ViPNet EndPoint Protection и ViPNet SafePoint – тандем защиты от внутренних и внешних нарушителей

Иван Кадыков

Руководитель продуктового направления

инфотекс ТЕХНОДЕСТ

Синий поток

Потенциальный внутренний нарушитель

«Классические» внутренние нарушители (инсайдеры)

сотрудники, которые злоупотребляют своим законным доступом к конфиденциальным данным в корыстных целях

Подкупленный сотрудник

нанятый внешними компаниями для кражи, изменения или удаления конфиденциальных данных

Недовольные бывшие сотрудники

которые хотят навредить своим работодателям

Безрассудные сотрудники

тип инсайдеров, которые пренебрегают ИБ-политиками

Потенциальный внешний нарушитель

Конкуренты / промышленный шпионаж

«лица», желающие получить дополнительную информацию или навредить конкурирующему бизнесу

Недобросовестные поставщики / партнёры

нанятый внешними компаниями для кражи, изменения или удаления конфиденциальных данных

Хакер «бизнесмен»

которые хотят навредить своим работодателям

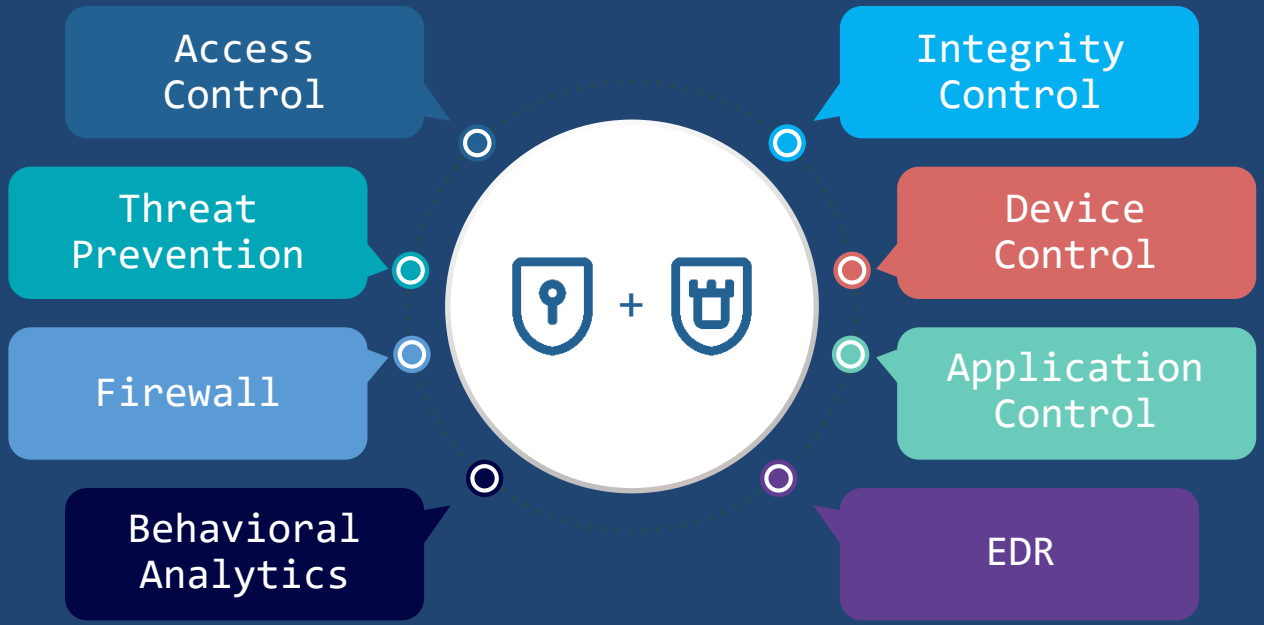
Службы (официальные и теневые) недружественных государств

тип инсайдеров, которые пренебрегают ИБ-политиками

Распространённые сценарии/векторы атак

- Атака на учётные записи (повышение привилегий)
- Хищение информации
- Фишинг
- Использование уязвимостей (как следствие эксплоитов)
- Удалённый запуск командного интерпретатора (из документов)
- Запуск сторонних приложений, скриптов
- и т.д.

Комбинирование механизмов – лучшее решение!



ViPNet SafePoint

ViPNet SafePoint –

сертифицированный программный комплекс защиты информации от несанкционированного доступа уровня ядра операционной системы (ОС)

ViPNet SafePoint –

устанавливается на рабочие станции и серверы в целях обеспечения мандатного и дискреционного разграничения доступа пользователей к критически важной информации и подключаемым устройствам

Ключевой набор функциональности для СЗИ от НСД

- Идентификация и аутентификация пользователей
- Дискреционная модель доступа (контроль доступа к файлам, реестру, процессам, службам)
- Замкнутая программная среда
- Контроль целостности
- Контроль времени работы
- Контроль подключения съемных носителей
- Мандатный контроль доступа

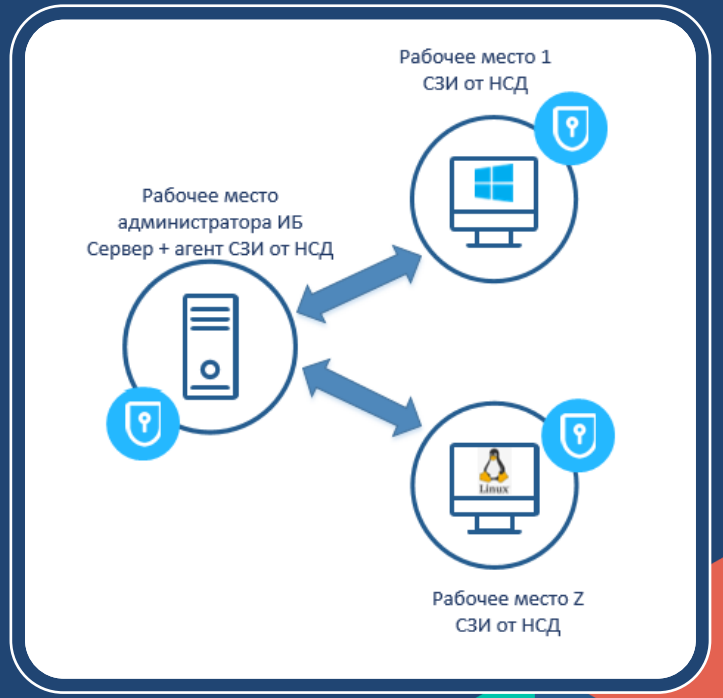
Управление привилегированными пользователями

В СЗИ от НСД – реализована защита и контроль непосредственно на хостах субъекта доступа

Формируется из трёх сущностей

- исходный идентификатор пользователя SID
- эффективный идентификатор пользователя (контекст безопасности (маркер-token) процесса при доступе)
- «полнопутевое» имя процесса (имя исполняемого файла процесса)

**PIM/PAM/PUM – контролируют подключение привилегированными пользователями к целевым системам и их работу только в соответствующих сессиях*



Защита от появления и исполнения зловредных программ

За счёт функции «Контроль доступа к файлам» можно создать политику:

- Файлы с расширением *.exe, *.bat, *.js и т.д. может создавать только администратор

За счёт функции «Контроль доступа к объектам реестра» можно создать политику:

- Доступ к настройке служб в реестре ОС разрешен только администратору (HKLM\SYSTEM*ControlSet*\services*)

ViPNet SafePoint предотвращает такие попытки для пользователя с фиксацией информации в журнале аудита

Защита от действий «неопытного» пользователя

Запрет запуск приложений, скриптов из писем (защита от фишинговых атак по почте). Переход по нежелательным ссылкам

Как реализовать:

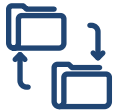
- запрет запуска, приложений из почтового клиента Outlook (кроме, например, Word, Excel, Acrobat Reader). Дополнительно политика на запрет запуска приложений, скриптов из Word, Excel, Reader
- Запуск файла из почты порождает процесс, этому процессу запрещено обращаться к ранее созданным размеченным файлам

Всё под контролем

- Контроль целостности и восстановление
  - Файлов
  - Объектов реестра ОС
- Контроль запуска разрешенных/запрещенных процессов
- Контроль активности обязательных процессов
- Контроль доступа к альтернативным потокам
- Контроль доступа к атрибутам файлов

Контроль подключения съемных носителей

Возможность использования только определённых (зарегистрированных) съемных устройств



Контроль копирования информации на съёмные носители (фиксация событий в журнале аудита)

Защита от запуска программ и скриптов с внешних накопителей

ViPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых», «бесфайловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия

ViPNet EndPoint Protection – комбинирование методов защиты

- Сигнатурные методы защиты:
  - правила белого/чёрного списка
  - правила для HIDS/HIPS
  - фильтры межсетевого экрана
- Эвристические методы защиты:
  - Поведенческий анализ
  - Эвристический антивирус (NGAV – бессигнатурный)
  - Математические модели, построенные при помощи искусственного интеллекта
- Средства мониторинга и передача событий для последующего анализа

Обнаружение и предотвращение вторжений

Непрерывная работа на уровне:

- Операционной системы
- Сети

Дополнительные механизмы:

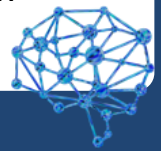
- Обнаружение аномалий с помощью критериев
- Обнаружение аномалий с помощью поведенческого анализа

Модуль поведенческого анализа

Используем модель нормальной активности защищаемого узла, построенной с помощью машинного обучения

Выявляем различного рода аномалии, например:

- Аномальный вход в систему
- Аномалия в создании процесса
- Аномальные запуски системных утилит, таких как powershell, rundll32, regsrv32 и т.д.
- Аномалия в создании задачи планировщику



Дополнительное в модуле системы обнаружения и предотвращения вторжений

TLS – инспекция

возможность расшифровывания трафика, проходящего через модули ViPNet EndPoint Protection. База «bad URL» поставляется в рамках БРП, обновляется регулярно

SafeBrowsing

безопасный сёрфинг в интернете (веб-фильтрация)

Межсетевой экран

- Фильтрация трафика Ipv4 и Ipv6
- Интеграция с ViPNet Client 4U/5

Добавление\Редактирование\Удаление фильтров защищённой сети из локальной консоли ViPNet EndPoint Protection (агент)

Контроль приложений

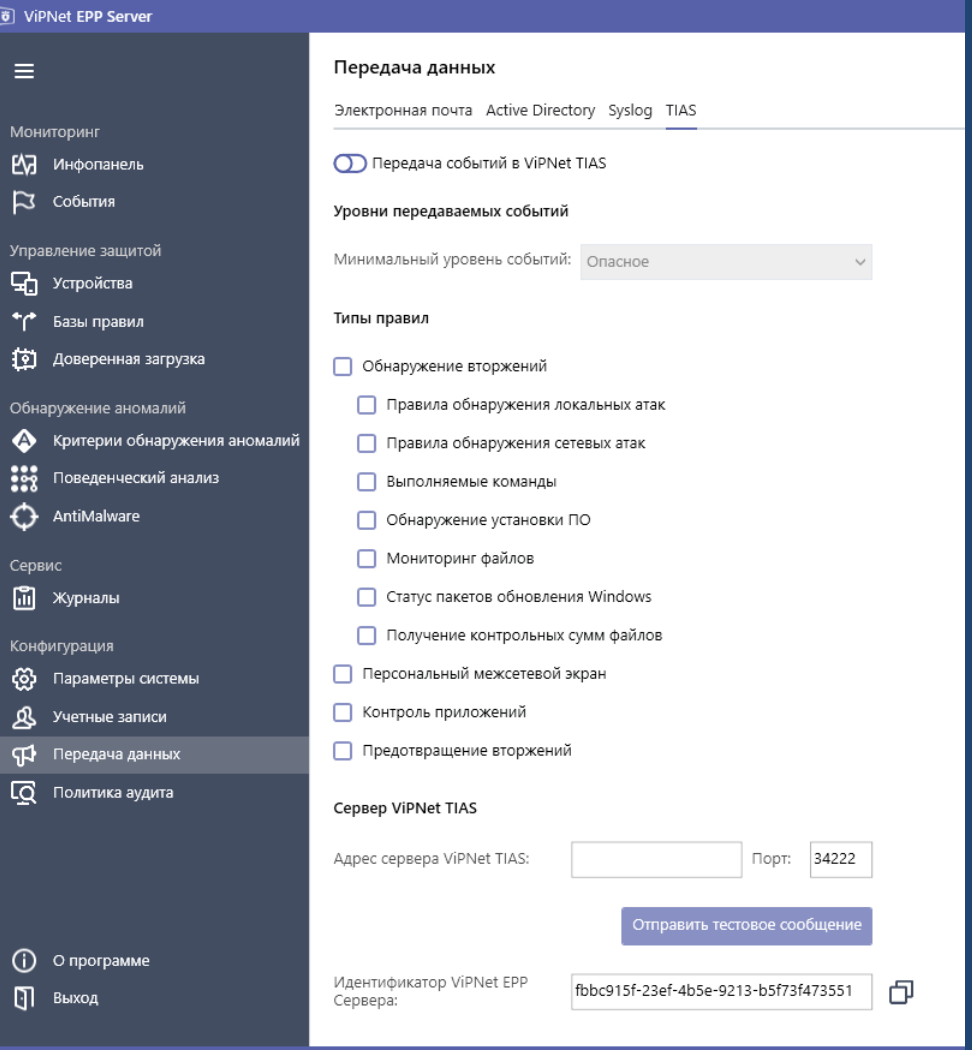
- Контроль запуска программ с использованием Черных и Белых списков программного обеспечения
- Анализ командной строки
- Защита файлов
- Защита реестра
- Контроль запуска программ, DLL-модулей, драйверов
- Контроль сетевой активности приложений

Эвристический Antimalware движок

Возможность сканирования исполняемых файлов и библиотек с целью выявления зловреда

Эвристический Antimalware использует собственную модель построенную с помощью машинного обучения

Модель постоянно обновляется в рамках подписки на БРП



Передача событий

Все события могут передаваться в:

- ViPNet TIAS
- В любую SIEM

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН · Актив · TS Solution · AXOFT

Подписывайтесь на наши соцсети