СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ
RUSSIAN POWER SYSTEM OPERATOR

СПОСОБЫ И ПУТИ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ИБ ВЫРАБОТКА ОПТИМАЛЬНОГО ПОДХОДА К АВТОМАТИЗАЦИИ

Малахов Александр
главный эксперт Службы информационной безопасности

КАКИЕ ПРОЦЕССЫ АКТИВНО АВТОМАТИЗИРУЕМ

РБПО

- проверки, выполняемые в рамках процессов РБПО
- формирование отчетов по РБПО

КОНТРОЛИ

- контроль работы средств защиты информации
- автоматизированная проверка компрометации системы со стороны атакующего и включение блокировки IP атакующего

ОТЧЕТЫ

- формирование статистики и отчетов по ИБ

ВАРИАНТЫ

1. Использование готовых платформ
2. Использование SGRC (*Security Governance, Risk Management and Compliance*)
3. Написание скриптов
4. Использование набора инструментов

ВЫРАБОТКА ОПТИМАЛЬНОГО ПОДХОДА К АВТОМАТИЗАЦИИ

Автоматизация процессов РБПО

- Автоматический запуск инструментов
- Выгрузка результатов проверки с приведением результатов к целевому формату
- Загрузка результатов в систему управления уязвимостями
- Вывод статистики результата проверки
- Рассылка информации о результатах проверки
- Блокировка дальнейшего выполнения при превышении порога замечаний

Необходимо выполнять в среде разработки

Используются инструменты среды разработки

ВЫРАБОТКА ОПТИМАЛЬНОГО ПОДХОДА К АВТОМАТИЗАЦИИ

Контроль работы средств защиты информации

- Состояние работы
- Параметры работы прикладного ПО
- Контроль изменений (с рассылкой изменений)

Автоматизированная проверка компрометации атакующего IP и включение длительной блокировки при превышении порога компрометации

- Получение списка атакующих
- Проверка атакующих
- Формирование и применение списка длительной блокировки

Необходим доступ к системам ИБ

Развернут отдельный набор системы автоматизации для защиты привилегированного доступа

ВЫРАБОТКА ОПТИМАЛЬНОГО ПОДХОДА К АВТОМАТИЗАЦИИ

Формирование статистики и отчетов по ИБ

- Сбор информации со средств защиты

Необходим доступ к системам ИБ → Используется отдельный набор системы автоматизации для защиты привилегированного доступа

- Приведение результатов к нужному формату
- Агрегирование результатов для отчета
- Вывод статистики
- Рассылка информации по срезам
- Отображение сводных результатов по событиям

Необходимо предоставление доступа к отчетам → Используется промежуточная БД для формирования данных для отчетов и статистики. Доступ к системе BI организуется к выделенной БД

СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ
RUSSIAN POWER SYSTEM OPERATOR

СПАСИБО ЗА ВНИМАНИЕ!

www.so-ups.ru
Официальный сайт

https://t.me/so_ups_official
Официальный телеграм-канал

Малахов Александр
главный эксперт службы информационной безопасности