



CYBER FENCE
INTELLIGENCE SYSTEMS

УСЛУГИ ПО ПРОВЕДЕНИЮ ТЕСТОВ НА ПРОНИКНОВЕНИЕ

Резидент Особой экономической
зоны Калининградской области





ОПИСАНИЕ

**КОМПЛЕКСА УСЛУГ
ПО ТЕХНИЧЕСКОМУ АУДИТУ**



ГРУППЫ РАБОТ ПО ТЕХНИЧЕСКОМУ АУДИТУ **ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

01 **#BLUE**

СИНИЙ

Сбор разведанных, инвентаризация и мониторинг утечек информации.

02 **#RED**

КРАСНЫЙ

Тестирование защищенности компании, ее сетей, сотрудников и объектов с уклоном в сторону компьютерных атак хакеров.

03 #YELLOW

ЖЁЛТЫЙ

Глубокое изучение защищенности web-приложений заказчика, участвующих в бизнес-процессах.

04 #PURPLE

ФИОЛЕТОВЫЙ

Тестирование продуктов заказчика, как программного обеспечения, так и программно-аппаратных решений. Как при наличии исходных кодов приложения и документации, так и при полном их отсутствии. Нами используется подход “обратной разработки/обратной инженерии” для компилируемых решений и анализа уязвимостей и недокументированных возможностей.

04 #GREEN

ЗЕЛЁНЫЙ

Аналитика имеющейся информации, консалтинг на тему повышения уровня защищенности и обработке рисков ИБ.

ВИДЫ РАБОТ ПО ТЕХНИЧЕСКОМУ АУДИТУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

#BLUE

Инвентаризация ресурсов, активов
и IT-периметров

Мониторинг и поиск утечек информации

#PURPLE

Аудит исходных кодов продуктов
и систем

Аудит приложений и сервисов

Аудит мобильных приложений

#RED

Внешнее тестирование на проникновение сети
Внутреннее тестирование на проникновение сети
Внешний аудит информационной безопасности сети
Внутренний аудит информационной безопасности сети
Социо-технический аудит
Физическое проникновение
Аудит безопасности WiFi-сетей



#GREEN

Аудит бизнес-процессов и бизнес-логики
Аналитика полученных данных и выявленных угроз
Разработка рекомендаций
Исправление выявленных и недостатков
Сопровождение и поддержка



#YELLOW

Аудит web-приложений





МЕТОДИКИ И

ИНСТРУМЕНТАРИЙ



НАШИ МЕТОДИКИ

01.

Open Source Security
Testing Methodology
Manual (OSSTMM)
–Institute for Security and
Open Methodologies
(ISECOM)

02.

Guideline on Network
Security Testing – National
Institute of Standards
and Technology
(NIST) –800-42

03.

Information Systems
Security Assessment
Framework – Open
Information Systems
Security Group (OISSG)

04.

A Penetration Testing
Model –Federal Office
for Information
Security in Germany (BSI)

05.

Information Systems
Security Assessment
Framework (ISSAF)

ИНСТРУМЕНТАРИЙ

Собственные разработки:
PSL TargetSearch, PSL AccessAuditor

Nmap/Amap/SuperScan

Nikto

Netcat

Dsniff

Wireshark

Ettercap-ng

Cain

Hydra

Smtplib-user-enum

Cisco-auditing-tool

Ssldump

Sslscan

Sslsniff

Sslstrip

Sslcaudit

WebScarab

Sqlmap

Wafw00f

LanScope

NetScanner

XScan

OWASP-ZAP

Burp Suite

HP Web Inspect

Acunetix

Metasploit

Nessus

XSpider 7.8

MaxPatrol

И другое ПО...

WORK
HARD

СОБСТВЕННЫЕ РАЗРАБОТКИ

PSL TARGET SEARCH

Автоматизированная система рекогносцировки инфраструктуры и сбора технических сведений об исследуемом объекте (IT OSINT)

PSL MONITOR

Система непрерывного мониторинга внешнего периметра исследуемого объекта на предмет изменений инфраструктуры с точки зрения информационной безопасности (IT Security Change Monitoring)

СИСТЕМА АВТОМАТИЗАЦИИ ЭКСПЛУАТАЦИИ И ПОВЫШЕНИЯ ПРИВИЛЕГИЙ

Моделируемого злоумышленника во внутренней сети исследуемого объекта, а также автоматического составления матрицы доступа пользователей и сервисов внутреннего периметра исследуемого объекта



**КОМАНДА И
ОПЫТ**

НАШИ ПРЕИМУЩЕСТВА

- | Certified Information Security Manager
- | Certified Information Systems Security Professional
- | ISO 27001 Lead Auditor
- | OSCP (Offensive Security Certified Professional), ID OS-101-07385
- | OSCP (Offensive Security Certified Professional), ID OS-101-07276

03 КОМАНДА И ОПЫТ



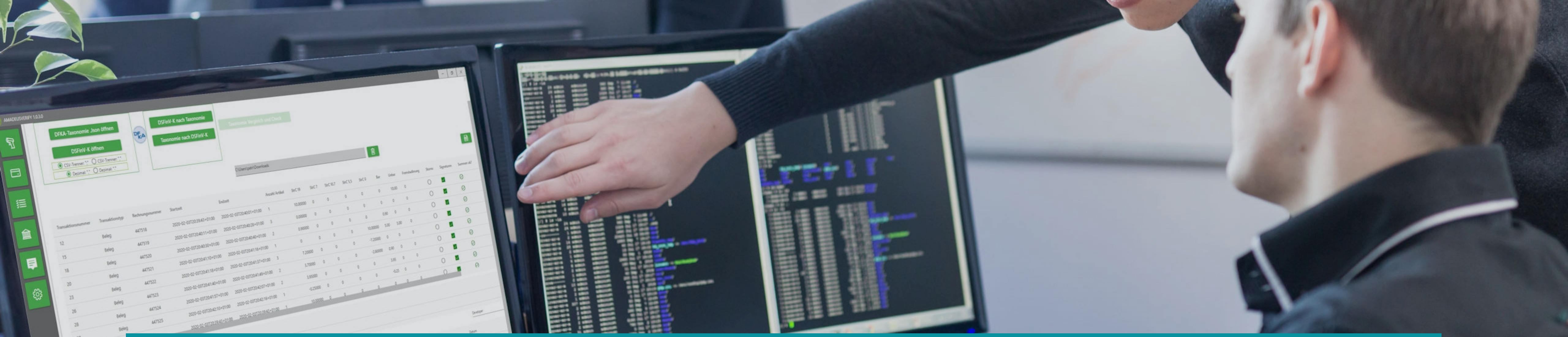
CYBER FENCE | INTELLIGENCE SYSTEMS

НАШИ ПРЕИМУЩЕСТВА

Проекты в госсекторе, в крупных и средних коммерческих заказчиках (выставочная деятельность, телеком, финансовый сектор, медиа, промышленность), заказчики со сложной филиальной структурой, международные компании.

Ведение комплексных проектов: от технического аудита и оценки защищенности до разработки проектных решений, внедрения подсистем ИБ и их аттестации по требованиям безопасности





Наши эксперты являются победителями публичных программ по поиску уязвимостей различных компаний:

AT&T BUG BOUNTY Q1-14

MICROSOFT

YANDEX

01 **ЛИЦЕНЗИИ ФСТЭК**

Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации № 3733 от 23.03.2020

Лицензия ФСТЭК на деятельность по разработке и производству средств защиты конфиденциальной информации № 1935 от 23.03.2020

02 **ЛИЦЕНЗИЯ ФСБ**

Лицензия ФСБ на осуществление разработки, производства, распространения шифровальных (криптографических) средств № 1163 от 19.11.2019

**СПАСИБО ЗА
ВНИМАНИЕ**

c-fence.com
