Маргарита Гаврилова
Руководитель развития
консалтинговых проектов

Экспертные сервисы по кибербезопасности

О спикере

Маргарита Гаврилова

Руководитель развития
консалтинговых проектов

Более 7 лет в практической кибербезопасности:

удалось поучаствовать в проектах
по информационной безопасности как на стороне
заказчика, так и на стороне вендора

Что входит в мои обязанности:

- Выявление потребностей заказчика и составление планов проведения работ по анализу защищенности и другим услугам
- Разработка и актуализация методологической базы услуг по кибербезопасности
- Управление проектами по информационной безопасности на всех стадиях

О чём поговорим?

- Экспертные направления Positive Technologies: Offensive и Defensive сервисы
- Что важно учесть при выборе сервиса по кибербезопасности
- Как подготовиться к проведению работ и получить максимальную пользу от услуги

Статистическая справка

56% киберинцидентов заканчиваются **утечками данных**

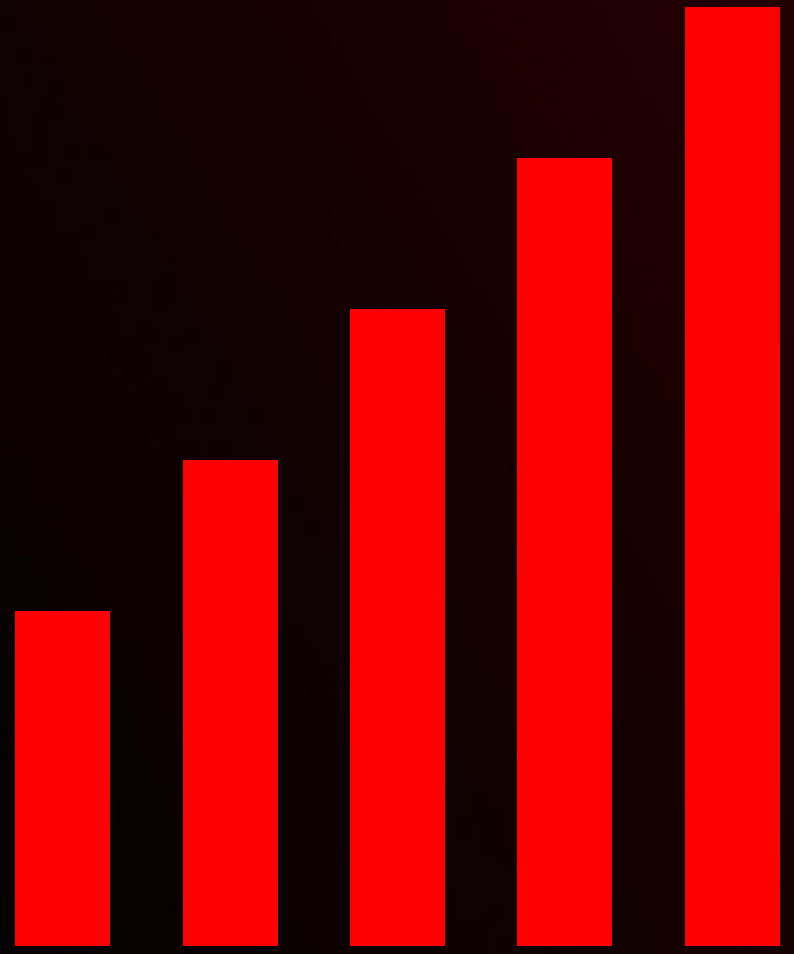
39% киберинцидентов заканчиваются **нарушением основной деятельности** организации

32% атак начинаются с **эксплуатации уязвимостей** на сетевом периметре

в 57% инцидентов злоумышленники остаются незамеченными в инфраструктуре **более месяца**

в 16% инцидентов злоумышленники остаются незамеченными в инфраструктуре **более полугода**

$ 8,7 трлн составил общий ущерб от кибератак во всём мире в 2023 году



Какие цели преследуют реальные хакеры?

Финансовые потери

Вывод денежных средств со счетов Организации или ее клиентов

Утечка конфиденциальных данных

Утечка/кража информации, составляющей коммерческую тайну, ПДн клиентов и т.д.

Прерывание функционирования

Остановка работы сервисов на длительный срок.

Утрата или искажение операционных и резервных данных

Удаление документов в системе ЭДО в результате работы ВПО.

Сервисы безопасности

OFFENSIVE SERVICES

Проводим атаки на инфраструктуру, ищем и эксплуатируем уязвимости — действуем как реальный злоумышленник, чтобы найти «слабые места» информационной безопасности Организации.

DEFENSIVE SERVICES

Выявляем факты компрометации инфраструктуры, реагируем и расследуем инциденты — делимся своей экспертизой и приходим на помощь в случае реальной атаки.

01

Offensive Services

Оценка киберустойчивости

Услуги по анализу защищенности

Команда PT-SWARM

Более 100 высококвалифицированных экспертов по анализу защищенности, специализирующихся на различных направлениях: тестирование на проникновение инфраструктуры, имитация атак APT-группировок, поиск уязвимостей в веб-приложениях, системах дистанционного банковского обслуживания, смарт-контрактах и тд.

Анализ защищенности инфраструктуры

Выявим векторы компрометации инфраструктуры путём проведения подконтрольных атак.

Анализ защищенности отдельных объектов инфраструктуры

Выявим уязвимости и недостатки в обеспечении безопасности, а также предоставим рекомендации по их устранению.

Тестирование на проникновение

Тестирование на проникновение (pentest) — услуга по поиску векторов компоромментации инфраструктуры.

Направления тестирования:

Внешнее тестирование

Проверка возможности преодоления сетевого периметра внешним нарушителем, действующим со стороны.

Тестирование беспроводных сетей

Выявление недостатков в архитектуре и организации беспроводного доступа, доступных реальному злоумышленнику.

Внутреннее тестирование

Проверка возможности получения доступа к критически важным системам и повышения привилегий со стороны нарушителя, находящегося или получившего доступ к сегменту сети.

Социотехническое тестирование

Оцениваем осведомленность сотрудников в вопросах ИБ, при помощи тестов, эмулирующих распространенные сетевые атаки с использованием методов социальной инженерии.

Особенности работ

Атаки проводятся **без сопротивления** со стороны SOC Заказчика

Методы анализа

Черный ящик: анализ **без знаний** внутреннего устройства системы

Red Team

Red Team — услуга по оценке эффективности защиты корпоративной инфраструктуры Организации путём имитации целенаправленной и скрытой атаки, проводимой экспертами Positive Technologies.

Наш подход:

Собираем информацию с целью поиска путей проникновения внешнего нарушителя в инфраструктуру. Проводим фишинговые атаки и атаки на беспроводные сети без уведомления.

Проникаем в максимальное количество сегментов инфраструктуры.

Закрепляемся в инфраструктуре: расширяем зону контроля над инфраструктурой и максимально скрываем следы своего пребывания.

Получаем контроль/доступ, максимальные привилегии в критичных системах Организации.

Задача вашей команды ИБ — оказывать сопротивлени атакам

Задача наших экспертов — не дать себя обнаружить в ходе реализации атак

В чем секрет эффективности?

Подготовка: обозначаем границы работ

Задействуем все виды атак, доступные потенциальному злоумышленнику

Помимо имитации атак на объекты периметра проводим **социотехнические атаки** на сотрудников, а также **анализируем беспроводные сети** с целью преодоления периметра.

Расширяем поверхность атаки сетей

Включаем в границы работ не только головную организацию, но и **дочерние зависимые общества**.

Смотрим глазами потенциального злоумышленника

Исполнитель проводит OSINT для **формирования перечня сетевых объектов** периметра Заказчика.

В чем секрет эффективности?

Ход работы: ставим цели для обеих сторон

Не накладываем ограничений по режиму работы
Атаки должны проводиться не только в рабочее время, но и в выходные дни. Оптимальный режим работ: 24/7.

Ставим цели для команды нападения
Совместно формируем перечень нежелательных событий/сценариев для верификации.

Работаем в режиме максимальной скрытности
Команда атакующих меняет IP-адреса, перечень IP-адресов не передаётся команде защиты.*

Реагирование и расследование инцидентов
Факт проведения работ не доносится до команды защиты. Реагирование на атаки должно происходить в штатном режиме.*

*актуально для redteaming

Анализ защищенности отдельных объектов

Какие компоненты корпоративной инфраструктуры и зачем анализируем?

Веб-приложения
для выявления уязвимостей, которые могут быть использованы для компрометации программного обеспечения, обхода бизнес-логики или нарушения взаимодействия между клиентской и серверной частями.

Блокчейн приложения
для оценки возможности реализации атак на программное обеспечение приложения, функционирование смарт-контрактов или нарушения бизнес-логики смарт-контрактов, лежащих в основе приложения.

Системы дистанционного банковского обслуживания (мобильные и веб-приложения)
для выявления уязвимостей, которые могут быть использованы для компрометации финансовых транзакций, обхода механизмов аутентификации и авторизации, а также искажения бизнес-логики операций клиентов.

Мобильные приложения на базе ключевых ОС iOS, Android, HarmonyOS
для оценки возможности реализации атак на мобильное программное обеспечение, подмены или перехвата данных, обхода механизмов аутентификации, а также нарушения безопасного взаимодействия с серверной частью.

Анализ защищенности отдельных объектов

Существует опция проверки корректности устранения выявленных уязвимостей специалистами Positive Technologies

Черный ящик

Анализ со стороны нарушителя, не имеющего каких-либо привилегий в Системе

Пример — внешний нарушитель, не имеющий учетной записи в приложении

Серый ящик

Анализ со стороны нарушителя, имеющего определенный уровень привилегий в Системе

Пример — пользователь приложения.

Белый ящик

Анализ исходного кода системы

Пример — разработчик веб-приложения

Анализ отдельных ресурсов

Размещение на платформе BUG BOUNTY

Организации определяют список исследуемых приложений или ИТ-систем компании, границы работ и уровень критичности уязвимостей.

За выявленные и подтвержденные уязвимости организации выплачивают независимым исследователям вознаграждения в соответствии с условиями программы.

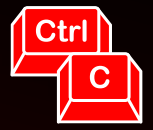
Независимые исследователи, соблюдая условия программы, ищут уязвимости и направляют отчеты о найденных багах организациям.

Компании устраняют уязвимости в соответствии с полученными отчетами, тем самым повышая уровень безопасности своей компании.

PT MAZE

Протектор мобильных приложений

защищает
от обратной разработки



усложняет
копирование приложения

ограничивает нелегальное
использование

Почему мы решили сделать PT MAZE?

Недостаточная защищенность кода — одна из самых расхожих и критически значимых слабостей современных приложений. В основе PT MAZE — многолетний опыт этичных хакеров Positive Technologies по анализу защищенности мобильных приложений.

За более чем **10 лет** анализа защищенности
нам встретилось **только одно приложение**, защиту которого
не удалось преодолеть за выделенное на проект время.

Поддерживает ОС

Android iOS

Комплементарен
ZERO-TRUST
концепции

No-code

SaaS

Нам не нужен доступ к исходному коду приложения,
а наш подход к архитектуре модулей защиты
усложняет путь злоумышленников к уязвимостям.

Сочетает в себе best-practice глобального рынка протекторов и уникальную экспертизу

- Модифицирует вместо дополнения
- Запускается одной кнопкой
- Использует распределенную защиту
- Разработан этичными хакерами

Используется ГОСТ-криптография. Хэш-функция ГОСТ 34.11 -2012 для проверки целостности приложения и подлинности установления TLS-соединения, а также симметричное блочное шифрование ГОСТ 34.12-2015 (ключ 256 бит).

02

Defensive Services

Выявление и реагирование на атаки

Услуги PT ESC

Команда PT ESC

Команда экспертов Positive Technologies, специализирующаяся на выявлении и анализе инцидентов информационной безопасности, расследовании и реагировании на кибератаки, исследовании вредоносного ПО, а также защите бизнеса и публичных мероприятий от современных киберугроз.

Ретроспективный анализ

Проводим поиск следов компрометации прошлых и текущих атак в IT-инфраструктуре

Реагирование и расследование

Восстановим хронологию и обстоятельства инцидента и локализуем атаку

Ретроспективный анализ событий информационной безопасности

> Ретроспективный анализ — поиск следов компрометации инфраструктуры посредством исследования образов систем, журналов событий, дампов памяти и сетевого трафика за определенный промежуток времени.

Направления тестирования:

Есть отраслевые риски

Если отрасль, в которой работает ваша организаций, входит в топ атакуемых и необходимо убедиться, что хакеры не добрались до вашей организации.

Есть подозрения

Если вы обнаружили следы подозрительной активности и хотите проверить был ли взлом и до чего хакеры смогли дотянуться.

Есть факт восстановлений

Если пришлось восстанавливаться из бэкапов по той или иной причине – чтобы убедиться в отсутствии следов компрометации на восстановленных хостах.

Есть изменения

Если в вашей организации обновились политики безопасностии необходимо проверить системы на соответствие новым правилам.

Ретроспективный анализ событий информационной безопасности

Варианты оказания услуги

Специализированный ретроспективный анализ

Ретроспективный анализ событий, зафиксированных отдельными СЗИ: MaxPatrol SIEM, PT NAD, PT AF.

Например:
Ретроспективный анализ событий PT AF — это услуга по анализу событий, зафиксированных WAF, направленная на выявление атак и фактов компрометации веб- приложений, а также разработку рекомендаций по усилению защиты веб-приложения.

Полный ретроспективный анализ

Включает сигнатурное сканирование файловой системы, оперативной памяти узлов инфраструктуры клиента, а также сбор и **глубокий** анализ ретроспективных и текущих forensic- артефактов.

Ретро-lite

Включает сигнатурное сканирование файловой системы, оперативной памяти **наиболее критичных узлов** инфраструктуры клиента, а также сбор и **быстрый** анализ ретроспективных и текущих forensic-артефактов.

Реагирование и расследование инцидента безопасности

Реагирование и расследование инцидента — услуга по восстановлению хронологии событий информационной безопасности, которые привели к инциденту, оценка его критичности и разработка мер по его устранению и предотвращению в будущем.

Когда необходимо реагирование и расследование?

Произошла утечка чувствительных данных или остановка операционной деятельности

Если затронуты чувствительные данные (например, персональные данные, данные, составляющие коммерческую тайну и др.) или произошла остановка операционной деятельности и необходимо корректно зафиксировать произошедший инцидент.

Необходима независимая оценка

Если необходимо независимое подтверждение локализации и устранения инцидента, например, для руководства, акционеров или партнеров

Инцидент выходит за рамки компетенций внутренней команды ИБ

Если у организации не достаточно внутренних ресурсов, инструментов или экспертизы в области цифровой криминалистики и/или анализа вредоносного ПО

Задать вопрос по теме выступления

SecServ@ptsecurity.com

ptsecurity.com

Спасибо!