Центр мониторинга и реагирования на инциденты ИБ Jet CSIRT использует уникальный поток данных об угрозах от «Лаборатории Касперского»

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky ICS CERT

«Инфосистемы Джет»

csirt.jet.su

Системный интегратор

- Входит в ТОП-3 крупнейших интеграторов России в рейтинге CNews Security 2019
- 24 года на рынке ИБ
- 1800+ сотрудников
- 250+ ИБ-экспертов
- 300+ комплексных проектов ежегодно

«Инфосистемы Джет» – одна из крупнейших ИТ-компаний в России. На рынке системной интеграции с 1991 года, реализует сложные и уникальные проекты в масштабах всей страны. Штат — более 1800 сотрудников. Компания имеет более 10 офисов и представительств в России и СНГ и ведет проекты в других странах. Основные направления деятельности: проектирование и внедрение вычислительных комплексов, сетевой инфраструктуры, инженерных систем и мультимедиа, заказная разработка, внедрение и сопровождение программных решений и бизнес-приложений enterprise-уровня, обеспечение информационной безопасности, ИТ-аутсорсинг и техническая поддержка.

Портфель услуг в области информационной безопасности включает консалтинг, проектирование, внедрение, сопровождение и техническую поддержку специализированных решений. Своей главной задачей компания ставит внедрение и создание решений, обеспечивающих реальную безопасность бизнеса.

Задача

В 2018 году компания запустила Центр мониторинга и реагирования на инциденты информационной безопасности Jet CSIRT.

Jet CSIRT объединяет в себе ключевые сервисные продукты компании по мониторингу и реагированию на инциденты ИБ, эксплуатации и поддержке средств защиты и позволяет закрывать задачи клиентов по обеспечению безопасности в режиме 24x7 «под ключ».

Команда Jet CSIRT насчитывает 40 экспертов, которые реализуют свыше 200 контрактов экспертных услуг. В качестве своих клиентов Jet CSIRT видит компании из самых разных отраслей, в том числе и крупные промышленные предприятия.

Для обеспечения высокого качества защиты промышленных инфраструктур и расследования инцидентов ИБ в этой сфере нужны специфичные данные о киберугрозах, актуальных для автоматизированных систем управления технологическим процессом (АСУ ТП). Вредоносные программы, обнаруживаемые на компьютерах АСУ ТП, часто являются уникальными и практически не встречаются на компьютерах в корпоративной сети.

Компании «Инфосистемы Джет» было необходимо найти надежного поставщика таких данных для своего Центра мониторинга и реагирования. Компания провела анализ рынка в поисках компании с глобальным присутствием и опытной командой исследователей угроз в АСУ ТП. Кроме того, компанию интересовало наличие продуманной MSSP-модели и удобной лицензионной политики.

«На определенном этапе развития нашего Центра мониторинга и реагирования на инциденты ИБ для нас стал актуальным вопрос о качественном обогащении инцидентов информацией по промышленным ИБ-угрозам. Проанализировав рынок, мы пришли к тому, что лидером этого направления является “Лаборатория Касперского”».

Алексей Мальнев, руководитель Центра мониторинга и реагирования на инциденты ИБ Jet CSIRT компании «Инфосистемы Джет»

Экспертиза
«Лаборатория Касперского» успешно помогает промышленным предприятиям, регулирующим органам и государственным учреждениям противостоять атакам и угрозам, нацеленным на критически важные инфраструктуры. В компании создан свой Центр исследования безопасности промышленных систем (Kaspersky ICS CERT).

Качество данных
Поток данных об угрозах регулярно обновляется на основе информации, получаемой через Kaspersky Security Network (KSN) **исключительно** с компьютеров АСУ ТП, защищаемых продуктами «Лаборатории Касперского».

Комплексный подход
«Лаборатория Касперского» помогает реализовать комплексный подход к кибербезопасности на всех уровнях, начиная с анализа защищенности и тренингов для сотрудников и заканчивая передовыми технологиями защиты АСУ ТП и реагированием на инциденты.

Решение

В качестве поставщика данных для Jet CSIRT «Инфосистемы Джет» выбрала «Лабораторию Касперского», единственного игрока, удовлетворяющего всем критериям компании и обладающего действительно уникальными данными о киберугрозах, актуальных для промышленных предприятий.

Постоянно обновляемый поток данных об угрозах в системах промышленной автоматизации предназначен для информирования службы информационной безопасности предприятия о рисках, связанных с киберугрозами, и их последствиях и помогает принимать меры защиты от кибератак до их начала и предотвращать инцидент.

Передаваемые данные об угрозах содержат индикаторы компрометации (IoC), позволяющие:

- обнаруживать попытки атак на системы промышленной автоматизации;
- выявлять случаи заражения системы промышленной автоматизации вредоносным ПО, в том числе в ходе проведения работ по реагированию на компьютерные инциденты;
- обогащать данные об угрозах и вредоносном ПО, обнаруженных в системах промышленной автоматизации.

Сбор и обработка

Поток данных регулярно обновляется на основе информации, получаемой через Kaspersky Security Network (KSN) с компьютеров АСУ ТП. Все полученные данные верифицируются и качественно улучшаются с помощью множества технологий, таких как анализ на основе статистических критериев, анализ экспертными системами компании («песочницы», эвристический анализ, анализ подобия, профилирование поведения и т.д.), проверка аналитиками и проверка по «белому списку».

Сценарии использования данных

Обнаружение атак

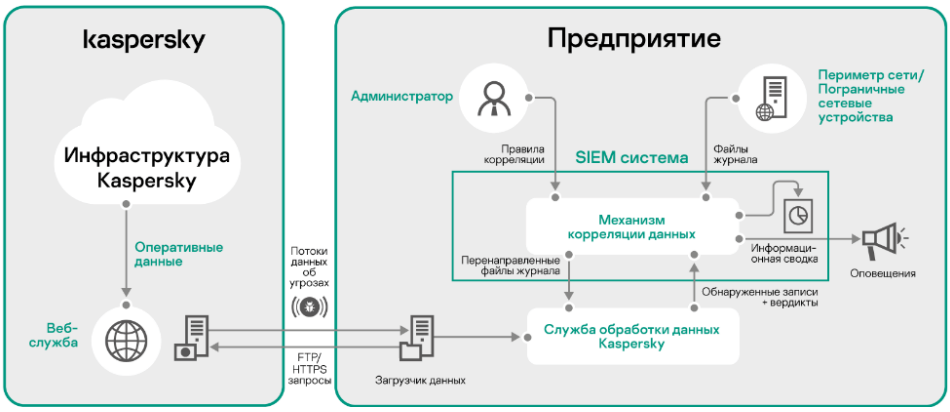
Поток данных об угрозах предоставляет дополнительный уровень защиты от вредоносных программ, позволяя обнаруживать вредоносное ПО и попытки атак на системы: получаемые данные сопоставляются с данными SIEM-систем, которые собираются с периметра сети, конечных узлов и файловых «песочниц».

Выявление случаев заражения

Данные об угрозах предоставляются в открытом JSON-формате и могут быть использованы различными системами анализа и сопоставления данных или переформатированы в любой другой формат данных. Таким образом данные об угрозах могут быть использованы для выявления атак и случаев заражения компьютеров АСУ ТП вредоносным ПО в ходе проведения расследований киберинцидентов.

Обогащение данных об угрозах

В ходе проведения расследований киберинцидентов специалистам часто требуется дополнительная информация об обнаруженных угрозах, которая позволила бы связать разрозненные факты о киберинциденте для получения полной картины.



Результаты

Подключение потока данных об угрозах, нацеленных на системы промышленной автоматизации, в системы Центра мониторинга и реагирования на инциденты информационной безопасности Jet CSIRT прошло в плановом порядке при поддержке специалистов «Лаборатории Касперского» и не вызвало сложностей.

По итогам нескольких месяцев работы специалисты Jet CSIRT с уверенностью могут сказать, что сделали правильный выбор: пилотные испытания показали успешную регистрацию ряда актуальных промышленных угроз. Jet CSIRT повысил уровень экспертных сервисов для промышленных предприятий.

www.kaspersky.ru
#ИстиннаяБезопасность

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, сетевых соединений и даже самих инженеров. При этом решение не влияет на непрерывность технологических процессов.

Узнайте больше на: www.kaspersky.ru/ics