VULNERABILITY MANAGMENT SERVICES

SOLIDLAB VMS — ИНТЕЛЛЕКТУАЛЬНАЯ ПЛАТФОРМА ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

Решение поможет построить полноценный процесс управления уязвимостями.

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

- Определение поверхности атак на периметре
- Инвентаризация ИТ-ресурсов и их компонентов
- Проверка стойкости учетных записей пользователей
- Выявление и блокировка фишинговых ресурсов и утечек
- Проведение единоразового сканирования
- Анализ защищенности веб-приложений
- Контроль функций API и исполняемых JS-скриптов
- Управление уязвимостями и патч-менеджмент

ПРЕИМУЩЕСТВА ПЛАТФОРМЫ

Максимально широкий набор инструментов

Решение включает в себя полный набор инструментов, необходимый для решения задач инвентаризации и управления уязвимостями.

Managed Services вместо SaaS

Аналитики SolidLab осуществляют полное сопровождение решения, включая валидацию обнаруженных недостатков и тонкую настройку решения под задачи заказчика.

Дополнительный фокус на WEB

Интеграция с SolidWall DAST для глубокого анализа веб-приложений и выявления уязвимостей.

Гибкая архитектура

Платформа является модульной, что позволяет выбирать набор используемых компонентов. Поддерживается подключение инструментов заказчика и управление через API.

Единый интерфейс мониторинга

Удобный веб-интерфейс для управления сервисами и найденными уязвимостями.

Полная поддержка импортозамещения

Платформа не использует проприетарные зарубежные продукты. Существенная часть платформы – это компоненты собственной разработки. Решение включено в реестр отечественного ПО.

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ ПЛАТФОРМЫ

Снижение числа критичных уязвимостей ↓

Повышение скорости реагирования на уязвимости ↑

Снижение количества ложных срабатываний ↓

Учет и оптимизация использования ресурсов ↑

ОСНОВНЫЕ КОМПОНЕНТЫ РЕШЕНИЯ

AVM **Application Vulnerability Manager**

Динамический сканер анализирует веб-приложения и их компоненты, находит уязвимости, а также точки входа для их эксплуатации, используя заданные алгоритмы.

EVM/LVM **External/Local Vulnerability Manager**

Автоматизированное сканирование внешнего периметра и локальной сети без использования агентов. Предназначен для поиска известных уязвимостей на основании анализа данных о портах, сервисах и службах.

DRP **Digital Risk Protection**

Контроль нарушений, связанных с неправомерным использованием бренда компании в сети интернет.

EASM **External Attack Surface Management**

Модуль изучения поверхности атаки ИТ-инфраструктуры компании из открытых источников, включая активный и пассивный поиск поддоменов, сбор данных об IP-адресах.

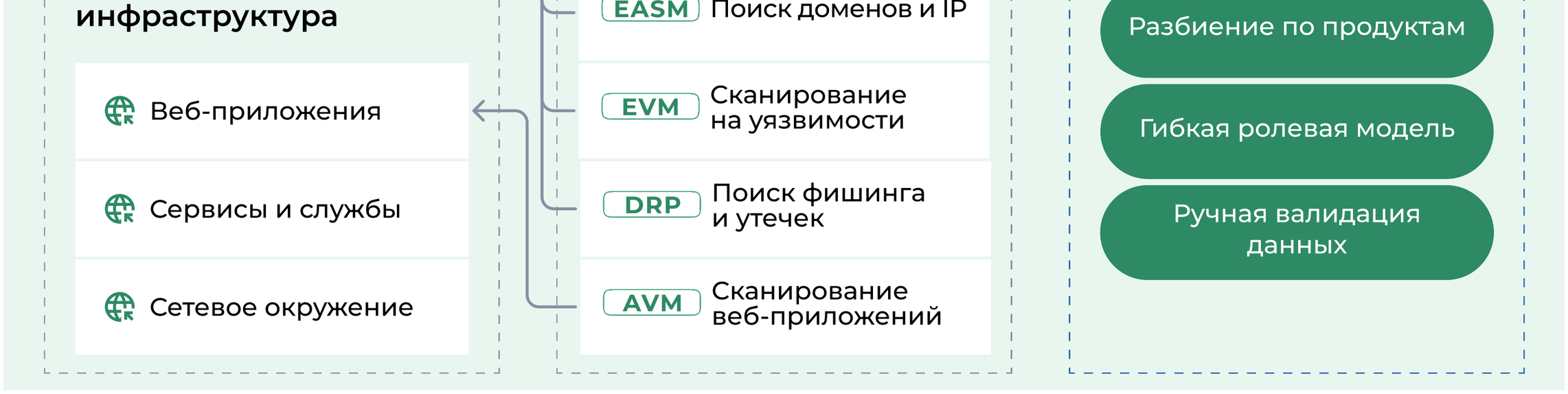
HVM **Host Vulnerability Manager**

Агентский модуль поиска уязвимостей. Устанавливается на узлы заказчика, собирает информацию об аппаратных и программных ресурсах, находит уязвимости в ИТ-инфраструктуре. Минимальные требования к установке. Контроль ПО на хостах.

UAT **User Account Testing**

Модуль тестирования парольной политики компании.

ПРИНЦИП РАБОТЫ ПЛАТФОРМЫ



ПРОФЕССИОНАЛЬНЫЕ СЕРВИСЫ

- Получение общей информации о хосте
- Поиск точек входа в веб-приложение
- Консультации по устранению недостатков
- Валидация найденных недостатков
- Тонкая настройка инструментов анализа
- Подготовка аналитических отчетов
- Реагирование на обнаруженные уязвимости

СОЗДАНИЕ ОТЧЕТОВ

Оценка уязвимостей

Процесс анализа и определения приоритетов уязвимостей, направленный на сокращение времени на принятие решений по критичным уязвимостям, что способствует снижению рисков и обеспечению безопасности системы.

Менеджмент уязвимостей

Возможность строить отчеты в разных разрезах, обеспечивая детальный анализ и визуализацию данных для принятия обоснованных решений и улучшения безопасности систем.

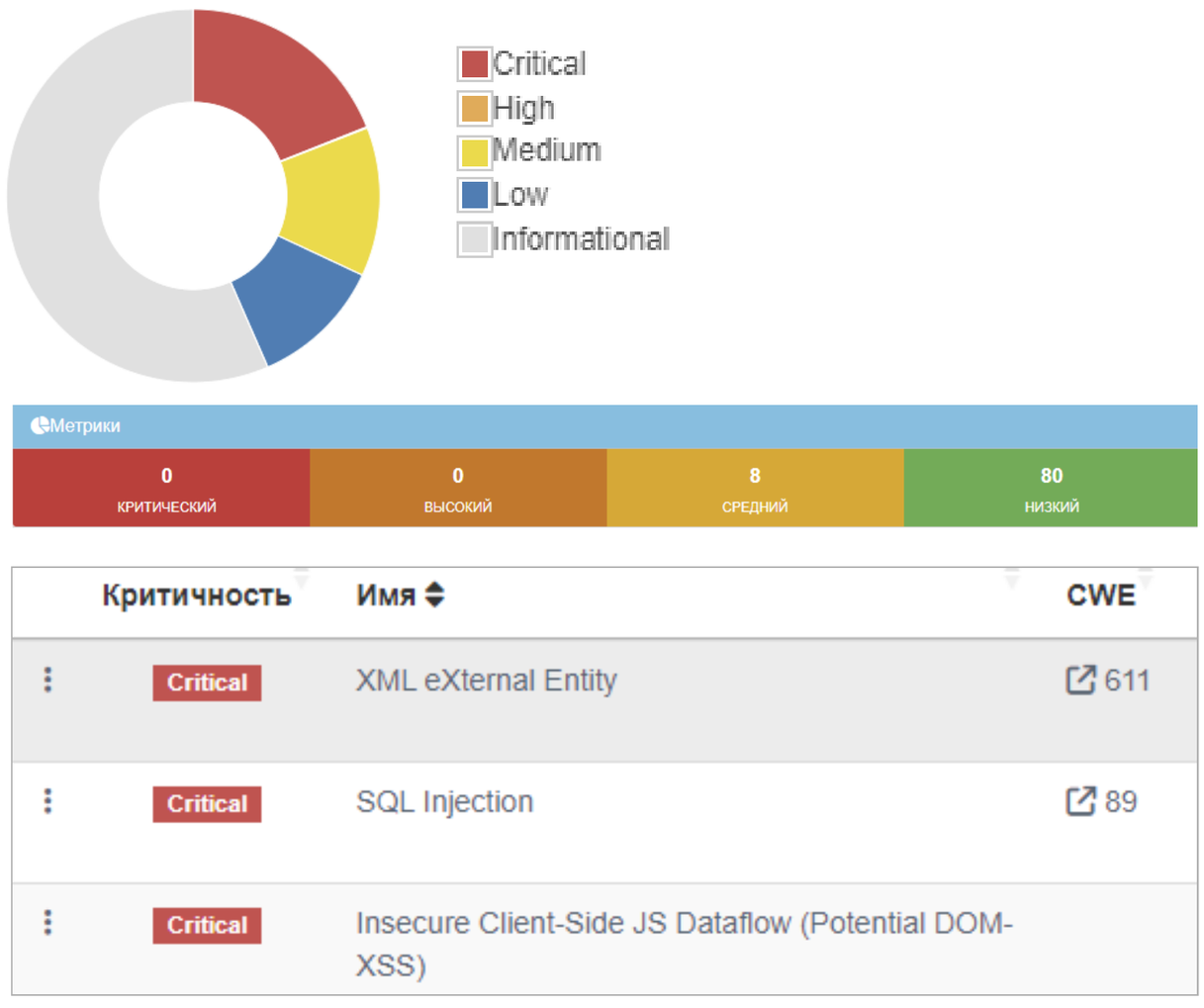
Дифференциальные отчеты

Функционал для сравнительного анализа данных предыдущих сканирований и демонстрации изменений. Помогает контролировать устранение уязвимостей и изменения в инфраструктуре.

Простые фильтры

Использование простых фильтров вместо сложного языка запросов, упрощающих процесс фильтрации данных и улучшения доступности информации.

ПОЛНОФУНКЦИОНАЛЬНЫЙ ИНТЕРФЕЙС



УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

Отслеживание изменений конфигурации и ПО

Возможность непрерывного сканирования устройства.

Сканирование агентским и безагентским способами

Анализ безопасности с использованием установленных агентов или безагентский подход, без дополнительных установок.

Выявление недостатков разработки

Проверка безопасности приложений на всех этапах эксплуатации для выявления скрытых уязвимостей.

Сканирование веб-приложений

Поиск уязвимостей в веб-приложениях по методологиям OWASP TOP 10, включая анализ точек ввода, JavaScript и SSRF.

Выявление уязвимых конфигураций

Анализ конфигураций систем на наличие слабых мест, которые могут быть использованы для атак.

Классификация, категоризация активов

Определение и приоритизация активов по критичности для эффективного распределения ресурсов безопасности.

Обнаружение слабых паролей

Проверка на наличие слабых и повторно используемых паролей, улучшение аутентификации.

Поддержание методики ФСТЭК

В DefectTracker реализованы все необходимые инструменты для реализации процесса, описанного в ФСТЭК.

МЕТОДЫ СКАНИРОВАНИЯ

Баннерные проверки

Сканер определяет версии ПО и ОС, а затем сверяет их с данными из внутренней базы уязвимостей. Ими могут быть баннеры сервиса, журналы, ответы приложений и их параметры, а также формат.

Единоразовое сканирование

Единовременное сканирование поверхности атак с использованием адаптированных модулей, соответствующих задачам разового анализа защищенности (пентест) для анализа инфраструктуры и приложений.

Template Scan

Инструмент для создания шаблонных сканирований и проверок веб-приложений на уязвимости, в том числе конфигурационных ошибок. Настроенные шаблоны по уязвимостям.

Преимущества:

- Полнота описания уязвимостей
- Классификация уязвимостей
- Централизованное управление и обновление сенсоров

ИСТОЧНИКИ И БАЗЫ УЯЗВИМОСТЕЙ

Преимуществом решения является широкий охват источников информации

Мы оперативно получаем самую актуальную информацию об уязвимостях, обеспечивая своевременное обновление данных и быстрый доступ к критически важной информации для выявления угроз.

Источники информации об уязвимостях

GitHub · NIST · CVE Common Vulnerabilities and Exposures · Microsoft · ATTACKERKB · OSV Open Source Vulnerabilities · ФСТЭК · Exploit Database · VulnDB · База SolidVMS

ТАРИФЫ СКАНИРОВАНИЯ

Тариф Т1

Базовое решение

- Анализ внешнего периметра
- Внутреннее агентское сканирование
- Рекомендации по устранению угроз

Тариф Т2

Полнофункциональное решение

- Анализ внутренней сети
- Полный состав модулей
- Валидация недостатков и реагирование
- Интеграция с SIEM/SOAR
- Тонкая настройка параметров запуска сканеров

Тариф Т3

Кастомизированное решение

- Расширенный функционал управления сканированием
- Интеграция с тикет-системой заказчика
- Управление решением через API
- Кастомные технические и аналитические отчеты

МЕТОДЫ ЛИЦЕНЗИРОВАНИЯ

Активные IP-адреса

EVM/LVM — Анализ уязвимостей ИТ-инфраструктуры

Цели сканирования

AVM — Анализ защищенности веб-приложений

Информационные системы

UAT — Тестирование стойкости УЗ

Число хостов

HVM — Агентское сканирование

Бренд компании

DRP — Выявление нарушений бренда

Домены второго уровня

EASM — Изучение поверхности атаки

125040, г. Москва, ул. Вавилова, д. 47А

+7 (499) 705-76-57

info@solidlab.ru

Группа компаний SolidLab работает в области информационной безопасности более 10 лет, защищая организации от киберугроз, предупреждая атаки, минимизируя риски финансовых и репутационных потерь. SolidLab предлагает полный комплекс услуг: от пентестов до защиты приложений, реагирования на инциденты и организации процессов SDLC.