ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

ЭКСПРЕСС-ПОВЫШЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ

sec.ussc.ru

Уральский центр систем безопасности (УЦСБ)

с 2007
обеспечиваем ИБ

> 1000
профессионалов в штате

> 4000
реализованных проектов

Входим в список 100 крупнейших ИТ-компаний России по версии CNews Analytics и TAdviser

Компетенции

- Информационная безопасность
- Информационные технологии
- Инженерно-технические средства охраны
- Анализ защищенности
- Центры обработки данных
- Учебные центры
- Сервисный центр

Экспресс-повышение уровня защищенности

Комплекс мероприятий для оперативного выявления наиболее критичных недостатков ИБ и повышения уровня защищённости ИТ-инфраструктуры за счёт применения рекомендованных безопасных конфигураций

ЦЕЛЬ

в короткие сроки и без значительных вложений укрепить безопасность критичных узлов ИТ-инфраструктуры и снизить вероятность инцидентов

ПОЛЬЗА

повышение защищенности критических узлов ИТ-инфраструктуры за счет эффективного использования уже имеющихся механизмов обеспечения ИБ

Экспресс-повышение уровня защищенности

4 модуля услуги

01
Экспресс-аудит

02
Харденинг

03
Мониторинг и реагирование (опция)

04
Экспресс-пентест (опция)

Для большей результативности мы рекомендуем воспользоваться всеми модулями услуги. Однако вы можете сократить их количество, отказавшись от тех, которые являются опциональными

ОПИСАНИЕ БЛОКОВ РАБОТ

01 Экспресс-аудит

ЦЕЛЬ

собрать сведения о критичных узлах и средствах защиты ИТ-инфраструктуры, оценить текущее состояние её защищённости и использовать полученные результаты как основу для последующих этапов работ

Что мы сделаем:

Проведём интервью по ключевым темам:

- Конфигурации АСО
- Политики МЭ
- Сегментирование
- Службы каталога
- Почтовые сервисы
- Веб-серверы
- Платформы виртуализации
- Серверы и АРМ: Windows, Linux
- СЗИ: SIEM, DLP, АВЗ, IDS, SOAR, прокси-серверы
- Политики ИБ

01 Экспресс-аудит

Проведём очное обследование:

- Экспресс-сканирование серверов и АРМ
- Инструментальный сбор данных о службах каталога
- Анализ вашей карты корпоративной сети
- Сбор типовых конфигураций АСО и МЭ

02 Харденинг

ЦЕЛЬ

повысить уровень защищённости инфраструктуры
за счёт совершенствования настроек систем
по лучшим практикам

Что мы сделаем:

- Предоставим инструкции, рекомендации и инструменты для безопасной настройки критичных систем, выявленных в ходе экспресс-аудита
- Выставим приоритеты по выполнению и при необходимости снабдим инструкции экспертными комментариями
- Укажем возможные риски влияния изменений на инфраструктуру и предложим оптимальные сценарии реализации

02 Харденинг

Рекомендации предоставляются для критичных систем:

- Службы каталога
- Почтовые сервисы
- Веб-серверы
- Платформы виртуализации
- Серверы и АРМ Windows
- Серверы и АРМ Linux
- АСО, МЭ

03 Мониторинг и реагирование (опция)

ЦЕЛЬ

обеспечить мониторинг инцидентов ИБ
и эффективное реагирование при их обнаружении

Что мы сделаем:

Основной сценарий – подключение к УЦСБ SOC:

- Подключим критичные узлы: настроим VPN-тоннель, установим ОС и компоненты SIEM, подготовим кластер для приема событий
- Настроим SIEM и подключим источники событий
- Сформируем и адаптируем набор правил корреляции под вашу инфраструктуру

Ограничение по подключению в рамках экспресс-услуги – до 100 активов или 200 EPS

03 Мониторинг и реагирование (опция)

Альтернативный сценарий – эффективное использование вашей SIEM:

- Предоставим базовый пакет правил корреляции для вашей SIEM, позволяющих выявлять типовые признаки вредоносной активности по принципу «20% усилий для 80% результата»
- Проведем краткое обучение ваших сотрудников по использованию пакета правил для обнаружения кибератак

04 Экспресс-пентест (опция)

ЦЕЛЬ

подтвердить устранение наиболее критичных уязвимостей и недостатков ИБ по выданным рекомендациям

Что мы сделаем:

- Проверим отсутствие критичных уязвимостей и недостатков ИБ внешних ресурсов, которые могут дать доступ к внутренней сети
- Проверим отсутствие критичных уязвимостей и недостатков ИБ внутренней сети, позволяющих получить привилегированный доступ к ключевым компонентам ИТ-инфраструктуры
- Сосредоточимся на ресурсах и системах, задействованных в предыдущих блоках, чтобы убедиться, что рекомендации были реализованы корректно и их эффект достигнут

Рекомендации и сроки

- Для максимальной результативности мы рекомендуем воспользоваться всеми модулями услуги
- Вы можете сократить их количество, однако обязательными остаются модули 1 и 2
- Срок оказания услуги — от 13 рабочих дней при максимальной вовлечённости Заказчика
- Подключение к УЦСБ SOC — 10–15 рабочих дней, срок действия подключения — 6 месяцев

Если хотите избежать инцидентов	Если есть подозрение на инцидент ИБ	Если инцидент уже произошел
		
УСЛУГА	**УСЛУГА**	**УСЛУГА**
Экспресс-повышение уровня защищенности	COMPROMISE ASSESSMENT	Расследование инцидентов

Compromise Assessment

Выявление следов компрометации

ЦЕЛЬ

подтвердить или опровергнуть гипотезу об успешных кибератаках на вашу ИТ-инфраструктуру

Что мы сделаем:

- Определим наиболее актуальные для вашей ИТ-инфраструктуры гипотезы компрометации
- Проверим выбранную гипотезу с помощью анализа:
  - журналов событий безопасности
  - снимков файловых систем
  - дампов памяти
  - исследования ВПО
  - сетевого трафика
  - артефактов и метаданных

Compromise Assessment

Выявление следов компрометации

Что мы сделаем:

- При подтверждении гипотезы оперативно предоставим рекомендации по реагированию и нейтрализации инцидента ИБ, а также подготовим отчет о расследовании с описанием причин, хронологии событий и портрета злоумышленника

После завершения поиска следов компрометации рекомендуем провести экспресс-повышение уровня защищённости, чтобы укрепить защиту инфраструктуры и повысить её устойчивость к кибератакам

Расследование инцидентов ИБ

ЦЕЛЬ

локализовать инцидент ИБ, устранить его последствия, выявить причины возникновения и выработать меры для предотвращения повторного появления подобных инцидентов

Что мы сделаем:

В первые 24 часа:

Сформируем проектную группу и поставим задачи

Подготовим срочные меры для минимизации ущерба

Расследование инцидентов ИБ

Во время расследования:

01

Проведём анализ инцидента

02

Локализуем и нейтрализуем инцидент

03

Поможем восстановить работоспособность систем

04

Подготовим итоговый отчёт с выводами и рекомендациями

После завершения расследования инцидента рекомендуем провести экспресс-повышение уровня защищенности, чтобы устранить уязвимости и снизить риск повторных инцидентов

ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

СПАСИБО
ЗА ВНИМАНИЕ!

sec.ussc.ru

cybersec@ussc.ru