

Обзор продуктов линейки ViPNet EndPoint Security

Свежий взгляд на классические
подходы к защите Endpoint

Кадыков Иван
Руководитель продуктового направления



техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Пролог

Рынок защиты рабочих станций многогранен



Все поддается структуризации

Классический Endpoint Protection

- знаем, что ищем (антивирус). Блокируем, что знаем (МЭ + HIPS), контролируем подключение устройств

Next Generation Endpoint Protection

- классический Endpoint + модули по обнаружению и противодействию современным угрозам (ransomware, fileless-атаки, never-before-seen attacks) – Sandbox, Appcontrol, Memory Protection...

Endpoint Detection & Response

- NG EPP + возможность расследования инцидента и формирование реакции на инцидент (forensic)



«Российский Endpoint»

Средство защиты
от несанкционированного
доступа

«Конечные
устройства» –
главная цель



Растущее количество атак и недоверенных аппаратных компонент

Доверие к платформе и обеспечение доверенной загрузки ОС

Разграничение доступа и защита данных

Пользователь - внутренний нарушитель, низкий уровень опыта

Удаленная работа, проведение частных разговоров

Обеспечение защищенных коммуникаций

Защита от внешних атак и угроз

Malware, Ransomware, Fileless & Never-seen-before attacks

ViPNet SafeBoot



ViPNet SafeBoot

Высокотехнологичный программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS.

Решаемые задачи ViPNet SafeBoot

Организация доверенной загрузки

Контроль целостности

Разграничение
доступа

UEFI BIOS

MBR

Таблицы
ACPI,
SMBIOS,
карты
распределе
ния памяти

Файлов

CMOS

Двухфакторная
аутентификация

Авторизация
в AD/LDAP

Релиз 2.1. Сертифицированная версия

- Защита от malware в UEFI BIOS
- Активация защиты на платформах AMD
- Поддержка токена Rutoken S
- Поддержка работы со считывателями смарт-карт – ACR38, JCR721, ASEDrive IIIe
- Поддержка SSO для входа в операционную систему и VipNet SafePoint v.1.2
- Поддержка сенсорных экранов, реализация сенсорной клавиатуры под UEFI
- Базовая поддержка ARM-архитектуры



Зловреды, атаки, уязвимости...

2016

Cr4sh/PeiBackdoor

PEI stage backdoor for UEFI compatible firmware

PeiBackdoor – один из первых «зловредов» для UEFI

2018

LOJAX

First UEFI rootkit found in the wild, courtesy of the Sednit group

Lojax – первый rootkit найденный сотрудниками компании ESET в «дикой среде»

2020



MosaicRegressor:
Lurking in the
Shadows of UEFI

BootHole

MosaicRegressor – bootkit найденный сотрудниками «Лаборатории Касперского», предназначенный для шпионажа.

BootHole – уязвимость в загрузчике

2021



ESpecter – bootkit предназначенный для целевых атак и шпионажа (найден сотрудниками ESET)

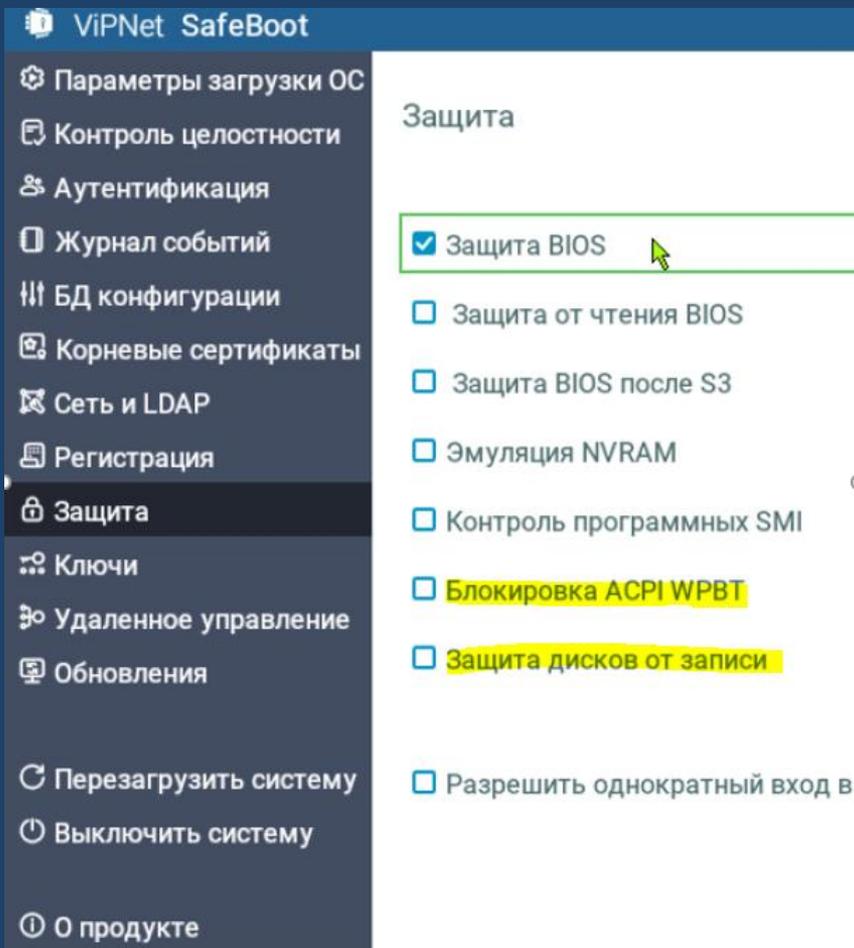
2022



MoonBounce позволяет изменить цепочку выполнения команд в UEFI BIOS и осуществить внедрение вредоносного кода, который запустится при старте машины.

CosmicStrand – рутки находится в образах прошивок материнских плат [Gigabyte](#) и [Asus](#), использующих чипсет H81 – 26.07.2022

Уязвимости в подписанных загрузчиках Microsoft – CVE-2022-34301(-34302, - 34303) –



Защита от Malware

Как действует malware?

- запись файлов malware из UEFI на диск посредством встроенного (собственного) драйвера файловой системы
- использование технологии Windows Platform Binary Table (WPBT)

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00



СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3823

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
14 ноября 2017 г.

Выдан: 14 ноября 2017 г.
Действителен до: 14 ноября 2020 г.
Срок действия продлен до: 14 ноября 2025 г.

Настоящий сертификат удостоверяет, что программный комплекс «Программный модуль доверенной загрузки VIPNet SafeBoot», разработанный и производимый АО «ИнфоТекС», является программным средством доверенной загрузки, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 2 уровню доверия, «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТ.СД/З.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00180-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 28.07.2017, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.5004), экспертного заключения от 12.10.2017, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), технического заключения от 16.04.2021, оформленного испытательной лабораторией ООО «ЦБИ», и экспертного заключения от 28.05.2021, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Заявитель: АО «ИнфоТекС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



В.Лютиков

Примечание: сертифицированной продукцией, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации.

Сертифицировано

Сертифицирован по:

- Требованиям к средствам доверенной загрузки уровня базовой системы ввода-вывода 2 класса
- Требованиям по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий по 2 уровню доверия



Задачи и потребности – Compliance

- Задача: соответствие требованиям ФСТЭК России по защите ИСПДн, ГИС, АСУ ТП и КИИ – выполнение полного комплекса мер по защите.
- Необходимость использования прописана в мерах защиты по первому и второму классу:
 - В ИСПДн и ГИС – УПД.17
 - В АСУ ТП и КИИ – УПД.3

29 угроз

в полной или косвенной мере относящиеся к угрозам BIOS/UEFI BIOS

Угроза	Угроза
УБИ.004: Угроза аппаратного сброса пароля BIOS	УБИ.053: Угроза невозможности управления правами пользователей BIOS
УБИ.005: Угроза внедрения вредоносного кода в BIOS	УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.008: Угроза восстановления аутентификационной информации	УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS
УБИ.006: Угроза внедрения кода или данных	УБИ.090: Угроза несанкционированного создания учётной записи пользователя
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS	УБИ.108: Угроза ошибки обновления гипервизора
УБИ.013: Угроза деструктивного использования декларированного функционала BIOS	УБИ.121: Угроза повреждения системного реестра
УБИ.018: Угроза загрузки нештатной операционной системы	УБИ.123: Угроза подбора пароля BIOS
УБИ.023: Угроза изменения компонентов системы	УБИ.124: Угроза подделки записей журнала регистрации событий
УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера	УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию	УБИ.144: Угроза программного сброса пароля BIOS
УБИ.032: Угроза использования поддельных цифровых подписей BIOS	УБИ.145: Угроза пропуска проверки целостности программного обеспечения
УБИ.035: Угроза использования слабых криптографических алгоритмов BIOS	УБИ.150: Угроза сбоя процесса обновления BIOS
УБИ.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS	УБИ.152: Угроза удаления аутентификационной информации
УБИ.045: Угроза нарушения изоляции среды исполнения BIOS	УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS
	УБИ.179: Угроза несанкционированной модификации защищаемой информации

VipNet SafeBoot 3.0

Выпущен VipNet SafeBoot 3.0, который будет сертифицироваться в двух исполнениях:

- Исполнение 1. «Локальный» VipNet SafeBoot – без механизмов удалённого управления, подключения к LDAP – в ФСБ России и в ФСТЭК России
- Исполнение 2. «Сетевой» VipNet SafeBoot – с механизмами удалённого управления – только в ФСТЭК России

Дополнительно реализовано:

- Доверенная загрузка ОС по сети
- Формирование отчёта о настройках продукта
- Поддержка токена Guardant ID версии 2
- Поддержка ALD PRO (Astra Linux)
- Поддержка работы на бездисковых станциях



**New
Version**

ViPNet SafePoint

VIPNet SafePoint



Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации.

Реализована разграничительная (пользователя к объектам) и разделительная (между пользователями) политика доступа, основанная на автоматической разметке создаваемых файлов.

С чего начинается защита от НСД?

Своих пользователей надо знать «в лицо», поэтому:

- Идентификация и аутентификация пользователей
- Выполняется собственными механизмами

Используем комбинации:

- Логин и пароль
- Логин и идентификатор



SSO (единый вход) для SafeBoot и SafePoint

В интерфейс SafePoint при добавлении/изменении пользователя добавлен дополнительный флаг:

- «Разрешить вход SSO (режим единого входа)»
- Флаг является индивидуальным для каждого пользователя
- Поддерживаемые версии
- ViPNet SafeBoot 2.1
- ViPNet SafeBoot 3.0

Редактирование данных пользователя

Пользователь: DESKTOP-SECQVOA\User1

Доверять паролю Windows

Пароль SafePoint:

Подтвердите пароль:

Пароль Windows:

Подтвердите пароль Windows:

Разрешить пользователю осуществлять вход с помощью:

Ввода имени и пароля

Электронного ключа ruToken

Электронного ключа Aladdin JaCarta

Разрешить вход при работе ОС в безопасном режиме

Разрешить вход SSO (режим единого входа)

Создание разграничительных политик для пользователя

После прохождения идентификации и аутентификации, необходимо чтобы пользователь:

- Работал только с тем ПО, которое разрешено
- Мог работать только с теми файлами/документами, для которых хватает прав(полномочий)
- В системе запускались, только разрешенные процессы
- Не модифицировал(-ись) важные модули



Разграничение доступа

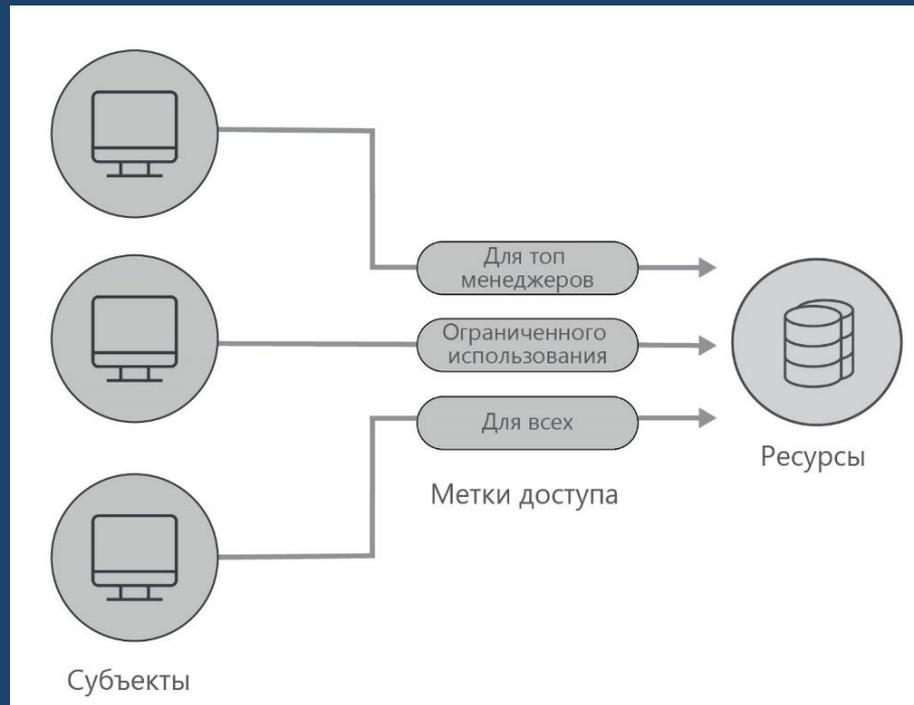
Дискреционный контроль доступа к

- Файловой системе (вкл. сменные)
- Прямому доступу к диску
- Реестру
- Принтерам
- Службам
- Устройствам
- Буфер обмена
- Виртуальным машинам



Мандатный контроль доступа пользователей и процессов

Разграничительная политика на основе меток безопасности



Замкнутая программная среда и контроль времени работы

Защита от
модификации
запускаемых
модулей (РПД)

Ограничение
по каталогам
запуска
(РПД)
%SystemRoot%
%ProgramFiles%

Контроль
запуска
скриптов (по
расширениям или
хост-процессу)

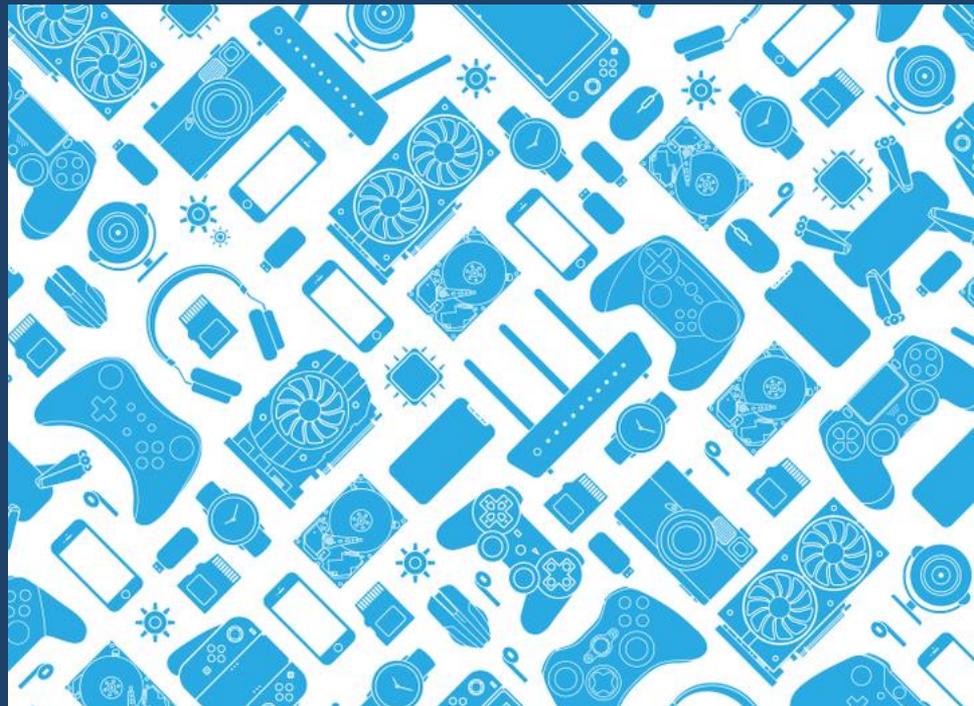
Разрешенные
процессы
%SystemRoot%
%ProgramFiles%

Обязательные
процессы
(Пользователь
+ командная
строка)

Расписание
работы
(Процесс +
День недели,
Начало,
Окончание,
Максимум,
Аудит)

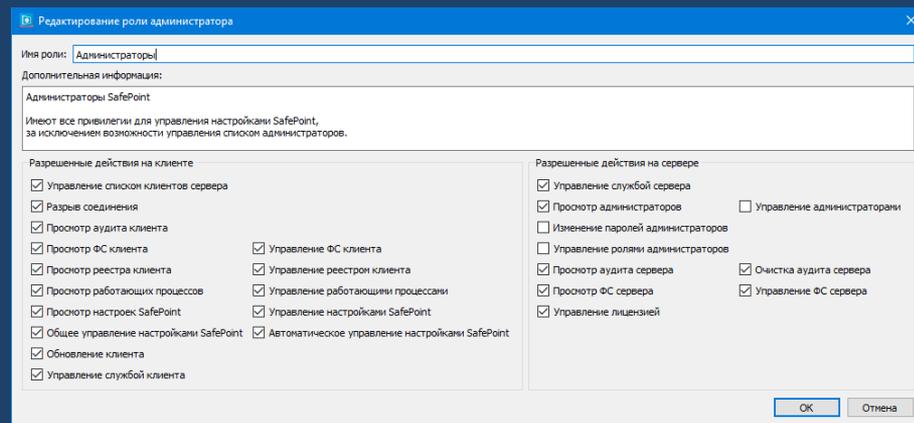
Контроль устройств

- Контроль и разграничение доступа к подключаемым внешним устройствам
- Разграничение доступа к принтерам



Ограничение действий администраторов

- Реализация настраиваемых ограничений в действиях администраторов – в части управления пользователями в Active Directory
- Делегирование административных полномочий (полных прав/части прав)



Централизованная установка и обновление продукта

Консоль развертывания SafePoint

Маленькие иконки

Объекты	Состояние	Отложенная задача	Версия	Файл установки	Файл обновления
domain.local					
Computers					
DESKTOP-8B086P9	Проверка состояния продукта		1.1.0.310	Z:\D:\Safe Point\safepoint_x64_1.1.0.310.msi	Z:\D:\Safe Point\sp_updater_x86_1.0.1.228.exe
DESKTOP-90625GI	Сервер RPC недоступен		1.1.0.299	Z:\D:\Safe Point\safepoint_x64_1.1.0.299.msi	Z:\D:\Safe Point\sp_updater_x64_1.1.0.310.exe
buh			1.1.0.296	Z:\D:\Safe Point\safepoint_x64_1.1.0.296.msi	Z:\D:\Safe Point\sp_updater_x64_1.1.0.299.exe
buh2			1.1.0.291	Z:\D:\Safe Point\safepoint_x64_1.1.0.291.msi	Z:\D:\Safe Point\sp_updater_x64_1.1.0.296.exe
test-compuet2	Проверка состояния продукта		1.0.1.243	Z:\D:\Safe Point\safepoint_x64_1.0.1.243.msi	Z:\D:\Safe Point\sp_updater_x64_1.1.0.291.exe
zzz			1.0.1.242	Z:\D:\Safe Point\safepoint_x64_1.0.1.242.msi	Z:\D:\Safe Point\sp_updater_x64_1.0.1.243.exe
buh2			1.0.1.229	Z:\D:\Safe Point\safepoint_x64_1.0.1.229.msi	Z:\D:\Safe Point\sp_updater_x64_1.0.1.242.exe
test-computer	Проверка состояния продукта		1.0.1.228	Z:\D:\Safe Point\safepoint_x64_1.0.1.228.msi	Z:\D:\Safe Point\sp_updater_x64_1.0.1.229.exe
win10-deploy-3	Проверка состояния продукта		1.0.1.227	Z:\D:\Safe Point\safepoint_x64_1.0.1.227.msi	Z:\D:\Safe Point\sp_updater_x64_1.0.1.228.msi
win10-deploy-4	Проверка состояния продукта		1.0.1.222	Z:\D:\Safe Point\safepoint_x64_1.0.1.222.msi	Z:\D:\Safe Point\safepoint_x64_1.0.1.227.msi
test-computer3	Проверка состояния продукта		1.0.1.218	Z:\D:\Safe Point\safepoint_x64_1.0.1.218.msi	Z:\D:\Safe Point\safepoint_x64_1.0.1.222.msi
buh3			1.0.0.214	Z:\D:\Safe Point\safepoint_x64_1.0.0.214.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.218.msi
buh4			1.0.0.213	Z:\D:\Safe Point\safepoint_x64_1.0.0.213.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.214.msi
win10-deploy-1	Не установлено		1.0.0.212	Z:\D:\Safe Point\safepoint_x64_1.0.0.212.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.213.msi
win10-deploy-2	Не установлено		1.0.0.211	Z:\D:\Safe Point\safepoint_x64_1.0.0.211.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.212.msi
todel			1.0.0.210	Z:\D:\Safe Point\safepoint_x64_1.0.0.210.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.211.msi
todel2			1.0.0.207	Z:\D:\Safe Point\safepoint_x64_1.0.0.207.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.210.msi
win81-64-pc	Не установлено		1.0.0.206	Z:\D:\Safe Point\safepoint_x64_1.0.0.206.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.207.msi
test-computer4	Проверка состояния продукта		1.0.0.197	Z:\D:\Safe Point\safepoint_x64_1.0.0.197.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.206.msi
WIN-G9TUM7B3KEO	Установлено. Версия 1.0.1.243		1.0.0.192	Z:\D:\Safe Point\safepoint_x64_1.0.0.192.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.197.msi
			1.0.0.170	Z:\D:\Safe Point\safepoint_x64_signed.msi	Z:\D:\Safe Point\safepoint_x64_signed.msi
			1.0.0.161	Z:\D:\Safe Point\safepoint_x64_1.0.0.161.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.170.msi
			1.0.0.160	Z:\D:\Safe Point\safepoint_x64_1.0.0.160.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.161.msi
			1.0.0.159	Z:\D:\Safe Point\safepoint_x64_1.0.0.159.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.160.msi
			1.0.0.158	Z:\D:\Safe Point\safepoint_x64_1.0.0.158.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.159.msi
			1.0.0.155	Z:\D:\Safe Point\safepoint_x64_1.0.0.155.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.158.msi
			1.0.0.154	Z:\D:\Safe Point\safepoint_x64_1.0.0.154.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.155.msi
			1.0.0.153	Z:\D:\Safe Point\safepoint_x64_1.0.0.153.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.154.msi
			1.0.0.149	Z:\D:\Safe Point\safepoint_x64_1.0.0.149.msi	Z:\D:\Safe Point\safepoint_x64_1.0.0.153.msi
			1.0.0.144	Z:\D:\Safe Point\safepoint_x64.msi	Z:\D:\Safe Point\sp_updater_x64_1.0.0.149.msi
			1.0.0.39	Z:\D:\Safe Point\safepoint_x64_fixDevMask.msi	Z:\D:\Safe Point\safepoint_x64.msi
			1.0.0.25	Z:\D:\Safe Point\safepoint_x64_pdc.msi	Z:\D:\Safe Point\safepoint_x64_fixDevMask.msi

СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 4468

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
18 октября 2021 г.

Выдан: 18 октября 2021 г.
Действителен до: 18 октября 2026 г.

Настоящий сертификат удостоверяет, что изделие «VIPNet SafePoint», разработанное и производимое АО «ИнфоТекС», является программным средством защиты информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014), «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ» (ФСТЭК России, 2014), «Средства вычислительной техники. Защита от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 5 классу защищенности и заданию по безопасности ФРКЕ.00240-01 98 01 при выполнении указанных по эксплуатации, приведенных в формуляре ФРКЕ.00240-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 15.07.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Е012), и экспертного заключения от 05.10.2021, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

Заявитель: АО «ИнфоТекС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ




В. Лютиков

Примечание: Сертифицированной продукцией, указанной в настоящем сертификате соответствия, на объектах (объектах информации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Сертифицировано

- 5 класс защищенности СВТ
- 4 класс защиты СКН (ИТ.СКН.П4.ПЗ)
- 4 класс ТДБ

VIPNet SafePoint 1.5

Релиз был выпущен 12.12.2022

Главное - Разработан Клиент Linux с функциональностью необходимой для соответствия требованиям СВТ5 и СКН4.

Поддерживаемые ОС:

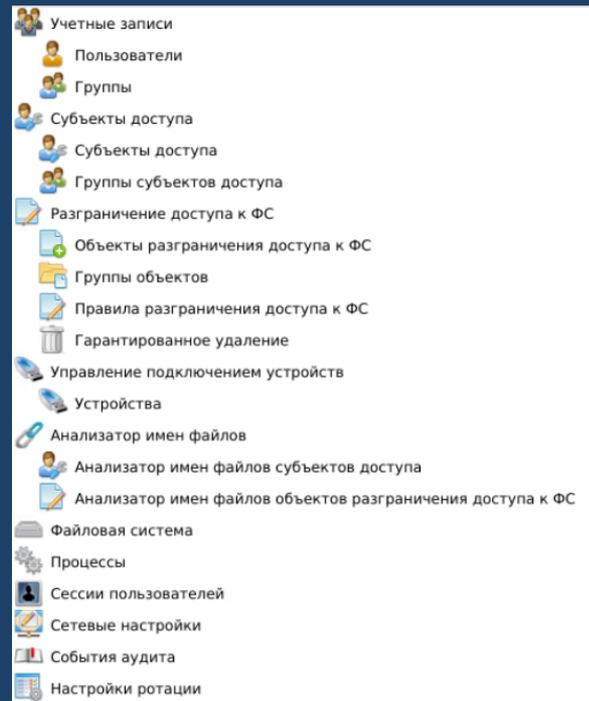
- Альт Рабочая станция 10.0, ядро Linux (std-def) 5.10.82
- РЕД ОС 7.3.1 МУРОМ x86_64, ядро Linux 5.15.10 (Рабочая станция)
- Debian 11 (64-разрядная), ядро 5.10.0-10-amd64
- Astra Linux Special Edition, РУСБ.10015-01 (Astra Linux Special Edition 1.7 «Воронеж» и «Орёл») – без режима замкнутой программной среды
- 25.01.2023 – закончили процедуру внесения изменений по линии ФСТЭК России – версия сертифицирована



Функциональность Linux агента

- Идентификация и аутентификация пользователей (без токенов)
- Управление учетными записями
- Дискреционное разграничение доступа
- Управление подключением устройств
- Гарантированное удаление файлов
- Очистка дисковых томов
- Самотестирование и контроль целостности
- Аудит событий безопасности

16/02/2023 буду проводить вебинар



Работаем над VipNet SafePoint версия 1.6

- Расширение шаблонов политик безопасности по требованиям приказов 17,21,31,239
- Реализация мандатных меток на устройства (перемещение файлов с метками)
- Динамический контроль целостности
- Мандатная модель в линукс агенте
- SSO с SafeBoot в линукс агенте
- Поддержка токенов для идентификации/аутентификации для линукс агентов
- Поддержка новых ОС Linux



ViPNet EndPoint Protection

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.



Защитные механизмы

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:

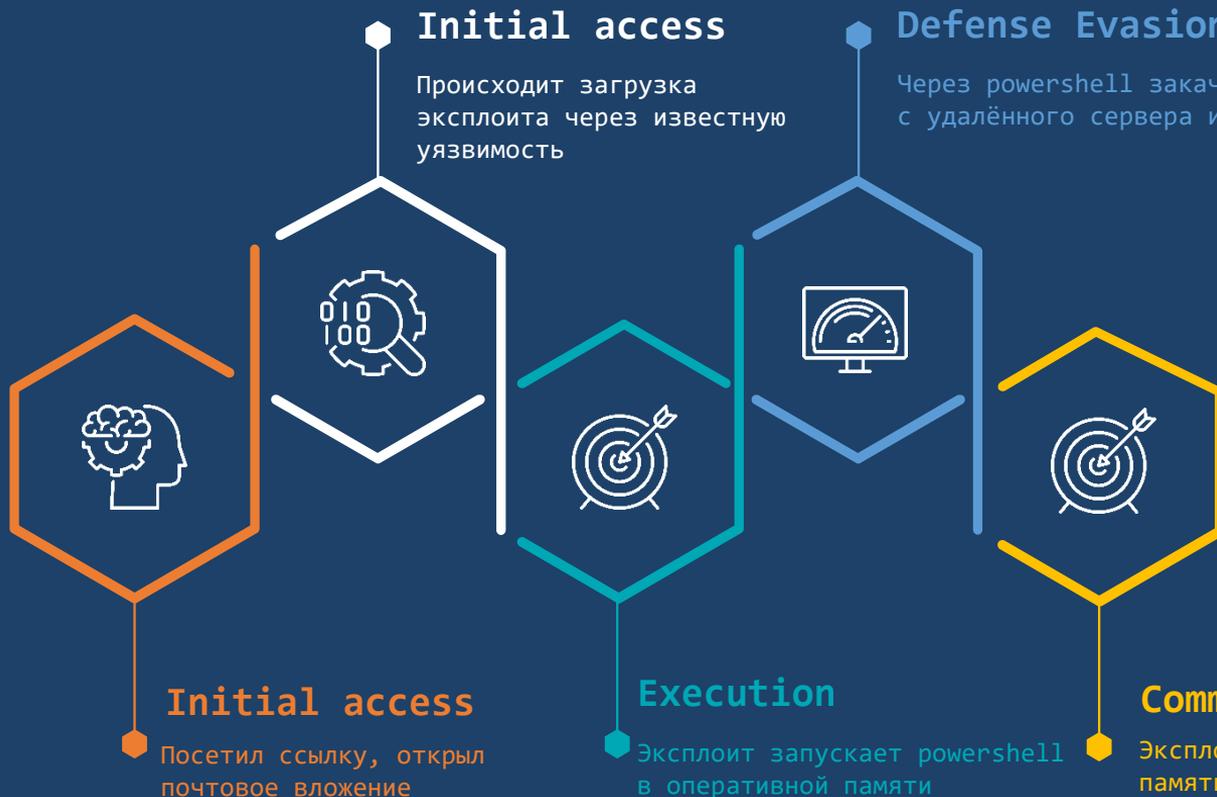
- Подозрительный сетевой трафик
- Атакующие хосты



Расширение функциональности NIPS

- Обнаружение и предотвращение бесфайловых атак
- 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)

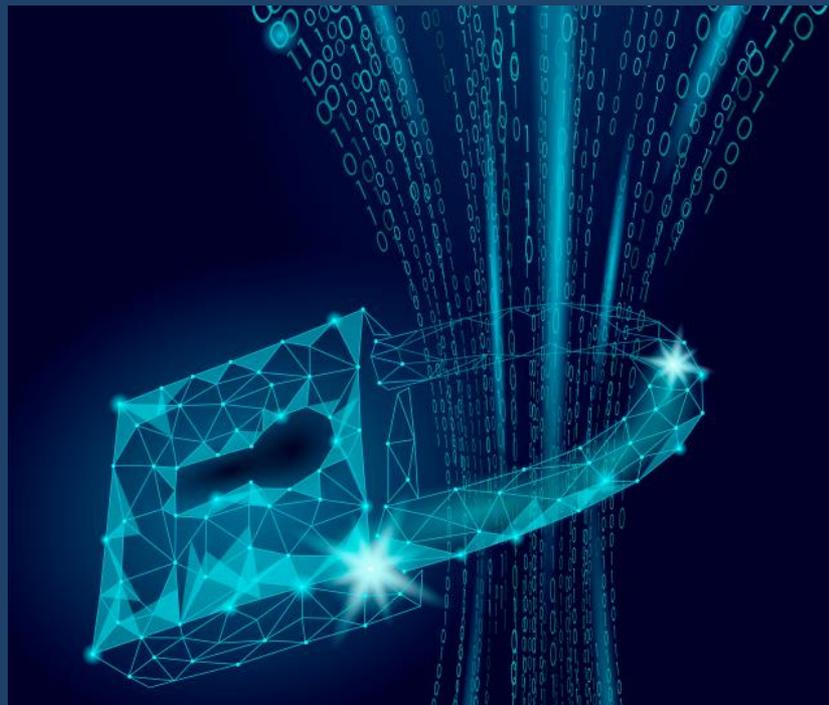




Как «действует» бесфайловая атака

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

Модуль поведенческого анализа

Behavioral analysis

- Выявление аномального поведения (запуска/остановки) системных утилит
- Эвристический движок antimalware



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



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



ViPNet Endpoint Protection



ViPNet Endpoint Protection

Консоль
управления



Сервер
ViPNet
Endpoint
Protection

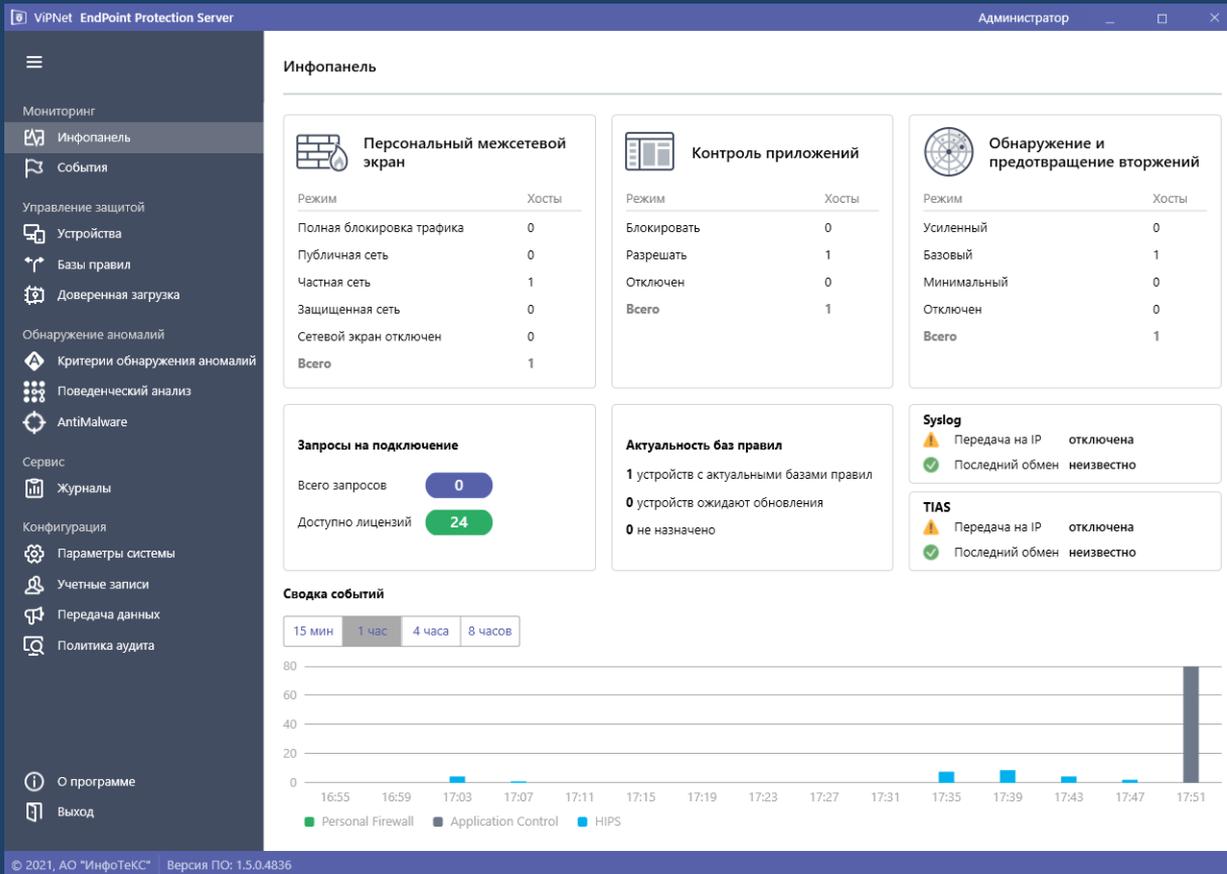
ViPNet Endpoint Protection



ViPNet Endpoint Protection

Архитектура ViPNet EndPoint Protection

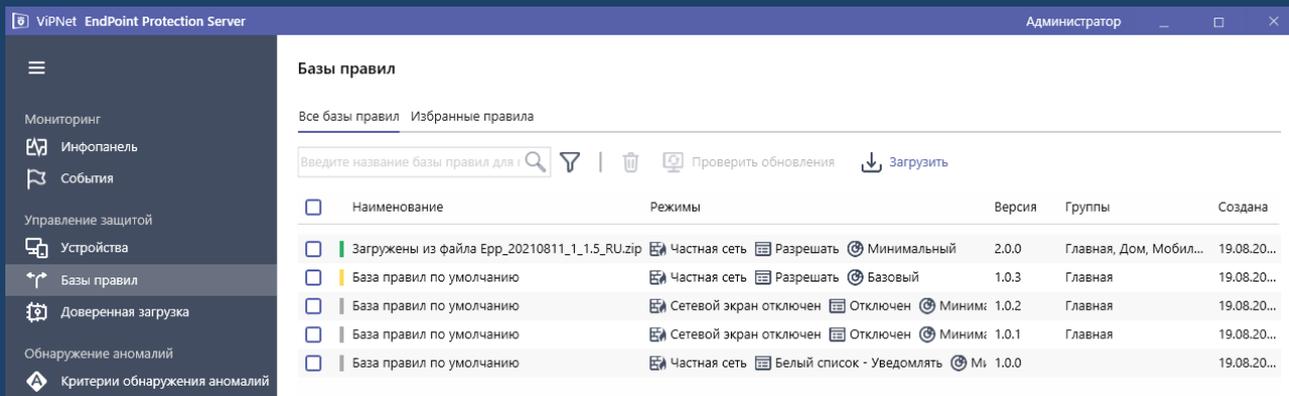
- Клиент
- Сервер
- Консоль управления



Консоль управления сервером

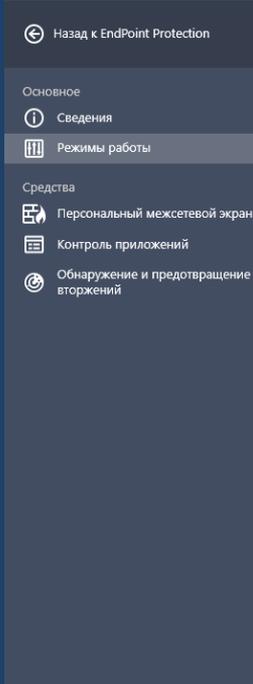
Работаем по правилам!

EndPoint Protection работает по БРП



Состоит из:

- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевое экрана
- Списков ПО для Черного и Белого списка
- Эвристический движок Anti-malware
- Движок обнаружения аномального поведения системных утилит



Редактор правил - Режимы работы

Сохранить

Отмена

Персональный межсетевой экран

**Полная блокировка трафика**

Блокируется любой входящий и исходящий трафик.

**Публичная сеть**

Подключение к общественной сети. Максимальная степень защиты, определяемая политикой безопасности.

**Частная сеть**

Подключение к частной сети. Пользователь может самостоятельно определять сетевые фильтры.

**Защищенная сеть**

Работа в защищенной сети. Пользователь самостоятельно определяет сетевые фильтры.

**Отключен**

Personal Firewall полностью отключен и не влияет на сетевой трафик.

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.

Обнаружение и предотвращение вторжений



Модуль обнаружения вторжений активен

**Усиленный**

Используется полный набор правил предотвращения вторжений, может приводить к снижению быстродействия компьютера.

**Базовый**

Используется оптимальный набор правил предотвращения вторжений, обеспечивающий достаточную защиту в большинстве случаев.

**Минимальный**

Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критических атак.

**Отключен**

Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.

Настройки модулей — Режимы работы

Администратор может использовать предоставленные нами режимы работы модулей или сам настроить режимы работы модулей

✓ Модуль обнаружения вторжений активен



Усиленный

Используется полный набор правил предотвращения вторжений, может приводить к снижению быстродействия компьютера.



Базовый ✓

Используется оптимальный набор правил предотвращения вторжений, обеспечивающий достаточную защиту в большинстве случаев.



Минимальный

Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критичных атак.



Отключен

Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.

Обнаружение и предотвращение вторжений

Обнаружение вторжений активно всегда.
Механизмы работы схожи с VipNet IDS HS:

- Загрузили БРП
- Назначили на группу агентов
- Агенты, получив БРП, мониторят события в соответствии с заданными политиками аудита

Предотвращение вторжений – имеется несколько уровней защиты – Усиленный, Базовый, Минимальный (разрабатывали совместно с ПМ)

Предотвращение вторжений

По категориям угроз

Обнаружение и предотвращение вторжений - Категории угроз

Попытка раскрыть информацию (attempted-recon)

События данной категории свидетельствуют о попытках сбора информации. Разведовательные атаки не являются сбором информации была успешной.

Прочие атаки (misc-attack)

События данной категории не относятся к какой-либо другой категории

Атака с использованием веб-приложения (web-application-attack)

События данной категории свидетельствуют об атаках, направленных на поиск и эксплуатацию уязвимостей веб-приложения: sql инъекции, внедрение кода, обход директорий, межсайтовый скриптинг, отказ в доступе и т.д.

Прочая активность (misc-activity)

События данной категории свидетельствуют о таких активностях как: посылка нестандартных HTTP запросов, обф. SMB, аномалии в трафике и т.д.

Обнаружена активность сетевого трояна (trojan-activity)

Правила реагируют на загрузку вредоносного семпла, а также на ответный трафик, генерируемый семплом с зар.

Попытка DDoS-атаки (attempted-dos)

События данной категории свидетельствуют о попытках DDoS-атаки

Активность web-приложения (web-application-activity)

События данной категории свидетельствуют о попытках доступа к потенциально уязвимому web-приложению, w

Потенциально опасный трафик (bad-unknown)

Правила обнаруживают обращения к подозрительным/вредоносным доменным именам, IP адресам. В большинстве случаев «черных списков», используемые злоумышленниками для организации командных центров ботнет содержимым, фишинговых писем, размещения вредоносного контента, проведении всевозможных атак и т.д.

Неудачная попытка использования прав пользователя (unsuccessful-user)

События данной категории свидетельствуют о попытках доступа к ресурсам системы, которые закончились неудачно.

По правилам

Редактор правил - Обнаружение и предотвращение вторжений - Правила режима работы 'Усиленный'

Правило	Действие	Протокол	Адрес источника	Порт источника	Направление	Адрес назначения	Порт назначения
3055560 - AM TROJAN Suspici	❗ Блокировать	TCP	\$HOME_NET	Все	→	\$EXTERNAL_NET	1433
3063112 - AM SCAN RDP brute	❗ Блокировать	TCP	\$EXTERNAL_NET	Все	→	\$HOME_NET	Все
3053736 - AM SCAN SSH brute	❗ Блокировать	TCP	\$HOME_NET	Все	→	\$EXTERNAL_NET	22
3023530 - AM SCAN Possible C	❗ Блокировать	TCP	\$HOME_NET	4786	→	\$EXTERNAL_NET	Все
3023529 - AM SCAN Possible C	❗ Блокировать	TCP	\$EXTERNAL_NET	Все	→	\$HOME_NET	4786
3006441 - AM SCAN Bruteforce	❗ Блокировать	TCP	\$HOME_NET	23	→	\$EXTERNAL_NET	Все
3004674 - AM SCAN Bruteforce	❗ Блокировать	TCP	\$EXTERNAL_NET	Все	→	\$HOME_NET	3306
3004672 - AM SCAN Hydra Bru	❗ Блокировать	TCP	\$EXTERNAL_NET	Все	→	\$HOME_NET	25
2101918 - GPL SCAN SolarWin	❗ Блокировать	ICMP	\$EXTERNAL_NET	Все	→	\$HOME_NET	Все
2101638 - GPL SCAN SSH Versi	❗ Блокировать	TCP	\$EXTERNAL_NET	Все	→	\$HOME_NET	22
2100617 - GPL SCAN ssh-resea	❗ Блокировать	TCP	\$EXTERNAL_NET	Все	→	\$HOME_NET	22
2029577 - ET SCAN Polaris Bot	❗ Блокировать	TCP	\$EXTERNAL_NET	\$HTTP_PORTS	→	\$HOME_NET	Все
2029473 - ET SCAN ELF/Mirai U	❗ Блокировать	TCP	\$EXTERNAL_NET	\$HTTP_PORTS	→	\$HOME_NET	Все
2029318 - ET SCAN Tomato Roi	❗ Блокировать	TCP	\$EXTERNAL_NET	Все	→	\$HOME_NET	\$HTTP_PORTS
2029317 - ET SCAN Tomato Roi	❗ Блокировать	TCP	\$EXTERNAL_NET	Все	→	\$HOME_NET	\$HTTP_PORTS
2100484 - GPL SCAN PING Snif	❗ Блокировать	ICMP	\$EXTERNAL_NET	Все	→	\$HOME_NET	Все
2100483 - GPL SCAN PING Cyb	❗ Блокировать	ICMP	\$EXTERNAL_NET	Все	→	\$HOME_NET	Все
2100476 - GPL SCAN webtrend	❗ Блокировать	ICMP	\$EXTERNAL_NET	Все	→	\$HOME_NET	Все
2100474 - GPL SCAN superscar	❗ Блокировать	ICMP	\$EXTERNAL_NET	Все	→	\$HOME_NET	Все
2100465 - GPL SCAN ISS Pinger	❗ Блокировать	ICMP	\$EXTERNAL_NET	Все	→	\$HOME_NET	Все



Полная блокировка трафика

Блокируется любой входящий и исходящий трафик.



Публичная сеть

Подключение к общественной сети. Максимальная степень защиты, определяемая политикой безопасности.



Частная сеть

Подключение к частной сети. Пользователь может самостоятельно определять сетевые фильтры.



Защищенная сеть

Работа в защищенной сети. Пользователь самостоятельно определяет сетевые фильтры.



Отключен

Personal Firewall полностью отключен и не влияет на сетевой трафик.

Межсетевой экран

- Несколько режимов работы с предустановленными фильтрами от производителя
- Администратор имеет возможность добавлять/изменять/удалять фильтры в режимах работы «Частная» и «Публичная сеть»

ViPNet EndPoint Protection Server Администратор

Назад к редактору

Сетевые фильтры

- Публичная сеть
- Частная сеть
- Защищенная сеть

Справочники

- Протоколы
- Адреса и сети
- Расписания

Редактор правил - Персональный межсетевой экран - Фильтры режима работы 'Публичная сеть'

Поиск по названию фильтра... + Добавить ↑ Добавить в избранное ↑ ↓ 🗑️

Название фильтра	Статус	Действие	Версия IP	Протокол	Источник	Назначение
<input type="checkbox"/> Фильтры политик безопасности						
<input type="checkbox"/> Веб-серфинг	<input checked="" type="checkbox"/>	Разрешить	IP v4	DHCP; DNS; HTTP; HT	Все	Все
<input type="checkbox"/> Почта	<input checked="" type="checkbox"/>	Разрешить	IP v4	IMAP; POP3; SMTP	Все	Все
<input type="checkbox"/> Доступ к частной сети	<input checked="" type="checkbox"/>	Разрешить	IP v4	Все	Мой компьютер	Частная сеть
<input type="checkbox"/> Обращения из частной сети	<input checked="" type="checkbox"/>	Разрешить	IP v4	Все	Частная сеть	Мой компьютер
<input type="checkbox"/> Доступ из корпоративной сети	<input checked="" type="checkbox"/>	Разрешить	IP v4	Все	Корпоративная сеть	Мой компьютер
Фильтры по умолчанию						
<input checked="" type="checkbox"/> Действие по умолчанию	<input type="checkbox"/>	Блокировать	IP v4,v6	Все	Все	Все

Межсетевой экран

Создание фильтров аналогично PFW, но т.к. это делается на сервере, имеется возможность рассылки на группы агентов с модулем персонального межсетевого экранирования

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.

Контроль приложений

Возможность выбора режима работы Черного/Белого списка с полной блокировкой или уведомлением о запуске

Приложения, которым разрешен запуск. Активность определяется правилами доступа к файлам, реестру, процессам.

Найти   [Добавить](#)  | [Добавить в избранное](#) | 

Глобальные 

- >  Слабое доверие
- >  Частичное доверие
- ▼  Доверенные
 -   ?\Windows\WinSxS**
 -  ?\Windows\SysWOW64**
 -  ?\Windows\SystemApps**
 -  ?\Windows\servicing**
 -  ?\Windows\Boot\PCAT**
 -  ?\Windows\ImmersiveControlPanel**
 -  ?\Windows\Microsoft.NET**
 -  ?\Windows\PrintDialog**
 -  ?\Windows\Speech\Common**
 -  ?\Windows\System32**
 -  ?\ProgramData\Microsoft\Windows Defender\Platform**
 -  ?\Program Files\Common Files\microsoft shared**
 -  ?\Program Files\InfoTeCS**
 -  ?\Program Files\internet explorer**
 -  ?\Program Files\PostgreSQL**
 -  ?\Program Files\Windows Defender**
 -  ?\Program Files\Windows Defender Advanced Threat Protection**
 -  ?\Program Files\Windows Mail**

Контроль приложений

Возможность формирования Белых и Черных списков

Выберите приложение или группу приложений для которых вы хотите настроить правила доступа

Найти Добавить |

Глобальные ▾

- > Слабое доверие
- ▼ Частичное доверие
 - cmd.exe
 - powershell.exe
 - WINWORD.EXE
 - EXCELEXE
 - POWERPNT.EXE
 - sysprep.exe
 - msxsl.exe
 - dccw.exe
 - spoolsv.exe
 - splwow64.exe
 - iexplore.exe
 - chrome.exe
 - NetworkLicenseServer.exe
 - AcroRd32.exe
 - ?:\Users**
 - ?:\Windows\Temp**
 - ?:\Windows\Tasks**
- > Доверенные

Правила доступа

Файлы | Реестр | Процессы | Команд

Задайте правила доступа к файлам и
Правила применяются по порядку с

Добавить правило |

N Объекты

1 По умолчанию

Контроль приложений – правила доступа

Возможность создания правил доступа для приложений к следующим объектам:

- Файлам
- Реестру
- Процессам
- Командной строке

AntiMalware

Обнаружение вредоносных файлов

Введите название устройства

Наименование

Все устройства > Главная

DESKTOP-ID9FDVG

Время начала	Время завершения
21.09.2021 18:54:12	21.09.2021 18:54:16
21.09.2021 18:47:53	21.09.2021 18:54:16
21.09.2021 18:41:52	21.09.2021 18:54:16
21.09.2021 18:36:56	21.09.2021 18:54:16
21.09.2021 18:36:32	21.09.2021 18:54:16
21.09.2021 18:36:14	21.09.2021 18:54:16
21.09.2021 18:30:30	21.09.2021 18:54:16
21.09.2021 18:28:46	21.09.2021 18:54:16
21.09.2021 18:27:48	21.09.2021 18:54:16
21.09.2021 18:27:32	21.09.2021 18:54:16

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

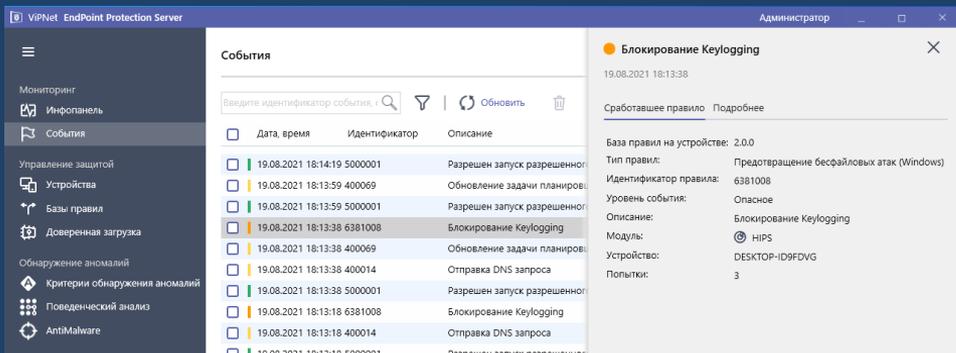
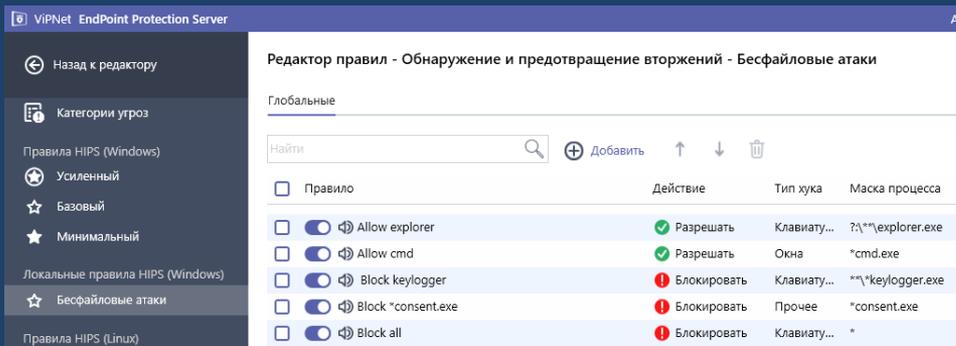
Поиск по путям

Файл (57)

Путь	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\trhhghgTRHTHT...	1,00
★ C:\Program Files\My program\dqkdlIIIOJIOBO...	1,00
★ C:\Program Files\My program\Bad process.exe	1,00

Antimalware движок

- Эвристический подход
- Регулярное обновление в составе БРП



Обнаружение и предотвращение бесфайловых атак

Входит в состав модуля «Обнаружения и предотвращения вторжений»

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, 🔍 | 🔄 Обновить | 🗑️

<input type="checkbox"/>	Дата, время	Идентификатор	Описание
<input type="checkbox"/>	21.09.2021 19:40:30	5000001	Разрешен запуск разрешенной задачи
<input type="checkbox"/>	21.09.2021 19:40:10	5000001	Разрешен запуск разрешенной задачи
<input type="checkbox"/>	21.09.2021 19:39:50	5000001	Разрешен запуск разрешенной задачи
<input type="checkbox"/>	21.09.2021 19:39:29	5000001	Разрешен запуск разрешенной задачи
<input checked="" type="checkbox"/>	21.09.2021 19:39:17	7000006	Аномалия в событии удаления
<input type="checkbox"/>	21.09.2021 19:39:17	7000006	Аномалия в событии удаления
<input type="checkbox"/>	21.09.2021 19:39:17	7000005	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000005	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<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 задачи
<input type="checkbox"/>	21.09.2021 19:38:49	5000001	Разрешен запуск разрешенной задачи
<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/IRETH): 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: Провести корреляцию с другими событиями ИБ.

© 2021, АО "ИнфоТекС" | Версия ПО: 1.5.0.4836

Выявление аномалий

Ожидание по сертификации – Q2 2023



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

Текущая концепция защиты рабочих станций



ViPNet SafeBoot

Доверие к платформе и обеспечение доверенной загрузки ОС



ViPNet SafePoint

Разграничение доступа и защита данных



ViPNet Client 4U

Обеспечение защищённых коммуникаций



ViPNet EndPoint Protection

Защита от внешних атак и угроз



Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363