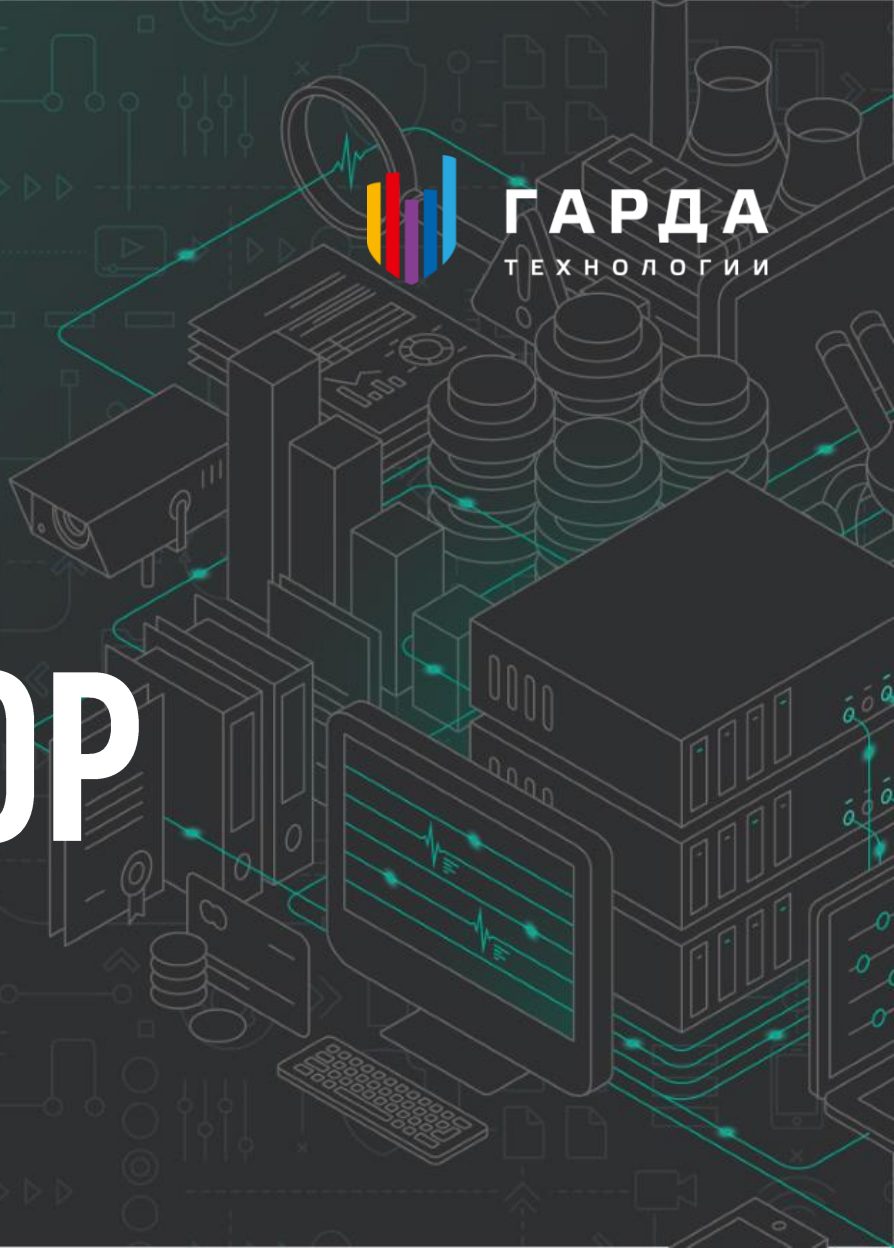
ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ



ГАРДА МОНИТОР

ВЫЯВЛЕНИЕ УГРОЗ И РАССЛЕДОВАНИЕ 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

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

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

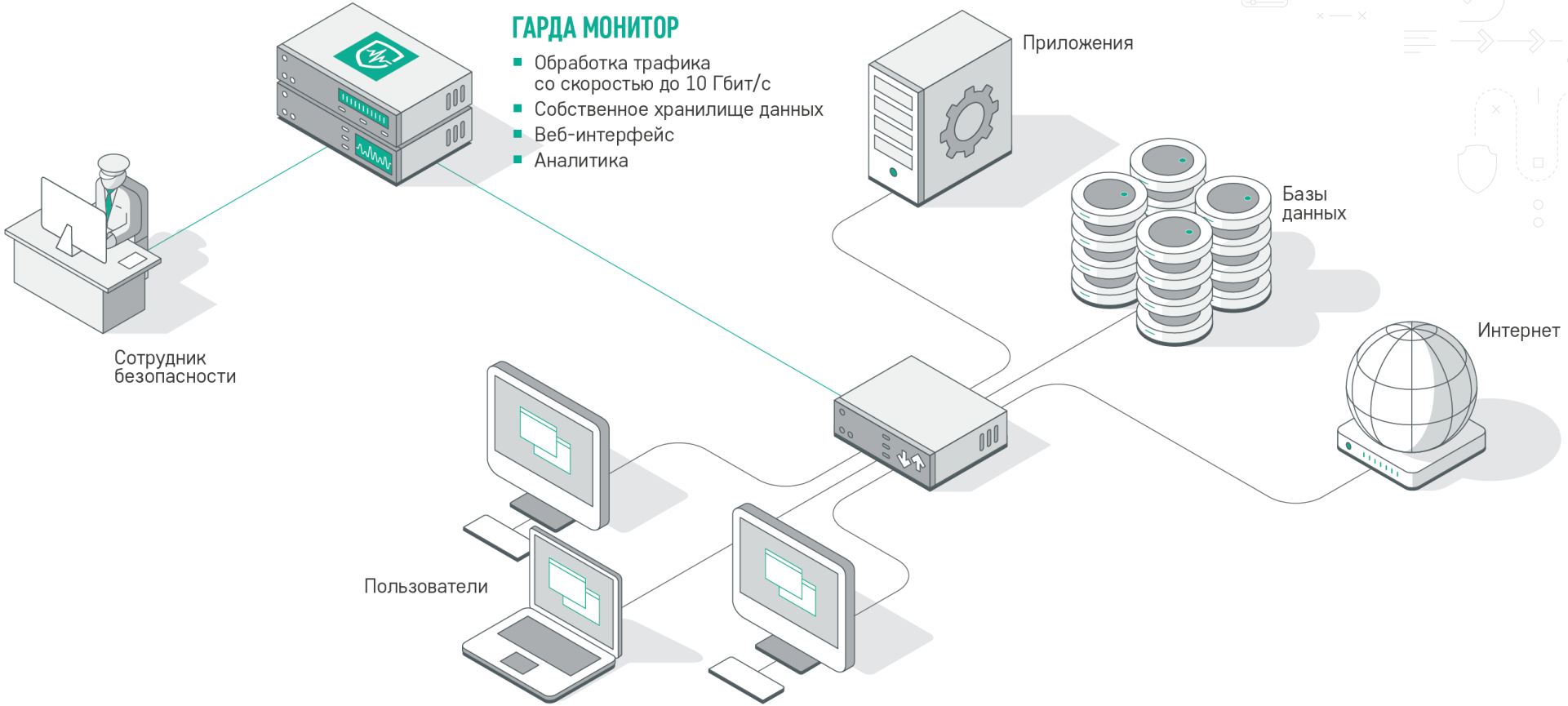
ПИК НАГРУЗКИ ПРИ АУДИТЕ

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

СХЕМА

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ



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

МУЛЬТИМЕДИА

- 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

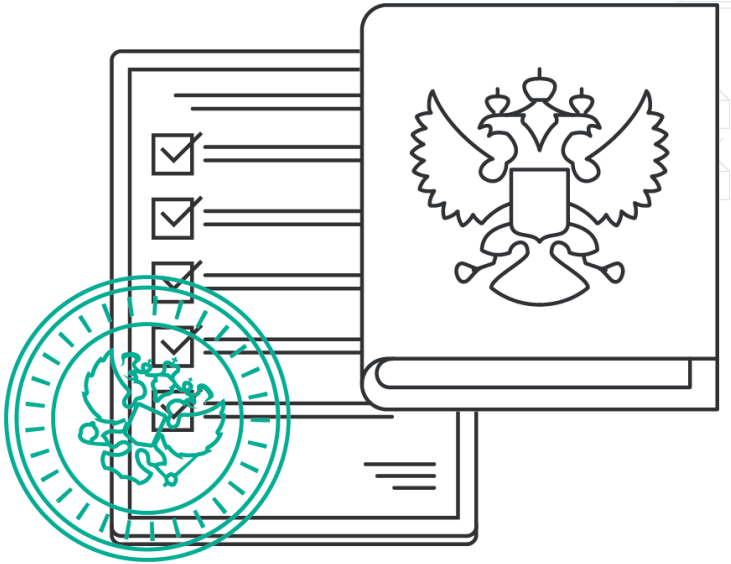
ПРОЧИЕ ПРОТОКОЛЫ

- 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

ГАРДА МОНИТОР ГАРДА ТЕХНОЛОГИИ

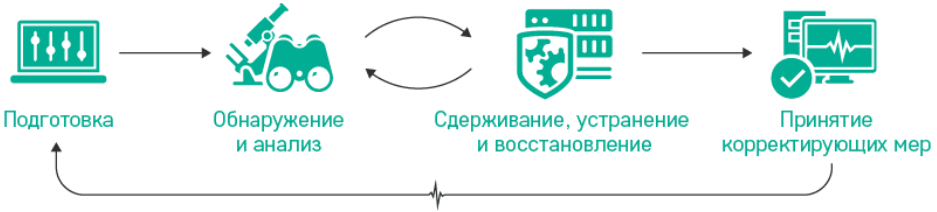
РЕШЕНИЕ ПОМОГАЕТ ВЫПОЛНИТЬ ТРЕБОВАНИЯ ЗАКОНОДЕТЕЛЬСТВА

- 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 РАЗРАБОТЧИК 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.

«Гарда Технологии» входит в российскую многопрофильную ИТ-группу «ИКС Холдинг».

150+
Внедрений на территории России

180 +
Высококвалифицированных сотрудников

16 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