софтлайн РЕШЕНИЯ

Актуальные подходы к борьбе с недетектируемыми угрозами

Противодействие целевым атакам

Александр Лебедев

Business Development Manager
Anti Apt (Борьба с целенаправленными атаками)

ПОЧЕМУ РЫНОК ДВИЖЕТСЯ К XDR?

СЛОЖНЫЕ ИНТЕГРАЦИИ

Интеграция “лучших в классе” решений друг с другом - трудоемко и долго

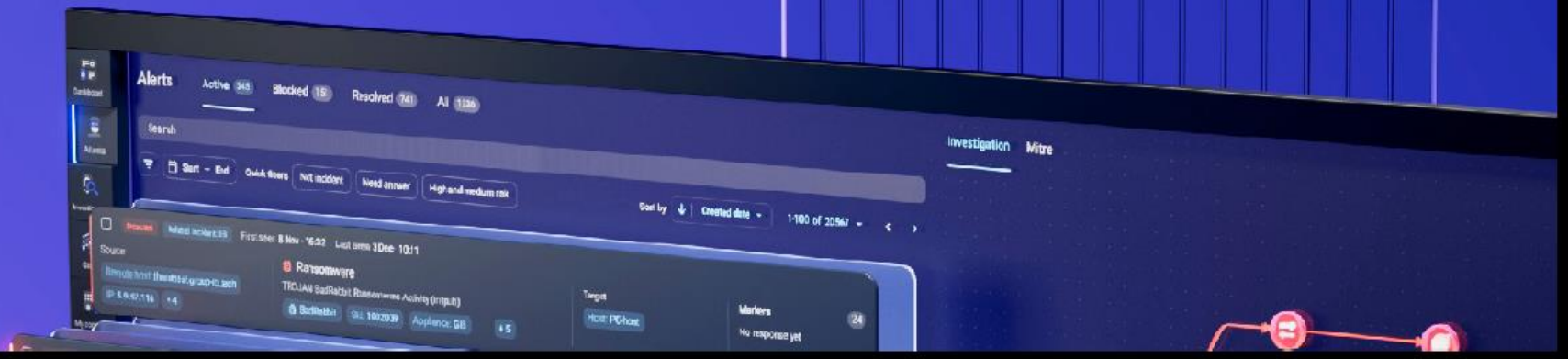
НЕДОСТАТОК РЕСУРСОВ

Сложно подбирать, обучать и удерживать экспертов для круглосуточного обеспечения ИБ

ДЛЯ ОТВЕТА НА ЭТИ И ДРУГИЕ ВЫЗОВЫ РЫНОК ДВИЖЕТСЯ В СТОРОНУ НОВОГО КЛАССА ПРОДУКТОВ

XDR

Системы с расширенными возможностями обнаружения и реагирования на угрозы ИБ



ЧТО ЗАМЕДЛЯЕТ КОМАНДЫ ИБ?

ПРЕПЯТСТВИЯ БЫСТРОМУ ОБНАРУЖЕНИЮ И РЕАГИРОВАНИЮ

ПЕРЕГРУЗКА АЛЕРТАМИ

Тысячи событий безопасности, возникающие каждую минуту в сложной инфраструктуре, замедляют работу аналитиков

ОГРАНИЧЕННЫЕ РЕСУРСЫ

Две трети компаний заявляют о недоукомплектованности и неспособности оперативно реагировать на современные угрозы

РАЗРОЗНЕННЫЕ РЕШЕНИЯ

Точечные решения со своими тонкостями, интерфейсами и интеграциями делают управление безопасностью времязатратным и неэффективным

РАЗВИВАЮЩИЕСЯ УГРОЗЫ

Атакующие становятся изощреннее и внедряют новые TTPs, пока сотрудники команды ИБ изо всех сил стараются не отставать

ОБЗОР MANAGED XDR

1 Индикаторы, телеметрия, артефакты и события
2 Контекст угроз, профили атакующих, обогащение

АНАЛИЗ СЕТЕВОГО ТРАФИКА

- Анализ трафика
- Обнаружение аномалий
- Выявление скрытых каналов
- Извлечение файлов
- Интеграция с другими системами

ЗАЩИТА КОНЕЧНЫХ СТАНЦИЙ И РЕАГИРОВАНИЕ

- Сбор событий с хостов
- Сбор криминалистических
- Данных
- Выявление атак в реальном времени
- Остановка процессов
- Изоляция хоста

ДЕТОНАЦИЯ ВРЕДОНОСНОГО ПО

- Поведенческий анализ
- Детальные отчеты
- MITRE TTPs
- Обнаружение техник обхода
- Ретроспективный анализ

ЗАЩИТА КОРПОРАТИВНОЙ ПОЧТЫ

- Анализ вложений и ссылок
- Фильтрация спама и фишинга
- Фильтрация контента по политикам
- Защита после доставки

БАЗА ДАННЫХ XDR

- Телеметрия с хостов, сетевого трафика и почтового потока
- Алерты и инциденты Сетевые логи
- Криминалистические данные кибербразведки
- Собственные правила IoC и IoA

XDR КОНСОЛЬ

- Единая точка входа
- Корреляция событий
- Совместная работа с экспертами, охотниками за угрозами, аналитиками
- Реагирование на инциденты
- Графовый анализ
- Управление инфраструктурой

СЕРВИСЫ

КРУГЛОСУТОЧНЫЙ МОНИТОРИНГ

- 24/7 триаж алертов
- Корреляция и классификация
- Атрибуция атак
- Уведомления

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

- Цифровая криминалистика
- Анализ вредоносного кода
- Рекомендации по реагированию и восстановлению IT-инфраструктуры

ПРОАКТИВНЫЙ ПОИСК НЕДЕТЕКТИРУЕМЫХ УГРОЗ

- Анализ телеметрии
- Персональный ландшафт угроз
- Создание и тестирование гипотез
- Подробные отчеты

THREAT INTELLIGENCE

Локальные центры исследования угроз, раскрытие инфраструктуры атакующих, анатомии атак и уникальные TTPs

ОБЗОР MANAGED XDR

1 Индикаторы, телеметрия, артефакты и события
2 Контекст угроз, профили атакующих, обогащение

АНАЛИЗ СЕТЕВОГО ТРАФИКА

- Анализ трафика
- Обнаружение аномалий
- Выявление скрытых каналов
- Извлечение файлов
- Интеграция с другими системами

ЗАЩИТА КОНЕЧНЫХ СТАНЦИЙ И РЕАГИРОВАНИЕ

- Сбор событий с хостов
- Сбор криминалистических
- Данных
- Выявление атак в реальном времени
- Остановка процессов
- Изоляция хоста

ДЕТОНАЦИЯ ВРЕДОНОСНОГО ПО

- Поведенческий анализ
- Детальные отчеты
- MITRE TTPs
- Обнаружение техник обхода
- Ретроспективный анализ

ЗАЩИТА КОРПОРАТИВНОЙ ПОЧТЫ

- Анализ вложений и ссылок
- Фильтрация спама и фишинга
- Фильтрация контента по политикам
- Защита после доставки

БАЗА ДАННЫХ XDR

- Телеметрия с хостов, сетевого трафика и почтового потока
- Алерты и инциденты Сетевые логи
- Криминалистические данные кибербразведки
- Собственные правила IoC и IoA

XDR КОНСОЛЬ

- Единая точка входа
- Корреляция событий
- Совместная работа с экспертами, охотниками за угрозами, аналитиками
- Реагирование на инциденты
- Графовый анализ
- Управление инфраструктурой

СЕРВИСЫ

КРУГЛОСУТОЧНЫЙ МОНИТОРИНГ

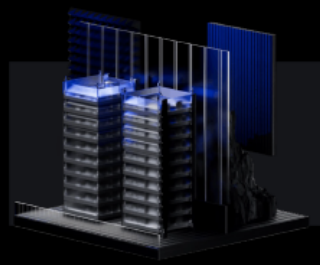
- 24/7 триаж алертов
- Корреляция и классификация
- Атрибуция атак
- Уведомления

ПРОАКТИВНЫЙ ПОИСК НЕДЕТЕКТИРУЕМЫХ УГРОЗ

- Анализ телеметрии
- Персональный ландшафт угроз
- Создание и тестирование гипотез
- Подробные отчеты

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

- Цифровая криминалистика
- Анализ вредоносного кода
- Рекомендации по реагированию и восстановлению IT-инфраструктуры



THREAT INTELLIGENCE

Локальные центры исследования угроз, раскрытие инфраструктуры атакующих, анатомии атак и уникальные TTPs

Рост количества целевых атак

Рост атак, исходящих от квалифицированных и хорошо организованных групп (APT)

целевые атаки за первые три квартала 2022 г.

целевые атаки за первые три квартала 2023 г.

Актуальность

84 минуты

среднее время проникновения злоумышленника в инфраструктуру компании

16 дней

медианное время незаметного присутствия злоумышленника в инфраструктуре

2023 Global Threat Report // CrowdStrike
M-Trends 2023 // Mandiant (Google Cloud)

Особенности целевых атак (APT)

Финансовые и технические возможности

Организация подготовленной группой: APT-группировкой

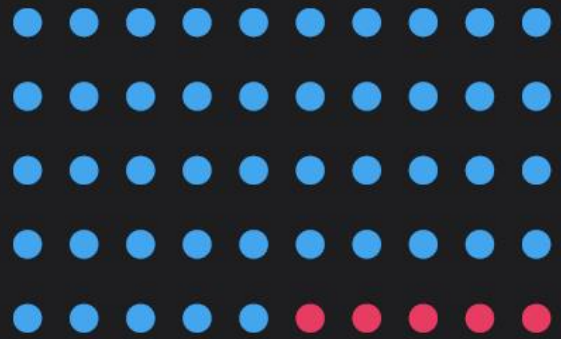
Долгосрочное и тщательное планирование: закупка инструментов, анализ инфраструктуры и другое

Сложности обнаружения: чистка логов и других следов

Нацеленность на конкретный объект: корпоративные секреты, исходники кода, топ-менеджмент

Длительности атаки: реализуется до конечного результата

Классические средства защиты



90% угроз

блокируют классические средства защиты

но не 10%

самых сложных

Используют поведенческий анализ

Опираются на описанную логику и правила

Быстро принимают решение

Проникновение в корпоративную сеть — вопрос времени

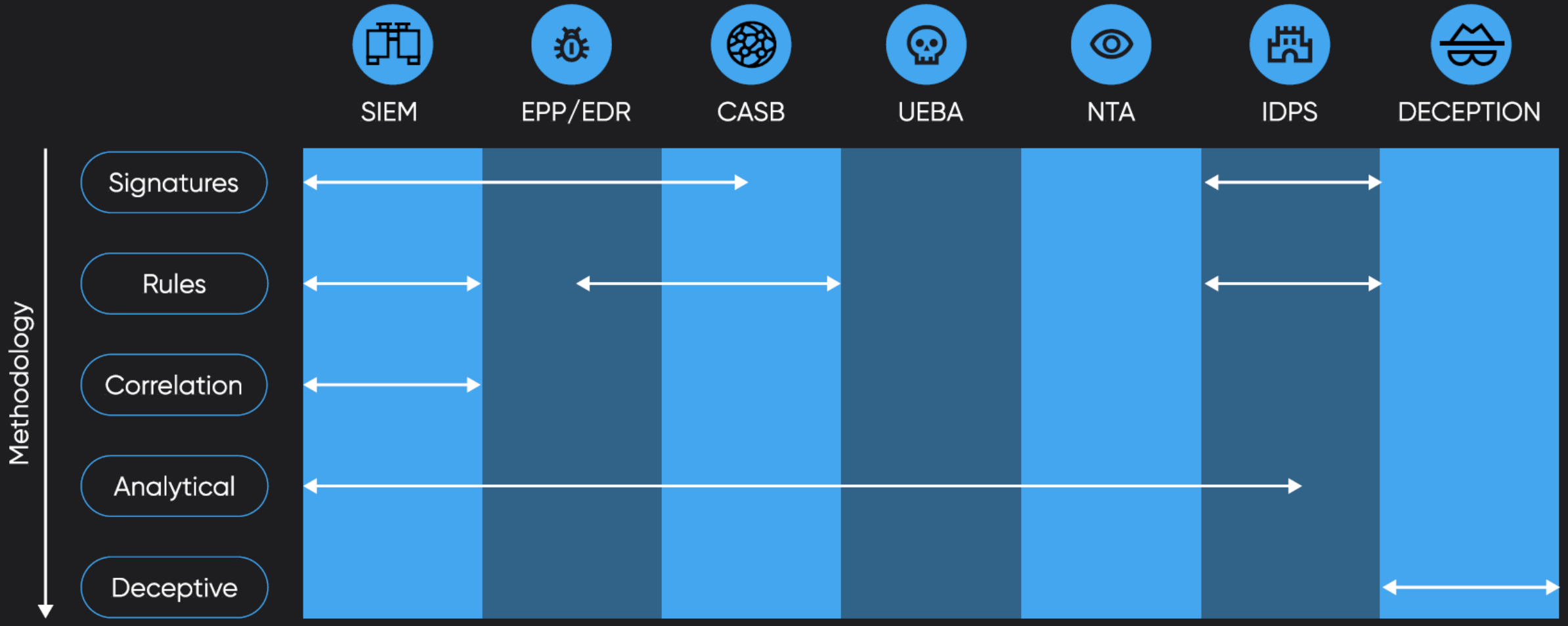
Уязвимости в Open Source компонентах

Снижение уровня защищённости

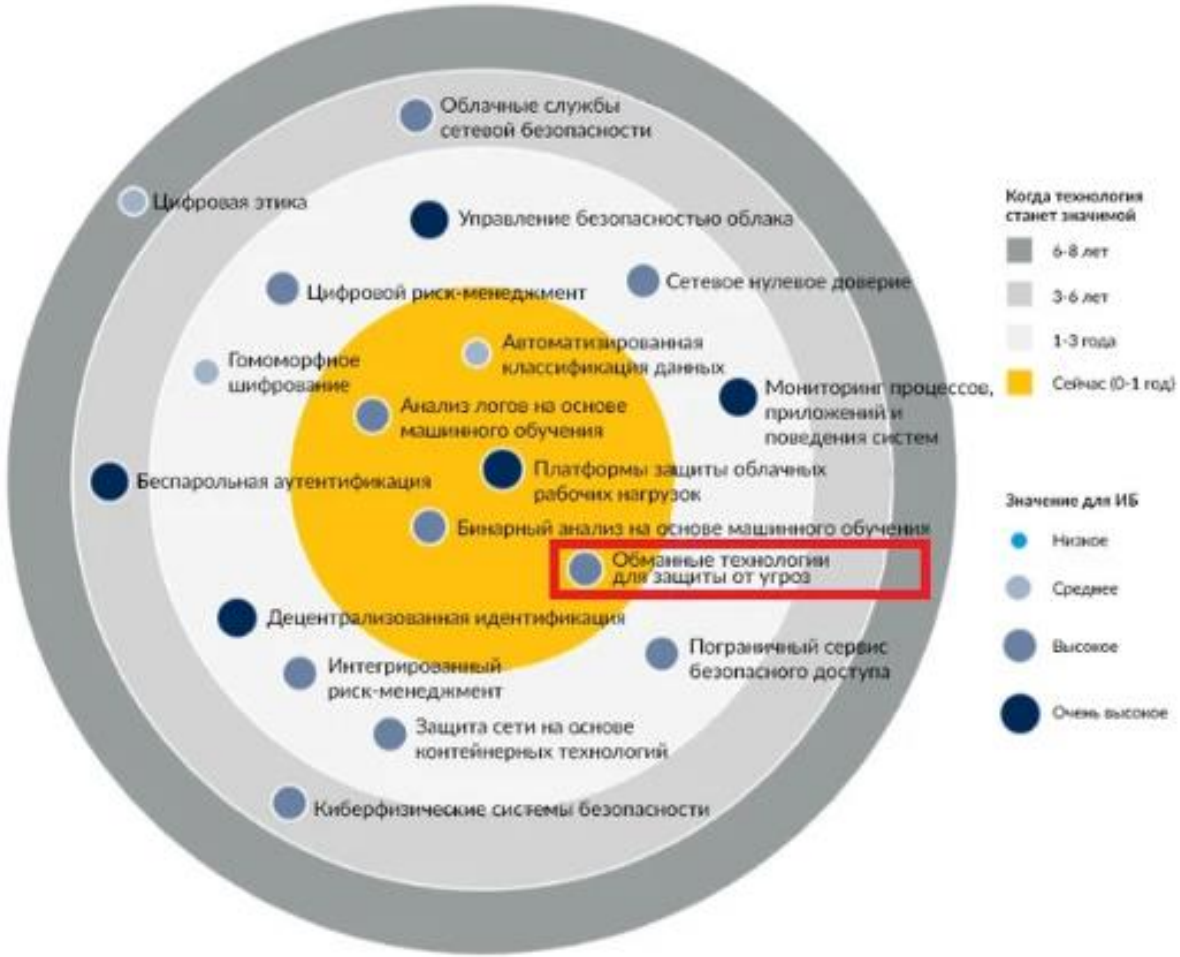
Компрометация менее защищённых компаний-подрядчиков

Использование методов социальной инженерии

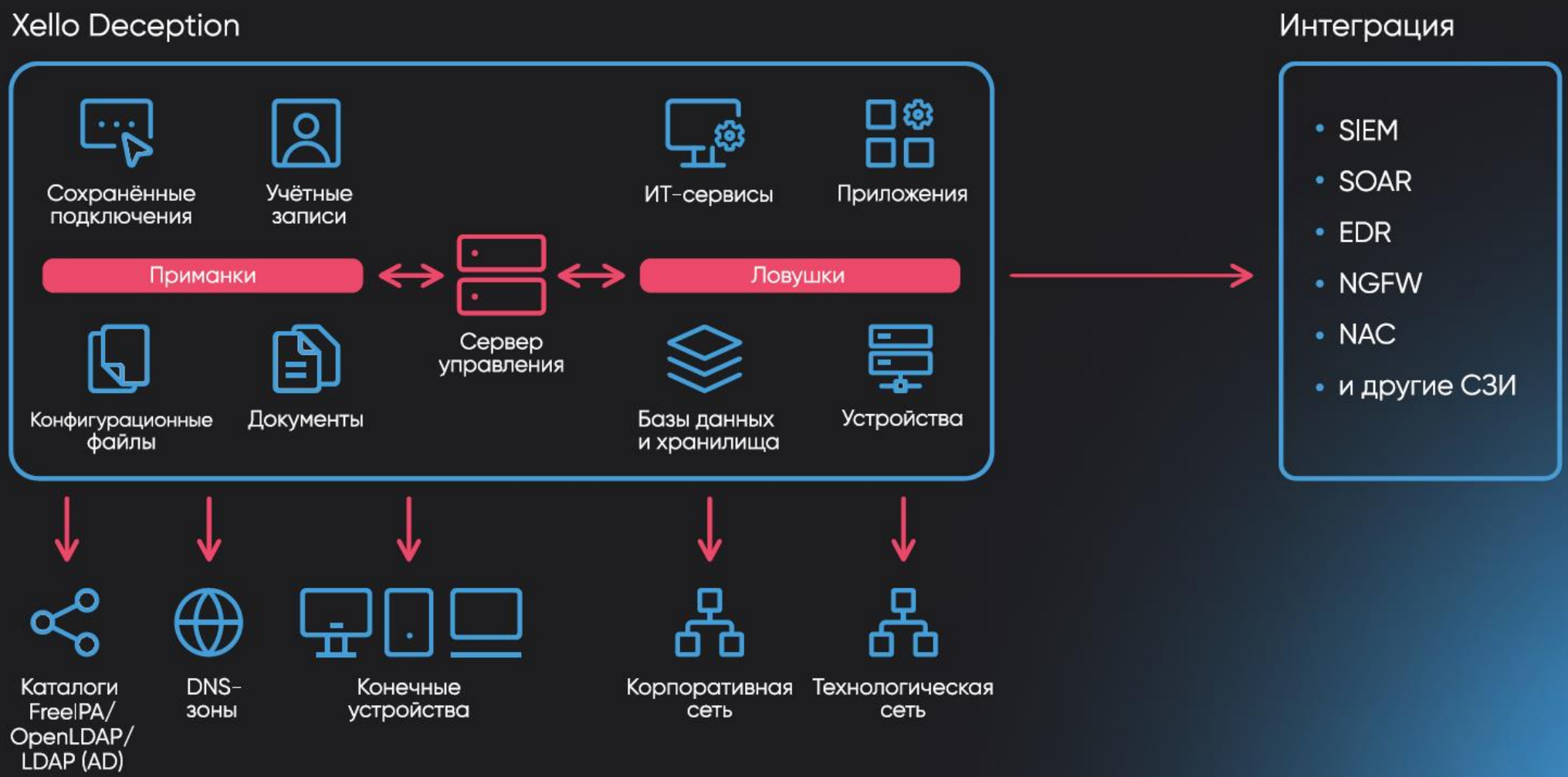
Другой подход выявления киберугроз



Радар новейших технологий и тенденций: Безопасность



Как это работает



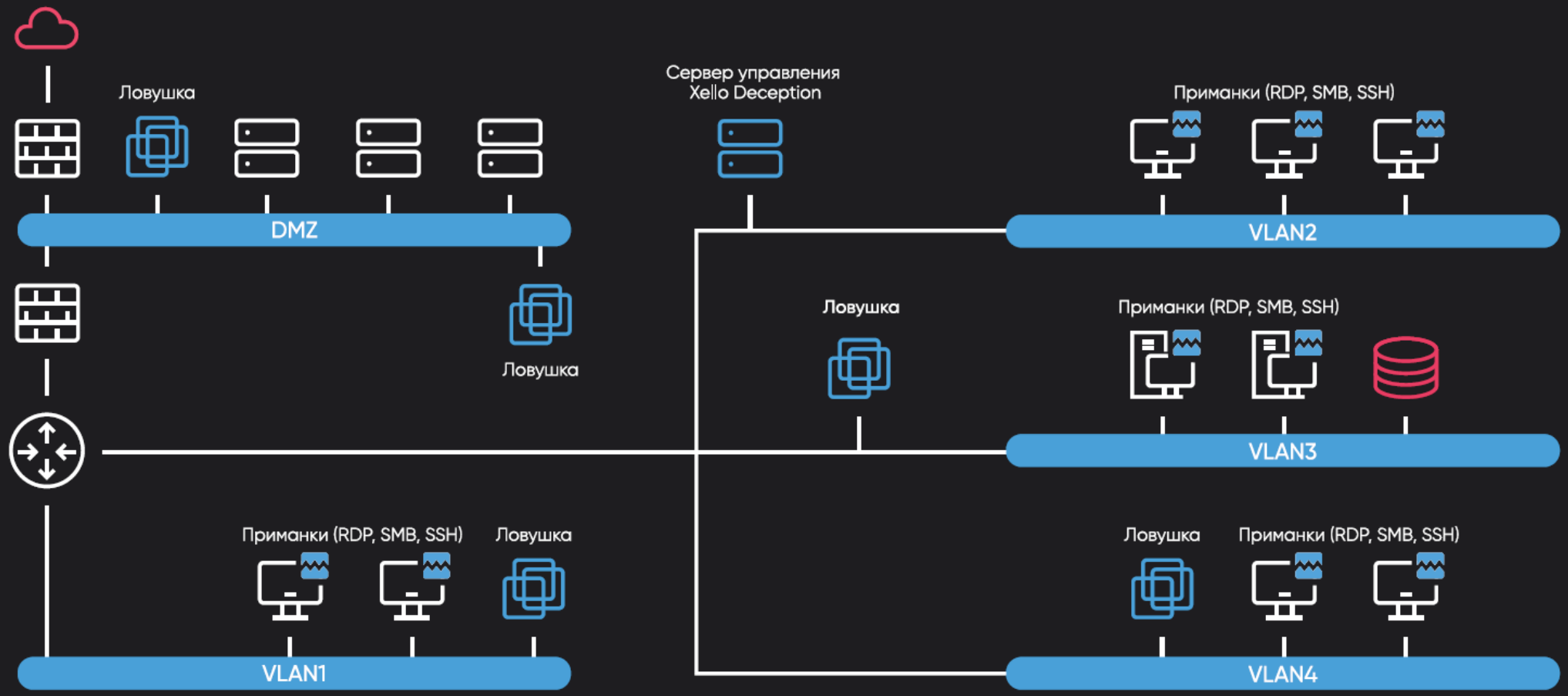
Место Xello Deception при APT-атаке

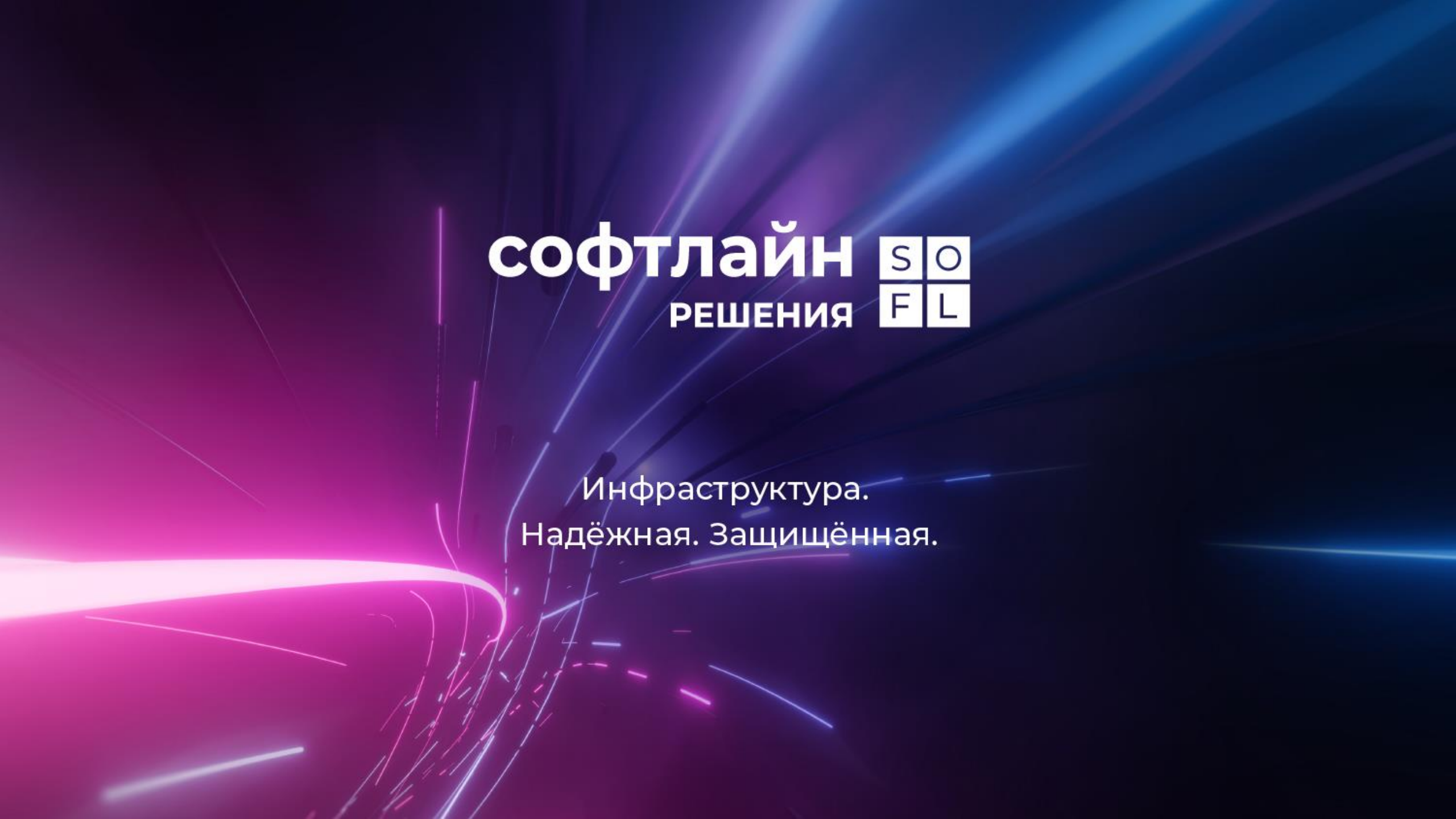
Горизонтальное передвижение — наиболее критический этап атаки

"

Периметровые средства защиты пропустили хакера и у него появляется возможность использовать легитимные протоколы и учётные записи для дальнейшей реализации кибератаки

Распределенные ложные данные и активы, которые невозможно избежать




софтлайн
РЕШЕНИЯ
SOFL
Инфраструктура.
Надёжная. Защищённая.