OFFENSIVE SECURITY

АНАЛИЗ ЗАЩИЩЕННОСТИ ПРИЛОЖЕНИЙ И ИТ-ИНФРАСТРУКТУРЫ

APPSEC

- Приложения с AI/ML
- Веб-приложения Серверное API
- Анализ кода
- Мобильные приложения

INFRASEC

- Внешний периметр
- Внутренняя сеть и Wi-Fi
- Окружение: k8s, контейнеры
- Облачные среды
- Active Directory

НАШИ ПРЕИМУЩЕСТВА

- **Контроль качества на каждом этапе проекта**
  Зрелое управление проектами и внутренний аудит качества анализа
- **Собственные инструменты и методики анализа**
  Используем внутренние разработки и наработанный практический опыт
- **Адаптация под специфику проекта**
  Методика тестирования и рекомендации учитывают контекст конкретного приложения/инфраструктуры
- **Ручной анализ и реальные сценарии атак**
  Проверяем бизнес-логику и нестандартные векторы атак, а не только «классический чек-лист»
- **Непрерывное повышение экспертизы за счет R&D**
  Команда регулярно участвует в исследованиях безопасности, CTF и bug bounty
- **Прозрачная работа с командой заказчика**
  Регулярные статусы, оперативное уведомление о критичных рисках, обсуждение результатов

ЛЮБЫЕ ФОРМАТЫ ПРОЕКТОВ ПОД ВАШИ ТРЕБОВАНИЯ

- Комплексный анализ
- Тестирование методами «черного ящика», «серого ящика», «белого ящика»
- Red Team/Киберучения
- Физический пентест, проверка СКУД, социальная инженерия

ПОЛУЧАЕМЫЕ РЕЗУЛЬТАТЫ

Выявление критичных уязвимостей до злоумышленника

Проверка эффективности текущих мер защиты

Обоснованные рекомендации по повышению защищенности

Повышение зрелости процессов ИБ, ИТ, разработки

ЦЕЛИ АНАЛИЗА ЗАЩИЩЕННОСТИ

Защита бизнес-процессов, клиентов и данных

Автоматизация бизнес-процессов и использование AI расширяет площадь возможных атак. Анализ защищенности позволяет вовремя идентифицировать и отреагировать на риски до реализации неприемлемых сценариев

Оценка эффективности ИТ и ИБ процессов

Анализ защищенности позволяет получить практическую оценку таких процессов, как управление учетными записями и доступом, управление обновлениями, сетевой сегментацией, оценку мониторинга и реагирования и т.д.

Оценка процессов разработки ПО и встраивания AI

Анализ прикладных компонентов методом «белого ящика» помогает выявить как точечные, так и системные проблемы на уровне архитектуры, процессов, встраивания сторонних компонентов и интеграций с внешними сервисами

ЧТО ВХОДИТ В ОТЧЕТ?

- Полный перечень выявленных уязвимостей
- Описание подтвержденных защитных мер
- Аналитическая оценка критичности уязвимостей, CVSS
- Детальные рекомендации по исправлению
- Отдельное резюме для руководства
- Демонстрация реализуемости атак и их цепочек
- Приложения с техническими деталями: PoC, журналы действий, снимки экранов и т.п.

ПОЧЕМУ МЫ?

Множество CVE
Google, Apple, Microsoft, VMWare и др.

Более 700+ успешных проектов
по анализу защищенности

Наличие сертификатов
OSWE, OSEP, OSCP, CRTP и пр.

Отражение нашей экспертизы
Статьи и конференции, победы в CTF, благодарности от компаний

Более 15 лет работы
в направлении анализа защищенности (Offensive Security)

Более 30 экспертов
в области практического анализа защищенности

98 % доля лояльных заказчиков
после завершения проектов

*80 пунктов согласно индексу NPS

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.