

СОВРЕМЕННЫЕ ПОДХОДЫ НЕУЯЗВИМОСТИ

ALPHA SYSTEMS



Сколково



ФСТЭК России



Реестр Российского ПО

Спикер:

CEO - Игорь Смирнов

ПРОБЛЕМЫ И ПОСЛЕДСТВИЯ

КОМПАНИИ ПЛОХО «УПАКОВАНЫ СЗИ»? НЕТ, ДЕЛО НЕ В ЭТОМ!

ALPHASYSTEMS.GROUP

8-800-505-64-54

1

НЕУЧТЕННЫЕ ИТ-АКТИВЫ
И ПУБЛИКАЦИИ В
ИНФРАСТРУКТУРЕ

Встречаются в 90% компаний, является источником более 60% атак.

2

ОТСУТСТВИЕ
РЕГУЛЯРНОГО АНАЛИЗА
ИТ-ИНФРАСТРУКТУРЫ

Скорость изменения ИТ ландшафта в компаниях достигает более 10% за 1 месяц.

3

НЕДООЦЕНКА УРОВНЯ
КРИТИЧНОСТИ НАЙДЕННЫХ
УЯЗВИМОСТЕЙ

Более 30% критических уязвимостей подразумевают легкую механику реализации.

4

ДОСТУПНОСТЬ
ИНСТРУМЕНТОВ И ПРОСТОТА
ОРГАНИЗАЦИИ АТАК

Низкая стоимость и размещение инструментария в открытом доступе.



ПРИМЕРЫ ИНЦИДЕНТОВ


ALPHASYSTEMS.GROUP

8-800-505-64-54

Провайдер ДОМ.РУ (dom.ru)

- Несанкционированный доступ, удаление данных.
- Получен доступ к инфраструктуре и камерам видеонаблюдения.

 Время простоя 24 часа.

 Ущерб: **БОЛЕЕ 165 МЛН.РУБ.** недополученной выручки (исходя из официальных данных о выручке сервиса dom.ru)


 Восстановление инфраструктуры как прямые издержки.

Деловые линии и Пони Экспресс (dellin.ru и ponyexpress.ru)

- Отказ в обслуживании.
- Атака на ресурсы и приложения.

 Время простоя 24 часа.


 Ущерб: **БОЛЕЕ 170 МЛН.РУБ.** недополученной выручки.

 Восстановление мощностей.

Перекресток (perekrestok.ru)

- Отказ в обслуживании.
- Атака на сайт и приложение.


 Время простоя более 48 часов.

 Ущерб: **ПОРЯДКА 384 МЛН.РУБ.** недополученной выручки (исходя из официальных данных о выручке сервиса vprok.ru)

Система контроля проезда (platon.ru)

- Отказ в обслуживании.
- Системы взимания платы выведены из строя.

 Время простоя более 5 дней.

 Ущерб: **ПОРЯДКА 480 МЛН.РУБ.** государственный бюджет недополучил сборов с оплаты проезда.

ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ СЕЙЧАС

ALPHASYSTEMS.GROUP

8-800-505-64-54

01

УЧЕТ ИТ-АКТИВОВ



02

УПРАВЛЕНИЕ
УЯЗВИМОСТЯМИ



03

ОТЧЕТНОСТЬ



УЧЕТ АКТИВОВ

ВСЕ В РУЧНОМ РЕЖИМЕ

ALPHASYSTEMS.GROUP

8-800-505-64-54

01

Определить в каком
состоянии процесс сейчас

02

Сформировать требования
и регламенты по
управлению и учёту
ИТ-активов

03

Аудит парка устройств и
формирование реестров

04

Оценка уровня
безопасности и
соответствие требованиям

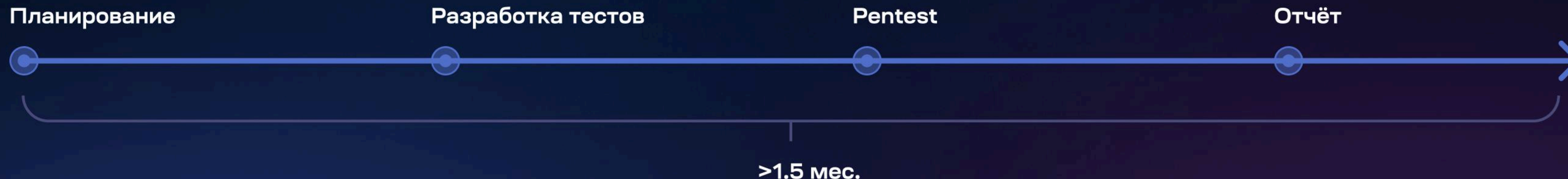


УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

ALPHASYSTEMS.GROUP

А МОЖЕТ МОЖНО АВТОМАТИЗИРОВАТЬ ?

8-800-505-64-54



СЛОЖНОСТИ BLACK BOX

1. Стоимость – от 1,5 млн руб.*
2. Сроки – от 1 месяца
3. Периодичность проведения – раз в квартал
4. Поиск уязвимостей происходит до первого «пробития» инфраструктуры

СЛОЖНОСТИ WHITE BOX

1. Стоимость – от 2,5 млн руб.
2. Сроки – от 1,5 месяцев
3. Периодичность проведения – 2 раза в год
4. Результаты быстро устаревают, так как постоянно меняется ИТ-ландшафт

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Результаты сильно зависят от качества подрядчика оказывающего услугу

* Банки и НКО обязаны проводить Pentest ежегодно, согласно положению 683-П ЦБ РФ

** Промышленные предприятия и объекты критической информационной инфраструктуры обязаны раз в год проводить Аудиты в соответствии с 187-ФЗ РФ

ОТЧЕТНОСТЬ

ALPHASYSTEMS.GROUP

8-800-505-64-54

ОСНОВНЫЕ СЛОЖНОСТИ:

- Огромные «простыни» неструктурированных данных
- Недолгий «срок жизни» отчетов
- Нет необходимой и достаточной информации
- Скорость подготовки и структурирования отчетов



РЕШЕНИЕ ЕСТЬ - ИБ ЭТО ПРОЦЕСС

ГОНКА НЕ ВООРУЖЕНИЙ, А МОЗГОВ!

ALPHASYSTEMS.GROUP

8-800-505-64-54



VULNERABILITY AUDITOR

ЗАМЕНА BLACKVOX И НОВЫЙ ПОДХОД К УПРАВЛЕНИЮ
УЯЗВИМОСТЯМИ

 **AlphaSense**

Системы класса Vulnerability Management (VM)



01

Аудит периметра,
Web компонентов,
сред контейнеризации

02

Полная инвентаризация
ИТ-активов

03

100% контроль изменений
ИТ-инфраструктуры

04

Автоподбор и проверки эксплойтов,
SQL инъекций, тестирование WAF

05

Кастомные ролевые отчеты

ASSET AUDITOR ALPHASYSTEMS.GROUP

ЗАМЕНА WHITEVOX И НОВЫЙ ПОДХОД К УПРАВЛЕНИЮ
ИТ-АКТИВАМИ 8-800-505-64-54

 **InfraRed**

Системы класса Asset Management (AM)



ТЕХНОЛОГИЯ

ALPHASYSTEMS.GROUP

8-800-505-64-54



ПЕРВОЕ В СВОЕМ РОДЕ РЕШЕНИЕ

применяющее ИИ для аудита и оценки защищённости ИТ-активов

ЕДИНСТВЕННОЕ РЕШЕНИЕ

с технологией обнаружения и подбора сценариев обхода WAF

МАКСИМАЛЬНЫЙ УРОВЕНЬ АУДИТА

внешний и внутренний периметры, WEB-приложения, среды контейнеризации

АВТОМАТИЧЕСКАЯ ФУНКЦИЯ

подбора и проверки действующих эксплойтов, SQL инъекций для WEB

УНИКАЛЬНАЯ ВОЗМОЖНОСТЬ

создания кастомных ролевых отчетов



Maven



node



О КОМПАНИИ ALPHA SYSTEMS

ALPHASYSTEMS.GROUP

8-800-505-64-54

10+

Опыт работы в кибербезопасности.

350+

Реализовано проектов по ИБ

16

Коммерческих внедрений (с июля 2023г.)

22

Пилотных проектов запущено



КОНТАКТЫ



info@alphasystems.group



8-800-505-64-54

НАМ ДОВЕРЯЮТ

ГИДРОМАШ



BAON

BIDZAAR



росинтер
ресторантс



ТРИНФИКО



ЕАПТЕКА



АКТИВ
БИЗНЕС
КОНСАЛТ



Внуково
МЕЖДУНАРОДНЫЙ АЭРОПОРТ



NETWELL