

VIPNet EndPoint Protection версия 1.5. Обзор новых возможностей продукта

Кадыков Иван
Руководитель направления



VIPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия. Ключевыми модулями системы являются персональный межсетевой экран, система обнаружения и предотвращения вторжений, а также контроль приложений.

Обнаружение и предотвращение атак

Используем:

- Эвристический анализ
- Сигнатурный анализ

Следим за:

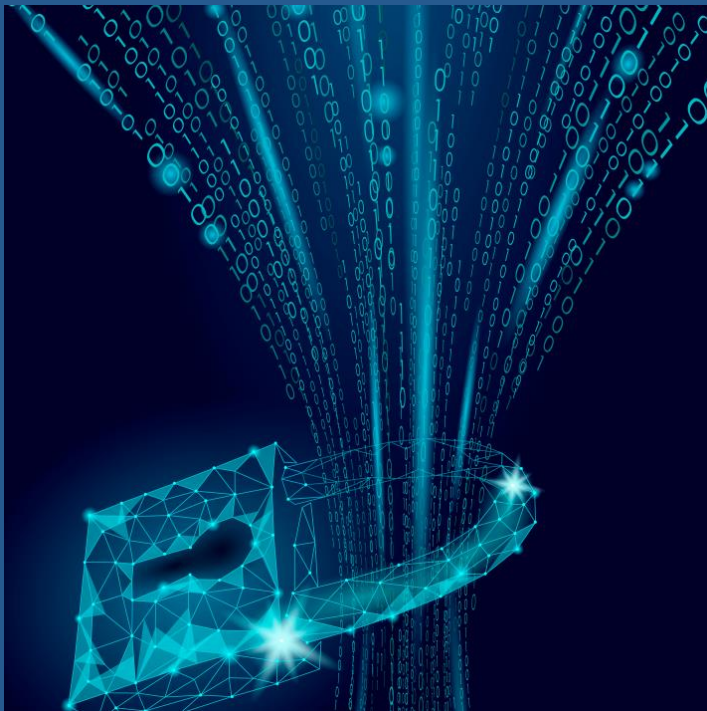
- Системными журналами Windows
- Журналами и логами приложений
- Изменениями в файловой системе и реестре
- Сетевым трафиком

Блокируем:

- Подозрительный сетевой трафик
- Атакующие хосты



Межсетевое экранирование



- Фильтрация трафика Ipv4 и Ipv6
- Работа сетевых фильтров по расписанию
- Наличие предустановленных фильтров
- Создание фильтров для определенных групп хостов
- Создание правил фильтрации из журнала трафика

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



WHITELIST



BLACKLIST

**NEW
VERSION**

**VIPNet EndPoint Protection
версия 1.5**

Новые защитные механизмы

Контроль приложений



Эвристический Anti-malware 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

Внешний вид Anti-malware

The screenshot displays the ViPNet EndPoint Protection Server interface. The main window is titled "AntiMalware" and shows the detection of malicious files on the device "DESKTOP-ID9FDVG". A table lists the scan results, including the start and end times of the scan. A detailed report window is open on the right, showing the scan configuration and a list of detected files with their severity levels.

DESKTOP-ID9FDVG

Обнаружение вредоносных файлов

Введите название устройства

Наименование	Время начала	Время завершения
DESKTOP-ID9FDVG	21.09.2021 18:54:12	21.09.2021 18:54:16
	21.09.2021 18:47:53	21.09.2021 18:48:00
	21.09.2021 18:41:52	21.09.2021 18:42:00
	21.09.2021 18:36:56	21.09.2021 18:37:00
	21.09.2021 18:36:32	21.09.2021 18:36:40
	21.09.2021 18:36:14	21.09.2021 18:36:20
	21.09.2021 18:30:30	21.09.2021 18:30:40
	21.09.2021 18:28:46	21.09.2021 18:28:50
	21.09.2021 18:27:48	21.09.2021 18:27:50
	21.09.2021 18:27:32	21.09.2021 18:27:35

Детали отчёта

Время начала: 21.09.2021 18:54:12
Время завершения: 21.09.2021 18:54:16
Сканирование: Выборочное
Проверено: 112
Опасных: 57
Неудачно: 0
Результат: Завершено

Поиск по путям

Файл (57)	Опасность
★ C:\Program Files\My program\Keylogger.exe	1,00
★ C:\Program Files\My program\PE_exec32bit.exe	1,00
★ C:\Program Files\My program\malware.exe	1,00
★ C:\Program Files\My program\trhhgfhgTRHTHT...	1,00
★ C:\Program Files\My program\dqldlllIOJOIOBO...	1,00
★ C:\Program Files\My program\Bad process.exe	1,00

Модуль поведенческого анализа

Используем модель нормальной активности защищаемого узла, построенную с помощью машинного обучения.

Выявляем различного рода аномалии, например:

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



ViPNet EndPoint Protection Server Администратор

Мониторинг
Инфопанель
События
Управление защитой
Устройства
Базы правил
Доверенная загрузка
Обнаружение аномалий
Критерии обнаружения аномалий
Поведенческий анализ
AntiMalware
Сервис
Журналы
Конфигурация
Параметры системы
Учетные записи
Передача данных
Политика аудита
О программе
Выход

События

Введите идентификатор события,

<input type="checkbox"/>	Дата, время	Идентификатор	Описание
<input type="checkbox"/>	21.09.2021 19:40:30	5000001	Разрешен запуск разрешенной программы
<input type="checkbox"/>	21.09.2021 19:40:10	5000001	Разрешен запуск разрешенной программы
<input type="checkbox"/>	21.09.2021 19:39:50	5000001	Разрешен запуск разрешенной программы
<input type="checkbox"/>	21.09.2021 19:39:29	5000001	Разрешен запуск разрешенной программы
<input type="checkbox"/>	21.09.2021 19:39:17	7000006	Аномалия в событии удаления файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000006	Аномалия в событии удаления файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000005	Аномалия в событии создания файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000005	Аномалия в событии создания файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания файла
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания файла
<input type="checkbox"/>	21.09.2021 19:39:09	400070	Удаление задачи планировщика
<input type="checkbox"/>	21.09.2021 19:39:09	300023	Удаление задачи (командная строка)
<input type="checkbox"/>	21.09.2021 19:39:09	400029	Установлена задача планировщика
<input type="checkbox"/>	21.09.2021 19:39:09	304000	Правило для модуля поведенческого анализа
<input type="checkbox"/>	21.09.2021 19:39:09	300022	Создание задачи (командная строка)
<input type="checkbox"/>	21.09.2021 19:39:09	300001	Создание процесса
<input type="checkbox"/>	21.09.2021 19:39:09	5000001	Разрешен запуск разрешенной программы
<input type="checkbox"/>	21.09.2021 19:38:49	5000001	Разрешен запуск разрешенной программы
<input type="checkbox"/>	21.09.2021 19:37:08	400014	Отправка DNS запроса

Аномалия в событии удаления задачи

21.09.2021 19:39:17

[Сработавшее правило](#) [Подробнее](#)

Тип правил:	Аномальная активность
Идентификатор правила:	7000006
Уровень события:	Важное
Превышение порога (IRE/RETh):	6.60/1.05
Описание:	Аномалия в событии удаления задачи
Модуль:	BA
Устройство:	DESKTOP-ID9FDVG
Попытки:	1
Дата:	21.09.2021 16:39:09
База правил на устройстве:	3.0.0
Тип правил:	Системная активность (Windows)
Идентификатор правила:	400070
Уровень события:	Опасное
Описание:	Удаление задачи планировщика
Модуль:	HIDS
Попытки:	2
Категория:	Подозрительная, потенциально опасная активность
Описание категории:	События данной категории могут свидетельствовать о компрометации системы либо указывать на факт компрометации, например: установка подозрительных служб/драйверов, изменение типа запуска служб, изменения в системном каталоге, изменения в группах пользователей, создание/удаление учетных записей, множественные неудачные попытки логина и т.д.
Рекомендуемые действия:	Рекомендуемые действия: провести корреляцию с другими событиями ИБ.

Выявление аномалий

Обнаружение и предотвращение бесфайловых атак

Расширение возможностей модуля обнаружения и предотвращения вторжений

Отслеживаем техники Keylogging и Process injection

- Credential API Hooking (T1056.004)
- Process Hollowing (T1055.012)
- Process Doppelganging (T1055.013)
- Dynamic-link library injection (T1055.001)
- Portable Executable Injection (T1055.002)



Как «действует» бесфайловая атака



VIPNet EndPoint Protection Server

Редактор правил - Обнаружение и предотвращение вторжений - Бесфайловые атаки

Глобальные

Найти + Добавить ↑ ↓ 🗑️

<input type="checkbox"/>	Правило	Действие	Тип хука	Маска процесса
<input type="checkbox"/>	<input checked="" type="checkbox"/> Allow explorer	✔ Разрешать	Клавиату...	?\.*\explorer.exe
<input type="checkbox"/>	<input checked="" type="checkbox"/> Allow cmd	✔ Разрешать	Окна	*cmd.exe
<input type="checkbox"/>	<input checked="" type="checkbox"/> Block keylogger	❗ Блокировать	Клавиату...	*\.*\keylogger.exe
<input type="checkbox"/>	<input checked="" type="checkbox"/> Block *consent.exe	❗ Блокировать	Прочее	*consent.exe
<input type="checkbox"/>	<input checked="" type="checkbox"/> Block all	❗ Блокировать	Клавиату...	*

Обнаружение и предотвращение бесфайловых атак

VIPNet EndPoint Protection Server

Администратор

События

Введите идентификатор события, 🔍 🔍 🔄 Обновить 🗑️

<input type="checkbox"/>	Дата, время	Идентификатор	Описание
<input type="checkbox"/>	19.08.2021 18:14:19	5000001	Разрешен запуск разрешенной программы
<input type="checkbox"/>	19.08.2021 18:13:59	4000069	Обновление задачи планировщика
<input type="checkbox"/>	19.08.2021 18:13:59	5000001	Разрешен запуск разрешенной программы
<input checked="" type="checkbox"/>	19.08.2021 18:13:38	6381008	Блокирование Keylogging
<input type="checkbox"/>	19.08.2021 18:13:38	4000069	Обновление задачи планировщика
<input type="checkbox"/>	19.08.2021 18:13:38	4000014	Отправка DNS запроса
<input type="checkbox"/>	19.08.2021 18:13:38	5000001	Разрешен запуск разрешенной программы
<input type="checkbox"/>	19.08.2021 18:13:18	6381008	Блокирование Keylogging
<input type="checkbox"/>	19.08.2021 18:13:18	4000014	Отправка DNS запроса
<input type="checkbox"/>	19.08.2021 18:13:18	5000001	Разрешен запуск разрешенной программы

Блокирование Keylogging

19.08.2021 18:13:38

Сработавшее правило: Подробнее

База правил на устройстве: 2.0.0

Тип правил: Предотвращение бесфайловых атак (Windows)

Идентификатор правила: 6381008

Уровень события: Опасное

Описание: Блокирование Keylogging

Модуль: HIPS

Устройство: DESKTOP-ID9FDVG

Попытки: 3

Входит в состав модуля «Обнаружения и предотвращения вторжений»

Введите название базы правил для | 🔍 | 🗑️ | 🔄 Проверить обновления | 📄 Загрузить

<input type="checkbox"/>	Наименование	Режимы	Версия	Группы	Создана
<input type="checkbox"/>	Загружены из файла Errp_20210811_1_1.5_RU.zip	Частная сеть Разрешать Минимальный	2.0.0	Главная, Дом, Мобил...	19.08.20...
<input type="checkbox"/>	База правил по умолчанию	Частная сеть Разрешать Базовый	1.0.3	Главная	19.08.20...
<input type="checkbox"/>	База правил по умолчанию	Сетевой экран отключен Отключен Миним:	1.0.2	Главная	19.08.20...
<input type="checkbox"/>	База правил по умолчанию	Сетевой экран отключен Отключен Миним:	1.0.1	Главная	19.08.20...
<input type="checkbox"/>	База правил по умолчанию	Частная сеть Белый список - Уведомлять М:	1.0.0		19.08.20...

Работаем по правилам!

БРП состоит из:

- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевое экрана
- Списков ПО для Черного и Белого списка
- Эвристического движка Anti-malware
- Движка обнаружения аномального поведения системных утилит

Поддержка Linux

Реализован ViPNet EndPoint Protection агент под следующие операционные системы:

- Astra Linux Special Edition «Смоленск» 1.6.
- РЕД ОС 7.2.
- Альт Рабочая станция 8 СП



Управление ViPNet SafeBoot

ViPNet EndPoint Protection Server Администратор

Доверенная загрузка

Устройства Лицензии

Введите название устройства 🔍 Выбрано 0 🗑️ ▶️ Выгрузить журнал аудита | Активировать лицензию

<input type="checkbox"/>	Наименование	Состояние	Версия SafeBoot	Лицензия
↑ Все устройства > Офис				
<input type="checkbox"/>	astra	Не в сети	Не установлен	Не распределена
<input type="checkbox"/>	DESKTOP-4FTK2QK	В сети	2.0.0.22	Не распределена

Контроль приложений



Блокировать

Запуск неизвестных приложений блокируется. Активность остальных приложений определяется правилами Контроля приложений.



Разрешать

Запуск неизвестных приложений разрешен. Активность остальных приложений определяется правилами Контроля приложений.



Отключен

Контроль приложений отключен и не влияет на активность приложений.

Изменение в режимах работы Контроля приложений

Теперь три варианта работы

Параметры системы

Параметры Агента Параметры Сервера Обновление баз правил Сервис

Использовать автоматическую загрузку обновлений баз правил

Дата и время последней проверки обновлений: неизвестно.

Сервер обновления

Адрес сервера обновлений:

Имя пользователя:

Пароль:

Прокси-сервер

Использовать прокси-сервер

Адрес сервера:

Авторизация

С текущей учетной записью

С учетной записью

Имя пользователя:

Пароль:

Автоматическая загрузка БРП и избранные правила

Появилась возможность автоматической загрузки БРП с сохранением ранее созданных правил.

Общая информация о ViPNet EndPoint Protection

ViPNet Endpoint Protection



ViPNet Endpoint Protection

Консоль
управления



Сервер
ViPNet
Endpoint
Protection

ViPNet Endpoint Protection



ViPNet Endpoint Protection

Архитектура ViPNet EndPoint Protection

- Клиент
- Сервер
- Консоль
управления

Поддерживаемые ОС

Сервер и агент

- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019



Только Агент

- Astra Linux Special Edition «Смоленск» 1.6.
- РЕД ОС 7.2.
- Альт Рабочая станция 8 СП



Полная защита



Решаемые задачи

Мониторинг
и противодействие
подозрительной
активности на хосте

Защита от сетевых атак

**ViPNet EndPoint
Protection**

Защита от внедрения
и выполнения вредоносных
программ и кода

Контроль запуска
приложений

Ожидание по сертификации



Продукт на сертификации по линии ФСТЭК России по требованиям к:

- Системам обнаружения вторжений уровня узла 4 класса ИТ.СОВ.У4.ПЗ
- Межсетевым экранам типа В класса 4 (ИТ.МЭ.В4.ПЗ)
- 4 классу ТДБ