

# Российская система для полного цикла управления уязвимостями

Рассказывает руководитель департамента перспективных проектов компании "Фродекс" **В.А.Михайлов**

DOI: 10.22184/2070-8963.2024.119.3.70.71



4 апреля на форуме "ТЕРРИТОРИЯ БЕЗОПАСНОСТИ 2024: все про ИБ" в Москве компания "Фродекс", один из ведущих российских разработчиков новых технологий и продуктов кибербезопасности, представила систему управления уязвимостями и анализа защищенности активов ИТ-инфраструктуры Vulns.io Enterprise Vulnerability Management (Vulns.io Enterprise VM). Появление данного уникального для российского рынка продукта выводит компанию на новый уровень. На полях форума о новой многофункциональной системе корреспонденту "ПЕРВОЙ МИЛИ" рассказал руководитель департамента перспективных проектов ООО "Фродекс" В.А.Михайлов.

## Каковы основные направления деятельности компании "Фродекс"?

Компания создана в 2011 году выходцами из "Уралсиба", которые создали полноценную систему информационной безопасности этого одного из крупнейших банков России. Первым флагманским решением "Фродекс" стала антифрод-система (система обнаружения мошеннических платежей) для юридических лиц FraudWall, защищающая банки и их клиентов от кражи средств злоумышленниками. Продукт позволяет контролировать легитимность платежей, постоянно совершенствуется в связи с появлением новых видов мошенничества.

Затем появились продукты-спутники FraudWall, которые "закрывали" появляющиеся запросы со стороны банков, в частности, по обеспечению требований регуляторных органов. Сегодня наши решения в промышленном режиме эксплуатируются примерно в 100 банках.

Компания предоставляет услуги аудита требований ИБ, управления рисками, технического анализа защищенности. В частности, наши специалисты осуществляют пен-тесты – анализ защищенности инфраструктуры, который

представляет собой попытку взлома компьютерной сети или ее сегмента, санкционированную заказчиком.

## Расскажите о новом продукте компании – Vulns.io Enterprise VM. В чем его уникальность?

Расширяя спектр своих услуг, несколько лет назад "Фродекс" в партнерстве с компанией "Инженерный центр систем безопасности" запустил коммерческий SOC – Security Operations Center (Центр мониторинга информационной безопасности). Одной из его ключевых функций является сканирование ИТ-инфраструктуры заказчиков и выявление уязвимостей. Накопив определенную экспертизу в данной сфере, мы увидели, что рынок нуждается в таком отечественном продукте для больших инфраструктур (более 10 тыс. активов). В то время были зрелые подобные решения от ряда зарубежных компаний, в частности Tenable, Rapid7. Аналогов от российских разработчиков не было и мы поставили себе задачу создать продукт, который может конкурировать с лучшими зарубежными разработками. И это было правильное решение – после февраля 2022 года западные поставщики VM-систем ушли с российского рынка.

В процессе разработки нами была существенно доработана технология, созданная изначально для SOC. При увеличении числа активов актуализировать защищенность инфраструктуры становится все сложнее – увеличивается объем данных и время их обработки. До определенного предела этот рост можно компенсировать, наращивая мощность вычислительного оборудования, но рано или поздно все равно встает вопрос горизонтального масштабирования. При создании нового продукта нам удалось ускорить процесс сканирования инфраструктуры.

При необходимости обработки огромных объемов данных Vulns.io Enterprise VM может быть развернута в кластере с использованием оркестратора Kubernetes. Эта возможность позволяет гибко настроить масштабирование компонентов продукта, распределить их по разным узлам кластера, в отдельных случаях можно настроить автоматическое выделение дополнительных ресурсов.

Новая система предлагает инструменты для всего цикла управления уязвимостями: выявление уязвимостей операционных систем и установленного ПО серверов и рабочих станций, а также сетевых устройств и docker-образов (в реестрах или на хостах); приоритизация уязвимостей по различным подходам, включая методику ФСТЭК; патч-менеджмент – обновление уязвимого ПО; контроль устранения уязвимостей, позволяющий наглядно отобразить изменение состояния актива.

Полученная информация анализируется с использованием имеющейся в системе базы данных уязвимостей. Процесс происходит асинхронно и параллельно. Это позволяет проводить сканирование с очень высокой скоростью (доли секунды на актив при одновременном сканировании большого количества активов) с минимальным использованием сетевого трафика.

#### **В чем отличие нового продукта "Фродекс" от других VM-решений, представленных сегодня на российском рынке?**

После ухода из нашей страны западных вендоров некоторые российские компании, которые занимаются продуктами в сфере ИБ, стали дополнять свои линейки VM-решениями. Как правило, это компании, предлагающие для предприятий целые экосистемы информационной безопасности. Мы же сконцентрировались именно на системе управления уязвимостями и научились делать это, как считаем, очень хорошо. По достигнутым скорости и возможности сканировать огромное количество объектов наше решение сегодня не имеет себе равных.

Следует добавить, что решение Vulns.io VM успешно функционирует как на Windows и Linux, так и на российских операционных системах, сканирует их на уязвимости,



Новый продукт "Фродекс" вызвал большой интерес участников форума

инвентаризирует и в целом выполняет весь спектр задач по управлению уязвимостями. Уже сертифицирована его совместимость с ОС: РЕД ОС Муром 7.3; ALT Linux K9.1, 10; РОСА Кобальт 7.9; Astra Linux Special Edition 1.6 и Astra Common Edition Orel 2.12.

#### **Представляет ли ваше решение интерес для операторов связи?**

Конечно, продукт универсален. Телекоммуникационные компании обладают разветвленной ИТ-инфраструктурой. Кроме того, в выявлении уязвимостей нуждается и сетевое оборудование, тем более поставленное вендорами, ушедшими из России. Например, мы можем подсказать, какое оборудование надо заменить в первую очередь. Уже осуществлены пилотные проекты для ряда крупных операторов связи.

#### **В каких направлениях компания планирует развивать Vulns.io Enterprise VM дальше?**

Мы планируем активно развивать направление поставки нашего VM-продукта как услуги – VMaaS, так как ощущаем к себе доверие многих компаний. В этом случае заказчику не надо размещать продукт на своих мощностях, осуществлять его поддержку. До сих пор в России такой сервис не предоставлялся, предлагалось сканирование только внешнего периметра предприятия.

В наших планах добавить в систему анализ уязвимостей исходного кода. Будем также развивать направление комплаенса – проверки того, насколько правильно сконфигурирована та или иная система или приложение, начиная от паролей и заканчивая настройкой баз данных.

**Спасибо за интересный рассказ.**

С В.А.Михайловым беседовал С.А.Попов