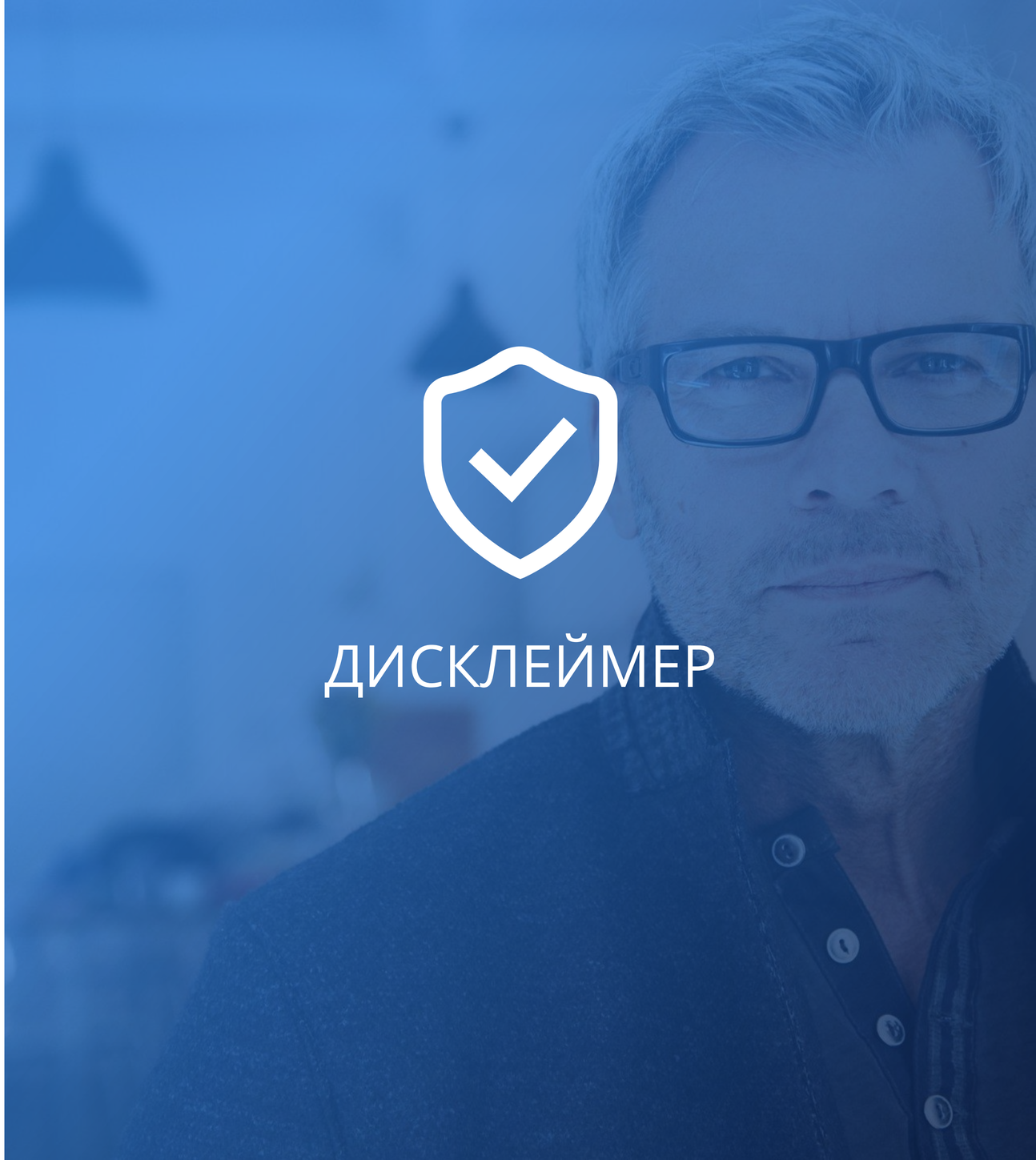
CYBER SECURITY

Описание комплекса услуг по аудиту
информационной безопасности.

ITERBI
consulting

© 2024, АО «АЙТЕРБИ»



ДИСКЛЕЙМЕР

СОДЕРЖАНИЕ

О КОМАНДЕ ITERBI

Описание опыта и сертификаты команды.

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ КОМАНДЫ

О КОМАНДЕ ITERBI

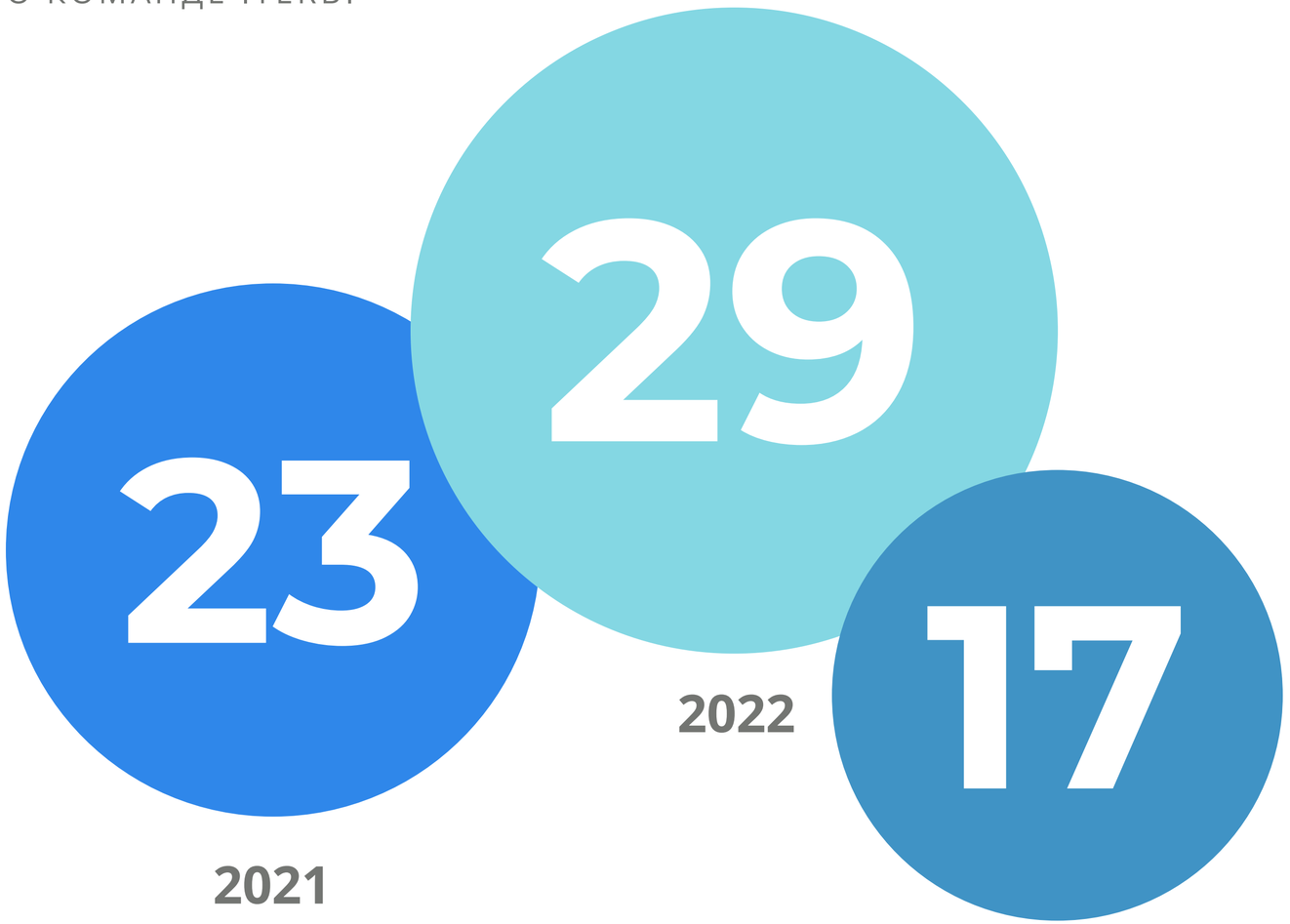
Команда ITERBI состоит из профессиональных специалистов по тестированию на проникновение, анализу защищенности и аудиту информационной безопасности. Мы оказываем полный спектр услуг в сфере аудита информационной безопасности компаний.

ЧЛЕНЫ КОМАНДЫ ОБЛАДАЮТ МЕЖДУНАРОДНЫМИ СЕРТИФИКАТАМИ

OSCP	Offensive Security Certified Professional - Offensive Security
BSCP	Burp Suite Certified Practitioner - PortSwigger WebSecurity Academy
CFE	Certified Fraud Examiner - Association of Certified Fraud Examiners
CIA	Certified Internal Auditor - The Institute of Internal Auditors
CISSP	Certified Information Systems Security Professional – ISC
CISM	Certified Information Security Manager - ISACA
OSWP	Offensive Security Wireless Professional - Offensive Security
OSWA	Offensive Security Web Assessor
CCNA	Cisco Certified Network Associate
CCNA SEC	Cisco Certified Network Associate Security
RHCE	Red Hat Certified System Administrator
CEH	Certified Ethical Hacker - EC-Council
CRT	CREST Registered Penetration Tester – CREST
CDP	Certified DevSecOps Professional

ОПЫТ КОМАНДЫ

О КОМАНДЕ ITERBI



КОЛИЧЕСТВО ПРОЕКТОВ

Строительные компании

Девелоперы

Электронные закупки

Маркетплейсы

СМИ

Виртуальные операторы связи

Регистраторы

Банки

Государственные порталы

Криптообменники

Страховые компании

НАПРАВЛЕНИЯ БИЗНЕСОВ

ПОДХОД К ПРОЕКТАМ

Методология для реализации проектов.

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

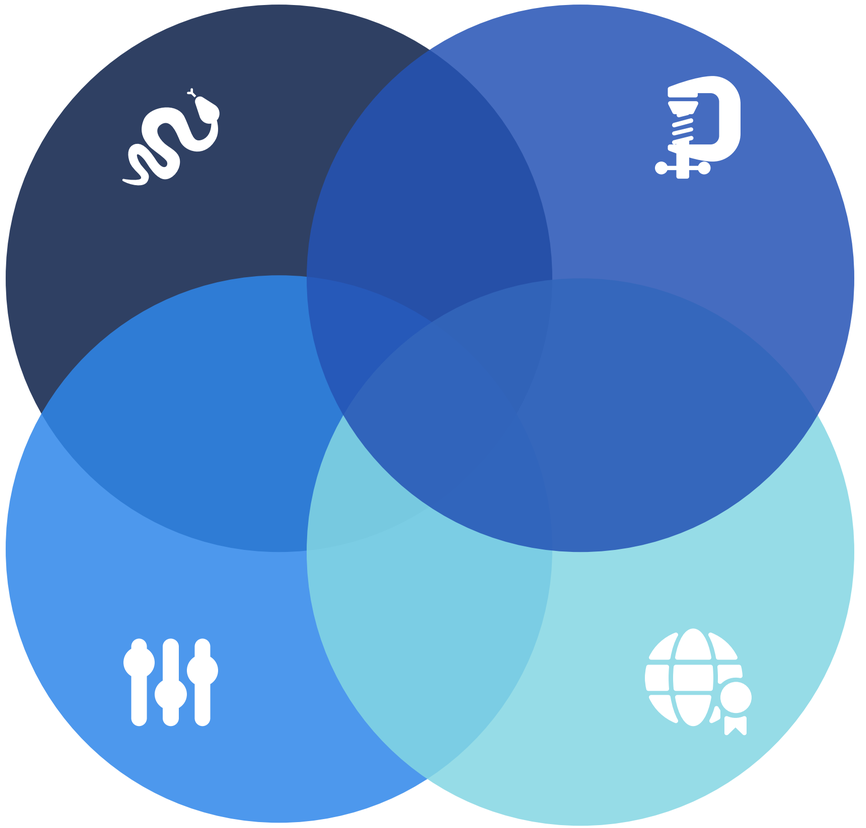
МЕТОДОЛОГИЯ

ПОДХОД К ПРОЕКТУ

ITERBI consulting

Гибкий подход

Гибкий подход на этапе технического пресейла.



Фиксированный подход

Реализации Проекта с фиксированным объемом работ, времени и результатов.

Внесение изменений

Возможность по необходимости внести корректировки в ходе реализации Проекта по согласованию сторон.

Профессиональная команда

Команда сертифицированных специалистов: OSCP, CEH, CRT, CISSP, CISM.

КАРТА ПРОЕКТОВ

Описание всех типов проектов.

ITERBI consulting

СОДЕРЖАНИЕ

ТИПЫ ПРОЕКТОВ

КАРТА ПРОЕКТОВ

Тесты на проникновение

RedTeaming и тестирование на проникновение.

Анализ защищённости

Анализ защищённости внешнего и внутреннего периметра, WEB – приложений.

Мобильные приложения

Анализ защищенности мобильных приложений Android и iOS.

Сотрудники

Социотехническое тестирование сотрудников.

Расследование инцидента

Расследование инцидента информационной безопасности.

Мониторинг

Непрерывный мониторинг защищенности внешнего периметра ИТ-инфраструктуры.

Разработка и продуктовая среда

Анализ защищенности инфраструктуры разработки и продуктовой среды. Внедрение и сопровождение SSDLC.

Нагрузочное тестирование

Нагрузочное тестирование веб-приложений.

ОЦЕНКА ЗАЩИЩЁННОСТИ

Анализ защищенности и тестирование на проникновение.

КАРТА ПРОЕКТОВ

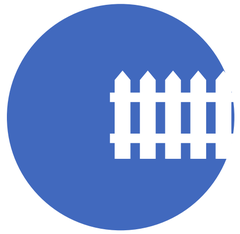
ITERBI consulting

СОДЕРЖАНИЕ

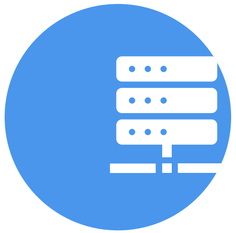
ВИДЫ ПРОЕКТОВ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ

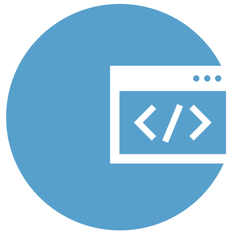
АНАЛИЗ ЗАЩИЩЕННОСТИ И ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ



Внешнего периметра



Локальной инфраструктуры



Отдельных веб-приложений

Беспроводных сетей

Мобильные приложения

ОЦЕНКА ЗАЩИЩЁННОСТИ

Анализ защищенности и тестирование на проникновение внешнего периметра.

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ВНЕШНЕГО ПЕРИМЕТРА

МОДЕЛЬ НАРУШИТЕЛЯ

Внешний нарушитель – злоумышленник, имеющий доступ к информационной системе из сети Интернет, обладающий навыками подготовки и проведения атак на информационные системы. Выполняется методами черного (без определенных прав доступа) или серого ящика (с определенными правами доступа).

Для старта проекта нужно:

Список ресурсов
Публичные IP адреса

ЗАДАЧИ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ВНЕШНЕГО ПЕРИМЕТРА

1. Определить уязвимости и возможные векторы атак сетевого периметра, операционных систем и приложений Заказчика, которые наиболее вероятно могут быть обнаружены и реализованы злоумышленником из сети Интернет.

2. Создать примеры эксплуатации обнаруженных уязвимостей для демонстрации возможностей злоумышленника при попытках компрометации информационных систем, доступных из сети Интернет.

3. Оценить уровень защищенности ИТ-инфраструктуры, доступной из сети Интернет.

4. Предоставить рекомендации по снижению рисков, устранению уязвимостей и общему повышению уровня защищенности ИТ-инфраструктуры.

РЕЗУЛЬТАТЫ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ВНЕШНЕГО ПЕРИМЕТРА

Определены уязвимости и возможные векторы атак

- Идентифицированы уязвимости в сетевом периметре, операционных системах и приложениях Заказчика.
- Произведен анализ потенциальных векторов атак из сети Интернет с учетом вероятности обнаружения и успешной реализации.

Вынесена общая оценка уровня защищенности ИТ-инфраструктуры

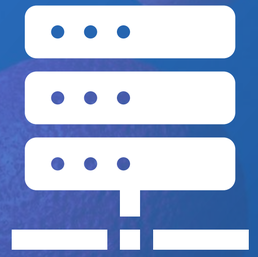
- Проанализированы результаты тестирования безопасности для формирования общей оценки уровня защищенности информационных систем, доступных из сети Интернет.
- Выявлены слабые стороны и уровни их воздействия на общую безопасность ИТ-инфраструктуры.

Показаны примеры эксплуатации уязвимостей

- Разработаны демонстрационные сценарии, иллюстрирующие возможности злоумышленника при компрометации информационных систем через выявленные уязвимости.
- Предоставлены конкретные эксплуатационные примеры для наглядного понимания потенциальных угроз.

Предоставлены рекомендации по снижению рисков и повышению уровня защиты

- Сформулированы конкретные рекомендации по снижению выявленных рисков и устранению выявленных уязвимостей.
- Разработаны общие стратегии для повышения уровня защищенности ИТ-инфраструктуры, включая рекомендации по внедрению дополнительных мер безопасности.



ОЦЕНКА ЗАЩИЩЁННОСТИ

Анализ защищенности и тестирование на проникновение локальной инфраструктуры.

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ЛОКАЛЬНОЙ ИНФРАСТРУКТУРЫ

МОДЕЛЬ НАРУШИТЕЛЯ

Внутренний нарушитель – злоумышленник, имеющий доступ к информационной системе из локальной сети организации, обладающий навыками подготовки и проведения атак на информационные системы.

Внутренний нарушитель с правами пользователя в исследуемой системе – злоумышленник, имеющий доступ к информационной системе из локальной сети организации и права пользователя в исследуемой системе, обладающий навыками подготовки и проведения атак на информационные системы.

ЦЕЛЬ УСЛУГИ

Оценка защищенности офисной сети Заказчика от возможных атак нарушителя, «гостя», получившего доступ к сети напрямую, через взлом кого-либо из сотрудников компании или через взлом оборудования, подключенного в сеть.

Для старта проекта нужно: количество IP адресов и внутренних сегментов сети, локация.

ЗАДАЧИ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ЛОКАЛЬНОЙ ИНФРАСТРУКТУРЫ

1. Определить уязвимости и возможные векторы атаки сетевого периметра, операционных систем и приложений Заказчика, которые наиболее вероятно могут быть обнаружены и реализованы злоумышленником из локальной сети организации.

2. Создать примеры эксплуатации обнаруженных уязвимостей для демонстрации возможностей злоумышленника при попытках повышения привилегий в локальной сети организации.

3. Оценить уровень защищенности ИТ-инфраструктуры локальной сети организации.

4. Предоставить рекомендации по снижению рисков, устранению уязвимостей и общему повышению уровня защищенности ИТ-инфраструктуры.

РЕЗУЛЬТАТЫ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ЛОКАЛЬНОЙ ИНФРАСТРУКТУРЫ

ITERBI consulting

Определены уязвимости и возможные векторы атак

- Проведен анализ сетевого периметра, операционных систем и приложений заказчика.
- Идентифицированы наиболее вероятные уязвимости, доступные для атаки из локальной сети.

Вынесена общая оценка уровня защищенности ИТ-инфраструктуры

- Обобщены результаты в целостную оценку общего уровня защиты ИТ-инфраструктуры.
- Выявлены уязвимости и потенциальные угрозы для формирования общей картины безопасности.

Показаны примеры эксплуатации уязвимостей

- Разработаны демонстрационные сценарии для проявления злоумышленником возможностей повышения привилегий.
- Подготовлены эксплойты для наглядного представления рисков в локальной сети.

Предоставлены рекомендации по снижению рисков и повышению уровня защиты

- Сформулированы рекомендации по устранению уязвимостей.
- Разработаны стратегии для снижения рисков и общего повышения уровня защищенности ИТ-инфраструктуры.

ОЦЕНКА ЗАЩИЩЁННОСТИ

Анализ защищенности и тестирование на проникновение отдельных веб-приложений.

Без анализа исходного кода

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ОТДЕЛЬНЫХ ВЕБ-ПРИЛОЖЕНИЙ | БЕЗ АНАЛИЗА ИСХОДНОГО КОДА

ITERBI consulting

МОДЕЛЬ НАРУШИТЕЛЯ

Внешний нарушитель – злоумышленник, имеющий доступ к информационной системе из сети Интернет, обладающий навыками подготовки и проведения атак на информационные системы.

Внешний нарушитель с правами пользователя в исследуемой системе – злоумышленник, имеющий доступ к информационной системе из сети Интернет и права пользователя в исследуемой системе, обладающий навыками подготовки и проведения атак на информационные системы.

ЦЕЛЬ УСЛУГИ

Выявление максимально возможного количества недостатков и уязвимостей, ведущих к получению злоумышленником возможности нарушения целостности, доступности и конфиденциальности информации обрабатываемой и хранимой в тестируемой информационной системе.
Для старта проекта нужно: количество методов API, бизнес логика и количество ролей

ЗАДАЧИ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ОТДЕЛЬНЫХ ВЕБ-ПРИЛОЖЕНИЙ | БЕЗ АНАЛИЗА ИСХОДНОГО КОДА

ITERBI consulting

1. Определить уязвимости и возможные векторы атаки приложений Заказчика, которые наиболее вероятно могут быть обнаружены и реализованы злоумышленником из сети Интернет.

2. Создать примеры эксплуатации обнаруженных уязвимостей для демонстрации возможностей злоумышленника при попытках компрометации веб-приложений организации.

3. Оценить уровень защищенности веб-приложений.

4. Предоставить рекомендации по снижению рисков, устранению уязвимостей и общему повышению уровня защищенности веб-приложений.

РЕЗУЛЬТАТЫ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ОТДЕЛЬНЫХ ВЕБ-ПРИЛОЖЕНИЙ | БЕЗ АНАЛИЗА ИСХОДНОГО КОДА

Определены уязвимости и возможные векторы атак

- Проанализированы веб-приложения Заказчика и выделены потенциальные уязвимости и их возможные векторы атак.
- Определены основные уязвимости, подверженные обнаружению и реализации злоумышленником через Интернет.

Вынесена общая оценка уровня защищенности веб-приложений

- Проведена комплексная оценка уровня защиты веб-приложений, учитывающая выявленные уязвимости и степень их критичности.
- Высокоуровневая оценка безопасности предоставляет обзор текущего состояния защиты веб-приложений организации.

Показаны примеры эксплуатации уязвимостей

- Разработаны примеры эксплуатации обнаруженных уязвимостей, демонстрирующие способы компрометации веб-приложений.
- Эксплуатационные сценарии предоставляют ясное представление о потенциальных угрозах и методах атаки.

Предоставлены рекомендации по снижению рисков и повышению уровня защиты

- Подготовлены рекомендации, направленные на снижение рисков и устранение обнаруженных уязвимостей.
- Рекомендации включают практические шаги для общего улучшения уровня защиты веб-приложений и предотвращения возможных атак.

ОЦЕНКА ЗАЩИЩЁННОСТИ

Анализ защищенности и тестирование на проникновение

отдельных веб-приложений.

Включая анализ исходного кода

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ОТДЕЛЬНЫХ ВЕБ-ПРИЛОЖЕНИЙ | ВКЛЮЧАЯ АНАЛИЗ ИСХОДНОГО КОДА

ITERBI consulting

МОДЕЛЬ НАРУШИТЕЛЯ

Внешний нарушитель – злоумышленник, имеющий доступ к информационной системе из сети Интернет, обладающий навыками подготовки и проведения атак на информационные системы.

Внешний нарушитель с правами пользователя в исследуемой системе – злоумышленник, имеющий доступ к информационной системе из сети Интернет и права пользователя в исследуемой системе, обладающий навыками подготовки и проведения атак на информационные системы.

Внутренний нарушитель с правами администратора в исследуемой системе – злоумышленник, имеющий доступ к информационной системе из сети Интернет, права администратора в исследуемой системе и доступ к исходному коду системы, обладающий навыками подготовки и проведения атак на информационные системы.

ЦЕЛЬ УСЛУГИ

Выявление максимально возможного количества недостатков и уязвимостей, ведущих к получению злоумышленником возможности нарушения целостности, доступности и конфиденциальности информации обрабатываемой и хранимой в тестируемой информационной системе.
Для старта проекта нужно: количество строк кода, технологический стек

ЗАДАЧИ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ОТДЕЛЬНЫХ ВЕБ-ПРИЛОЖЕНИЙ | ВКЛЮЧАЯ АНАЛИЗ ИСХОДНОГО КОДА

ITERBI consulting

1. Определить уязвимости и возможные векторы атаки приложений Заказчика, которые наиболее вероятно могут быть обнаружены и реализованы злоумышленником из сети Интернет.

2. Создать примеры эксплуатации обнаруженных уязвимостей для демонстрации возможностей злоумышленника при попытках компрометации веб-приложений организации.

3. Оценить уровень защищенности веб-приложений.

4. Предоставить рекомендации по снижению рисков, устранению уязвимостей и общему повышению уровня защищенности веб-приложений.

РЕЗУЛЬТАТЫ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ОТДЕЛЬНЫХ ВЕБ-ПРИЛОЖЕНИЙ | ВКЛЮЧАЯ АНАЛИЗ ИСХОДНОГО КОДА

ITERBI consulting

Определены уязвимости и возможные векторы атак

- Проведен анализ приложений Заказчика для выявления наиболее вероятных уязвимостей, которые могут быть обнаружены и использованы злоумышленником из сети Интернет.
- Выделены ключевые точки входа, потенциальные слабые места и точки эксплуатации веб-приложений.

Вынесена общая оценка уровня защищенности веб-приложений

- Проведена комплексная оценка уровня безопасности веб-приложений с учетом выявленных уязвимостей и возможных сценариев атак.
- Предоставлена общая оценка текущего состояния защиты приложений от потенциальных угроз.

Показаны примеры эксплуатации уязвимостей

- Разработаны демонстрационные сценарии, представляющие возможные атаки и компрометацию веб-приложений.
- Предоставлены конкретные примеры эксплуатации обнаруженных уязвимостей для иллюстрации потенциальных угроз и последствий.

Предоставлены рекомендации по снижению рисков и повышению уровня защиты

- Составлены рекомендации по устранению обнаруженных уязвимостей и улучшению общей защиты веб-приложений.
- Предложены меры по снижению рисков и повышению уровня безопасности на основе результатов анализа уязвимостей.

ОЦЕНКА ЗАЩИЩЁННОСТИ

Анализ защищенности и тестирование на проникновение беспроводных сетей.

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ БЕСПРОВОДНЫХ СЕТЕЙ

МОДЕЛЬ НАРУШИТЕЛЯ

Внешний нарушитель – злоумышленник, имеющий доступ к информационной системе из сети Интернет, обладающий навыками подготовки и проведения атак на информационные системы.

ЦЕЛЬ УСЛУГИ

Оценка защищенности беспроводных сетей компании Заказчика от возможных атак нарушителя и анализ нежелательных беспроводных сетей на территории офиса Заказчика.
Для старта проекта нужно: Количество уникальных точек Wi-Fi, SID.

ЗАДАЧИ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ БЕСПРОВОДНЫХ СЕТЕЙ

1. Оценить уровень защищенности беспроводных сетей компании Заказчика.

2. Найти уязвимости конфигурации беспроводных сетей и построить векторы атаки, демонстрирующие риски нарушения безопасности информации.

3. Предоставить общие и детальные рекомендации по повышению уровня защищенности беспроводных сетей компании Заказчика.

РЕЗУЛЬТАТЫ

ПРОВЕРКА НА ПРОНИКНОВЕНИЕ БЕСПРОВОДНЫХ СЕТЕЙ

Определены уязвимости и возможные векторы атак

- Идентифицированы потенциальные уязвимости в конфигурации беспроводных сетей, подвергающие компанию Заказчика риску нарушения безопасности данных.
- Разработаны векторы атак, демонстрирующие реальные сценарии эксплуатации уязвимостей, с целью визуализации возможных угроз.

Предоставлены рекомендации по повышению уровня защищенности

- Составлены детальные рекомендации по устранению выявленных уязвимостей, включая изменения в конфигурации и обновление программного обеспечения.
- Предложены общие стратегии и меры для улучшения общего уровня безопасности беспроводных сетей компании, соответствующие современным стандартам и лучшим практикам.

Произведена оценка защищенности беспроводных сетей

- Проведен анализ текущего состояния беспроводных сетей, выявлены уровни уязвимости и оценена степень их критичности.
- Оценены меры защиты, применяемые в сети Заказчика, с учетом стандартов безопасности, и выделены сильные и слабые стороны.

Предоставлен отчет с подробным описанием результатов и рекомендаций

- Представлен подробный отчет, содержащий результаты оценки защищенности, выявленные уязвимости и построенные векторы атак.
- Включены четкие и практические рекомендации для совершенствования безопасности беспроводных сетей компании, с фокусом на улучшении предотвращения атак и реагирования на инциденты.

МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ

Анализ защищенности мобильных приложений

Android и iOS.

Без анализа исходного кода

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

АНАЛИЗ ЗАЩИЩЕННОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ANDROID И IOS | БЕЗ АНАЛИЗА ИСХОДНОГО КОДА

ITERBI consulting

МОДЕЛЬ НАРУШИТЕЛЯ

Внешний нарушитель – злоумышленник, имеющий доступ к информационной системе из сети Интернет, обладающий навыками подготовки и проведения атак на информационные системы.

Внешний нарушитель с правами пользователя в исследуемой системе – злоумышленник, имеющий доступ к информационной системе из сети Интернет и права пользователя в исследуемой системе, обладающий навыками подготовки и проведения атак на информационные системы.

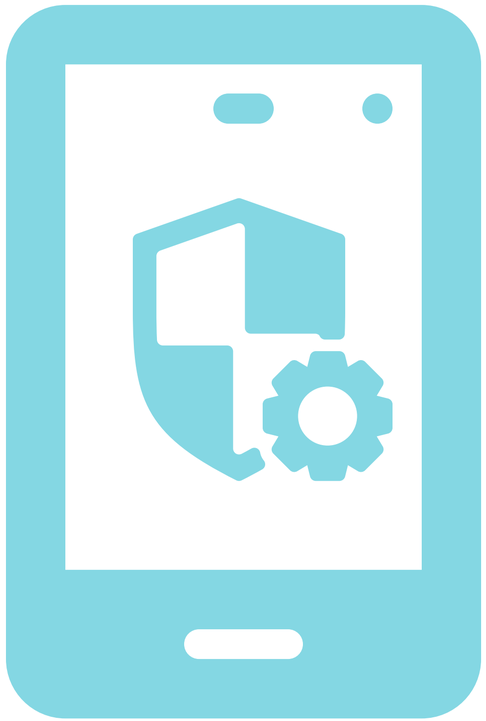
ЦЕЛЬ УСЛУГИ

Выявление максимально возможного количества недостатков и уязвимостей, ведущих к получению злоумышленником возможности нарушения целостности, доступности и конфиденциальности информации обрабатываемой и хранимой в тестируемой информационной системе.
Для старта проекта нужно: количество ролей, платформа (Android/IOS)

ЗАДАЧИ

АНАЛИЗ ЗАЩИЩЕННОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ANDROID И IOS | БЕЗ АНАЛИЗА ИСХОДНОГО КОДА

ITERBI consulting



1. Определить уязвимости и возможные векторы атаки на мобильные приложения Заказчика, которые наиболее вероятно могут быть обнаружены и реализованы злоумышленником из сети Интернет.

2. Создать примеры эксплуатации обнаруженных уязвимостей для демонстрации возможностей злоумышленника при попытках компрометации мобильных приложений организации.

3. Оценить уровень защищенности мобильных приложений.

4. Предоставить рекомендации по снижению рисков, устранению уязвимостей и общему повышению уровня защищенности мобильных приложений.

РЕЗУЛЬТАТЫ

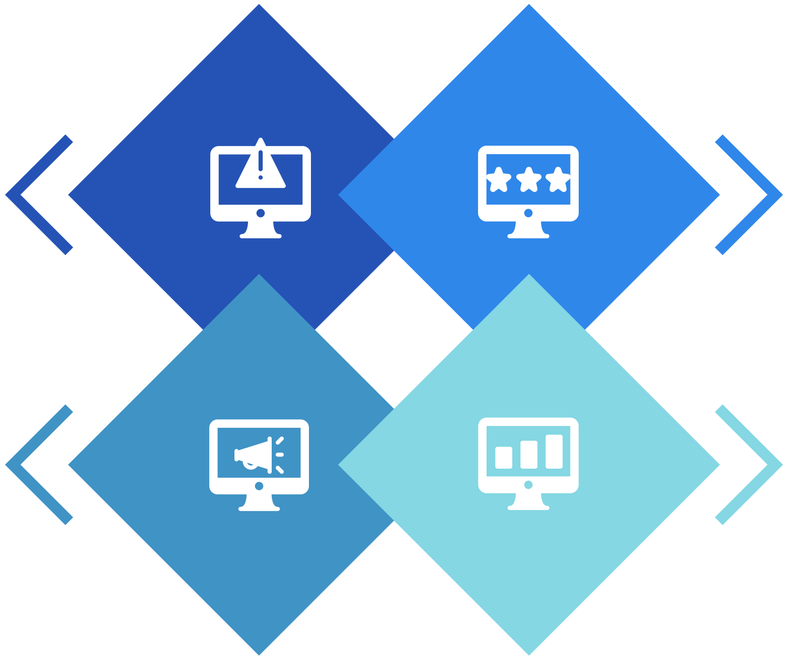
ПРОВЕРКА НА ПРОНИКНОВЕНИЕ ВНЕШНЕГО ПЕРИМЕТРА

Определены уязвимости и возможные векторы атак

- Идентифицированы уязвимости, представляющие наибольший потенциал для злоумышленников из сети Интернет.
- Выполнен анализ возможных векторов атак, оценены их вероятность и потенциальные последствия для безопасности мобильных приложений.

Вынесена общая оценка уровня защищенности мобильных приложений

- Проведена общая оценка уровня защищенности мобильных приложений, учитывая выявленные уязвимости и риски.
- Предоставлена детальная характеристика текущего состояния безопасности с присвоением соответствующей оценки.



Показаны примеры эксплуатации уязвимостей

- Разработаны примеры эксплуатации уязвимостей, предоставляющие демонстрацию возможностей злоумышленника при попытках компрометации мобильных приложений.
- Эксплуатационные сценарии позволяют организации лучше понимать угрозы и разрабатывать соответствующие контрмеры для защиты.

Предоставлены рекомендации по снижению рисков и устранению уязвимостей

- Разработаны рекомендации по снижению рисков и устранению обнаруженных уязвимостей.
- Предложены конкретные шаги для общего повышения уровня защищенности мобильных приложений.
- Рекомендации охватывают как технические аспекты (патчи, обновления), так и организационные меры (обучение персонала, улучшение политик безопасности).

МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ

Анализ защищенности мобильных приложений

Android и iOS.

Включая анализ исходного кода

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

АНАЛИЗ ЗАЩИЩЕННОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ANDROID И IOS | ВКЛЮЧАЯ АНАЛИЗ ИСХОДНОГО КОДА

ITERBI consulting

МОДЕЛЬ НАРУШИТЕЛЯ

Внешний нарушитель – злоумышленник, имеющий доступ к информационной системе из сети Интернет, обладающий навыками подготовки и проведения атак на информационные системы.

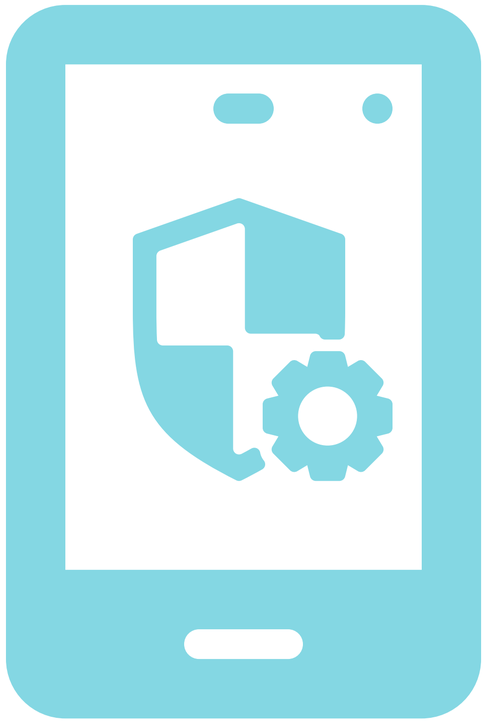
Внешний нарушитель с правами пользователя в исследуемой системе – злоумышленник, имеющий доступ к информационной системе из сети Интернет и права пользователя в исследуемой системе, обладающий навыками подготовки и проведения атак на информационные системы.

ЦЕЛЬ УСЛУГИ

Выявление максимально возможного количества недостатков и уязвимостей, ведущих к получению злоумышленником возможности нарушения целостности, доступности и конфиденциальности информации обрабатываемой и хранимой в тестируемой информационной системе.
Для старта проекта нужно: количество строк кода, технологический стек.

ЗАДАЧИ

АНАЛИЗ ЗАЩИЩЕННОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ANDROID И IOS | ВКЛЮЧАЯ АНАЛИЗ ИСХОДНОГО КОДА



1. Определить уязвимости и возможные векторы атаки на мобильные приложения Заказчика, которые наиболее вероятно могут быть обнаружены и реализованы злоумышленником из сети Интернет, а также злоумышленником, имеющим доступ к исходным кодам приложений.

2. Создать примеры эксплуатации обнаруженных уязвимостей для демонстрации возможностей злоумышленника при попытках компрометации мобильных приложений организации.

3. Оценить уровень защищенности мобильных приложений.

4. Предоставить рекомендации по снижению рисков, устранению уязвимостей и общему повышению уровня защищенности мобильных приложений.

РЕЗУЛЬТАТЫ

АНАЛИЗ ЗАЩИЩЕННОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ANDROID И IOS | ВКЛЮЧАЯ АНАЛИЗ ИСХОДНОГО КОДА

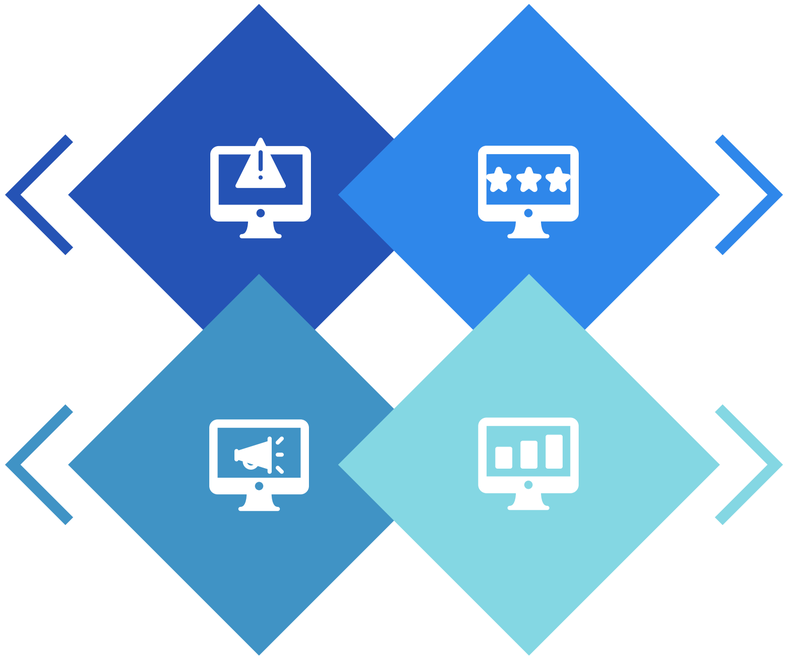
ITERBI consulting

Определены уязвимости и возможные векторы атак

- Идентифицированы уязвимости, представляющие наибольший потенциал для злоумышленников из сети Интернет и лицом, имеющим доступ к исходным кодам приложений.
- Выполнен анализ возможных векторов атак, оценены их вероятность и потенциальные последствия для безопасности мобильных приложений.

Вынесена общая оценка уровня защищенности мобильных приложений

- Проведена общая оценка уровня защищенности мобильных приложений, учитывая выявленные уязвимости и риски.
- Предоставлена детальная характеристика текущего состояния безопасности с присвоением соответствующей оценки.



Показаны примеры эксплуатации уязвимостей

- Разработаны примеры эксплуатации уязвимостей, предоставляющие демонстрацию возможностей злоумышленника при попытках компрометации мобильных приложений.
- Эксплуатационные сценарии позволяют организации лучше понимать угрозы и разрабатывать соответствующие контрмеры для защиты.

Предоставлены рекомендации по снижению рисков и устранению уязвимостей

- Разработаны рекомендации по снижению рисков и устранению обнаруженных уязвимостей.
- Предложены конкретные шаги для общего повышения уровня защищенности мобильных приложений.
- Рекомендации охватывают как технические аспекты (патчи, обновления), так и организационные меры (обучение персонала, улучшение политик безопасности).

СОТРУДНИКИ

Социотехническое тестирование сотрудников.

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

СОЦИОТЕХНИЧЕСКОЕ ТЕСТИРОВАНИЕ СОТРУДНИКОВ

МОДЕЛЬ НАРУШИТЕЛЯ

Внешний нарушитель – злоумышленник, имеющий доступ к информационной системе из сети Интернет, обладающий навыками подготовки и проведения атак на информационные системы.

Внешний нарушитель с правами пользователя в исследуемой системе – злоумышленник, имеющий доступ к информационной системе из сети Интернет и права пользователя в исследуемой системе, обладающий навыками подготовки и проведения атак на информационные системы.

ЦЕЛЬ УСЛУГИ

Повышение осведомленности сотрудников компании Заказчика в вопросах информационной безопасности и повышение защищенности почтовой IT-инфраструктуры компании Заказчика по отношению к атакам из сети Интернет.
Для старта проекта нужно: количество сотрудников, электронные почты.

ЗАДАЧИ

СОЦИОТЕХНИЧЕСКОЕ ТЕСТИРОВАНИЕ СОТРУДНИКОВ

01 | Осведомленность

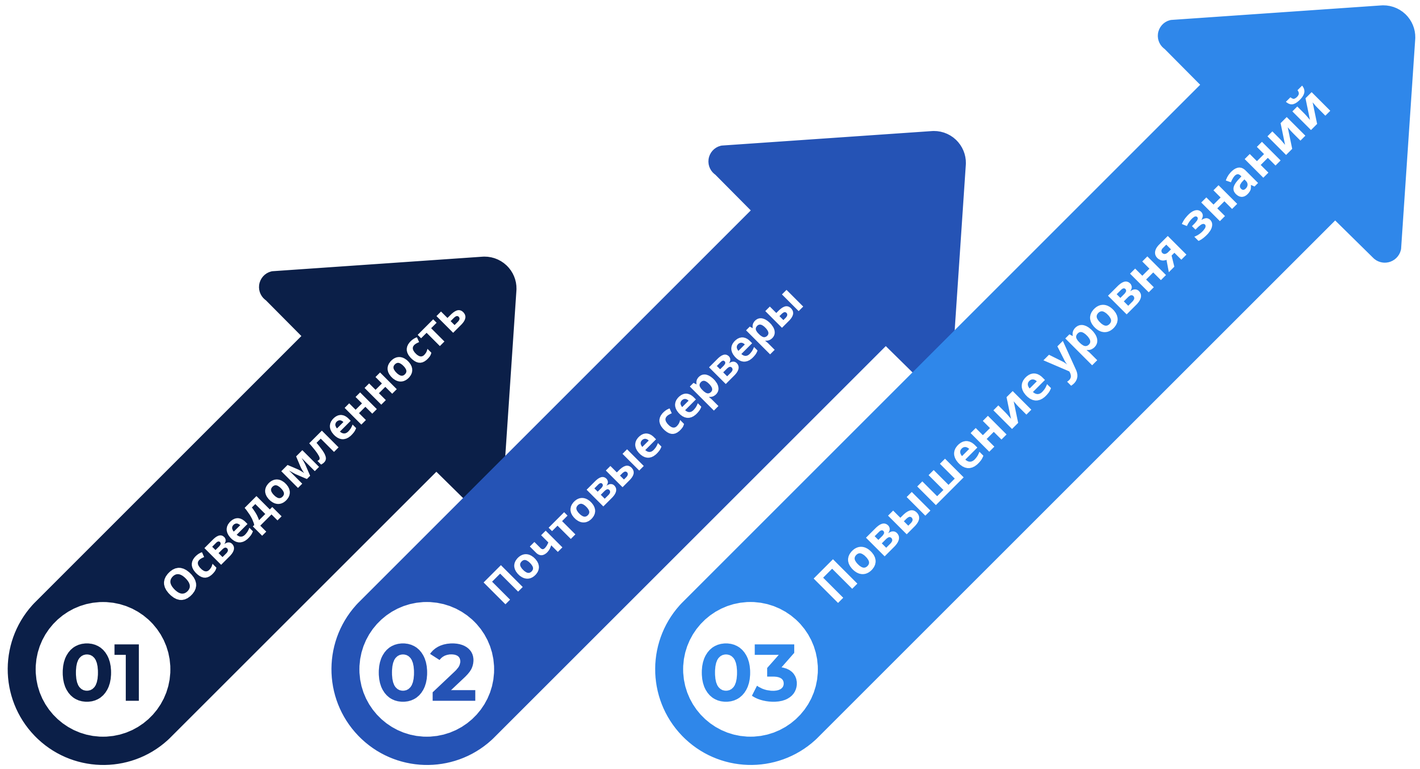
- Создание анкеты или опросника, включающего вопросы о знании основных принципов информационной безопасности, уровне осведомленности о типичных угрозах (например, фишинг, социальная инженерия, вредоносные программы).
- Сбор и анализ данных, включая оценку общего уровня осведомленности сотрудников, выявление слабых мест и потребностей в обучении.

02 | Почтовые серверы

- Анализ текущей архитектуры и конфигурации почтовых серверов и сервисов компании.
- Анализ результатов тестирования и выявление уязвимостей и слабых мест в защите почтовых сервисов.

03 | Повышение уровня знаний

- Разработка рекомендаций по усилению защиты почтовых сервисов на основе выявленных уязвимостей и результатов тестирования на проникновение.
- Проведение обучения для сотрудников компании по основам информационной безопасности.



РЕЗУЛЬТАТЫ

СОЦИОТЕХНИЧЕСКОЕ ТЕСТИРОВАНИЕ СОТРУДНИКОВ

01 | Оценка осведомленности сотрудников компании в вопросах информационной безопасности

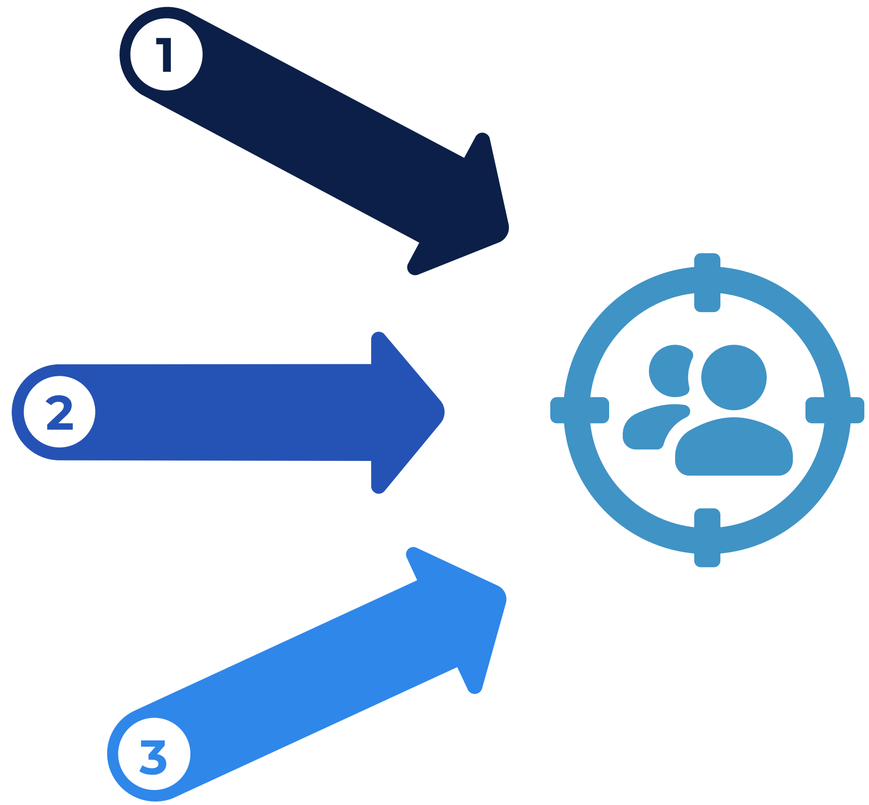
- Проведен опрос сотрудников компании для оценки их знаний и понимания основных принципов информационной безопасности.
- Анализ результатов опроса позволил выявить уровень осведомленности сотрудников и идентифицировать слабые места, где требуется дополнительное обучение и внимание.

02 | Оценка защищенности почтовых сервисов компании по отношению к атакам злоумышленников

- Проведена аналитическая оценка текущего состояния почтовых сервисов компании с учетом существующих угроз и уязвимостей.
- Проанализированы логи и данные о попытках несанкционированного доступа к почтовым сервисам.
- Выявлены уязвимые места и потенциальные точки входа для злоумышленников.

03 | Предоставление детальных и общих рекомендаций по повышению уровня защищенности

- Разработаны рекомендации по улучшению защищенности почтовых сервисов, включая внедрение дополнительных мер безопасности, обновление программного обеспечения и усиление мониторинга.
- Разработаны планы обучения сотрудников в области информационной безопасности.
- Предложены меры по улучшению культуры безопасности в организации, включая проведение регулярных проверок, создание политик безопасности и сознательное вовлечение персонала в процессы обеспечения безопасности информации.



НАГРУЗОЧНОЕ ТЕСТИРОВАНИЕ

Нагрузочное тестирование веб-приложений.

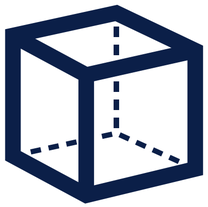
КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

НАГРУЗОЧНОЕ ТЕСТИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЙ



ОБЪЕКТЫ

- 1 Веб-приложение Заказчика.
- Предоставляемая нагрузка 1 Гб\сек, до 10 000 rps.
- В область тестирования входит до 3х сценариев тестирования.
- Без учета себестоимости вычислительных мощностей.

ЦЕЛЬ УСЛУГИ

Определение максимальной производительности системы, при которой система удовлетворяет требованиям по качеству облуживания, временам отклика и пр.
Выявление «узких мест».
Для старта проекта нужно: лимит нагрузки, время проведения, приложение, СЗИ.

ЗАДАЧИ

НАГРУЗОЧНОЕ ТЕСТИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЙ

РЕЗУЛЬТАТЫ

НАГРУЗОЧНОЕ ТЕСТИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЙ

ITERBI consulting

01 | Разработка тестового сценария

- Определены API запросы, необходимые для тестирования системы.
- Созданы тестовые сценарии, описывающие последовательность запросов и действий.
- Учтены различные сценарии использования, включая типичные и экстремальные случаи.

02 | Реализация сценария в JMeter

- Сценарии были перенесены и настроены в приложении JMeter.
- Созданы необходимые HTTP запросы, параметры, и данные для имитации реального трафика.
- Настроены контроллеры и логика выполнения тестовых сцена.

03 | Настройка мониторинга системы

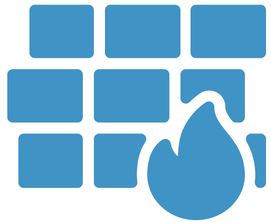
- Определены ключевые метрики для мониторинга системы во время нагрузочного тестирования.
- Настроены инструменты мониторинга для сбора данных о производительности и состоянии системы в реальном времени.
- Разработаны оповещения и предупреждения для случаев превышения пороговых значений метрик.

04 | Проведение нагрузочного тестирования

- Были запущены нагрузочные тесты с использованием JMeter, согласно разработанным сценариям.
- Наблюдалось увеличение нагрузки на систему, с целью проверки ее производительности и устойчивости под нагрузкой.
- Проведены тесты на различных уровнях нагрузки, включая пиковые и постепенное увеличение.

05 | Анализ результатов

- Получены данные о производительности системы, включая среднее время ответа, загрузку ресурсов, и распределение нагрузки по компонентам.
- Проанализированы результаты нагрузочного тестирования с учетом заданных критериев производительности и стабильности.
- Сделаны выводы о работоспособности системы под нагрузкой, выявлены узкие места и проблемы, предложены рекомендации по их улучшению.



РАССЛЕДОВАНИЕ ИНЦИДЕНТА

Расследование инцидента информационной безопасности.

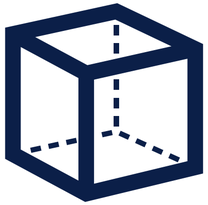
КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

РАССЛЕДОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ОБЪЕКТЫ

Программно-аппаратный объект - операционная система, расположенная в ИТ инфраструктуре, предоставляемой Заказчиком, доступная через сеть Интернет.

ЦЕЛИ УСЛУГИ

Установить личность, спровоцировавшую инцидент информационной безопасности, на основе улик явно свидетельствующих о том, что действия, приведшие к инциденту, были произведены этой личностью.

Если личность установить невозможно, определить улики, которые свидетельствуют о том, как произошел инцидент, и что необходимо сделать, чтобы получить информацию о такой личности.

При невозможности установить детали инцидента и возможных действий злоумышленника на системе предоставить техническое описание проведенных техник расследования с их описанием.

ЗАДАЧИ

РАССЛЕДОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исследование состояния информационной системы

- Оценка текущего состояния информационной системы.
- Анализ конфигурации и настроек системы.
- Выявление потенциальных уязвимостей и слабых мест.

Восстановление хронологии событий инцидента

- Подробное восстановление последовательности событий.
- Идентификация первичных причин и факторов, спровоцировавших инцидент.

Выявление программного обеспечения злоумышленника

- Обнаружение вредоносных программ и инструментов, использованных злоумышленником.
- Анализ действий программного обеспечения для определения его целей и методов атаки.

Сбор цифровых доказательств

- Систематический сбор и документирование цифровых следов инцидента.
- Обеспечение целостности и достоверности собранных доказательств.

Определение векторов атаки

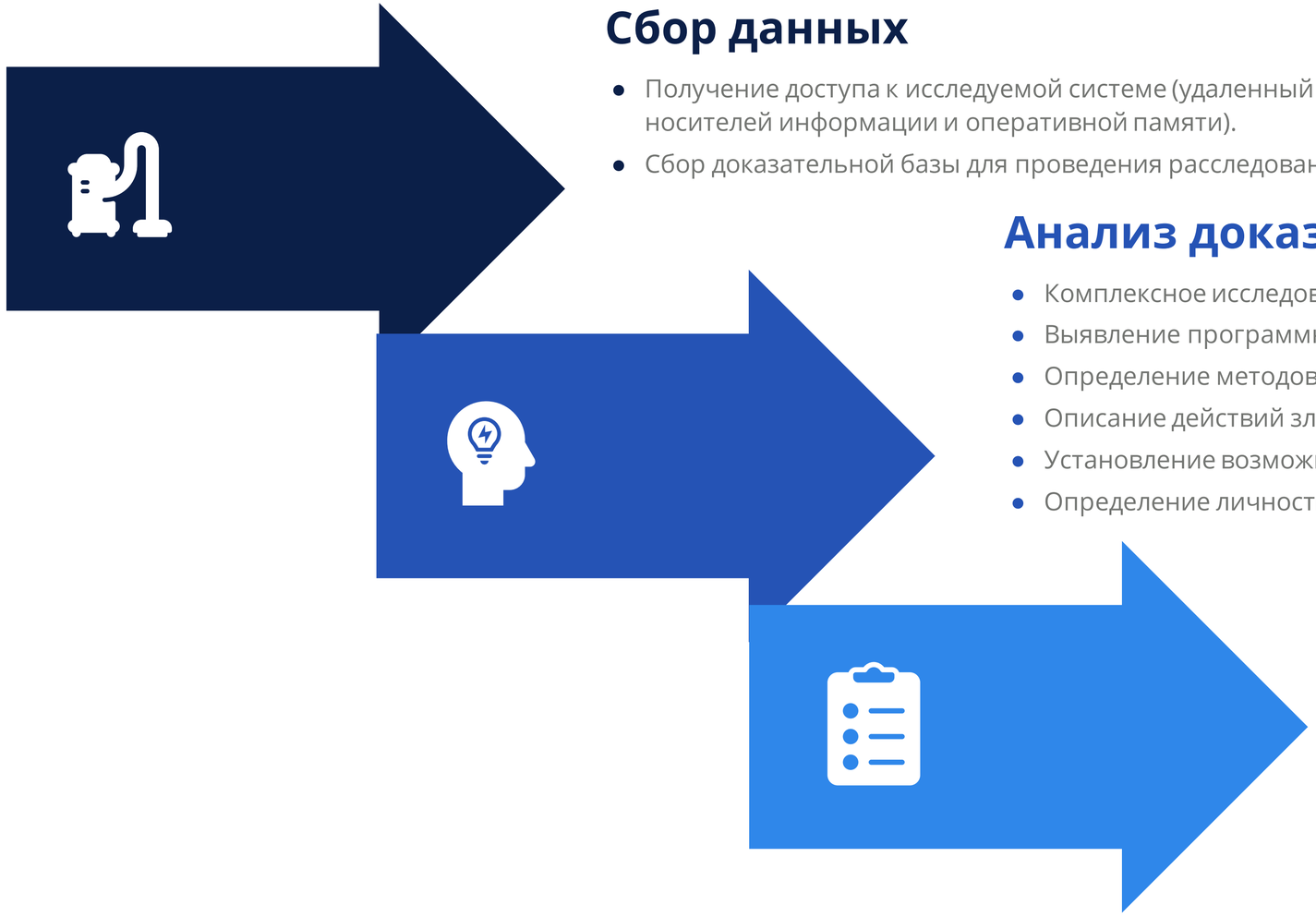
- Анализ использованных методов атаки и путей проникновения.
- Выявление уязвимостей, которые могут быть использованы для дальнейших атак.

Экспертная оценка возможной личности нарушителя

- Анализ информации для идентификации потенциальных нарушителей.
- Оценка вероятности того, что конкретный субъект мог быть причастен к инциденту.
- Предоставление экспертного заключения на основе доступных данных.

ЭТАПЫ ПРОЕКТА

РАССЛЕДОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Сбор данных

- Получение доступа к исследуемой системе (удаленный доступ или полная копия носителей информации и оперативной памяти).
- Сбор доказательной базы для проведения расследования.

Анализ доказательной базы

- Комплексное исследование данных от системы.
- Выявление программного обеспечения для удаленного управления исследуемой системой.
- Определение методов закрепления злоумышленника на системе.
- Описание действий злоумышленника на системе.
- Установление возможных векторов компрометации системы.
- Определение личности злоумышленника (если это возможно).

Подготовка отчета

- Создание отчета о проведенном расследовании.
- Выработка рекомендаций по изменению состояния компьютерной безопасности для предотвращения похожих инцидентов в будущем.

РЕЗУЛЬТАТЫ

РАССЛЕДОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исследовано состояние информационной системы с использованием специалистами Исполнителя.

Восстановлена хронология событий инцидента для выявления всех этапов происходящих событий.

Идентифицировано и проанализировано программное обеспечение, используемое злоумышленником.

Собраны и систематизированы цифровые доказательства, необходимые для дальнейшего анализа и проведения расследования.

Определены векторы атаки нарушителя, что позволяет оценить уязвимости информационной системы.

При возможности установления личности нарушителя, специалисты предоставили экспертную оценку, идентифицируя возможных субъектов, которые могли создать условия для возникновения данного инцидента.

МОНИТОРИНГ

Непрерывный мониторинг защищенности

ИТ-инфраструктуры.

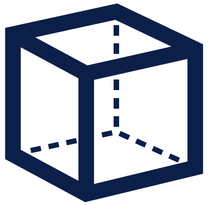
КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ЗАЩИЩЕННОСТИ ИТ-ИНФРАСТРУКТУРЫ



ОБЪЕКТЫ

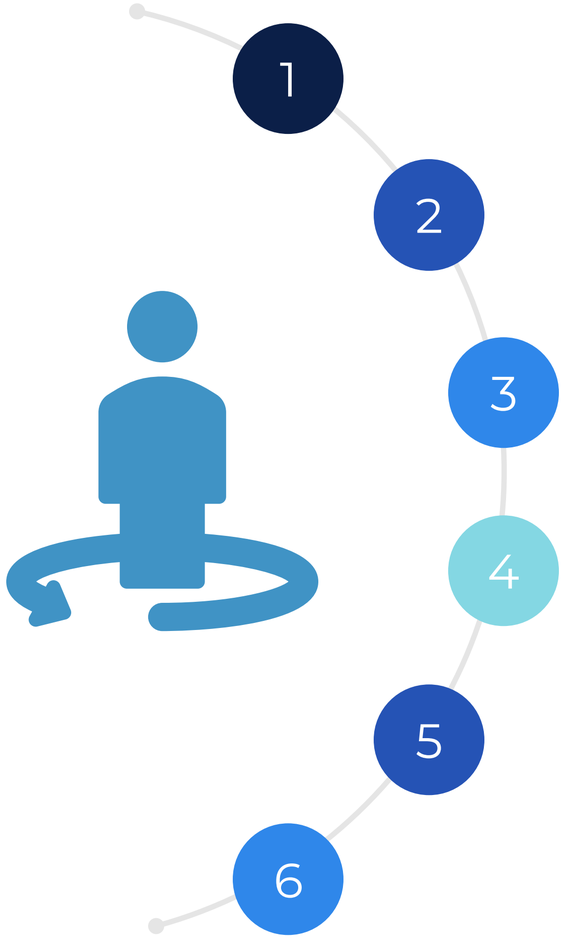
- Внешний сетевой периметр (до 15 публичных IP-адресов).
- До 2 доменов (до 15 поддоменов).

ЦЕЛЬ УСЛУГИ

Обеспечение непрерывного контроля защищенности внешнего периметра IT- инфраструктуры компании, в течение периода оказания услуг.

ЗАДАЧИ

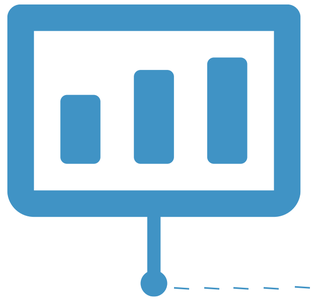
НЕПРЕРЫВНЫЙ МОНИТОРИНГ ЗАЩИЩЕННОСТИ ВНЕШНЕГО ПЕРИМЕТРА ИТ-ИНФРАСТРУКТУРЫ



1. Первичное тестирование на проникновение внешнего сетевого периметра ИТ-инфраструктуры Заказчика. (опционально)
2. Непрерывный мониторинг защищенности внешнего сетевого периметра с помощью автоматизированных инструментов анализа уязвимостей.
3. Анализ и ручная верификация обнаруженных уязвимостей разбор срабатываний автоматических инструментов.
4. Создание примеров эксплуатации обнаруженных уязвимостей и моделирование векторов атак для демонстрации возможностей злоумышленника при попытках компрометации информационных систем, доступных из сети Интернет.
5. Вынесение общей оценки уровня защищенности ИТ-инфраструктуры, доступной из сети Интернет.
6. Предоставление рекомендаций по снижению рисков, устранению уязвимостей общему повышению уровня защищенности ИТ-инфраструктуры.

РЕЗУЛЬТАТЫ

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ЗАЩИЩЕННОСТИ ВНЕШНЕГО ПЕРИМЕТРА ИТ-ИНФРАСТРУКТУРЫ



1. Проведено первичное тестирование на проникновение внешнего сетевого периметра ИТ-инфраструктуры Заказчика. (опционально)
2. Осуществлен непрерывный мониторинг защищенности внешнего сетевого периметра с помощью автоматизированных инструментов анализа уязвимостей.
3. Проведен анализ и ручная верификация обнаруженных уязвимостей, а также разбор срабатываний автоматических инструментов.
4. Созданы примеры эксплуатации обнаруженных уязвимостей и моделирование векторов атак для демонстрации возможностей злоумышленника при попытках компрометации информационных систем, доступных из сети Интернет.
5. Вынесена общая оценка уровня защищенности ИТ-инфраструктуры, доступнойиз сети Интернет.
6. Предоставлены рекомендации по снижению рисков, устранению уязвимостей и общему повышению уровня защищенности ИТ-инфраструктуры.

РАЗРАБОТКА И ПРОДУКТОВАЯ СРЕДА

Анализ защищенности инфраструктуры разработки и продуктовой среды.

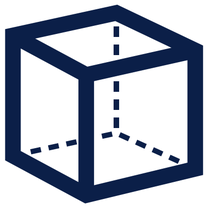
КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФРАСТРУКТУРЫ РАЗРАБОТКИ И ПРОДУКТОВОЙ СРЕДЫ



ОБЪЕКТЫ

- Source Code Management (github/gitlab/bitbucket/etc.).
- CI/CD (gitlab/jenkins/teamcity/etc.).
- Artifact Repository Manager (nessus/artifactory/etc.).
- Image Registry.
- Container Orchestrations System (kubernetes/openShift/swarm/etc.).

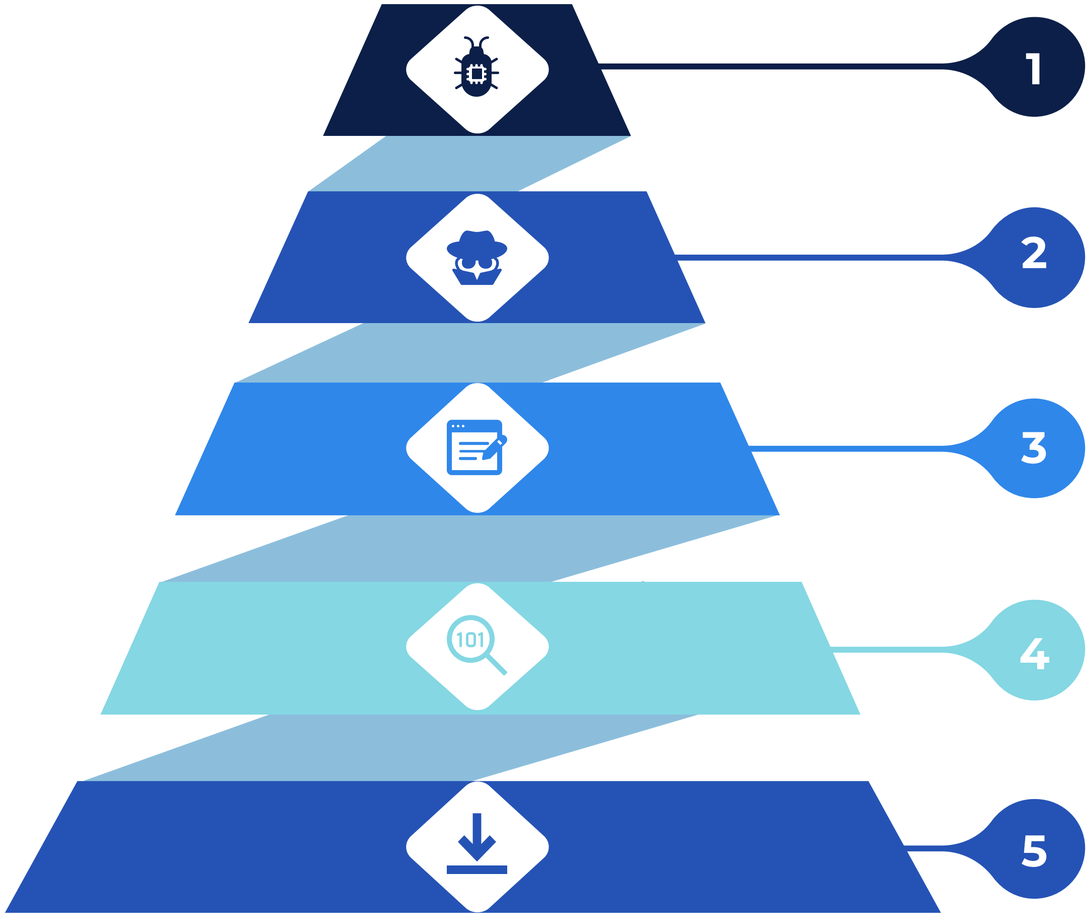
ЦЕЛЬ УСЛУГИ

Оценка защищенности инфраструктуры разработки и продуктовой среды от возможных атак внутреннего нарушителя - разработчика или другого сотрудника, а также от атак внешнего/внутреннего злоумышленника, получившего доступ во внутреннюю сеть с правами разработчика или другого сотрудника путем его взлома.

Услуга выполняется путем имитации действий потенциального злоумышленника.

ЗАДАЧИ

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФРАСТРУКТУРЫ РАЗРАБОТКИ И ПРОДУКТОВОЙ СРЕДЫ



1. Определение уязвимостей компонентов инфраструктуры разработки и продуктовой среды.
2. Определение возможностей злоупотребления имеющимися доступами для влияния на проекты других команд, а такжена инфраструктуру разработки в целом.
3. Определение возможностей влиять на деплои продуктовых приложений.
4. Определение возможностей подмены и/или перезаписи артефактов и образов.
5. Предоставление рекомендаций по снижению обнаруженных рисков, а также их приоритезация.

РЕЗУЛЬТАТЫ

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФРАСТРУКТУРЫ РАЗРАБОТКИ И ПРОДУКТОВОЙ СРЕДЫ

ITERBI consulting

- Компоненты инфраструктуры разработки и продуктовой среды были проверены на наличие уязвимостей.
- Проведен анализ доступов с целью выявления возможных злоупотреблений, которые могли бы повлиять на проекты других команд и общую инфраструктуру разработки.
- Исследованы возможности воздействия на деплои продуктовых приложений.
- Оценены возможности подмены и/или перезаписи артефактов и образов.
- Предоставлены рекомендации по уменьшению обнаруженных рисков, а также их приоритизация.

ПРОЦЕССЫ БЕЗОПАСНОЙ РАЗРАБОТКИ SSDLC

Внедрение и сопровождение процессов безопасной разработки программного обеспечения.

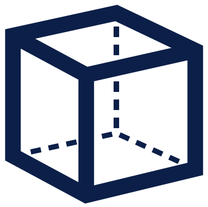
КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

ОПИСАНИЕ

ПРОЦЕССЫ БЕЗОПАСНОЙ РАЗРАБОТКИ SSDLC



ОБЪЕКТЫ

- ИТ-инфраструктура и процесс разработки 1 приложения (может состоять из нескольких компонентов).
- Общий размер кодовой базы приложения ограничен 2 млн. строк исходного кода, разработанного с использованием широко распространенных современный технологий построения программного обеспечения.

ЦЕЛЬ УСЛУГИ

Повышение общей безопасности приложения Заказчика, снижение стоимости устранения и общего количества уязвимостей.
Соответствие лучшим практикам и требования регуляторов по обеспечению процесса безопасной разработки.

ЗАДАЧИ

СОПРОВОЖДЕНИЕ ПРОЦЕССА БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Анализ текущего процесса разработки программного обеспечения с точки зрения наличия контролей безопасности в соответствии с лучшими практиками.

2. Ручной и полуавтоматизированный анализ защищенности приложения.

3. Разбор технического долга.

4. Доработка конфигурации (в том числе определение Quality Gates), а также новых правил срабатывания для используемых решений по организации процесса безопасной разработки.

5. Ручные проверки и верификация новых срабатываний.

6. Участие в процессе разработки в качестве центра компетенций по вопросам безопасности (включая моделирование угроз, анализ архитектуры, дизайн-обзор для новых компонентов).

РЕЗУЛЬТАТЫ

СОПРОВОЖДЕНИЕ ПРОЦЕССА БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Проведен анализ текущего процесса разработки программного обеспечения с учетом наличия контролей безопасности в соответствии с лучшими практиками.
2. Осуществлен ручной и полуавтоматизированный анализ защищенности приложения.
3. Проведен разбор технического долга для выявления и устранения накопившихся проблем.
4. Произведена доработка конфигурации, включая определение Quality Gates и новых правил срабатывания для используемых решений по организации процесса безопасной разработки.
5. Осуществлены ручные проверки и верификация новых срабатываний для обеспечения соответствия стандартам безопасности.
6. Принималось активное участие в процессе разработки, действуя в качестве центра компетенций по вопросам безопасности, что включало моделирование угроз, анализ архитектуры и дизайн-ревью для новых компонентов.

КОНТАКТЫ

Контактные лица по предложению

и реквизиты обратной связи.

КАРТА ПРОЕКТОВ

ITERBI consulting

СОДЕРЖАНИЕ

Контакты

Андрей Волков

Менеджер по развитию бизнеса

Andrey.Volkov@iterbi.ru

Антон Витвицкий

Директор по консалтингу

Anton.Vitvitskiy@iterbi.ru

ОСТАЕМСЯ НА СВЯЗИ

ITERBI consulting

Бизнес Центр Victory Park

119136, Минская 2Ж, г. Москва

+7 (495) 221-77-73

iterbi.ru

СОДЕРЖАНИЕ

КАРТА ПРОЕКТОВ

ITERBI consulting

СПАСИБО

Надеемся на долгосрочное сотрудничество.