Техническое описание

Платформа OTM – Analytics Policy Engine

Центральная платформа аналитики APE обеспечивает визуализацию, прогнозирование, обнаружение угроз и устранение угроз для Платформы открытого управления угрозами Seceon. APE использует машинное обучение вместе с ультрасовременной параллельной архитектурой обработки Big Fast, реализуя отлично масштабируемое, доступное решение, прекрасно работающее на сети любого размера в режиме реального времени. Оно чрезвычайно эффективно при обнаружении как внешних, так и внутренних атак и угроз.

APE предоставляет Вам картину поведения ИТ инфраструктуры Вашей сети. В частности, оно предлагает уникальное понимание происходящего на Вашей сети, обеспечивая:

• Способность обнаружить необычное поведение внутренних или внешних пользователей, устройств, приложений и процессов
• Продвинутый набор правил обнаружения угроз моделированного поведения
  – допускает пошаговый подход для устранения проблем
• Анализ мероприятий, необходимых для устранения угрозы – как принятые меры отразятся на работоспособности клиентов, сетевых устройств или сети в целом
• Автоматизированная блокировка - устраняет угрозы в режиме реального времени
• Автоматическое определение ресурсов сети: Серверы, виртуальные машины, приложения и базы данных
• Сбор данных о приложениях, процессах и учётных данных пользователей
• Наблюдение за доступом и использованием основной сервисной инфраструктуры
• Наблюдение за коммутаторами, маршрутизаторами и другими элементами инфраструктуры безопасности
• Контроль соблюдения сетевых политик – обнаружение и блокирование нарушений политики
• Автоматизированная классификация и визуализация важных сетевых ресурсов
• Анализ тенденций в пределах от группы ресурсов до отдельного устройства/пользователя
• Интеллектуальное отслеживание инцидентов и их корреляций
• Упрощенное развертывание за несколько часов без обучения персонала
  – Не требует начальной настройки, при этом допускает конфигурацию по требованиям пользователя
• Устанавливается как на одну виртуальную машину, так и на кластер
• Разработано на платформе OTM, объединяющей центральную аналитику APE распределённую структуру сбора данных CCE.

APE предоставляет мощное решение для защиты всей Вашей IT-инфраструктуры. Получая собранные данные от CCE, APE формирует полную картину происходящего на сети для того, чтобы Вы смогли принять надлежащие меры по устранению несанкционированного доступа.

APE приложение разработано для Linux, и может быть развернуто как в центральном офисе, так и на публичных облачных сервисах, а также, на гибридной вычислительной среде.

Техническое описание

Требования и спецификации

Виртуальное устройство

- Dual multi-core 2.3Ghz E5 Xeon процессор или выше
- С по крайней мере доступными 16 ядрами
- 128 GB доступной DDR4 RAM или выше
- 16 TB доступного прямого доступа к месту на диске
- Поддерживаемая VM инфраструктура:
- VMware ESXi 5.5, или выше

Виртуальное облако

- AWS
- Azure

Физическое устройство

- Dual 8 Core 2.3Ghz E5 Xeon процессор
- 128 GB от DDR4 RAM
- 16 TBs прямой доступ SSDs
- Форм-фактор для подключения в шасси
- Двойное избыточное электроснабжение
- Два 10GigE порта или Четыре 1 GigE