

Вебинар

17 сентября, 11:00 МСК

Что важнее SOC'а?

9 вопросов, которые мониторинг не закрывает



Сергей Прохоров

Эксперт в области
кибербезопасности ITG Security



Станислав Грибанов

Руководитель продуктового
направления группы компаний «Гарда»

Девять открытых вопросов

Логи видим. А сеть?

NDR

Кто остановит атаку?

SOC MDR

Через что взломают завтра?

VM

Что о нас уже продают?

OSINT

Кто заметит тихое
перемещение?

DECEPTION

Кто введёт пароль
в фишинг?

AWARENESS

Кто приедет тушить?

IRR

Вычистили – и докажем?

DFIR

А если взломали раньше?

CA

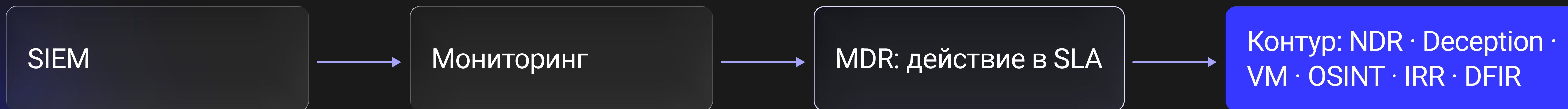
Как это выглядит сегодня



Ущерб наступает раньше, чем первое действие

8 мин против 40+

Куда движется рынок



МИР

- MDR вместо алертов
- EDR + NDR + логи
- Непрерывная поверхность атаки
- Ретейнер и ловушки — норма

РОССИЯ

- Кадры и 24/7 → сервисная модель
- Зрелый отечественный NDR
- Сроки уведомления регулятора
- Атаки через подрядчиков, утечки

300 дней или один день?

энергетика, 2023

БЕЗ СЕТЕВОГО МОНИТОРИНГА

Littleton Electric

Массачусетс, США

● февраль

VOLTZITE / Volt Typhoon входит в сеть коммунальной компании

● весь год

LotL-техники сливаются с админской активностью и не попадают в логи

● ноябрь

Сигнал приходит звонком из ФБР. Только после этого находят SMB-traversal и RDP

УЩЕРБ

300+ дней внутри

Выгружены OT-процедуры и схема энергосети — «где бить» во второй фазе

С СЕТЕВЫМ МОНИТОРИНГОМ

SektorCERT

22 компании, Дания

● 11 мая

Атака на 16 организаций через уязвимости в межсетевых экранах Zyxel

● тот же день

Сенсорная сеть SektorCERT засекает активность, команда реагирования выезжает

● 22-25 мая

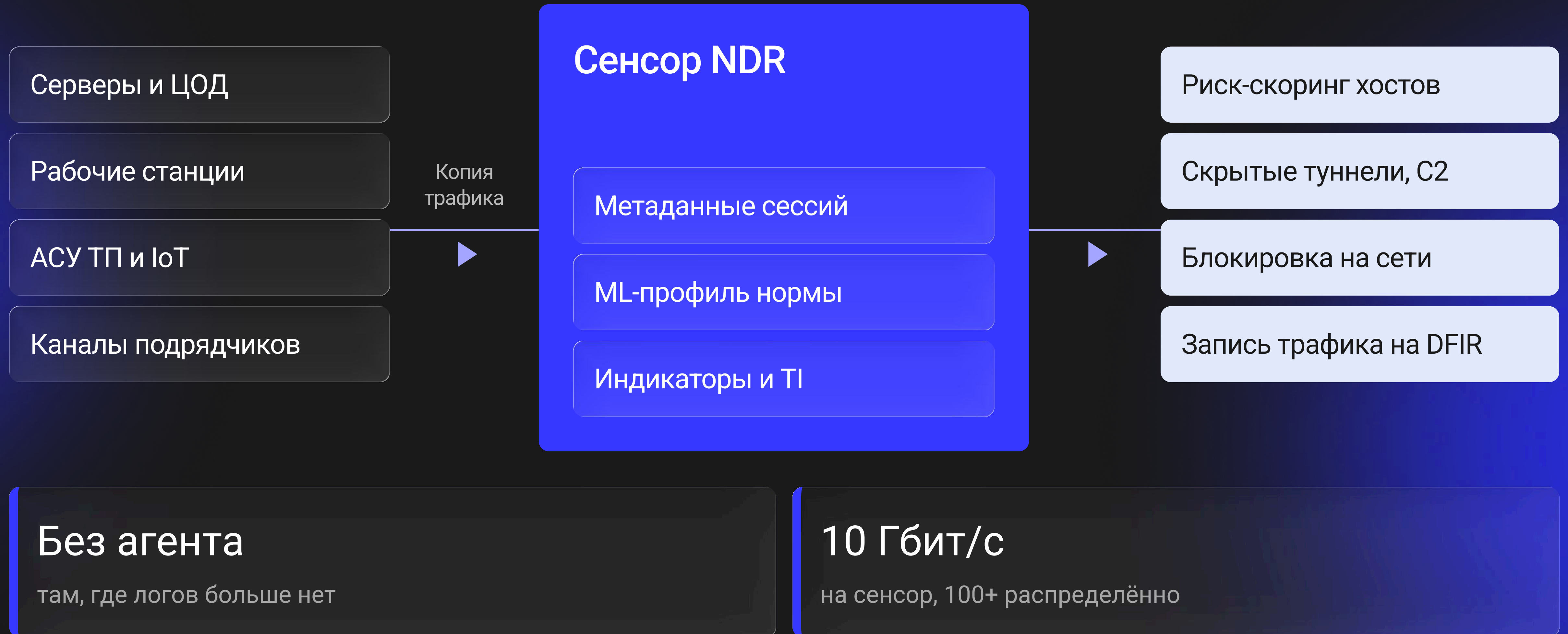
Вторая волна на двух 0-day: патчи вышли 24 мая, сигнатуры не работали в принципе

ИТОГ

Закрыто в тот же день

Доступ был и здесь — но развить его не дали ни в первой волне, ни во второй

Логи видим. А сеть?



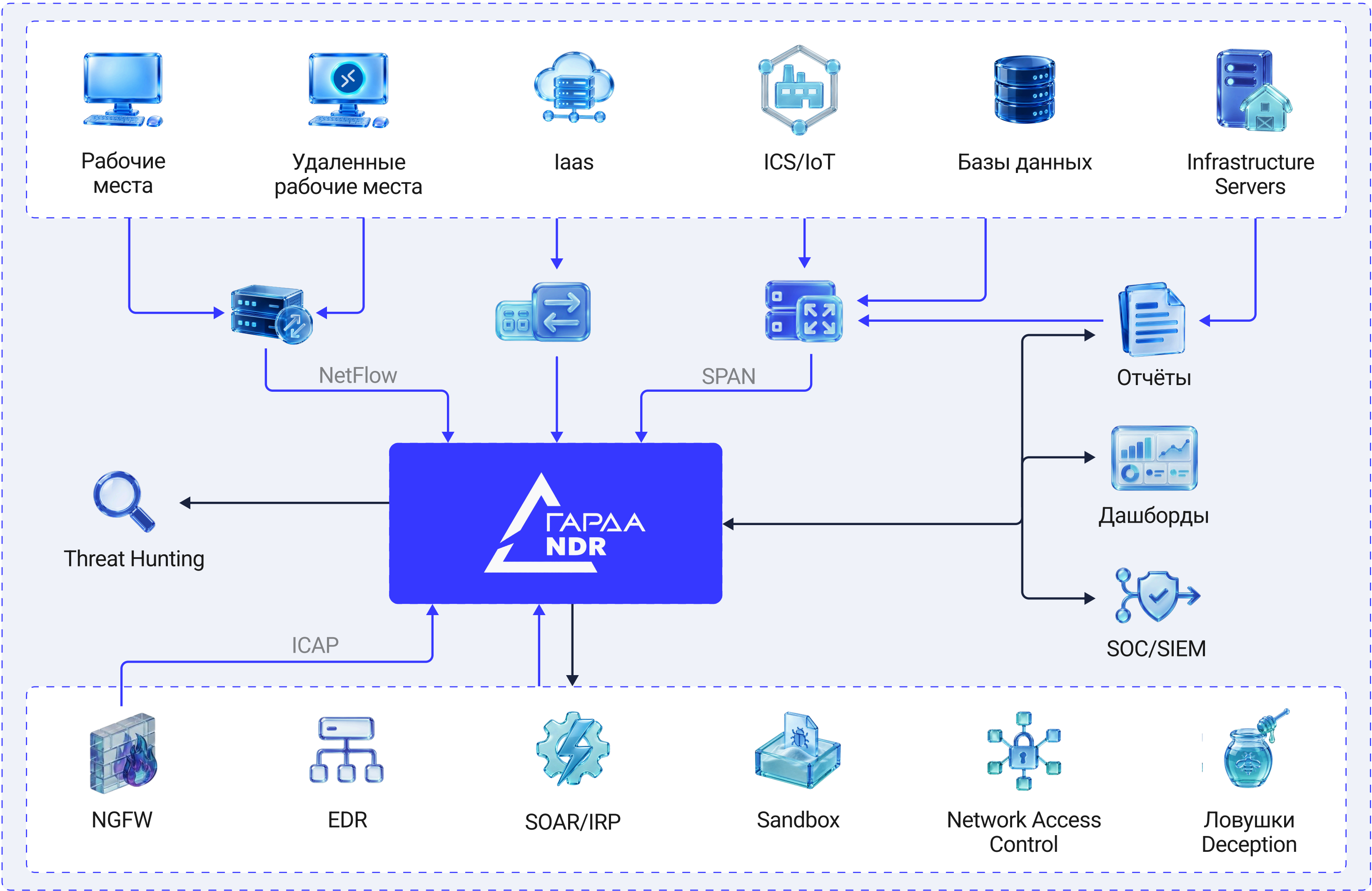
Без агента

там, где логов больше нет

10 Гбит/с

на сенсор, 100+ распределённо

Гарда NDR на схеме защиты сети



01 Источники

Данные от инфраструктуры — серверов, рабочих станций, баз данных, промышленных систем, IaaS — через копию трафика или телеметрию. Копию снимают роутеры, коммутаторы и пакетные брокеры.

02 Роль в SOC

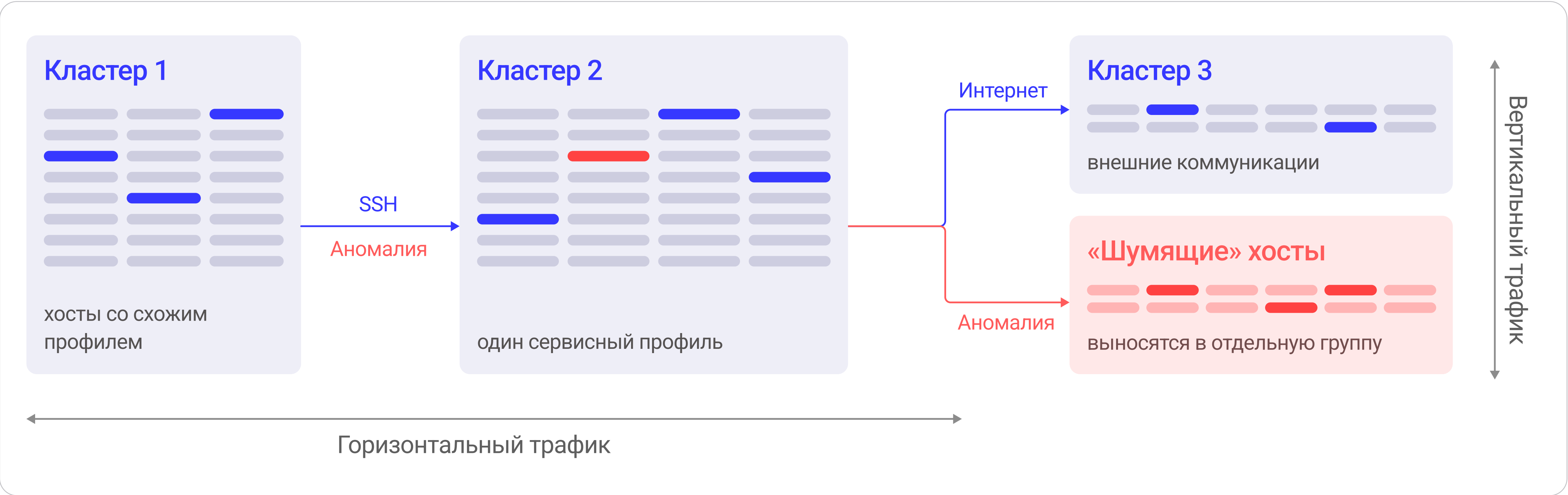
Неотъемлемый компонент для построения SOC.

03 Интеграции

Обмен с СЗИ и сетевым оборудованием: получение данных и телеметрии, активное реагирование.

- NetFlow, IPFIX, NSEL · SPAN, RSPAN, TAP, GRE/ERSPAN
- ICAP · реагирование и интеграции

ML-моделирование нормального поведения групп хостов



Кластеры хостов

группы со схожим сетевым поведением

Аномалия

отклонение от поведения своей группы

Угрозы, детектируемые на основе нормального поведения групп хостов

01

Горизонтальное
перемещение

LoTL — RDP, SSH, VNC,
TeamViewer и другие

02

Туннелирование
коммуникаций
с C&C

03

Медленная
эксфильтрация

04

Распространение
ransomware внутри
сети

05

Обращение
к нетипичным
внешним ресурсам

Метрики зависят от детектора аномалий и трафика

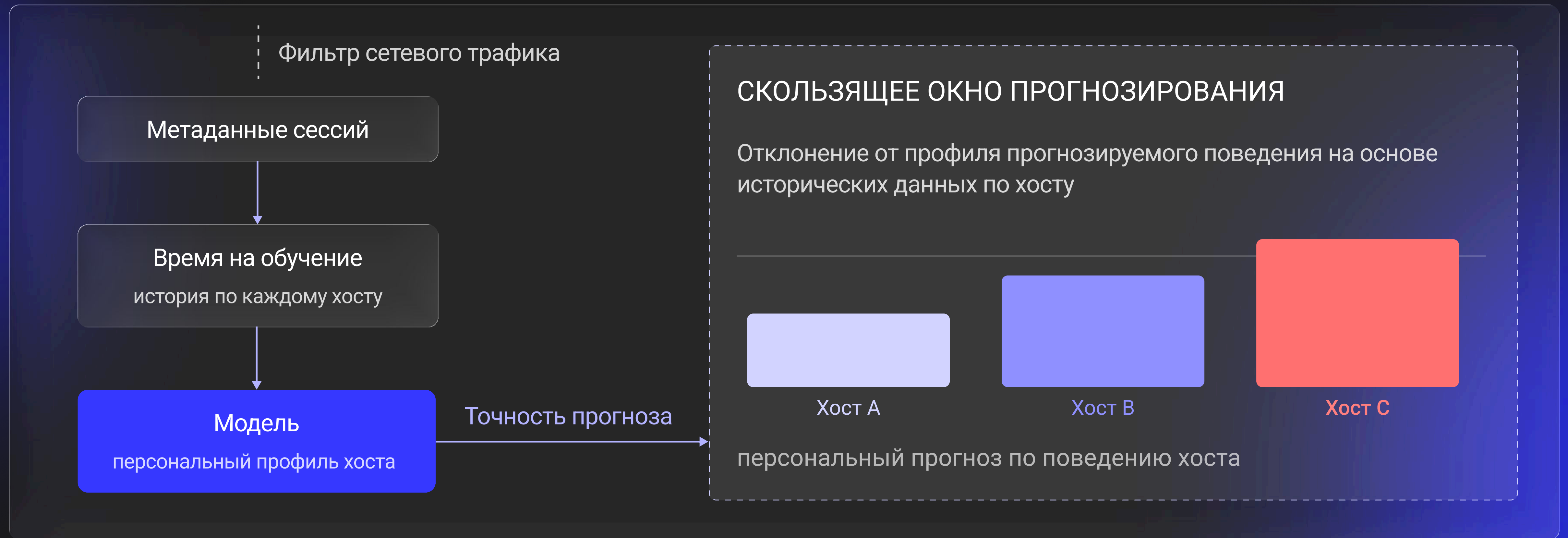
ML-прогнозирование поведения хоста

Детектирование Living off the Land

NetFlow

SPAN

TI feeds



Угрозы, детектируемые на основе ML-прогнозирования поведения хоста

01 Аутентификация

- Брутфорс (SSH, RDP, SMB, HTTP, HTTPS, LDAP, SQL)
- Распыление пароля SMB, Kerberos
- Подмена LLMNR/NBT-NS-ответа и ретрансляция SMB
- Кража или подделка билетов, Kerberos AS-REP-роастинг
- Керберостинг, уязвимые конфигурации Kerberos

02 Сканирование и разведка

- Сканирование IP и портов
- Изучение сетевых служб
- Активное сканирование — поиск уязвимостей
- SNMP-трафик с попыткой организовать утечку данных MIB

03 Перемещения и DDoS

- Горизонтальное перемещение (Living off the Land)
- DoS / DDoS

04 Туннели и обход периметра

- DNS / ICMP / SSH и другие туннели
- Туннелирование C&C в трафике легальных приложений
- Преодоление границ сети, изменение конфигурации NAT
- Прокси-сервер / пивот

05 Эксфильтрация

- Эксфильтрация данных по каналу управления
- Эксфильтрация данных в репозиторий или облачное хранилище

06 Социальная инженерия

- Обнаружение фишинга с вложением или ссылкой
- Поведенческий анализ

Детектирование коммуникаций с C&C и медленной эксфильтрации

NetFlow

SPAN

ML

DGA

TI feeds

Cobalt Strike HTTPS Jitter 10%



Ровная периодика обращений — признак маяка: интервалы и объёмы повторяются даже при джиттере.

Угрозы, детектируемые на основе ML-моделей: C&C и DGA

01

Туннелирование C&C
в трафике легальных
приложений

02

Соединения
с командными
серверами по
зашифрованным
каналам

03

Экспфильтрация
по расписанию

04

Экспфильтрация
через веб на сайт
для хранения текста
(pastebin)

Метрики

Отличаются в зависимости
от детектора аномалий и трафика
на площадке.

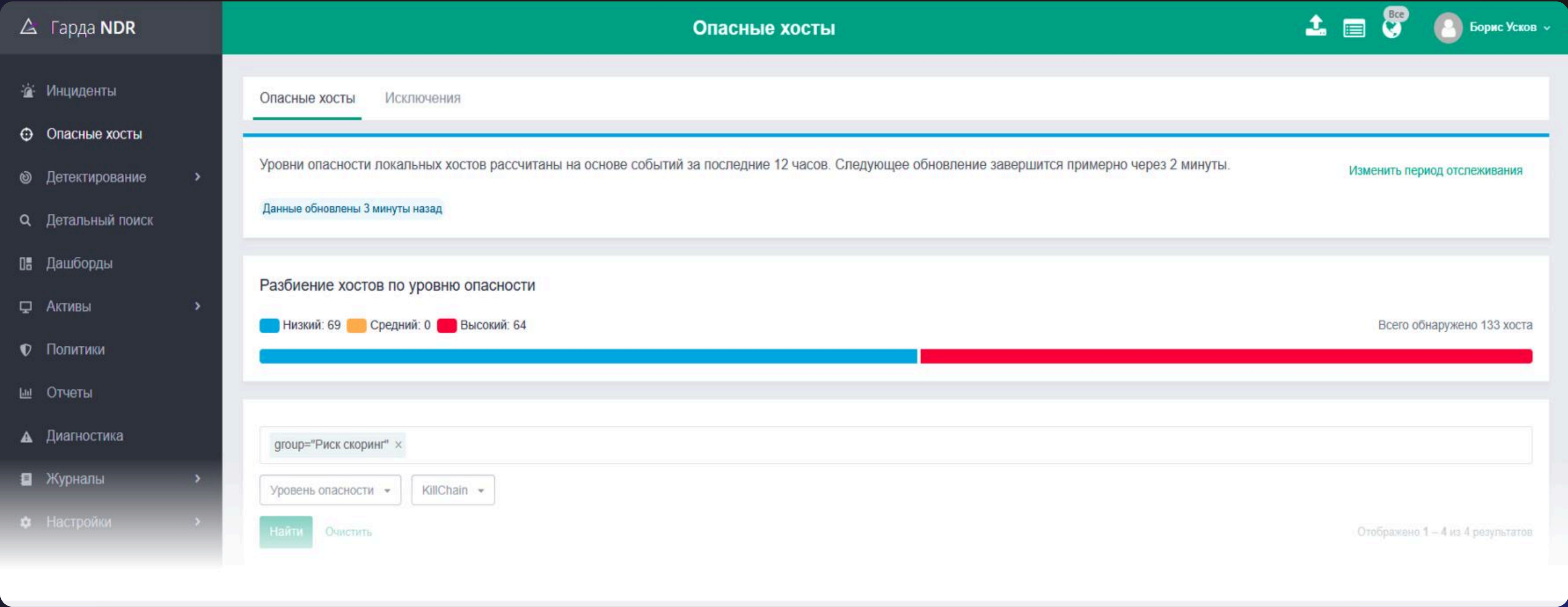
Белый список

Домены легальных ресурсов
поставляем из коробки.

Сочетание моделей

Максимальная точность: DGA + C&C
или TI feeds + C&C.

Автоматический риск-скоринг хостов



12 часов

окно расчёта уровня опасности

133 хоста

обнаружено в сегменте

64 ВЫСОКИХ

по событиям за окно наблюдения

19 дней или 30 минут?

одна украденная сессия

МОНИТОРИНГ БЕЗ СДЕРЖИВАНИЯ

Target ритейл, США, 2013

- 30 ноября
Установлена малварь для эксфильтрации. FireEye поднимает срочные алерты
- 2–3 декабря
Алерты повторяются при обновлениях малвари, срабатывает и Symantec. Автоудаление не разрешено
- середина декабря
О взломе Target узнаёт от Минюста — банки вычислили общую точку компрометации

УЩЕРБ

19 дней до остановки

40 млн карт и данные 70 млн человек. \$18,5 млн с 47 генпрокурорами, ушли CEO и CIO

ДЕТЕКТ → РЕШЕНИЕ → ОТЗЫВ ДОСТУПА

BeyondTrust 2 октября 2023

- по просьбе поддержки
Админ загружает в портал Okta HAR-файл — с сессионной cookie внутри
- +30 минут
Cookie использована. Кастомные детекты подсвечивают вторжение
- сдерживание
Backdoor-учётку отключили и отозвали доступ до того, как ею воспользовались

ИТОГ

Ноль воздействия

Сама Okta подтвердила компрометацию лишь 19 октября — за эти 17 дней пострадали Cloudflare и 1Password

Кто остановит атаку?

Атака

ВХОД

закрепление

перемещение

эксfiltrации нет

MDR

01

Детект

02

Плейбук

03

Изоляция хоста и учётки

04

Разбор и усиление

действие в минутах, а не письмо

от 300 тыс. ₺

против 1,41 млн. за свой SOC

Недели

вместо 1-1,5 года своими силами

SLA

ответственность за скорость

Кто проверит, что патч дошёл?

патч есть, процесса нет

СКАНЕР ЕСТЬ, ПРОЦЕССА НЕТ

Equifax

Apache Struts, 2017

● 7–9 марта

Вышел патч, US-CERT лично уведомил компанию, админам разослали указание

● 15 марта

Сканирование не нашло уязвимость — покрытие никто не проверил

● 13 мая

Компрометация и 76 дней эксфильтрации из 48 баз данных

УЩЕРБ

147 млн человек

До \$700 млн по соглашению с FTC, CFPB и генпрокурорами 50 штатов

КАРТА ВНЕШНЕЙ ПОВЕРХНОСТИ

DIVD · Kaseya VSA

Нидерланды, 2021

● апрель

DIVD находит уязвимости и ведёт координированное раскрытие

● до атаки

Скан интернета: карта всех доступных снаружи инстансов с привязкой к customer ID

● 2 июля

REvil опережает патч — но владельцы уже известны и оповещены

ИТОГ

2200+ → менее 140

Доступных из интернета VSA-серверов за 48 часов. В Нидерландах — ноль к 4 июля

ТЕЗИС ● Провал был не в отсутствии сканера, а в отсутствии процесса: покрытие, контроль закрытия и проверка, что инструмент жив

Через что взломают завтра?

01

Сканирование
по расписанию

Периметр, внутренняя
сеть и приложения –
регулярно, а не отчёт раз
в год

02

Проверка аналитиком

Триаж: отсев ложных
срабатываний и
проверка,
эксплуатируется ли
уязвимость в вашей
конфигурации

03

Приоритет по риску
бизнеса

Не по баллу CVSS. Триаж
– хорошо, приоритизация
– ещё лучше

04

Контроль
до устранения

Задача уходит в ваш
процесс – доводим до
факта устранения с
повторной проверкой

цикл, а не отчёт раз в год

Если патч
поставить нельзя

Выдаём рекомендации по компенсирующим
мерам – риск закрывается и без обновления

Регуляtorика

Непрерывное управление уязвимостями – часть
соответствия ГОСТ Р 57580.1

Ваши креды уже продали?

один кейс

МОНИТОРИНГА УТЕЧЕК НЕ БЫЛО

Snowflake · UNC5537 клиентские инстансы, 2024

- с 2020 года
Инфостилеры собирают креды сотрудников и подрядчиков на посторонних машинах
- 2024
Массовые входы в клиентские инстансы: логин и пароль, без эксплойтов и без MFA
- вывод Mandiant
Ничего нового в ТТР — масштаб дала экономика инфостилеров и незащищённые учётки

УЩЕРБ

≈165 организаций

Ticketmaster ≈560 млн записей, AT&T, Santander. Сам Snowflake взломан не был

ЧТО ЛОВИТ МОНИТОРИНГ РЕГИСТРАЦИЙ

Oktapus шаблон фишинговых доменов

- 169 доменов
Столько уникальных фишинговых доменов насчитали в одной кампании
- ключевые слова
SSO, VPN, ОКТА, MFA, HELP — типовой набор в имени домена
- окно
Регистрация видна до начала рассылки — есть время закрыть вход

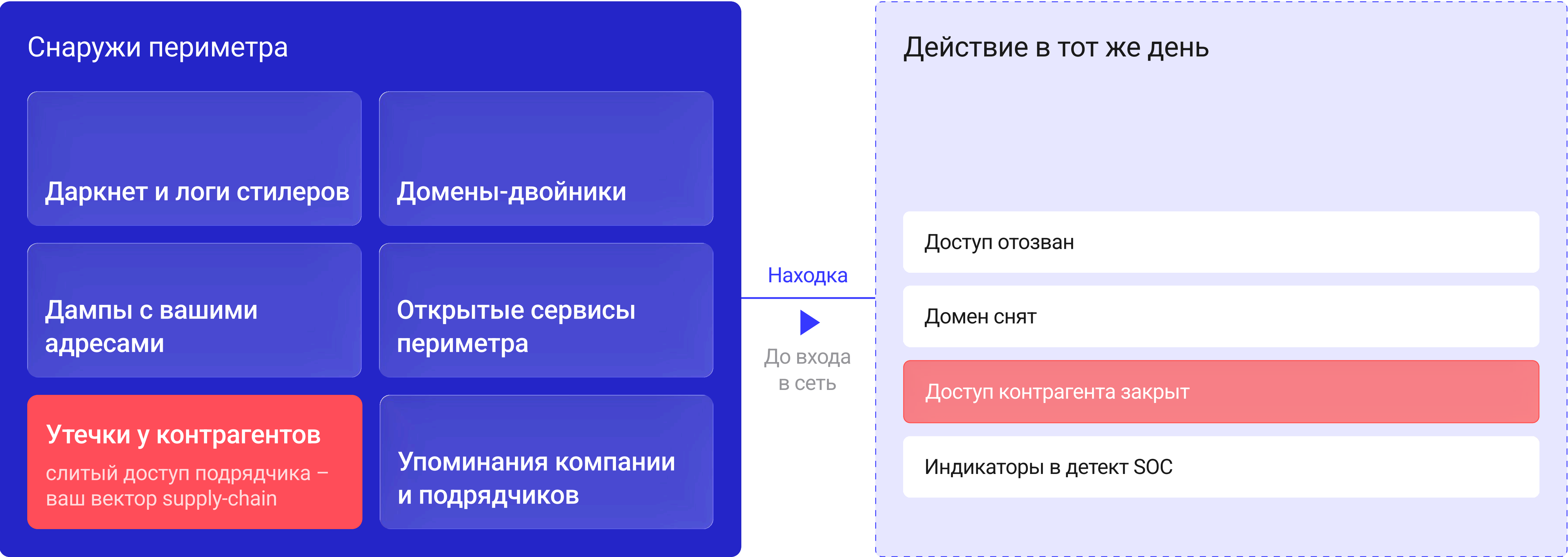
ВОЗМОЖНОСТЬ

За годы до атаки

Данные для предотвращения лежали в открытом доступе — их никто не смотрел

ТЕЗИС ● OSINT — это не отчёт о трендах, а список ваших собственных кредов и доменов-двойников до того, как ими воспользуются

Что о нас уже продают?



supply-chain

Утечка у контрагента становится атакой на вас: пока его доступ к вашим системам жив, атакующий заходит «по доверенности». Находим утечку → закрываем доступ → атака не состоялась

Часы в шарах или алерт сразу?

кто первым найдёт секрет

БЕЗ ЛОВУШЕК

Uber

сентябрь 2022

● ВХОД

MFA-fatigue: сотрудник в итоге подтверждает запрос

● несколько часов

Атакующий ползает по сетевым шарам в поисках секретов — на это никто не смотрит

● находка

PowerShell-скрипты с зашитыми учётными данными администратора PAM-системы

УЩЕРБ

Доступ ко всему

AWS, GCP, Google Drive, Slack, SentinelOne, админка HackerOne. Легитимный пользователь honeu-креды не трогает никогда

ТОКЕНЫ РАЗЛОЖЕНЫ ЗАРАНЕЕ

Grafana Labs

апрель 2025

● до инцидента

Фейковые AWS-ключи разложены в GitHub Secrets организации и репозиториях

● вторжение

Атакующий выгружает секреты и прогоняет их через TruffleHog

● срабатывание

Вызов sts:GetCallerIdentity по canary-токену — мгновенный алерт

ИТОГ

Локализация за минуты

Ни изменений в коде, ни доступа к прод-системам и данным клиентов. Токен оказался главным сигналом о присутствии

Кто заметит тихое перемещение?

Сеть заказчика – Сапёр

006

00:01

	1						
1	2	3					
1							

honeypot «1C»
canarytoken

honeypot «SharePoint»
учётная запись «Admin1»

honeypot «SMB-шара»
таблица «M&A_targets» в Tableau

«passwords.docx» – на рабочем столе у всех

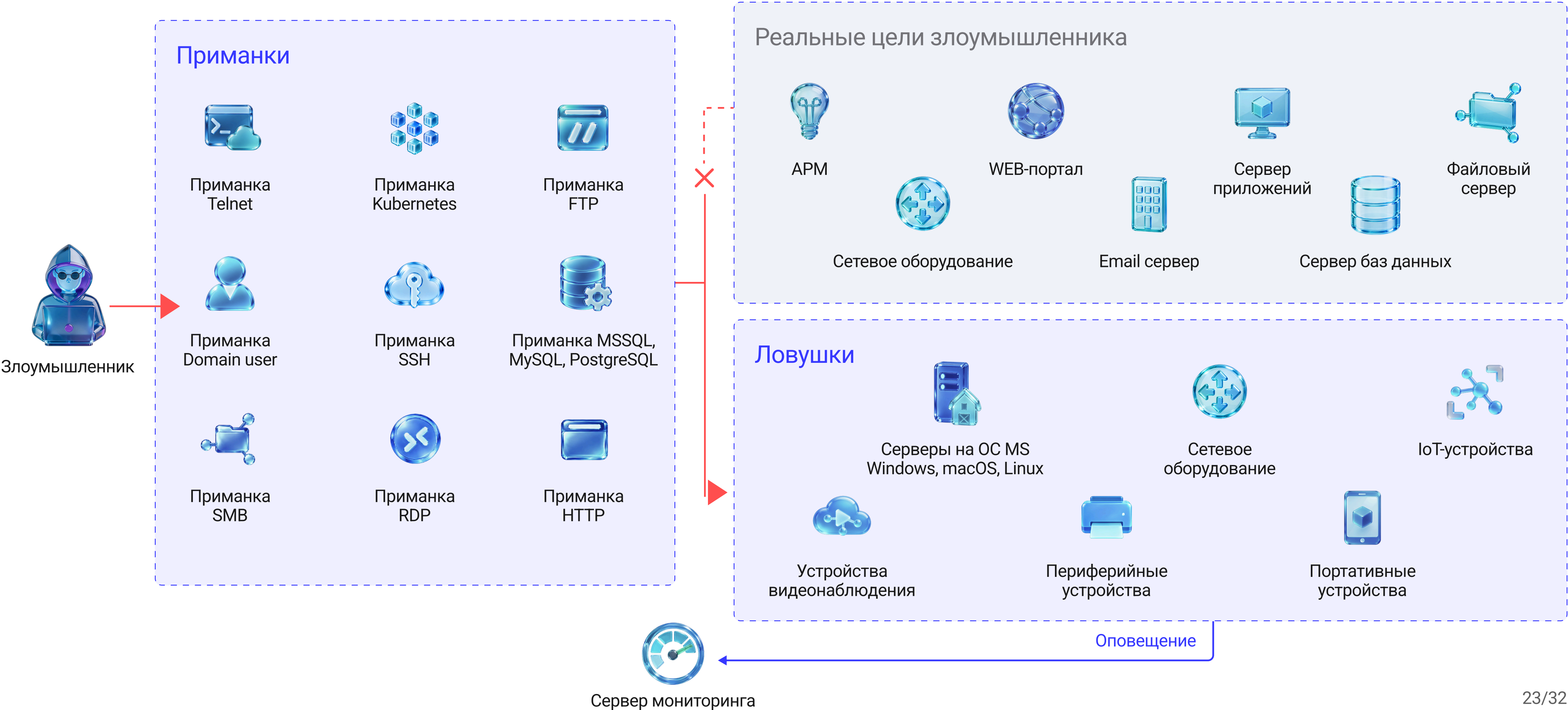
Касание мины = инцидент

легитимных обращений к ловушке не бывает — сигнал в SOC сразу с хостом и учётной записью

Дни

на запуск, без агентов и изменений в продуктиве

Возможности Deception в Гарда NDR Extended



Одна рассылка, два исхода

август 2022, одна кампания

CLICK RATE НЕИЗВЕСТЕН

Twilio

SMS под ИТ-департамент

- **рассылка**

SMS якобы от ИТ со ссылкой на поддельную страницу входа

- **клик**

Сотрудники логинятся на фишинговой странице и отдают креды

- **вход**

Логина и пароля достаточно, чтобы войти в реальную систему — второго барьера нет

УЩЕРБ

163 клиента

Плюс 93 аккаунта Authy. Кампания шла по десяткам компаний одновременно, по одному шаблону

КОНТРОЛЬ ПОД ДОПУЩЕНИЕ «КЛИКНУТ»

Cloudflare

та же рассылка, тот же домен

- **клик**

Трое сотрудников ввели свои данные на фишинговой странице

- **барьер**

Физические аппаратные ключи обязательны для доступа ко всем приложениям

- **стоп**

Кредов недостаточно: атаку остановили на входе

ИТОГ

Ни одна система не скомпрометирована

Компания заранее знала свой click rate — потому что регулярно его измеряла

ТЕЗИС ● Разница не в людях — кликнули и там, и там. Симуляции нужны, чтобы знать, что произойдёт после клика

Кто введет пароль в фишинг?

ВОРОНКА КАМПАНИИ

Получили письмо

Открыли

Перешли

Ввели пароль

Сообщили в ИБ

Ваша поверхность атаки

метрика, которую растим

ЦИКЛ

Сценарии от аналитиков SOC
Почта, мессенджеры, звонки
Метрики по подразделениям
Обучение тех, кто ошибся
Повтор → динамика

Кому вы позвоните в первый час?

первый час инцидента

БЕЗ РЕТЕЙНЕРА

Maersk

NotPetya, 2017

- удар

NotPetya выносит корпоративную инфраструктуру целиком

- 10 дней

Переустановка 4000 серверов, 45 000 ПК и 2500 приложений

- оценка сверху

Председатель совета директоров: нормальный срок такой работы — полгода

УЩЕРБ

\$250–300 млн

В десять дней уложились героическим усилием. Героизм — не операционная модель

ВНЕШНЯЯ КОМАНДА В ПЕРВЫЕ ЧАСЫ

Norsk Hydro

LockerGoga, 2019

- первые часы

Запрошена помощь внешней команды реагирования Microsoft DART

- три решения сразу

Выкуп не платить, звать внешних, говорить публично и открыто

- операции

Заводы переведены в ручной режим, восстановление из резервных копий

ИТОГ

550–650 млн NOK

Страховка к концу третьего квартала покрыла лишь около 5% — готовность дешевле полиса

Кто придет тушить?

БЕЗ РЕТЕЙНЕРА

поиск подрядчика

договор, цена, NDA, доступы

знакомство с архитектурой,
маршрутами потоков данных,
сетевыми схемами

первые действия

3-5 дней – всё это время атакующий работает, артефакты затираются

С РЕТЕЙНЕРОМ

договор и SLA заранее

разработанный и протестированный
план реагирования

звонок

сдерживание и сбор артефактов

первые часы – архитектура и план уже знакомы команде

Дни слепоты или один алерт?

что именно скомпрометировано

БЕЗ ФОРЕНЗИКИ

Colonial Pipeline

май 2021

● записка

Сотрудник диспетчерского центра видит требование выкупа

● решение

Операции остановлены, чтобы изолировать OT-сеть от атаки

● слепота

CEO в Сенате: чтобы увидеть, что происходит в системах, нужны дни

УЩЕРБ

Остановлено 5500 миль трубопровода

Около 45% топлива Восточного побережья. Проникновения в OT так и не нашли

ФОРЕНЗИКА ПО ТИХОМУ АЛЕРТУ

FireEye

декабрь 2020

● сигнал

Регистрация чужого устройства в MFA по украденным кредам — тревога нулевой критичности

● разбор

Пакетные захваты и логи форензик-агентов на эндпоинтах

● сходимость

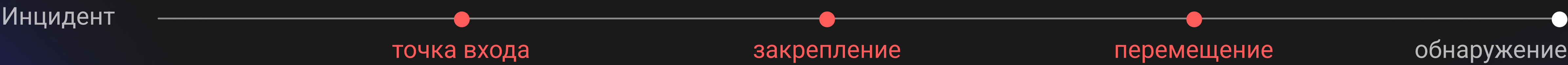
Всё сошлось на системе с SolarWinds: 50 000 строк кода и найденный бэкдор

ИТОГ

Малвари не было

Противник действовал под видом легитимного пользователя. С этого алерта вскрыли всю кампанию

Вычистили – и докажем?



◀ восстанавливаем хронологию назад -----

01

Фиксация доказательств

Образы дисков и памяти,
контрольные суммы,
цепочка хранения

02

Точка входа и техники

Как вошли, чем
закрепились, куда пошли
– по NIST, ISO и SANS

03

Границы компрометации

Полный список
затронутых систем – что
действительно чистить

04

**Отчёт для регулятора
и суда**

Доказательный вывод:
индикаторы уходят
в детект SOC

До расследования

Переустановка сервера «для чистоты» уничтожает артефакты безвозвратно – точка входа останется открытой, и атакующий вернётся тем же путём

«Мы уже взломаны?» — до сделки

до сделки или после

КОМПРОМЕТАЦИЮ КУПИЛИ С АКТИВОМ

Marriott · Starwood

2014–2018

● 2014

Веб-шелл у Starwood, затем малварь для привилегированного доступа и сбор кредитов

● сентябрь 2016

Marriott покупает Starwood — вместе с уже действующей компрометацией

● сентябрь 2018

Компрометацию наконец обнаруживают: четыре года незамеченного доступа

УЩЕРБ

≈339 млн записей

Включая незашифрованные паспорта. Штраф £18,4 млн: ICO указал на недостаточную due diligence

НАШЛИ ДО ЗАКРЫТИЯ СДЕЛКИ

Verizon · Yahoo

февраль 2017

● до закрытия

Раскрыты две утечки Yahoo: 500 млн и более 1 млрд аккаунтов

● пересогласование

Цена снижена с \$4,83 млрд до \$4,48 млрд

● важнее скидки

Yahoo берёт 50% обязательств по негосударственным искам и SEC-расследованиям

ИТОГ

–\$350 млн к цене

Знание о компрометации стало условием сделки, а не претензией регулятора через два года

А если взломали раньше?

до SOC
Слепая зона: кто уже внутри?

МОНИТОРИНГ ВКЛЮЧЁН
Видим только вперед

01

Телеметрия за период

Хосты, домен, сеть, почта,
журналы – артефакты
за месяцы, а не снимок
на сегодня

02

Хантинг по гипотезам

По MITRE: механизмы
закрепления, C2,
аномальные учётки
и туннели

03

Вердикт: чисто или
находки

Чисто – отчёт и
рекомендации;
находки – фиксируем
доказательства

04

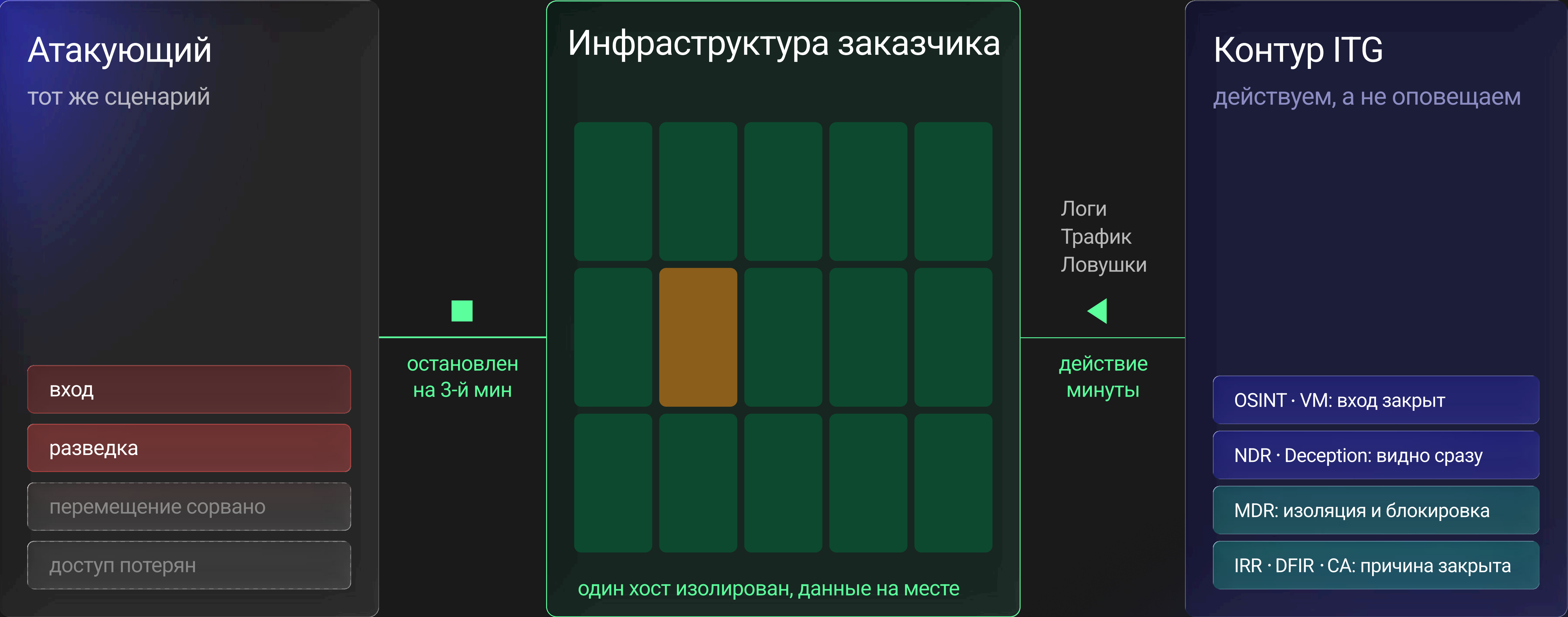
Переход в DFIR

Полное расследование той
же командой, без смены
подрядчика

от 200 000 ₽ фиксированная стоимость – известна до старта

Первый шаг логичная точка входа перед подключением SOC

Та же атака, закрытый контур



Спасибо за внимание

 itgsecurity.ru

 info@itgsecurity.ru

 sales@itgsecurity.ru

