Программа сотрудничества «Лаборатории Касперского» с промышленными исследовательскими лабораториями

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Industrial CyberSecurity

Программа сотрудничества «Лаборатории Касперского» с промышленными исследовательскими лабораториями

С каждым годом количество киберугроз для промышленных предприятий растет. Появляются новые угрозы, происходят массовые заражения и целенаправленные атаки. Повсеместная цифровизация промышленных процессов и интеграция промышленных систем и сетей с внешними сетями открывают новые пути для несанкционированного вмешательства в работу оборудования, отвечающего за работу критических промышленных процессов, что в свою очередь может привести к прерыванию промышленных процессов, финансовым и репутационным потерям, а также более серьезным экологическим, социальным и макроэкономическим последствиям.

Рост угроз вынуждает государства, отраслевые организации и промышленные предприятия разрабатывать требования к процессам кибербезопасности в промышленности. Но зачастую промышленные предприятия не готовы к современному уровню угроз, не имеют эффективных технологий противодействия и квалифицированного персонала для борьбы с угрозами.

Для решения проблем в области промышленной кибербезопасности создаются исследовательские лаборатории и полигоны на базе различных организаций. В целях поддержки их работы «Лаборатория Касперского» запустила программу сотрудничества с промышленными лабораториями.

Профиль партнеров

Программа сотрудничества распространяется на организации различных типов, включая образовательные учреждения, исследовательские подразделения промышленных компаний, центры мониторинга безопасности (SOC) поставщиков услуг кибербезопасности, групп реагирования на чрезвычайные ситуации (CERT и CSIRT) и многие другие, имеющие лаборатории и проводящие исследования и обучение специалистов.

Условием сотрудничества является:

1. Наличие или планирование создания испытательных стендов, состоящих из физических или виртуальных компонентов для моделирования технологических процессов в различных отраслях, таких как добыча, транспортировка и переработка нефти и газа, энергетика, химическая промышленность, металлургия, машиностроение, производство, водоснабжение, и многих других.

2. Наличие образовательных программ/модулей по промышленной кибербезопасности или планов исследований, таких как анализ последствий атак, анализ эффективности систем мониторинга кибербезопасности и защиты, анализ уязвимостей, разработка политик и стандартов безопасности, создание комплекса коммерческих систем кибербезопасности.

3. Наличие команды или выделенных специалистов, отвечающих за эксплуатацию, обслуживание и развитие лаборатории.

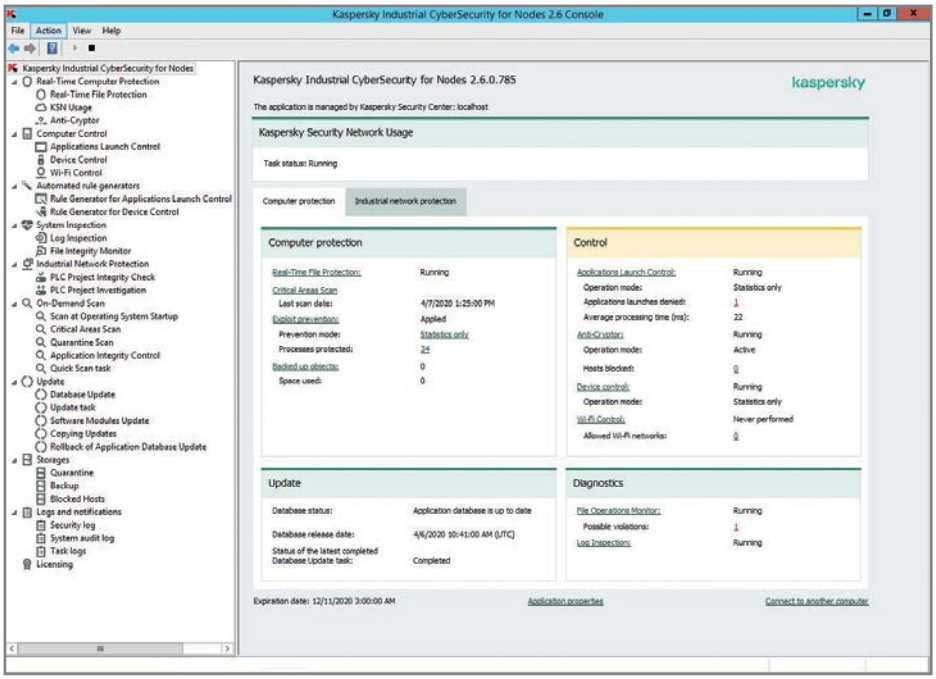
Предлагаемые технологии и экспертиза

Для проведения обучения и исследований на базе лабораторий, отвечающих условиям программы, «Лаборатория Касперского» предлагает на специальных условиях специализированные продвинутые инструменты и экспертизу по кибербезопасности АСУ ТП, включающие:

Преимущества:

- ✓**Комплексная защита конечных точек**
- ✓**Низкое воздействие на защищаемое устройство**
- ✓**Централизованное управление**

1. **Kaspersky Industrial CyberSecurity (KICS) for Nodes** – решение для защиты инженерных рабочих станций, станций операторов, человеко-машинного интерфейса (HMI), серверов ICS/SCADA. Обеспечивает контроль запуска приложений (whitelisting), контроль целостности файлов, контроль периферийных устройств, обнаружение и блокирование вредоносного ПО.

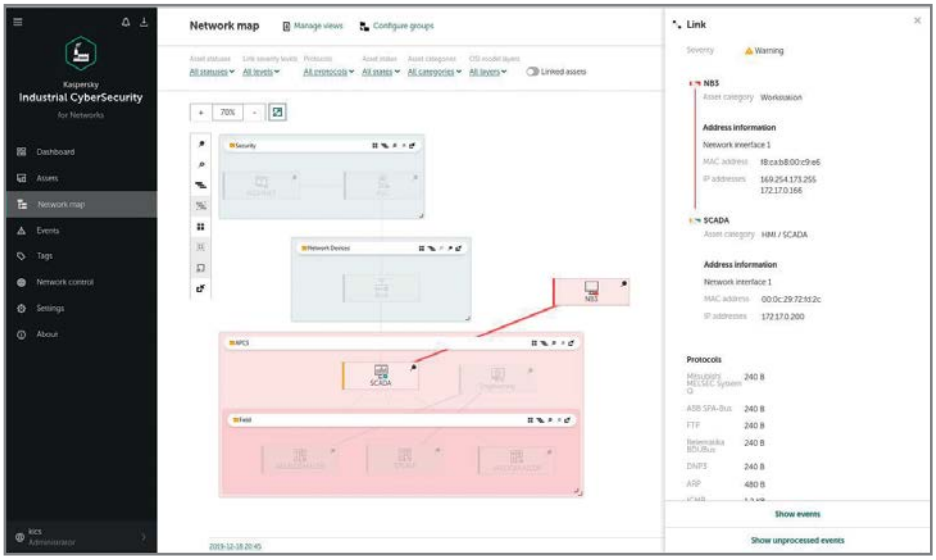


Интерфейс KICS for Nodes

Преимущества:

- ✓**Инвентаризация активов**
- ✓**Визуализация сетевых потоков**
- ✓**Раннее обнаружение атак и аномалий**
- ✓**Мониторинг параметров технологического процесса**
- ✓**Внешняя интеграция**

2. **Kaspersky Industrial CyberSecurity (KICS) for Networks** – решение для пассивной инвентаризации устройств и сетевых коммуникаций в промышленной сети, а также пассивного мониторинга атак и аномалий в трафике промышленной сети с инспекцией промышленных протоколов (DPI) для контроля команд и технологических параметров процесса.

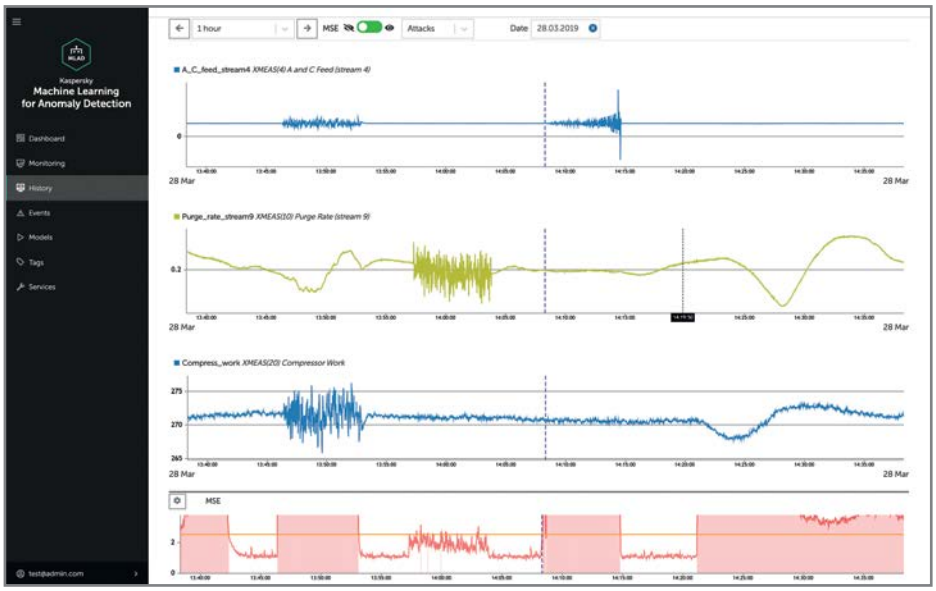


Интерфейс KICS for Networks

Преимущества:

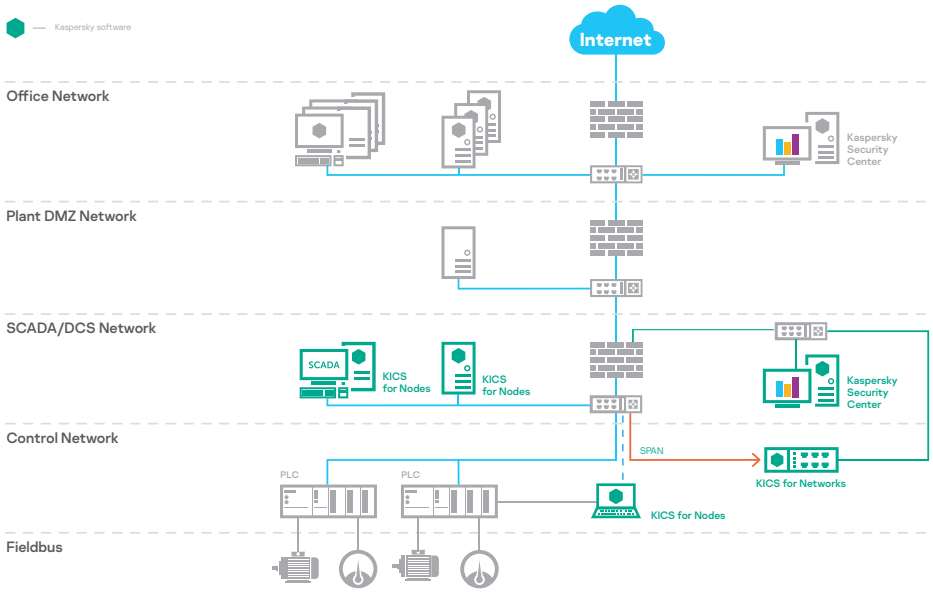
- ✓**Раннее обнаружение аномалий**
- ✓**Визуализация и группировка аномалий процесса**
- ✓**Построение модели поведения процесса с использованием машинного обучения**
- ✓**Низкие затраты человеческих ресурсов**

3. **Kaspersky Machine Learning for Anomaly Detection (MLAD** – решение для обнаружения и интерпретации аномалий в промышленной телеметрии на самых ранних этапах их развития. Kaspersky MLAD детектирует аномалии по инновационной технологии с использованием машинного обучения и позволяет обнаруживать аномалии независимо от того, чем они были вызваны: кибератакой, ошибкой человека или поломкой оборудования. Решение автоматически визуализирует любую аномалию процесса, группируя похожие аномалии. Рекомендации экспертов для одной аномалии могут быть использованы для целой группы схожих аномалий.



Интерфейс Kaspersky MLAD

4. Консультационную поддержку наших специалистов по созданию лабораторной среды, развертыванию и конфигурированию наших инструментов, моделированию сценариев кибератак, интеграции решений в процессы центров мониторинга (SOC) и разработке правил корреляции событий.



Пример развертывания компонентов KICS для Manufacturing

Наш опыт

В настоящее время компания «Лаборатория Касперского» уже имеет опыт подобного сотрудничества с рядом образовательных и исследовательских организаций, в частности в России (РГУ нефти и газа им. И.М. Губкина, Московский энергетический институт, Казанский государственный энергетический университет, Южно-Уральский государственный университет, Чувашский государственный университет им. И.Н. Ульянова), в Италии (Campus of Savona, University of Genoa), в Сингапуре (Singapore University of Technology and Design).

«Чувашский государственный университет известен своей научной и исследовательской работой в области электро-энергетики, а большая часть выпускников вуза остаются работать на многочисленных электротехнических предприятиях города. Именно поэтому наше сотрудничество с «Лабораторией Касперского» – компанией, обладающей столь обширным опытом борьбы с самыми сложными кибер-угрозами, – имеет решающее значение для подготовки высококвалифицированных специалистов, чья деятельность будет неразрывно связана с новыми технологиями»,

Андрей Александров,
Ректор Чувашского
государственного университета

Так, например, на базе лаборатории Чувашского государственного университета действует научно-технический центр информационной безопасности в электроэнергетике «Лаборатории Касперского». На базе центра осуществляется подготовка специалистов международного уровня, а также проводятся научные исследования в сфере информационной безопасности. Это позволяет молодым специалистам получать доступ к самой актуальной информации о методах защиты от киберугроз, нацеленных на информационные инфраструктуры критически важных объектов, в частности таких, которые участвуют в выработке и распределении электрической энергии.

Кроме того, в рамках данной программы мы хотим применить наш опыт защиты реальных промышленных объектов из разных стран. С публичными кейсами нашего сотрудничества с некоторыми из промышленных компаний и производителями систем промышленной автоматизации можно ознакомиться здесь: истории успеха, сертификации.

Наши цели

Предлагая наши технологии и экспертизу промышленным лабораториям, мы хотим внести свой вклад в повышение уровня знаний и профессиональной квалификации специалистов по промышленной кибербезопасности, в поиск способов обнаружения и блокирования новых векторов атак в различных промышленных отраслях, использовать полученный совместный опыт для совершенствования наших технологий кибербезопасности, а также иметь возможность демонстрировать совместные успехи представителям промышленных предприятий, правительств и академической среды.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity — это набор технологий и сервисов, созданных для защиты различных уровней промышленной инфраструктуры и других элементов предприятия, в том числе серверов SCADA, операторских панелей, инженерных рабочих станций, ПЛК и сетевых соединений. При этом решение не оказывает влияния на непрерывность технологических процессов.

Узнайте больше на: www.kaspersky.ru/ics

Всё о кибербезопасности ICS:
https://ics-cert.kaspersky.ru

Новости о киберугрозах:
www.securelist.ru

#Kaspersky
#BringontheFuture

www.kaspersky.ru

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* World Leading Internet Scientific and Technological Achievement Award at the 3rd World Internet Conference

** China International Industry Fair (CIIF) 2016 special prize