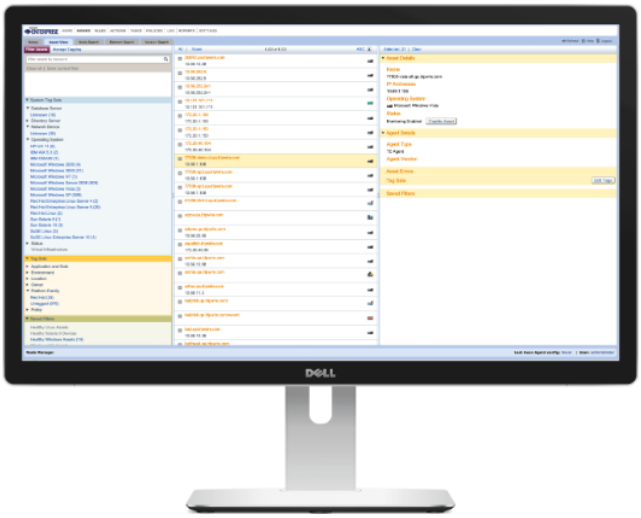
АО «Аксофт»
Адрес: 115088, Москва, 2-ой Южнопортовый проезд, д. 31, стр. 1
Телефон: +7 (495) 232-52-15
Факс: +7 (495) 232-52-15
E-mail: tripwire@axoft.ru

Предложение пилотного проекта

Флагманский продукт Tripwire является отраслевым стандартом для мониторинга целостности и контролем за конфигурациями. Обнаруживает угрозы, изменения в инфраструктуре и обеспечивает контроль за соответствием требованиям безопасности предприятия. Компании могут использовать Tripwire® Enterprise одновременно как в качестве решения для контроля конфигураций, так и в качестве самостоятельного инструмента, позволяющего производить проверку целостности файлов, управлять политиками безопасности и проверять инфраструктуру на соответствие требованиям.

Tripwire Enterprise – позволяет сотрудникам отделов ИБ и ИТ оперативно достигать необходимого уровня безопасности во всей ИТ-инфраструктуре за счет контроля целостности и наглядности всех производимых изменений внутри инфраструктуры.



Ключевые компоненты продукта:

- Tripwire File Integrity Manager (FIM) – Является решением для мониторинга целостности файлов. Оно проверяет большие, неоднородные, системы для мгновенного понимания конфигурации и обнаружения угроз.
- Tripwire Policy Manager устанавливает и поддерживает постоянную непрерывную настройку конфигурации на основе агентов на основе агентов и без агента, с более чем 650 комбинациями платформ и политикой безопасности и соответствия, стандартами, правилами и рекомендациями поставщиков.
- Tripwire Remediation Manager компонент, который позволяет отделу IT-безопасности автоматизировать восстановление конфигураций до необходимого состояния в случае обнаружения отклонений или изменений.
- Tripwire Event Sender компонент, позволяющий интегрировать Tripwire со сторонней SIEM системой. Позволяет дополнить события, направляемые в SIEM системы информацией об изменениях внутри инфраструктуры.
- Tripwire Dynamic Software Reconciliation компонент создает список установленных обновлений, запрашивает репозитории Microsoft TechNet и yum для Linux и извлекает манифесты на уровне файлов для каждого обновления. Благодаря этому вы можете контролировать валидность изменений при обновлении на отслеживаемых системах.;
- Tripwire Axon™ Platform обеспечивает гибкий сбор данных и гибкую связь большого количества устройств, облачных и виртуализированных систем. Платформа Tripwire Axon решает проблемы сбора данных с помощью расширяемого и ресурсоэффективного агента и асинхронных методов обмена сообщениями. Агент Tripwire Axon Agent и его плагины предназначены для эффективной работы, оптимизации использования ресурсов системы и улучшения пропускной способности сети.

Условия и план тестирования продукта Tripwire Enterprise

Убедиться в эффективности продукта Вы можете самостоятельно, заказав проведение бесплатного пилотного проекта силами специалистов Axoft. Все работы в рамках пилота проводятся на удаленной основе. Для проведения пилота со стороны Заказчика требуется выполнить следующие условия:

1. Создать рабочую группу для решения оперативных организационных и технических вопросов.
2. Предоставить необходимые ресурсы и удаленный доступ для проведения настройки системы.

Специалисты компании Axoft гарантируют, что произведенные работы не окажут влияния на производительность и работу систем.

Тестирование продукта может включать следующие сценарии, в связке, либо по отдельности:

1. Отслеживание изменений системных файлов/директорий/веток реестра, агентским способом получения информации (Axon и TE agent) в системах Windows и Linux. Отслеживание изменений возможно производить, как в режиме реального времени, так и задачами, работающими по расписанию.
2. Отслеживание изменений в конфигурации оборудования безагентским способом (подключение по протоколам удаленного доступа).
3. Отслеживание изменений в БД.

Рекомендуемые характеристики оборудования:
Сервер (VM): CPU 2x2ГГц | 4-8 Гб RAM | 80 Гб HDD | сетевой интерфейс | RHEL / CentOS

Ключевые этапы пилота

Пилотный проект занимает от 14 до 30 дней и состоит из следующих этапов:

Этап 1. Подготовка системы

1. Установка и настройка сервера Tripwire Enterprise.
2. Первоначальная конфигурация системы для работы с агентами.
3. Генерация агентов, инсталляция на интересующие узлы.
4. Создание задач на мониторинг сетевого оборудования безагентским способом.
5. Подключение БД и подготовка SQL запросов к ней для отслеживания изменений в выдаче, в случае необходимости данного сценария.
6. Создание задач на мониторинг, расписания, действий, бейзлайн отслеживаемых систем.
7. Настройка оповещений.

Этап 2. Тестирование системы

1. Изменение системного файла отслеживаемой системы, отслеживание изменения внутри системы.
2. Изменение файла в директории, заданной пользователем, отслеживание изменения внутри системы.
3. Изменение конфигурации сетевого оборудования, отслеживание изменения внутри системы.
4. Добавление/изменение отслеживаемой записи/сущности в БД, отслеживание данного изменения внутри системы.

Этап 3. Подведение итогов тестирования

Результаты тестирования

По завершению пилотного проекта Вы получите:

1. Представление о работе продукта, как со стороны пользователя системы, так и со стороны администратора.
2. Понимание, насколько продукт решает задачи заказчика.
3. Представление о различных вариантах встраивания решения в инфраструктуру заказчика, согласно его потребностям.

Если желаете заказать проведение пилота или получить дополнительную информацию по продукту отправьте заявку на **tripwire@axoft.ru**
