Информация об уязвимостях и угрозах для АСУ ТП

Проблема

Нехватка или отсутствие специализированных данных о текущих угрозах для систем промышленной автоматизации, а также об уязвимостях в промышленном ПО и оборудовании, и как результат — отсутствие у организации достаточной основы для реалистичной оценки рисков и принятия эффективных мер для их снижения.

Решение

Доступ к порталу Kaspersky Threat Intelligence с достоверными и подробными сведениями об атаках на промышленные организации, а также об уязвимостях в наиболее популярных АСУ и других системах и компонентах, часто используемых в среде промышленной автоматизации. Эта информация помогает принимать эффективные решения по оценке рисков и обеспечению кибербезопасности организации как в текущих обстоятельствах, так и в рамках стратегического планирования.

Для кого

Службы информационной безопасности промышленных предприятий, поставщики услуг по управлению кибербезопасностью (MSSP), центры реагирования на компьютерные инциденты (CERT), центры мониторинга информационной безопасности (SOC), центры обмена информацией и анализа (ISAC), национальные проекты по безопасности, государственные регуляторы, поставщики промышленной автоматизации и услуг в сфере кибербезопасности, разработчики продуктов для защиты промышленных систем управления.

Проблематика

В условиях постоянно растущего уровня и разнообразия киберугроз обеспечивать информационную безопасность организации и непрерывность технологических процессов, превентивно выявлять свою потенциальную незащищенность перед развивающимися угрозами в секторе и регионе, обоснованно планировать бюджет, равно как и своевременно обнаруживать признаки вероятной компрометации и эффективно расследовать киберинциденты на компьютерах АСУ возможно лишь, опираясь на проверенные данные об угрозах, включающие в себя необходимые технические детали.

Необходимо понимать цели и фокус злоумышленников, их методы, тактики, техники и инструменты. Иными словами — знать, кто и каким образом атакует предприятия аналогичного профиля, какие меры предпринять, чтобы снизить риск успешной атаки, и что делать в первую очередь при обнаружении признаков компрометации.

Обеспечение информационной безопасности на предприятиях часто сопряжено с рядом проблем:

- Неидентифицированные угрозы, как отраслевые и региональные, так и кросс-отраслевые и кросс-региональные, слепые зоны в ландшафте угроз.
- Неэффективный проактивный поиск угроз (threat hunting), сложность в выявлении реальных угроз.
- Слабое прогнозирование OT-рисков: планирование защиты и долгосрочные инвестиции в безопасность вслепую.
- Невозможность точно измерить и обосновать эффективность инвестиций в кибербезопасность, сложности с защитой бюджета.
- Несоответствие учений и проверок готовности реальным TTP атакующих, переоценка уровня защищенности.
- Замедленное реагирование на инциденты, поскольку нехватка контекста тормозит принятие решений и увеличивает последствия инцидентов.

Для минимизации рисков эксплуатации уязвимостей в продуктах АСУ и других системах и компонентах, часто используемых в среде промышленной автоматизации, и, что не менее важно, эффективной приоритизации и распределения ресурсов для их устранения необходима достоверная информация, позволяющая определить реальные последствия эксплуатации уязвимости и принять решение об адекватных мерах по ее устранению. Это полная информация о самой уязвимости и ее реальной критичности (мы часто видим на практике уязвимости как с нулевой, так и с заниженной критичностью), список реально уязвимых продуктов и практические рекомендации, включающие меры смягчения риска до установки обновлений, а также в том случае, когда по каким-либо причинам установить обновление невозможно.

Что мы предлагаем

Полные сведения об уязвимостях и угрозах для систем промышленной автоматизации.

Сведения об угрозах

Отчеты об угрозах, содержащие информацию об APT-группах, масштабных заражениях вредоносным ПО и других кампаниях, нацеленных на промышленные организации. Этот тип отчетов решает несколько задач:

обеспечение организаций подробной информацией об угрозах, которые могут повлиять на деятельность этих организаций или их клиентов, а также рекомендация мер для эффективного предотвращения, обнаружения, реагирования на инциденты, а также для их расследования. Кроме того, такие отчеты являются качественной экспертной базой для принятия долгосрочных стратегических решений по кибербезопасности и повышения уровня осведомленности и подготовки руководства и сотрудников к потенциальным атакам различной структуры и сложности.

Отчет включает в себя:

- резюме с краткими выводами для руководителей;
- технические подробности: описание метода атаки и последовательности действий злоумышленников (kill chain), используемый инструментарий, TTP (тактики, техники и процедуры);
- данные об инфраструктуре управления и контроля (C2), используемой злоумышленниками для управления зараженными устройствами;
- описание актора, стоящего за атакой;
- профиль затронутых организаций;
- выводы и детальные рекомендации о предотвращении и сдерживании с правилами корреляции для SIEM-систем;
- индикаторы компрометации (хеши, IP-адреса, URL, домены) и YARA-правила;
- сопоставление с матрицей MITRE ATT&CK.

Статистические данные об угрозах по ряду регионов и отраслям, описывающие ландшафт угроз для сред промышленной автоматизации за прошедший месяц. Задача таких отчетов — предоставить специалистам по безопасности важную информацию о текущих трендах промышленных угроз и системных проблемах, требующих особого внимания.

Отчет включает в себя:

- резюме с ключевыми показателями и их изменением для руководителей;
- обзор региона, содержащий статистику по региону в целом, странам, типам и источникам угроз, сопоставление показателей за текущий месяц в сравнении с мировыми показателями, а также динамику показателей за год;
- обзор показателей угроз и их изменение по отраслям: нефть и газ, электроэнергетика, автоматизация зданий, производство, строительство, биометрия, инжиниринг и интеграторы АСУ;
- рекомендуются меры, направленные как на снижение всех показателей, так и на снижение рисков, связанных с конкретными типами угроз и векторами атак.

Ежемесячные обзоры угроз, атак и инцидентов, связанных с промышленными организациями по всему миру и раскрытых в отчетном месяце. Задача таких отчетов — предоставить организациям актуальную информацию о недавних киберугрозах, которые могут повлиять на их

деятельность, а также данные для проверки на предмет наличия признаков атаки в организации и принятия эффективных мер первичной защиты.

Обзор включает в себя:

- резюме с краткими выводами для руководителей;
- описание киберинцидентов;
- индикаторы компрометации: хеши, IP-адреса, URL, домены и т. д.

Ранние предупреждения об угрозах, дающие возможность оперативно защитить организацию, до появления полных отчетов об угрозах и атаках.

Сведения об уязвимостях

Анализ командой Kaspersky ICS CERT известных уязвимостей в АСУ или связанном программном и аппаратном обеспечении с изначально неточной оценкой и рекомендациями. Основная задача таких отчетов — предоставить организациям корректные данные об уязвимостях для обоснованной оценки рисков кибербезопасности и планирования адекватных мер по их снижению или принятию.

Отчет содержит первоначальную информацию от вендора, анализ достоверности этой информации от наших экспертов, выводы и итоговую оценку уязвимости, а также практические рекомендации по устранению уязвимости согласно выявленной в результате анализа ее реальной критичности.

Отчет включает в себя:

- резюме с ключевыми выводами для руководителей;
- технический анализ: подробное описание и обоснование полученных в результате анализа данных, в том числе особенности затронутых продуктов, а также скорректированные вектор и рейтинг CVSS;
- выводы;
- перечень затронутых продуктов и соответствующих обновлений, в том числе снятых с поддержки продуктов;
- меры по снижению рисков: практические рекомендации Kaspersky ICS CERT и вендора, Suricata, OVAL;
- сопоставление с матрицей ICS MITRE ATT&CK.

Оповещения об уязвимостях для предотвращения их эксплуатации до выпуска официальных исправлений.

Отчеты об исследованиях уязвимостей нулевого дня в наиболее популярных продуктах и технологиях, используемых в технологической среде и АСУ, а также промышленном интернете вещей в различных отраслях.

Преимущества отчетов и обзоров Kaspersky Threat Intelligence

- **Только проверенные факты.** Информация, представленная в отчетах и обзорах, способна стать фундаментом для оценки рисков и разработки мер по минимизации и устранению уязвимостей.
- **Экспертиза Kaspersky ICS CERT.** Отчеты подготовлены командой практиков, обладающих обширным опытом исследования угроз и уязвимостей в области АСУ и расследования киберинцидентов.
- **Большие телеметрические данные.** При исследовании угроз используются собственные телеметрические данные об угрозах, заблокированных защитными решениями Kaspersky на более чем 3 млн компьютеров АСУ по всему миру.
- **Детальный экспертный анализ уязвимостей.** Посредством этого анализа мы помогаем вендорам в оценке уязвимостей и выборе мер и подходов по их устранению и предотвращению. Мы придерживаемся принципа ответственного раскрытия и поддерживаем обмен опытом.
- **Глубокое понимание региональных и отраслевых особенностей.** Выявление региональных и отраслевых угроз, определение трендов на основе ежемесячной, ежеквартальной и годовой статистики.
- **Собственная база данных об уязвимостях АСУ.** Каждая запись в этой базе — результат кропотливого анализа экспертов Kaspersky ICE CERT.

Что получает клиент

Эффективный инструмент для решения оперативно-тактических и стратегических задач в области кибербезопасности

Подробная информация об угрозах, которые могут повлиять не только на конкретную организацию, но и на целый сектор или даже несколько секторов, а также об уязвимостях в программных и аппаратных компонентах промышленных систем — это эффективный инструмент, который можно и нужно использовать при решении оперативно-тактических и стратегических задач.

Этот инструмент помогает:

- проактивно управлять OT-рисками — более точно прогнозировать и приоритизировать угрозы и уязвимости на основе достоверных данных;
- осуществлять защиту критически важных активов и непрерывности техпроцесса — выявлять и предотвращать известные угрозы и тем самым не допустить остановки производства;

- быстрее обнаруживать и реагировать — сопоставлять подозрительную активность в промышленной среде с известными кампаниями и TTP злоумышленников, ускоряя расследование и сдерживание инцидентов;
- осмысленно управлять уязвимостями — принимать, учитывая оценку масштаба и критичность уязвимостей, обоснованные решения: устанавливать обновления, внедрять компенсирующие меры или менять конфигурации;
- сократить количество и продолжительность инцидентов — и, следовательно, сократить возможные потери за счет уменьшения количества незапланированных остановок, меньших затрат на восстановление;
- продемонстрировать уровень зрелости информационной безопасности организации ее руководству, а также регуляторам, страховщикам;
- инвестировать в привязке к реальным угрозам — а значит, проще обосновывать бюджеты и CAPEX, демонстрировать окупаемость кибербезопасности;
- повысить боеготовность команд — разработать реалистичные сценарии на основе реальных атак для red/blue/purple-учений и эффективной координации.

Начать бесплатно

Мы предлагаем попробовать сервис Kaspersky Threat Intelligence в работе, прежде чем принять взвешенное решение о необходимости оформления подписки.

В рамках демодоступа предоставляются около 10 примеров отчетов, содержащих данные об атаках на промышленные организации, результаты исследований уязвимостей в промышленных решениях, а также информацию об угрозах, с которыми сталкиваются системы промышленной автоматизации.

Кроме того, демодоступ позволяет оценить возможности интерфейса по поиску информации, а также диапазон и формат предоставляемых данных, в частности индикаторов компрометации (IoC) и YARA-правил, которые можно скачать и использовать в защитных решениях.

Запросить демодоступ или консультацию специалиста

Рекомендуем дополнительно

- Разработка руководства и обучение реагированию на инциденты

- Аналитика известных уязвимостей АСУ для принятия критически важных решений в части информационной безопасности
- Поток данных об угрозах для систем промышленной автоматизации
- Анализ ландшафта угроз по индивидуальном заказу
- Спроси эксперта

Запросить демодоступ или 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