{NETWORK VISIBILITY}

БЕЗОПАСНОСТЬ И ПРОЗРАЧНОСТЬ КОРПОРАТИВНЫХ ПРОЦЕССОВ

Уразбахтин Илья
Руководитель направления
Центра Компетенций ИБ

ГАРДА
ТЕХНОЛОГИИ

О СПИКЕРЕ

ГАРДА
ТЕХНОЛОГИИ

УРАЗБАХТИН ИЛЬЯ

Руководитель направления
Центра Компетенций
Информационной Безопасности

ЧТО ВЫ ЗНАЙТЕ О ВАШЕЙ СЕТИ ?

ГАРДА
ТЕХНОЛОГИИ

АНОНИМНЫЙ ОПРОС

SCAN ME

СОБЛЮДАЙТЕ РЕГИСТР

ankt.cc/WuqknR

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.

РЕЗУЛЬТАТЫ ЭКСПРЕСС-ОПРОСА

СТАТИСТИКА

ГАРДА
ТЕХНОЛОГИИ

70%

СПЕЦИАЛИСТОВ
НЕ ОБЛАДАЮТ ПОЛНОЙ ИНФОРМАЦИЕЙ О ТОМ КАКИЕ УСТРОЙСТВА НАХОДЯТСЯ В ИХ СЕТИ*

*По опросу SANS Network Visibility and Threat Detection Survey (2020)

СТАТИСТИКА

ГАРДА
ТЕХНОЛОГИИ

59%

СПЕЦИАЛИСТОВ
СЧИТАЮТ, ЧТО
НЕДОСТАТОЧНАЯ ВИДИМОСТЬ =
ВЫСОКИЙ РИСК ИБ

*По опросу SANS Network Visibility and Threat Detection Survey (2020)

VISIBILITY

ГАРДА ТЕХНОЛОГИИ

СУЩЕСТВИТЕЛЬНОЕ

ОПРЕДЕЛЕНИЕ
- Способность что-либо легко заметить
- Возможность восприятия

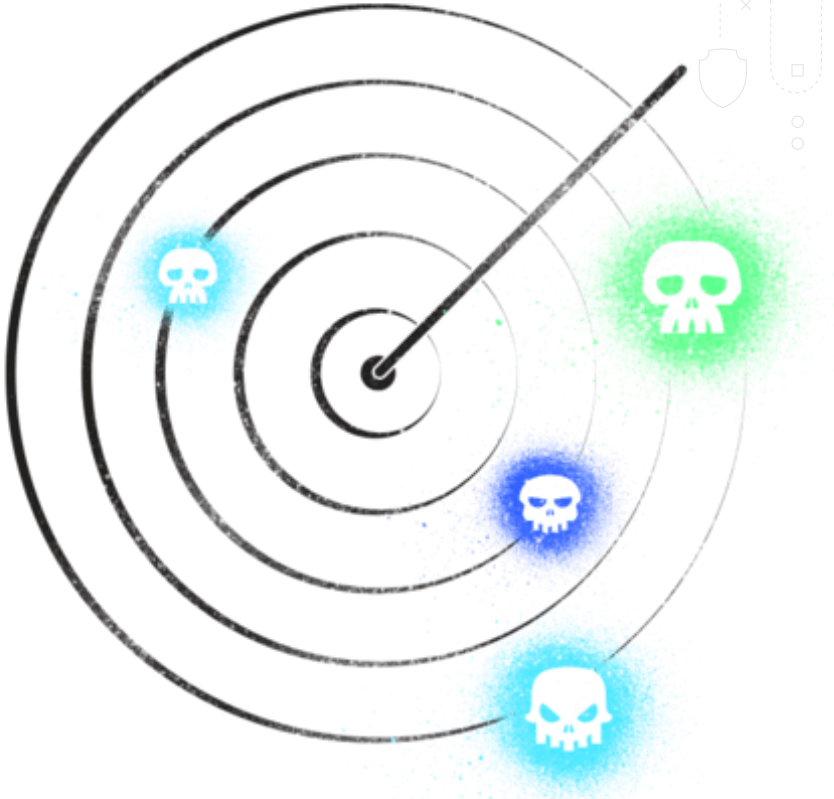
ХАРАКТЕРИСТИКИ:
- Скорость реакции
- Локализация в пространстве
- Степень ясности, глубина
- Количественное определение

NETWORK VISIBILITY

ГАРДА ТЕХНОЛОГИИ

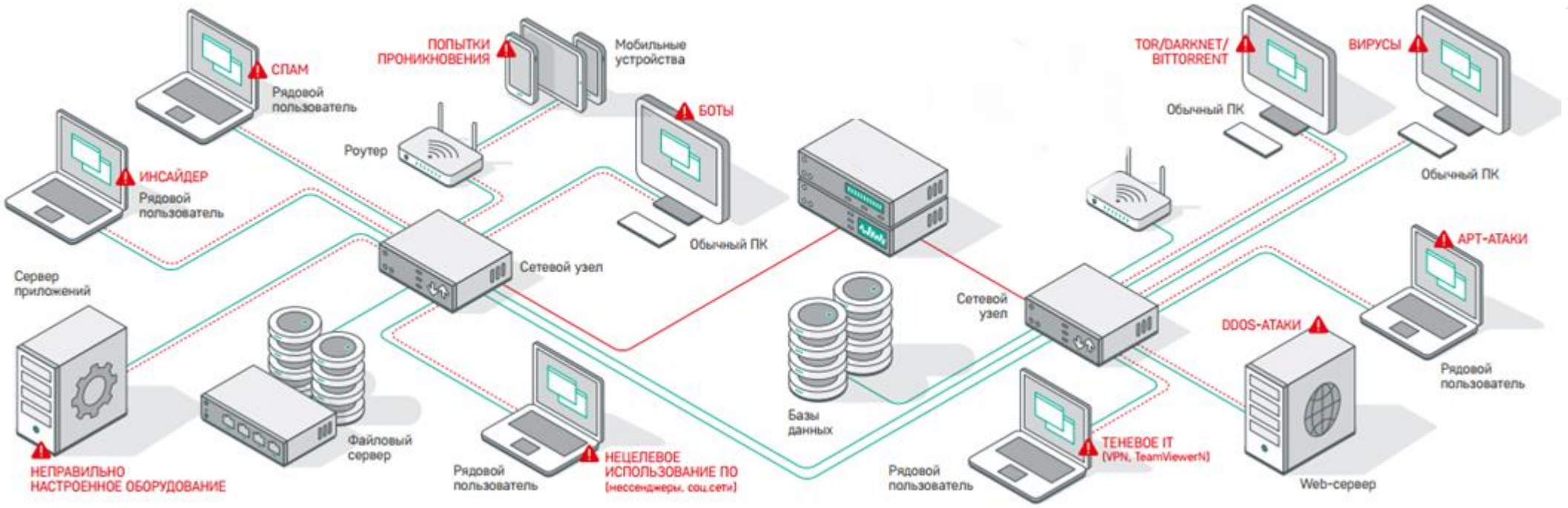
СПОСОБНОСТЬ ЛЕГКО ЗАМЕЧАТЬ И ВОСПРИНИМАТЬ СЕТЕВЫЕ СОБЫТИЯ.

ХАРАКТЕРИСТИКИ:
Скорость реакции (Когда?);
Локализация (Где?)
Степень ясности, глубина (Что?)
Количественное понимание (Сколько?)



ЧТО СКРЫВАЕТ ВАША СЕТЬ?
СЛЕПЫЕ ЗОНЫ

ГАРДА
ТЕХНОЛОГИИ



ПРИЧИНЫ СЛЕПЫХ ЗОН ИБ

- Слияние и поглощение
- Разделение сетей
- Удаленная работа
- Модернизация и рост сети
- Разрозненность сети
- Увольнение ключевых сотрудников
- Нехватка ресурсов

ГАРДА
ТЕХНОЛОГИИ

ПОЧЕМУ НЕДОСТАТОЧНО ХОСТОВЫХ РЕШЕНИЙ ?

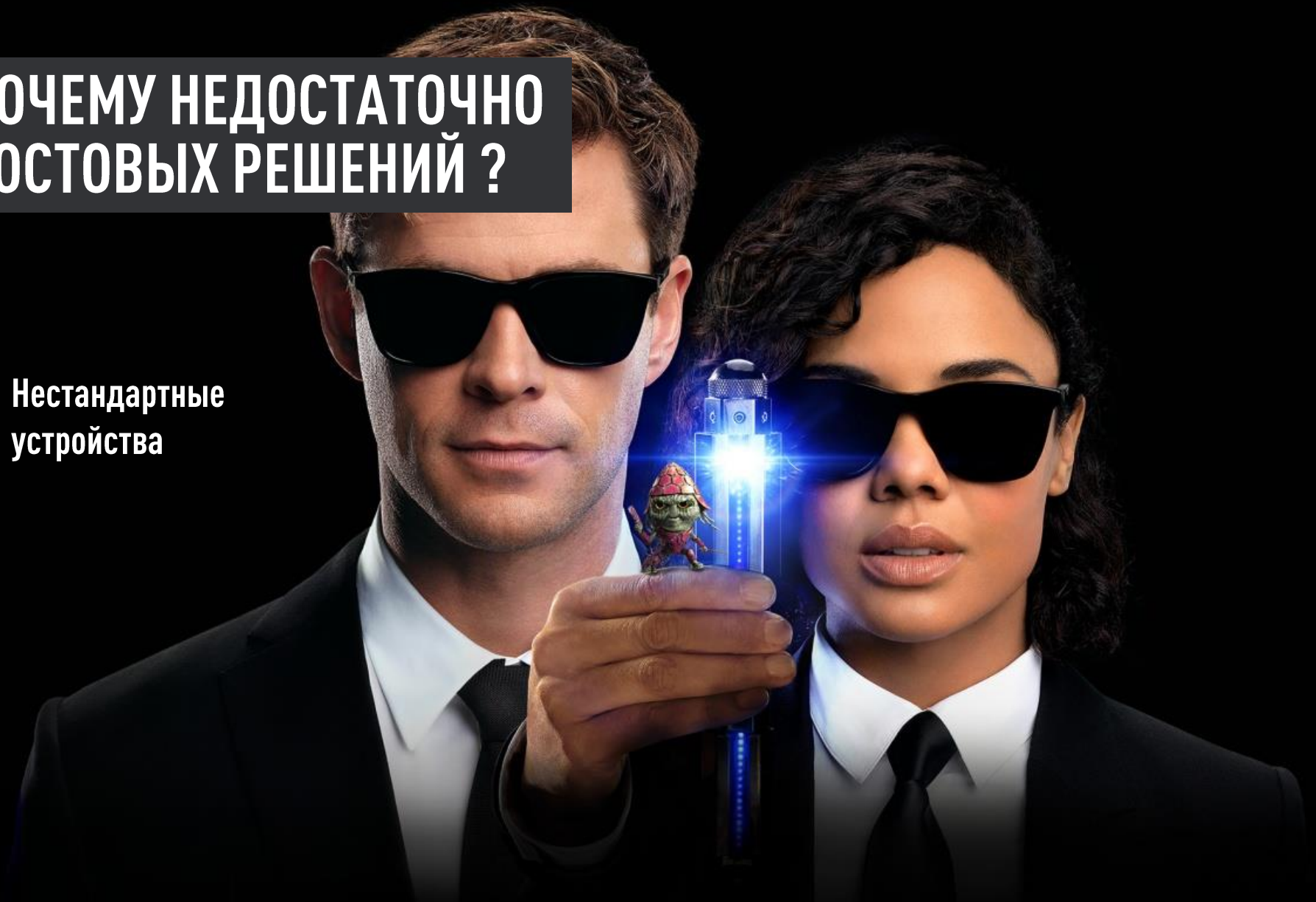
- Изменчивость
- Нестабильность

ПОЧЕМУ НЕДОСТАТОЧНО ХОСТОВЫХ РЕШЕНИЙ ?

- Лицензии
- Лимиты

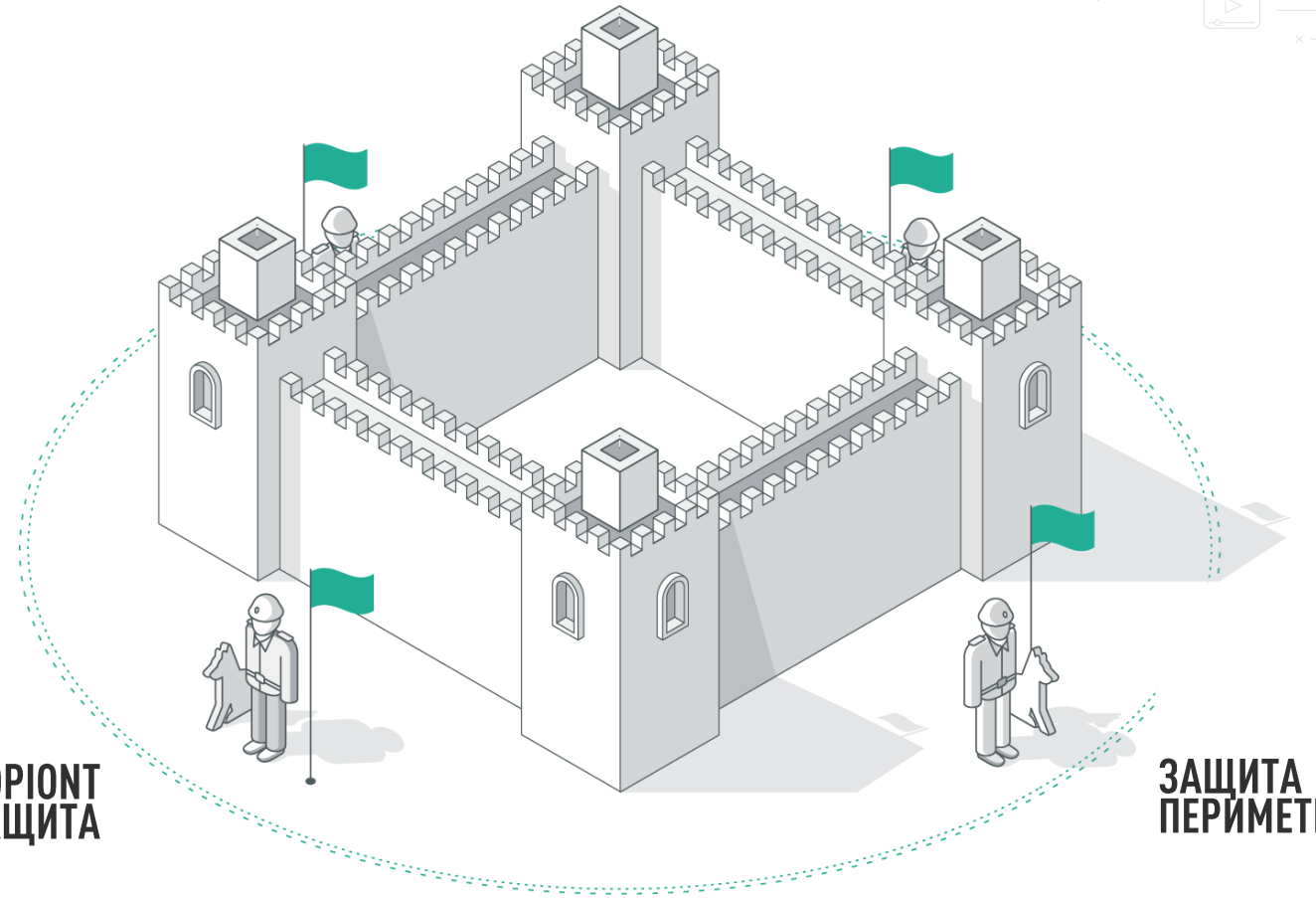
ПОЧЕМУ НЕДОСТАТОЧНО ХОСТОВЫХ РЕШЕНИЙ ?

- Нестандартные устройства



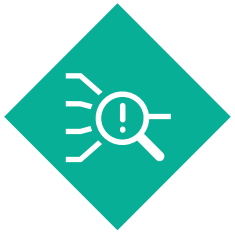
ИНФОРМАЦИОННЫЙ ВАКУУМ

ГАРДА
ТЕХНОЛОГИИ



КАК ВИДЕТЬ БОЛЬШЕ?

ГАРДА ТЕХНОЛОГИИ



АНАЛИЗ СЕТЕВОГО ТРАФИКА NETWORC TRAFFIC ANALYSIS (NTA)

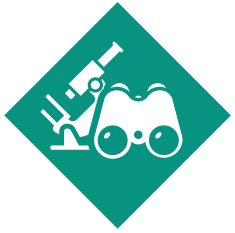
Анализ трафика на основе глубокого разбора содержимого сетевых пакетов (DPI) для выделения свойств сетевых соединений и определения прикладных протоколов

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ INTRUSION DETECTION DYSTEM (IDS)

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

ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА ENTITY BEHAVIOR ANALYTICS (EBA)

Выявление отклонений в поведении сущностей от их “нормального” профиля на основе машинного обучения и статистических методов



СЕТЕВАЯ ФОРЕНЗИКА (NETWORK FORENSICS)

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

ПРИНЦИП РАБОТЫ NTA

ГАРДА ТЕХНОЛОГИИ

ПЕРЕХВАТ, ДЕКОДИРОВАНИЕ ДО L7

IP-трафика в режиме реального времени.

ЗАПИСЬ ДАННЫХ

Запись метаданных, статистики и «сырых» данных

АНАЛИЗ ТРАФИКА

- На соответствие политикам информационной безопасности
- На выявление аномальной активности
- Сигнатуры
- Репутационные списки, TI и т.д.

РЕАГИРОВАНИЕ

Реагирование на выявленные инциденты ИБ в режиме реального времени

АНАЛИТИКА И УПРАВЛЕНИЕ

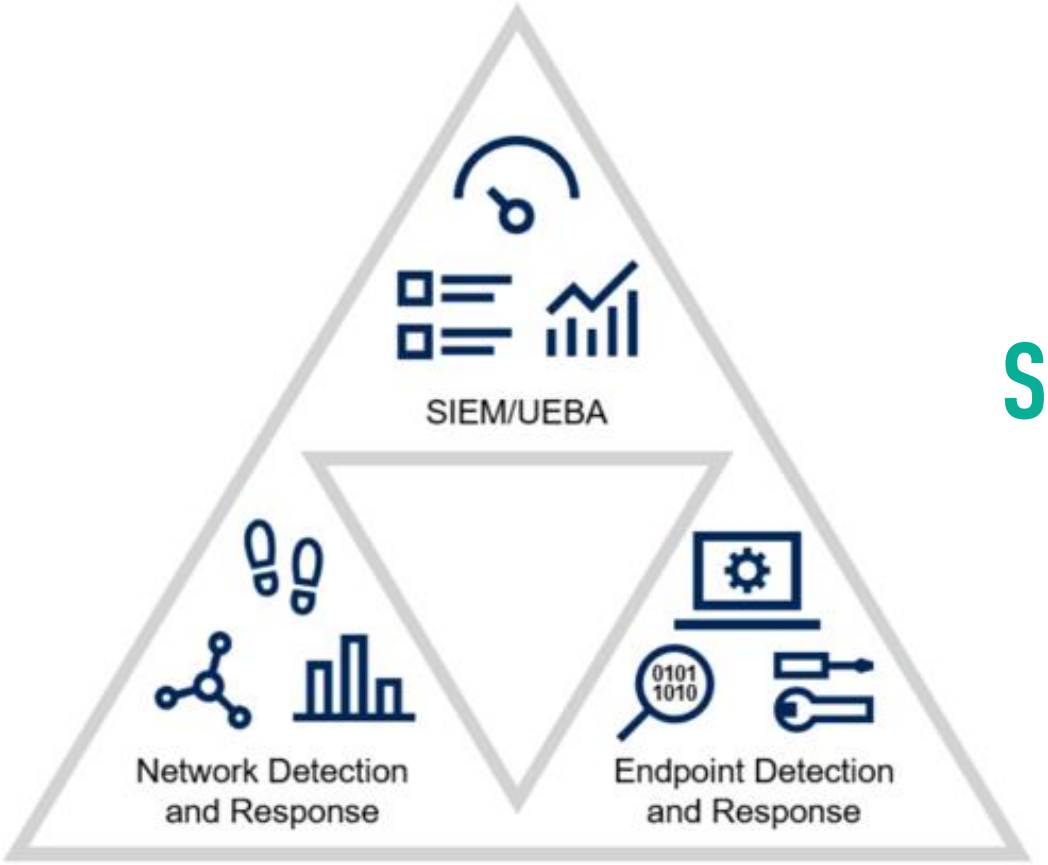
Быстрый поиск, дашборды, выгрузки

СЕКРЕТНЫЕ «ФИЧИ»

ML, эвристика, корреляции и т.д.

ДЛЯ ВНУТРЕННЕГО SOC (1/2)

ГАРДА
ТЕХНОЛОГИИ

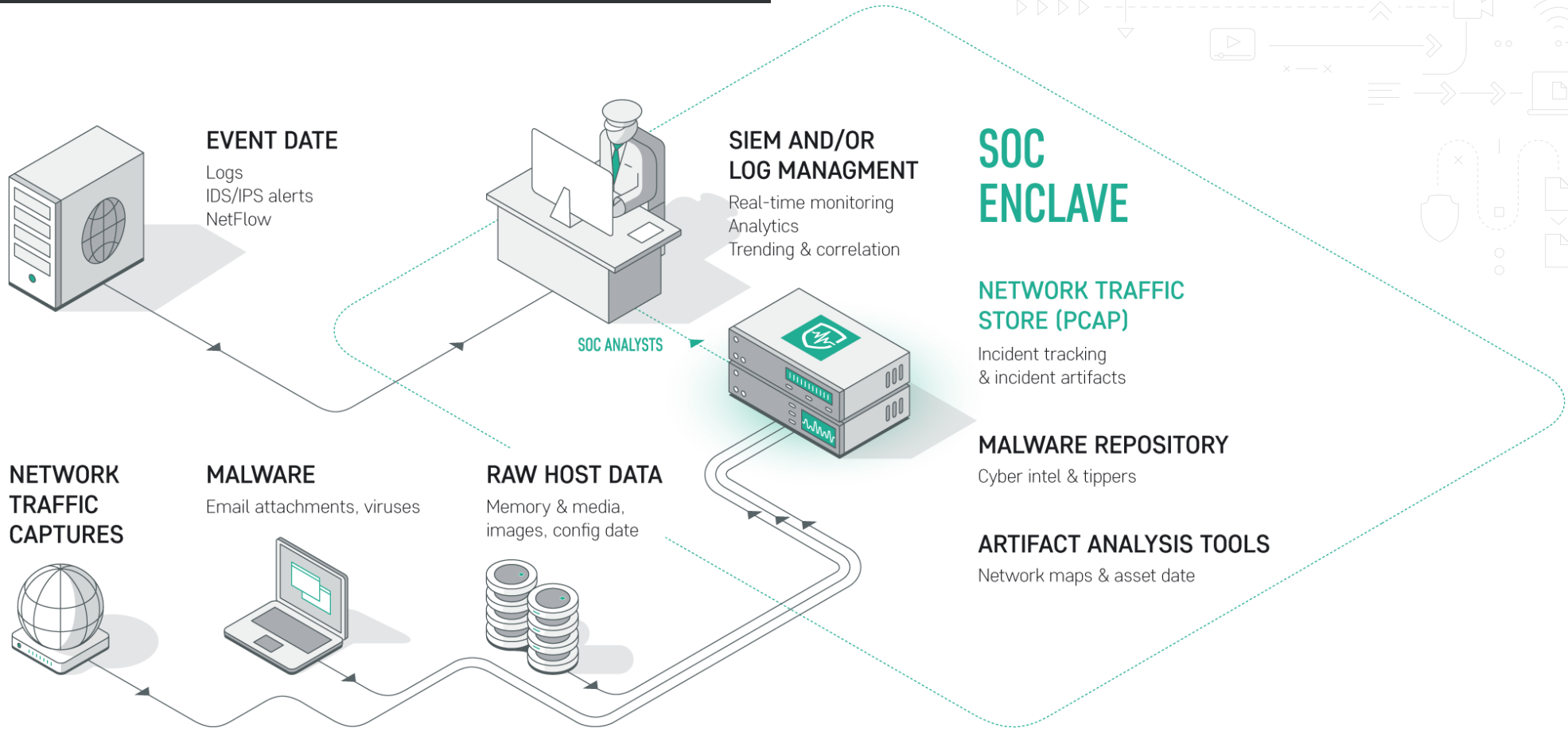


SOC Visibility Triad

*GARTNER

ДЛЯ ВНУТРЕННЕГО SOC (2/2)

ГАРДА
ТЕХНОЛОГИИ



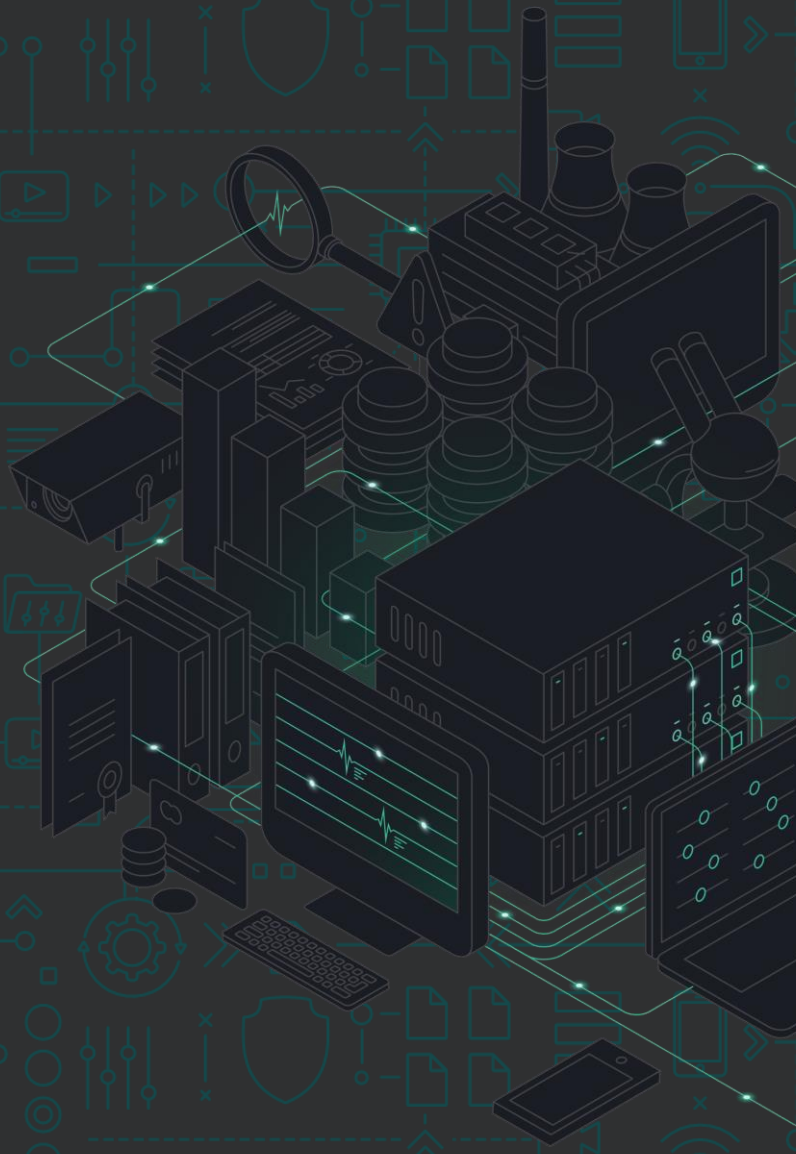
*MITRE

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

ГАРДА МОНИТОР

ВЫЯВЛЕНИЕ УГРОЗ И РАССЛЕДОВАНИЕ СЕТЕВЫХ ИНЦИДЕНТОВ



ЗАЧЕМ НУЖЕН «ГАРДА МОНИТОР»

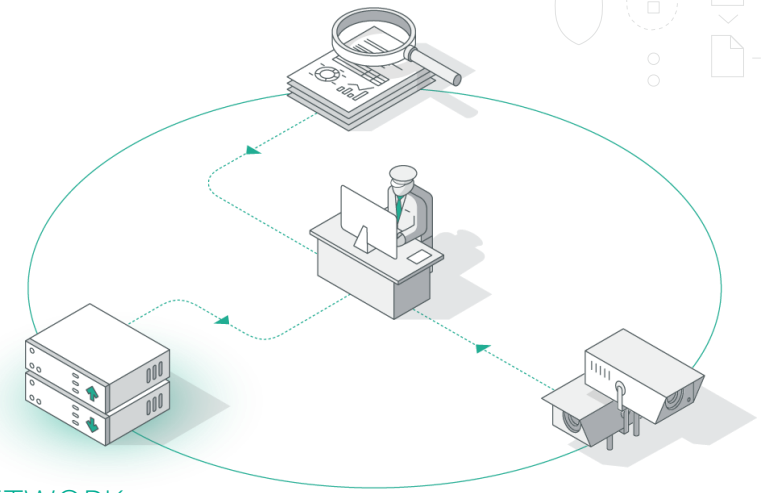
ГАРДА

ТЕХНОЛОГИИ

ГАРДА МОНИТОР = NTA + IDS + NFT + EBA

- Видеть сеть в крупной компании, когда недостаточно endpoint
- Защита от администраторов
- Когда антивирус – это уже поздно, а FW – пропустил угрозу
- Незаменим в расследованиях и при доказывании
- Поведенческий анализ по совокупности факторов
- 4+ технологии и все в одном окне
- Много нестандартных, мобильных или IoT устройств

АНАЛИЗ ЛОГОВ – **SIEM**



NETWORK
АНАЛИЗ СЕТЕВОГО ТРАФФИКА - NTA

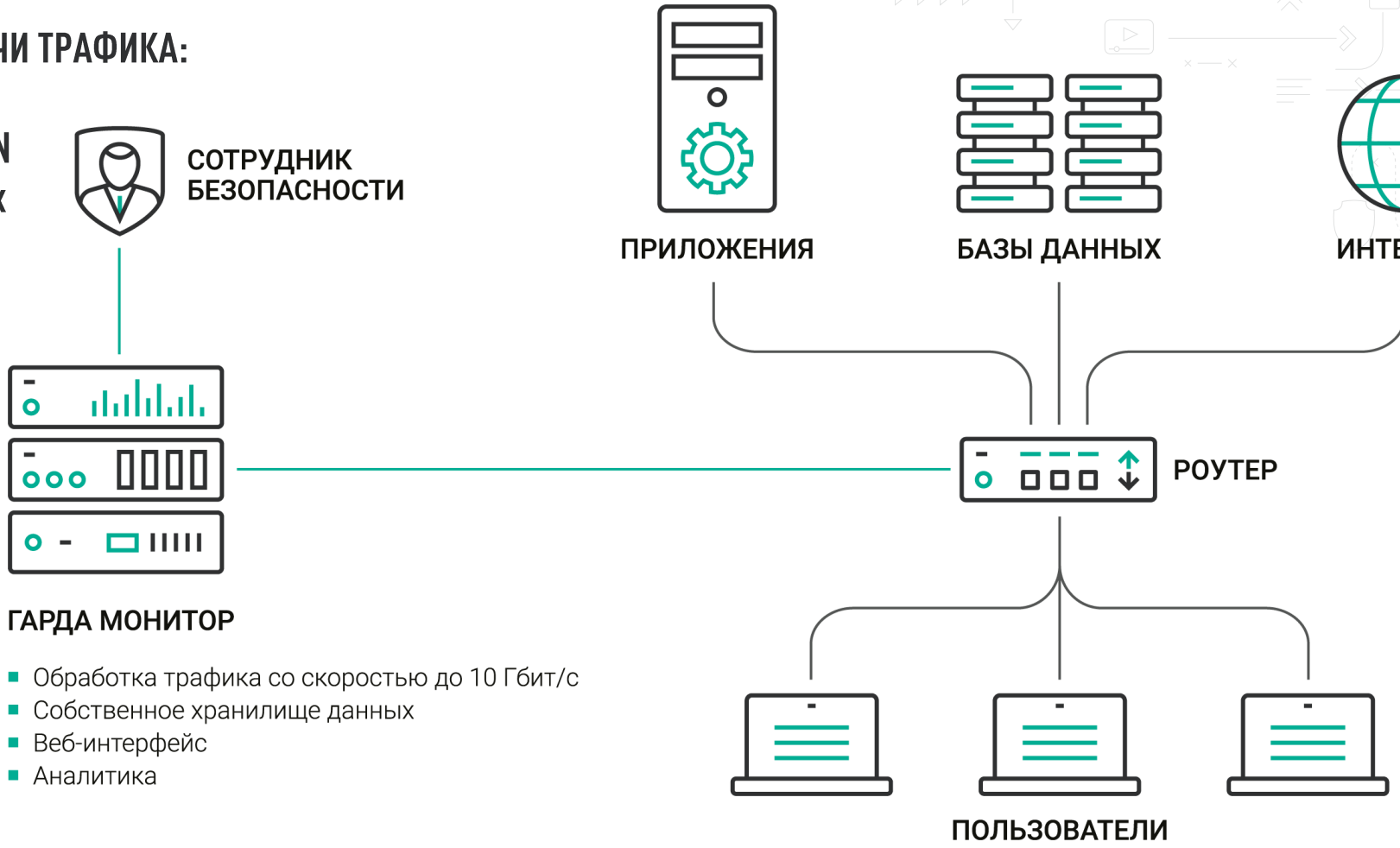
АНАЛИЗ АКТИВНОСТЕЙ НА КОНЕЧНЫХ ТОЧКАХ - **EDR**

СХЕМА

ГАРДА ТЕХНОЛОГИИ

СПОСОБЫ ПОДАЧИ ТРАФИКА:

- SPAN/ERSPAN
- netFlow/IPFIx
- ICAP
- GRE
- Агенты



ГАРДА МОНИТОР

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

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

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 и сканирования на периметре и внутри сети

Автоматически строит **Карту межсетевых взаимодействий**

Обеспечивает **тотальную запись** сетевых потоков, с возможностью выгрузки

Анализирует события, определяет поведенческие отклонения (**UBA**), фиксирует доменные авторизации на машинах

Позволяет выполнять **расследования** сетевых инцидентов

Обнаруживает и оповещает о **новых устройствах и сервисах**

ИНСТРУМЕНТ ДЛЯ ЕЖЕДНЕВНОЙ РАБОТЫ

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 наруше-ниям политик безопасности в компании

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, lateral movement

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 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

ПОЛИТИКИ ВМЕСТО АРМИИ АНАЛИТИКОВ

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'у/URL'у
- Использование уязвимых протоколов
- Использование TOR, VPN
- Использование ПО для удалённого доступа
- «Нерабочий» траффик (Игры, соц. сети)
- Использование DoH/DoT
- Факты «Сетевой разведки»

ДЕТЕКТИРОВАНИЕ ПРОТОКОЛОВ DARKNET, P2P, АУТЕНТИФИКАЦИИ, ОБЛАЧНЫХ СЕРВИСОВ, ПРОТОКОЛОВ УДАЛЁННОГО 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

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ #1

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 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 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

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ #4

ГАРДА ТЕХНОЛОГИИ

ПРОМЫШЛЕННЫЕ ПРОТОКОЛЫ

- MODBUS
- OPC UA
- S7Comm

В БЛИЖАЙШИХ ПЛАНАХ

- IEC-60870-5-101 & 104
- DNP3
- IEC 61850/MMS
- BACnet
- PROFINET
- GOOSE

Готовы рассматривать необходимые Вам протоколы в качестве приоритетных к доработке

ПРЕИМУЩЕСТВА АПК «ГАРДА МОНИТОР»

ГАРДА ТЕХНОЛОГИИ

- Высокая производительность: анализ трафика со скоростью 10Гбит/с на модуль, хранение более 100Тб данных
- Различные способы подачи трафика (SPAN, NetFlow, Агенты, GRE, ICAP)
- Поддержка Гео-распределенной инфраструктуры
- 250+ поддерживаемых протоколов, их постоянное дополнение, глубокий анализ
- 4 глобальных технологии в одном решении + полезные «мелочи»
- Автоматизация всех модулей (политики)
- Библиотека предустановленных политик выявления инцидентов
- Возможности интеграции/импорта/экспорта (FEEDs, списки, SIEM и др.)
- Простота внедрения без нарушений топологии сети
- Не требует сторонних лицензий
- Построение визуальных отчетов «на лету»
- Партнерство с ведущими поставщиками сведений об угрозах
- [СКОРО] Активное реагирование (блокировки)
- [СКОРО] Произвольный Dashboard-мониторинг

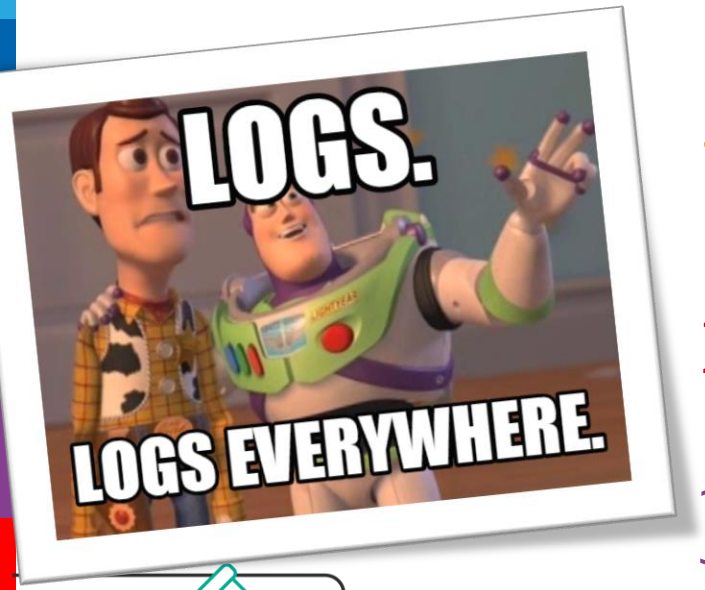
ТОР 2020 НАХОДОК В СЕТИ КОМПАНИИ

ГАРДА ТЕХНОЛОГИИ

- УСТАРЕВШИЕ, УЯЗВИМЫЕ ПРОТОКОЛЫ
- НЕШИФРОВАННЫЙ ТРАФИК С «СЕРКРЕТАМИ»
- МЕДЛЕННО РАЗВИВАЮЩИЕСЯ ЗАРАЖЕНИЯ
- ОБХОД КОРПОРАТИВНЫХ ОГРАНИЧЕНИЙ
- НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ

ЗАЧЕМ «ГАРДА МОНИТОР», КОГДА ЕСТЬ SIEM

ГАРДА ТЕХНОЛОГИИ



1 ГАРДА МОНИТОР – НЕЗАМЕНИМЫЙ ИСТОЧНИК СОБЫТИЙ ДЛЯ SIEM

2 В SIEM НЕ ВСЕГДА ВОЗМОЖНЫ РЕТРОСПЕКТИВНЫЕ РАССЛЕДОВАНИЯ

3 В SIEM НЕТ ВСЕХ ТЕХНОЛОГИЙ АНАЛИЗА ТРАФИКА

4 ДЛЯ ВЫЯВЛЕНИЯ АТАК В SIEM НУЖНО ИНТЕГРИРОВАТЬ КУЧУ ВСЕГО

5 НЕ ПОПАЛО В ЛОГ (СРАБОТКУ) В SIEM – ВЫ ОБ ЭТОМ НЕ УЗНАЕТЕ

ЗАЧЕМ «ГАРДА МОНИТОР», КОГДА ЕСТЬ FW+IDS

ГАРДА ТЕХНОЛОГИИ

1 ЕСЛИ НУЖНА ЗАПИСЬ, РЕТРОСПЕКТИВА И РАССЛЕДОВАНИЕ

2 ДЛЯ ПРОВЕРКИ, ВСЁ ЛИ РАБОТАЕТ КАК НАДО

3 ДЛЯ «СКЛЕИВАНИЯ» ПОТОКОВ ТРАФИКА
И СРАБОТОК ПО УГРОЗАМ

4 МОНИТОРИНГ И ПРИМЕНЕНИЯ ПОЛИТИК
ДЛЯ ВНУТРЕННИХ СЕГМЕНТОВ

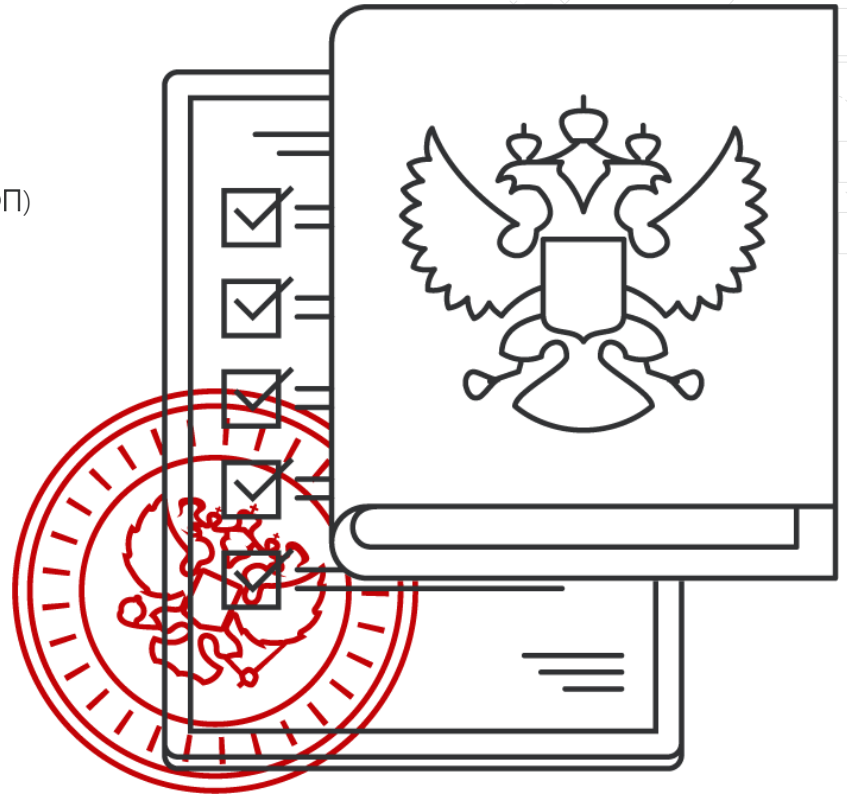
5 КОГДА НЕДОСТАТОЧНО ТОЛЬКО
ТЕХНОЛОГИИ СИГНАТУРНОГО АНАЛИЗА

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

ГАРДА ТЕХНОЛОГИИ

СИСТЕМА ПОМОГАЕТ ВЫПОЛНИТЬ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

- 152-ФЗ «О персональных данных» (ИСПДн)
- 8-ФЗ «Обеспечение доступа к информации государственных органов» (ИСОП)
- 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ГИС)
- GDPR (Европейский регламент по защите ПДн)
- 187-ФЗ «О безопасности КИИ»
- Банковские требования: 382-П, 683-П, 684-П, ГОСТ 57580
- Включено в Единый реестр российских программ Минцифры РФ
- Международные стандарты: NIST SP 800-61, CIS TOP-20 Controls, MITRE ATT&CK



ОБХОД КОРПОРАТИВНЫХ ОГРАНИЧЕНИЙ

ГАРДА ТЕХНОЛОГИИ

КЕЙС №1

СИТУАЦИЯ

Использование средств удаленного управления (TeamViewer, VNC и т.д.) запрещено.
Установка и запуск блокируется политиками.

Уже на этапе пилотного проекта в сети компании обнаружено множество соединений TeamViewer.

	Дата и время	Группа пр...	Протокол	IP отправителя	IP получателя	Порт от...	Порт п...	Аккаунт отправит...
⌄	28.11.2020 18:15:57	Удаленно...	TCP ▸ TEAMVIEWER	192.168 [redacted]	37.252.254.181	62743	5938	v[redacted]@[redacted]
⌄	28.11.2020 18:15:56	Удаленно...	TCP ▸ TEAMVIEWER	192.168 [redacted]	37.252.254.181	62742	5938	v[redacted]@
⌄	26.11.2020 12:49:48	Удаленно...	TCP ▸ TEAMVIEWER	192.168 [redacted]	213.227.168.134	57549	5938	v[redacted]@
⌄	26.11.2020 12:49:47	Удаленно...	TCP ▸ TEAMVIEWER	192.168 [redacted]	188.172.233.178	57548	5938	v[redacted]@

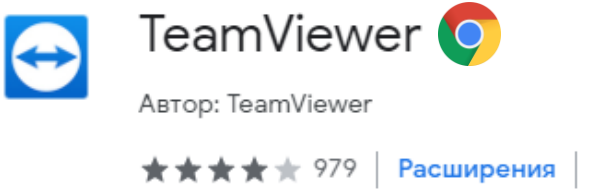
ОБХОД КОРПОРАТИВНЫХ ОГРАНИЧЕНИЙ

ГАРДА ТЕХНОЛОГИИ

КЕЙС №1

РАССЛЕДОВАНИЕ

Сотрудники обходят ограничение
используя расширения для браузера Google Chrome.



РЕЗУЛЬТАТ ВНЕДРЕНИЯ АПК «ГАРДА МОНИТОР»

автоматическое обнаружение и контроль попыток
использования средств удаленного управления ПК.

Служба ИБ видит использование всех популярных
протоколов удаленного управления в корпоративной сети
вне зависимости от способа их запуска на ПК пользователя.

ВРЕДОНОСНЫЕ СОЕДИНЕНИЯ

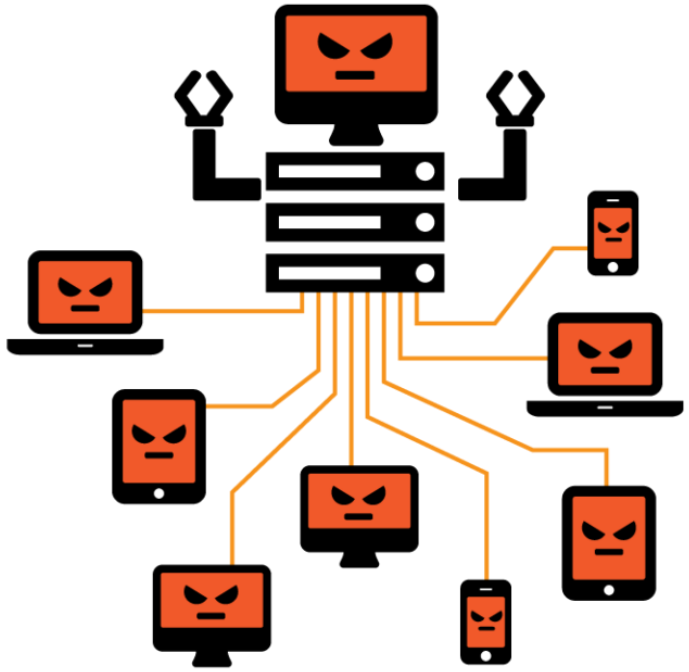
ГАРДА
ТЕХНОЛОГИИ

КЕЙС №2

СИТУАЦИЯ

В корпоративной сети компании разрозненный парк пользовательских устройств.

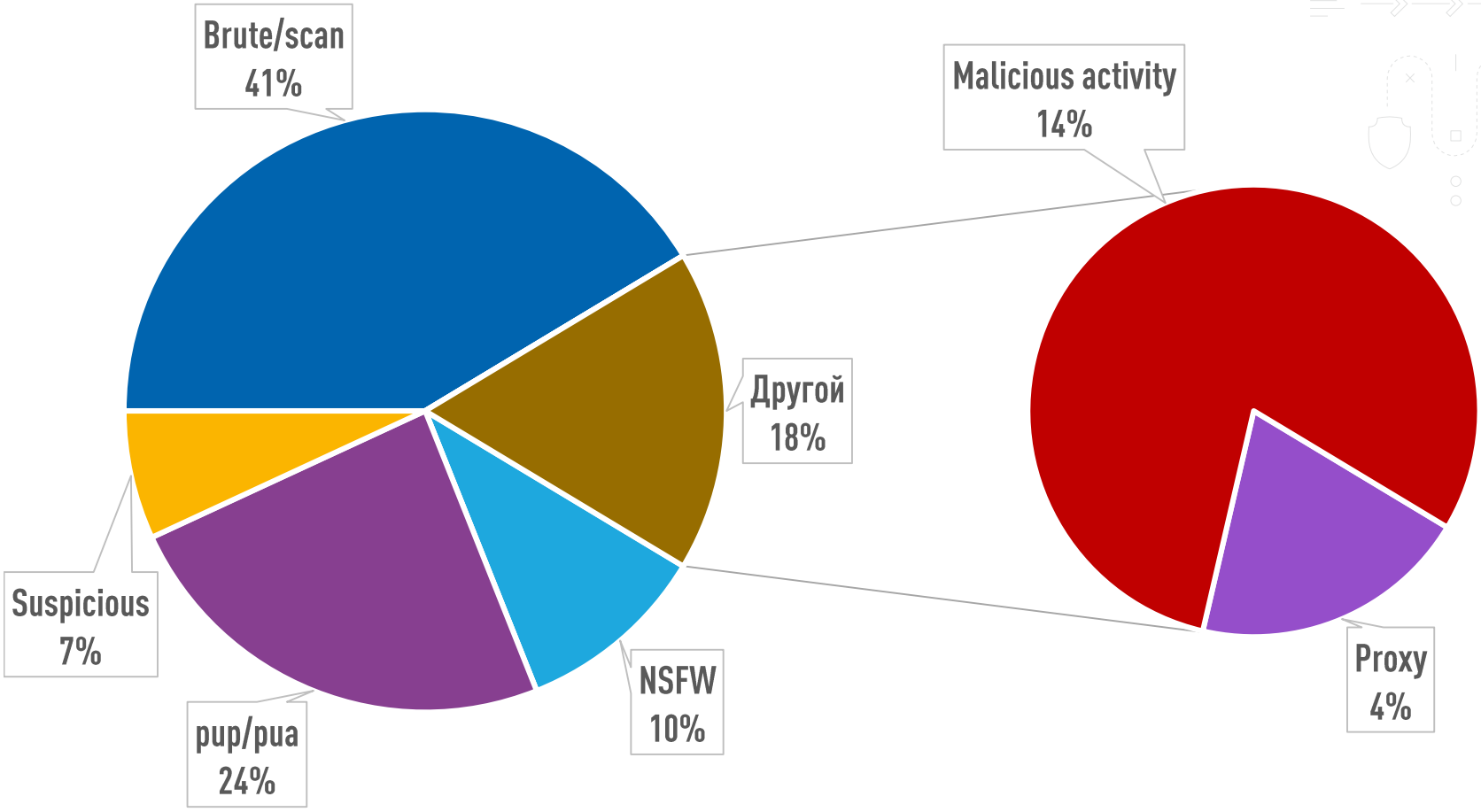
Уже на этапе пилотного проекта в сети обнаружены соединения с IP-адресами командных центров ботнета.



ВРЕДОНОСНЫЕ СОЕДИНЕНИЯ

ГАРДА ТЕХНОЛОГИИ

КЕЙС №2



ВРЕДОНОСНЫЕ СОЕДИНЕНИЯ

КЕЙС №2

РАССЛЕДОВАНИЕ

Несколько мобильных устройств и ПК сотрудников заражены вредоносным ПО.

РЕЗУЛЬТАТ ВНЕДРЕНИЯ АПК «ГАРДА МОНИТОР»

Служба ИБ предотвратила дальнейшее распространение и активацию ВПО.

Служба ИБ в автоматическом режиме обнаруживает вредоносную и подозрительную активность в корпоративной сети.

АНОМАЛЬНАЯ АКТИВНОСТЬ

ГАРДА ТЕХНОЛОГИИ

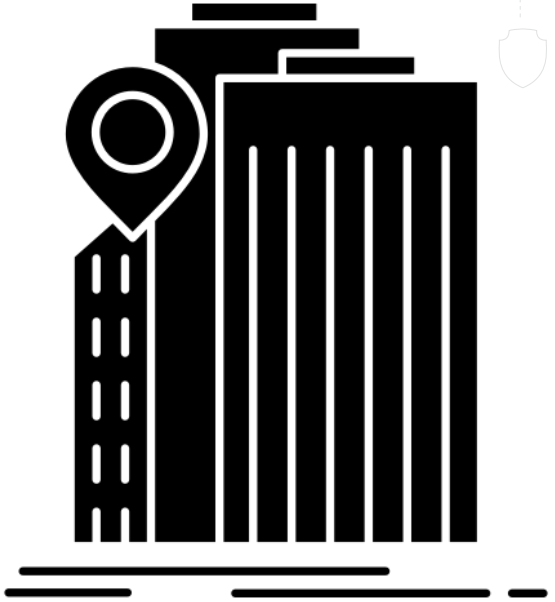
КЕЙС №3

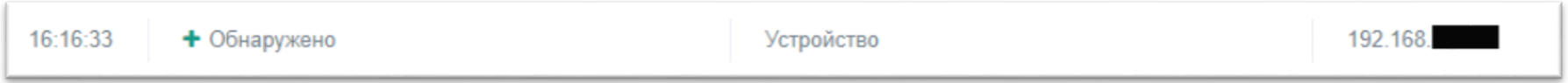
СИТУАЦИЯ

В компании, (гос. сектор) используется большое количество изолированных подсетей с критичными сервисами.

ПИЛОТНЫЙ ПРОЕКТ

Обучение системы.
Обнаружен новый хост в одном из контуров.
Обнаружена аномальная SSH-активность хоста.





АНОМАЛЬНАЯ АКТИВНОСТЬ

КЕЙС №3

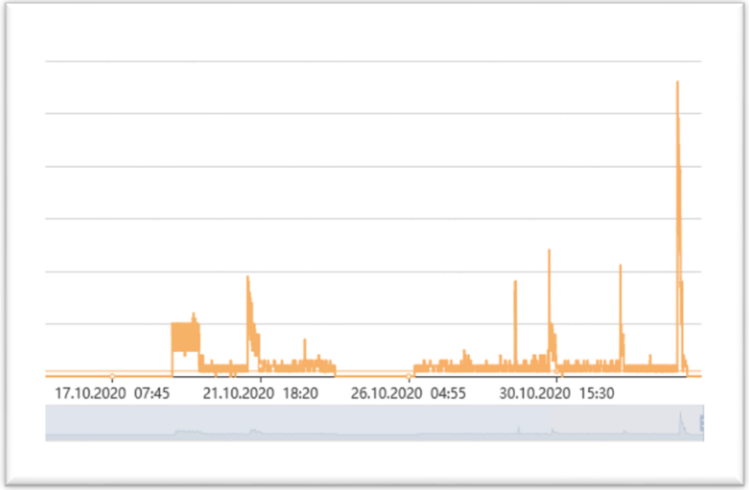
РАССЛЕДОВАНИЕ

Сотрудник использовал revers-SSH соединение для доступа к своей машине внутри корпоративной сети.

РЕЗУЛЬТАТ ВНЕДРЕНИЯ АПК «ГАРДА МОНИТОР»

Служба ИБ предупредила неконтролируемый доступ к критичному сегменту компании и снизила риск её компрометации.

Служба ИБ обнаруживает ранее не видимые инциденты безопасности, контролирует все сетевые потоки и обнаруживает аномальную активность в сети.



НАШ ПОДХОД К ПИЛОТНЫМ ПРОЕКТАМ

ГАРДА ТЕХНОЛОГИИ

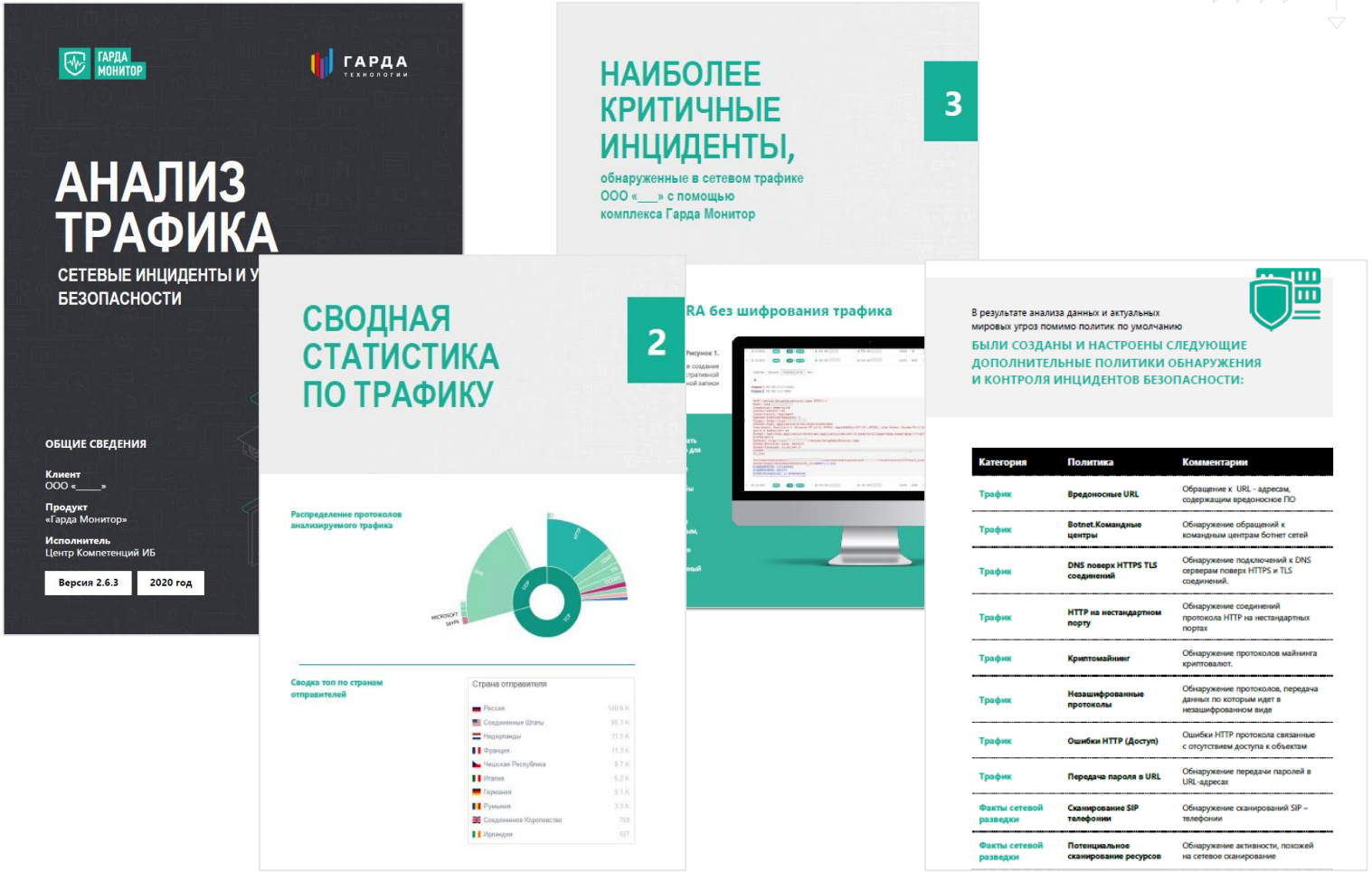
ФОРМИРОВАНИЕ ПЕРЕЧНЯ ЗАДАЧ НА ПИЛОТ, ЗАПОЛНЕНИЕ ОПРОСНОГО ЛИСТА

РАЗВЕРТЫВАНИЕ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА НА СЕТИ ЗАКАЗЧИКА

НАКОПЛЕНИЕ ДАННЫХ, АНАЛИЗ ТРАФИКА, ВЫЯВЛЕНИЕ УГРОЗ, ОПОВЕЩЕНИЕ О КРИТИЧНЫХ ИНЦИДЕНТАХ

ИТОГОВЫЙ ОТЧЕТ И РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ УРОВНЯ БЕЗОПАСНОСТИ

ОТЧЁТ



ГАРДА ТЕХНОЛОГИИ

SECURITY CHECK UP ВАШЕЙ СЕТИ:

- Описание ключевых рисков
- Сводка актуальных угроз
- Рекомендации

ДЕМО

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

info@gardatech.ru
+7 (831) 422 12 21
gardatech.ru

УДАЛЕННОЕ УПРАВЛЕНИЕ ЧЕРЕЗ БРАУЗЕР

ПЕРИМЕТР

ГАРДА ТЕХНОЛОГИИ

ЗАДАЧА

Как правило, службой ИБ запрещает сотрудникам компании пользоваться приложениями для удаленного управления (TeamViewer, VNC и т.д.), их установка блокируется политиками.
При этом сотрудники обходят это ограничение, используя расширения для браузера Google Chrome.

РЕШЕНИЕ

Гарда Монитор позволяет обнаружить использование средств удаленного доступа вне зависимости от способа их запуска на ПК пользователя.

Домашний ПК

Удаленный доступ в обход политик ИБ

Офисный ПК

ПОПЫТКА ЗАЙТИ НА ФИШИНГОВЫЙ САЙТ

ПЕРИМЕТР

ГАРДА ТЕХНОЛОГИИ

ЗАДАЧА

Фишинг – одна из самых больших проблем для компании любого профиля. Сотрудник получает сообщение, ссылка в котором ведет на фишинговую страницу, затем переходит по ссылке и попадает на мошеннический сайт.

РЕШЕНИЕ

Гарда Монитор в автоматическом режиме обнаруживает подозрительную активность в сети компании, в том числе и такую как переход по фишинговым ссылкам или загрузка вредоносного ПО

СПАСИБО ЗА ВНИМАНИЕ!

ГАРДА МОНИТОР

ГАРДА ТЕХНОЛОГИИ

info@gardatech.ru
+7 (831) 422 12 21
gardatech.ru