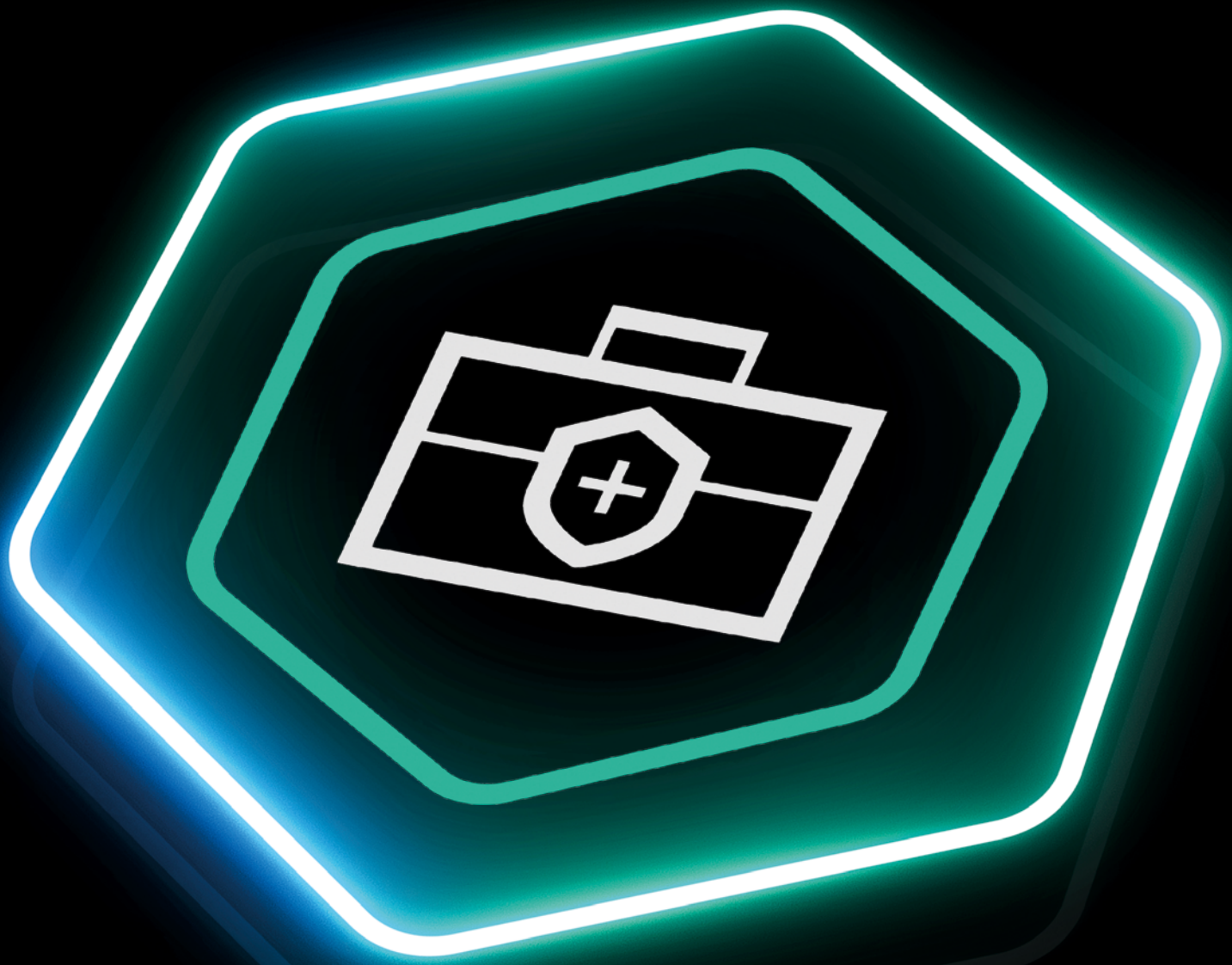

Kaspersky Industrial Emergency Kit

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Оперативная помощь для кибербезопасности АСУ ТП

Современные реалии промышленной кибербезопасности

- **Уязвимости** в АСУ ТП и усложнение ландшафта киберугроз
- **Ослабление** текущей системы информационной безопасности из-за ухода зарубежных вендоров
- **Рост** интереса хактивистов к системам автоматизации
- **Увеличение** числа APT-угроз в промышленном сегменте
- **Низкий уровень** осведомленности в области информационной безопасности АСУ ТП

Уже 25 лет мы обеспечиваем компаниям во всем мире надежную информационную защиту. Многолетняя экспертиза по исследованию угроз безопасности, глубокое понимание тактик и техник злоумышленников, разработанные нами решения для защиты критически важных промышленных систем – все это легло в основу Kaspersky Industrial Emergency Kit.

Данное предложение построено на экспертизе международного подразделения Kaspersky Industrial Control Systems Cyber Emergency Response Team (ICS CERT), которое оказывает услуги в области кибербезопасности промышленных объектов.

В рамках Kaspersky Industrial Emergency Kit наши эксперты оценят текущий уровень защиты АСУ ТП промышленного объекта. Вы получите отчеты о возможных киберугрозах для вашего предприятия и рекомендации, как своевременно реагировать на киберинциденты, а также сможете повысить осведомленность сотрудников в области промышленной кибербезопасности.

Экспресс-оценка защищенности и отчетность

- Kaspersky Industrial CyberSecurity for Networks — Экспресс-аудит инфраструктуры
- Kaspersky Digital Footprint Intelligence — Персонализированный отчет об угрозах на организацию
- Kaspersky ICS TI Reporting — Аналитические отчеты об угрозах на промышленный сектор

Повышение осведомленности

- Kaspersky ICS CERT Training — Обучение по программе «Основы информационной безопасности АСУ ТП»

Старт работ | 1 месяц | 2 месяц | 3 месяц

Результат

- Kaspersky Ask the Analyst — Консультация с экспертом по результату проведенной работы, интерпретация отчетов и предоставление рекомендаций

> С конца февраля 2022 года мы наблюдаем существенный рост интереса хактивистов к системам автоматизации, смежным подсистемам и цепочкам поставок. Большинство атак пока не достигают значимого результата, однако количество грозит перейти в качество.
>
> **Евгений Гончаров,**
> Руководитель центра исследования безопасности промышленных систем «Лаборатории Касперского»

Индустрии, которые мы поддерживаем:

- Электроэнергетика (генерация, распределение)
- Промышленность (металлургия, машиностроение, химическая, целлюлозо-бумажная)
- Нефтегазовый сектор (добыча, переработка, транспортировка)
- Критически-важная городская инфраструктура (ЖКХ, Водоканал)
- Транспортная инфраструктура (железнодорожная, авиационная, автомобильная, судоходная)
- Умные здания и смежные системы

Что входит в Kaspersky Industrial Emergency Kit

Kaspersky ICS Express Audit. Экспресс-оценка защищенности промышленной сети с использованием решения Kaspersky Industrial CyberSecurity for Networks в портативном режиме. Проведем детальный анализ трафика на уровне промышленных протоколов и подготовим отчёт об анализе защищенности.

Kaspersky ICS Threat Intelligence Reporting. Доступ к аналитическим отчетам, подготовленным командой Kaspersky ICS CERT: о важных изменениях в ландшафте угроз для АСУ ТП, о критических факторах, которые влияют на безопасность и уязвимость систем промышленной автоматизации.

Kaspersky Digital Footprint Intelligence. Отчет на основе данных, полученных в результате автоматического и ручного анализа общедоступных источников информации и ресурсов даркнета, а также внутренней базы знаний «Лаборатории Касперского». В отчете вы найдете аналитические данные и рекомендации, которые позволят сократить количество потенциальных векторов атаки и риски информационной безопасности для организации.

Kaspersky ICS CERT Training. Тренинги по повышению осведомлённости в области кибербезопасности для сотрудников промышленных предприятий. Проводится в удалённом режиме или с помощью онлайн-платформы.

Kaspersky Ask the Analyst. Итоговая консультация с нашими экспертами. Вы получите интерпретацию всех полученных результатов и отчетов, подготовленных в ходе сервиса, и рекомендации.

Результат проведенной работы

Kaspersky Industrial Emergency Kit поможет организациям за 3 месяца оценить текущий уровень безопасности АСУ ТП и получить рекомендации экспертов «Лаборатории Касперского», как усилить информационную безопасность промышленной инфраструктуры.

Международное признание

80+

Более 80 сертификатов о совместимости с оборудованием вендоров АСУ ТП.

«Лаборатория Касперского» провела сертификацию KICS for Networks на соответствие стандарту **МЭК 62443-4-1**, который подтверждает соответствие высоким требованиям к безопасности жизненного цикла разработки продуктов для использования в промышленных компаниях.

FORRESTER

«Лаборатория Касперского» признана лидером по результатам исследования Forrester Wave: External Threat Intelligence Services, Q1 2021

FROST & SULLIVAN

«Лаборатория Касперского» признана международной компанией года на рынке промышленной кибербезопасности по данным Frost & Sullivan в 2020 году

VDC|Research

«Лаборатория Касперского» получила платиновую награду VDC Research 2020 в категории «Промышленная безопасность»

industrial internet CONSORTIUM

«Лаборатория Касперского» участник консорциума промышленного интернета (Industrial Internet Consortium).

Как заказать Kaspersky Industrial Emergency Kit

Свяжитесь с нами по электронной почте ics-emergency@kaspersky.com или обратитесь к вашему аккаунт-менеджеру, чтобы получить коммерческое предложение и план-график работ.

Kaspersky Industrial Emergency Kit

Узнать больше

www.kaspersky.ru

© 2022 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.