kaspersky

Спроси эксперта

Проблема

Злоумышленники используют все более изощренные методы и инструменты для атаки на промышленные предприятия. Для успешного противостояния сложным атакам не всегда достаточно внутренних ресурсов организации – опытной команде по кибербезопасности требуются актуальная информация об угрозах, которая не всегда есть в открытых источниках, а также помощь внешних экспертов. В ситуациях, когда нужно действовать решительно, быстро и точно, крайне важно иметь возможность получить эксклюзивную информацию и экспертную поддержку без задержек.

Решение

Подписка на услугу «Спроси эксперта». Оформив подписку, можно оперативно получать информацию об угрозах и уязвимостях, актуальных для технологических сетей, рекомендации или консультацию экспертов Kaspersky ICS CERT.

Для кого

Промышленные предприятия различных отраслей, провайдеры услуг информационной безопасности (Managed Security Service Providers, MSSP), центры мониторинга информационной безопасности (Security Operation Center, SOC), производители АСУ, центры исследования безопасности (Cyber Emergency Response Team, CERT), центры анализа и обмена информацией (Information Sharing and Analysis Center, ISAC).

Проблематика

Ландшафт угроз непрерывно меняется, поскольку технический уровень и инструментарий злоумышленников постоянно развиваются. Для атак на промышленные предприятия используются все более продвинутые техники. Киберинциденты все чаще становятся следствием бесфайловых атак, атак без вредоносных программ с использованием легитимных инструментов, уязвимостей нулевого дня и архитектурных недостатков традиционных информационных и операционных технологий, а также следствием сложных атак, в ходе которых комбинируются различные тактики. Результатом кибератаки на промышленное предприятие могут стать кража конфиденциальных данных, остановка производства и физический ущерб.

В таких условиях роль компетентной команды по кибербезопасности невозможно переоценить. При этом даже опытные специалисты не всегда

могут противостоять быстро развивающимся угрозам самостоятельно – им требуется специфическая информация и поддержка сторонних экспертов. Внешняя экспертиза помогает выявить наиболее вероятные векторы сложных и целевых атак и составить практические рекомендации по эффективной борьбе с ними.

Что мы предлагаем

Услуга «Спроси эксперта» – это дополнение к комплексу информационных сервисов Kaspersky ICS CERT об угрозах и уязвимостях. Подписавшись на нее, клиент может обращаться к нашим экспертам за поддержкой и полезной информацией по конкретным угрозам и уязвимостям. Таким образом он задействует экспертизу и инструменты Kaspersky ICS CERT и внутренний автоматизированный аналитический пайплайн «Лаборатории Касперского», что позволяет существенно улучшить киберзащиту организации.

Преимущества

Экспертная поддержка

Можно в любой момент обратиться за консультацией к эксперту в конкретной предметной области в сфере кибербезопасности технологических сетей, а значит, нет необходимости искать и нанимать в штат узкопрофильных специалистов, которых на рынке труда очень мало.

Быстрое и точное обнаружение и реагирование

Более оперативное выявление угроз и оптимальное реагирование на угрозы и уязвимости для блокировки обнаруженных векторов атак по рекомендациям экспертов Kaspersky ICS CERT.

Эффективное расследование

С персонализированной и подробной контекстной информацией о выявленной угрозе гораздо проще приоритизировать и эффективно расследовать инциденты.

Расширение знаний

Возможность повысить уровень своих компетенций в области анализа уязвимостей, угроз и реагирования на инциденты благодаря взаимодействию с экспертами Kaspersky ICS CERT, которые готовы делиться своими знаниями и опытом, отвечая на конкретные вопросы наших клиентов.

Что получает клиент

Необходимую информацию об угрозах и уязвимостях, в том числе ту, которой нет в отрытых источниках, персональные рекомендации и консультации с экспертами Kaspersky ICS CERT.

Основные возможности

Запросы, связанные с АСУ ТП и прочими OT-системами

- Детальный анализ доступной информации по известным инцидентам и атакам;
- Дополнительная информация к опубликованным отчетам;
- Информация об уязвимостях в продукте или технологии;
- Анализ ландшафта угроз OT и новых тенденций, актуальных для организации клиента;
- Информация, касающаяся нормативных требований и стандартов.

Анализ вредоносного ПО

- Анализ вредоносных программ, обнаруженных в контуре OT;
- Рекомендации по противодействию и устранению последствий.

Анализ угроз в даркнете*

- Исследование даркнета на предмет конкретных артефактов, IP-адресов, доменных имен, имен файлов, адресов электронной почты, ссылок или изображений;
- Поиск и анализ информации, представляющей для клиента угрозу инцидентов информационной безопасности.

Описание угроз, уязвимостей и связанных с ними индикаторов компрометации

- Общее описание конкретных семейств вредоносного ПО;
- Дополнительный контекст для индикаторов компрометации (связанные хеши, URL, командные серверы, географическое распространение, затронутые отрасли и типы инфраструктур, и т. д.);
- Информация о конкретных уязвимостях (актуальный уровень критичности, перечень скомпрометированных версий и конфигураций, конкретные рекомендации экспертов Kaspersky ICS CERT по снижению рисков, например, какие механизмы продуктов «Лаборатории Касперского» защищают от указанных уязвимостей, и прочие технические средства и меры защиты, которые помогут в

* Уже включено в подписку Kaspersky Digital Footprint Intelligence.

том случае, когда установка исправлений невозможна или обновление неэффективно).

Сценарии использования

1. Уточнение информации из ранее опубликованных отчетов об угрозах.
2. Получение дополнительной информации по уже обнаруженным индикаторам компрометации.
3. Получение уникального описания уязвимостей и рекомендаций по защите от их эксплуатации.
4. Получение сведений об угрожающей клиенту активности на ресурсах даркнета.
5. Получение общего отчета по семейству вредоносного ПО, включая его функциональные возможности и возможные последствия атаки с его использованием, подробное описание связанной активности, известной «Лаборатории Касперского».
6. Повышение эффективности приоритизации оповещений об угрозах и (или) инцидентах с помощью подробной контекстной информации и категоризации связанных индикаторов компрометации.
7. Запрос помощи в определении природы подозрительной активности (целевая атака или широкомасштабное заражение, предположения относительно злоумышленников и их целей).
8. Отправка вредоносных файлов на комплексный анализ, чтобы понять функциональность предоставленных образцов.
9. Запрос анализа тенденций ландшафта угроз, актуальных для организации клиента. Такой анализ полезен как при краткосрочном, так и при долгосрочном планировании изменений в части обеспечения кибербезопасности.

Рекомендуем дополнительно

- Аналитические отчеты об угрозах и уязвимостях АСУ ТП на портале Kaspersky Threat Intelligence
- Аналитика известных уязвимостей АСУ для принятия критически важных решений в части информационной безопасности
- Поток машиночитаемых данных об уязвимостях АСУ ТП
- Анализ ландшафта угроз по индивидуальному заказу
- Расследование киберинцидентов на промышленных предприятиях
- Цифровая криминалистика и расследование инцидентов в АСУ ТП. Тренинг

- Разработка руководства и обучение реагированию на инциденты

Запросить консультацию специалиста

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com