Рекомендации по развитию

Имя: **ФИО356 [ID324354]**

Компетенция: **Информационная безопасность. Анализ защищенности данных от внешних угроз**

Год чемпионата: **2022**

Как пользоваться этим отчетом?

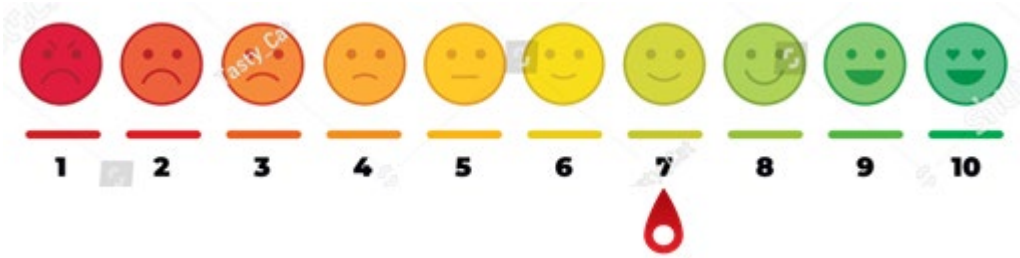
Этот отчет призван помочь вам сформировать оптимальный план развития ключевых профессиональных компетенций, необходимых для достижения успеха при решении более сложных, ответственных и масштабных рабочих задач.

В отчете используется стандартная модель компетенций UCF. Отчет опирается на результаты выполнения Вами конкурсных заданий Корпоративного Чемпионата «ATOMSKILLS-2022 год». Представленные в отчете рекомендации отталкиваются от индивидуальных особенностей личностного профиля (разным людям при одинаковых общих оценках по компетенции могут быть предложены существенно различные рекомендации по развитию).

Отчет содержит лишь рекомендации и не заменяет полноценный план индивидуального развития.

СВОДНЫЙ ПРОФИЛЬ

Модуль А «CTF»

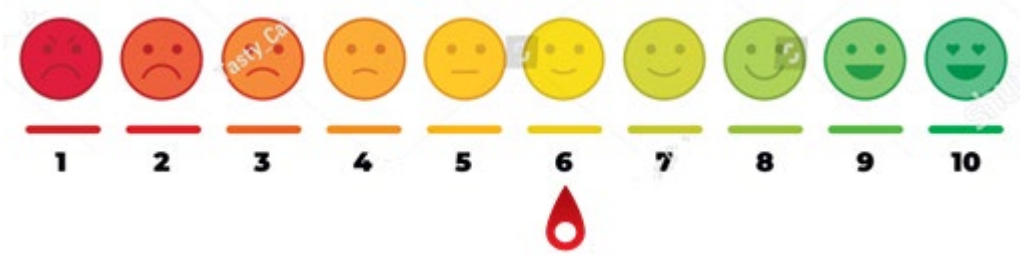


Наиболее распространенные ошибки:

1. **Пропуск очевидных подсказок**
2. **Не сохранять результаты выполнения команд в файлах**
3. **Пропуск основных команд для повышения привилегий**
4. **Выполнение ручных тестов на повышение привилегий**
5. **Пропуск процессов**

Рекомендации: На результатах сказывается недостаток опыта. Опытные участники обычно быстрее новичков. Они знают распространенные ловушки и способы выявления повторяющихся паттернов. Кроме того, они владеют множеством инструментов, в то время как новички могут испытывать трудности с базовыми командами. Однако все дело только в практике, поэтому не отказывайтесь от участия в следующих чемпионатах.

Модуль В «Защита корпоративной ИТ-инфраструктуры»



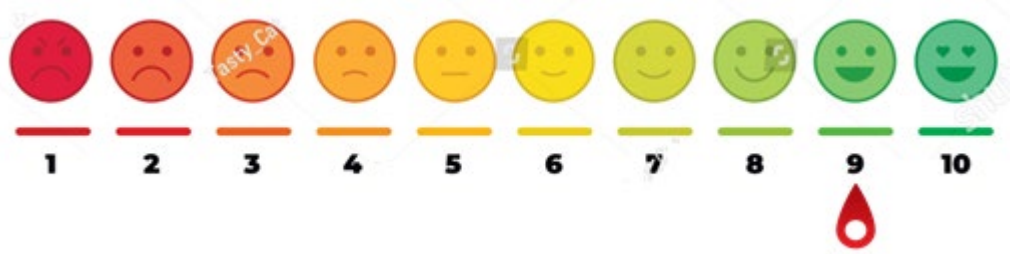
Наиболее распространенные ошибки:

1. **Неадекватная сетевая фильтрация**
2. **Публичный доступ к интерфейсам управления**
3. **Слабые пароли учетных записей**
4. **Уязвимости в веб-приложениях**

Рекомендации: Отработать общепринятые подходы к защите инфраструктуры; атаковать и искать уязвимые стороны с позиции злоумышленника; отработать взаимодействие по обнаружению и устранению ИБ-инцидентов в команде центра мониторинга и реагирования; разработать и оценить эффективность планов восстановления после чрезвычайной ситуации и механизмов их запуска.

ATOMSKILLS

Модуль С «Расследование инцидентов информационной безопасности»



Наиболее распространенные ошибки:

1. **Отсутствие навыков разработки плана реагирования**
2. **Отсутствие навыков работы с инфраструктурой сбора событий**
3. **Недостаточная информация об активах**
4. **Отсутствие навыков разработки документации**

Рекомендации: Необходимо развивать навыки фиксации состояния информационных ресурсов, которые были задействованы; уметь координировать работу по прекращению влияния информационных атак, проведение которых спровоцировало появление инцидента; использовать инструменты сбора данных для установления причин происшествия; уметь разрабатывать политик безопасности и подробного перечня рекомендаций, направленных на совершенствование всей нормативной документации.