КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Когда антивирус не справляется.

Как поможет антивирус Dr.Web

Dr.WEB®
с 1992 года

Вячеслав Медведев
ООО «Доктор Веб»

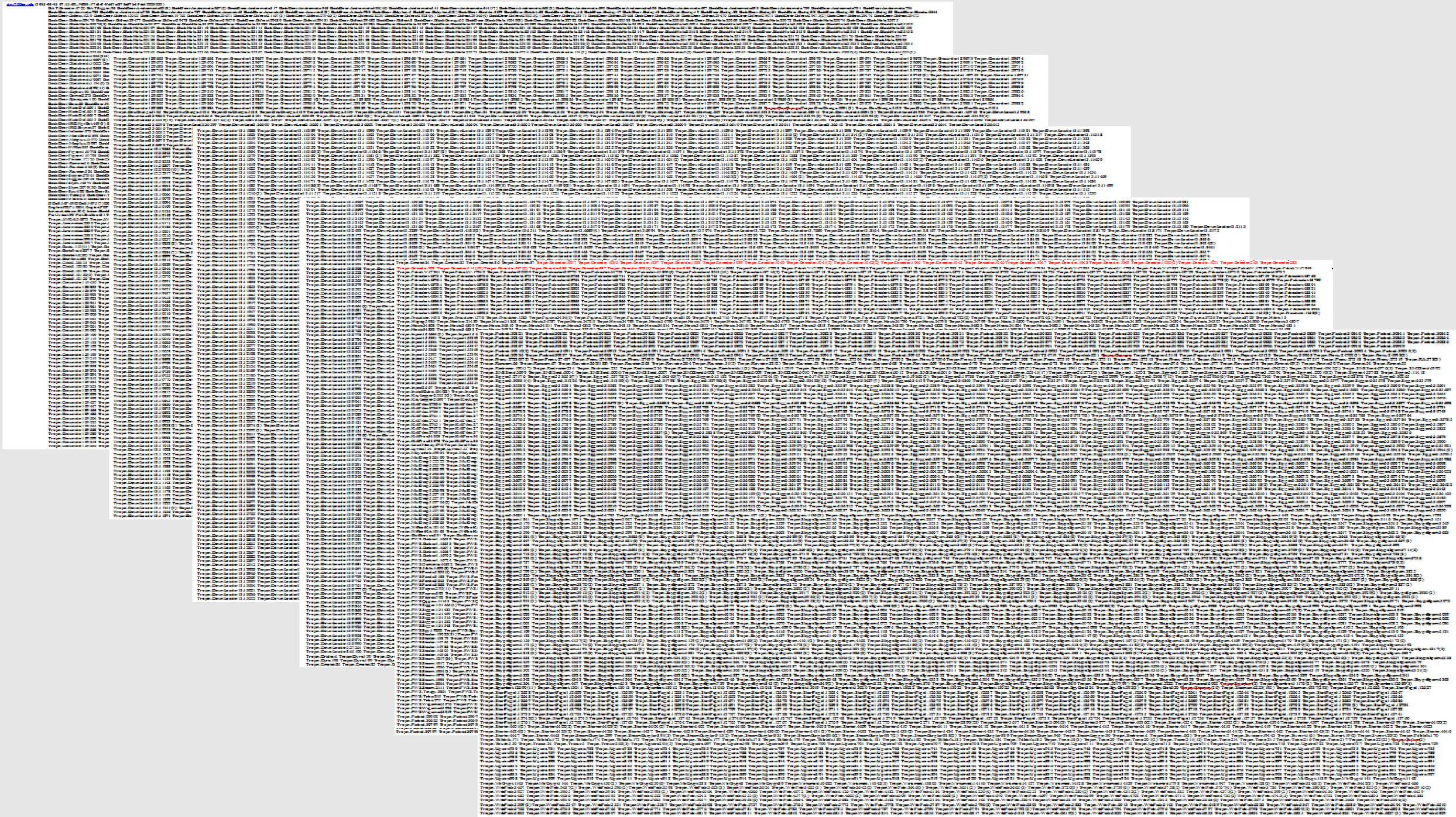
ТЕЛЕФОН: +7 495 789-45-87

EMAIL: v.medvedev@drweb.com

14 ноября 2019
Самара

Dr.WEB®
с 1992 года

суточно на анализ в «Доктор Веб» поступает до миллиона подозрительных образцо



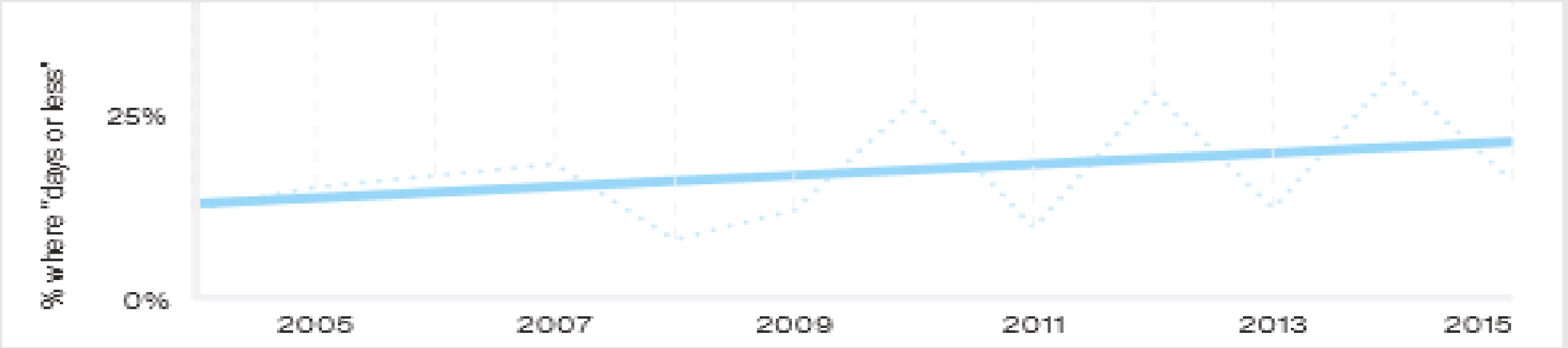
Dr.WEB®
с 1992 года

Вредоносные программы разрабатываются не хакерами-одиночками, но криминальными структурами, что позволяет “выпускать на рынок” вредоносные программы, протестированные на необнаружение антивирусами

Справка. Тесты на обнаружение неизвестных вирусов определяют возможность обнаружения угроз подобных ранее известным и ничего не говорят о возможности решения противостоять угрозе, заточенной на необнаружение конкретным решением

Dr.WEB®
с 1992 года

Менее четверти вредоносных программ становится известными в течении рабочего дня



https://regmedia.co.uk/2016/05/12/dbir_2016.pdf

А ловить надо 100%

Dr.WEB®
с 1992 года

Обновления для обнаружения новейшего ПО поступают всегда после того, как это ПО начинает использоваться в атаках!

А ловить надо 100% и в момент атаки!

Справка. Любой современный антивирус сигнатурно определяет не более 30% водящихся в дикой природе вредоносных программ

http://www.solutionary.com/dms/solutionary/Files/SERT/Solutionary-SERT_Q42012_Research.pdf

Dr.WEB®
с 1992 года

Согласно статистике, в среднем от обнаружения новой вредоносной программы до получения обновления проходит **2 часа**

Можно ли считать антивирусную защиту, основывающуюся только на знаниях, содержащихся в антивирусных базах – актуальной? Очевидно (на самом деле нет), что нет

Dr.WEB®
с 1992 года

Сдаваться? Ни в коем случае!

Dr.WEB®
с 1992 года

Что бы противостоять угрозам сегодня – мало добавлять сигнатуры, увеличивая потребление ресурсов – нужно переходить на новые технологии

Dr.WEB®
с 1992 года

Антивирус обязан:

- ✓ иметь систему самозащиты, не позволяющую неизвестной вредоносной программе нарушить нормальную работу антивируса
- ✓ нормально функционировать до поступления обновления, позволяющего пролечить заражение
- ✓ иметь систему сбора информации, позволяющую максимально быстро передавать в антивирусную лабораторию всю необходимую для решения проблемы информацию

Справка. Тесты на лечение активных заражений проводятся на уже достаточное время известных вирусах. Победа в этих тестах ничего не говорит о возможности антивируса сопротивляться неизвестным вредоносным программам

Dr.WEB®
с 1992 года

Антивирус обязан:

- ✓ Работать без необходимости использования сторонних компонентов
- ✓ Уметь лечить активные заражения
- ✓ Иметь все необходимые сертификаты

Dr.WEB®
с 1992 года

Мы – можем!

Dr.Web:

- ✓ Возможность установки на любую платформу
- ✓ Низкие системные требования
- ✓ Отличная самозащита
- ✓ Технологии, позволяющие лечить любую заразу

Dr.WEB®
с 1992 года

Почему Dr.Web?

Технология Fly-Code — позволяет обнаружить вирусы, упакованные даже неизвестными антивирусному ПО Dr.Web упаковщиками.

Создание неизвестных антивирусу Dr.Web вредоносных программ – не простая задача!

Dr.WEB®
с 1992 года

Почему Dr.Web?

Dr.Web HyperVisor:

- ✓ Существенно улучшил систему обнаружения и лечения угроз, а также усилил самозащиту Dr.Web путем использования возможностей современных процессоров.
- ✓ Позволил разработчикам Dr.Web преодолеть ограничения, накладываемые на антивирусы особенностями 64-битных операционных систем, вынуждавших антивирус функционировать на том же уровне, что и вредоносные программы.

Компонент запускается и работает **на минимально возможном уровне операционной системы**, что обеспечивает контроль всех программ, процессов и работы самой ОС, а также невозможность перехвата вредоносными программами контроля над защищаемой Dr.Web системой.

Dr.WEB®
с 1992 года

Почему Dr.Web?

Dr.Web ShellGuard – следующее поколение Dr.Web Process Heuristic не просто не позволяет вредоносным объектам внедриться в процессы других программ, а контролирует процессы изнутри

Dr.WEB®
с 1992 года

Почему Dr.Web?

ScriptHeuristic:

- ✓ предотвращает исполнение любых вредоносных скриптов в браузере и PDF-документах, не нарушая при этом функциональности легитимных скриптов
- ✓ Защищает от любых вредоносных скриптов в HTML и PDF-документах
- ✓ Защищает компьютер от заражения неизвестными вирусами через веб-браузер
- ✓ Работает независимо от состояния вирусной базы Dr.Web
- ✓ Работает с любыми веб-браузероми

Dr.WEB®
с 1992 года

Антивирус это не только антивирусные базы

#CODEIB

Защита от известных угроз

Защита от неизвестных угроз

БАЗА СИГНАТУР

Одна запись — защита от сотен и тысяч вирусов, даже от тех, которые, возможно, будут созданы злоумышленниками

УЛУЧШЕНО!

НЕСИГНАТУРНЫЕ ТЕХНОЛОГИИ

- Эвристический анализатор — с 1994 года!
- Технология Origins Tracing
- Модуль эмуляции исполнения
- Технология Fly-Code
- Комплексный анализатор упакованных угроз
- Технология Script Heuristic
- Технология анализа структурной энтропии
- и много других технологий

НОВОЕ!

ТЕХНОЛОГИИ ДЕТЕКТИРОВАНИЯ ВПО С ПОМОЩЬЮ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

УЛУЧШЕНО!

ТЕХНОЛОГИИ ПРЕВЕНТИВНОЙ ЗАЩИТЫ

- Защита от новейших неизвестных вирусной базе вредоносных программ
- Анализ «на лету» поведения программ и немедленное завершение вредоносных процессов
- Защита до момента полной загрузки ОС
- Автономная работа без Интернета

Защита от известных угроз

Защита от неизвестных угроз

Защита от неизвестных угроз

Защита от известных угроз

Защита от неизвестных угроз

Защита от неизвестных угроз

Защита от неизвестных угроз

Защита от не

Dr.WEB®
с 1992 года

Несигнатурные методы детектирования неизвестных угроз Dr.Web Enterprise Security Suite

- ✓ Возможность обнаружения угроз без постоянного обращения к вирусным базам – что положительно сказывается как на быстродействии, так и качестве обнаружения новейших угроз
- ✓ Обнаружение угроз до фактического исполнения их кода
- ✓ Обнаружение популярных в данных момент действий злоумышленников - использование вредоносных майнеров, загрузчиков вредоносного ПО - как активных, так и предназначенных к запуску во всех областях системы

Dr.WEB®
с 1992 года

Для защиты от угроз неизвестных антивирусному ядру нужно использовать:

- ✓ Ограничение доступа к заведомо вредоносным ресурсам
- ✓ Ограничение прав пользователя
- ✓ Контроль запускаемых программ

Dr.WEB®
с 1992 года

В Dr.Web Enterprise Security Suite 12.0 вошел новый компонент **Контроль приложений**.

Компонент осуществляет мониторинг активности всех процессов на защищаемых станциях, позволяет системному администратору разрешать или запрещать запуск приложений на станциях антивирусной сети.

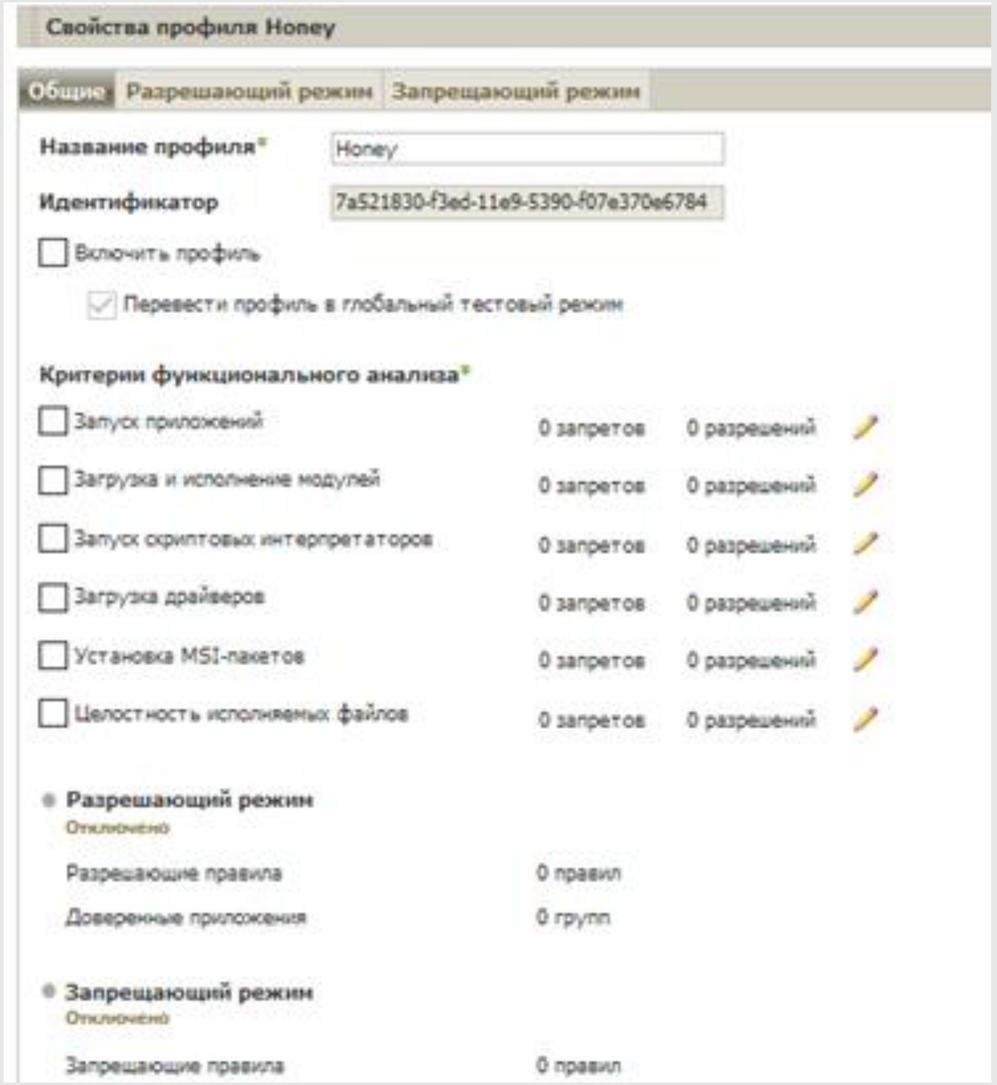
Dr.WEB®
с 1992 года

Контроль приложений Dr.Web Enterprise Suite например позволяет сф

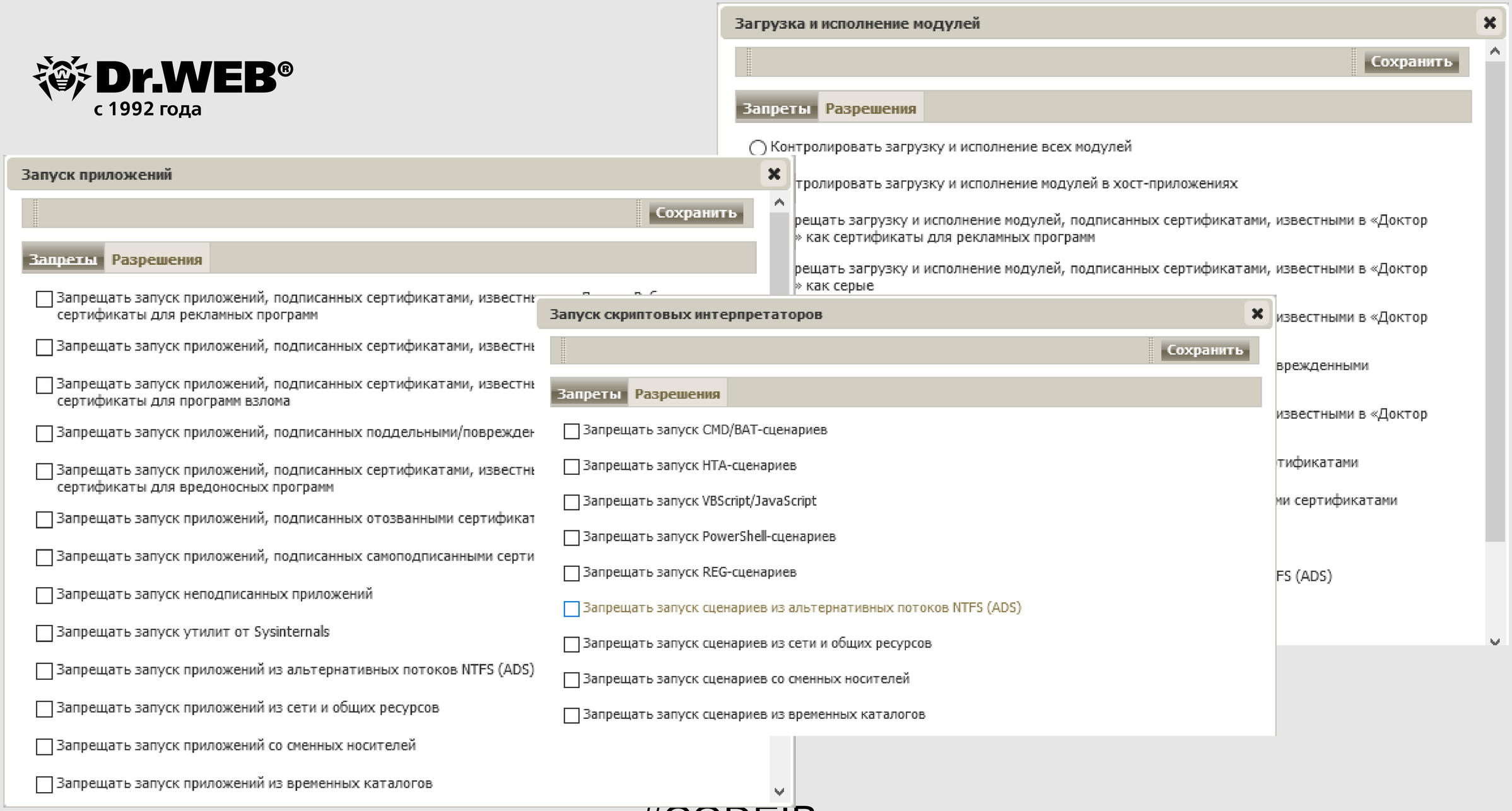
Dr.WEB®
с 1992 года

6 групп функционального анализа:

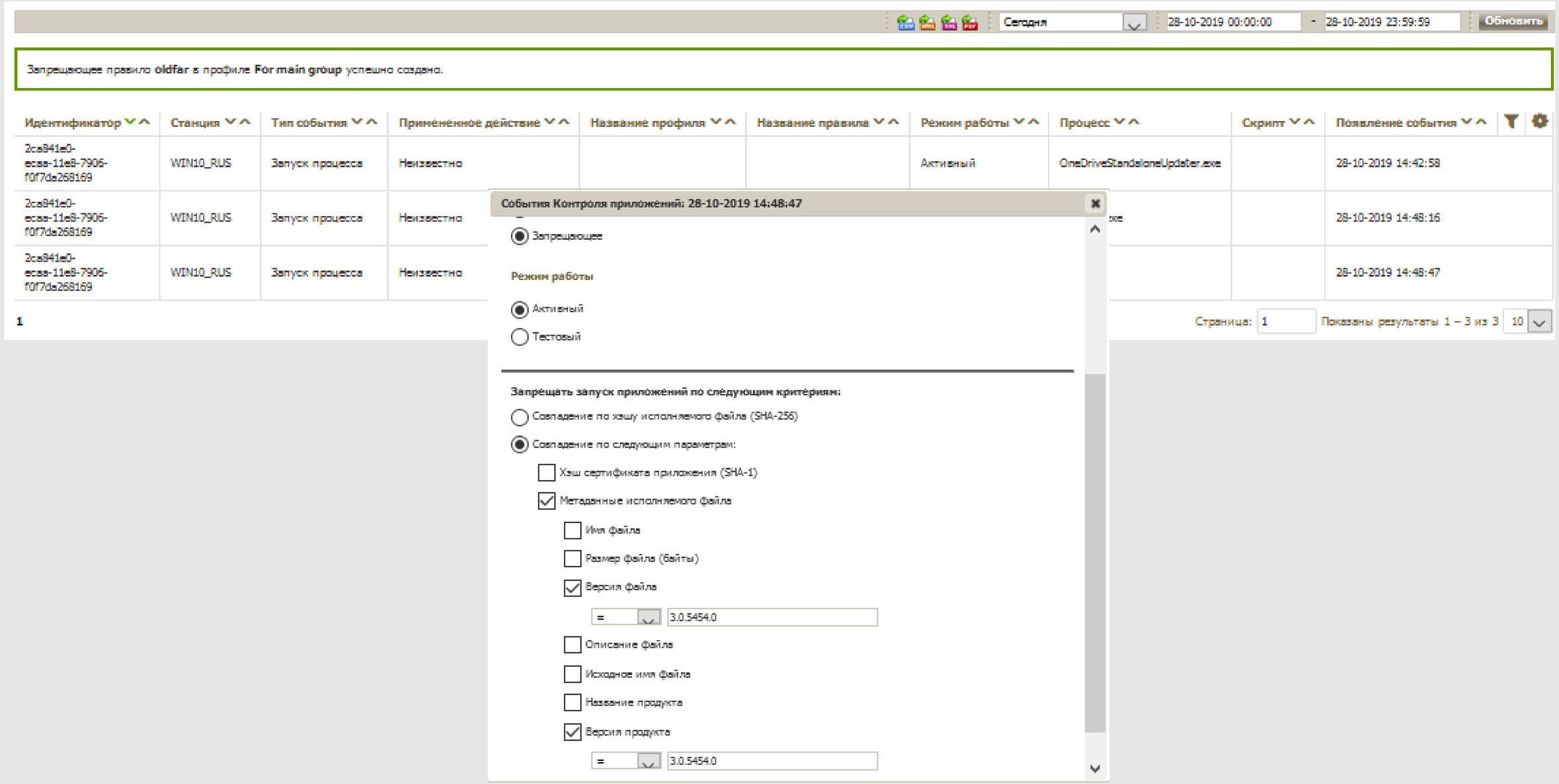
- ✓Запуск приложений
- ✓Загрузка и исполнение модулей
- ✓Запуск скриптовых интерпретаторов
- ✓Загрузка драйверов
- ✓Установка MSI-пакетов
- ✓Целостность исполняемых файлов



Dr.WEB®
с 1992 года



#CODEIB


Сегодня
28-10-2019 00:00:00
28-10-2019 23:59:59
Обновить
Запрещающее правило oldfar в профиле For main group успешно создано.
Идентификатор
Станция
Тип события
Применённое действие
Название профиля
Название правила
Режим работы
Процесс
Скрипт
Появление события
2ca841e0-ecaa-11e8-7906-f0f7da268169
WIN10_RUS
Запуск процесса
Неизвестно
Активный
OneDriveStandaloneUpdater.exe
28-10-2019 14:42:58
28-10-2019 14:48:16
28-10-2019 14:48:47
1
Страница: 1
Показаны результаты 1 – 3 из 3
10
События Контроля приложений: 28-10-2019 14:48:47
Запрещающее
Режим работы
Активный
Тестовый
Запрещать запуск приложений по следующим критериям:
Совпадение по хэшу исполняемого файла (SHA-256)
Совпадение по следующим параметрам:
Хэш сертификата приложения (SHA-1)
Метаданные исполняемого файла
Имя файла
Размер файла (байты)
Версия файла
=
3.0.5454.0
Описание файла
Исходное имя файла
Название продукта
Версия продукта
=
3.0.5454.0

#CODEIB

Dr.WEB®
с 1992 года

И просто вопрос

Что проще – купить, настроить и спать спокойно или заплатить?

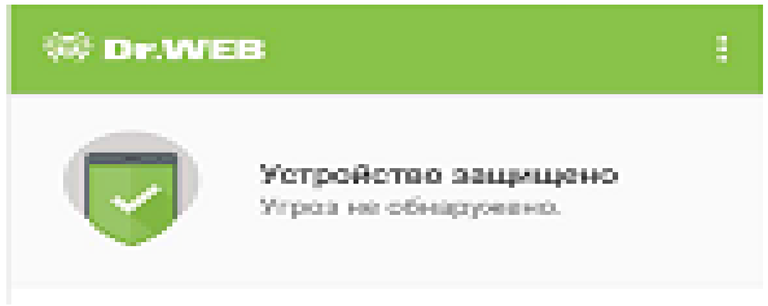
Dr.WEB®
с 1992 года

Лишь в 30% случаев компании получают код для разблокировки

http://www.cnews.ru/articles/2017-05-11_kiberbezopasnost_kak_strategiya_zashchity_biznesaanaliz_ugroz

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Благодарим за внимание!



Номер службы технической поддержки

8-800-333-7932

Запомнить просто! –
возникла проблема – набери DRWEB!

8-800-33-DRWEB

Убедитесь, что на ваших компьютерах нет вирусов

Dr.WEB®
с 1992 года

#CODEIB