Техническое описание

Платформа OTM – Контроль & Сбор

Платформа Seceon OTM и приложение сбора данных CCE обеспечивает распределенный сбор данных для Платформы Seceon OTM. CCE эффективно собирает информацию о внешних нападениях, а также о внутренних угрозах.

CCE предоставляет данные для поведенческого анализа и понимания ситуации на ИТ инфраструктуре Вашей сети. Предлагает уникальное представление Вашей основной сети, собирая данные по следующим параметрам:

• поведение пользователей, систем, приложений, и процессов.

• Сервер, VM, приложение и открытие базы данных

• Контроль доступа и использования основной сервисной инфраструктуры

• Контроль коммутатора, маршрутизатора и других элементов инфраструктуры безопасности

• Преобразование любого сетевого устройства в датчик данных Seceon

• Прозрачный масштабируемый доступ ко всем данным
- без запроса данных, не требуя переключения сигналов,

Эти возможности достигаются через сбор данных о событиях, пользовательских данных Active Directory, данных о потоках и сведений о пакетах. CCE применяет передовые полиморфные технологии выделения признаков, чтобы собрать и, затем, переработать эту информацию.

Вся переработанная информация поставляется в головное приложение аналитики, которое производит дальнейшую обработку данных, проводя поведенческий анализ, и сообщает о потенциальных угрозах. CCE работает с обратной связью от APE, чтобы, при необходимости, извлечь дополнительную информацию, а также, обратить внимание на необычные угрозы и их объем распространения. Это происходит с минимизацией сетевого трафика и без увеличения загрузки центрального процессора рабочего сервера, поэтому достигается высочайшая эффективность контроля кибербезопасности на базе уникального решения Seceon.

CCE обеспечивает мощную распределенную структуру для защиты всех ваших основных внутренних и внешних сетевых ресурсов. Взаимодействуя с APE Seceon, CCE предоставляет исчерпывающую информацию для того, чтобы немедленно обнаружить и блокировать любой несанкционированный доступ к данным.

CCE – разработано на Linux, может быть развернуто в качестве виртуальной машины на любом сервере, который соответствует минимальным требованиям. Также, компонент может быть развернут на автономный сервере, если это необходимо.

Техническое описание

Требования и спецификации

Виртуальное устройство

- Dual multi-core 2.3Ghz E5 Xeon Processor
- не менее, чем 2 ядра
- 8 GB доступной DDR3 RAM
- 500 GB пространства на диске
- Поддерживаемая VM инфраструктура:
- VMware ESXi 5.5, или выше

Виртуальное облако

- AWS
- Azure

Физическое устройство

- Dual Core 2.3Ghz E5 Xeon процессор
- 8 GB of DDR4 RAM
- 500 GB direct access HDDs
- Форм-фактор для крепления в стойку
- Резервированное электропитание
- Два 10GigE порта или четыре 1 GigE