КОД безопасности

Secret Net Studio для Linux 8.2

Комплексная система защиты для ОС семейства Linux

- Оперативная поддержка новых ядер ОС
- Совместный режим работы с Соболем
- Возможность управления из новой системы на базе Linux

Сценарии использования

- Выполнение требований приказов ФСТЭК России на отечественных ОС семейства Linux.
- Расширение функций безопасности ОС семейства Linux.

Комплексный подход к защите информации

Разграничение доступа к файлам	Межсетевой экран уровня хоста	Средство обнаружения вторжений	Антивирус	Контроль устройств
Контроль печати	Защита от вирусов, атак и сетевых угроз			Контроль целостности
Затирание остаточной информации	Защита данных		Защита системы	Замкнутая программная среда
Резервное копирование	Централизованное управление	Регистрация событий ИБ и формирование отчетов	Аудит действий пользователей	Идентификация и аутентификация пользователей

Управление и мониторинг

Возможности

Защита от несанкционированного доступа

- Контроль входа пользователей в систему по логину/паролю или с использованием электронных идентификаторов.
- Механизм дискреционного разграничения доступа для контроля и управления правами доступа пользователей и групп пользователей к объектам файловой системы – файлам и каталогам.
- Контроль целостности ключевых компонентов Secret Net Studio для Linux и критических объектов файловой системы:
  - Настройка режимов реакции на нарушение целостности объектов;
  - Расписание запуска контроля целостности;
  - Поддержка полного контроля над объектами;
  - Поддержка контроля целостности в реальном времени.
- Замкнутая программная среда обеспечивает запрет запуска программ, явно неразрешенных администратором безопасности.
- Уничтожение (затирание) содержимого конфиденциальных файлов при их удалении пользователем. Очистка освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств).

Поддерживаемые операционные системы

- Альт 8 СП, Альт Рабочая станция/Сервер 10, Astra Linux Special Edition 1.7/1.8 new, Ред ОС 7.3/8 new, AlterOS 7.5, MosOS Arbat 15.04.

Персональный межсетевой экран

- Контроль сетевого трафика.
- Нейтрализация угроз, связанных с сетевым взаимодействием.
- Разграничение сетевого доступа.
- Контроль папок общего доступа.
- Контроль именованных каналов.
- Контроль использования сети приложениями.
- Фильтрация входящих соединений с использованием данных отправителя пакетов.
- Принудительное завершение TCP-соединений.
- Блокировка ошибочных пакетов.

Контроль подключаемых устройств

- Разграничение доступа пользователей и групп пользователей к шинам USB, SATA и подключаемым к ним устройствам.
- Правила подключения задаются:
  - На шину;
  - На классы устройств, связанные с шиной;
  - На конкретные модели и экземпляры устройств.

Управление настройками защиты ОС

- Управление политиками ОС Astra Linux, полученными с Security Code Orchestrator.
- Контроль неизменности примененных настроек.
- Периодический запрос настроек с Security Code Orchestrator.
- Запрос политик по команде администратора.
- Сбор событий и отправка на syslog-сервер Security Code Orchestrator.

Управление и мониторинг

- Централизованное управление через Security Code Orchestrator/сервер безопасности SNS для Windows:
  - Управление политиками безопасности;
  - Сбор и хранение журналов управляемых объектов;
  - Хранение и отправка состояний защитных компонентов и системы в целом на Security Code Orchestrator; new
  - Возможность совместной работы сервера безопасности и Security Code Orchestrator: результирующие политики суммируются с приоритетом у Security Code Orchestrator.
- Фиксация событий безопасности в журнале. Журнал включает события, связанные с доступом пользователей к защищаемым файлам, устройствам и узлам вычислительной сети. Фильтрация событий безопасности, контекстный поиск в журнале событий безопасности.
- Аудит действий субъектов с защищаемыми объектами (файлами, каталогами, сетевыми соединениями). Возможность автоматического построения отчетов по результатам аудита.

Антивирус

- Настройка профилей сканирования.
- Настройка расписания сканирования.
- Формирование списка исключений для процедуры сканирования.
- Запуск сканирования вручную.
- Просмотр и управление содержимым карантина.

Обнаружение вторжений

- Анализ сетевого трафика:
  - Сигнатурный анализ;
  - Эвристический анализ;
  - Анализ трафика по базе вредоносных IP- и URL-адресов. new
- Анализ состояния объекта защиты:
  - Контроль безопасной конфигурации;
  - Проверка на руткиты;
  - Проверка запущенных процессов;
  - Проверка скрытых портов;
  - Проверка наличия интерфейсов в неразборчивом режиме.
- Анализ журналов.

Сертификаты

ФСТЭК России

- 5-й класс защищенности СВТ
- 4-й класс защиты МЭ типа «В»
- 4-й класс защиты СКН
- 4-й уровень доверия
- Применяется для защиты значимых объектов КИИ до 1 категории, ИСПДн до УЗ1, ГИС до К1 и АСУ ТП до К1 включительно