

Принципы организации безопасности на платформах с открытым кодом

Общая модель угроз



Системный уровень

Загрузчик

1. Уязвимости загрузчика
2. Доверенная загрузка
3. Контроль загрузки ОС

Ядро

1. Уязвимости ядра
2. Встроенные системы защиты
3. Проблемы конфигураций

Системное ПО

1. Уязвимости ПО
2. Проблемы конфигураций

Прикладной уровень

Свободное ПО

Проприетарное ПО

Вредоносное ПО

1. Уязвимости Open Source
2. Репозитории

1. Уязвимости
2. Трудность исправления

1. Экспериментальное ПО
2. Вредоносное ПО

Организационный уровень

Внутренние угрозы

1. Пользователь
2. Администрирование
3. Обучение персонала
4. Организационные мероприятия

Внешние угрозы

1. Шпионаж
2. Взлом и проникновение
3. Удаленный доступ

Дополнительные требования

Опыт

- Быстрое развертывание
- Шаблоны инструкций для отдельных пользователей
- Гибкость конфигураций

Требования заказчика

- Сертификация и соответствие требованиям
- Возможность создания индивидуальных профилей безопасности
- Централизованное управление СЗИ
- Гибкость администрирования
- Эргономичный интерфейс

СПАСИБО ЗА ВНИМАНИЕ!

ООО «Конфидент»
192029 г. Санкт-Петербург
пр. Обуховской обороны 51 лит. К
Телефон/факс (812) 325-1037
E-mail: isc@confident.spb.ru