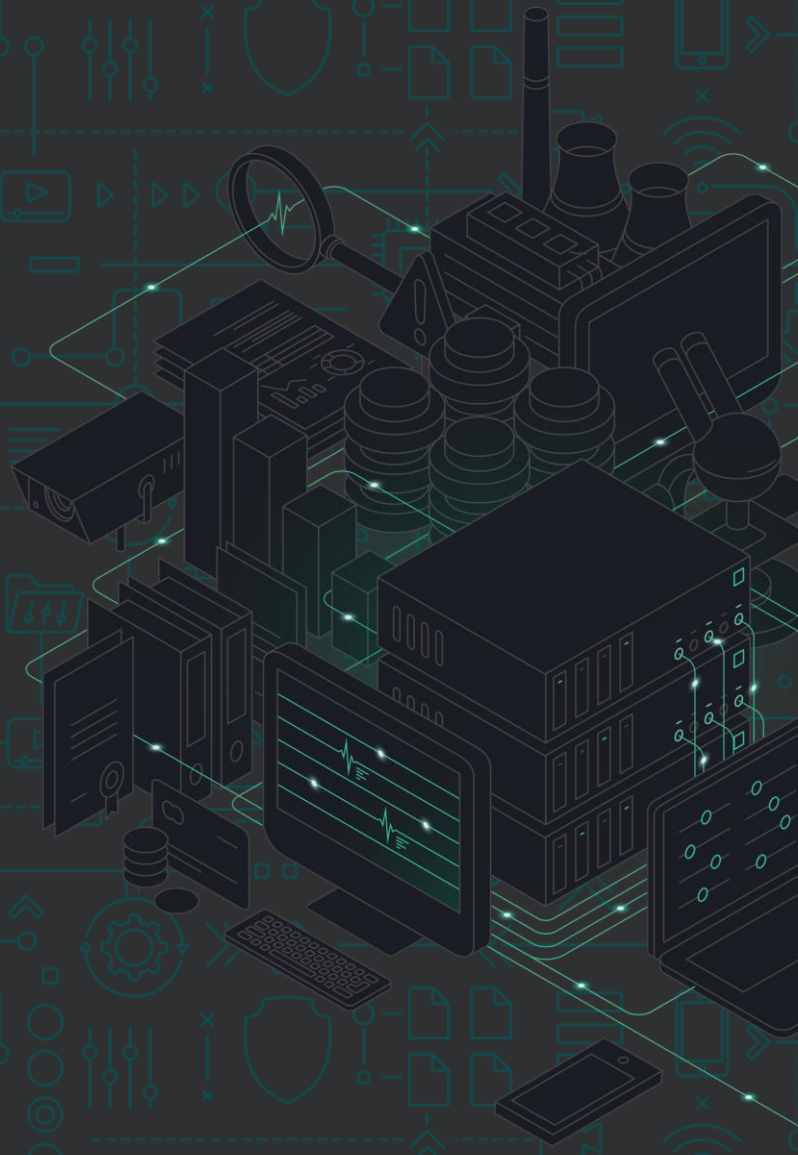
ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ГАРДА МОНИТОР

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ АНАЛИЗА И РАССЛЕДОВАНИЯ СЕТЕВЫХ ИНЦИДЕНТОВ



ПРОЦЕСС РЕАГИРОВАНИЯ НА ИНЦЕДЕНТ

ФАЗЫ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ *

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

КОНТРОЛЬ И АНАЛИЗ ТРАФИКА

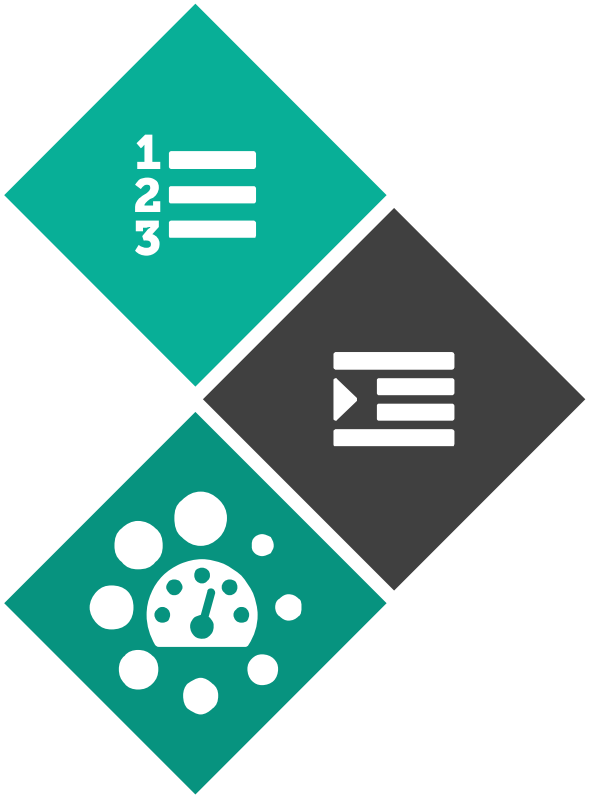
Мониторинг IP-трафика локальных сетей и выявление сетевых инцидентов безопасности

Ведение архива объектов информационного обмена для ретроспективного анализа событий

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

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

ИЗВЕСТНЫЕ ПРОБЛЕМЫ ПРИ АНАЛИЗЕ РАБОТЫ СЕТИ



БОЛЬШОЕ КОЛИЧЕСТВО ПОТОКОВ

Анализ логов каждой системы занимает
много времени

НЕЗАЩИЩЁННЫЕ ЛОГИ

Возможность изменения этих логов администратором системы.

ПИК НАГРУЗКИ ПРИ АУДИТЕ

Аудит сетевой активности на системах и устройствах
создаёт дополнительную нагрузку на них.

ПОЛНЫЙ КОНТРОЛЬ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ГАРДА МОНИТОР СОЗДАНА ДЛЯ ЭФФЕКТИВНОГО АНАЛИЗА СЕТЕВОЙ АКТИВНОСТИ

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

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)
- Анализ трафика по сигнатурам

#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

#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

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.

#4 Предоставление образцов трафика:

«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.

АНАЛИТИКА & БЫСТРЫЙ ПОИСК ПО ПЕРЕХВАЧЕННЫМ ДАННЫМ

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

СПАСИБО
ЗА ВНИМАНИЕ!

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

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