Охота на хакера в сетевом трафике: почему нужен целый арсенал технологий

Станислав Грибанов,
группа компаний «Гарда»

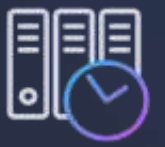
ГАРДА

Многолетний опыт в высокоскоростном снятии и анализе трафика

«Гарда» занимает четвертое место среди крупнейших российских поставщиков средств сетевой защиты[1] и третье место – среди поставщиков решений по защите данных.[2]

Собственный сервис «Гарда TI Feeds», выявление ранее неизвестных сетевых и DDoS-атак

Более 10 лет экспертизы в высокоскоростном снятии и обработке сетевого трафика



Технологии собственной разработки:

- специализированная файловая система и база данных для хранения сырого трафика
- высокоскоростной модуль снятия сетевого трафика
- компоненты глубокого анализа сетевого трафика (DPI) и сетевой телеметрии (Netflow)
- протокол высокоскоростной индексации данных
- система обогащения индексированных данных

[1] CNews Security: Крупнейшие отечественные поставщики средств сетевой защиты

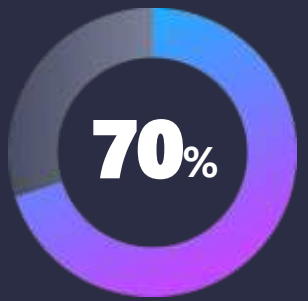
[2] CNews Security: Крупнейшие поставщиками средств защиты данных

Изменение тренда ИБ

ГАРДА

100% защита от взлома

Оперативное детектирование проникновения и реагирование на него



уязвимостей эксплуатировались как уязвимости нулевого дня

3 года хакеры находились в инфраструктуре мобильного оператора SK Telecom T1

194 дня требуется для детектирование проникновения в инфраструктуру IBM

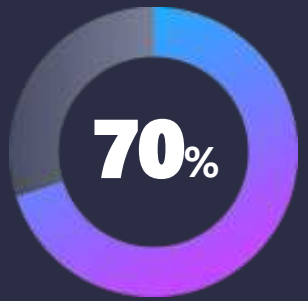
1,9 млрд фунтов ущерба и 6 недель простоя производства Jaguar LandRover

36 процентов от всех проникновений было реализовано через социальную инженерию

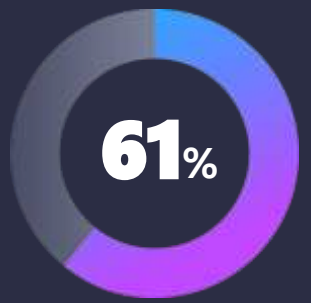
Возможности для сокрытия проникновения в инфраструктуру

ГАРДА

Хосты, не поддерживающие агентов EPP/EDR

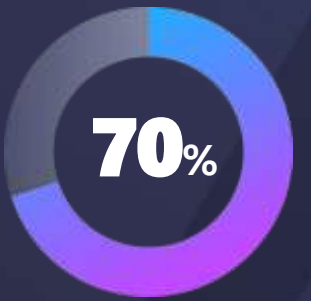


организаций имеют уязвимые IoT- устройства[1]

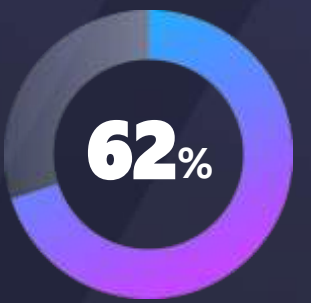


клиентов, использующих IDS-системы, отмечают их низкую точность и большое количество ложных срабатываний[3]

Атаки в горизонтальном зашифрованном трафике



организаций как минимум дважды становились жертвами атак в зашифрованном трафике[2]

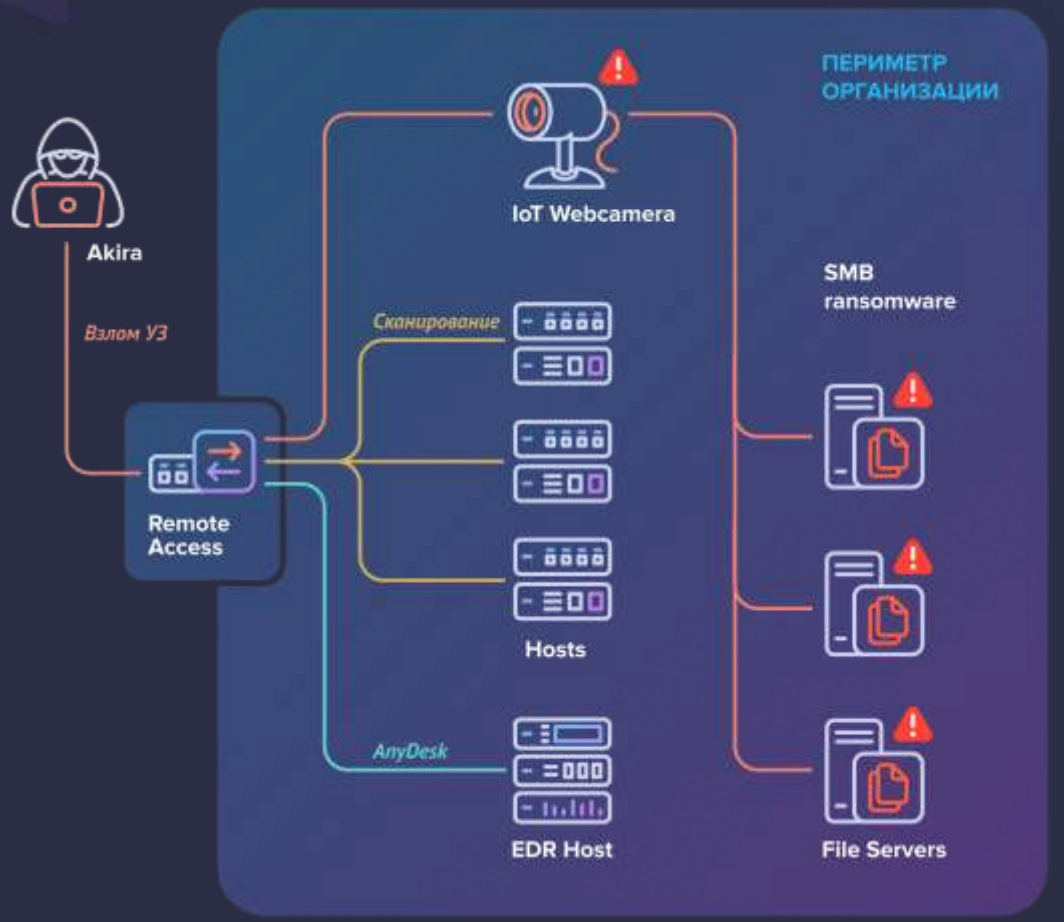


За детектированных атак были без ВПО с использованием легитимных инструментов (LOTL)

1. https://stellarcyber.ai/wp-content/uploads/2023/03/esg-the-evolving-role-of-ndr.pdf
2. https://stellarcyber.ai/wp-content/uploads/2023/03/esg-the-evolving-role-of-ndr.pdf
3. https://www.enea.com/insights/state-of-network-threat-detection/
4. https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023?utm_source=Securitylabru

IoT-устройства как вектор атаки

Всего одна уязвимость способна привести к краху всей системы ИБ



Группировка Akira проникла в сеть компании через взлом УЗ удалённого доступа. Был установилен Anydesk, через который злоумышленники подключились к хосту и попытались доставить исходники для ransomware, но EDR заблокировал запуск шифровальщика на Windows. Далее провели сканирование, обнаружив веб-камеру на Linux без EDR. Доставили на нее исходники для сборки шифровальщика и использовали её для подключения к SMB-ресурсам, обойдя защиту, и затем запустили шифрование данных на сетевых дисках.

Атака достигла своей цели из-за отсутствия обновлений прошивки и невозможности защитить на IoT-устройства средствами EDR.

0-day уязвимости для преодоления периметра

- Атака хакеров на критическую инфраструктуру США, через 0-day уязвимость CVE-2025-20362/333 в Cisco ASA
- 0-day уязвимость CVE-2025-8088 в WINRAR позволяет устанавливать malware поддерживающую коммуникацию C&C
- Критическая уязвимость CVE-2025-9242 в NGFW WatchGuard позволяет удаленно запускать вредоносный код
- 0-day уязвимость CVE-2025-7775 в NetScaler ADC и NetScaler Gateway позволяет удаленно запускать вредоносный код

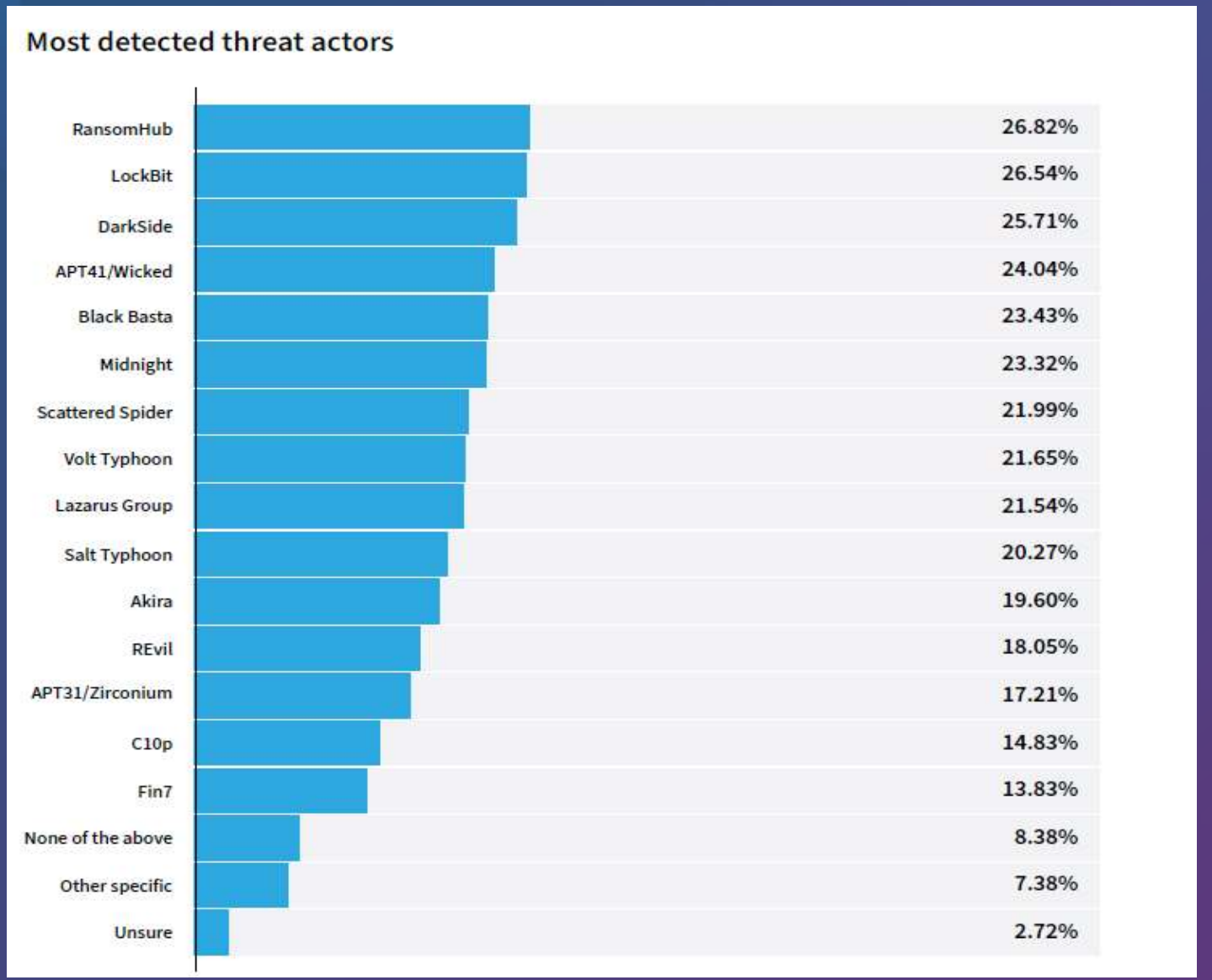
US sounds alarm over hackers targeting Cisco security devices

By **Raphael Satter**

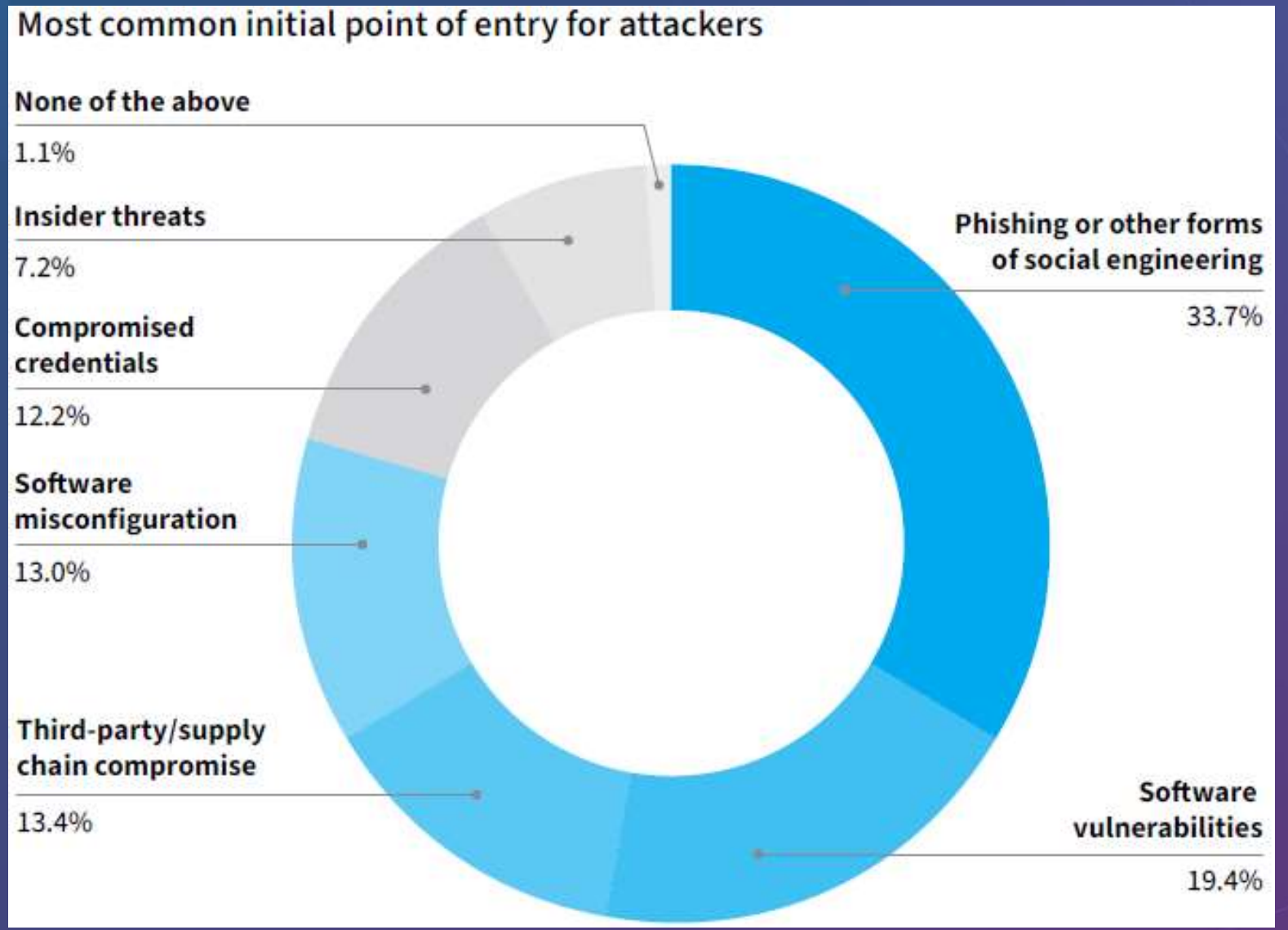
September 26, 2025 12:24 AM GMT+3 · Updated September 26, 2025

The logo of U.S. networks giant Cisco Systems is seen in front of their headquarters in Issy-les-Moulineaux, near Paris, France August 6, 2022. REUTES/Sarah Meyssonnier/File Photo Purchase Licensing Rights

Активность APT-группировок



Проникновение в инфраструктуру



Как защищаться?

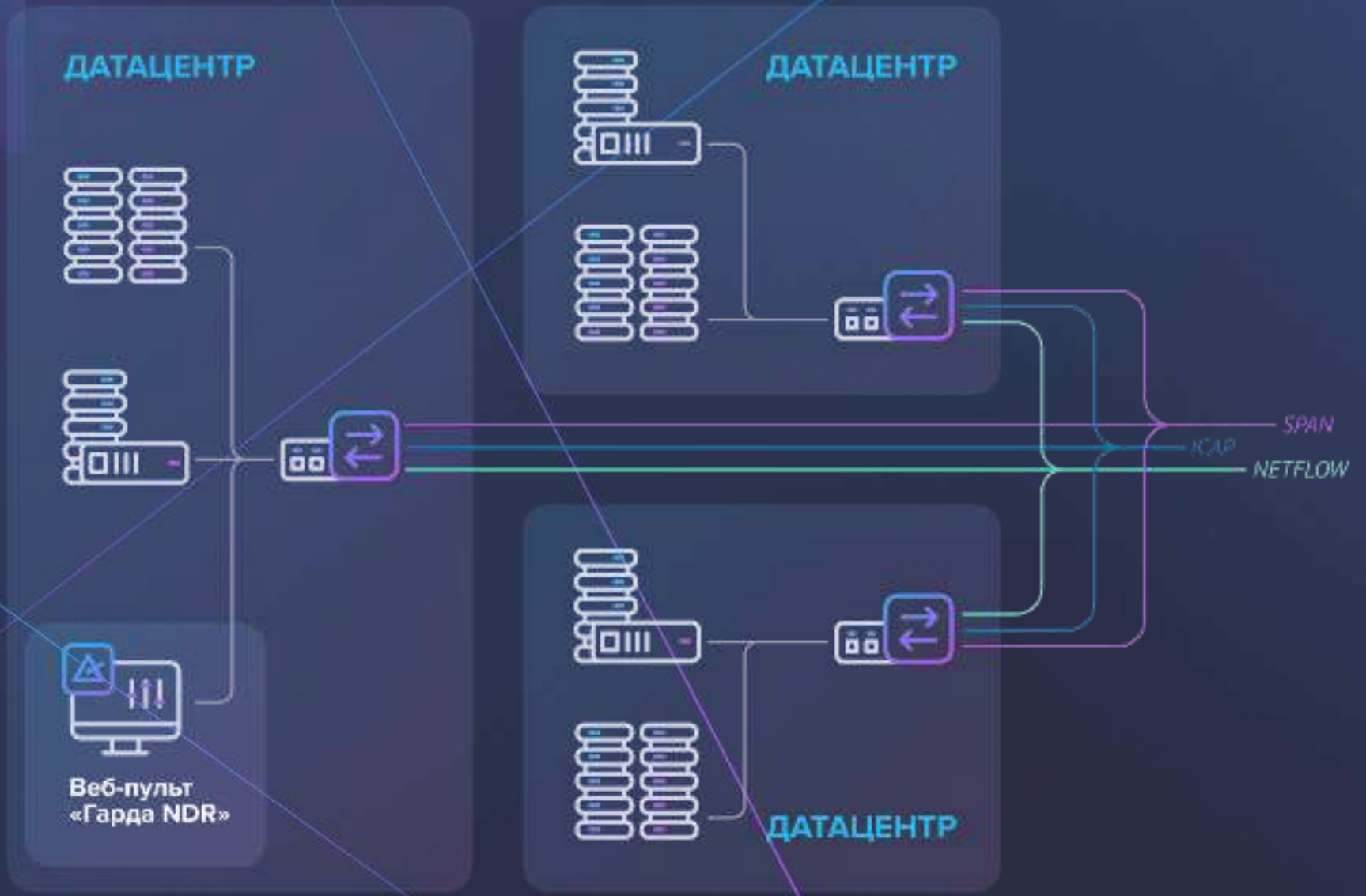
Направления сетевого трафика

ГАРДА

DPI

NetFlow

Видимость всей сети



NetFlow для видимости в ЦОД и филиалах

NetFlow это протокол статистики сетевых соединений, позволяет детектировать угрозы в сетях, с которых сложно или невозможно получить копию сетевого трафика.

ЦОД обрабатывает огромные потоки данных в сотни/тысячи Гбит/с, сложность получения копии трафика такого объема делают Netflow единственным источником данных о сети в ЦОД.

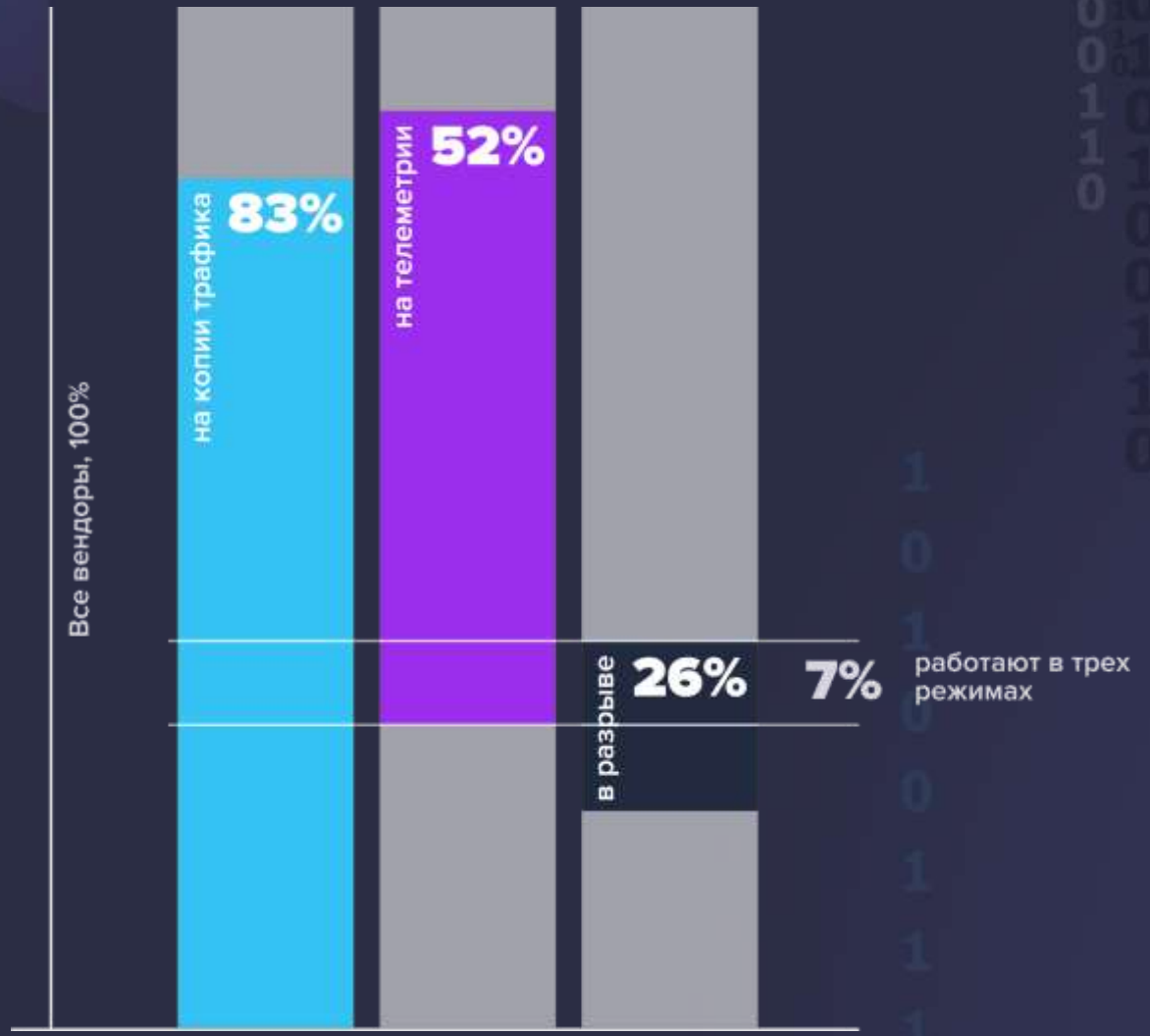
Георасределенные децентрализованные сети с большим количеством отдельных точек выхода в интернет (магазины, небольшие офисы, образовательные учреждения, медицинский учреждения и т.п.), а снять копию трафика (SPAN) бывает сложно из-за устаревшего оборудования или ограничений каналов связи или сетевой топологии.

По данным исследования группы компаний «Гарда» более 50 % решений класса NDR на мировом рынке работают с сетевой телеметрией (Netflow и аналоги), что доказывает достаточность такого типа данных для успешного детектирования угроз.

Источники телеметрии

Для сбора телеметрии служит широкий спектр оборудования разных производителей от Enterprise Cisco, Huawei, Eltex, Juniper, Extreme, Fortinet до SoHo Mikrotik, D-Link, TP-Link, Zyxel, Asus и другие.

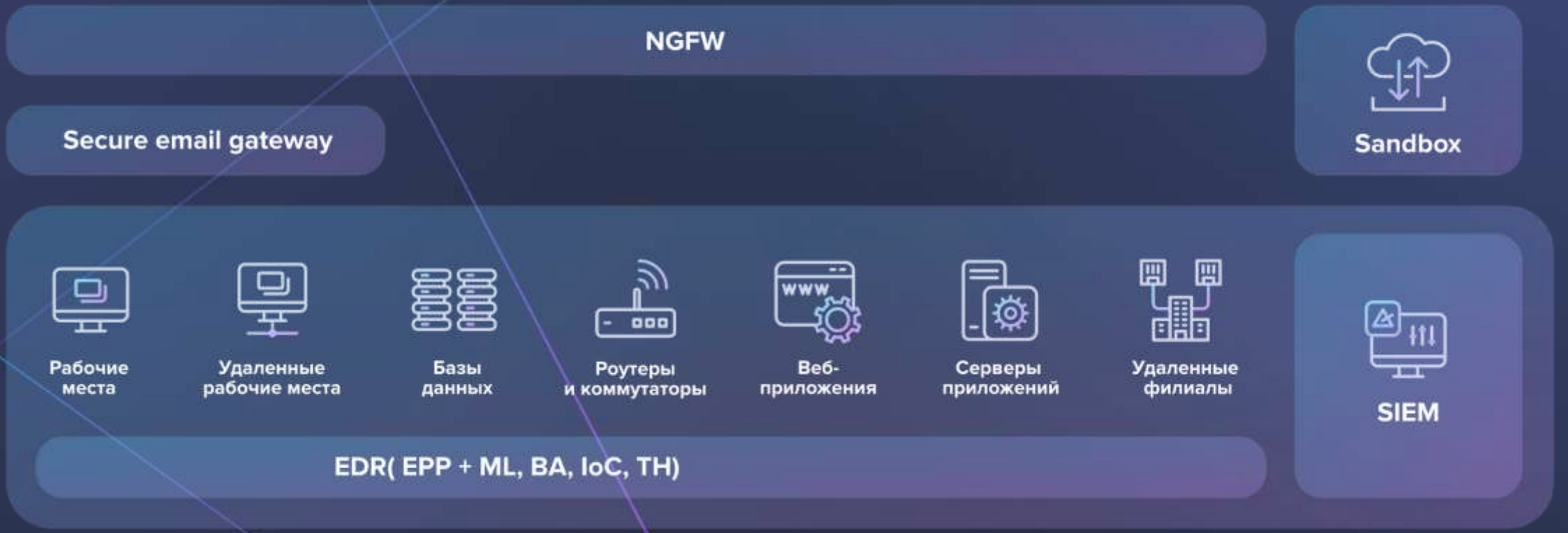
Использование источников трафика в сегменте NDR в мире



Как обеспечить безопасность?

ГАРДА

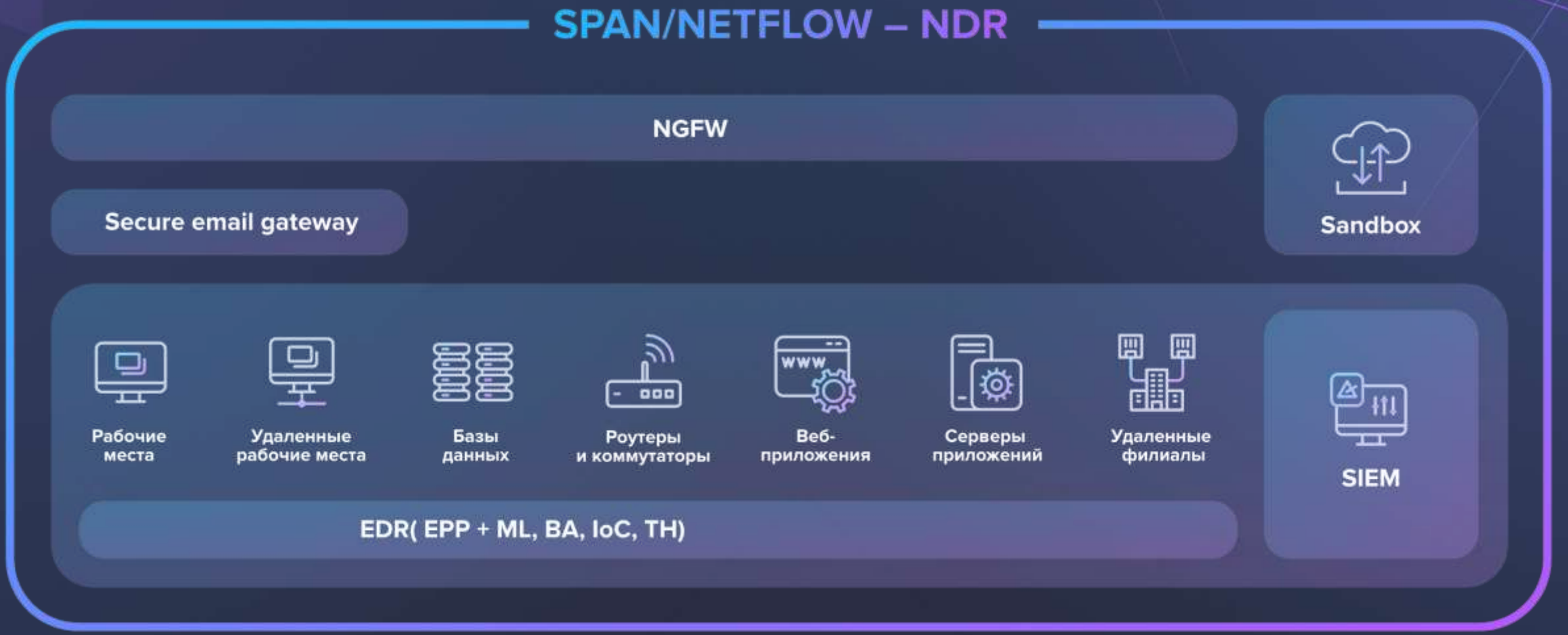
Стандартная система защиты



Анализ всего сетевого трафика

ГАРДА

Продвинутая система защиты



Как находить известные угрозы в сети?

Базовые технологии анализа сетевого трафика (NGIDS)

Детектирование известных угроз

- Сигнатуры IDS
- Репутационные списки TI
- Уязвимые протоколы

- **Различные атаки и уязвимости**
- **Инструменты горизонтального перемещения**
- **Инструменты Red team**
- **Инструменты с открытым кодом, используемые хакерами**
- **Инструменты с закрытым кодом, используемые хакерами**

Как эффективно использовать IDS?

ГАРДА

Разработка сигнатур

- Собственные сигнатуры
- Исследование сигнатур из открытых источников

Анализ актуальности сигнатур

- Гибкая и многоступенчатая система фильтров
- Применение LLM для определения соответствия сигнатуры угрозе
- Категоризация источников информации об угрозе
- Фильтры по ключевым словам
- Учёт даты последней в песочницах

Анализ эффективности работы

- Органический трафик + дампы (инструменты redteam), собственная база ВПО
- Трафик песочниц
- Актуальные типы атак
- Статический анализ (эффективность/нагрузка)

Собственная система метрик эффективности

Общий рейтинг сигнатуры формируется из:

- рейтинга угрозы
- влияния на производительность

Рейтинг угрозы: множество параметров и весовых коэффициентов

Результат

- Эффективный набор 11,5 тысяч собственных сигнатур: максимум True Positive при минимальном количестве сигнатур
- Снижение False Positive
- Снижение нагрузки на сенсор за счёт учёта влияния на производительность
- Будущее: уникальные наборы сигнатур для разных типов инфраструктур

Детектирование хакерских инструментов с закрытым кодом в NDR

- DARP
- Rebirth
- DDoS HsFlood
- Impacket(guid)
- CodRun
- TheClient
- ToneShell Lizar/DiceLoader APT FIN7
- RadX RAT
- wmRAT
- Xeno-RAT
- GoProxy
- Talisman PlugX
- PureLogs
- Doser C#RAT
- RedDriver
- Broext (APT Oilrig)
- JanelaRAT
- Menorah (APT34)
- GoGateway proxy
- BitRAT
- SheetRat
- DynamicRAT
- DDosia

Репутационные списки Гарда TI

ГАРДА

C&C Botnet host

данные управляющих центров бот-сетей, ранжированных по категориям и типам ботнетов (mirai, mozi, conficke и т.д.)

Botnet hosts

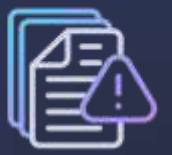
данные об IP и узлах бот-сетей, которые нельзя классифицировать как командные центры

Suspicious hosts

иные IP-адреса узлов, которые попали в списки вредоносных, но не были классифицированы под конкретную категорию.

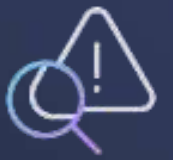
Phishing

DNS и URL-адреса из фишинговых писем



Malware

url-адреса относящиеся к вредоносному ПО



Netflow поддерживает IP и Host

Mining

адреса, домены связанные с майнингом

DNS-over-HTTPS

IP-адреса и хосты, обеспечивающие выполнение DNS-запросов поверх HTTPS

ГАРДА

Защита от угроз, для которых нет заранее известного payload

Как детектировать угрозу, если ее признаки заранее не известны?

ГАРДА

- **Аномальное поведение**
  ML/поведенческий анализ
- **Поймать атакующего в ловушку**
  Deception- honeypot, honeytoken, lure
- **Автоматическая категоризация**
  Машинное обучение
- **Продвинутая аналитика**
  Корреляция не событий, а инцидентов с уровнем критичности и автоматическим скорингом результатов

Горизонтальные перемещения внутри инфраструктуры (Lateral movement)

Использование легальных инструментов (Living off the Land)

Аномальное поведение узлов сети

ГАРДА

Детектирование Living off the Land

Выявление аномалий

- Брутфорс (SSH, RDP, SMB, HTTP, HTTPS, LDAP, SQL) – ML/поведенческий анализ без payload
- DNS/ICMP/SSH и другие туннели ML/поведенческий анализ без payload
- Любые сканирования – ML /поведенческий анализ без payload
- Установление новых IP и портов в сети
- Туннелирование C&C в трафике легальных приложений ML/поведенческий анализ без payload
- Подмена LLMNR_NBT-NS-ответа и ретрансляция SMB ML/поведенческий анализ без payload

  Эксфильтрация данных по каналу управления поведенческий анализ без payload
- Детектирование соединения с командными серверами по зашифрованным каналам без payload
- Распыление пароля SMB, Kerberos поведенческий анализ без payload
- Обнаружение фишинга с вложением или ссылкой поведенческий анализ
- Эксфильтрация данных в репозиторий или облачное хранилище поведенческий анализ
- Эксфильтрация по расписанию ML без payload
- Коммуникации с C&C в любом трафике ML без payload

Детектирование Cobalt Strike HTTPS Jitter 10%

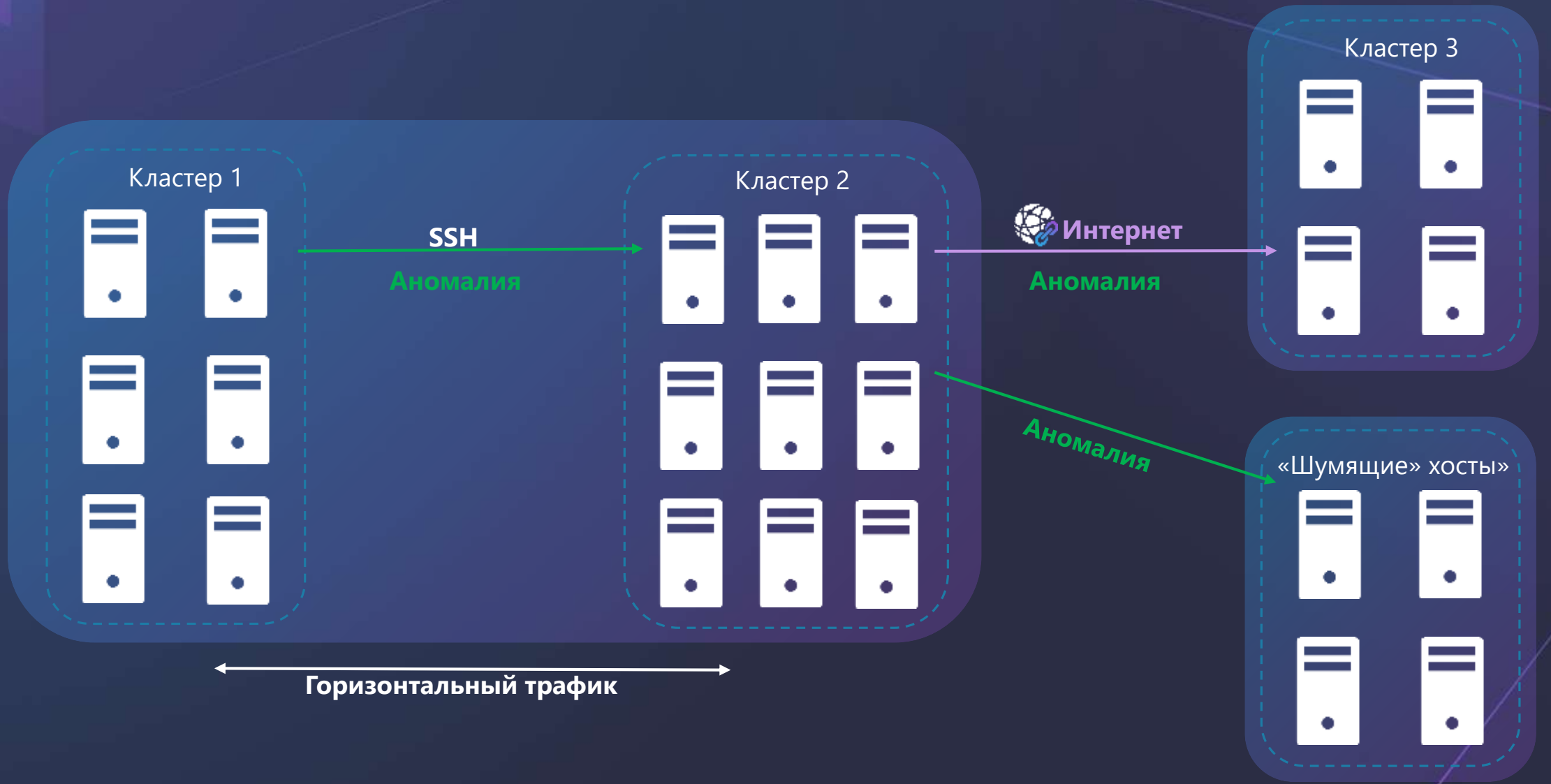
ГАРДА

Гарда NDR детектирует коммуникации ботнетов, Cobalt Strike, Brute Ratel C4, Sliver, Malware, криптомайнинговых хостов

ML-модель | SPAN | NetFlow

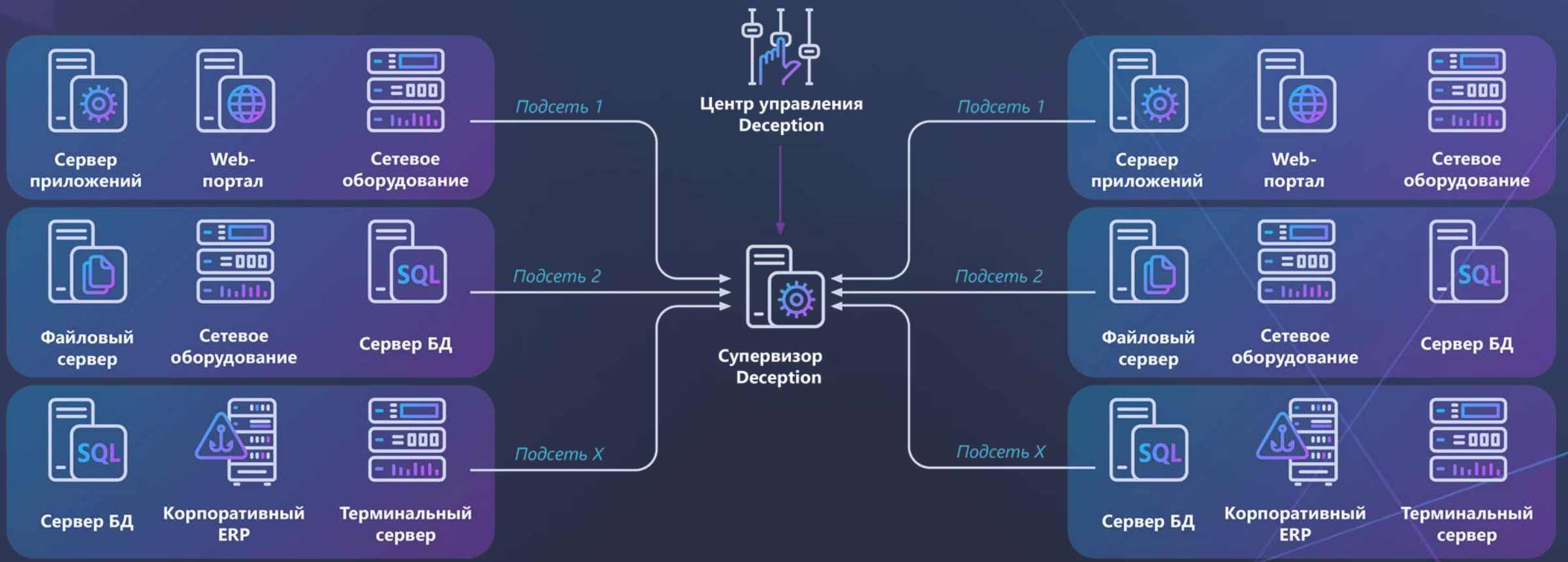
Аномальное поведение узлов сети

ГАРДА



Возможности Deception detection

ГАРДА



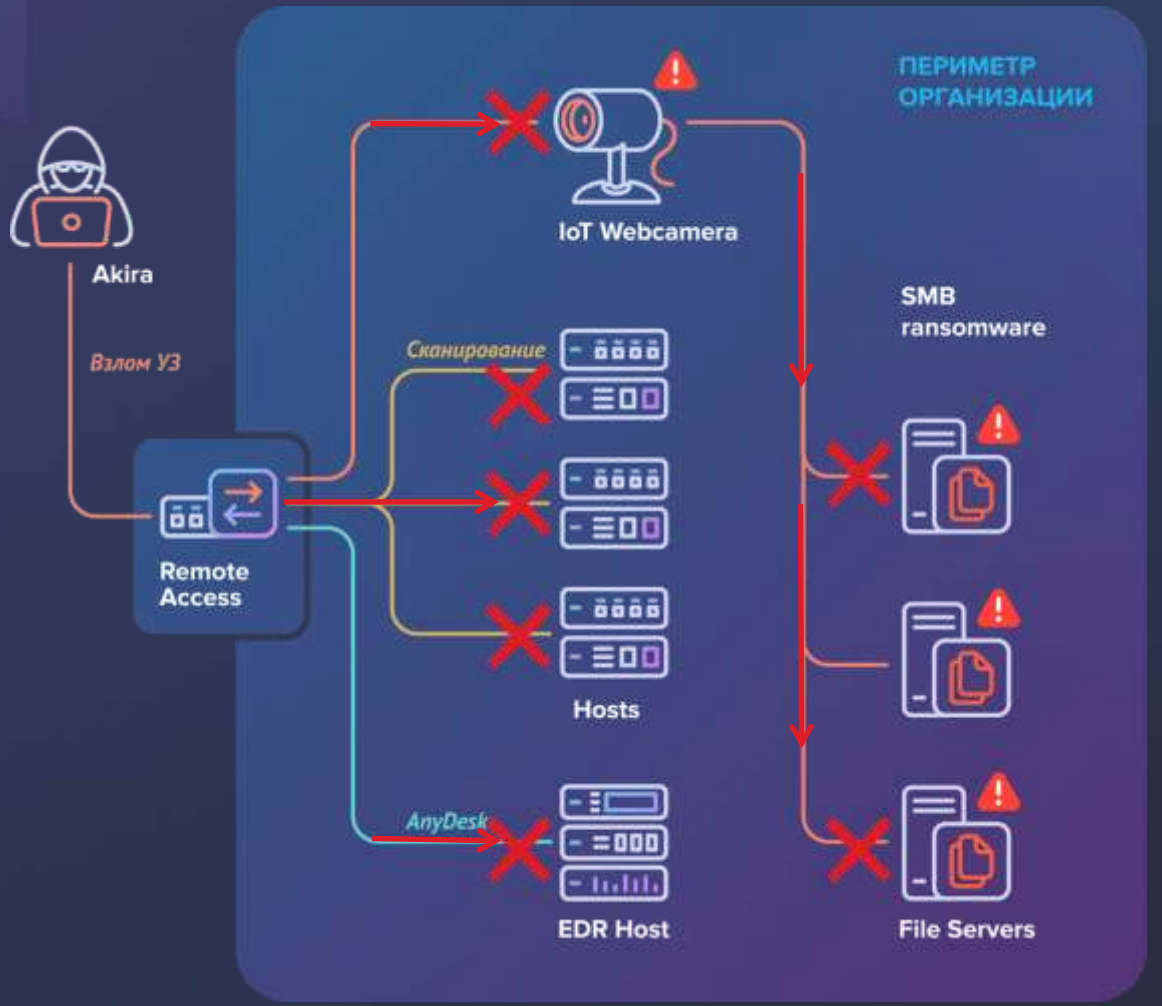
Применение Deception detection в NDR

ГАРДА

Имитация сетевых служб и протоколов:

- FTP, RDP, PPTP, SMB, Telnet/SSH, MQTT
- Memcache, MongoDB, MySQL, MSSQL, PostgreSQL
- TCP/UDP blackhole
- HTTP proxy, HTTP/HTTPs
- Kubernetes
- MITM для LLMNR

Автоматическое детектирование горизонтального перемещения



NDR обнаруживает горизонтальные перемещения, аномальную активность, закрывает слепые зоны и блокирует атаку до момента нанесения ущерба.

Автоматическое расследование и приоритизация

ГАРДА

Распределение AI-технологий для расследований и снижения ложных срабатываний

37,5%
AI Analyst

31,3%
AI Triage

12,5%
AI Investigations

12,5%
AI Search Assistant

6,2%
AI Prioritization

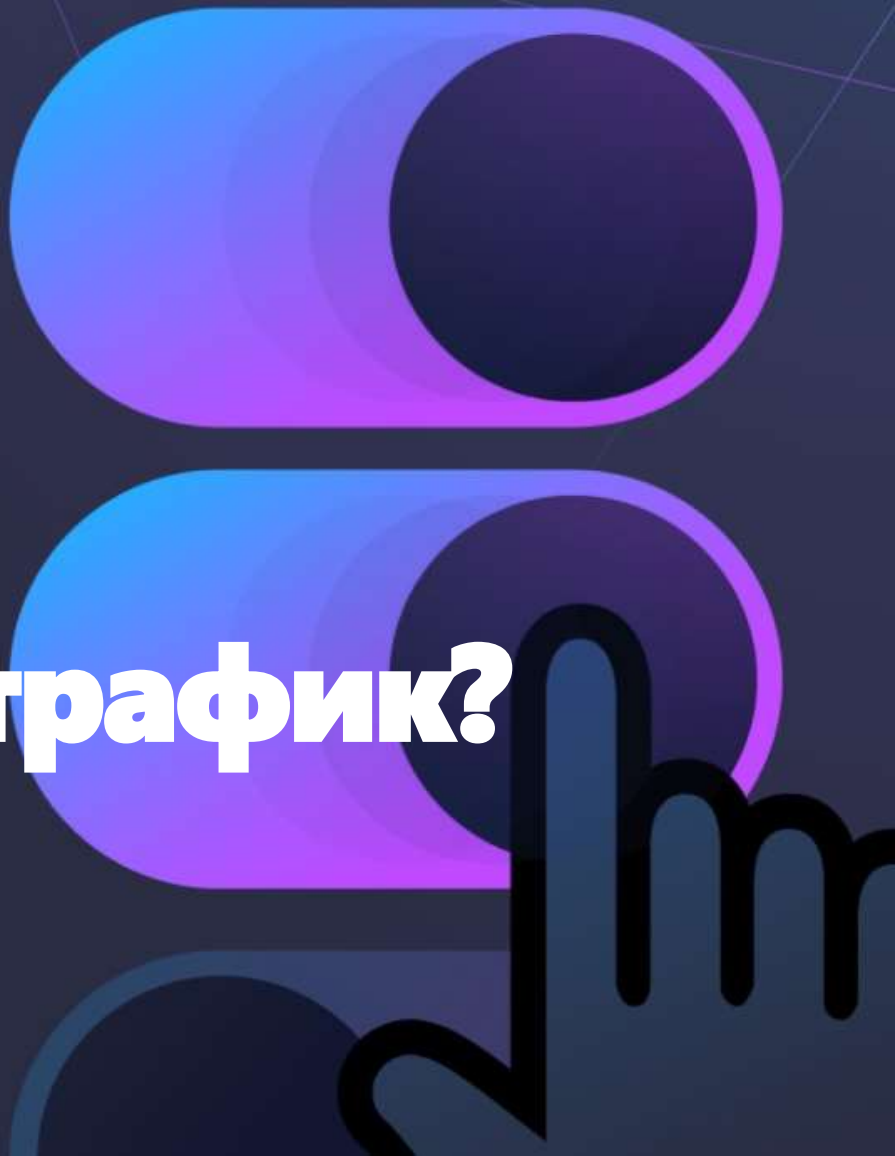
AI Investigations/AI Analyst – *функция автоматизированного расследования инцидентов с поддержкой анализа цепочек событий и скоринга уверенности при детектировании цепочек горизонтального перемещения.*

AI Triage – *функция автоматической приоритизации инцидентов на основе динамической оценки их критичности с учётом контекста и потенциального воздействия.*

AI Prioritization – *функция автоматической категоризации и ранжирования объектов (триаж учетных записей и хостов) на основе расчетного риск-индекса, уровня критичности и уверенности в потенциальной компрометации.*

ГАРДА

Как еще можно использовать сетевой трафик?



Проблемы производительности сети

ГАРДА

- Непонимание причин отсутствия доступа к бизнес-приложениям
- Нестабильная работа бизнес-приложений
- Отсутствие картины нормального поведения в сети
- Модификации ранее проведенных атак

Производительность сети NPM

ГАРДА

Видимость происходящего в сети

Понимание сетевого трафика, приложений и их взаимодействий в сети

Обнаружение проблем производительности сети с помощью метрик

Увеличение времени установления соединения, сбросы, повторные передачи пакетов, увеличение времени ответа приложения, увеличение времени ответа сети

Построение проактивного мониторинга производительности сети

Обнаружение проблем, ML-прогнозирование поведения сети, реагирование на события

Расследование проблем и сетевых инцидентов

Поиск источника проблемы, подтверждение отсутствия проблем на сети

Метрики сетевых соединений

ГАРДА

- **Время установления соединения**

  Время начального отклика сервера, время подтверждения соединения, время установления соединения

- **Количество ретрансмитов**

  Количество ретрансмитов в сессии, направления отправитель/получатель

- **Размер TCP окна**

  Минимальный, средний и максимальный размер окна в сессии отправитель/получатель

- **TCP пакеты с 0 размером окна**

  Количество пакетов отправитель/получатель

- **Время ответа приложения (Application delay)**

  Время ответа для отправителя/получателя в сессии

- **Время ответа сети(Network delay)**

  Время ответа для отправителя/получателя в сессии

GARDA

Подписывайтесь
на телеграм-канал **garda.ai**

garda.ai

Спасибо за внимание!