
CYBER NOVA
Ваш надежный
партнер в сфере
КиберБезопасности

О компании

CYBERNOVA — Ваш надежный партнер по обеспечению **результативной кибербезопасности.** Защищаем бизнес от цифровых угроз, утечек важных данных и корпоративного мошенничества. Разрабатываем клиент ориентированные решения, помогаем выявить и устранить цифровые угрозы для бизнеса. Консультируем по вопросам информационной безопасности, подбираем оптимальные решения с учетом требований и особенностей бизнеса.

25+
Проведено тестирований на проникновение

7+
Расследовано инцидентов ИБ

6+
Призовых мест в CFT

15+
экспертов в области кибербезопасности

Услуги и сервисы для анализа защищенности

CYBER NOVA

Инфраструктура компании

Анализ защищенности
Комплексная услуга проверки инфраструктуры на наличие уязвимостей

Тестирование на проникновение
Услуга направленная на выявление возможности проникновения в сетевую инфраструктуру

Red Team
Комплексная услуга симуляции целевых атак и проверки устойчивости системы безопасности

Социотехническое тестирование
Услуга проверки устойчивости сотрудников к атакам методами социальной инженерии

Приложения

Анализ защищенности приложений
Поиск уязвимостей и недекларированных возможностей

Анализ защищенности приложений позволяет РУКОВОДИТЕЛЮ:

CYBER NOVA

Выявить возможность проникновение в инфраструктуру компании

Выявить недекларированные возможности приложений

Определить способы получения несанкционированного доступа конфиденциальным данным

Проверить на соответствие требованиям регуляторов

**Получите независимую оценку безопасности*

Состав услуги

CYBERNOVA

Методы:
черный, серый, белый ящик

Срок проведения:
от 2 недель

Проверяем возможность осуществить несанкционированный доступ (НСД)

НСД к ресурсам компании	Серверам, локальной сети, интеллектуальной собственности
НСД к ресурсам приложений	Персональным и платежным данным пользователей или любой другой информации, которую обрабатывают приложения

Даем рекомендации по устранению уязвимостей для предотвращения НСД и его последствий

Эксперты CYBERNOVA

Этапы работ

CYBER NOVA

0

Планируем проект и выбираем подход к проведению анализа защищенности

1

Собираем информацию об объекте тестироания

2

Проводим анализ защищенности

3

Готовим итоговый отчет с информацией для руководителей и специалистов

4

Выполняем контрольную проверку устранения уязвимостей *

* - контрольная проверка устранения уязвимостей проводится опционально

Возможности для **руководителя**

CYBER NOVA

Результаты работы фиксируются в едином документе и позволяют:

- выявить возможные репутационные и финансовые угрозы
- определить, в достаточной ли мере вы контролируете безопасность компании
- вовремя узнать о некачественной работе подрядчиков или критических ошибках в собственной разработке
- получить информацию для принятия стратегических решений по дальнейшему развитию компании
- соответствовать требованиям регуляторов

Посмотреть полный отчет можно здесь:

Анализ защищенности веб-приложений

Анализу защищенности мобильных приложений

Возможности для **специалиста**

CYBER NOVA

- Узнать векторы атак, развитие которых может привести к компрометации компании
- Устранить уязвимости до того, как ими воспользуется злоумышленник
- Выявить уязвимые и слабые места используемых технологий
- Ознакомиться с лучшими практиками по безопасной разработке, которые подходят для вашего бизнеса

Посмотреть полный отчет можно здесь:

Анализ веб-приложений

Анализ мобильных приложений

Пример описания уязвимостей

SQL Injection	Атака оснвана на внедрении кода, когда контролируемые пользователем параметры используются при составлении запросов к БД напрямую. Сложность эксплуатации – легко Тип - удаленная Сложность обнаружения – легко	**10.0**	OWASP SQL Injection: https://www.owasp.org/index.php/SQL_Injection Public exploit: http://www.exploit-db.com/exploits/22877/ CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') http://cwe.mitre.org/data/definitions/89.html	OWASP top 10 A1 Injection CWE-89: Improper Neutralization of Special Elements used in an SQL Command

Пример эксплуатации уязвимостей

```
[14:49:45] [INFO] NULL connection is supported with GET header 'Range'
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: URI
Parameter:
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: http://                                          /397 AND (SELEC
T 7896 FROM(SELECT COUNT(*),CONCAT(0x3a7564643a,(SELECT (CASE WHEN (7896=7896) T
HEN 1 ELSE 0 END)),0x3a7466623a,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARA
CTER_SETS GROUP BY x)a)

    Type: stacked queries
    Title: MySQL > 5.0.11 stacked queries
    Payload: http://                                          '397; SELECT SL
EEP(5)--

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: http:/                                           AND SLEEP(
5)
---
[14:49:45] [INFO] testing MySQL
```

Наши компетенции

CYBER NOVA

Профессионализм наших сотрудников подтвержден ведущими международными организациями

Offensive Security Web Expert

Offensive Security Certified Professional

Offensive Security Wireless Professional

Offensive Security Certified Expert

CREST Registered Penetration Tester

Certified Information Systems Security Professional

Certified Ethical Hacker

Blockchain Security Professional

Остались вопросы?

CYBER NOVA

Свяжитесь с нами

Мы проведем брифинг и ответим на ваши вопросы

Выберем подходы к анализу защищенности с учетом специфики вашего бизнеса

Согласуем ход проекта

Проведем анализ защищенности