SSL Visibility 5.0 Administration

Описание курса

Курс «SSL Visibility 5.0 Администрирование» предназначен для сетевых администраторов и специалистов по ИБ, которые хотят узнать, как настраивать у управлять устройствами SSL Visibility для защиты сетевого окружения.

Метод преподавания

Очные занятия и Виртуальная академия

Продолжительность

3 дня

Задачи курса

По окончанию курса вы сможете:
- формулировать потребности в управлении зашифрованным трафиком (ETM)
- выбирать лучшие решения для внедрения в вашей сети
- настраивать вируальные устройства и конфигурировать политики в соответствии с вашими потребностями
- интегрировать SSLV в существующий PKI
- оптимально настраивать SSLV

На кого рассчитан курс

Курс «SSL Visibility 5.0 Администрирование» предназначен для слушателей, перед которыми стоят задачи внедрять и управлять виртуальными устройствами SSLV в рабочей среде.

Предварительные требования к слушателям

Слушатели должны иметь рабочие знания в:
- SSL/TSL
- TCP/IP
- Network security devices
- ProxySG

Интерактивность

Содержание и практическая часть курса дадут Вам глубокое понимание SSLV решений. По завершении тренинга слушатель будет конфигурировать SSLV в нескольких наиболее распространённых применениях, чтобы инспектировать зашифрованный трафик, отправляя его и на активные, и на пассивные устройства безопасности.

Содержание курса.

Модуль 1: Знакомство с управлением зашифрованным трафиком

• Описание актуальных задач, которые вызвали увеличение потребности в SSL/TLS. Данный урок также охватывает фундаментальные основы SSL и TLS зашифрованных коммуникаций.

Модуль 2: Знакомство с виртуальным устройством SSLV

• Описание нового виртуального устройства (SV-VA). Различия между виртуальными и аппаратными устройствами.

Модуль 3: Знакомство с управлением зашифрованным трафиком с помощью Symantec SSLV

• Описание архитектуры и возможностей аппаратных устройств SSLV и того как происходит шифрование.

Модуль 4: Применение SSLV

• Описание архитектуры и инструментов внедрения аппаратного устройства SSLV и базовые настройки дешифрования SSL/TLS в трёх распространённых схемах внедрения.

Модуль 5: Мигрирование и обновление SSLV

• Описание процессов миграции, обновления и требований предъявляемым к аппаратным устройствам SSLV.

Модуль 6: Предоставление зашифрованного входящего трафика для устройств безопасности с сохранением уровня безопасности

• Описание конфигурации SSLV для инспектирования входящего трафика на управляемых Вами серверах. Использование пассивных и активных устройств и установление соответствующего крипто уровней.

Модуль 7: Предоставление зашифрованного исходящего трафика для устройств безопасности и предотвращение потери данных

• Описание конфигурации SSLV для инспектирования исходящего трафика и использование DLP для мониторинга потери данных.

Модуль 8: Предоставление зашифрованных угроз для Forensic Analysis While Maintaining Compliance Regulations

• Описание конфигурации SSLV для предоставления дешифрованного трафика на пассивные устройства, таких как Security Analytics и соблюдение международных требований анонимности.

Модуль 9: Offload SSL Decryption для увеличения эффективности ProxySG

• Последовательность действий при применении SSL Decryption offload с одним или несколькими устройствами ProxySG/ASG с целью увеличения пропускной способности зашифрованного трафика в вашей сети. Различные ProxySG/ASG устройства и схемы применения.

Модуль 10: Облегчение управления несколькими виртуальными устройствами SSLV с помощью Management Center

• Описание возможностей Management Center в работе с SSLV для прозрачности, облегчения управления и централизации политик.