Центр научно-технической информации и библиотек – филиал ОАО «РЖД»

Дифференцированное Обеспечение Руководства

3/2022

Решение по кибербезопасности для железных дорог от израильского стартапа Cylus

За последние пять лет количество кибератак, ориентированных на железнодорожные перевозки, во всем мире увеличились в несколько раз. Только в США их рост за последний год составил 173%, при этом каждый месяц в среднем выявляется один крупный инцидент. По мере того, как железнодорожные системы претерпевают цифровую революцию и становятся гораздо более взаимосвязанными и сложными, их операторы сталкиваются с растущим количеством и многообразием угроз.

Для решения подобных задач и защиты объектов железнодорожного транспорта от киберугроз компания Cylus (Израиль) разработала набор сервисов под общим названием CylusOne. Это комплексное решение создано для защиты наиболее обширных и сложноустроенных железнодорожных сетей с соблюдением самых строгих стандартов. Основываясь на сравнении получаемых данных с эталонными показателями, CylusOne непрерывно выполняет оценку уязвимостей сети. Когда решение обнаруживает аномалии в рамках базы данных общеизвестных уязвимостей информационной безопасности (CVE), оно генерирует оповещения в режиме реального времени, оценивает риски и выдает практические рекомендации по решению проблем.

Сервисы CylusOne совместимы с системой управления движением поездов по радиоканалу CBTC и европейской системой управления движением поездов ETCS.

Определение наиболее эффективной последовательности действий для устранения обнаруженной угрозы в системе реализуются с помощью

функции искусственного интеллекта. CylusOne выявляет киберугрозы для сетей сигнализации и управления движением поездов, связи, бортовых и напольных систем. Несанкционированный доступ, вредоносное ПО, DOS-атаки и многое другое CylusOne обнаруживает, используя Deep Packet Inspection (DPI)[1]. С помощью анализа полезной нагрузки DPI можно классифицировать различные угрозы и создавать типологию. Для ускорения обнаружения несанкционированного доступа и вредоносного программного обеспечения технология использует машинное обучение.

Панель мониторинга CylusOne предлагает современные инструменты визуализации (например, модель Rail-Purdue), а также расширенную аналитику угроз для индивидуальных отчетов, аудитов и судебных расследований. Эти аналитические инструменты позволяют экспертам по кибербезопасности создавать эффективные планы реагирования на инциденты и протоколы для противодействия массовым кибератакам. Но что еще более важно, CylusOne позволяет железнодорожным операторам/владельцам инфраструктуры виртуально разделять железнодорожную сеть на зоны безопасности и каналы, тем самым изолируя надвигающиеся угрозы и уязвимые активы, что необходимо для выполнения требований администрации TSA.

Cylus также предлагает дополнительные услуги в области кибербезопасности, такие как оценка уязвимостей на месте/удаленно, сервис Red Team[2], консультации и обучение. Таким образом, железнодорожные операторы/владельцы инфраструктуры могут использовать опыт Cylus в области кибербезопасности железных дорог для проведения первоначальной оценки уязвимости еще до развертывания решения.

Решение Cylus предлагает непрерывный мониторинг и защиту по всем фронтам в режиме реального времени для многих железнодорожных систем, независимо от размера и местоположения, что позволяет не только вовремя обнаруживать угрозы, проводить расширенную судебную экспертизу и мероприятия по ликвидации последствий, упрощать операции по обеспечению безопасности, но и многое другое. Установка CylusOne занимает всего несколько часов, не требует перерывов в движении, полностью интегрируется с новыми и устаревшими системами без каких-либо изменений в сетевой архитектуре, обеспечивая полную видимость всех активов в течение нескольких секунд.

Cylus обеспечивает максимальную эксплуатационную совместимость

---

[1] Deep Packet Inspection (сокр. DPI) – технология проверки сетевых пакетов по их содержимому с целью регулирования и фильтрации трафика, а также накопления статистических данных. В отличие от брандмауэров, Deep Packet Inspection анализирует не только заголовки пакетов, но и полезную нагрузку.

[2] Компания проводит симуляцию кибератак. «Красная команда»выступает в роли хакеров, в то время, как «синяя» осуществляет мониторинг работы решения CylusOne.

(интегрируется как в подвижной состав, так и в инфраструктуру) при одновременной защите стационарных и подвижных компонентов в поездах. Кроме того, комплексный подход компании позволяет клиентам взаимодействовать не с несколькими, а с одним поставщиком решений для обеспечения кибербезопасности на железнодорожном транспорте.

В середине декабря 2021 года представители Cylus объявили, что стартап закрыл очередной раунд финансирования суммой 30 млн долларов – капитализация компании таким образом выросла до 57 млн долларов. Как отмечает генеральный директор Cylus Амир Левинталь, компания направит эти средства на совершенствование своего продукта, а также на расширение его применения на рынках Северной Америки, Европы и Азиатско-Тихоокеанском региона.

«За последние несколько лет мы стали свидетелями масштабной волны цифровизации в железнодорожной отрасли. Несмотря на то, что это очень позитивная тенденция, она ведет к экспоненциальному расширению возможностей хакеров, которые могут совершать атаки на железнодорожный транспорт, входящий в перечень объектов критически важной инфраструктуры. Это может привести к очень серьезным последствиям», – заявил Гал Гиттер, партнер и управляющий директор Ibex Investors[3]. – Cylus решает эту проблему, предоставляя самую передовую и комплексную платформу кибербезопасности для операторов подвижного состава и инфраструктуры. Платформа Cylus уже используется многими ведущими мировыми железнодорожными компаниями, и мы считаем, что она станет стандартом для всей отрасли».

Источник: techcrunch.com, 15.12.2021 (англ. яз.),
по материалам компании Cylus (cylus.com),
craft.co, 20.12.2021

[3] Ibex Investors – американская инвестиционная фирма, нацеленная на чрезмерную доходность с помощью нишевых, некоррелированных, дифференцированных стратегий.