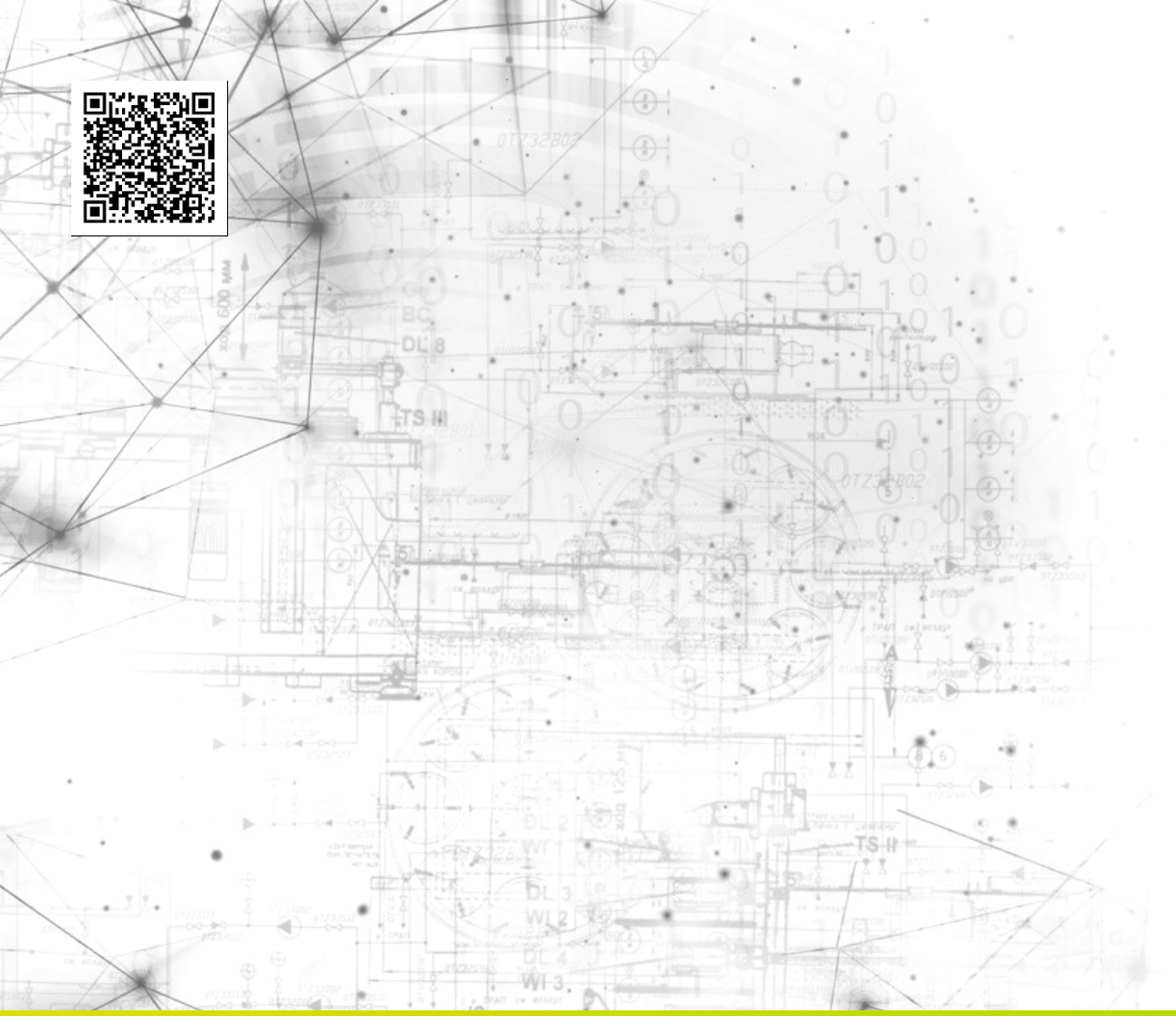


Simplity
CYBERSECURITY

КАК НЕ БОЯТЬСЯ ХАКЕРОВ И НАЧАТЬ СПАТЬ СПОКОЙНО?

ВАМ НУЖЕН БЕЛЫЙ ХАКИНГ

02

УСПЕХИ ХАКЕРОВ В РОССИИ

Simplity
CYBERSECURITY

Более
6 трлн. руб

Превысили суммарные потери российской экономики от атак хакеров

Более
4 раз

Составил рост киберинцидентов в российских компаниях

Более
96 %

Крупнейших компаний России уязвимы для хакеров

В 100% организаций была доказана возможность получить привилегии администратора домена (это значит злоумышленник сможет выполнять любые действия в инфраструктуре компании)

Около
50 %

Атак на информационные системы составляет взлом сервисов доступных на периметре

Остальные атаки связаны с фишинговыми рассылками, атаками через подрядчиков и использования вредоносного программного обеспечения

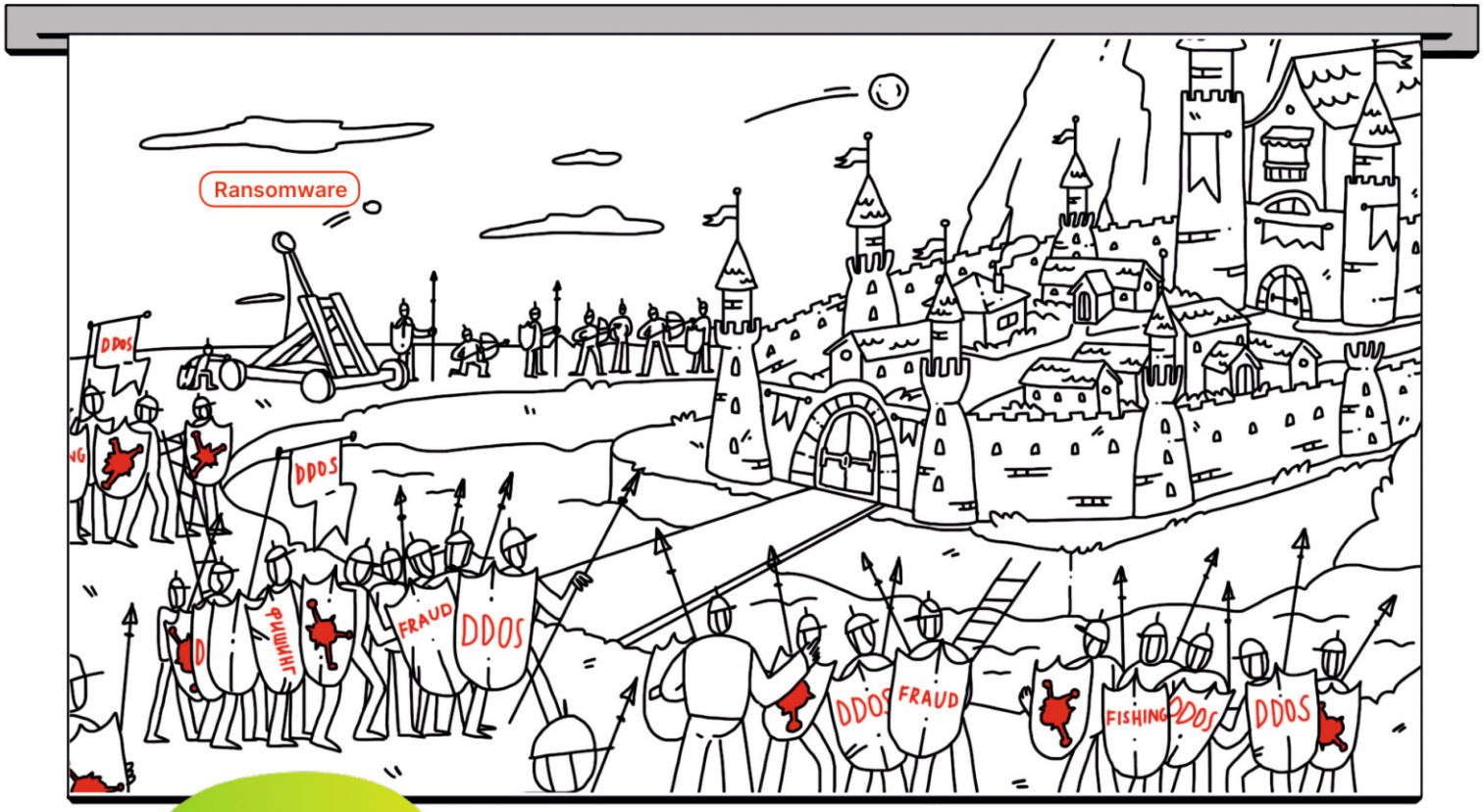
Менее
6 дней

Требуется в среднем на то, чтобы злоумышленнику получить доступ во внутреннюю сеть компании

03

БЕЛЫЙ ХАКИНГ
ПРОСТО О СЛОЖНОМ

Simplity
CYBERSECURITY



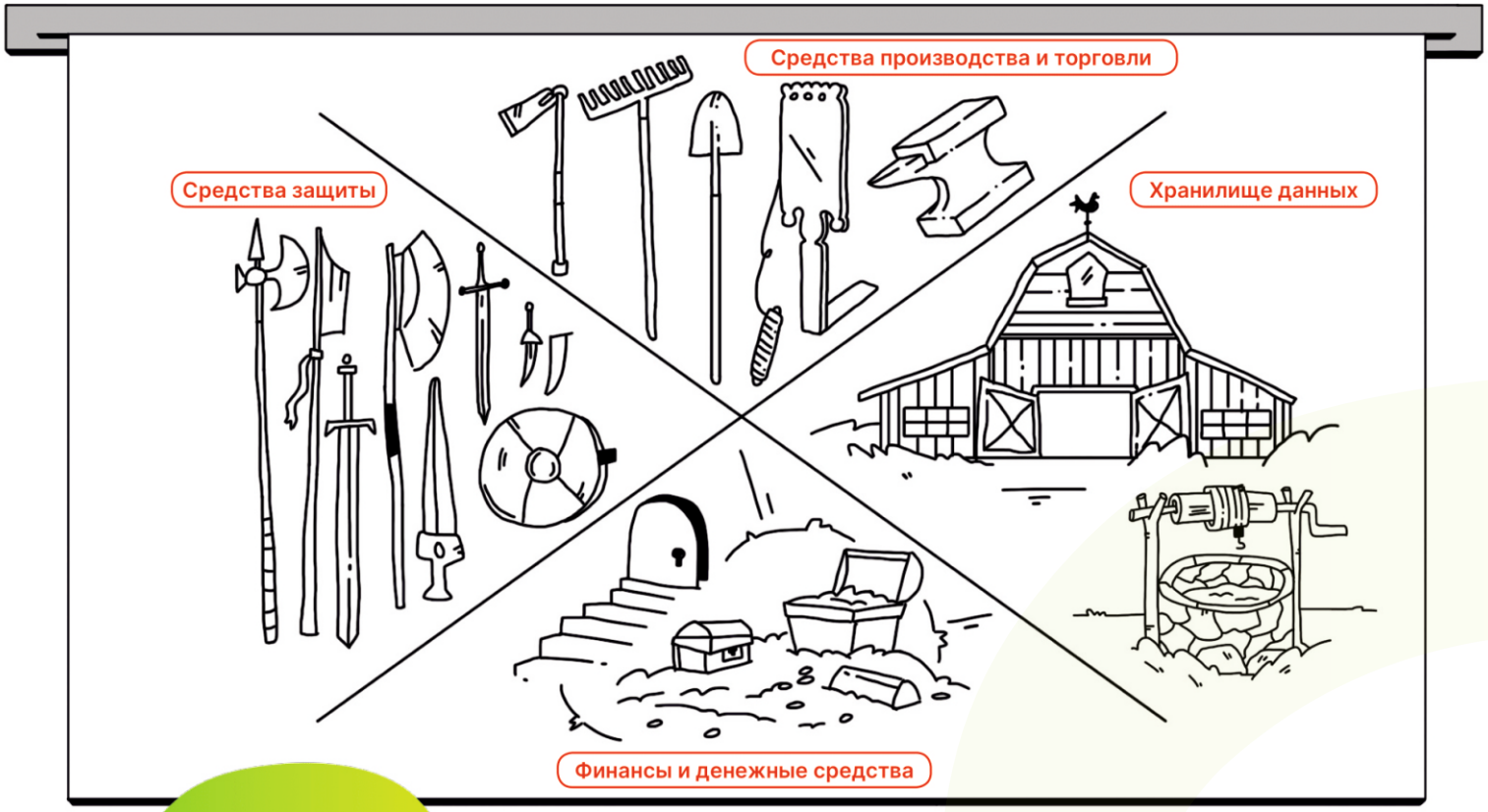
Мы можем представить любую современную Организацию в цифровом пространстве, как осажденный недоброжелателями Город

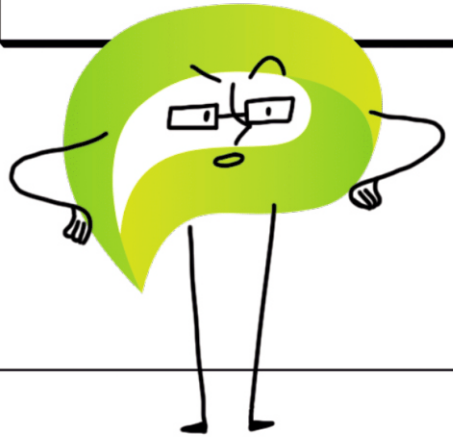
Этот Город производит товары, услуги, активно развивается, в этом Городе живут жители, в него приходят гости

04

БЕЛЫЙ ХАКИНГ
ПРОСТО О СЛОЖНОМ

Simplity
CYBERSECURITY



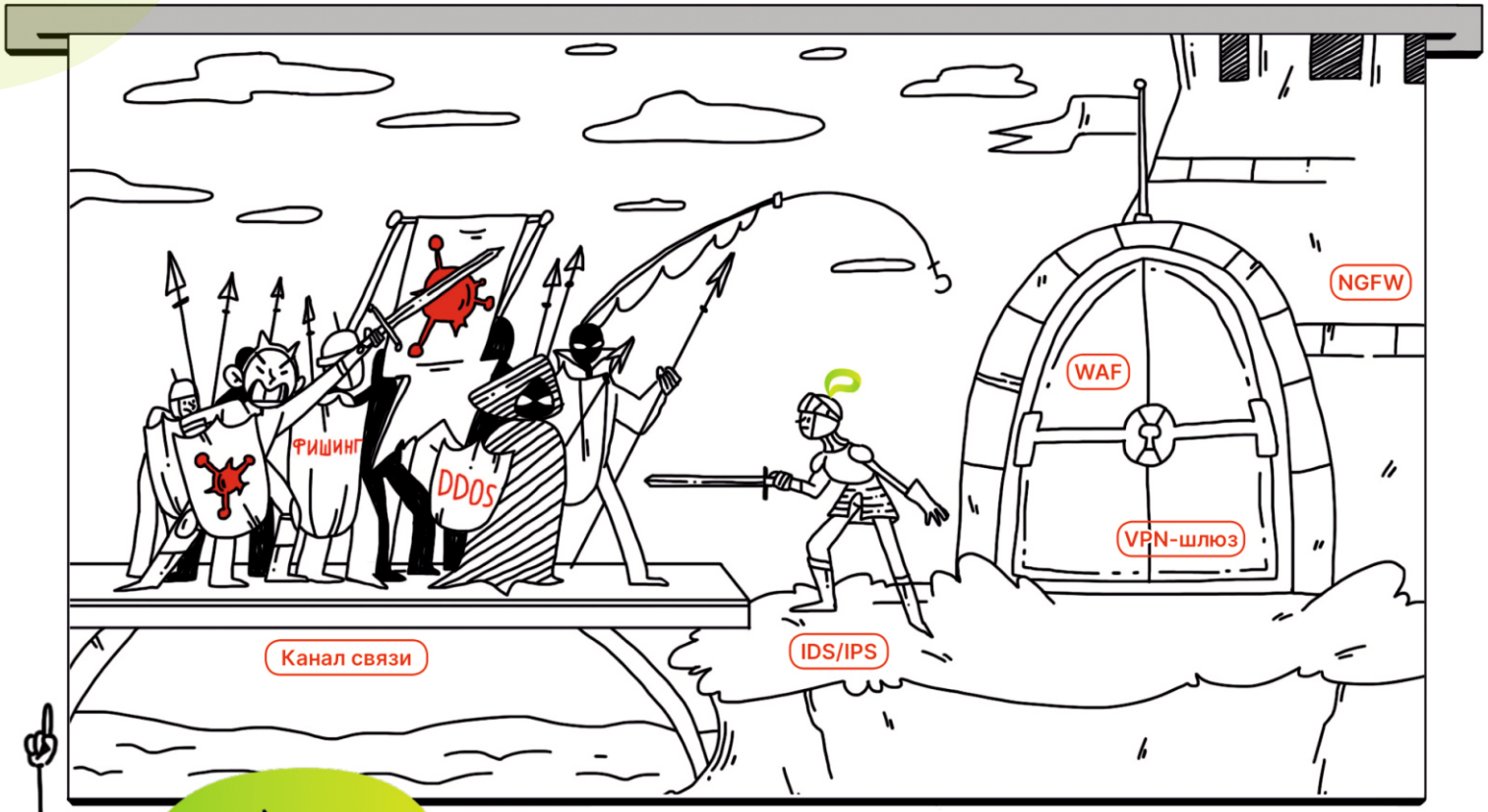


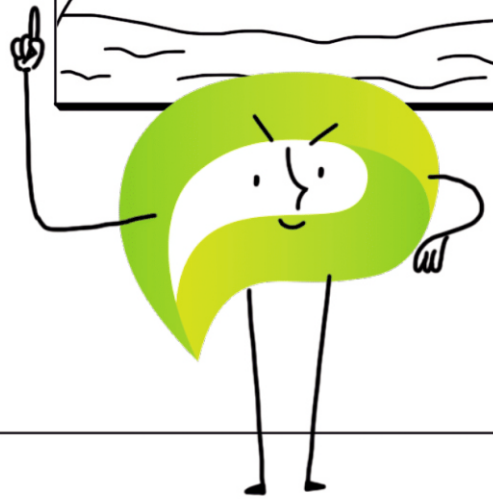
В Городе есть ключевые ресурсы, без которых Город может погибнуть

05

БЕЛЫЙ ХАКИНГ
ПРОСТО О СЛОЖНОМ

Simplity
CYBERSECURITY





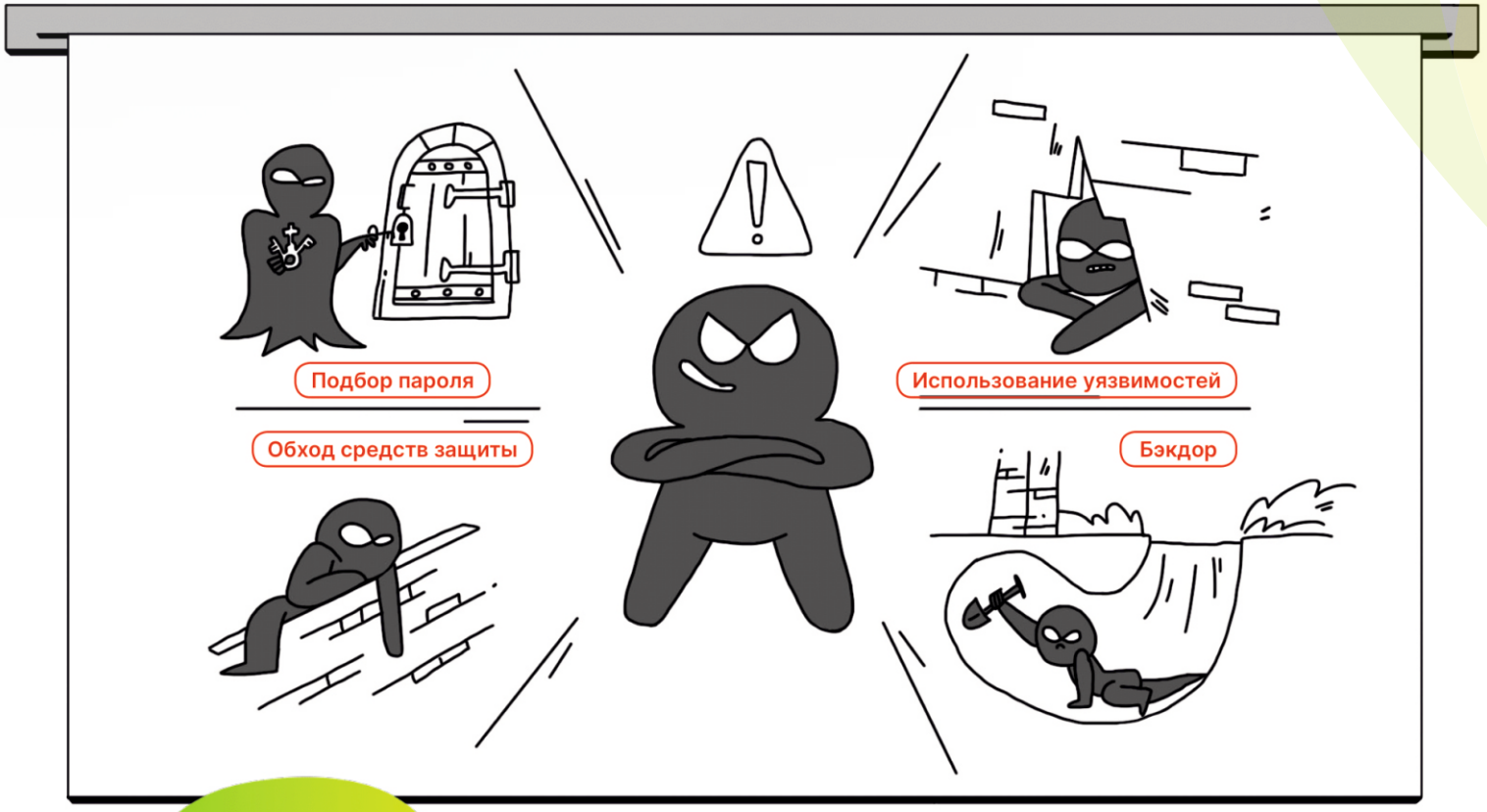
От внешних врагов Город (Организацию) защищают крепкие стены и бдительные караульные

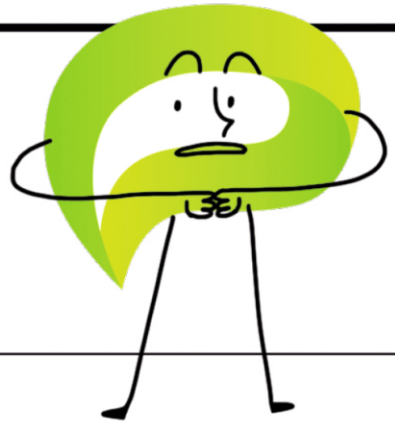
- Где стены – технические средства, установленные на границе между внутренней сетью и Интернетом
- Ворота – интерфейс доступа к ресурсам Организации для легитимных пользователей
- Мост через ров – канал связи
- А караульные – это средства антивирусной защиты, обнаружения вторжений, ИБ служба и тому подобное

06

БЕЛЫЙ ХАКИНГ
ПРОСТО О СЛОЖНОМ

Simplity
CYBERSECURITY



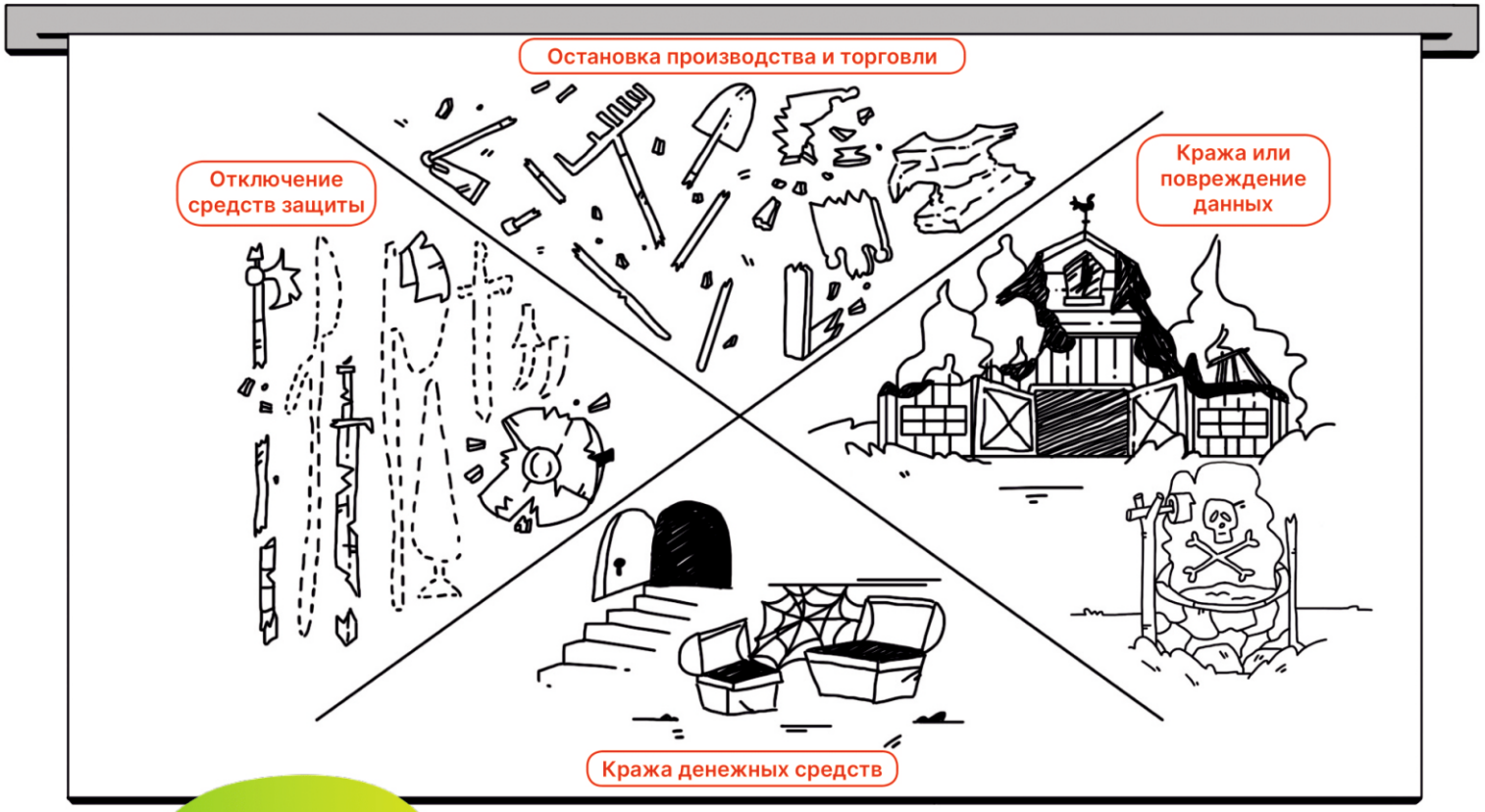


Но помимо обычных угроз (DDOS, Вирусы, Ransomware, Fraud, Фишинг) особую опасность представляет спец-наз киберпреступности – Хакеры
Для проникновения они используют всевозможные уязвимости (к примеру, не установленные вовремя обновления)

07

БЕЛЫЙ ХАКИНГ
ПРОСТО О СЛОЖНОМ

Simplity
CYBERSECURITY

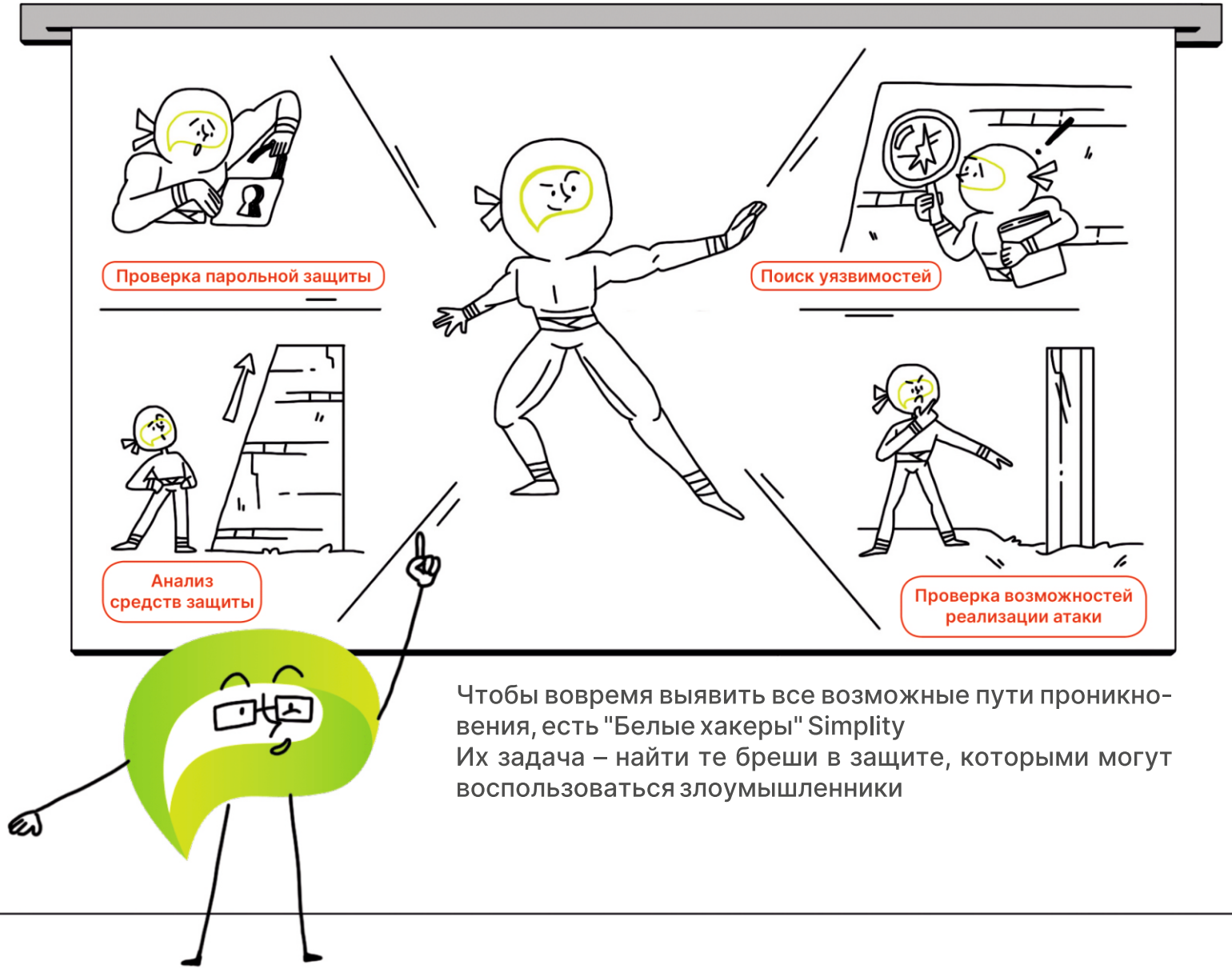


Проникнув во внутреннюю сеть Организации, хакеры могут нанести непоправимый ущерб

08

БЕЛЫЙ ХАКИНГ
ПРОСТО О СЛОЖНОМ

Simplity
CYBERSECURITY

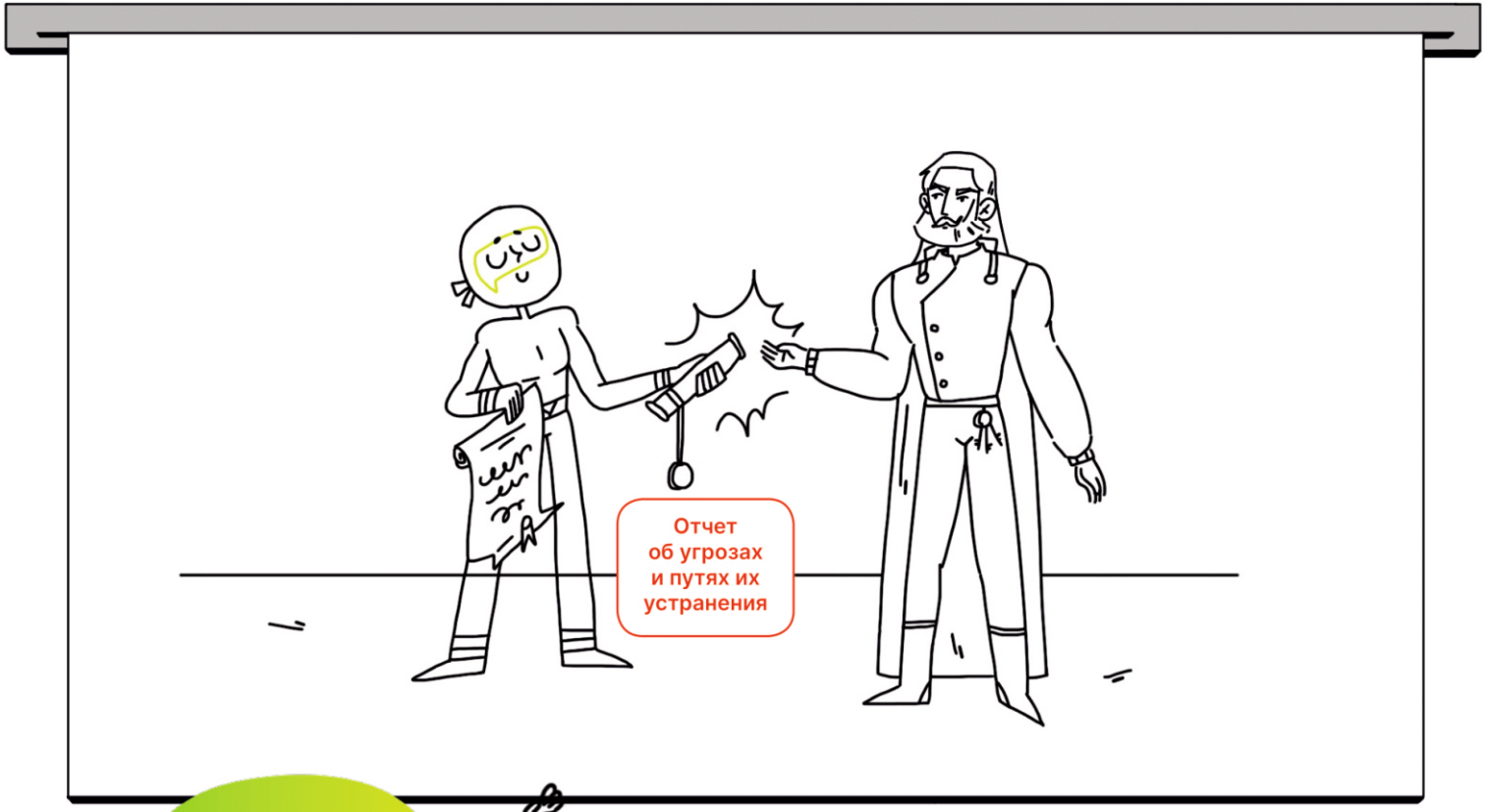


Чтобы вовремя выявить все возможные пути проникновения, есть "Белые хакеры" Simplity
Их задача – найти те бреши в защите, которыми могут воспользоваться злоумышленники

09

БЕЛЫЙ ХАКИНГ
ПРОСТО О СЛОЖНОМ

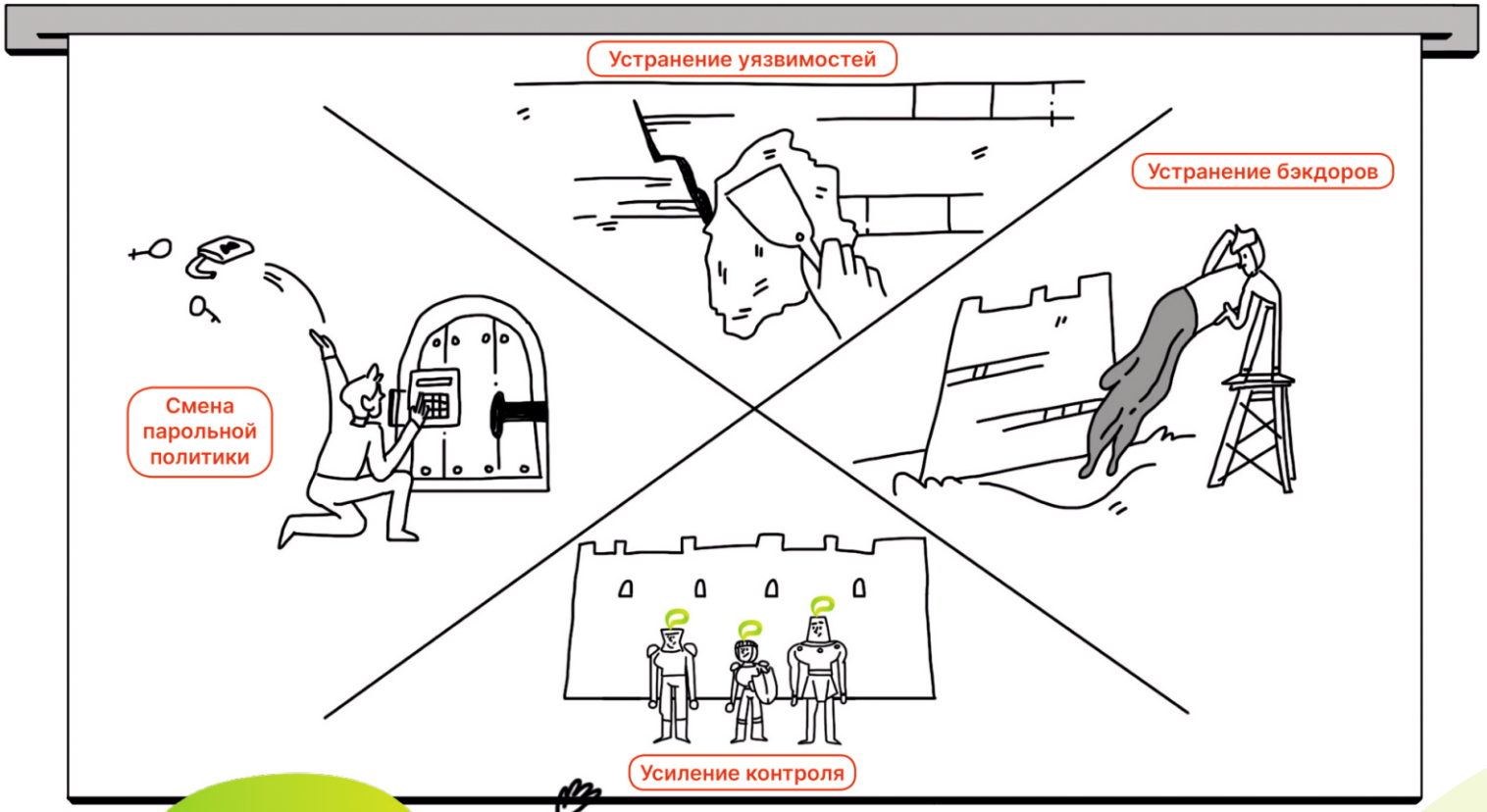
Simplity
CYBERSECURITY



По итогам исследования Simplity предоставляет Клиенту подробный отчет с указанием выявленных уязвимостей, векторов атак, результатов их эксплуатации и перечень мероприятий по устранению угроз

БЕЛЫЙ ХАКИНГ
ПРОСТО О СЛОЖНОМ

Simplity
CYBERSECURITY



В результате Клиент закрывает выявленные угрозы, внедряет необходимые средства защиты и не тратит на ИБ больше чем нужно

БЕЛЫЙ ХАКИНГ ДО 10 РАЗ СНИЖАЕТ ВЕРОЯТНОСТЬ УСПЕХА ТАРГЕТИРОВАННЫХ АТАК ХАКЕРОВ

Simplity
CYBERSECURITY

Более
90%

Уязвимостей организаций позволяют вовремя закрывать периодическое проведение силами «белых хакеров» тестов на проникновение, учебных фишинговых атак и исследований Darknet

Белый хакинг позволяет кратно повышать навыки сотрудников организаций противостоять методам социальной инженерии хакеров

Увеличение эффективности

Увеличивается эффективность использования уже имеющихся у Вас средств защиты

Снижение простоев

Уменьшается время простоя Вашего производства и точек продаж, вызванное атаками хакеров, а значит, вы не теряете время и деньги

Обоснованность

Затраты на ИБ становятся обоснованными и счетными. Вы покупаете и внедряете только то, что реально защищает Ваше производство, продажи, данные работников и клиентов

АУТСОРСИНГ ОТ SIMPLITY
НАШИ КЛИЕНТЫ НЕ ПОПАДАЮТ В НОВОСТИ О ЖЕРТВАХ АТАК ХАКЕРОВ

Simplity
CYBERSECURITY

Госсектор

Являемся доверенным ИБ подрядчиком для государственных корпораций, министерств и ведомств

Частный сектор

Являемся подрядчиком крупнейших российских частных компаний

Лицензии

Имеем все необходимые лицензии ФСТЭК и ФСБ России

Акредитация

Входим в реестр аккредитованных организаций, осуществляющих деятельность в области информационных технологий Министерства цифрового развития, связи и массовых коммуникаций РФ

13

БЕЛЫЙ ХАКИНГ ЭТО ДОРОГО?
НЕТ, С SIMPLITY ЭТО НЕ ТАК

Simplity
CYBERSECURITY

Потратив от
500 тыс. руб

Средняя по размеру организация, по нашему опыту, может получить ощутимый результат

Прозрачное ценообразование

Стоимость зависит от числа элементов вашей инфраструктуры, подлежащих исследованию: числа исследуемых хостов и web-сервисов

Гибкий подход

Можно не устраивать тотальную проверку всего, а отобрать пробные и особо критичные сегменты и сервисы

Выберите только важное

Из всего перечня услуг Белый хакинг вы можете выбрать только важные для себя

Понятная калькуляция

Калькуляция цены от Simplity очень наглядная и доступная

ЧТО ДАЛЬШЕ?

Изучите
презентацию

Выберите
заинтересовавшие
Вас услуги

Свяжитесь с нами
и заполните предоставленный
опросный лист для подготовки
для Вас коммерческого
предложения

Заключите
с нами контракт
на оказание услуг

Получите
отличный результат
и не бойтесь хакеров

ТЕПЕРЬ ВЫ С Simplity CYBERSECURITY

ГОТОВЫ ОТВЕТИТЬ НА ЛЮБЫЕ ВАШИ ВОПРОСЫ

+7 (499) 288-88-18
WWW.SIMPLITY.EXPERT
PRODUCTS@SIMPLITY.EXPERT

ТЕХНИЧЕСКОЕ ПРИЛОЖЕНИЕ

БЕЛЫЙ ХАКИНГ ОТ SIMPLITY
ПРЕДЛАГАЕМ

Simplity
CYBERSECURITY

Black/white box

Исследование по моделям black/ /grey/whitebox текущего состояния Ваших ИТ

Darknet

Поиск сведений в отношении Вашей организации в Darknet (учетные данные и уязвимости, выставленные на продажу, базы данных и так далее)

Red team

Оценка реагирования уже имеющихся у Вас средств ИБ на тестовые атаки наших специалистов

Vulnerability

Поиск уязвимостей и определение способов их эксплуатации

Exploit

Эксплуатация уязвимостей и проверка способов получения доступа к Вашим целевым системам

Фишинг

Проведение тестовых и учебных атак на Ваших сотрудников с использованием методов социальной инженерии

Снижение рисков

Подготовка перечня конкретных действий по устранению найденных уязвимостей, по повышению уровня защищенности ИТ и снижению вероятности успеха таргетированных атак хакеров

БЕЛЫЙ ХАКИНГ
ИСПОЛЬЗУЕМЫЕ МЕТОДЫ И ИНСТРУМЕНТЫ

Simplity
CYBERSECURITY

Разведка

Первоначальный сбор информации об инфраструктуре производится в ручном режиме и автоматизированными средствами, в том числе собственной разработки

Атаки

В обязательном порядке анализируется возможность проведения специфичных атак:

- NTLM-Relay,
- Pass-the-hash,
- Kerberoasting,
- Delegation attacks,
- атаки на ADCS,
- и многие другие

Анализ

В процессе анализа защищенности используются как известные методики OSSTMM, OWASP, SANS, так и собственные подходы

WEB

Веб ресурсы тестируются в том числе на наличие инъекций:

- SQL injection
- LDAP injection
- XML injection
- SSI injection
- Xpath injection
- Code injection

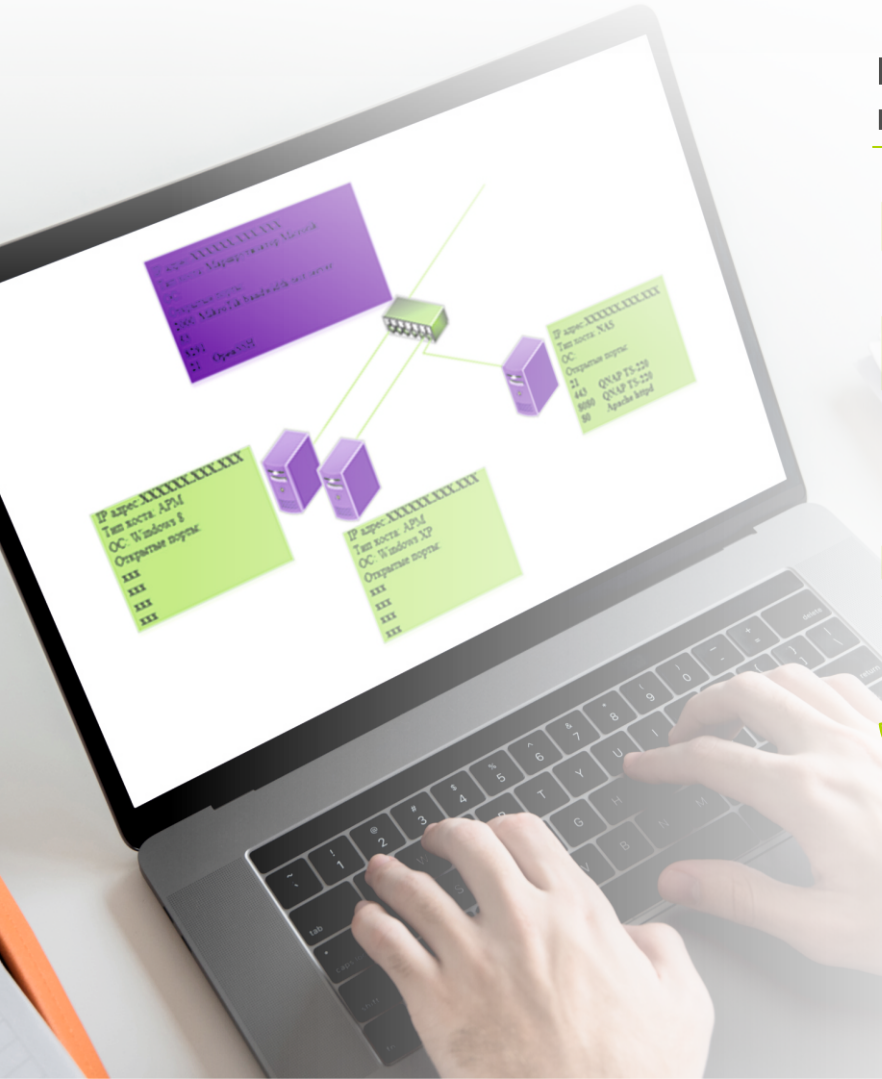
Social

В качестве «вишенки на торте» применяются методы социальной инженерии:

- адресный фишинг как стандартный, например, письмо от портала Госуслуги, ИФНС, так и более творческий, глубоко проработанный
- сбор информации из открытых источников
- заход через социальные сети
- имперсонация

БЕЛЫЙ ХАКИНГ
ИССЛЕДОВАНИЕ ТЕКУЩЕГО СОСТОЯНИЯ ИТ

Simplity
CYBERSECURITY



Вы получите карту ИТ инфраструктуры с указанием

- Типа хостов
- Наименования и версии ОС или прошивки
- IP-адреса
- Открытых портов, опубликованных служб
- Наличия критических уязвимостей

В процессе тестирования по модели whitebox в обязательном порядке сверяем реальное состояние хостов с заявленными Вами эталонными

На карте ИТ инфраструктуры указываем хосты, несоответствующие переданным Вами эталонным параметрам, а также описываем суть несоответствий

19

БЕЛЫЙ ХАКИНГ
ПОИСК УЯЗВИМОСТЕЙ И ОПРЕДЕЛЕНИЕ СПОСОБОВ ИХ ЭКСПЛУАТАЦИИ

Simplity
CYBERSECURITY

Передаем Вам

Vulnerability

Перечень обнаруженных уязвимостей хостов

Атаки

Описание векторов атаки, направленных на получение привилегированного доступа к элементам IT

Результаты будут представлены в таблице

DNS имя	IP- адрес	Обнаруженная уязвимость	Вектор атаки	Критичность	Технология реализации

«Уязвимость CVE-2020-1472 Zerologon позволяет нарушителю выдать себя за компьютер-клиент и заменить пароль контроллера домена. В результате атакующий может получить права администратора домена.
Степень риска для КИС — критическая.
Рекомендации по снижению выявленного риска
Необходимо применить обновления безопасности, рекомендованные производителем ПО Microsoft KB4601348 (дата выпуска 9.02.2021).»

20

БЕЛЫЙ ХАКИНГ
ПОИСК СВЕДЕНИЙ В DARKNET

Simplity
CYBERSECURITY

Поиск

Передаем Вам найденные в Darknet сведения с указанием ссылок на площадку размещения и никнеймов лиц, разместивших информацию

Закупка

По Вашему указанию мы проведем контрольную закупку с передачей полученных данных для тестирования

Результаты будут представлены в таблице

Ссылка на площадку	Никнейм разместившего сведения	Характер размещенных сведений (БД, учетные данные, уязвимость «нулевого дня»)	Контрольная закупка (осуществлялась/ не осуществлялась)	Достоверность данных

21

БЕЛЫЙ ХАКИНГ
ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

Simplity
CYBERSECURITY

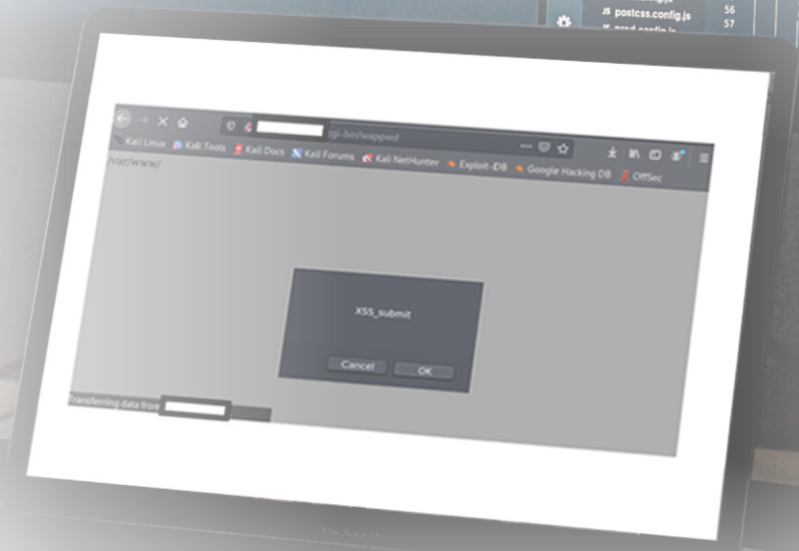
Эксплуатация

На этом этапе мы осуществляем практическую эксплуатацию найденных уязвимостей и реализуем векторы атак

Результат

В результате получаем учетные данные к целевому элементу ИТ, выполняем произвольный код на узле и тому подобное

Эксплуатация осуществляется только по Вашему указанию



POST /cgi-bin/wappwd HTTP/1.1 host: 95.84.146.180 Accept: */* Accept-Encoding: deflate, gzip user-agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebkit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.122 Safari/537.36 pragma: no-cache cache-contr ol: no-cache content-type: application/x-www-form-urlencoded Content-Length: 113
FILEOK=camera.htm&FILEFAIL=<script>confirm(«XSS_Submit»)</
При внедрении в указанный параметр Веб-страницы вредоносного кода, при заходе пользователя на сайт, возможен перехват передаваемых пользовательских данных (в том числе учетных) и передаче их нарушителю по каналам связи, что в дальнейшем ведет к компрометации всего узла и развитии атаки на внутреннюю инфраструктуру организации.

22

БЕЛЫЙ ХАКИНГ
ОЦЕНКА РЕАКЦИИ СРЕДСТВ ИБ НА АТАКИ

Simplity
CYBERSECURITY

Моделирование

Задачей настоящего этапа является моделирование достаточности или недостаточности уже применяемых Вами средств защиты для детектирования и предотвращения эксплуатации найденных векторов атак без устранения уязвимостей на хостах

Оценка

При оценке обязательно учитывается наличие у Вас средств обнаружения и предотвращения атак и прочих решений и методов, которые могут быть искусственно не задействованы на этапе поиска и эксплуатации уязвимостей

Результат

Результатом выполнения этапа является аналитическая записка с описанием для каждого опробованного вектора атак уже применяемых мер ИБ, а также результатов моделирования

23

БЕЛЫЙ ХАКИНГ
ТЕСТОВЫЕ АТАКИ МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Simplity
CYBERSECURITY

Методика

В качестве базовой методики социальной инженерии используются фишинговые рассылки.
Инструмент может быть развернут внутри Компании на выделенных виртуальных ресурсах (данные за периметр не предаются)

Учитываем реальные бизнес процессы

Самостоятельно или совместно с Вами формируются шаблоны фишиногвых писем на основе особенностей бизнес-процессов Вашей организации, формируются группы рассылок, а также график

По отдельному запросу мы можем использовать и другие методы социальной инженерии

24

БЕЛЫЙ ХАКИНГ
ТЕСТОВЫЕ АТАКИ МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Simplity
CYBERSECURITY

Статистика

По результатам реализации запланированных программ рассылок Вы получите подробную статистику по действиям пользователей при получении фишинговых писем

Результаты будут представлены в таблице

Письмо открыто

Пользователь прошел по ссылке

Пользователь ввел данные в поддельное окно авторизации

25

БЕЛЫЙ ХАКИНГ
ВЫРАБОТКА РЕКОМЕНДАЦИЙ

Simplity
CYBERSECURITY

Снижение рисков

Вы получите перечень мероприятий по снижению рисков реальной эксплуатации хакерами выявленных векторов атак

Результаты будут представлены в таблице

Хост	Вектор атаки/ уязвимость	Необходимость в мероприятиях по снижению риска	Предполагаемые мероприятия по снижению риска эксплуатации	
			Технические мероприятия	Организационные мероприятия

Simplity
CYBERSECURITY

ООО "Вымпел-Профит"
121351, Россия, Москва, ул. Бобруйская, д. 1
+7 499 288 88 18
e-mail: info@simplity.expert
www.simplity.expert