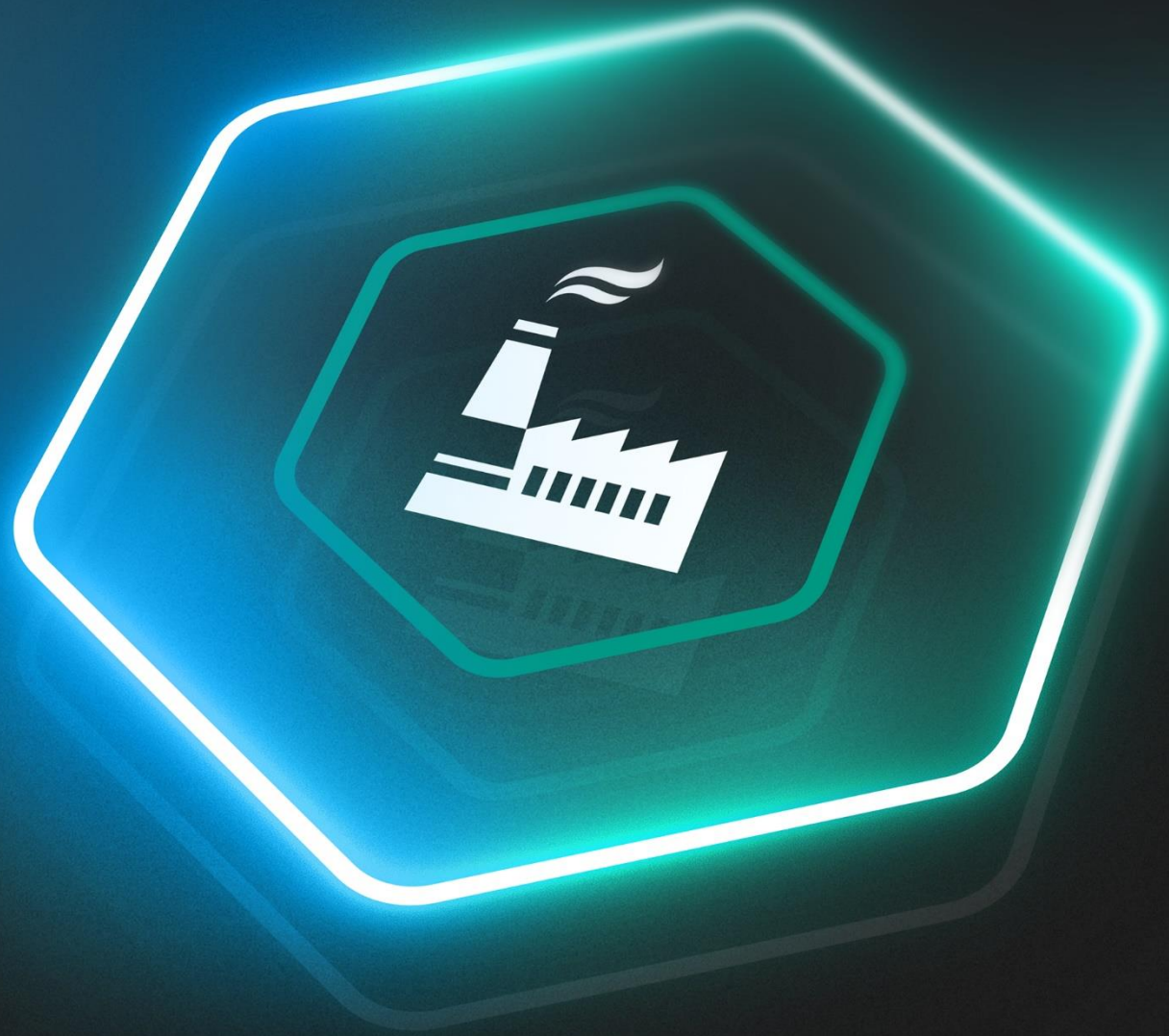
Знания

Достоверная аналитика угроз в АСУ ТП и специальные тренинги

Экспертиза

Набор экспертных сервисов для комплексной промышленной кибербезопасности

Kaspersky Industrial CyberSecurity



Kaspersky Industrial CyberSecurity

Промышленная XDR-платформа

KICS сегодня:

45 000+

Промышленных АРМ / серверов под защитой KICS for Nodes

300+

Клиентов по всему миру

350+

Промышленных сетей под защитой KICS for Networks

260

Количество проектов в 2021

Не просто обновление. Эволюция

	Mission-critical functions	Become groundbreaking advantages with KICS for Networks
OT Visibility	• Список активов и коммуникаций, логическая карта сети • Выявление аномалий тех. процесса • Контроль целостности сети и обнаружение вторжений	• Аудит безопасности, оценка рисков, ситуационная осведомленность и отчеты • Обнаружение уязвимостей промышленного оборудования • Интеграция с KICS for Nodes (события EPP, обогащение сетевых событий, достоверная инвентаризация)
Asset management	• Пассивное обнаружение активов	• Активный опрос узлов • Топологическая карта сети • Плагин для централизованного мониторинга нескольких инсталляций продукта
Integration	• Интеграция по API со сторонними СЗИ	• Наличие встроенных коннекторов для интеграции с внешними системами • Развитая экосистема решения для OT

Архитектура XDR-платформы

Kaspersky Industrial CyberSecurity for Nodes

Инструменты класса
EPP и EDR, аудит

- Сервер
- Рабочая станция
- Портативные сканеры

Kaspersky Industrial CyberSecurity

- Единая консоль
- Нативная интеграция
- Кросс-продуктовые сценарии
- Общий kill-chain

Управление рисками и активами

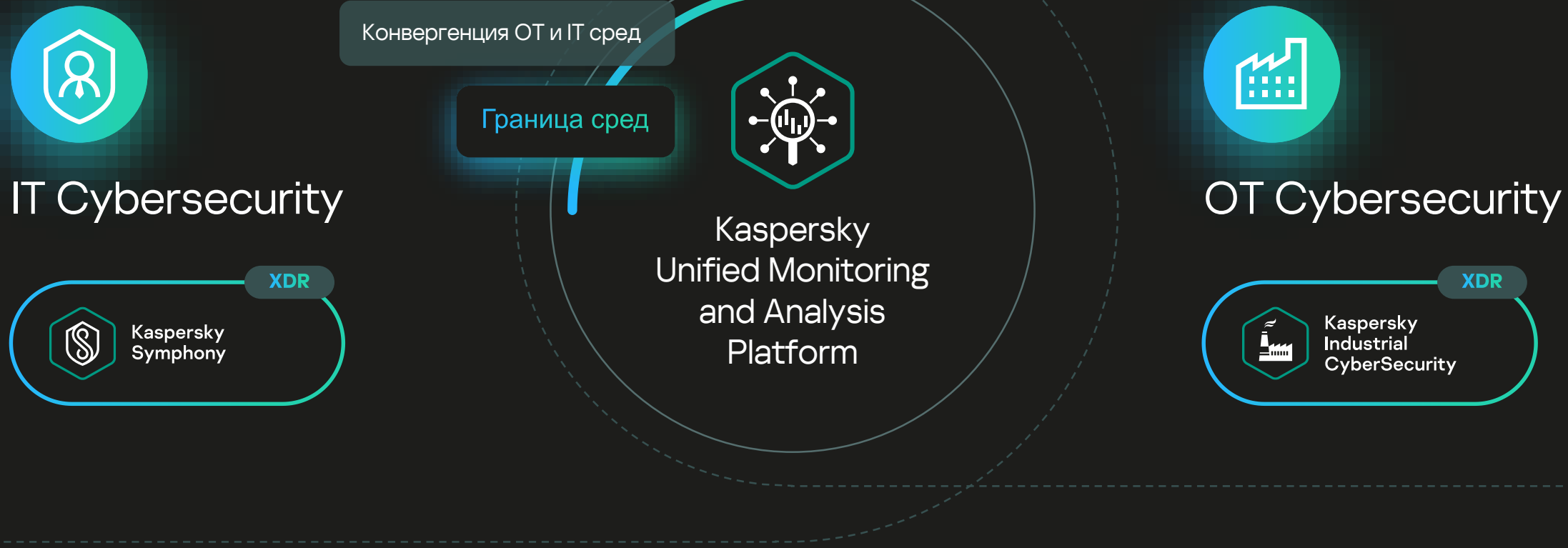
- Пассивное обнаружение компонентов и уязвимостей OT
- Дополнительный активный опрос, ориентированная на риск ситуационная осведомленность и отчетность

Kaspersky Industrial CyberSecurity for Networks

Анализ сетевого трафика
(ICS DPI, IDS)

- Сервер
- Сенсор

Цельное предложение для защиты OT и IT сред



Потоковое обогащение событий

Решения

«Лаборатории Касперского»

Логи

Алерты

Телеметрия

+

Источники данных
передают «сырые» события

Приложения

АРМ

Сетевые СЗИ

Collector

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky CyberTrace

Kaspersky Threat Data Feeds

«Обогащение» событий

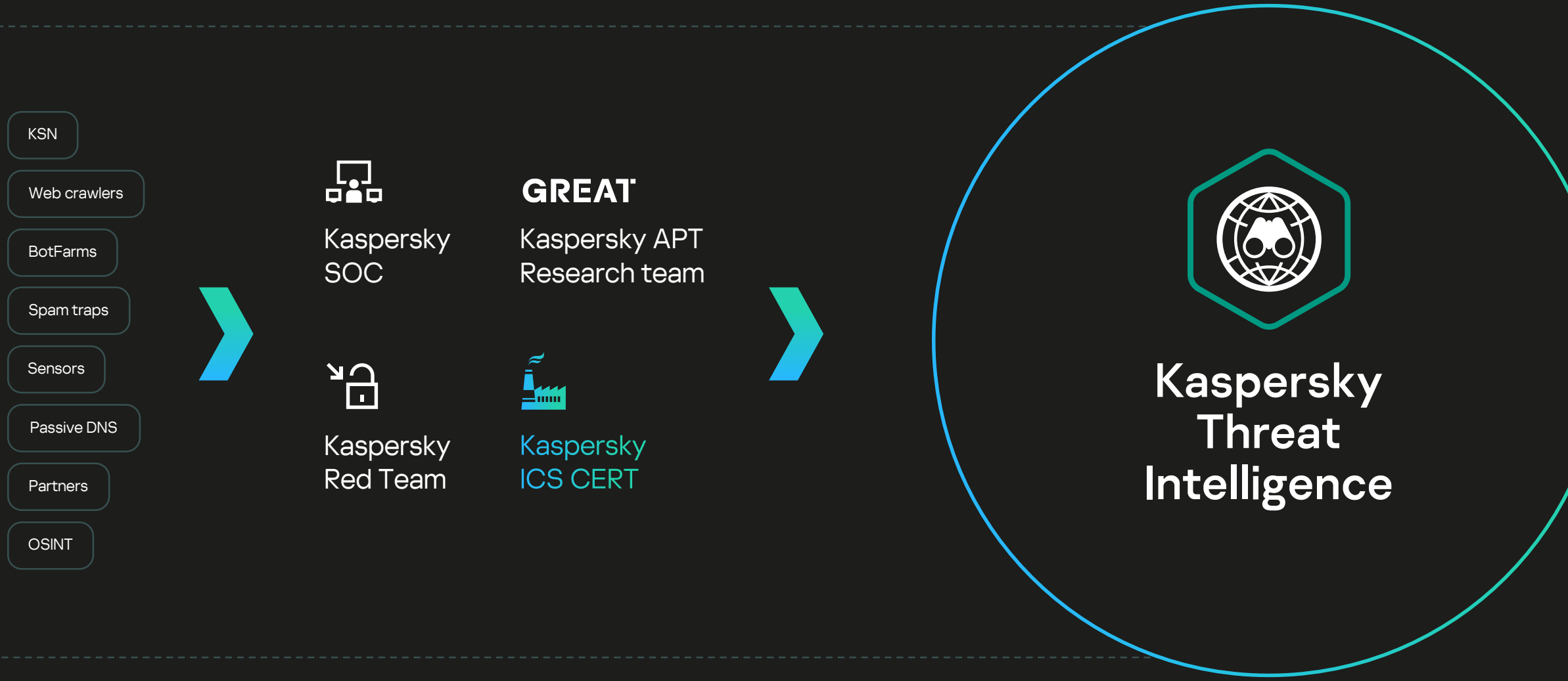
Correlator

Kaspersky Unified Monitoring and Analysis Platform

«Обогащенные» события

Источники
Threat Intelligence

Threat Intelligence — источники



Kaspersky ICS CERT

Обнаружили несколько сотен уязвимостей «нулевого дня» в компонентах АСУ ТП и IIoT

Более 30 экспертов в области исследования угроз и уязвимостей, расследования инцидентов и анализа защищенности АСУ ТП

Статус CVE Numbering Authority (CNA)

Регулярно анализируем статистику и ландшафт угроз промышленной безопасности. Отслеживаем APT-активности

Первый индустриальный CERT в коммерческой организации

Членство в международных организациях:

ITU IEEE Global Platform enisa ISO FIRST Industry IoT Consortium

Проблематика

Специфика АСУ ТП

- Приоритет – надежность и доступность
- Жизненный цикл более 10 лет
- Устаревшее ПО и оборудование
- Сложности обновления
- Плановое обслуживание 1 раз в год
- Удаленная поддержка и обслуживание

Подверженность угрозам

- Геополитические
- Киберпреступники
- Устаревшие угрозы
- Общие ИТ-угрозы
- Инсайдер
- Случайные заражения

Незащищенность

- Не обновленные, снятые с поддержки ОС и ПО
- Мнимая изоляция и воздушный зазор
- Плоские сети
- Устаревшие базы данных угроз
- Неизвестные уязвимости
- Недонастроенные или выключенные средства защиты
- Слабый контроль доступа
- Неучтенные интерфейсы, доступные извне

Kaspersky Industrial Threat Intelligence

Kaspersky Threat Data Feeds

ICS Hashes Data Feed
ICS Vulnerability Data Feed
ICS Vulnerability Data Feed в формате OVAL

Машиночитаемые потоки данных об угрозах и уязвимостях промышленной кибербезопасности

Простые форматы распространения данных (JSON, CSV, OpenIoC, STIX) через HTTPS, TAXII и специализированные методы доставки для интеграции в ИБ-решения

Kaspersky Intelligence Reporting

Industrial Reports на портале Kaspersky Threat Intelligence

Подписка на регулярные публикации об угрозах и уязвимостях промышленной кибербезопасности на веб-портале Kaspersky Threat Intelligence Portal

- Оповещения
- Детальные технические отчеты
- Ежемесячные обзоры
- Статистика и тренды

Kaspersky Ask the Analyst

Ask The Analyst — консультация с экспертом Kaspersky ICS CERT

Позволяет получить индивидуальную консультацию по угрозам и уязвимостям промышленной кибербезопасности, статистике и ландшафту угроз, индустриальным стандартам и пр. от экспертов Kaspersky ICS CERT

Публикации об угрозах и уязвимостях АСУ ТП

Kaspersky Industrial Reports

Регулярные публикации об угрозах и уязвимостях промышленной кибербезопасности от экспертов Kaspersky ICS CERT

- Оповещения
- Ежемесячные обзоры
- Тренды и статистика
- Детальный технический анализ
- Индикаторы компрометации
- Правила для обнаружения
- Инциденты
- Вредоносное ПО
- Уязвимости 0-го дня
- Разбор известных уязвимостей
- APT

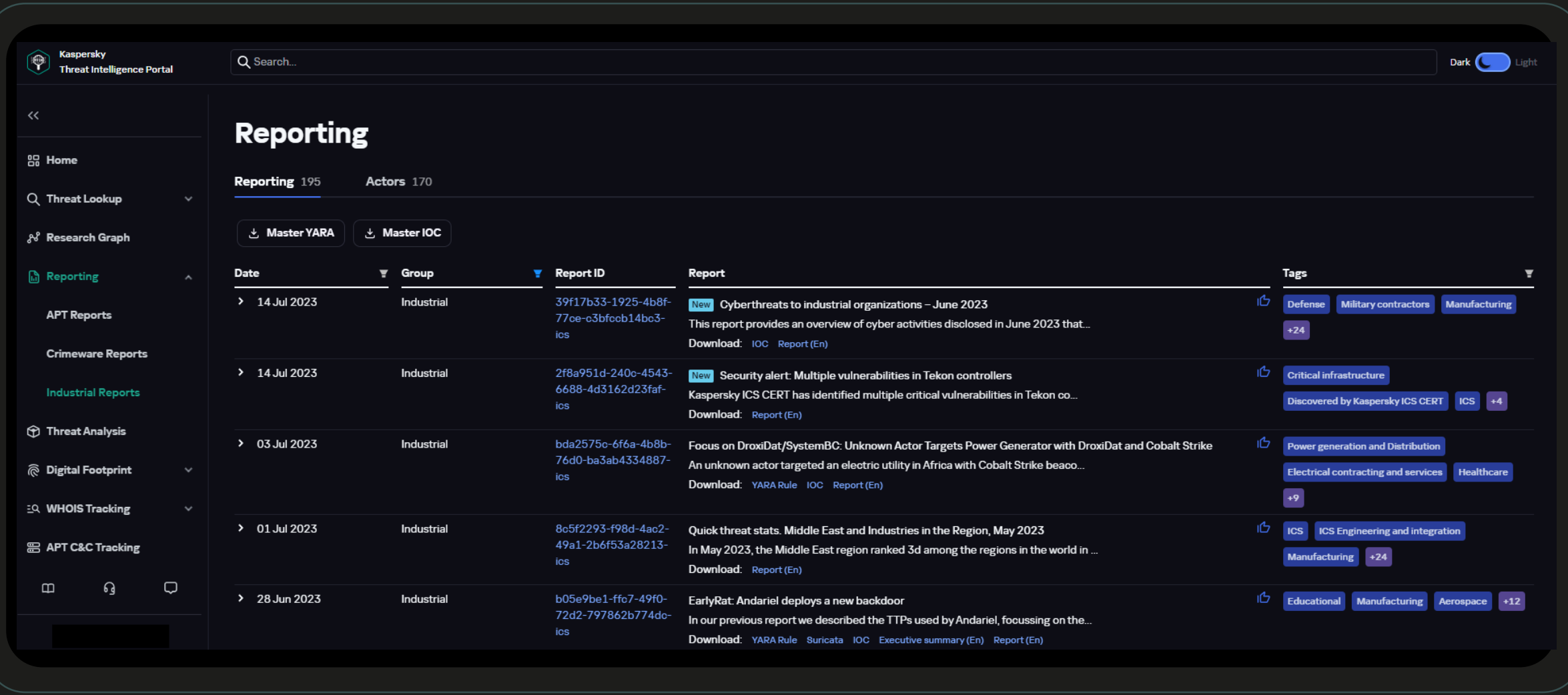
Для получения отчетов достаточно

tip.kaspersky.com

Доступ из любой точки через веб-портал Kaspersky Threat Intelligence Portal

Возможность подключения по API

Веб-портал Kaspersky Threat Intelligence



Быть готовым к угрозам промышленной кибербезопасности вместе с Kaspersky Industrial Reports

Обнаруживать следы присутствия комплексных угроз и масштабных атак вредоносного ПО

Эффективно расследовать инциденты кибербезопасности, реагировать и устранять последствия

Повышать уровень подготовки сотрудников отделов кибербезопасности

Своевременно выявлять наиболее слабые места и точки входа в промышленной инфраструктуре

Выбирать и обосновывать меры по усилению защиты на основе фактологических данных

Выстраивать стратегию кибербезопасности на основе информированных решений

Kaspersky Industrial Reports: Типы отчетов

Отчеты по угрозам, направленным на промышленные предприятия

Отчеты об APT, целевых атаках, массовых заражениях вредоносным ПО и других значимых кампаниях, направленных на промышленные организации с предоставлением обновлений по мере развития ситуации

Обзоры ландшафта и статистики угроз

- Описание значимых изменений ландшафта угроз для АСУТП, критических факторов, влияющих на безопасность АСУТП и подверженность атакам
- Регулярные отчеты по статистике угроз, детектируемых в регионах и индустриях

Ежемесячные обзоры по угрозам

Регулярные отчеты с рассмотрением угроз, атак и инцидентов, относящихся к промышленным организациям, использующим АСУ ТП

Оповещения об угрозах

Ранние оповещения об опасности дают возможность защитить предприятие до выпуска полноценных отчетов об угрозах и атаках

Kaspersky Industrial Reports: Типы отчетов

Отчеты с результатами исследований уязвимостей

Отчеты об уязвимостях нулевого дня в наиболее популярных продуктах и технологиях, используемых в АСУТП, IIoT и инфраструктурах в различных отраслях

Оповещения об уязвимостях нулевого дня

Важные оповещения об уязвимостях для предотвращения эксплуатации еще до публикации официальных исправлений

Аналитика известных уязвимостей

Детальные отчеты по известным уязвимостям с анализом от экспертов «Лаборатории Касперского», включают практические предложения по закрытию уязвимостей и корректируют информацию от вендоров

Отчеты об угрозах для промышленных предприятий

Краткий обзор

- Информация для руководителей

Профиль злоумышленника

Соответствие фреймворкам

- MITRE ATT&CK

Выводы и рекомендации

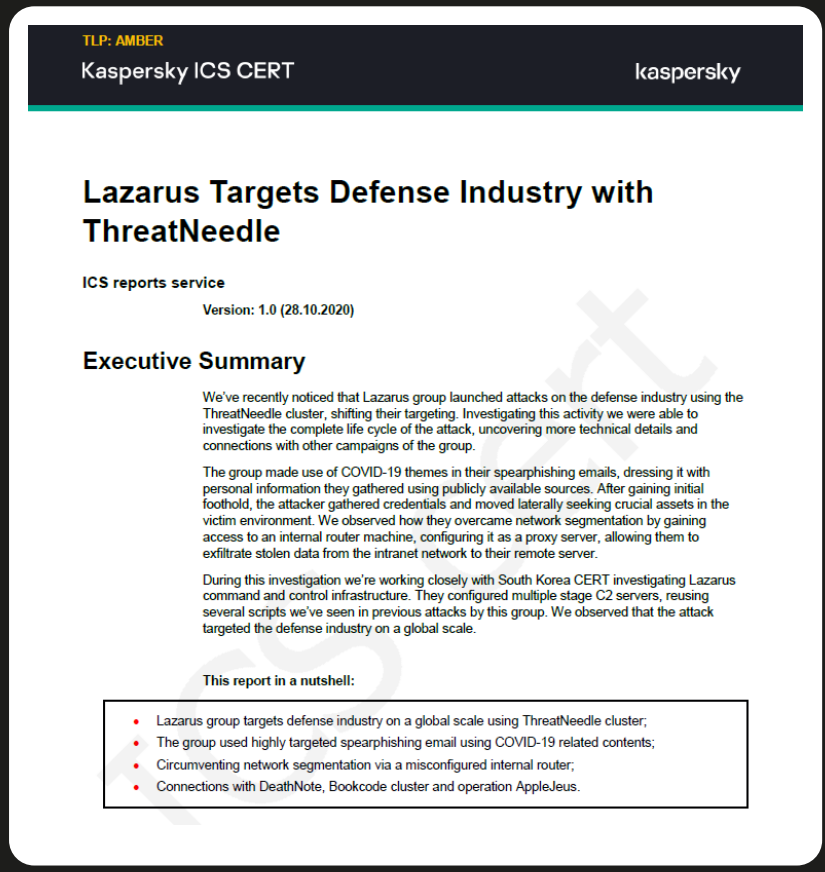
Машиночитаемые данные для обнаружения

- YARA
- IoC

Периодичность: по обнаружению и подтверждению

Детальный технический анализ

- Техники и тактики
- Эксплуатируемые уязвимости
- Атрибуция угрозы
- Анализ утечки данных
- Профиль потерпевшего
- C&C инфраструктура и протоколы
- Инструменты



TLP: AMBER

Kaspersky ICS CERT kaspersky

Lazarus Targets Defense Industry with ThreatNeedle

ICS reports service

Version: 1.0 (28.10.2020)

Executive Summary

We've recently noticed that Lazarus group launched attacks on the defense industry using the ThreatNeedle cluster, shifting their targeting. Investigating this activity we were able to investigate the complete life cycle of the attack, uncovering more technical details and connections with other campaigns of the group.

The group made use of COVID-19 themes in their spearphishing emails, dressing it with personal information they gathered using publicly available sources. After gaining initial foothold, the attacker gathered credentials and moved laterally seeking crucial assets in the victim environment. We observed how they overcame network segmentation by gaining access to an internal router machine, configuring it as a proxy server, allowing them to exfiltrate stolen data from the intranet network to their remote server.

During this investigation we're working closely with South Korea CERT investigating Lazarus command and control infrastructure. They configured multiple stage C2 servers, reusing several scripts we've seen in previous attacks by this group. We observed that the attack targeted the defense industry on a global scale.

This report in a nutshell:

- Lazarus group targets defense industry on a global scale using ThreatNeedle cluster;
- The group used highly targeted spearphishing email using COVID-19 related contents;
- Circumventing network segmentation via a misconfigured internal router;
- Connections with DeathNote, Bookcode cluster and operation AppleJeus.

Отчеты о ландшафте угроз для АСУ ТП

Фокус отчета

- Период
- Регион
- Отрасль

Краткий обзор

- Информация для руководителей

Выводы
и рекомендации

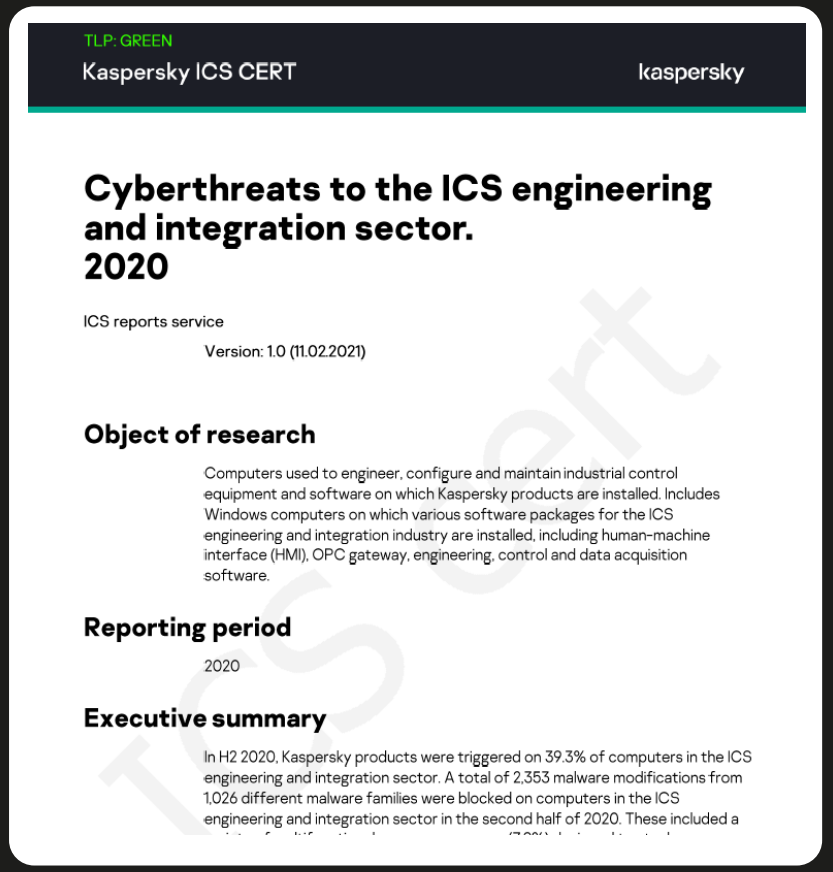
Машиночитаемые данные
для обнаружения

- IoC

Периодичность:
каждые полгода, при значимых изменениях ландшафта

Статистические данные

- Источники угроз
- Типы угроз
- Географическое распределение
- Факторы влияния
- Проблемы безопасности



TLP: GREEN

Kaspersky ICS CERT kaspersky

Cyberthreats to the ICS engineering and integration sector. 2020

ICS reports service

Version: 1.0 (11.02.2021)

Object of research

Computers used to engineer, configure and maintain industrial control equipment and software on which Kaspersky products are installed. Includes Windows computers on which various software packages for the ICS engineering and integration industry are installed, including human-machine interface (HMI), OPC gateway, engineering, control and data acquisition software.

Reporting period

2020

Executive summary

In H2 2020, Kaspersky products were triggered on 39.3% of computers in the ICS engineering and integration sector. A total of 2,353 malware modifications from 1,026 different malware families were blocked on computers in the ICS engineering and integration sector in the second half of 2020. These included a

Отчеты об анализе известных уязвимостей АСУ ТП

Краткий обзор

Информация для руководителей

Рекомендации

- От производителя
- Оценка применимости
- Kaspersky ICS CERT
- Snort / Suricata

Технический анализ

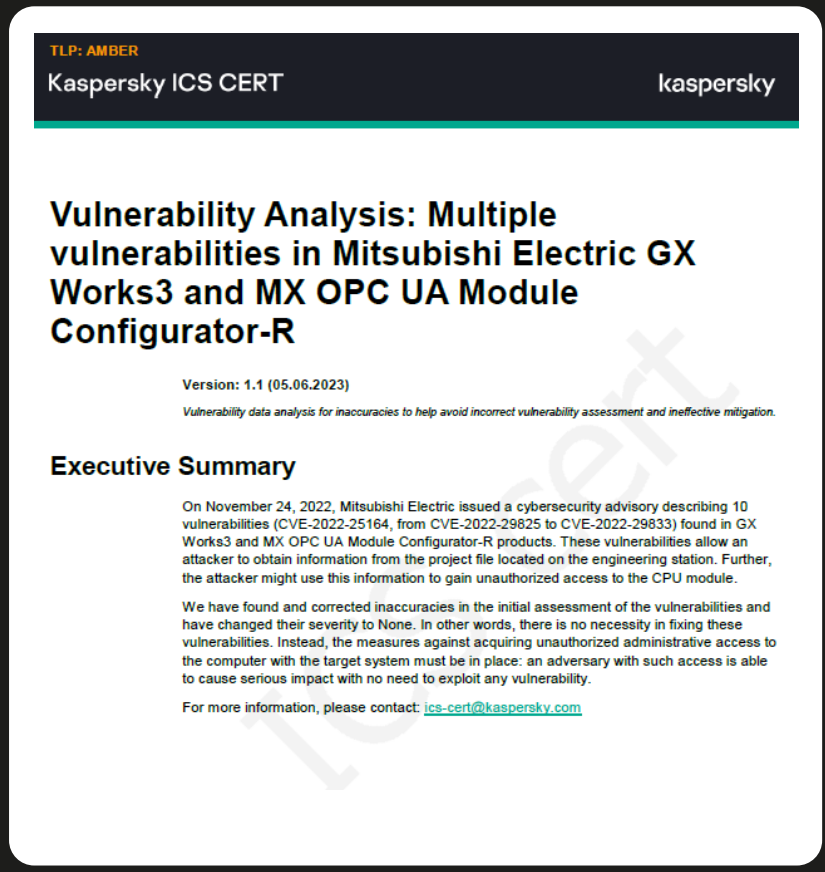
- Продукт
- Уязвимость
- Проверка
- Уязвимые версии

Выводы

- Найденные неточности
- Наша оценка

Периодичность:

каждые 1-2 месяца



TLP: AMBER

Kaspersky ICS CERT kaspersky

Vulnerability Analysis: Multiple vulnerabilities in Mitsubishi Electric GX Works3 and MX OPC UA Module Configurator-R

Version: 1.1 (05.06.2023)

Vulnerability data analysis for inaccuracies to help avoid incorrect vulnerability assessment and ineffective mitigation.

Executive Summary

On November 24, 2022, Mitsubishi Electric issued a cybersecurity advisory describing 10 vulnerabilities (CVE-2022-25164, from CVE-2022-29825 to CVE-2022-29833) found in GX Works3 and MX OPC UA Module Configurator-R products. These vulnerabilities allow an attacker to obtain information from the project file located on the engineering station. Further, the attacker might use this information to gain unauthorized access to the CPU module.

We have found and corrected inaccuracies in the initial assessment of the vulnerabilities and have changed their severity to None. In other words, there is no necessity in fixing these vulnerabilities. Instead, the measures against acquiring unauthorized administrative access to the computer with the target system must be in place: an adversary with such access is able to cause serious impact with no need to exploit any vulnerability.

For more information, please contact: ics-cert@kaspersky.com

Предупреждения об уязвимости нулевого дня

Описание уязвимости

CVE | CWE

Серьезность

CVSS бал | CVSS вектор

Условия эксплуатации

и потенциальные последствия

План устранения уязвимости

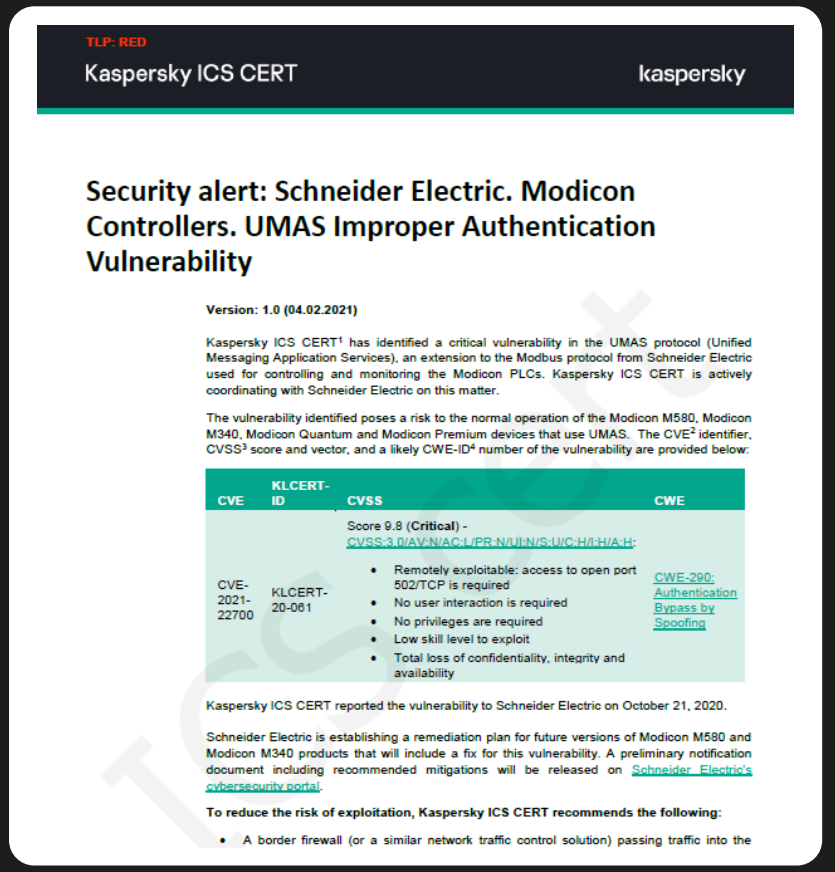
производителем уязвимого продукта

Рекомендации

по снижению риска эксплуатации

Периодичность:

незамедлительно и в соответствии с политикой ответственного разглашения



TLP: RED

Kaspersky ICS CERT kaspersky

Security alert: Schneider Electric. Modicon Controllers. UMAS Improper Authentication Vulnerability

Version: 1.0 (04.02.2021)

Kaspersky ICS CERT[1] has identified a critical vulnerability in the UMAS protocol (Unified Messaging Application Services), an extension to the Modbus protocol from Schneider Electric used for controlling and monitoring the Modicon PLCs. Kaspersky ICS CERT is actively coordinating with Schneider Electric on this matter.

The vulnerability identified poses a risk to the normal operation of the Modicon M580, Modicon M340, Modicon Quantum and Modicon Premium devices that use UMAS. The CVE[2] identifier, CVSS[3] score and vector, and a likely CWE-ID[4] number of the vulnerability are provided below:

CVE	KLCERT-ID	CVSS	CWE
CVE-2021-22700	KLCERT-20-061	Score 9.8 (**Critical**) - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H: • Remotely exploitable: access to open port 502/TCP is required • No user interaction is required • No privileges are required • Low skill level to exploit • Total loss of confidentiality, integrity and availability	CWE-290: Authentication Bypass by Spoofing

Kaspersky ICS CERT reported the vulnerability to Schneider Electric on October 21, 2020.

Schneider Electric is establishing a remediation plan for future versions of Modicon M580 and Modicon M340 products that will include a fix for this vulnerability. A preliminary notification document including recommended mitigations will be released on Schneider Electric's cybersecurity portal.

To reduce the risk of exploitation, Kaspersky ICS CERT recommends the following:

- A border firewall (or a similar network traffic control solution) passing traffic into the

Получать ценную информацию просто

Быстрое оформление подписки

1 год

3 года

Индивидуальный сертификат

Отдельная учетная запись для каждого сотрудника

Пробный период использования по запросу

Спроси Аналитика

Kaspersky Ask the Analyst

Kaspersky Ask the Analyst

Всегда на связи с лучшими экспертами

Унифицированная подписка: запрос-ответ

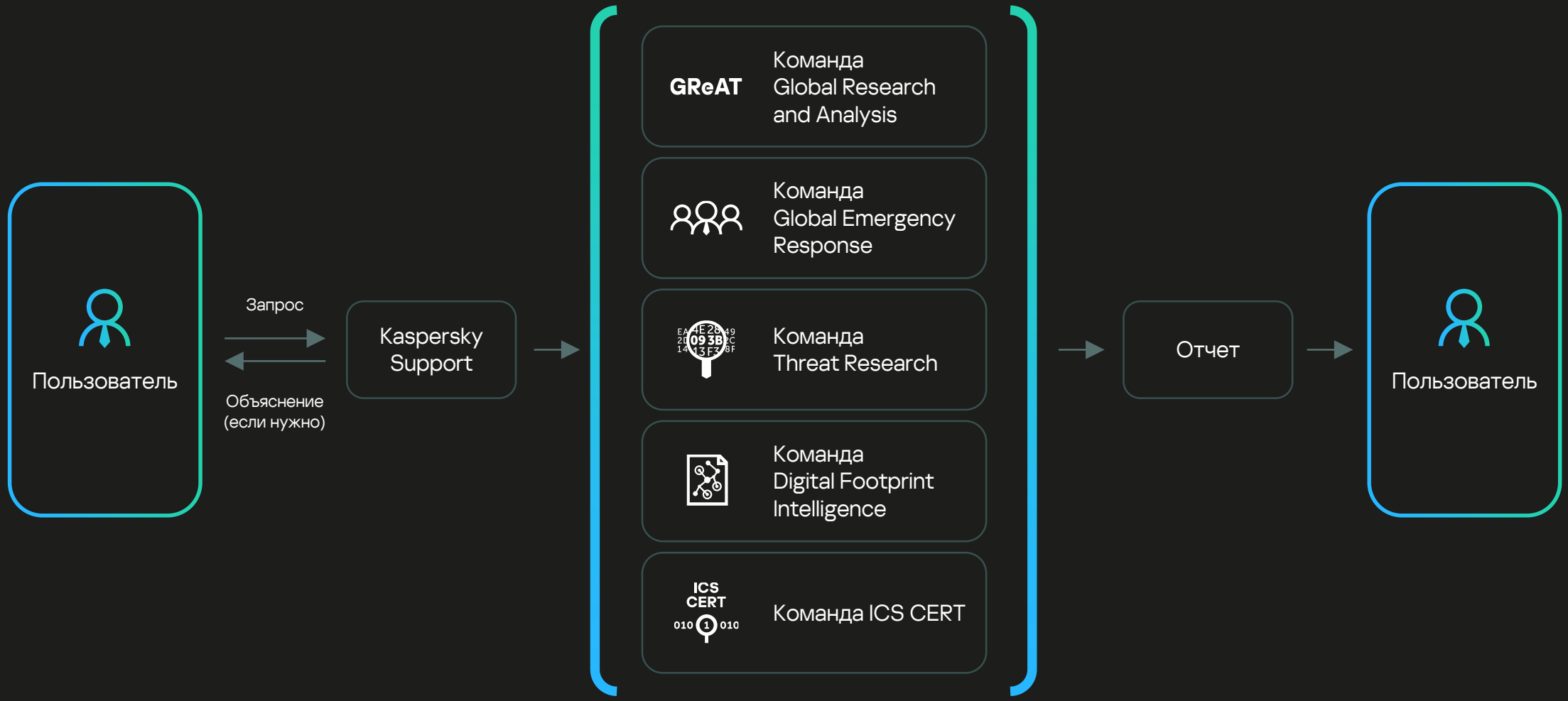
Разъяснения по поводу выпущенных отчетов

Помощь с анализом АСУ ТП-зловредов

Дополнительная информация по поводу уязвимостей АСУ ТП

Разъяснения по нормативно-регуляторной базе и стандартам

Как это работает



Потоки данных

Kaspersky ICS Threat Data Feeds

Kaspersky ICS Hashes Data Feed

Kaspersky ICS Vulnerability Data Feed

Kaspersky ICS Vulnerability Data Feed in OVAL format

Поток данных об угрозах для АСУ ТП

Kaspersky ICS Hashes Data Feed

Простой и понятный JSON формат

Возможность использования других форматов представления и передачи данных

- STIX
- TAXII

Интеграция напрямую и посредством Kaspersky CyberTrace — специализированной платформы агрегации и корреляции большого объема данных

Интеграции со сторонними решениями по кибербезопасности

- SIEM
- Защита конечных узлов
- Портативные сканеры
- Антивирусная защита
- Управление приложениями
- EDR
- Обнаружение вторжений
- Сетевые экраны
- SOAR
- XDR
- MDR
- TI платформы

Kaspersky ICS Hashes Data Feed: Пример записи


```
{
"id": "Идентификатор записи. (пример: 1204640879)"
"MD5": "MD5 хэш вредоносного объекта. (пример: 202cb962ac90…b4b0752d234b70)"
"SHA1": "SHA-1 хэш вредоносного объекта. (пример: d471FEC3726b7b…24fcc457b2)"
"SHA256": "SHA-256 хэш вредоносного объекта. (пример: a665459422f9d…86f7f7a27ae3)"
"first_seen": "Дата и время первого детекта (UTC). (пример: 08.04.2014 16:45)"
"last_seen": "Дата и время последнего детекта (UTC). (пример: 12.02.2015 13:56)"
"popularity": "Популярность записи на основе количества пользователей, у которых был обнаружен вредоносный объект. 5 – высокая
популярность, 1 – низкая популярность. (пример: 3)"
"threat": "Имя угрозы (класс, платформа, семейство) согласно системе классификации Лаборатории Касперского. (пример: Net-Worm.Win32.Kido)"
"geo": "Топ 10 стран, в которых пользователи Лаборатории Касперского наиболее часто встречались. (пример: EN,FR,RU,GE,CH)"
"file_type": "Формат вредоносного объекта. (пример: DLL)"
"file_size": "Размер вредоносного объекта. (пример: 486)"
"file_names": "Топ 10 имен файлов вредоносного объекта. (пример: kaspersky_reset_trial_5.1.0.29.exe, krt_5.1.0.29.exe, krt v5.1.0.29.exe,
kaspersky_reset_trial_5.1.0.29_yasdl.com.exe, krt v5.1.0.29.kuyhaa.exe, krt 5.1.0.29.exe, krt_5.1.0.29_softgozar.com.exe, trial reset.exe,
zolsky_kaspersky2017.exe, krt_5.1.0.29.rar)"
“IP":"Топ 10 IP-адресов, с которых объект был загружен. (пример: 95.110.219.123, 95.110.240.37, 213.136.64.165)"
"urls":[Начало массива URL-адресов, с которых вредоносный объект был загружен.
        {
        "url": "URL-адрес, с которого вредоносный объект был загружен. (пример: lloadbom.ee7pp.pro/15022018)"
        }
]
}
```

Kaspersky ICS Hashes Data Feed: Условия получения

Получить поток данных угроз для АСУ ТП

Быстрое оформление подписки

1 год | 3 года

Безопасная доставка по индивидуальному сертификату через HTTPS

Возможность тестового использования по запросу

Помощь выделенной команды высококвалифицированных инженеров по интеграции

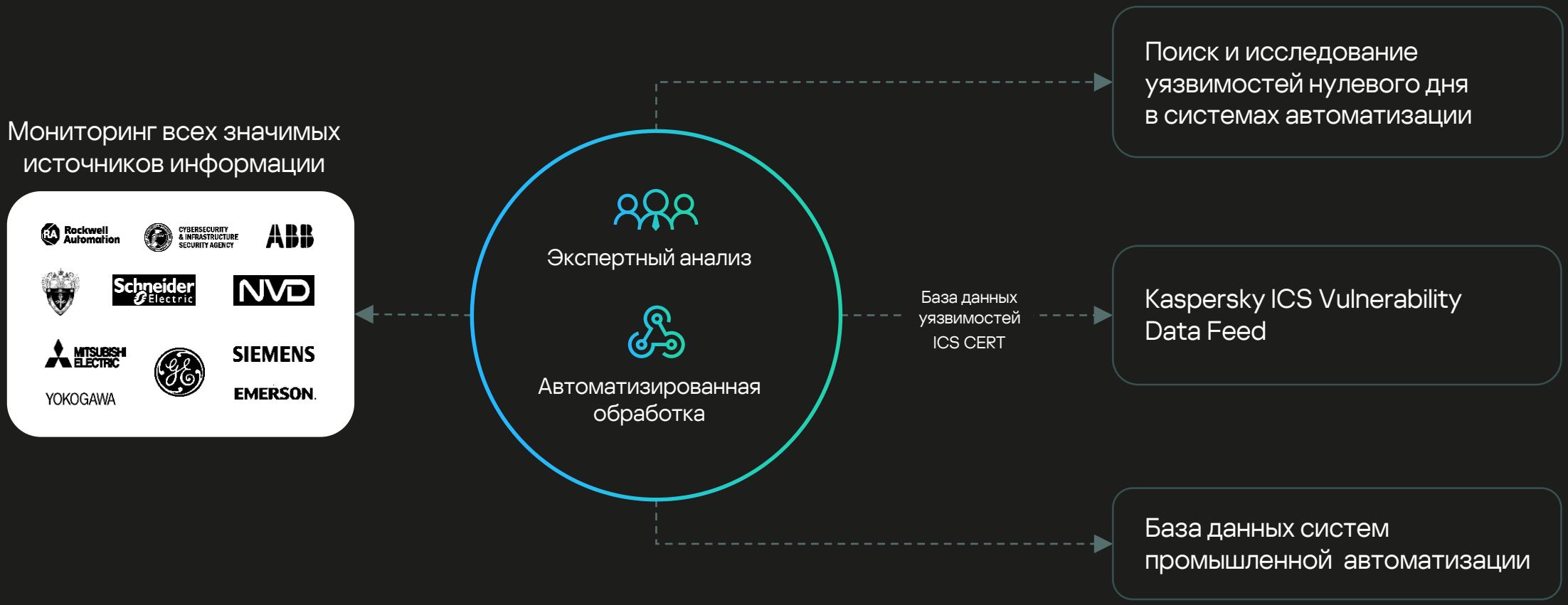
Исчерпывающая документация

Поток данных об уязвимостях АСУ ТП

Kaspersky ICS Vulnerability Data Feed

Kaspersky ICS Vulnerability Data Feed: Процесс сбора и обработки информации

Анализ от экспертов Kaspersky ICS CERT



Kaspersky ICS Vulnerability Data Feed

Позволяет

Точно выявить уязвимость

Адекватно оценить серьезность

Приоритизировать

Выбрать эффективные меры по устранению

Содержит

детальную информацию об уязвимости и подверженных ей продуктах

- CVE
- Ссылки на первоисточники
- Описание уязвимости
- Уязвимые версии
- Рекомендации вендора
- CVSS вектор
- Рекомендации Kaspersky ICS CERT
- CPE имя уязвимых версий
- CVSS балл

Проверен

на наличие ошибок, дополнен важной информацией

Учитывает

снятые с поддержки продукты

Kaspersky ICS Vulnerability Data Feed: Условия получения

Получить поток данных уязвимостей АСУ ТП

Быстрое оформление подписки

1 год

3 года

Безопасная доставка по индивидуальному сертификату через HTTPS

Пилотирование

Помощь выделенной команды высококвалифицированных инженеров по интеграции

Исчерпывающая документация

Поток данных об уязвимостях АСУ ТП в формате OVAL

Kaspersky ICS Vulnerability Data Feed in OVAL format

Open Vulnerability and Assessment Language — открытый язык описания и оценки уязвимостей, международный стандарт по информационной безопасности

Стандартизирует формат описания информации об уязвимости, правила анализа системы на наличие уязвимостей и результат

Используется в решениях по кибербезопасности и источниках данных об уязвимостях

Является частью стандарта SCAP (Security Content Automation Protocol)

Kaspersky ICS Vulnerability Data Feed in OVAL формат

Позволяет

Автоматизировать выявление уязвимостей

Адекватно оценивать серьезность и приоритизировать уязвимости

Получать список уязвимых продуктов и их уязвимостей

Выбирать эффективные меры по устранению

Содержит

всю необходимую информацию для автоматического выявления уязвимостей

- CVE
- CVSS балл
- CVSS вектор
- Описание уязвимости
- Уязвимые версии
- Записи реестра
- Рекомендации по закрытию

Kaspersky ICS Hashes Data Feed: Условия получения

Получить поток данных уязвимостей АСУ ТП

Быстрое оформление подписки

1 год

3 года

Безопасная доставка по индивидуальному сертификату через HTTPS

Пилотирование

Помощь выделенной команды высококвалифицированных инженеров по интеграции

Исчерпывающая документация

Наши преимущества

Уникальные данные
от 1 000 000 ICS Endpoints
через наше облако KSN

Выделенная команда
Threat Research и Security
Analysis

Выделенная команда Vulnerability Research с большим числом найденных Zero-Days

Мы участвуем
в создании ключевых
индустриальных стандартов

Налаженные каналы
взаимодействия
с вендорами оборудования АСУ ТП

Ссылки

Интересный репорт по теме:

https://ics-cert.kaspersky.com/vulnerability-analysis-schneider-electric-modicon-controllers-and-ecostruxure-software-remote-code-execution-vulnerability-you-should-not-care-about/

Наши недавние вебинары:

Vulnerability Identification with OVAL

https://www.brighttalk.com/webcast/15591/589992

Safeguarding the future: cybersecurity risks in alternative energy sources

https://www.brighttalk.com/webcast/15591/590762

Ссылки для заказа пилотов по нашим услугам:

https://ics-cert.kaspersky.com/industrial-oval-data-feed/

https://ics-cert.kaspersky.ru/services/

Спасибо!

kaspersky