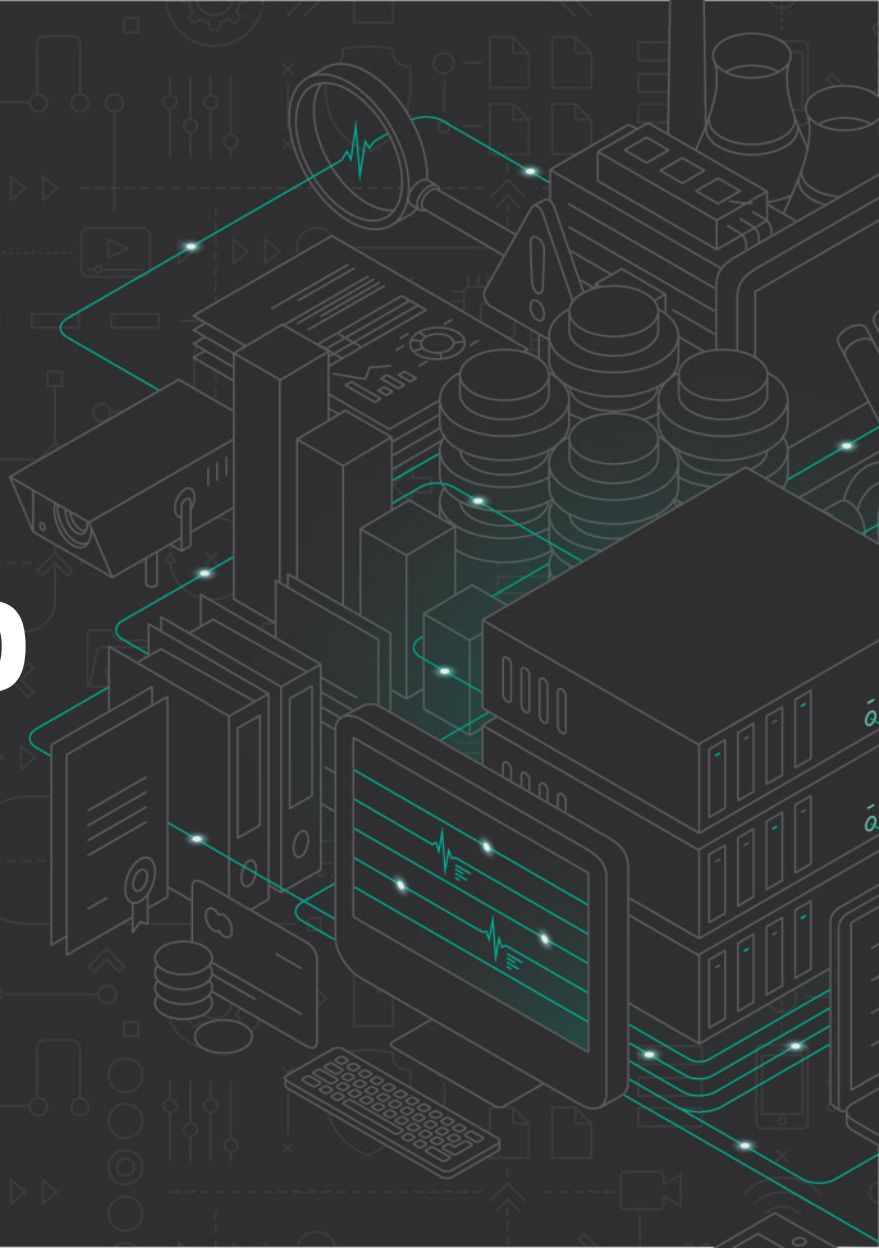
ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

# ГАРДА МОНИТОР

## ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ АНАЛИЗА И РАССЛЕДОВАНИЯ СЕТЕВЫХ ИНЦИДЕНТОВ



# ПРОЦЕСС РЕАГИРОВАНИЯ НА ИНЦЕДЕНТ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

## ФАЗЫ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ *

* В соответствии с руководством по обработке инцидентов компьютерной безопасности NIST SP 800-61 R2


## КОНТРОЛЬ И АНАЛИЗ ТРАФИКА

Мониторинг IP-трафика локальных сетей и выявление сетевых инцидентов безопасности

Поведенческая аналитика: построение профилей сетевой работы устройств, выявление аномалий в поведении и существенных отклонений от «типового» поведения

Ведение архива объектов информационного обмена для ретроспективного анализа событий

Анализ информационных потоков по протоколам удаленного управления, туннелирования, онлайн-игр и др.

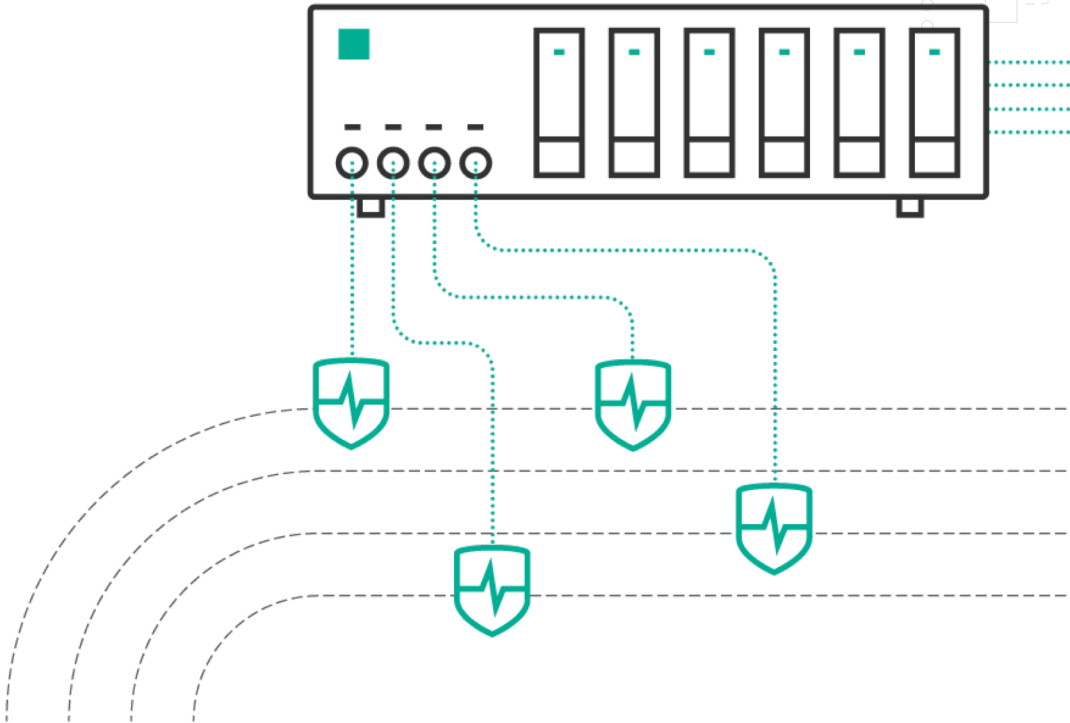
# КОСВЕННЫЕ ПРИЗНАКИ ИНЦИДЕНТОВ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

## ЛЮБАЯ АКТИВНОСТЬ ЗЛОУМЫШЛЕННИКА ОСТАВЛЯЕТ СЛЕДЫ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ:

- Появление протоколов удаленного подключения
- Появление VPN каналов
- Нестандартные DNS-запросы хоста
- Протоколы аутентификации
- Другие следы сетевого взаимодействия



## ИЗБЕЖАТЬ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ НЕВОЗМОЖНО

Косвенные признаки помогут выявить инцидент, даже когда он остался незамеченным другими системами

# ЗАДАЧИ, ТРЕБУЮЩИЕ РЕШЕНИЯ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

**«ГАРДА МОНИТОР» ОБЕСПЕЧИТ СБОР ВСЕХ ДАННЫХ ИЗ ЛЮБОЙ ТОЧКИ СЕТИ И КАЖДОГО ЕЁ СЕГМЕНТА — ДЛЯ ЭФФЕКТИВНОГО АНАЛИЗА СОБЫТИЙ СЕТЕВОЙ БЕЗОПАСНОСТИ**

Полный контроль сетевого трафика

Выявление аномалий и инцидентов безопасности

Расследование инцидентов

Обеспечение прозрачности сетевой инфраструктуры

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

# ИЗВЕСТНЫЕ ПРОБЛЕМЫ ПРИ АНАЛИЗЕ РАБОТЫ СЕТИ

## БОЛЬШОЕ КОЛИЧЕСТВО ПОТОКОВ

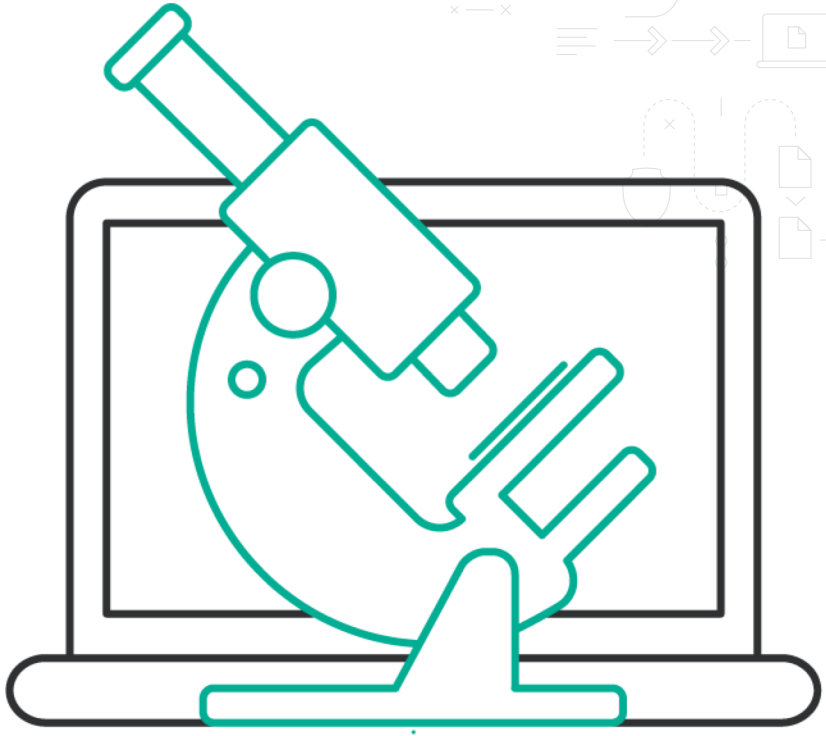
Большое количество сетевых устройств и как следствие объем данных для анализа

## НЕЗАЩИЩЁННЫЕ ЛОГИ

Возможность изменения этих логов администратором системы.

## СЛОЖНОСТЬ АНАЛИЗА

Работа с данными требует хороших знаний и много времени



# ПОЛНЫЙ КОНТРОЛЬ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

ГАРДА МОНИТОР ГАРДА ТЕХНОЛОГИИ

## ГАРДА МОНИТОР СОЗДАНА ДЛЯ ЭФФЕКТИВНОГО АНАЛИЗА СОБЫТИЙ СЕТЕВОЙ БЕЗОПАСНОСТИ

### ЗАПИСЬ ВСЕХ ДАННЫХ L2-L7 УРОВНЯ В ХРАНИЛИЩЕ

Запись всего трафика предприятия, внутренней локальной сети и Интернет-трафика, а также повторное воспроизведение любого потока данных

### КЛАССИФИКАЦИЯ ПАКЕТОВ И ПОТОКОВ ДАННЫХ

Классификация трафика по протоколам, определение географического положения источника и получателя данных, запись всех метаданных

### ВЫЯВЛЕНИЕ АНОМАЛИЙ

Оповещение о выявленных аномалиях в режиме реального времени, таких как: всплески или падение сетевой активности, использование нестандартных портов, протоколов, приложений

# КОМПОНЕНТЫ СИСТЕМЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

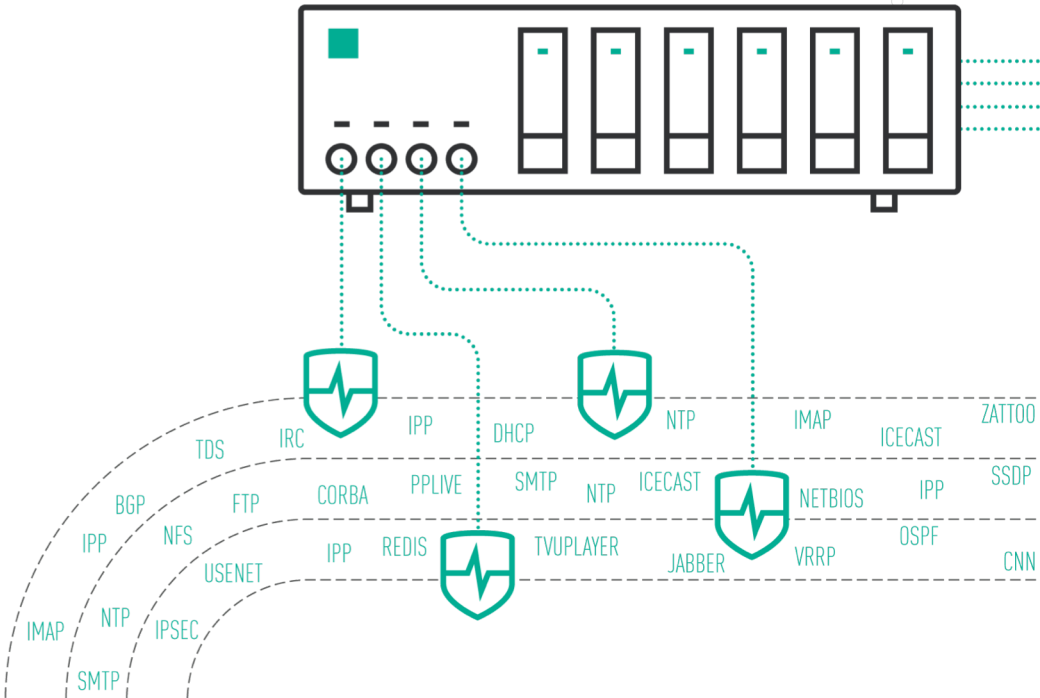
## 1 СБОР ДАННЫХ

2

Система непрерывно собирает
и анализирует трафик в реальном времени.

В случае распределённых схем внедрения,
все данные доступны в едином центре управления

- ☑ Возможность построения геораспределенного кластера
- ☑ Работа с большими списками в режиме реального времени
- ☑ Гибкое внедрение: Netflow и копия трафика



# КОМПОНЕНТЫ СИСТЕМЫ

ГАРДА МОНИТОР

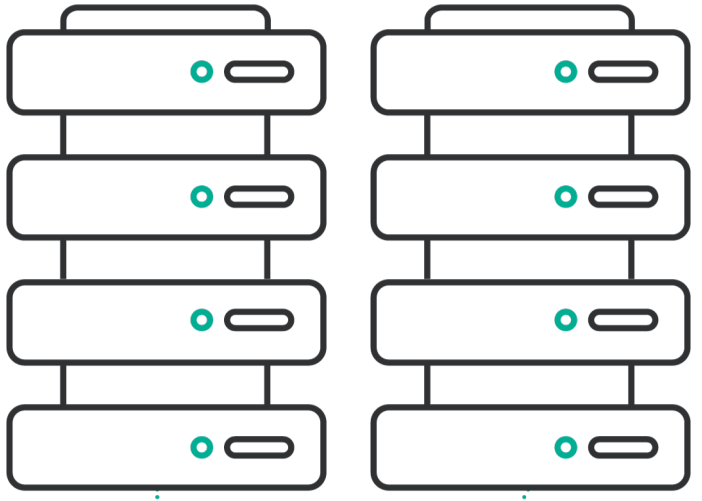
ГАРДА ТЕХНОЛОГИИ

## 2 ХРАНЕНИЕ ВСЕХ ДАННЫХ

1 ⟵ 3

Нереляционное хранилище с быстрым доступом к данным, не требующее дорогостоящего оборудования и дополнительных лицензий, является собственной разработкой компании «Гарда Технологии» класса DataWarehouse. Циклическая перезапись с сохранением инцидентов.

- [x] Гибкие настройки параметров записи



# КОМПОНЕНТЫ СИСТЕМЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

## 3 АНАЛИТИКА И УПРАВЛЕНИЕ

2

- Анализ трафика на соответствие правилам
- Выявление подозрительных событий и инцидентов
- Перехваченные объекты отображаются в удобном для чтения виде
- Разнообразные виды предустановленных отчетов

Решение класса DPI
**DEEP PACKET INSPECTION**

Технологии EBA
**ENTITY BEHAVIOR ANALYTICS**

Network Forensics
Network Monitoring

Персонификация трафика
**IDENTITY TRACKING**

# ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

## #1 ВЫЯВЛЕНИЕ ДЕЙСТВИЙ ВРЕДОНОСНОГО ПО:

- Аномально большое количество почтовых сообщений с компьютера (Спам-бот)
- Аномально большое количество DNS-запросов с компьютера (Троян или ботнет)
- Выявление потоков по IP-адресам из базы данных «плохих» адресов

## #2 ВЫЯВЛЕНИЕ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЕЙ:

- Детектирование фактов использования ПО на рабочих местах: обращения к облачным хранилищам, онлайн-игры
- Детектирование использования пользователями сетей DarkNet (Tor, I2P)
- Выявление подозрительных сервисов (Неопознанные СУБД, веб-сервера внутри сети)

# ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

**Важной особенностью** АПК «Гарда Монитор» является то, что данные о сетевых потоках хранятся отдельно от устройств, их генерирующих.

Это позволяет **исключить возможность вмешательства** пользователей для удаления или подделки данных.

## #3 ВЫЯВЛЕНИЕ ПОДОЗРИТЕЛЬНОГО ВЗАИМОДЕЙСТВИЯ С ВНЕШНИМИ СЕТЯМИ:

- Детектирование попыток удаленного доступа из внешних сетей к внутренним серверам из других стран
- Выявление VPN-каналов до адресов других стран

## #4 ЛОГИРОВАНИЕ ПОТОКОВ ПО ВРЕМЕНИ:

«Гарда Монитор» не только позволяет выявлять данные потоки, но также записывает их содержимое с привязкой ко времени.

**Это позволяет:**

- Выгрузить данные для дальнейшего детального анализа
- Использовать эти потоки как доказательства в расследовании и суде.

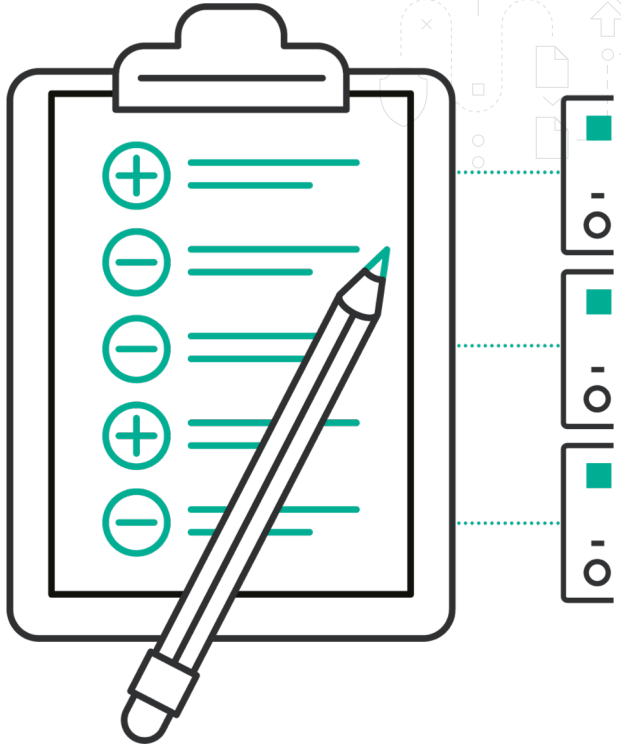
# ПОЛИТИКИ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

## БОЛЬШОЙ СПИСОК ПРЕДУСТАНОВЛЕННЫХ ПОНЯТНЫХ И ПОЛЕЗНЫХ ПОЛИТИК

- Обращение к скомпрометированному IP-адресу и с него
- Обращение к скомпрометированному Host'y/URL'y
- Попытка DNS-резолва скомпрометированного Host'a
- Использование TOR, VPN
- Использование ПО для удаленного доступа
- «Нерабочий» трафик (Игры, мобильные store)
- Рекомендации FinCERT
- Факты «Сетевой разведки»



# АНАЛИТИКА И ПОИСК

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

## АНАЛИТИЧЕСКИЕ ВОЗМОЖНОСТИ

### ИНСТРУМЕНТЫ НАСТРАИВАЕМЫХ ПАНЕЛЕЙ ОТЧЁТОВ

Набор инструментов экспертного анализа связей (Визуализация, инфографика, операции над графами и пр.)

### ENTITY BEHAVIOR ANALYTICS (EBA)

Построение профилей сетевой работы устройств, выявление аномалий в поведении и существенных отклонений от «типового» поведения.

## ПРИМЕРЫ КРИТЕРИЕВ ПОИСКА

- По MAC-адресам источника и получателя
- По IP-адресам источника и получателя
- По портам источника и получателя
- По учетным записям источника и получателя
- По доменным именам источника и получателя
- По версии протокола IP
- По типу протокола транспортного уровня
- По типу прикладного протокола
- По стране источника и получателя
- По размеру передаваемых данных

# СИГНАТУРНЫЙ АНАЛИЗ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

## ОБНОВЛЕНИЕ

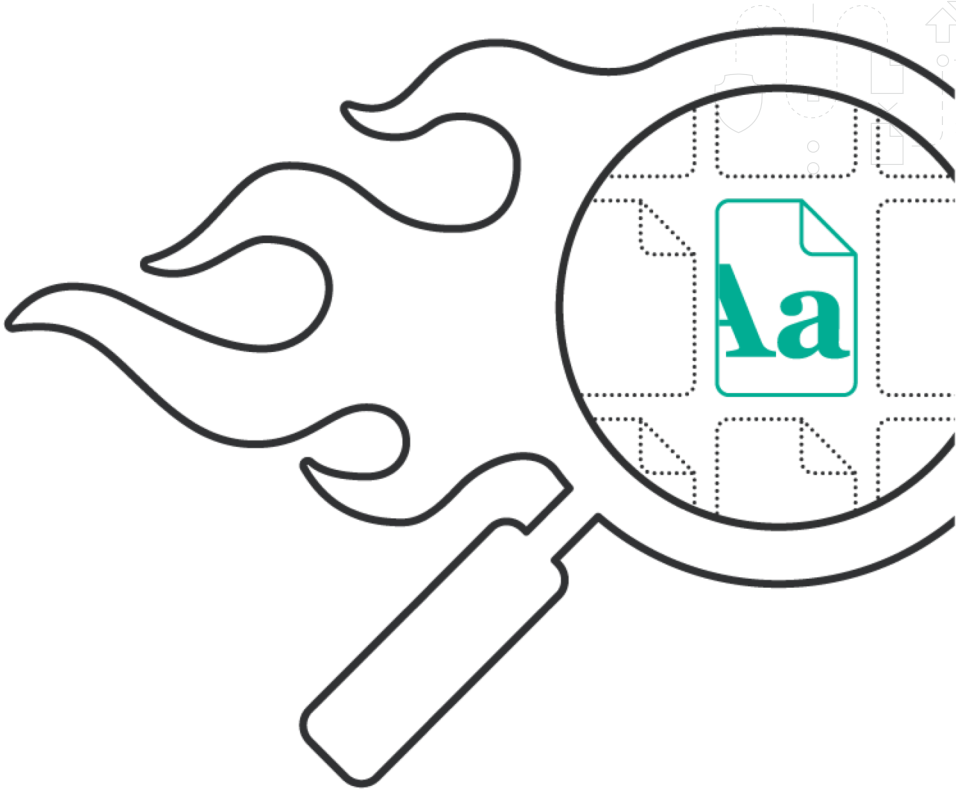
Автоматическое обновление баз сигнатур и правил.

## ИНТЕРФЕЙС УПРАВЛЕНИЯ

Применение сигнатур и правил на всю инфраструктуру системы через единый интерфейс управления.

## БАЗЫ СИГНАТУР

При установке система уже содержит подключенные и обновляемые базы сигнатур.



# КОНСТРУКТОР ОТЧЁТОВ

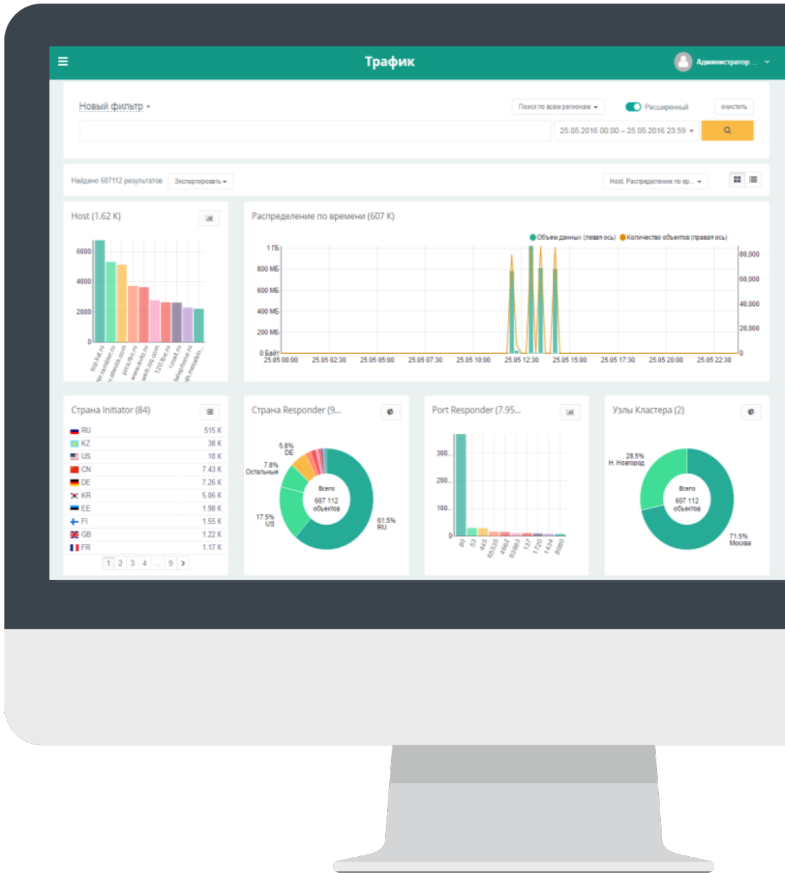
ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

**ДЛЯ ЛЕГКОГО ВЕРХНЕУРОВНЕВОГО АНАЛИЗА СЕТЕВОЙ АКТИВНОСТИ РАЗНООБРАЗНЫЕ ОТЧЁТЫ СТРОЯТСЯ В РЕАЛЬНОМ ВРЕМЕНИ**

## ДОСТУПНЫЕ ВИДЫ ОТЧЁТНОСТИ:

- Графические статистические отчёты
- Предустановленные шаблоны отчётов
- Построение отчётов по отобранным данным и временным рамкам



# ИНТЕГРАЦИЯ И ЭКСПОРТ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

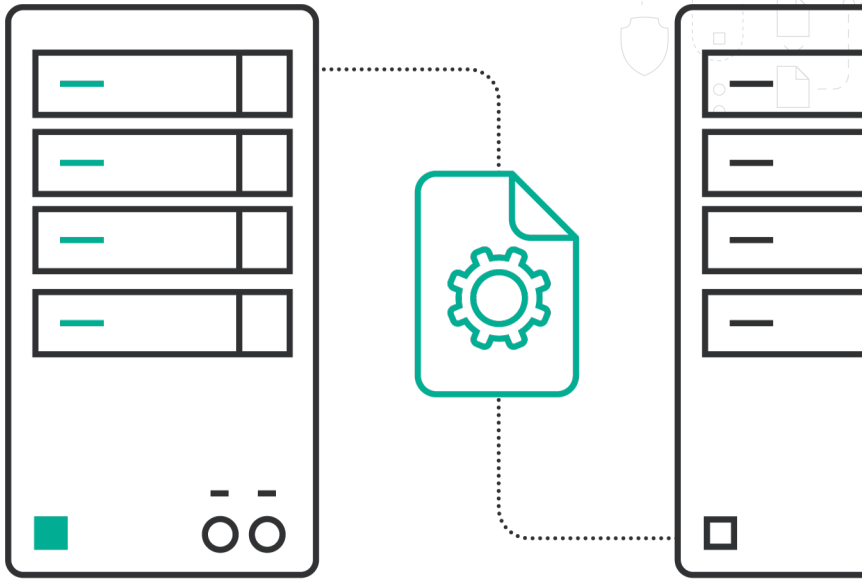
**ДЛЯ ИНТЕГРАЦИИ С SIEM-СИСТЕМАМИ И МЕЖДУНАРОДНЫМИ БАЗАМИ ИНФОРМАЦИИ ПРЕДУСМОТРЕНА ВОЗМОЖНОСТЬ ЭКСПОРТА И ИМПОРТА ИНФОРМАЦИИ В РАЗЛИЧНЫХ ВИДАХ**

## ДОСТУПНЫЕ ФОРМЫ

- CSV
- XML
- PDF
- SysLog
- Электронная почта

## МИРОВЫЕ БАЗЫ

- Базы репутации IP-адресов
- Базы скомпрометированных сайтов
- Базы скомпрометированных e-mail адресов (Спам, фишинг)



# СПАСИБО
# ЗА ВНИМАНИЕ!

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

info@gardatech.ru
8 (831) 422 12 21
**gardatech.ru**