|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  |  |  |  |
|  | |  |  |  | | --- | --- | --- | |  | **ISS.25** | **Непрерывное тестирование на проникновение** |   **1.1. Описание услуги** | | | | | | |  |
|  | В рамках оказания услуги предполагается выявление и классификация уязвимостей в информационных системах Заказчика. Осуществляется тестирование каналов передачи данных и тестирование на уязвимости доступной сетевой инфраструктуры Заказчика.  Итогом оказания услуги является подтверждение или опровержение рисков информационной безопасности в инфраструктуре Заказчика в виде экспертного заключения (отчёта) с перечнем всех действий, принятых для тестирования системы заказчика, выявленных уязвимостей и детальным планом действий по их устранению и обеспечению защиты ресурсов компании от атак, а также составление предписания для устранения найденных уязвимостей. | | | | | | |  |
|  | **1.2. Способ подключения к ИТ-системе (если необходимо и в зависимости от технической возможности организации)** | | | | | | |  |
|  | * Ярлык на Портале терминальных приложений * Прямая ссылка на Web-ресурс из КСПД * Прямая ссылка на Web-ресурс из интернет (требуется СКЗИ на АРМ / не требуется) * «Толстый клиент» на АРМ пользователя (требуется СКЗИ на АРМ / не требуется) * Другой способ \_\_\_не требуется\_\_\_\_\_\_\_\_\_ | | | | | | |  |
|  | **1.3. Группа корпоративных бизнес-процессов / сценариев, поддерживаемых в рамках услуги** | | | | | | |  |
|  | Для данной услуги не применяется | | | | | | |  |
|  | **1.4. Интеграция с корпоративными ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  |  |  | Для данной услуги не применяется | | | | |  |
|  |  |  | Для данной услуги не применяется | | | | |  |
|  |  |  | Для данной услуги не применяется | | | | |  |
|  | **1.5. Интеграция с внешними ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  |  |  | Для данной услуги не применяется | | | | |  |
|  |  |  | Для данной услуги не применяется | | | | |  |
|  | **1.6. Состав услуги** | | | | | | |  |
|  | Центр поддержки пользователей |  | Для данной услуги не применяется | | | | |  |
|  | Функциональная поддержка |  | В рамках услуги осуществляется реализация модели угроз. С инфраструктурой Заказчика проводятся следующие работы:   1. Согласование с Заказчиком целей тестирования и уровня осведомлённости персонала о проводимых мероприятиях. (возможны три варианта: полная осведомлённость, осведомлённость ответственных сотрудников и нулевая осведомлённость); 2. Разведка инфраструктуры (Инвентаризация информационных систем и их версий); 3. Поиск уязвимостей в ИТ-инфраструктуре (поиск возможных уязвимостей в информационных системах с использованием стороннего ПО свободного распространения и/или с возможностью использования собственного ПО); 4. Согласование целей и методов атак с Заказчиком. 5. Эксплуатация выявленных уязвимостей (подтверждение или опровержение их влияния); 6. Повышение привилегий в системе, к которой получен доступ (после данного шага может повториться пункт 1); 7. Составление экспертного заключения (отчёта) c подробным отчётом с перечнем проведённых работ, списком уязвимостей с примерами эксплуатации, рекомендациями по их устранению, риски, связанные с данными уязвимостями, схемами целевых атак и, в случае необходимости, оценка реагирования личного персонала на действия группы red team. 8. Взаимодействие команды Red team с подразделением, обеспечивающим защиту информации, с целью оказания помощи в устранении указанных в отчёте уязвимостей. 9. Контроль исправления уязвимостей. 10. Предотвращение утечек информации об уязвимостях заказчика | | | | |  |
|  | Поддержка интеграционных процессов |  | Для данной услуги не применяется | | | | |  |
|  | ИТ-инфраструктура |  | Для данной услуги не применяется | | | | |  |
|  | Модификация ИТ-системы |  | Для данной услуги не применяется | | | | |  |
|  | **1.7. Наименование и место хранения пользовательской документации:** | | | | | | |  |
|  | * ИТ-система |  | Для данной услуги не применяется | | | | |  |
|  | * Портал Госкорпорации «Росатом» |  | Для данной услуги не применяется | | | | |  |
|  | * Иное место |  | Для данной услуги не применяется | | | | |  |
|  |  |  |
|  |  |  |
|  | **1.8. Ограничения по оказанию услуги** | | | | | | |  |
|  | Непрерывное тестирование на проникновение возможно только после проведение первичного тестирования.  Тестирование может затрагивать виртуальные и физические серверы в различных сегментах сети (в том числе в зоне теста и разработки), а также рабочие места пользователей  Следующие нормативы услуги не применяются в случае наличия у заказчика услуги ISS.23:   * Рассылка персональных фишинговых писем – 0,001 ПРМ (Единица измерения – работник, единожды в рамках отчётного периода) * Рассылка персональных фишинговых писем – 0,0005 ПРМ (Единица измерения – работник, ежемесячные работы)   Для оказания услуги необходим доступ к ЛВС заказчика с привилегиями согласно реализуемой модели угроз.  Для помощи в устранении обнаруженных уязвимостей, а именно разъяснения положений экспертного заключения (отчёта), необходимо предоставить контакты работников из подразделения, обеспечивающего защиту информации в сети Заказчика. Доверенный канал взаимодействия оговаривается дополнительно, по умолчанию ЕОСДО.  В случае необходимости проведения тестирования с использованием коммерческого ПО тестирование осуществляется при наличии лицензии у заказчика.  Работа в сети Заказчика осуществляется с применением специальным образом подготовленных ноутбуков (без выхода в Интернет). Информация о ходе работ и обнаруженных уязвимостях в информационных системах Заказчика передаётся только по доверенным каналам связи, в том числе с применением шифрования. Иные меры защиты информации об уязвимостях оговариваются дополнительно. | | | | | | |  |
|  | **1.9. Норматив на поддержку** | | | | | | |  |
|  | **Подразделение** |  | **Предельное значение трудозатрат на поддержку 1 единицы объемного показателя по услуге** (чел.мес.) | | | | |  |
|  | Функциональная поддержка |  | |  |  |  |  | | --- | --- | --- | --- | |  | | | | | **Наименование драйвера** | **Единица измерения объемного показателя** | **Отчетный период для расчета норматива** | **Значение нормативов трудозатрат на поддержку 1 единицы объемного показателя (чел. мес.)** | | **Первичное тестирование** | | | | | **Серверы** | | | | | **Стадия 1 "Разведка инфраструктуры"** | | | | | Сканирование сети | Сервер | По факту | 0,0035 | | Инвентаризация версий компонентов информационных систем | Сервер | По факту | 0,0030 | | Получение базовой информации о системе, активная инвентаризация версий и подсистем | Сервер | По факту | 0,0040 | | Поиск дополнительных сведений об инфраструктуре из сторонних источников | Сервер | По факту | 0,0045 | | **Стадия 2 "Поиск уязвимостей в инфраструктуре "** | | | | | Подбор стандартных и простых паролей | Сервер | По факту | 0,0090 | | Поиск известных уязвимостей в компонентах информационных систем | Сервер | По факту | 0,0050 | | Фазинг компонентов ИС | Сервер | По факту | 0,0100 | | Поиск ошибок в настройке компонентов ИС | Сервер | По факту | 0,0100 | | **Стадия 3 "Эксплуатация найденных уязвимостей"** |  |  |  | | Написание ПО для эксплуатации найденной уязвимости | Сервер | По факту | 0,0050 | | Запуск ПО | Сервер | По факту | 0,0040 | | Закрепление в скомпрометированной системе | Сервер | По факту | 0,0046 | | **Стадия 4 "Повышение привилегий"** |  |  |  | | Просмотр файлов и работающих процессов в скомпрометированной системе | Сервер | По факту | 0,0050 | | Изъятие полезной информации в том числе ХЭШ паролей с последующей попыткой их взлома | Сервер | По факту | 0,0041 | | Горизонтальная или вертикальное повышение привилегий в системе | Сервер | По факту | 0,0048 | | **Сегменты ЛВС** | | | | | **Стадия 1 "Разведка инфраструктуры"** |  |  |  | | Поиск уязвимостей в сегменте сети заказчика на сетевом уровне (Первичное тестирование) | Сегмент сети | Месяц | 0,0020 | | **Стадия 2 "Поиск уязвимостей в инфраструктуре "** |  |  |  | | Эксплуатация сетевых уязвимостей в сегменте сети (Первичное тестирование) | Сегмент сети | Месяц | 0,0015 | | **Персонал** | | | | | **Стадия 3 "Эксплуатация найденных уязвимостей"** |  |  |  | | Реализация различного рода атак нацеленных на персонал (Первичное тестирование) | Работник | Месяц | 0,0020 | | Рассылка персональных фишинговых писем (Первичное тестирование) | Работник | Месяц | 0,0010 | | **Непрерывное тестирование** | | | | | **Серверы** | | | | | **Стадия 1 "Разведка инфраструктуры"** |  |  |  | | Сканирование сети (Непрерывное тестирование) | Сервер | По факту | 0,0005 | | Инвентаризация версий компонентов информационных систем (Непрерывное тестирование) | Сервер | По факту | 0,0005 | | Получение базовой информации о системе, активная инвентаризация версий и подсистем (Непрерывное тестирование) | Сервер | По факту | 0,0006 | | Поиск дополнительных сведений об инфраструктуре из сторонних источников (Непрерывное тестирование) | Сервер | По факту | 0,0006 | | **Стадия 2 "Поиск уязвимостей в инфраструктуре "** |  |  |  | | Подбор стандартных и простых паролей (Непрерывное тестирование) | Сервер | По факту | 0,0005 | | Поиск известных уязвимостей в компонентах информационных систем (Непрерывное тестирование) | Сервер | По факту | 0,0006 | | Фазинг компонентов ИС (Непрерывное тестирование) | Сервер | По факту | 0,0007 | | Поиск ошибок в настройке компонентов ИС (Непрерывное тестирование) | Сервер | По факту | 0,0005 | | **Стадия 3 "Эксплуатация найденных уязвимостей"** |  |  |  | | Написание ПО для эксплуатации найденной уязвимости (Непрерывное тестирование) | Сервер | По факту | 0,0005 | | Запуск ПО (Непрерывное тестирование) | Сервер | По факту | 0,0008 | | Закрепление в скомпрометированной системе (Непрерывное тестирование) | Сервер | По факту | 0,0006 | | **Стадия 4 "Повышение привилегий"** |  |  |  | | Просмотр файлов и работающих процессов в скомпрометированной системе (Непрерывное тестирование) | Сервер | По факту | 0,0005 | | Изъятие полезной информации в том числе ХЭШ паролей с последующей попыткой их взлома (Непрерывное тестирование) | Сервер | По факту | 0,0005 | | Горизонтальная или вертикальное повышение привилегий в системе (Непрерывное тестирование) | Сервер | По факту | 0,0005 | | **Сегменты ЛВС** | | | | | **Стадия 1 "Разведка инфраструктуры"** |  |  |  | | Поиск уязвимостей в сегменте сети заказчика на сетевом уровне (Непрерывное тестирование) | Сегмент сети | Месяц | 0,0006 | | **Стадия 2 "Поиск уязвимостей в инфраструктуре "** |  |  |  | | Эксплуатация сетевых уязвимостей в сегменте сети (Непрерывное тестирование) | Сегмент сети | Месяц | 0,0005 | | **Персонал** | | | | | **Стадия 3 "Эксплуатация найденных уязвимостей"** |  |  |  | | Реализация различного рода атак нацеленных на персонал (MITM, DNS spoofing и т д) (Непрерывное тестирование) | Работник | Месяц | 0,0005 | | Рассылка персональных фишинговых писем (Непрерывное тестирование) | Работник | Месяц | 0,0005 | | | | | |  |
|  | Поддержка интеграционных процессов |  | Для данной услуги не применяется | | | | |  |
|  | ИТ-инфраструктура |  | Для данной услуги не применяется | | | | |  |
|  | **1.10. Дополнительные параметры оказания услуги** | | | | | | |  |
|  | 1.10.1. Допустимый простой ИТ-ресурса в течении года, часов |  | Для данной услуги не применяется | | | | |  |
|  | 1.10.2. Срок хранения данных резервного копирования (в календарных днях) |  | Для данной услуги не применяется | | | | |  |
|  | 1.10.3. Целевая точка восстановления ИТ-ресурса (RPO) (в рабочих часах) |  | Для данной услуги не применяется | | | | |  |
|  | 1.10.4. Целевое время восстановления ИТ-ресурса (RTO) (в рабочих часах) |  | Для данной услуги не применяется | | | | |  |
|  | 1.10.5. Обеспечение катастрофоустойчивости  ИТ-ресурса |  | Для данной услуги не применяется | | | | |  |