Максим Степченков (RuSIEM): Необходимо уметь слушать заказчика

Почему развеялся миф о том, что SIEM нужна только для готовых инфраструктур, а также о других трендах этого рынка «Б.О» рассказал Максим Степченков, совладелец компании RuSIEM



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

— Максим, SIEM-система сегодня для финансовых организаций — это must have или все же факультатив?

— Практически все рынки постоянно видоизменяются, а продукты, их составляющие, непрерывно совершенствуются. Если что-то в этом механизме остановилось, то в большинстве случаев этот рынок можно тихо-мирно хоронить. Сегмент SIEM-систем, я вас уверяю, напротив, активно развивается. Сюда приходят инвестиции, здесь осуществляются сделки по слиянию и поглощению, а также появляются стартапы.

Одним из мощных импульсов для развития, впрочем, как и для ИБ в целом, стал COVID-19 с его режимом самоизоляции и массовым уходом бизнеса в онлайн, а работников — на удаленный режим работы. Соответственно количество средств защиты информации, необходимых в новых условиях, существенно выросло. Хотя необходимо отметить, что и раньше SIEM-системы были востребованы, но новый виток их эволюции пришелся именно на этот период.

На сегодня тренд таков, что бизнес не очень-то стремится назад, в офлайн-режим, а лучшие ИБ-практики тех времен никто на свалку отправлять не хочет. Поэтому в IT-архитектуре современных финансовых компаний прочно закрепился такой компонент, как SIEM-система. Более того, условия кибервойны, в которой мы все находимся

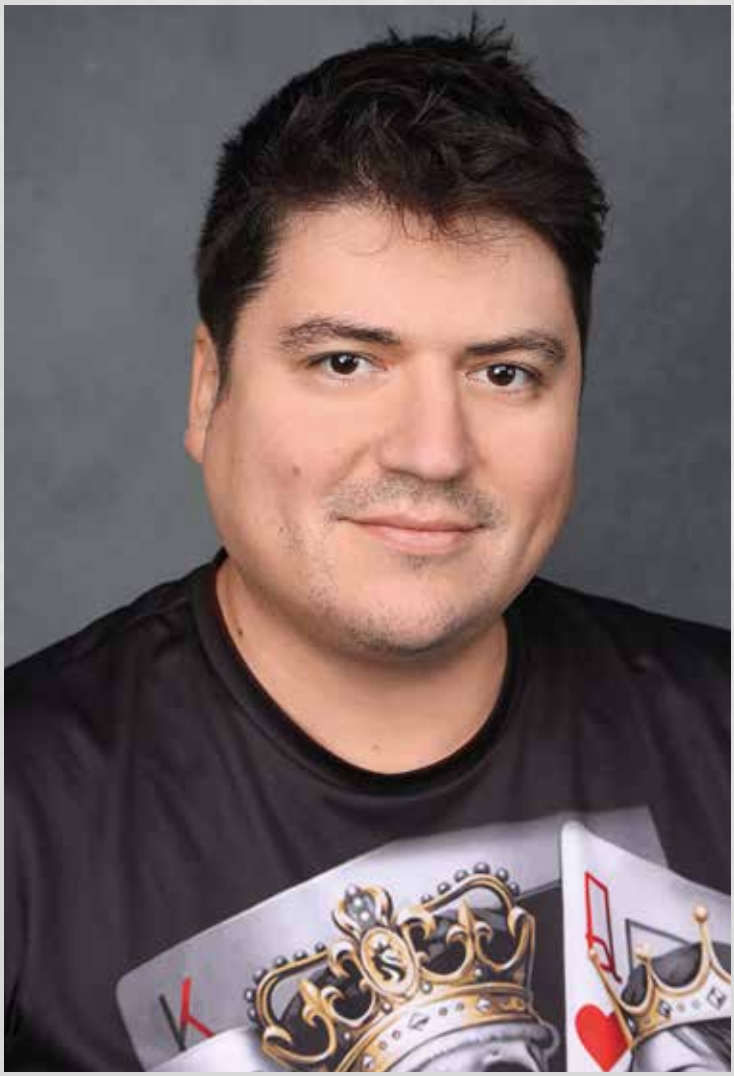


Фото: RuSIEM

с февраля 2022 года, привели к усилению нормативных требований и внимания к субъектам критической информационной инфраструктуры (КИИ), что способствует активному технологическому развитию отечественных решений для финансистов.

Добавлю к сказанному: нет ни одного нормативного документа в области ИБ, в котором было бы предписано обязательное использование SIEM-системы. Никто не запрещает альтернативные подходы к обеспечению ИБ. Тем не менее я считаю, что даже при наличии такой свободы выбора SIEM близка к тому, чтобы быть must have для организаций финансового сектора.

— Какие основные тренды на рынке и какие требования к системе предъявляют крупные, средние и малые банки?

— Ответ на этот вопрос надо начать с того, что после ухода западных аналитических агентств резко возросла роль такого менеджерского навыка, как умение слушать клиентов. Что касается нашей компании, то практически все наши специалисты собирают информацию от заказчиков: что происходит у них, а что у их коллег, а также в целом по рынку. Причем диалог идет на уровне как «технарей», так и менеджеров. Из компиляции этих данных становится понятно, куда именно движется рынок и какие тренды на нем присутствуют.

Одним из общих трендов, на который мы ориентируемся, стал кадровый голод как у разработчиков, так и у заказчиков из среднего и малого бизнеса, эксплуатирующих систему. Есть и другие векторы. Путей решения, как нам видится, здесь несколько. Во-первых, включение в состав SIEM по умолчанию новых аналитических инструментов, например, на базе ИИ и ML, которые помогают справиться с недостатком компетенций и навыков у имеющихся сотрудников. Так, заказчик не может самостоятельно настраивать новые правила корреляций и обнаружения отклонений от паттернов, что не позволяет выявлять новые инциденты. SIEM-система — это не тот продукт, который один раз настроил и забыл. Наоборот, необходима постоянная ее донастройка. Во-вторых, всем сегодня предельно понятно: IT-инфраструктура и ИБ-инфраструктура не должны быть собраны из решений одного вендора. Это накладывает на разработчиков дополнительные требования к их продуктам, например к совместимости. В-третьих, завышение цен рядом вендоров на их продукты это тупиковый путь. И, наконец, благодаря повышению уровня ИБ-культуры развеялся миф о том, что SIEM нужна только для готовых инфраструктур. На самом деле это не так. Теперь требуется научиться делать наоборот, а это непросто. На этот вызов я отвечаю цитатой из мультфильма «Рататуй»: «Готовить может каждый, но лишь бесстрашные достигают величия!».

Что касается специфики организаций разных категорий, то с учетом сказанного о трендах остается наложить их на бизнес-требования, а также на финансовые и кадровые возможности. Всем известна триада ИБ: конфиденциальность, целостность и доступность. Банкам, например, важны все три компоненты, другим организациям — конфиденциальность и доступность. Поэтому надо выбрать то, что требуется именно в данной ситуации с учетом нормативных документов Банка России, а не гнаться за разрекламированными брендами с их заоблачными ценами.

Кроме того, для финансовых организаций очень важно строить архитектуру не столько под средства защиты информации, сколько под интеграцию с бизнес-приложениями. Например, для некоторых организаций антифрод немыслим без нее. Мне известно, что даже с 1С зачастую не осуществляется интеграция, а если она и есть, то на уровне простого логирования входа в систему и отслеживания неудачных попыток входа пользователей. Эта ситуация требует изменений!

— Под брендом RuSIEM разрабатывается линейка продуктов. В чем их особенности?

— В первую очередь мы движемся в сторону комплементарных продуктов. Достаточно много клиентов хотят иметь такие решения, которые дополняли бы собой ядро системы в виде SIEM. В их числе, например, EDR и система ИТ-мониторинга. Но учитывая то, что я говорил о недопустимости зависимости заказчика от одного вендора, мы точно не будем заниматься разработкой антивирусов или некоторых других решений, например межсетевых экранов. Наша ниша — продукты, дополняющие систему мониторинга.

— Насколько много заимствований сторонних компонентов с архитектурной точки зрения? Как найти оптимальный баланс между скоростью разработки и требованиями Реестра отечественного ПО?

— Наш базовый продукт, и мы этого не скрываем, изначально стартовал с open-source, однако позже был полностью переработан собственными программистами. Причиной этого стали архитектурные и прочие особенности кода, которые ограничивали возможности масштабирования и т.д. Но для выхода на рынок в то время это было оправдано. Однако для сопровождения и развития зрелого решения нужна собственная команда разработчиков. Да и для включения в Реестр отечественного ПО — это важное условие.

Второй вариант развития компании связан приобретением продуктов на рынке. Мы рассматриваем предложения стартапов, готовы к покупкам. Здесь в приоритете вопрос соотношения цена-качество, а также «горящие глаза» участников команды. С ними у нас есть о чем поговорить.

Наконец, третий вариант — это R&D в чистом виде. В нашем случае оптимальна пропорция 50:50 — в 50% случаев мы смотрим в сторону собственной разработки новых продуктов, т.е. R&D, а другие 50% посвящены приобретениям и коллаборации с другими нишевыми игроками.

С точки зрения технологий наш фокус находится в области микросервисной архитектуры по двум основным причинам. Первая из них — повышенная отказоустройчивость. Вторая — возможность разнесения микросервисов с одного сервера на их множество, что обеспечивает масштабирование и расширяемость функционала.

— Какова роль аналитических инструментов в дальнейшем развитии?

— Аналитика сейчас должна быть везде! Например, далеко не все могут позволить себе SOC с их экспертами, а расследовать и предотвращать инциденты ИБ им необходимо. Для крупных банков, где кадровая проблема не столь остра, аналитические инструменты являются дополнительной конкурентной фишкой вендора.

А о второй причине я говорил выше — существует реальная потребность в том, чтобы часть компетенций и экспертизы производителя была «зашита» им в систему. Это помогает поддерживать SIEM с точки зрения настроек «в полной боевой готовности» в любой момент времени без наличия квалифицированного персонала. Б.О

реклама