s•terra

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК

Система обнаружения вторжений (СОВ) – необходимый компонент защиты

Злоумышленнику, чтобы получить доступ к информации Вашей компании, необходимо пройти несколько эшелонов защиты. При этом он может использовать уязвимости и некорректные настройки конечных рабочих станций, телекоммуникационного оборудования или социальную инженерию. Атаки на информационную систему (ИС) происходят постепенно: проникновение в обход политик информационной безопасности (ИБ), распространение в ИС с уничтожением следов своего присутствия и только потом непосредственно атака. Весь процесс может занять несколько месяцев, или даже лет. Зачастую ни пользователь, ни администратор ИБ не подозревают об аномальных изменениях в системе и проводимой на нее атаке. Все это приводит к угрозам нарушения целостности, конфиденциальности и доступности информации, обрабатываемой в ИС.

Для противодействия современным атакам недостаточно традиционных средств защиты, таких как межсетевые экраны, антивирусы и т.п. Требуется система мониторинга и обнаружения потенциально возможных атак и аномалий, реализующая следующие функции:

- обнаружение попыток вторжений в информационные системы;
- детектирование атак в защищаемой сети или ее сегментах;
- отслеживание неавторизованного доступа к документам и компонентам информационных систем;
- обнаружение вирусов, вредоносных программ, троянов, ботнетов;
- отслеживание таргетированных атак.

Важно учесть, что если в ИС компании обрабатывается информация, подлежащая обязательной защите в соответствии с требованиями российского законодательства (например, персональные данные), то необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки соответствия регуляторами ФСТЭК России и/или ФСБ России.

С-Терра СОВ

На протяжении многих лет компания «С-Терра СиЭсПи» производит VPN-продукты для организации криптографической защиты передаваемых данных и межсетевого экранирования. В связи с возросшими потребностями пользователей в повышении общего уровня безопасности ИС, компания «С-Терра СиЭсПи» разработала специальное средство защиты информации, обеспечивающее обнаружение атак и аномальных активностей.

С-Терра СОВ представляет собой средство защиты, позволяющее администраторам информационной безопасности выявлять атаки, основываясь на анализе сетевого трафика. В основе работы данного средства защиты лежит использование механизмов сигнатурного анализа.

При анализе сетевого трафика с помощью сигнатурного метода администратор всегда сможет точно установить, какой конкретно пакет или группа пакетов вызвали срабатывание сенсора, отвечающего за детектирование аномальной активности. Все правила чётко определены, для многих из них можно проследить всю цепочку: от информации о деталях уязвимости и методах её эксплуатации, до результирующей сигнатуры. В свою очередь, база правил сигнатур обширна и регулярно обновляется, тем самым гарантируя надежную защиту ИС компании.

Для минимизации рисков от принципиально новых атак нулевого дня, для которых отсутствуют сигнатуры, в состав продукта С-Терра СОВ включен дополнительный метод анализа сетевой активности – эвристический. Этот метод анализа активности строится на основе эвристических правил, т.е. на основе прогноза активности ИС и ее сопоставления с нормальным «шаблонным» поведением, которые формируются во время режима обучения данной системы на основе ее уникальных особенностей. За счет применения данного механизма защиты, С-Терра СОВ позволяет обнаружить новые, ранее неизвестные атаки или любую другую активность, не попавшую ни под какую конкретную сигнатуру.

Сочетание сигнатурного и эвристического анализов позволяет обнаружить несанкционированные, нелегитимные, подозрительные действия со стороны внешних и внутренних нарушителей. Администратор ИБ может прогнозировать возможные атаки, а также выявлять уязвимости для предотвращения их развития и влияния на ИС компании. Оперативное детектирование возникающих угроз позволяет определить расположение источника атаки по отношению к локальной защищаемой сети, что облегчает расследование инцидентов ИБ.

Таблица 1. Функциональность С-Терра СОВ

Возможности продукта	Подробное описание
Варианты исполнения	• Программно-аппаратный комплекс • В виде виртуальной машины
Операционная система	Debian 7
Определение атак	• Сигнатурный анализ • Эвристический анализ
Управление	• Графический интерфейс • Командная строка
Регистрация атак	• Запись в системный журнал • Отображение в графическом интерфейсе
Обновление базы данных сигнатур	• Off-line режим • On-line режим
Механизмы оповещения	• Вывод на консоль администратора • Электронная почта • Интеграция с SIEM-системами
Работа с инцидентами	• Выборочный контроль отдельных объектов сети • Поиск, сортировка, упорядочивание данных в системном журнале • Включение/отключение отдельных правил и групп правил
Дополнительные механизмы защиты	• Защита канала управления с использованием технологии VPN IPsec по ГОСТ 28147-89, ГОСТ Р 34.10-2001/2012 и ГОСТ Р 34.11-2001/2012 • Контроль целостности программной части и конфигурации СОВ
Сертификаты соответствия	ФСТЭК России: СОВ 4 класс ФСБ России: СОА В

Система обнаружения атак С-Терра СОВ имеет удобный интерфейс, управление и контроль осуществляется по защищенному каналу с применением технологии IPsec на отечественных криптоалгоритмах ГОСТ.

Использование С-Терра СОВ в качестве компонента защиты повышает общий уровень защищенности ИС благодаря постоянному анализу изменений ее состояния, выявлению аномалий и их классификации. Наглядный и функциональный веб-интерфейс управления и контроля над системой обнаружения вторжений, а также наличие дополнительных утилит управления, позволяет корректно настроить сенсоры событий, эффективно обрабатывать и представлять результаты анализа трафика.

Схема включения С-Терра СОВ

С-Терра СОВ размещается в сегменте локальной сети (например, DMZ-зоне), весь трафик, циркулирующий в этом сегменте, дублируется и перенаправляется на средство защиты через «зеркалирующий» span-порт коммутатора. Управление осуществляется через отдельный интерфейс по защищенному каналу. Более подробная схема включения в ИС компании представлена на рисунке 1.

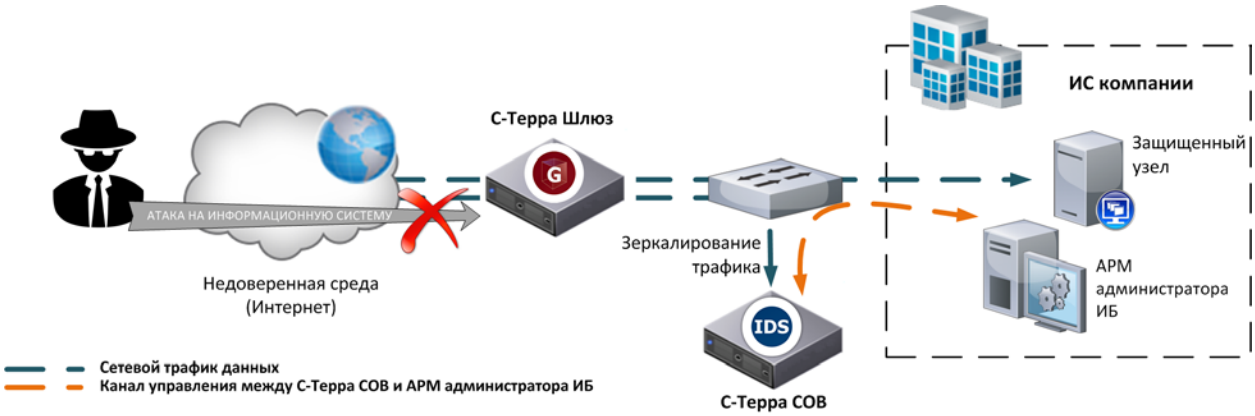

Рисунок 1. Схема включения отдельных С-Терра СОВ и С-Терра Шлюз

На одном устройстве могут одновременно работать С-Терра Шлюз для шифрования трафика и межсетевого экранирования, а также С-Терра СОВ – для обнаружения сетевых атак. Подробная схема такого включения представлена на рисунке 2.

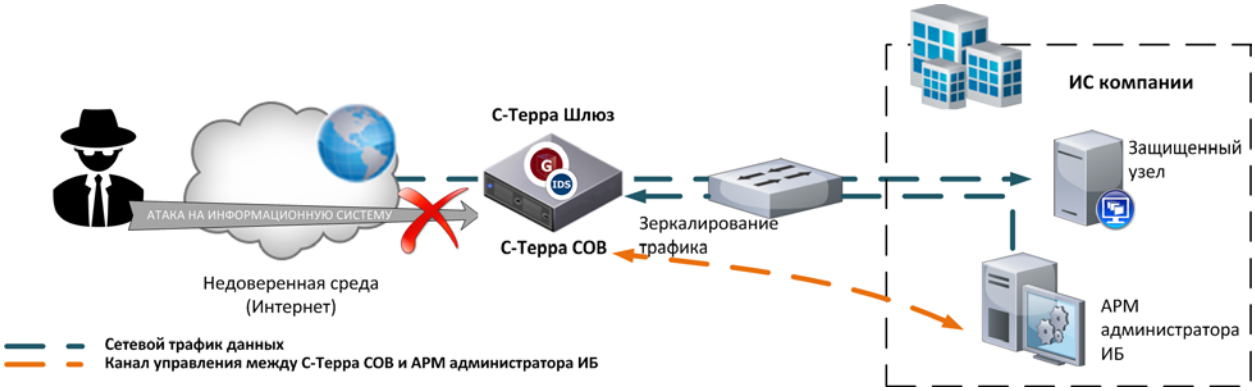

Рисунок 2. Схема включения совместной работы С-Терра СОВ и С-Терра Шлюз

Выбор продуктов

С-Терра СОВ поставляется в виде программно-аппаратного комплекса или в виде виртуальной машины для популярных гипервизоров (VMware ESX, Citrix XenServer, Parallels, KVM).

Выбор конкретного исполнения зависит от объемов передаваемой по сети информации, количества используемых сигнатур и других факторов.

Если предпочтительной является аппаратная платформа, то есть возможность выбрать из трех вариантов производительности анализа информации – для скоростей 10, 100 и 1000 Мбит/с.

Производительность Виртуальной СОВ может изменяться в широких пределах и зависит от используемых настроек гипервизора и ресурсов аппаратной платформы, на которой виртуальная СОВ работает.

Получить помощь в подборе оборудования, а так же расчет стоимости для вашей организации вы можете получить, обратившись к нашим менеджерам:

- по телефону +7 (499) 940-90-61
- или по электронной почте: sales@s-terra.com

О компании «С-Терра СиЭсПи»

ООО «С-Терра СиЭсПи» основано в 2003 году и является ведущим российским разработчиком и производителем средств сетевой информационной безопасности на основе технологии IPsec VPN.

Компания «С-Терра СиЭсПи» предлагает органично входящие в сетевую инфраструктуру решения, которые используют набор протоколов IPsec и российские сертифицированные криптографические алгоритмы ГОСТ. Решения характеризуются отличной масштабируемостью, надежностью и рекордной производительностью, что обеспечивает высокую экономическую эффективность.

Продукты и решения С-Терра обеспечивают защиту каналов связи любой производительности (как на сетевом, так и на канальном уровне), безопасный удаленный доступ, в том числе с мобильных платформ, а также предоставляет эффективное управление VPN-инфраструктурой С-Терра.

Продукты С-Терра сертифицированы ФСТЭК России и ФСБ России, в том числе как средства криптографической защиты информации (СКЗИ) по классу КС1, КС2, КС3, а также как межсетевой экран.

Компания является первым российским технологическим партнером Cisco (Cisco Solution Technology Integrator), Серебряным партнером Samsung и Авторизованным партнером Huawei.

Партнерская сеть компании "С-Терра СиЭсПи" состоит из более чем 400 компаний, включая всех крупнейших российских системных интеграторов. Имеется представительство компании в Республике Беларусь.