ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Экспресс-повышение уровня защищенности

Комплекс мероприятий для оперативного выявления наиболее критичных недостатков ИБ и повышения уровня защищенности ИТ-инфраструктуры за счет 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 информационной безопасности.

Компоненты услуги

МОДУЛЬ 1 ! #core

ЭКСПРЕСС-АУДИТ

Сбор данных о критичных узлах ИТ-инфраструктуры компании через интервью. Инструментальный анализ компонентов, оценка текущего состояния ИБ.

МОДУЛЬ 2 ! #core

ХАРДЕНИНГ

Выдача готовых к применению инструкций и инструментов для безопасной конфигурации критичных систем с учетом особенностей инфраструктуры. Подготовка плана устранения недостатков с приоритеза-цией. При необходимости — точечное обучение персонала выполнению изменений в настройках.

МОДУЛЬ 3

МОНИТОРИНГ И РЕАГИРОВАНИЕ

Подключение к УЦСБ SOC. Сбор и анализ событий с ключевых компонентов ИТ-инфраструктуры для выявления атак в течение 6 месяцев. Ограничение по подключению в рамках комплексной услуги — до 100 активов или 200 EPS. В качестве альтернативы — предоставление базового пакета правил для вашей SIEM с обучением персонала их использованию для выявления кибератак.

sec.ussc.ru
cybersec@ussc.ru

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Экспресс-повышение уровня защищенности

МОДУЛЬ 4

ЭКСПРЕСС-ПЕНТЕСТ

Проверка выполнения рекомендаций, выданных на этапе харденинга, через тестирование на проникновение с фокусом на критические векторы атак. Генерация событий для тренировки персонала под контролем специалистов УЦСБ — при подключении к сервису SOC.

Длительность

От 13 рабочих дней — время прямых работ команды УЦСБ. Подключение к УЦСБ SOC — в течение 10-15 рабочих дней на 6 месяцев.

Результат

За счет применения экспертных практик и готовых решений УЦСБ ИТ-инфраструктура получает надежную защиту от типовых киберугроз.

Атаки, не блокируемые встроенными механизмами защиты, выявляются и нейтрализуются сотрудниками УЦСБ SOC или обученным персоналом Заказчика.

Для дальнейшего повышения уровня защищенности подготовлена дорожная карта технических мер и инициатив по развитию компетенций сотрудников, ответственных за безопасность.

Для большей результативности мы рекомендуем воспользоваться всеми модулями услуги. Однако вы можете сократить их количество, при этом обязательными остаются модули со знаком ! #core