UserGate

ЧЕК-ЛИСТ ПО БЕЗОПАСНОСТИ

СИСТЕМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ **(СОВ / IDPS)**

UserGate NGFW содержит в себе модуль системы обнаружения и предотвращения вторжений (IDPS), который позволяет обнаруживать попытки эксплуатации уязвимостей в ИТ-инфраструктуре. Движок обработки сетевого трафика UserGate без потери производительности обрабатывает большое количество сетевых соединений и исследует их сигнатурным методом. Здесь показаны основные действия, которые необходимо выполнить для корректной и надежной работы данного модуля.

Шаг 1. **Сегментация сети**

Сначала необходимо провести сегментацию сети, разделить ресурсы на логические единицы (сегменты) по определенным признакам, например, по решаемым бизнес-задачам в рамках сегмента. Классическое деление: зоны Trusted, Untrusted, DMZ, Management. Сегментов можно создавать сколько угодно. В UserGate для этого есть понятие «Зоны безопасности».

Шаг 2. **Инвентаризация ресурсов**

Для грамотного обеспечения безопасности в первую очередь необходимо узнать, что именно подлежит защите. Соберите информацию об используемых внутри сегментов сети операционных системах и их версиях, прикладном ПО, серверном ПО, оборудовании и так далее.

Шаг 3. **Управление уязвимостями**

На основе созданного реестра активов необходимо ознакомиться с существующими уязвимостями сети. Для этого есть база данных CVE, а также различные инструменты, автоматизирующие этот процесс.

Шаг 4. **Формирование профиля сигнатур**

На основе списка уязвимостей, которые актуальны именно для сегментов вашей сети, в UserGate создается «Профиль», куда вы добавляете из списка те сигнатуры, которые сопоставлены с вашими уязвимостями.

Шаг 5. **Анализ срабатываний**

В процессе эксплуатации наблюдаем за журналом событий СОВ и соотносим их с реальной ситуацией. В случае необходимости корректируем профиль сигнатур: добавляем и удаляем сигнатуры.

Работа с системой обнаружения вторжений – это непрерывный процесс, требующий от службы ИБ постоянного мониторинга, анализа происходящего и дополнительной настройки правил и профилей безопасности.