СЛЁРМ

Основные процессы построения безопасности в организации

1 Организована инфраструктурная безопасность

- Организовано сетевое сегментирование корпоративной сети
  - Выделены основные сегменты
    - DMZ
    - Inside
    - Специфичные сегменты (такие как PCI DSS, рабочие места, сервера и т.д.)
  - Между всеми сегментами сети установлены межсетевые экраны (FW)
- Организация единой точки входа на внешнем периметре сети (с настроенным FW)
- В наиболее уязвимых местах установлены IPS и IDS
- Все внешние сетевые потоки зашифрованы (например, при помощи TLS)
- Для подключения сотрудников к корпоративной сети используется VPN с многофакторной аутентификацией
- Проводится регулярное сканирование инфраструктуры (сервера, сеть, ПО) на предмет наличия актуальных уязвимостей

2 Организован процесс безопасной разработки ПО

- В CI/CD пайплайны встроены SAST и DAST
- Настроено сканирование уязвимостей информационной безопасности
  - Библиотек и конмонентов (SCA)
  - API
  - Образов и контейнеров
- К разработке привлечены специалисты ИБ (Архитектор ИБ, AppSec, Консультант по ИБ и т.д.)
- Для каждой системы спроектирована безопасная архитектура
  - Настроена межсервисная аутентификация
  - Настроено разграничение прав доступа к критичным ресурсам
  - Настроено логирование и мониторинг критичных ресурсов
  - Чувствительные данные (ПДн, карточные данные и прочее) хранятся и передаются в зашифрованном виде
  - Настроена интеграция с WAF при обмене данными с веб-приложениями
  - Продакшен среда должна быть отделена от сред разработки и тестирования
  - Должен быть ограничен доступ к системам администрирования из сети Интернет
- Внедрён RASP для обеспечения безопасности приложения в реальном времени

3 Спроектирована и внедрена полноценная система защиты информации

- Разработаны и введены в действие политики ИБ (парольная, контроль и предоставление прав доступа, обработка информации и т.д.)
- Разработана модель угроз
- SIEM настроена и подключена ко всему прикладному/системному ПО и СЗИ
- Организован процесс управления уязвимостями иБ
- Определены и классифицированы основные информационные активы (ПДн, Банковская тайна, Тайна связи т.д.)
- Разработаны планы реагирования на инциденты ИБ
- Проработан план аварийноого восстановления (DRP)
- Организованы регулярное тестирование на проникновение и аудиты ИБ
- Настроено DLP