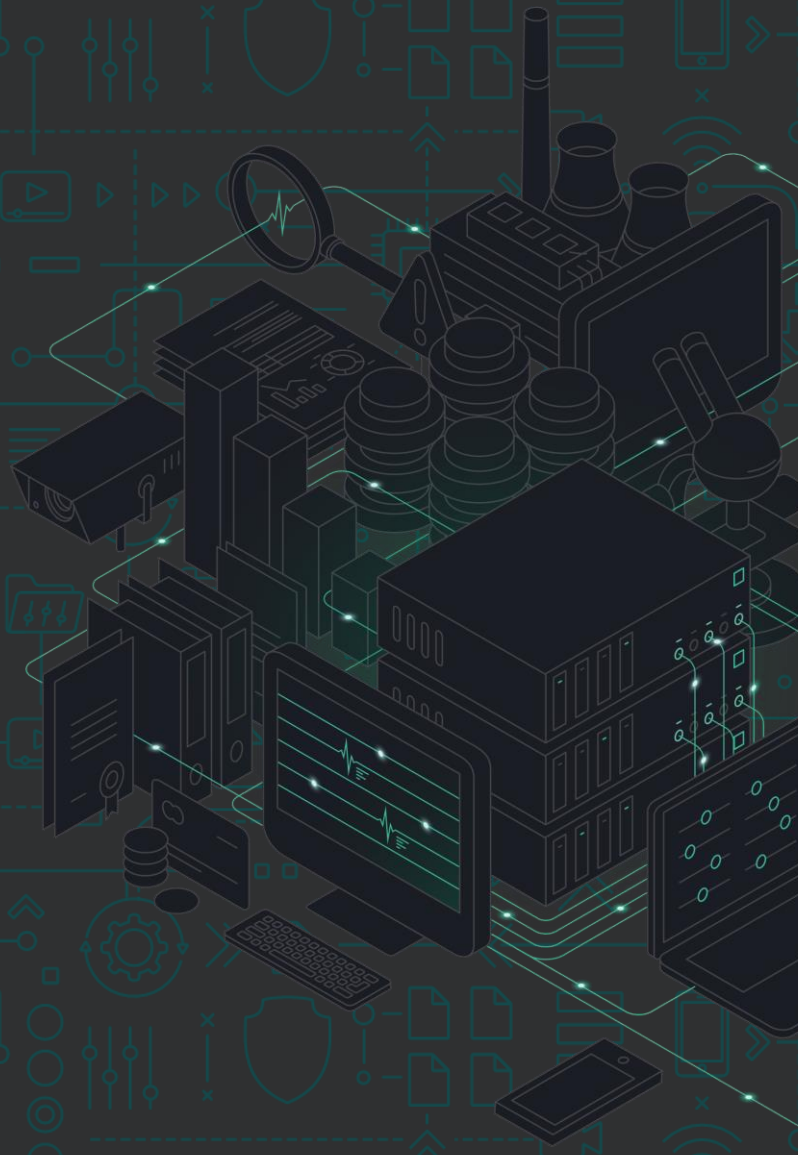
ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ГАРДА МОНИТОР

ВЫЯВЛЕНИЕ УГРОЗ И РАССЛЕДОВАНИЯ СЕТЕВЫХ ИНЦИДЕНТОВ



КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

«ГАРДА МОНИТОР» - СИСТЕМА ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ И РАССЛЕДОВАНИЯ СЕТЕВЫХ ИНЦИДЕНТОВ, АНАЛИЗА ТРАФИКА, ОБНАРУЖЕНИЯ АТАК НА ПЕРИМЕТРЕ И ВНУТРИ СЕТИ.

Выявляет признаки вредоносного ПО в сетевом трафике

Осуществляет мониторинг и сбор данных о сетевой активности

Выявляет атаки на периметре и внутри сети

Обеспечивает **тотальную запись** сетевых потоков

Анализирует события сетевой безопасности

Позволяет выполнять **расследования** сетевых инцидентов

УВЕЛИЧЕНИЕ ЭФФЕКТИВНОСТИ СЛУЖБ ИБ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

«ГАРДА МОНИТОР» ПОВЫШАЕТ ЭФФЕКТИВНОСТЬ РАБОТЫ ЦЕНТРОВ МОНИТОРИНГА (SOC), ХОЛДИНГОВЫХ СТРУКТУР, ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ КОМПАНИЙ И ДРУГИХ СЕКТОРОВ БИЗНЕСА:

- Промышленные и производственные предприятия
- Государственный сектор
- IT-компании
- Финансовые и инвестиционные компании
- Телеком
- И другие

ИНСТРУМЕНТ ДЛЯ ЕЖЕДНЕВНОЙ РАБОТЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

«ГАРДА МОНИТОР» ПОЗВОЛЯЕТ:

- Навести порядок в сети компании
- Обнаружить аномалии и потенциально уязвимые места сети
- Анализировать сетевые события
- Оценить – что предшествовало инциденту и каковы последствия
- Проверить корректность настройки IT-оборудования
- Выявить нецелевое использование ресурсов
- Обеспечить тотальный контроль сети

ПОМОГАЕТ ДИРЕКТОРУ ПО ИБ:

- Обнаружить попытки взлома критических бизнес-ресурсов и нелегитимного доступа к конфиденциальным данным
- Получить оперативную сводку по угрозам безопасности, в т.ч. сведения о попытках атак на инфраструктуру
- Увидеть подробную статистику по нарушениям политик безопасности в компании

ПОМОГАЕТ ОФИЦЕРУ ИБ:

- Выявлять и детектировать вредоносную активность и сетевые атаки
- Инвентаризировать используемые устаревшие и уязвимые протоколы
- Выявлять использование нелегального шифрования, нелегального удаленного доступа (прокси, TOR, VPN и др.)

ПОМОГАЕТ АНАЛИТИКУ SOC:

- Проводить подробное расследование инцидентов
- Собирать артефакты попыток совершения атаки
- Обнаруживать следов злонамеренного сканирования портов, служб и сервисов
- Выявить присутствие хакеров внутри корпоративной инфраструктуры

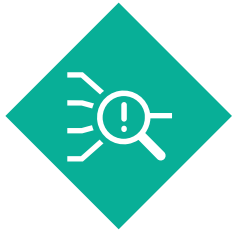
ПОМОГАЕТ РУКОВОДИТЕЛЮ ПО ИТ:

- Собирать статистику используемых протоколов и сетевых служб
- Повышать прозрачность сетевых потоков компании
- Выявить «всплески» и «провалы» в сетевой активности
- Выявить нецелевое использование корпоративных ресурсов

КЛАССИФИКАЦИЯ СИСТЕМЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ



АНАЛИЗ СЕТЕВОГО ТРАФИКА NETWORC TRAFFIC ANALYSIS (NTA)

Анализ трафика на основе глубокого разбора содержимого сетевых пакетов (DPI) для выделения свойств сетевых соединений и определения прикладных протоколов

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ INTRUSION DETECTION DYSTEM (IDS)

Выявление сетевых атак, попыток эксплуатации уязвимостей и работы вредоносного ПО (вирусы, трояны и т.д.) на основе сигнатурного анализа.

Детектирование фактов обращения к командным центрам бот-сетей.

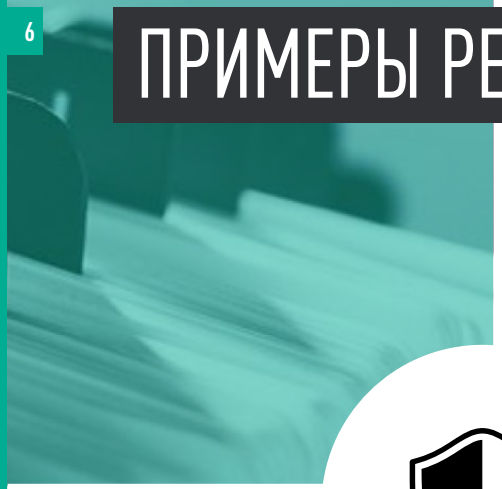
СЕТЕВАЯ ФОРЕНЗИКА (NETWORK FORENSICS)

Криминалистика, а именно комплекс мер для выявления и расследования внутрикорпоративных киберпреступлений и случаев мошенничества, поиска уязвимостей в сетевой инфраструктуре компании

ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА ENTITY BEHAVIOR ANALYTICS (EBA)

На основе машинного обучения и статистических методов позволяет выявлять отклонения в поведении сущностей от их “нормального” профиля

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ



- Детектирование загрузки файлов с внешних неизвестных хостов
- Обнаружение попыток удаленного выполнения кода
- Выявление использования слабой парольной политики в компании
- Обнаружение использования протоколов анонимных сетей DarkNet (Tor, I2P)
- Контроль использования некорпоративного DNS
- Выявление использования программного обеспечения, предназначенного для загрузки пиратского контента (Torrent)
- Обнаружение сетевых протоколов на нестандартных портах
- Выявление майнинга
- И прочие

ПРИНЦИП РАБОТЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

КОНТРОЛЬ СЕТЕВЫХ КАНАЛОВ

- На соответствие передаваемых потоков данных политикам информационной безопасности
- На выявление аномальной активности

ОПТИМИЗИРОВАННОЕ ХРАНЕНИЕ

- Гибкие настройки параметров записи:
  - Запись с сохранением «сырых» данных
  - Запись только статистики по всем потокам
- Индексация и быстрый поиск по всему объёму поступающих данных благодаря высокопроизводительной системе хранения

ПЕРЕХВАТ, АНАЛИЗ И ЗАПИСЬ

IP-трафика в режиме реального времени.

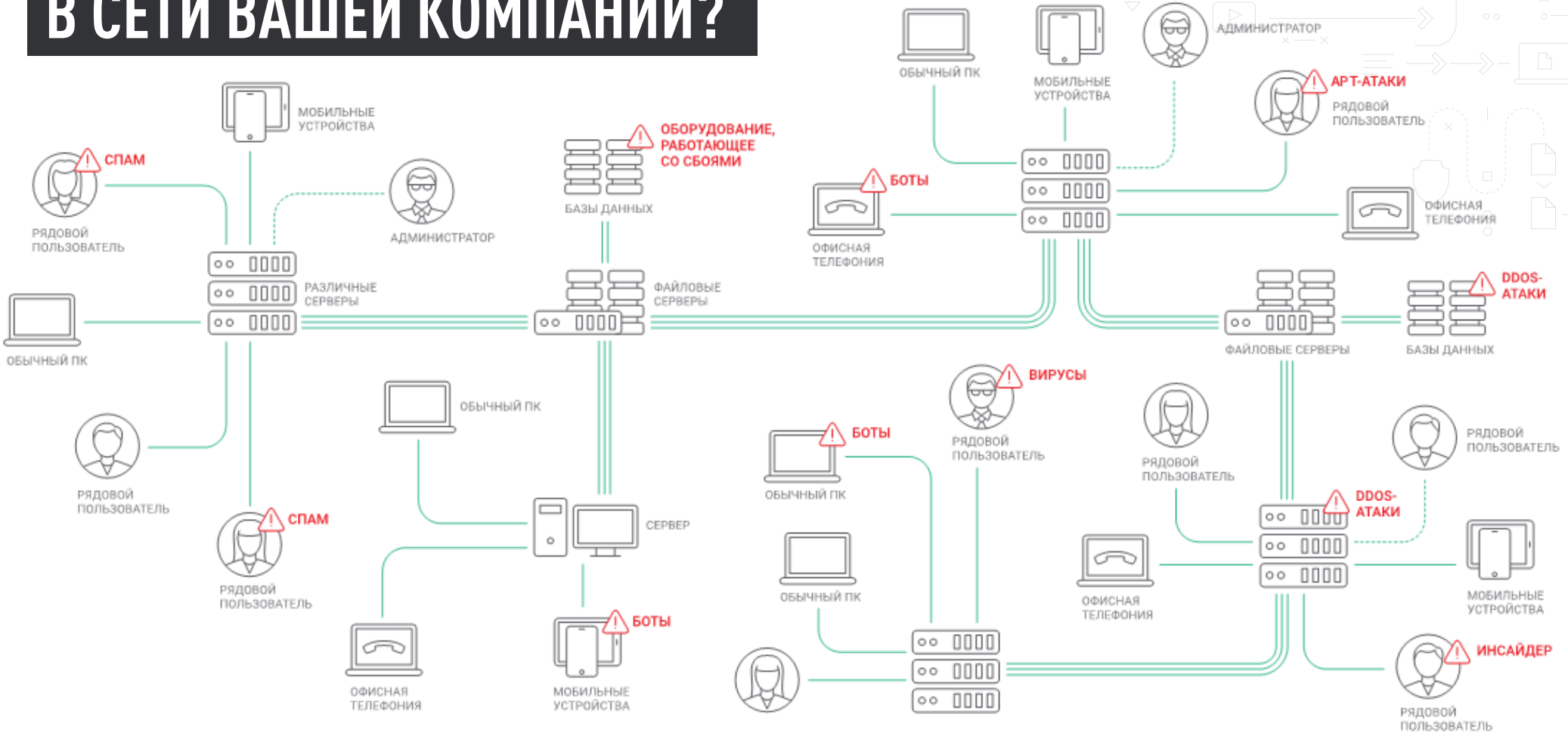
УДОБНЫЙ ВЕБ-ИНТЕРФЕЙС

Многоуровневые отчеты и настраиваемый рабочий экран для удобного управления и решения задач сетевой форензики

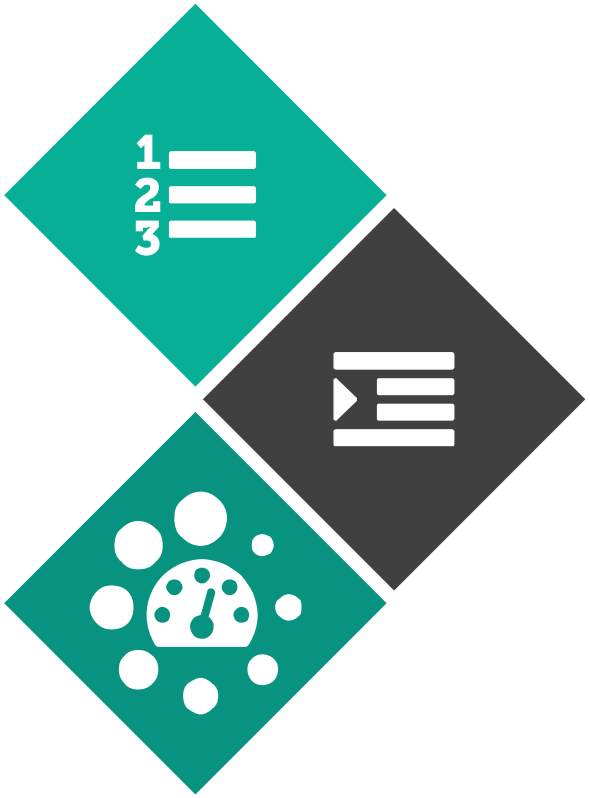
ЧТО ПРОИСХОДИТ В СЕТИ ВАШЕЙ КОМПАНИИ?

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ



ИЗВЕСТНЫЕ ПРОБЛЕМЫ ПРИ АНАЛИЗЕ РАБОТЫ СЕТИ



БОЛЬШОЕ КОЛИЧЕСТВО ПОТОКОВ

Анализ логов каждой системы занимает
много времени и требует специальных знаний.

НЕЗАЩИЩЁННЫЕ ЛОГИ

Возможность изменения этих логов администратором системы.

ПИК НАГРУЗКИ ПРИ АУДИТЕ

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

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

КОМПОНЕНТЫ СИСТЕМЫ И ИХ ПРОИЗВОДИТЕЛЬНОСТЬ

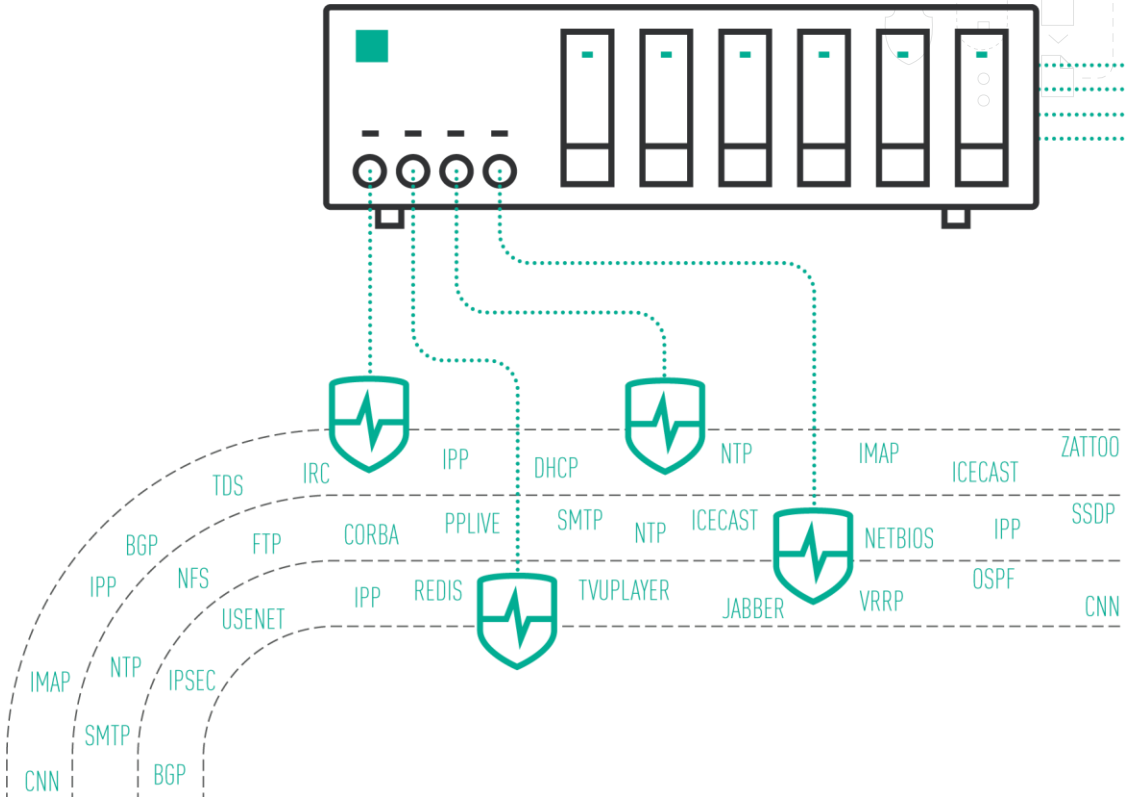
1 СБОР ДАННЫХ

2

Система непрерывно собирает и анализирует трафик в реальном времени.

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

ПРИ УСТАНОВКЕ СИСТЕМА УЖЕ СОДЕРЖИТ ПОДКЛЮЧЁННЫЕ И ОБНОВЛЯЕМЫЕ БАЗЫ СИГНАТУР, РЕПУТАЦИОННЫЕ СПИСКИ

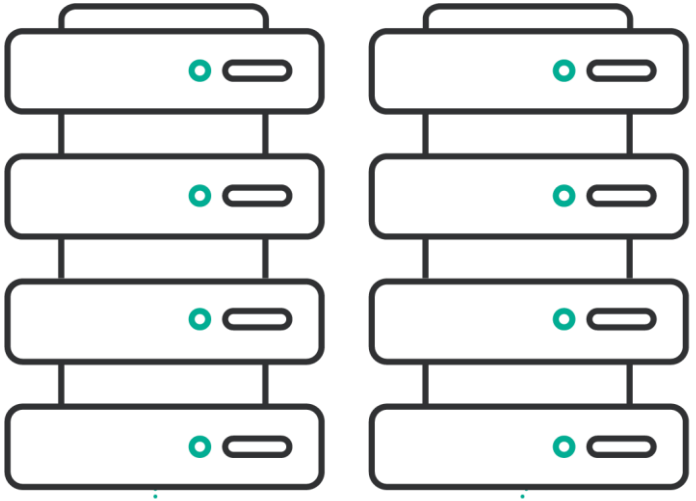


КОМПОНЕНТЫ СИСТЕМЫ И ИХ ПРОИЗВОДИТЕЛЬНОСТЬ

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.



Гибкие настройки параметров записи

(Например, возможность отключить запись содержимого шифрованного трафика)

ГАРДА МОНИТОР

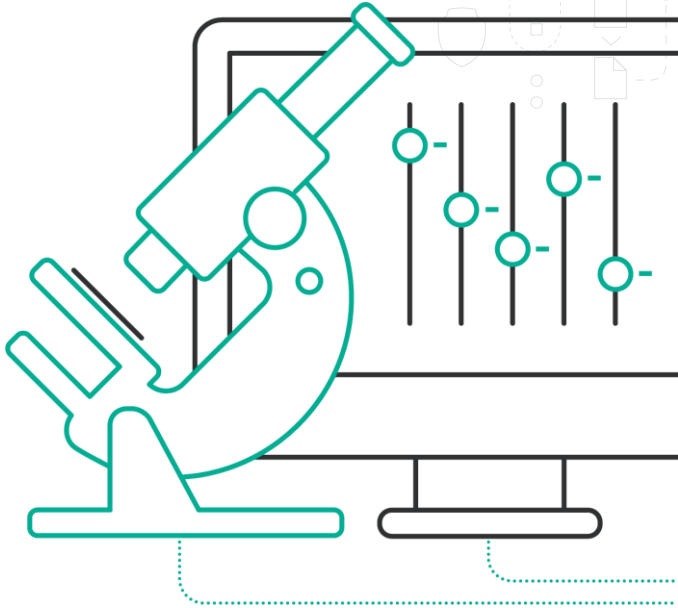
ГАРДА ТЕХНОЛОГИИ

КОМПОНЕНТЫ СИСТЕМЫ И ИХ ПРОИЗВОДИТЕЛЬНОСТЬ

3 АНАЛИТИКА И УПРАВЛЕНИЕ

2

- Гибкий многокритериальный поиск
- Выявление подозрительных событий и инцидентов
- Перехваченные объекты отображаются в удобном для просмотра виде
- Разнообразные виды предустановленных отчётов

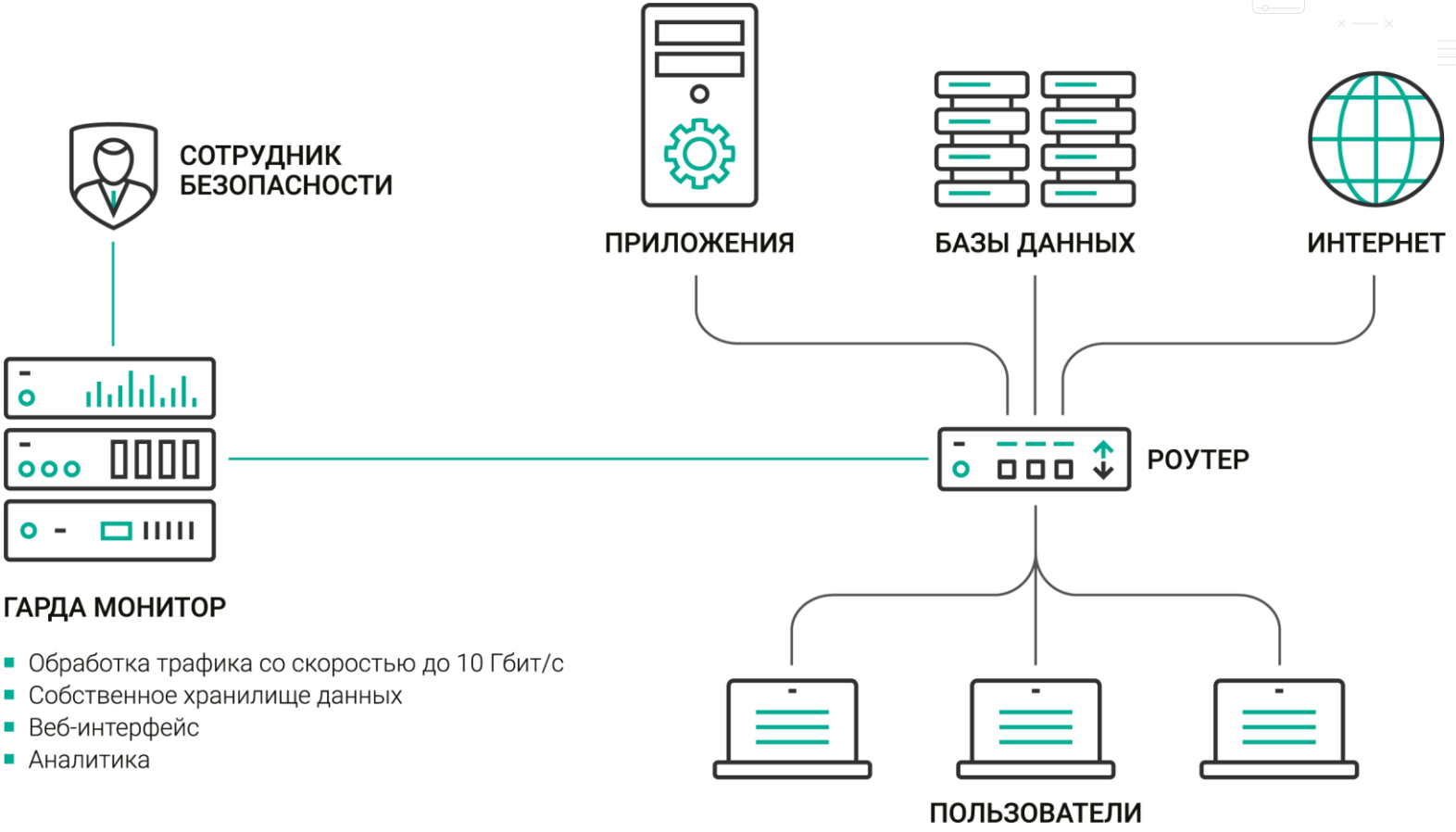


Технологии EBA
ENTITY BEHAVIOR ANALYTICS

Решение класса DPI
DEEP PACKET INSPECTION

Персонификация трафика
IDENTITY TRACKING

СХЕМА ВНЕДРЕНИЯ



- Обработка трафика со скоростью до 10 Гбит/с
- Собственное хранилище данных
- Веб-интерфейс
- Аналитика

КЕЙСЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

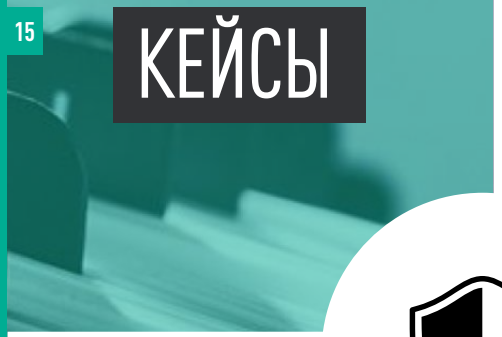
#1 ВЫЯВЛЕНИЕ ДЕЙСТВИЙ ВРЕДОНОСНОГО ПО:

- 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)

КЕЙСЫ



ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

#3 ВЫЯВЛЕНИЕ ПОДОЗРИТЕЛЬНОГО ВЗАИМОДЕЙСТВИЯ С ВНЕШНИМИ СЕТЯМИ:

- Детектирование попыток удаленного доступа из внешних сетей к внутренним серверам
- Выявление VPN-каналов

#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 потоки в формате *.pcap
- Использовать эти потоки как доказательства в расследовании и суде

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.

КЕЙСЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

#5 СИГНАТУРНЫЙ АНАЛИЗ ТРАФИКА:

- Выявление активности вредоносного и подозрительного ПО, эксплуатации уязвимостей.
- Наличие собственной базы данных уязвимостей и экспертного центра
- Возможность выгрузки образцов сетевого трафика для последующего анализа
- Категорирование угроз
- Автоматизированные политики по выявлению угроз сетевой безопасности
- Детектирование фактов сетевой разведки
- Автоматическое обновление базы данных сигнатур

#6 ПРОФИЛИРОВАНИЕ И ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА:

- Построение поведенческой модели по политикам контроля сетевого трафика
- Выявление отклонений по объему потоков, количеству и другим параметрам.

ПРИМЕРЫ:

- Аномально большое количество DNS запросов от хоста
- Аномально большой объем данных, передаваемых по SSH за периметр
- Аномальное количество отправляемой почты с хоста или сервера

ПОЛНЫЙ КОНТРОЛЬ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ГАРДА МОНИТОР СОЗДАНА ДЛЯ ЭФФЕКТИВНОГО АНАЛИЗА СОБЫТИЙ СЕТЕВОЙ БЕЗОПАСНОСТИ

Хранение более 100 Тб трафика

Анализ трафика 10 Гбит/с на модуль

Классификация трафика свыше 250 типов протоколов

ЗАПИСЬ ВСЕХ ДАННЫХ L2-L7 УРОВНЯ В ХРАНИЛИЩЕ

Запись всего трафика предприятия, внутренней локальной сети и интернет-трафика, а также возможность выгрузить содержимое потока в формате *.pcap

КЛАССИФИКАЦИЯ ПАКЕТОВ И ПОТОКОВ ДАННЫХ

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

УВЕДОМЛЕНИЕ ОБ ИНЦЕДЕНТАХ ИБ

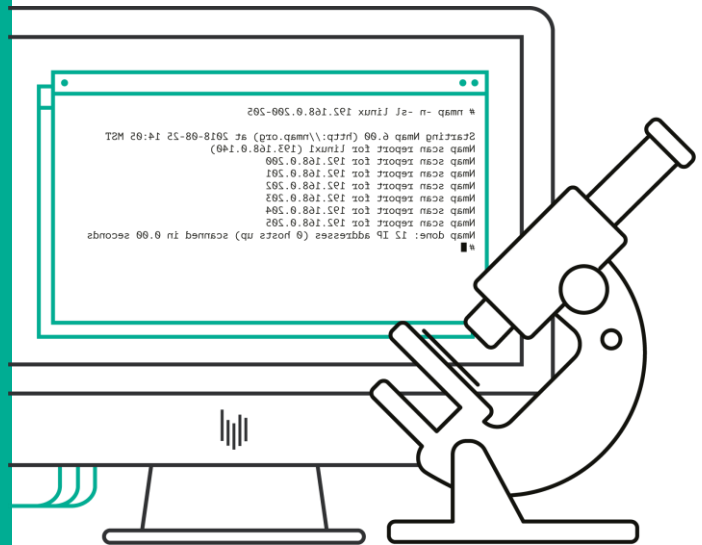
Оповещение о выявленных инцидентах ИБ в режиме реального времени, таких как: использование запрещенных приложений (TOR, BitTorent и т.д.), подключение из внешних сетей, использование нестандартных портов, протоколов, приложений

КОНТРОЛЬ «ВНЕШНЕГО ПЕРИМЕТРА» & ВЫЯВЛЕНИЕ УГРОЗ ИБ

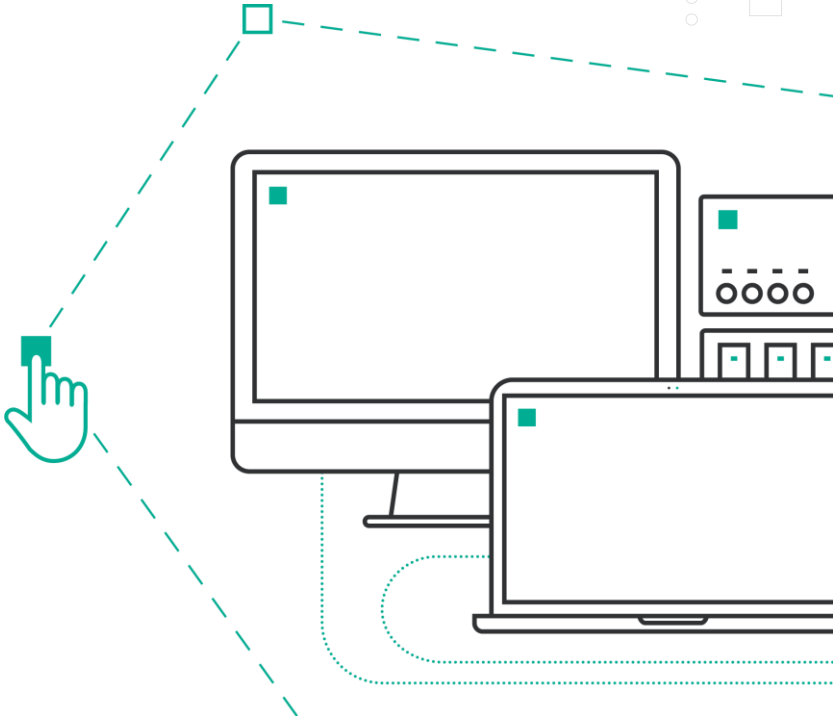
ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

- DoS-атаки (SYN-flood, ICMP-flood)
- Сканирование портов
- Сканирование хостов



- Обнаружение фактов подключения «извне» к точкам, не входящим во внешний периметр
- Указание точек внешнего периметра



ПОЛИТИКИ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

КЛАССИФИКАЦИЯ ТРАФИКА (СВЫШЕ 250 ПРОТОКОЛОВ, БОЛЕЕ 30 СЕТЕВЫХ ПАРАМЕТРОВ)

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» траффик (Игры, соц. сети)
- ☑ Рекомендации FinCERT
- ☑ Факты «Сетевой разведки»

ДЕТЕКТИРОВАНИЕ ПРОТОКОЛОВ DARKNET, P2P, АУТЕНТИФИКАЦИИ, ОБЛАЧНЫХ СЕРВИСОВ, ПРОТОКОЛОВ УДАЛЕННОГО ДОСТУПА, SSH, HTTP(S), ПОЧТОВЫХ ПРОТОКОЛОВ И Т.Д.

ШИРОКИЕ ВОЗМОЖНОСТИ ПО ПОСТРОЕНИЮ ПОЛИТИКИ:

- ☑ IP-адреса (включая группы) и порт
- ☑ MAC-адрес
- ☑ DNS-имя
- ☑ Тип протокола
- ☑ Длительность, размер потока
- ☑ Данные геолокации («Source-Destination»)
- ☑ Учетная запись, почтовый адрес, URL и другие
- ☑ Направление (входящий\исходящий)
- ☑ HTTP-метод
- ☑ Наличие вложений
- ☑ Ключевые слова в содержимом потока

АНАЛИТИКА & ПОЛНОТЕКСТОВЫЙ ПОИСК ПО ПЕРЕХВАЧЕННЫМ ДАННЫМ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

АНАЛИТИЧЕСКИЕ ВОЗМОЖНОСТИ

КАРТА СЕТИ

Отображение карты сетевых взаимодействий и экспертного анализа над связями (визуализация, инфографика)

ENTITY BEHAVIOR ANALYTICS (EBA)

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

ПРИМЕРЫ КРИТЕРИЕВ ПОИСКА:

- По IP-адресам источника и получателя
- По портам источника и получателя
- По типу протокола транспортного уровня
- По типу прикладного протокола
- По имени рабочей станции
- По Vlan ID
- По MAC-адресам источника и получателя

КОНСТРУКТОР ОТЧЁТОВ

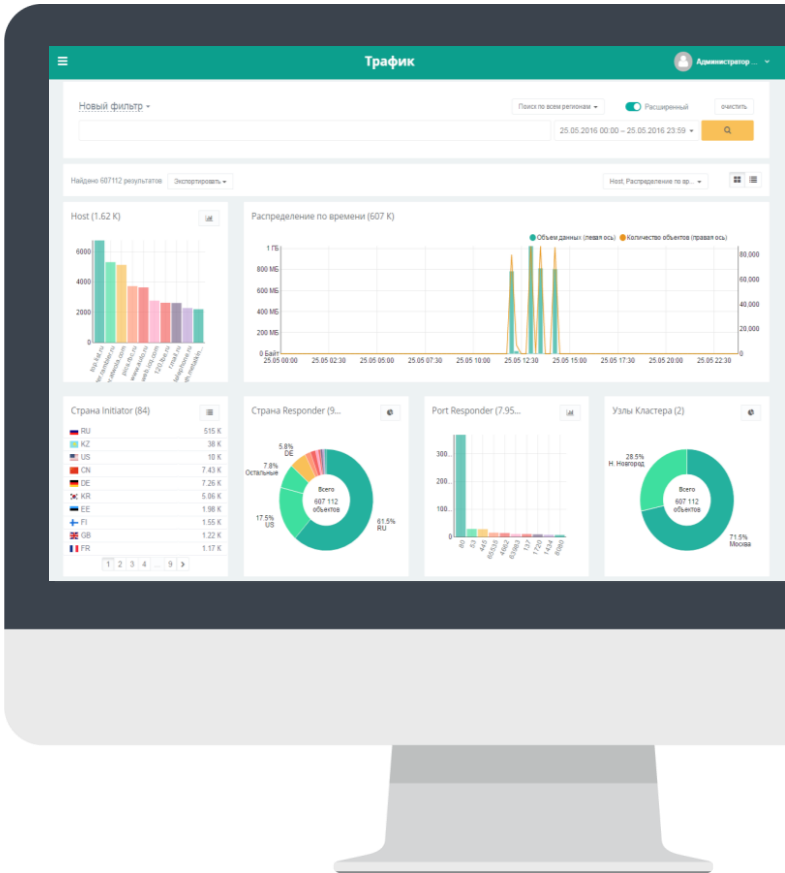
ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ДЛЯ ЛЕГКОГО ВЕРХНЕУРОВНЕВОГО АНАЛИЗА СЕТЕВОЙ АКТИВНОСТИ РАЗНООБРАЗНЫЕ ОТЧЁТЫ СТРОЯТСЯ В РЕАЛЬНОМ ВРЕМЕНИ В ПРОСТОМ И ПОНЯТНОМ ГРАФИЧЕСКОМ ИНТЕРФЕЙСЕ

ДОСТУПНЫЕ ВИДЫ ОТЧЁТНОСТИ:

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



ИНТЕГРАЦИЯ И ЭКСПОРТ-ИМПОРТ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

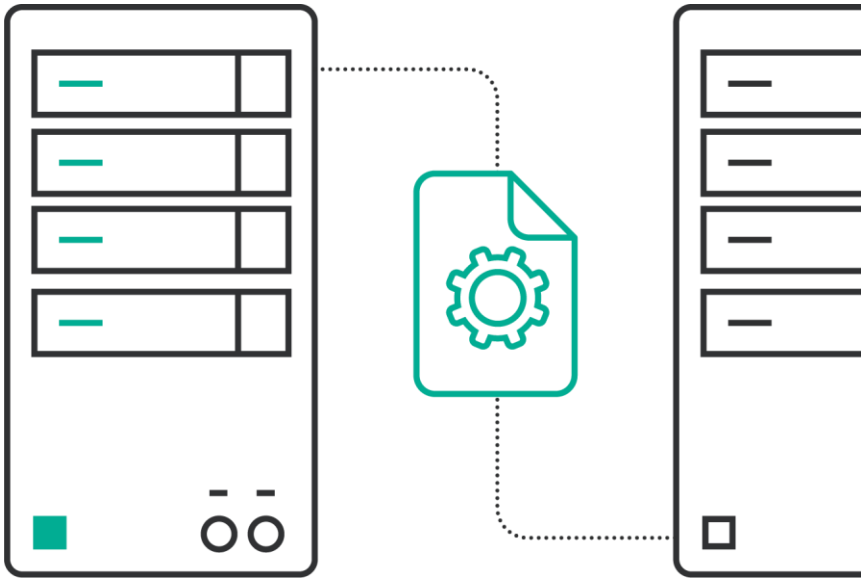
ДОСТУПНЫЕ ФОРМЫ

- [x] CSV
- [x] XML
- [x] PDF
- [x] SysLog
- [x] Электронная почта

МИРОВЫЕ БАЗЫ

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

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



ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ РЕШЕНИЯ

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

КОМПЛЕКС НАСТРОЕН И ГОТОВ К РАБОТЕ СРАЗУ ПОСЛЕ ИНСТАЛЛЯЦИИ (ИЗ КОРОБКИ)

Политики, правила, автоматическое обновление сигнатур и репутационные списки и пр .

РАСПРЕДЕЛЕННАЯ АРХИТЕКТУРА: МОНИТОРИНГ ТРАФИКА ВСЕХ ФИЛИАЛОВ КОМПАНИИ ИЗ ЕДИНОГО ЦЕНТРА

Гибкие политики безопасности как для всего гео-кластера, так и на конкретные филиалы.

ГИБКАЯ СИСТЕМА ФИЛЬТРОВ

Многокритериальный поиск в реальном времени

МАСШТАБИРУЕМОСТЬ КОМПЛЕКСА

Неограниченный объем записи трафика и оперативный доступ к данным за любой период времени

МНОЖЕСТВО СПОСОБОВ ПОДАЧИ ТРАФИКА

SPAN, NetFlow, Агенты, GRE

ПРОЗРАЧНОСТЬ СЕТЕВЫХ ПОТОКОВ ДАННЫХ

Полная картина происходящего в сети

КОМБИНАЦИЯ РАЗЛИЧНЫХ ТЕХНОЛОГИЙ ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ И ОБНАРУЖЕНИЯ СЕТЕВЫХ ИНЦИДЕНТОВ

На основе сигнатурного анализа, поведенческого анализа, детектирования по спискам

УДОБНЫЙ ИНТЕРФЕЙС

Гибкие отчеты, дашборды, статистика по трафику, гибкий поиск с функциональной строкой

КОМПЛЕКС НЕ ТРЕБУЕТ СТОРОННИХ ЛИЦЕНЗИЙ

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ (ИТОГО)

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

- Запись сетевого трафика в исходном виде
- Гибкий поиск по свойствам, выделенным из записанных потоков информации (IP-адреса, порты, mac-адерса, email, учетные записи, страна отравителя/получателя, протокол и пр.)
- Классификация трафика по протоколам (HTTP, POP3, FTP,SSH и ещё свыше 250 типов протоколов)
- Возможность добавить пользовательские протоколы
- Возможность выгрузки содержимого интересующей сессии в формате PCAP
- Построение графических отчётов по найденным массивам информации
- Возможность задать срок хранения статистики и трафика (например, статистику храним в течение 1 месяца, а содержимое – 3 дня)
- Возможность указать правила записи трафика (например, для шифрованных потоков сохраняем только статистику)
- Определение географического положения источника и получателя данных
- Выявление фактов сетевой разведки и атак на узлы сети с помощью сигнатурных решающих правил
- Выявление обращений к скомпрометированным ресурсам на основе принадлежности к репутационным спискам
- Выявление аномального поведения устройств и пользователей
- Возможность просмотра истории авторизации пользователей на рабочих станциях
- Автоматически обновляемые решающие правила
- Автоматически обновляемые базы репутационных списков (скомпрометированные IP-адреса, email, url)
- Автоматически обновляемая база определения географического положения IP-адресов
- Автоматическое выявление инцидентов информационной безопасности
- Настройка автоматического уведомления об инцидентах сотрудника ИБ
- Единый центр управления для контроля всех участков сети (в т.ч. и распределённой), детектирования атак и оперативного реагирования на киберугрозы
- Интеграция с SIEM системами

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ #1

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ПЕРЕДАЧА ДАННЫХ

- HTTPS
- HTTP
- WAP
- FTP
- TFTP
- SMB
- BitTorent
- Filetopia
- iMESH
- OpenFT
- Kazaa/Fasttrack
- eDonkey
- DirectConnect
- AppleJuice
- PANDO
- StealthNet
- AFP (Apple Filing Protocol, AppleShare)

ОБМЕН СООБЩЕНИЯМИ

- OSCAR (ICQ v7, v8, v9)
- IRC (Согласно RFC 2810-2813)
- MMP (Mail.Ru Агент)
- XMPP (QIP, Jabber)
- Tencent (QQ)
- MSN
- Yahoo
- MEEBO
- Skype
- WhatsApp
- Viber

АВТОРИЗАЦИЯ

- RADIUS
- TACACS+
- Diameter
- Kerberos

БАЗЫ ДАННЫХ

- PostgreSQL
- MySQL
- TDS
- MSSQL
- ORACLE
- Redis

СЕТЕВЫЕ СЛУЖБЫ

- RTP
- RTCP
- DNS
- SNMP
- SSH
- RDP
- RFB (VNC)
- NNTP
- MGCP
- TOR
- Opera Mini

ПРИВАТНЫЕ СЕТИ

- OpenVPN
- CiscoVPN
- HotspotShield VPN

ПОЧТОВЫЕ ПРОТОКОЛЫ

- SMTP
- IMAP4
- POP3
- NNTP
- MS Exchange (MAPI)

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ #2

ГАРДА МОНИТОР
ГАРДА ТЕХНОЛОГИИ

ИГРЫ & РАЗВЛЕЧЕНИЯ

- XBOX
- Steam
- Battlefield
- Quake
- Halflife2
- World of Warcraft
- WARCRAFT3
- Stracraft
- Armagetron
- World of Kung Fu
- Guildwars
- Florensia
- Dofus
- CrossFire

ОБМЕН СООБЩЕНИЯМИ

- OSCAR (ICQ v7, v8, v9)
- IRC (Согласно RFC 2810-2813)
- MMP (Mail.Ru Агент)
- XMPP (QIP, Jabber)
- Tencent (QQ)
- MSN
- Yahoo
- MEEBO
- Skype
- WhatsApp
- Viber

УДАЛЁННОЕ УПРАВЛЕНИЕ

- SSH
- TeamViewer
- RDP
- VNC
- PCAnywhere

МУЛЬТИ-МЕДИА

- RealMedia
- Windowsmedia
- Icecast
- PPLive
- PPStream
- Zattoo
- SHOUTCast
- SopCast
- TVAnts
- TVUplayer
- VeohTV
- QQLive
- GloboTV
- Deezer

VOIP

- SIP
- Megaco (H.248)
- H.323
- SCCP (SKINNY)
- MGCP
- IAX
- WhatsApp Voice
- Webex
- TeamSpeak

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ #3

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

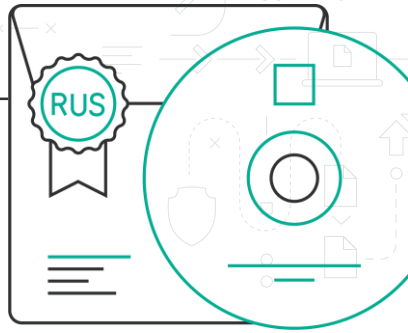
ПРОЧИЕ ПРОТОКОЛЫ

- 99Taxi
- Aimini
- Apple (iMessage, FaceTime…)
- Apple iCloud
- Apple iTunes
- AVI
- BGP
- Citrix
- CitrixOnline & GotoMeeting
- CNN
- Collectd
- Corba
- DCE RPC
- DHCP
- DHCPv6
- DirectDownloadLink
- DNS
- DropBox
- EGP
- FaceBook
- Feidian
- Fiesta
- Flash
- GaduGadu
- Gmail
- Gnutella
- Google
- Google Maps
- GRE
- GTP
- I23V5
- ICMP
- ICMPv6
- IGMP
- Instagram
- IPP
- IPSEC
- KakaoTalk Voice and Chat
- Kontiki
- LDAP
- LLMNR
- LotusNotes
- MapleStory
- MDNS
- Microsoft Cloud Services
- MMS
- MOVE
- MPEG
- NETBIOS
- Netflix
- NetFlow_IPFIX
- NFS
- NOE
- NTP
- OFF
- OGG
- OpenSignal
- OSPF
- Popo
- PPTP
- QUIC
- QuickTime
- RemoteScan
- RSYNC
- RTCP
- RTP
- RTSP
- SAP
- SCTP
- sFlow
- Simet
- Snapchat
- SNMP
- Socrates
- Soulseek
- Spotify
- SSDP
- SSL
- STUN
- Syslog
- Telnet
- Teredo
- Thunder Webthunder
- TOR
- Truphone
- Tuenti
- Twitch
- Twitter
- UbuntuONE
- UPnP
- USENET
- VMware
- VRRP
- Whois-DAS
- Wikipedia
- WindowsUpdate
- WinMX
- XDMCP
- YouTube
- ZeroMQ

РЕШЕНИЕ ПОМОГАЕТ ВЫПОЛНИТЬ ТРЕБОВАНИЯ ЗАКОНОДЕТЕЛЬСТВА

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ



- 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов…»
- 152-ФЗ «О персональных данных»
- 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»
- Отдельные разделы GDPR (Генеральный регламент о защите персональных данных ЕС)
- Обеспечивает реализацию мер, рекомендованных международным стандартом по работе с инцидентами компьютерной безопасности NIST-800-61 (Руководство по управлению инцидентами компьютерной безопасности).

ФАЗЫ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

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

О КОМПАНИИ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ТЕХНОЛОГИИ — РОССИЙСКИЙ ПРОИЗВОДИТЕЛЬ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Команда разработчиков обладает многолетним опытом в сфере информационных технологий и создаёт решения для различных задач безопасности.

Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ.

100+
Внедрений на территории России

180 +
Высококвалифицированных сотрудников

10 ЛЕТ
Опыт разработки систем высокой сложности

5
Запатентованных технологий собственного исследовательского центра

ПОЛНОСТЬЮ РОССИЙСКИЕ РЕШЕНИЯ

- Собственная технологическая платформа для хранения информации не требует сторонних лицензий.
- Решения сертифицированы ФСТЭК.
- Включены в реестр отечественного программного обеспечения.

СПАСИБО
ЗА ВНИМАНИЕ!

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

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