ViPNet IDS

ViPNet IDS – это программно-аппаратный комплекс, выполненный в виде отдельно стоящего сетевого устройства, предназначенный для обнаружения вторжений в информационные системы на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным.

Ключевые возможности:

- обнаружение компьютерных атак (вторжений) на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным;
- регистрация компьютерных атак (вторжений) в момент времени, близкий к реальному;
- отображение обобщенной статистической информации об атаках;
- журналирование обнаруженных событий и атак для последующего анализа (см. рис.1);
- выборочный поиск событий (атак) в соответствии с заданными фильтрами (по временному диапазону, IP-адресу, порту, степени критичности и др.);
- экспорт журнала атак (вторжений) в файл формата CSV для последующего анализа в сторонних приложениях;
- обновление баз решающих правил в автоматизированном режиме с Сервера обновлений при предоставлении новой версии указанной базы производителем;
- механизм, обеспечивающий маскирование ПАК ViPNet IDS в составе контролируемой сети;
- выборочное использование отдельных правил обнаружения или групп правил на усмотрение администратора ViPNet IDS;
- добавление собственных правил для анализа сетевого трафика;
- выборочный контроль ресурсов сети на уровне отдельных объектов;
- регистрация, отображение и экспорт в файл формата PCAP IP-пакетов, соответствующих зарегистрированным событиям (атакам) для последующего анализа в стороннем ПО;
- автоматическая передача обобщенной информации о сетевых атаках (вторжениях) системе централизованного мониторинга ViPNet StateWatcher по протоколу SNMP;
- контроль целостности исполняемых и конфигурационных файлов;
- контроль целостности загружаемых баз правил обнаружения атак.

Сертификаты:

Сертификат ФСБ № СФ/СЗИ-0122 (соответствует требованиям ФСБ России к системам обнаружения компьютерных атак класса В) от 12.12.2016. Действителен до 31.12.2019.
Сертификат ФСТЭК № 3804 (требования к СОВ (сети четвертого класса защиты ИТ.СОВ.С4.П3)) от 10.10.2017. Действителен до 10.10.2020.

Наши контактные данные:

ул. Ленина, д.20, (четвертый этаж), каб. 422, 423. Остановка "Яблонька".
e-mail: info@ooo-skb.ru (ссылка для отправки email);
тел. 8 (3812) 53-20-18