



ABB и IBM объединились для укрепления кибербезопасности промышленных предприятий

ABB и IBM объявили о сотрудничестве, направленном на объединение кибербезопасности и операционных технологий (OT). В качестве первого шага этого сотрудничества ABB разработала программу для мониторинга событий безопасности OT, которая сочетает в себе опыт разработок ABB в области систем управления процессами и портфель решений IBM

Системы управления промышленными предприятиями всё чаще становятся объектами кибератак. Фактически, в последнем ежегодном отчете IBM X-Force Threat Intelligence Index



указывается, что с 2018 года по сегодняшний день количество атак на промышленные и производственные объекты увеличилось более чем на 2000%.

СИСТЕМЫ УПРАВЛЕНИЯ ПРОЦЕССАМИ КОМПАНИИ ABB МОГУТ ПОДКЛЮЧАТЬСЯ К ПЛАТФОРМЕ БЕЗОПАСНОСТИ IBM ДЛЯ ОТСЛЕЖИВАНИЯ ЦИФРОВЫХ УГРОЗ

Чтобы надежнее связать данные OT с более широкой экосистемой IT-безопасности, ABB разработала новое приложение, которое позволяет отправлять информацию от ABB на платформу IBM QRadar Security Intelligence.

Данное техническое решение ABB было разработано в соответствии с эталонной архитектурой совместно с IBM. Оно представляет собой программу, необходимую для быстрого реагирования на инциденты в области безопасности управления процессами, и особенно подходит для сложных промышленных процессов в таких отраслях, как нефтегазовая, химическая и горнодобы-

вающая. Новое программное обеспечение для сбора и пересылки информации о событиях, обеспечивающее эту интеграцию, в настоящее время уже используется первыми клиентами и будет широко доступно в ближайшие месяцы.

Это сотрудничество знаменует собой первый случай, когда опыт в области данных OT и обрабатывающей промышленности вводится непосредственно в систему мониторинга информации и событий безопасности (SIEM), что позволяет управлять угрозами в рамках более широких операций и стратегии кибербезопасности организации.

«Сотрудничество ABB с IBM позволяет анализировать события управления процессами в контексте безопасности и воздействия на операционную среду, обеспечивая значительное улучшение видимости киберугроз в ОТ по всем направлениям», — отметил Роберт Путман (Robert Putman), глобальный менеджер службы кибербезопасности департамента промышленной автоматизации ABB.

Сбои в производстве из-за кибератак или технических неполадок могут быть дорогостоящими с точки зрения потерь и повреждения физических активов.

Наиболее продуманный операционный мониторинг сосредоточен на производительности объекта, будь то газовая турбина для выработки электроэнергии, горнопроходческое оборудование, или простой мониторинг выбросов загрязняющих веществ на химическом предприятии.

Новое приложение ABB предлагает технологию сбора данных системой управления процессами и передачи их в IBM QRadar Security, которая использует автоматизацию и искусственный интеллект для выявления аномалий безопасности и потенциальных угроз.

IBM® QRadar® Security Information and Event Management (SIEM) помогает специалистам по безопасности обеспечить высокую точность обнаружения угроз и расстановки приоритетов. Данное решение дает возможность быстро реагировать на инциденты и минимизировать их последствия. Консолидация событий в журналах и потоках данных, поступающих в сеть с тысяч устройств, конечных точек и приложений, дает QRadar возможность сопоставлять разнообразную информацию, объединять взаимосвязанные события и выдавать точечные предупреждения для ускорения анализа и устранения инцидентов.

«Мы рассматриваем интеграцию этих решений как объединение лидирующих на рынке возможностей для единого представления о безопасности ОТ, — подчеркнул д-р Андреас Кюмичел, технический директор подразделения решений для нефтехимической и газовой промышленности IBM. — С более полной прозрачностью ОТ и IT-безопасности мы сможем помочь клиентам снизить риск внезапного прерывания производства из-за нарушения защищенности, что приводит к дорогостоящим простоям и большему риску для компании».

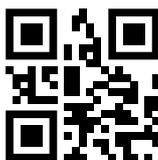
Технологии ABB и IBM, используемые в этом решении, разработаны на открытых платформах, что позволяет им работать на периферии и легко развертываться в гибридных облачных средах — как в локальных, так и в общедоступных. Совместное решение разработано таким образом, что



тестирование систем безопасности происходит автоматически и не нарушает производственные процессы. Анализ безопасности в QRadar осуществляется через библиотеку вариантов использования, которая автоматически помечает инциденты и запускает соответствующие сигналы тревоги.

Обе компании планируют продолжить сотрудничество в области безопасности ОТ, чтобы предоставить своим клиентам новые возможности, которые помогут решать их задачи более эффективно. 

ABB (ABBN: SIX Swiss Ex) — ведущая глобальная инженеринговая компания, которая стимулирует преобразование общества и промышленности для достижения более эффективного и устойчивого будущего. Соединяя программное обеспечение со своим портфолио в области электрификации, робототехники, автоматизации и мобильности, ABB раздвигает границы технологий, чтобы вывести производство на новый уровень. История ABB насчитывает более 130 лет, а её успех обеспечивается 110 000 талантливых сотрудников из более чем 100 стран мира.



IBM Security — предлагает одну из самых передовых программ корпоративной безопасности, разработанную и поддерживаемую всемирно известной исследовательской группой IBM X-Force®. Она позволяет организациям эффективно управлять рисками и защищаться от возникающих угроз. IBM — это одна из крупнейших в мире организаций, занимающихся исследованиями, разработками и поставками услуг в области безопасности. Её подразделения ежедневно отслеживают 70 миллиардов событий в сфере безопасности, происходящих в более чем 130 странах мира. Компания обладает свыше 10 000 патентов на системы безопасности, зарегистрированных по всему миру.

