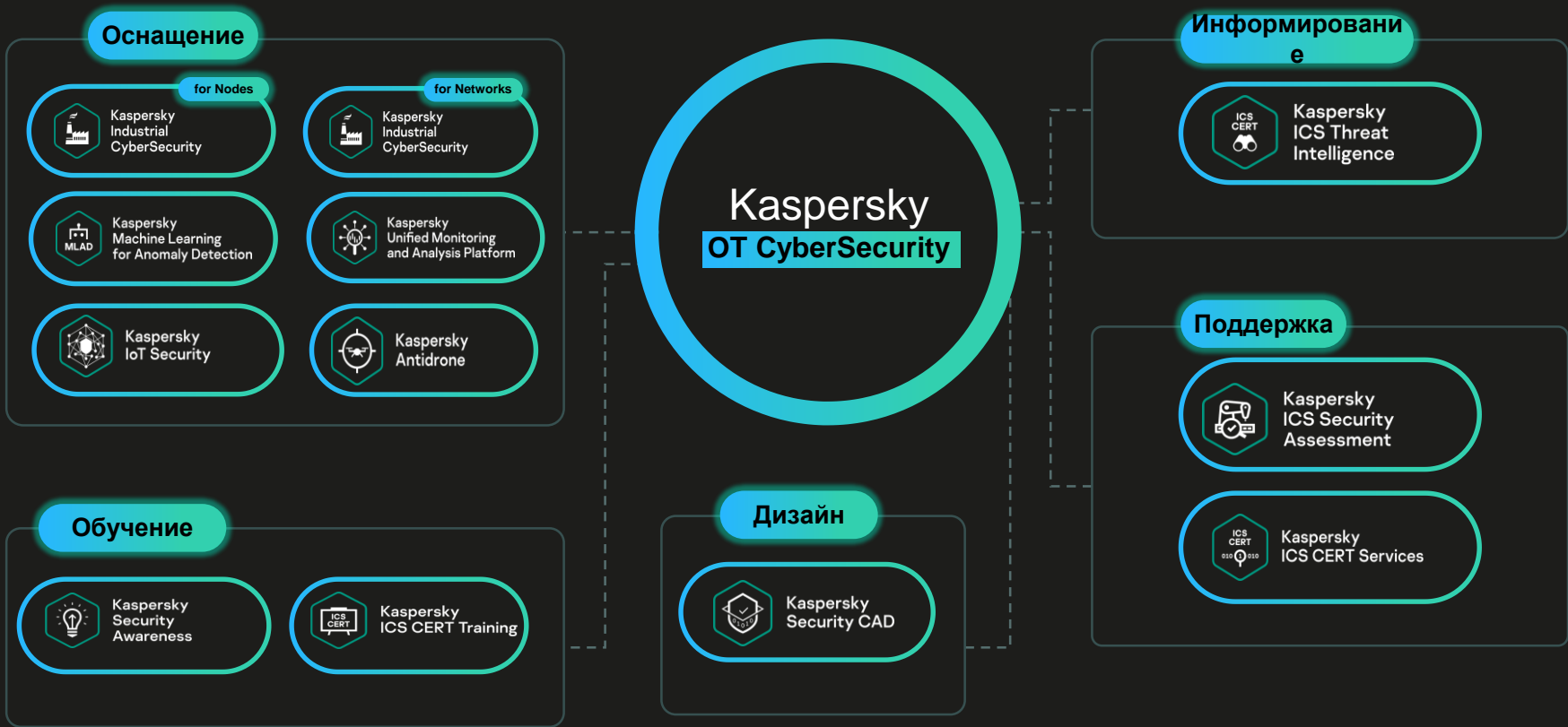


Оперативная помощь по информационной безопасности АСУ ТП

kaspersky

go.kaspersky.com/ru-ics-kit

Экосистема решений для обеспечения безопасности ОТ



45 000+

Промышленных АРМ/серверов
под защитой KICS for Nodes

350+

Промышленных сетей под защитой
KICS for Networks

260

Количество проектов в 2021

300+

Клиентов по всему миру

Что нового?



РОСЭНЕРГОАТОМ
РОСАТОМ

Лаборатория Касперского внесла вклад в обеспечение безопасности Ленинградской АЭС



Усть-Каменогорская ГЭС используется KICS для обеспечения ИБ АСУ ТП



ЗАРУБЕЖНЕФТЬ
ДОБЫЧА ХАРЬЯГА
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

Эмерсон и Лаборатория Касперского объединили усилия для киберзащиты «ЗАРУБЕЖНЕФТЬ-добыча Харьяга»

KAMAZ

Промышленная инфраструктура завода «КАМАЗ» под защитой «Лаборатории Касперского»



YOKOGAWA



EMERSON

PcVue Solutions

Лаборатория Касперского развивает сотрудничество с АСУ ТП вендорами

ЭКРА SIEMENS

Современные ИБ-реалии

1.

Уход зарубежных вендоров АСУ ТП и ИБ с российского рынка

2.

Низкий уровень осведомленности персонала об угрозах ИБ в АСУ ТП

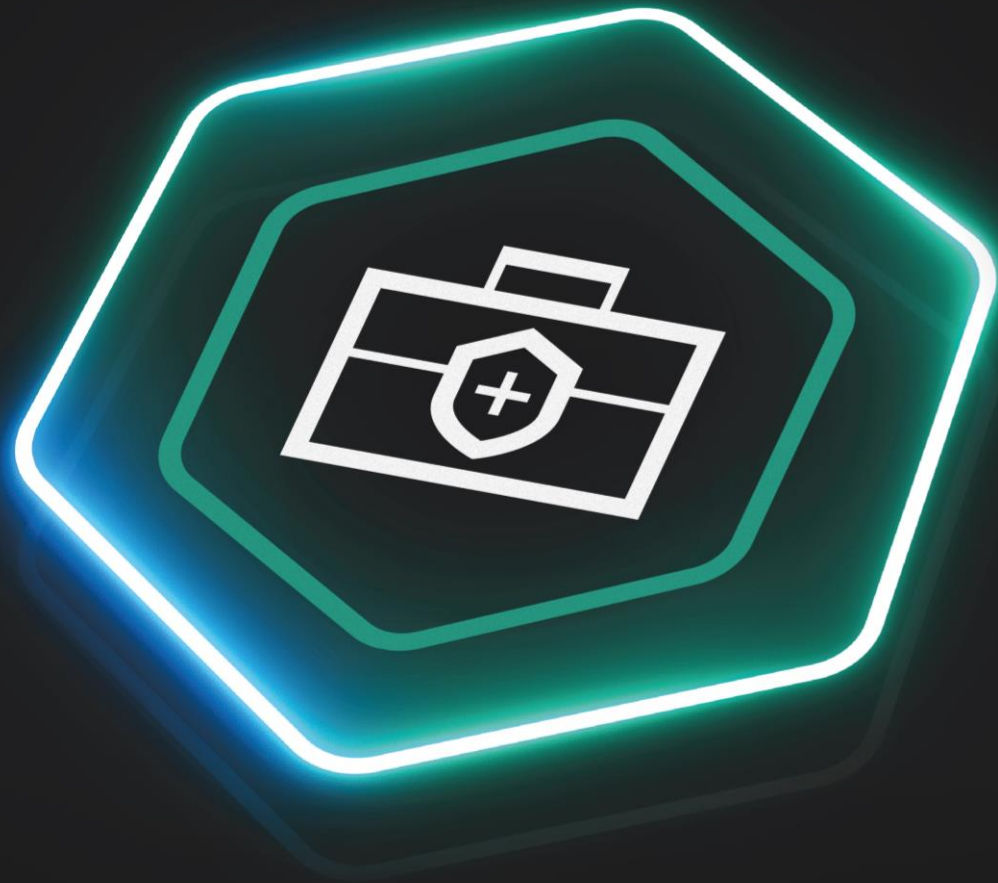
3.

Повышенный уровень киберагрессии в отношении российских промышленных предприятий

4.

Ослабление уровня защищенности корпоративной инфраструктуры

Kaspersky Industrial Emergency Kit



kaspersky

План оперативной помощи в рамках сервиса Kaspersky Industrial Emergency Kit

7

Экспресс-оценка защищенности и отчетность



Экспресс-аудит
инфраструктуры



Персонализированный
отчет об угрозах
на организацию



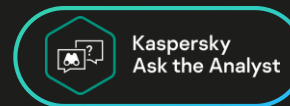
Аналитические отчеты
об угрозах на промышленный
сектор

Создание цифровой модели системы ИБ

Обследование и подготовка данных
для загрузки в Kaspersky Security CAD



Паспортизация
и разработка модели угроз
и нарушителей



Результат

Повышение осведомленности



Обучение по программе «Основы информационной безопасности АСУ ТП»

Консультация с экспертом
по результату проведенной
работы, интерпретация
отчетов и предоставление
рекомендаций

Старт работ

1 месяц

2 месяц

3 месяц

Kaspersky Industrial
Emergency Kit

Kaspersky ICS Express Audit



kaspersky

READY

Plug and play



Time-critical planning



Отчет об аудите

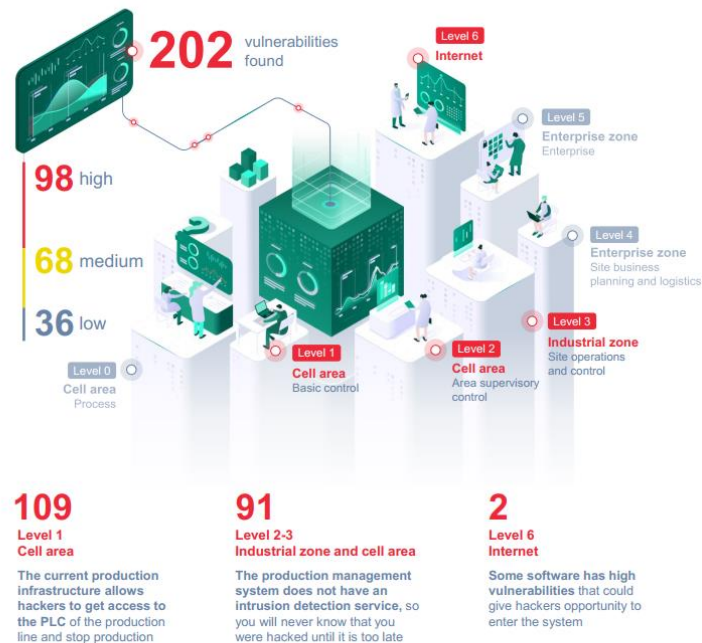
1. Executive summary (одностраничный обзор для топ-менеджмента)

2. Описание системы (результат работы модуля инвентаризации KICS for Networks)

3. Описание обнаруженных уязвимостей и угроз

4. Рекомендации по повышению уровня защищенности

EXECUTIVE SUMMARY



Summary of recommendations



Conduct a deep security audit to detect hidden vulnerabilities



Install software for monitoring changes in the production management system and filtering suspicious traffic



Implement a control policy for industrial network access by defining distinct areas in the network architecture

Kaspersky Industrial
Emergency Kit

Kaspersky Digital Footprint Intelligence



kaspersky



Цель

Определение поверхности потенциальных компьютерных атак и получение информации о готовящихся или уже реализуемых атаках на организацию



Исследуемые ресурсы

Главный офис, локальные офисы и подразделения, дочерние общества



Сервис

Только пассивные методы анализа

- Исключение активного взаимодействия с инфраструктурой

Результат

- Отчет с результатами анализа и описанием технических деталей
- Все полученные данные в формате Excel



Инвентаризация периметра сети¹

- Доступные сервисы
- Выявление уязвимостей
- Анализ эксплойтов



Интернет, даркнет и глубокая сеть

- Активность киберпреступников
- Утечки информации и учетных данных
- Инсайдеры
- Поведение сотрудников в социальных сетях



База знаний Kaspersky

- Анализ экземпляров вредоносных программ
- Отслеживание ботнетов и фишинга
- Sinkhole-серверы и серверы с ВПО
- Аналитические отчеты об АРТ-угрозах
- Потоки данных об угрозах

¹ Включая облачные сервисы, указанные заказчиком

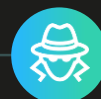


Kaspersky Digital Footprint Intelligence



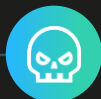
Угрозы, связанные с уязвимостями на сетевом периметре

- Ошибки конфигурации сетевых сервисов
- Идентификация уязвимостей
- Скомпрометированные ресурсы



Угрозы со стороны киберпреступников

- Мошеннические схемы и планы
- Украденные кредитные карты и скомпрометированные аккаунты
- Инсайдерская активность



Анализ активности вредоносного ПО

- Фишинговые атаки
- Активность ботсетей
- Таргетированные атаки
- АРТ-кампании



Анализ утечек данных

- Корпоративные документы в публичном доступе
- Информация, публикуемая в социальных сетях
- Скомпрометированные учетные записи

Ваши данные

- IP адреса
- Доменные имена
- Организационная структура
- Ключевые слова



Исследование
сетевого
периметра



Анализ
активности
вредоносного
ПО и угроз со
стороны
киберпреступ
ников



Kaspersky
Knowledge
Base

Аналитические
отчеты

Уведомления
об угрозах

Real-time поиск в базах
знаний Kaspersky и
darknet ресурсах

Kaspersky Industrial
Emergency Kit

Kaspersky Security CAD



kaspersky

**Комплексное цифровое
представление объектов
защиты и системы ИБ**

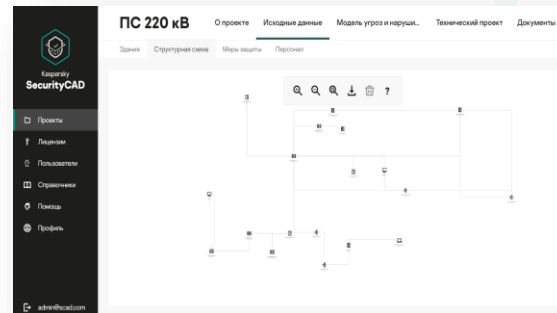
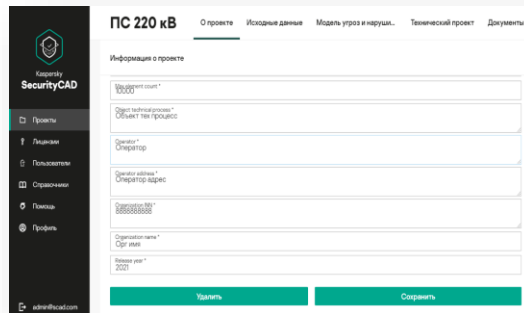
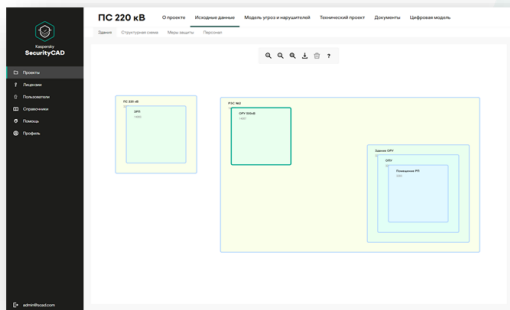
**Единая справочная платформа
по предприятию и его системам
ИТ, ОТ, ИБ**



**Автоматизирование
моделирование угроз
и мер защиты**

**Автоматическое
документирование
по ГОСТ**

Паспортизация объектов (здесь и сейчас)



Сбор данных
из разных
источников

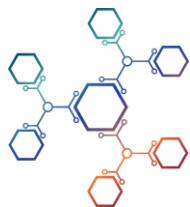
Преобразование
и систематизация данных
в машиночитаемый формат

Структурирование информации
в виде модели объекта
на базе заданных ЛК правил

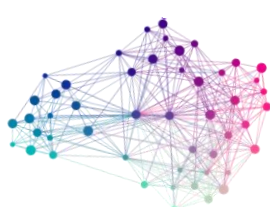
Цифровая модель
в интерфейсе
пользователя

Разработка модели угроз и проектных решений (сразу или при необходимости)

20



Модель объекта



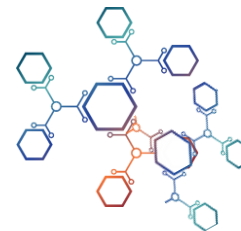
Расчёт угроз

ИИ ведётся перебор техник и тактик из методики ФСТЭК, с учётом особенностей объектов и их свойств



Расчёт мер защиты

Для сформированных актуальных угроз, ИИ выбираются оптимальные меры, для полного выполнения 187 ФЗ



Модель спроектированного объекта



**Документ
«Модель угроз
и нарушителей»**

Проектные документы:

- пояснительная записка,
- структурная схема ИБ,
- спецификация

Kaspersky Industrial
Emergency Kit

Kaspersky ICS Threat Intelligence

Подписочный сервис с доступом
к регулярным отчетам через веб-
портал

kaspersky



Kaspersky ICS CERT

Первый индустриальный CERT в коммерческой организации

30+ экспертов в области исследовании угроз ICS, реагирования на инциденты и анализа безопасности

Имеем статус [CVE Numbering Authority \(CNA\)](#) с правом регистрации CVE IDs для уязвимостей

Официально [авторизованы](#) использовать наименование CERT от Carnegie Mellon University

Обнаружили значительное число новых (zero-day) уязвимостей в области ICS и IIoT

Являемся членами многих международных организаций





Отчеты по конкретным актуальным угрозам направленным на АСУ ТП



Регулярные отчеты по угрозам АСУ ТП



Обзоры ландшафта угроз



Ранние оповещения об угрозах



Результаты глубоких исследований уязвимости продуктов и технологий



Отчеты с анализом известных уязвимостей



(Уже скоро) Аналитика по безопасности конкретных продуктов



Оповещения об уязвимостях нулевого дня

ICS Reporting на Threat Intelligence Portal: Пример

Kaspersky Threat Intelligence Portal

- Home
- Threat Lookup
- Research Graph
- Reporting
 - APT Reports
 - Crimeware Reports
 - ICS Reports**
- Threat Analysis
- Digital Footprint
- WHOIS Tracking
- APT C&C Tracking
- Data feeds
- What's New and Upcoming
- News

Reporting 147 Actors 81

Master YARA Master IOC

Date	Group	Report
28 Mar 2022	ICS	Vulnerability Analysis: Schneider Electric Modicon M340 and M580. Denial-of-service through specially crafted project file Four denial-of-service vulnerabilities were found in the Schneider Electric Mod... Download: Report (En)
23 Mar 2022	ICS	ISaPWN – research on the security of ISaGRAF Runtime In early 2020, Kaspersky ICS CERT found nine vulnerabilities in the ISaGRAF Runt... Download: Executive summary (En) Report (En)
10 Mar 2022	ICS	Cyberthreats to industrial organizations – February 2022 This report provides an overview of cyber activities disclosed in February 2022 ... Download: IOC Report (En)
22 Feb 2022	ICS	Vulnerability Analysis KLCERT-18-104: Siemens SIMATIC/SIPLUS S7-1500 CPUs. Disclosure of in "Foreshadow-NG") Three vulnerabilities leading to information leakage exist in Intel microprocess... Download: Report (En)
16 Feb 2022	ICS	Cyberthreats to industrial organizations – January 2022 This report provides an overview of cyber activities disclosed in January 2022 L... Download: IOC Report (En)
14 Feb 2022	ICS	PryingKomodo leverages Exchange vulnerabilities to deploy ShadowPad against building automation systems In mid-October 2021, we discovered an active ShadowPad backdoor that affected a ... Download: YARA Rule IOC Executive summary (En) Report (En)
3 Feb 2022	ICS	Advisory KLCERT-19-158: Emerson PACSystems RX3i CPL410 CPUs. VxWorks RTOS. Denial of Service and remote code execution via TCP "Urgent" pointer state confusion ***UPD: Suricata rule has been added as a separate file*** CVE-2019-12261. CVSS... Download: Suricata Report (En)

Типы отчетов

- Отчеты Vulnerability Analysis
- Отчеты Vulnerability Research
- Отчеты по Threat landscape
- Отчеты по угрозам APT
- Рекомендации по уязвимостям
- ...

Defense Energy Manufacturing +19

Logistics Manufacturing Telecommunications +4

Advisory Emerson ICS +12

- Threat actor profiles
- Mapping to ATT&CK
- Executive summary
 - C-level oriented information
- Deep technical analysis
 - Attack methods
 - Exploits used
 - Malware description
 - C&C infrastructure and protocols description
 - Victim analysis
 - Data exfiltration analysis
 - Attribution
- Conclusions and recommendations
- Indicators of Compromise and YARA rules
- Periodicity: Immediately after discovery

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.

Уведомления о 0-day

TLP: RED
Kaspersky ICS CERT kaspersky

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

Version: 1.0 (04.02.2021)

Kaspersky ICS CERT¹ 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 CVE² identifier, CVSS³ score and vector, and a likely CWE-ID⁴ number of the vulnerability are provided below:

CVE	KLCERT-ID	CVSS	CWE
		Score 9.8 (Critical) - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
CVE-2021-22700	KLCERT-20-001	<ul style="list-style-type: none">Remotely exploitable: access to open port 502/TCP is requiredNo user interaction is requiredNo privileges are requiredLow skill level to exploitTotal 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 device's network segment should be configured to allow traffic to port 502/TCP from authorized parties only.

- Vulnerability description
- CVSS score and vector
- Attack conditions and potential impact
- Vendor's plan
- Workaround recommendations
- Periodicity: ASAP according to Responsible Disclosure Policy

Kaspersky Industrial
Emergency Kit

Kaspersky ICS CERT Training

Модуль по безопасности АСУ ТП
на платформе Automated
Security Awareness (ASAP)

kaspersky



Kaspersky ICS CERT

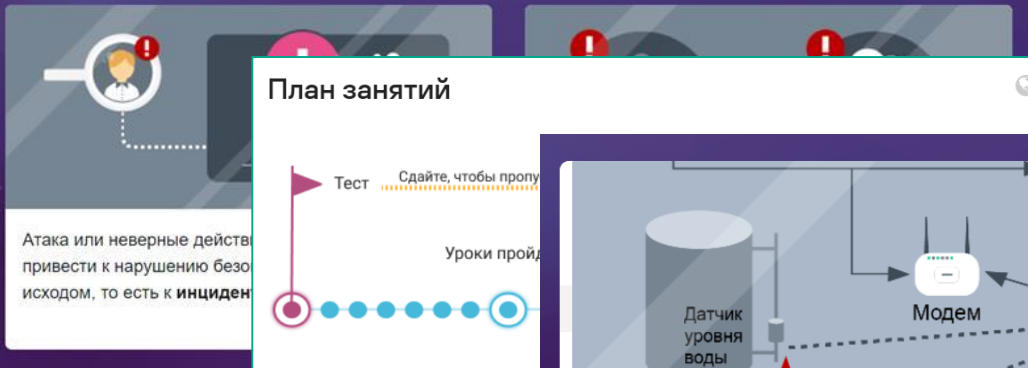
Automated Security Awareness Platform

Платформа включает курсы по всем ключевым темам кибербезопасности для сотрудников разного уровня, включая тематический модуль по индустриальной (АСУТП) кибербезопасности



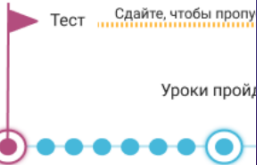
- Электронная почта
- Пароли и учетные записи
- Веб-сайты и Интернет
- Социальные сети и мессенджеры
- Безопасность ПК
- Безопасность мобильных устройств
- Защита конфиденциальных данных
- GDPR
- Кибербезопасность промышленных систем
- Безопасность банковских карт и PCI DSS

ИНЦИДЕНТ И ЕГО ПОСЛЕДСТВИЯ



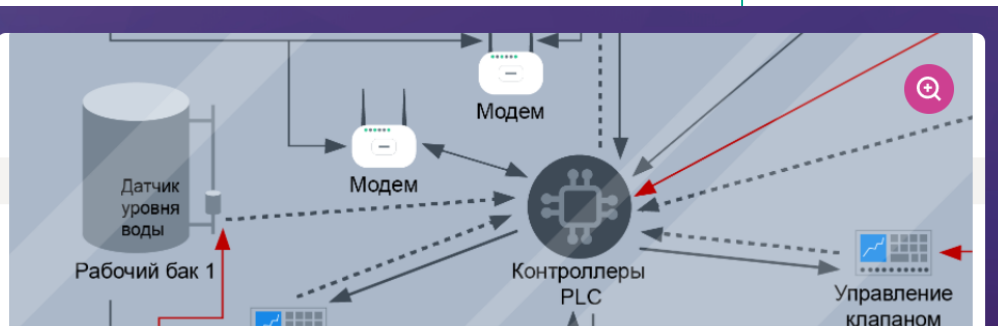
План занятий

Доступные языки



Урок

- Почему процесс организации...
- Взаимодействие инженерных систем
- Мониторинг в АСУ ТП
- Почему в защите АСУ ТП...
- Как обеспечить безопасность...
- Особенности обновления...
- Взаимодействие систем...



Рассмотрим пример возникновения уязвимости промышленной системы из-за неправильного администрирования. Взгляните на схему сети НПЗ на изображении. Невооруженным взглядом заметно, что в структуре сети и предприятия происходит беспорядок. Почему так вышло?

Kaspersky Ask the Analyst





APT and
Crimeware



Malware
Analysis



ICS Related
Requests

разъяснения по поводу
выпущенных отчетов

дополнительная
информация по поводу
уязвимостей АСУТП

помощь с анализом
АСУТП-зловредов

разъяснения по
нормативно-
регуляторной базе
и стандартам



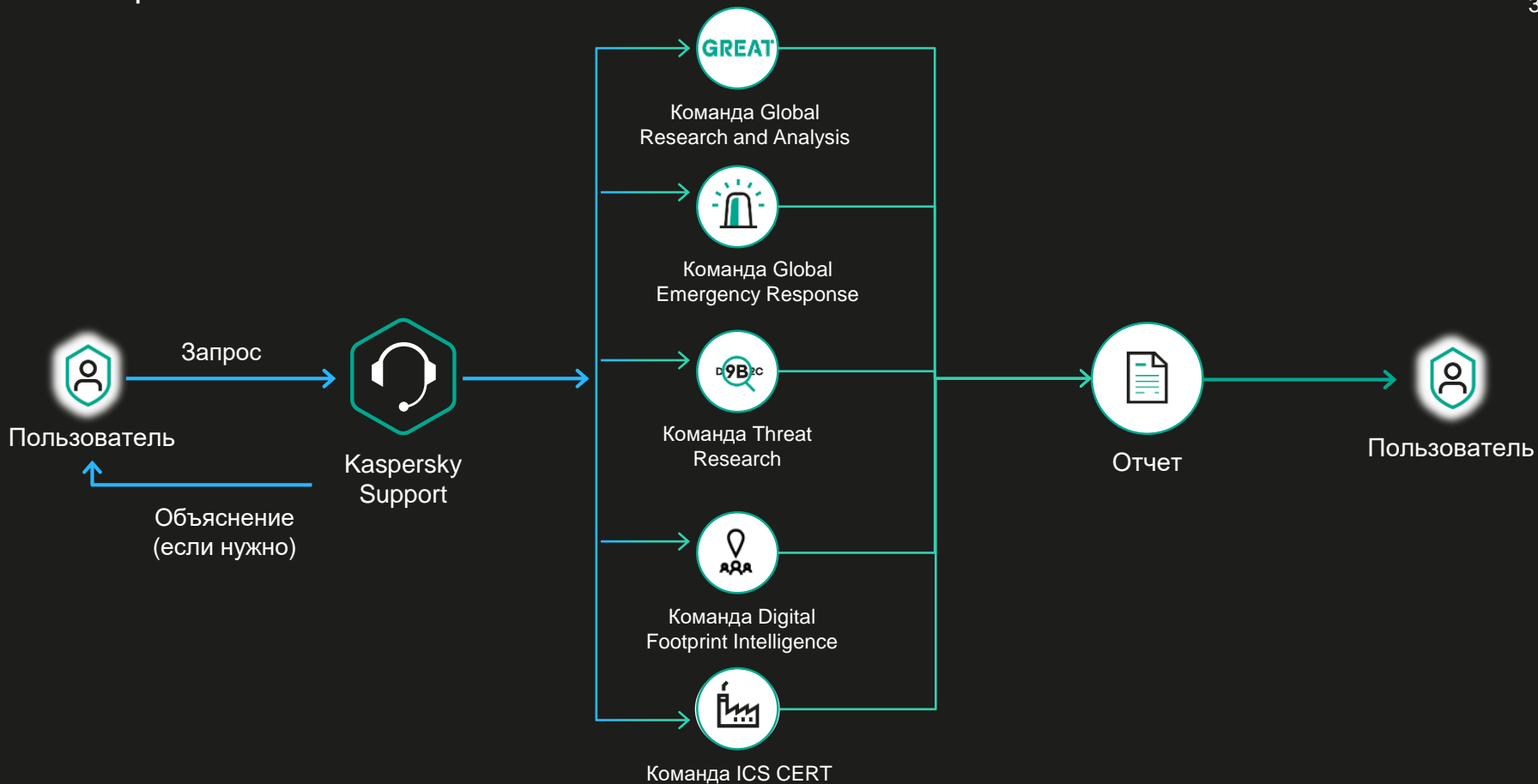
Descriptions of threats,
vulnerabilities and related
IoCs



Darkweb
Intelligence

В «аптечку» ИБ входит фиксированное количество часов консультации с экспертом

Как это работает



План оперативной помощи в рамках сервиса Kaspersky Industrial Emergency Kit

Экспресс-оценка защищенности и отчетность

for Networks

Kaspersky Industrial CyberSecurity

Экспресс-аудит инфраструктуры

Kaspersky Digital Footprint Intelligence

Персонализированный отчет об угрозах на организацию

ICS CERT Kaspersky ICS Threat Intelligence

Аналитические отчеты об угрозах на промышленный сектор

Создание цифровой модели системы ИБ

Обследование и подготовка данных для загрузки в Kaspersky Security CAD

Kaspersky Security CAD

Паспортизация и разработка модели угроз и нарушителей

Повышение осведомленности

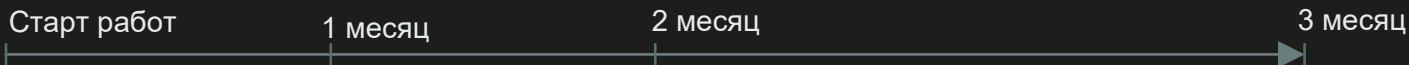
ICS CERT Kaspersky ICS CERT Training

Обучение по программе «Основы информационной безопасности АСУ ТП»






Результат

Kaspersky Ask the Analyst

Консультация с экспертом по результату проведенной работы, интерпретация отчетов и предоставление рекомендаций



Наши преимущества

-  Бренд, известный во всем мире. Одна из крупнейших частных компаний в сфере кибербезопасности
-  Более 10 лет «Лаборатория Касперского» разрабатывает и предлагает решения для защиты промышленных предприятий
-  «Лаборатория Касперского» обладает проектным опытом внедрения в разных отраслях: добыча полезных ископаемых, электроэнергетика, промышленность, транспорт и пр.
-  Компания имеет в своем составе специализированные экспертные подразделения (ICS CERT, GREAT), в составе которых работают эксперты международного уровня
-  Качество решений и сервисов подтверждено международными аналитическими агентствами

Активируй будущее!



go.kaspersky.com/ru-ics-kit