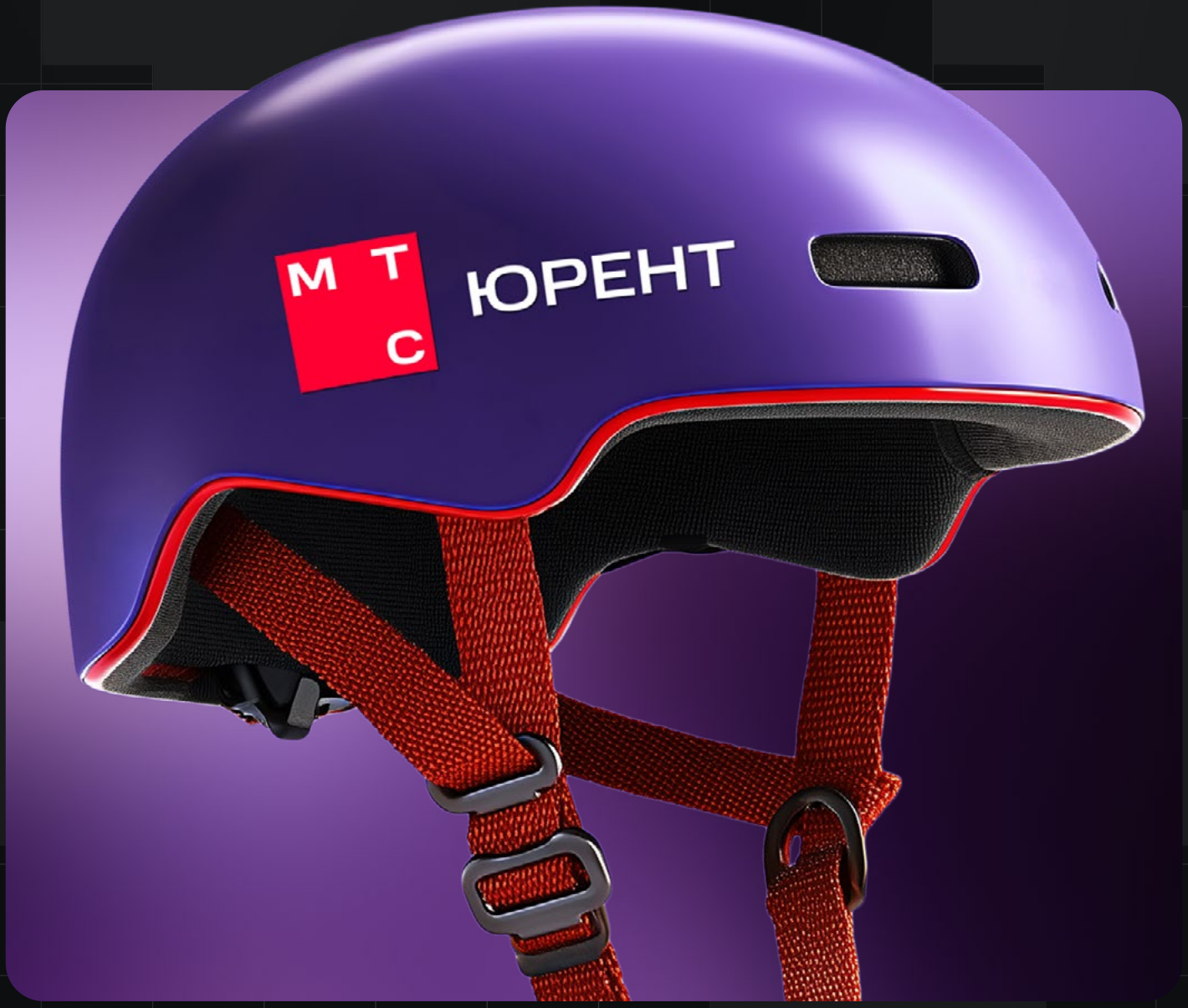
F6

Threat Intelligence | История успеха



МТС Юрент и F6: утечки под прицелом, доступы под контролем

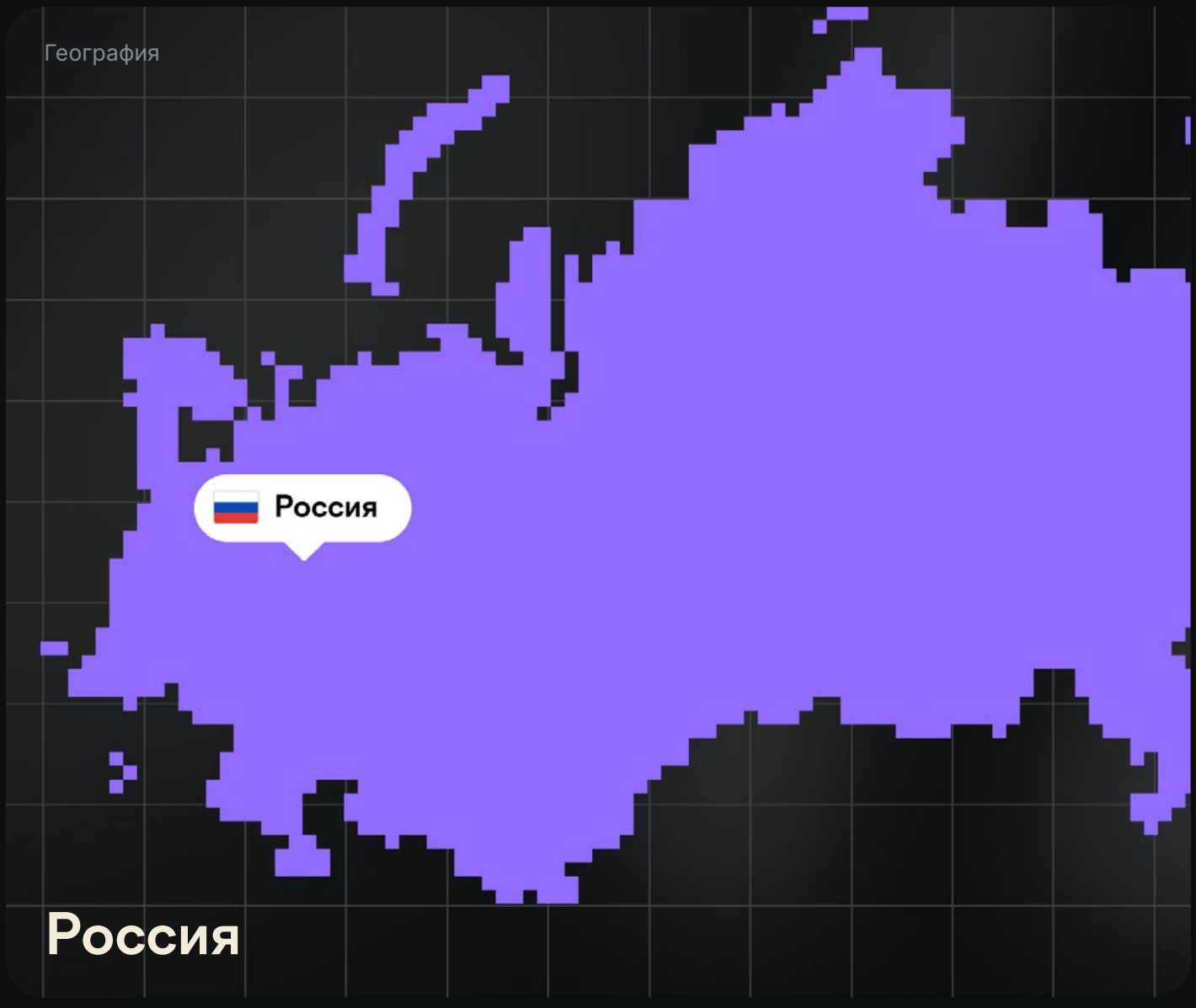
О компании

МТС Юрент — один из крупнейших российских сервисов кикшеринга. Компания управляет парком электросамокатов и электровелосипедов, работает в сотнях городов и полностью зависит от цифровой инфраструктуры: приложения, облака, распределённые офисы, партнёры.

Команда ИБ небольшая, при этом бизнес живёт в режиме постоянного масштабирования: летом нагрузка и количество хостов резко растут, в межсезонье снижаются.

МТС Юрент использует несколько продуктов F6, в том числе **F6 MXDR** и **F6 Threat Intelligence**. В этом кейсе фокус на том, как вокруг Threat Intelligence выстроена динамическая модель угроз и работа с утечками.

География



Россия

От классического ИБ к полностью цифровому бизнесу

Руководитель ИБ МТС Юрент пришёл в компанию с опытом работы в крупных организациях, которые находились под длительными атаками со стороны злоумышленников. Этот опыт сразу задал практичный подход: защита должна опираться на актуальные данные и давать бизнесу возможность действовать быстро.

В МТС Юрент условия были другими:

- полностью Digital продукт без «заводов и цехов»
- высокая доля облаков и внешних платформ
- географически распределённые команды
- постоянно меняющееся количество хостов в зависимости от сезона и спроса

Это создавало реальный риск: атакующий мог найти то, о чём сама компания уже не помнила.

Почему ставка сделана на Threat Intelligence

В МТС Юрент определили две ключевые задачи:

1. Понимать, какие угрозы актуальны прямо сейчас и как они меняются.
2. Быстро получать сигналы о продаже доступов, утечках и подготовке атак на компанию.

Для этого выбрали **F6 Threat Intelligence** в качестве основы динамической модели угроз.

Динамическая модель угроз

Классический подход: модель угроз утверждается на три-пять лет, любые изменения согласуются неделями. В быстро меняющейся цифровой среде это не работает.

В МТС Юрент зафиксировали в документах, что модель угроз динамическая и обновляется на основе данных Threat Intelligence. Команда регулярно заходит в **F6 Threat Intelligence** и смотрит:

- какие вредоносные кампании сейчас активны
- что меняется в тактиках и техниках атак
- какие тренды видны по профилю компании и индустрии
- где появляются риски у партнёров и подрядчиков, с целью исключения атак через цепочку поставок

На основе этой аналитики меняются настройки средств защиты информации, устанавливаются патчи безопасности, обновляется ПО.

«Утвердить модель угроз на три года и жить по ней в digital-среде — архаичный подход. Мы перешли на динамическую модель, которая опирается на Threat Intelligence и меняется вместе с ландшафтом угроз».

Герман Обручников

CISO МТС Юрент

Итог: защита подстраивается под реальные атаки, а не под устаревший документ.

Кейсы использования F6 Threat Intelligence

1. Продажа доступа к одной из систем

На даркнет-площадке появилось объявление о продаже доступа к одному из сервисов компании с уровнем прав «техник». Лот оценили в символическую сумму.

Как сработал F6 Threat Intelligence:

- модуль мониторинга даркнета зафиксировал объявление и сгенерировал алерт
- в течение нескольких минут команда ИБ увидела уведомление и связалась с поддержкой F6
- учётные записи проверили, доступы заблокировали, провели санацию и анализ происхождения утечки
- команда аналитиков оперативно отреагировала на появившееся объявление, проработала риск и предотвратила возможное использование доступа злоумышленниками

Расследование показало, что источник проблемы — личные смартфоны сотрудников, установивших сторонее приложение с встроенным трояном. Вредонос получил доступ к браузеру, забрал сохранённые пароли и передал их злоумышленникам. Через синхронизацию браузера данные попали и личные рабочие станции.

Критичный момент — время реакции. Без алерта **F6 Threat Intelligence** информация о продаже могла разойтись по другим площадкам и попасть к реальным покупателям. Здесь цепочку оборвали в момент появления объявления.

2. Утечки доступов сотрудников и быстрая санация

Другой эпизод связан с агрегатором утечек. **F6 Threat Intelligence** уведомил, что в опубликованной базе появились данные, соответствующие двум сотрудникам с доступом к внутренним системам.

Дальнейшие шаги:

- доступы оперативно отключили
- по артефактам и телеметрии нашли заражённые рабочие места
- провели санацию, выдали доступ только после очистки

Расследование показало, что первичный риск был у контрагента: на рабочей станции с доступом в административную панель пользователи параллельно заходили на небезопасный ресурс, устройство было заражено, а рабочей станцией пользовались несколько пользователей посменно.

Threat Intelligence в этой ситуации дал не абстрактный факт «где-то есть утечка», а конкретный повод запустить расследование, найти слабое место у партнёра и закрыть его.

3. Использование утечек в обучении сотрудников

В МТС Юрент Threat Intelligence встроен и в процессы повышения осознанности персонала.

Подход:

- анализируют ранее выявленные утечки, связанные с корпоративными пользователями МТС Юрент, и дополняют их проверенной информацией из открытых источников
- небольшая команда red team агрегирует информацию о сотрудниках, их публичных профилях и цифровых следах
- на этой базе строятся сценарии фишинговых сообщений, максимально похожие на реальные
- проводятся кампании по проверке устойчивости сотрудников к таким письмам и запросам

Сотрудники сталкиваются не с условными «учебными письмами», а с ситуациями, которые практически неотличимы от настоящих атак, построенных на реальных утечках.

Дополнительная роль MXDR и единой панели

Хотя основной акцент в этой истории на Threat Intelligence, в МТС Юрент отдельно отмечают связку с F6 MXDR и единой панелью управления.

Инфраструктура МТС Юрент постоянно увеличивается и уменьшается в зависимости от нагрузки. Раньше при таком режиме другие EDR-решения постоянно теряли хосты, создавали дубликаты в консоли управления и путаницу в учетных записях.

«В классических EDR при каждом пике нагрузки хосты терялись и дублировались. С продуктами F6 всё иначе: раздулись, сдулись — вся картина по хостам остаётся прозрачной, ничего не превращается в хаос».

Герман Обручников

CISO МТС Юрент

С текущей связкой MXDR и Threat Intelligence, компания существенно поднимает свой уровень Detection & Response на инциденты — видит актуальный состав хостов и может подключиться к каждому, даже если рабочая станция не подключена по VPN.

Для небольшой команды это критично: все данные по угрозам, утечкам и состоянию хостов собираются в одном месте, а реакции запускаются из одной панели.

Результат

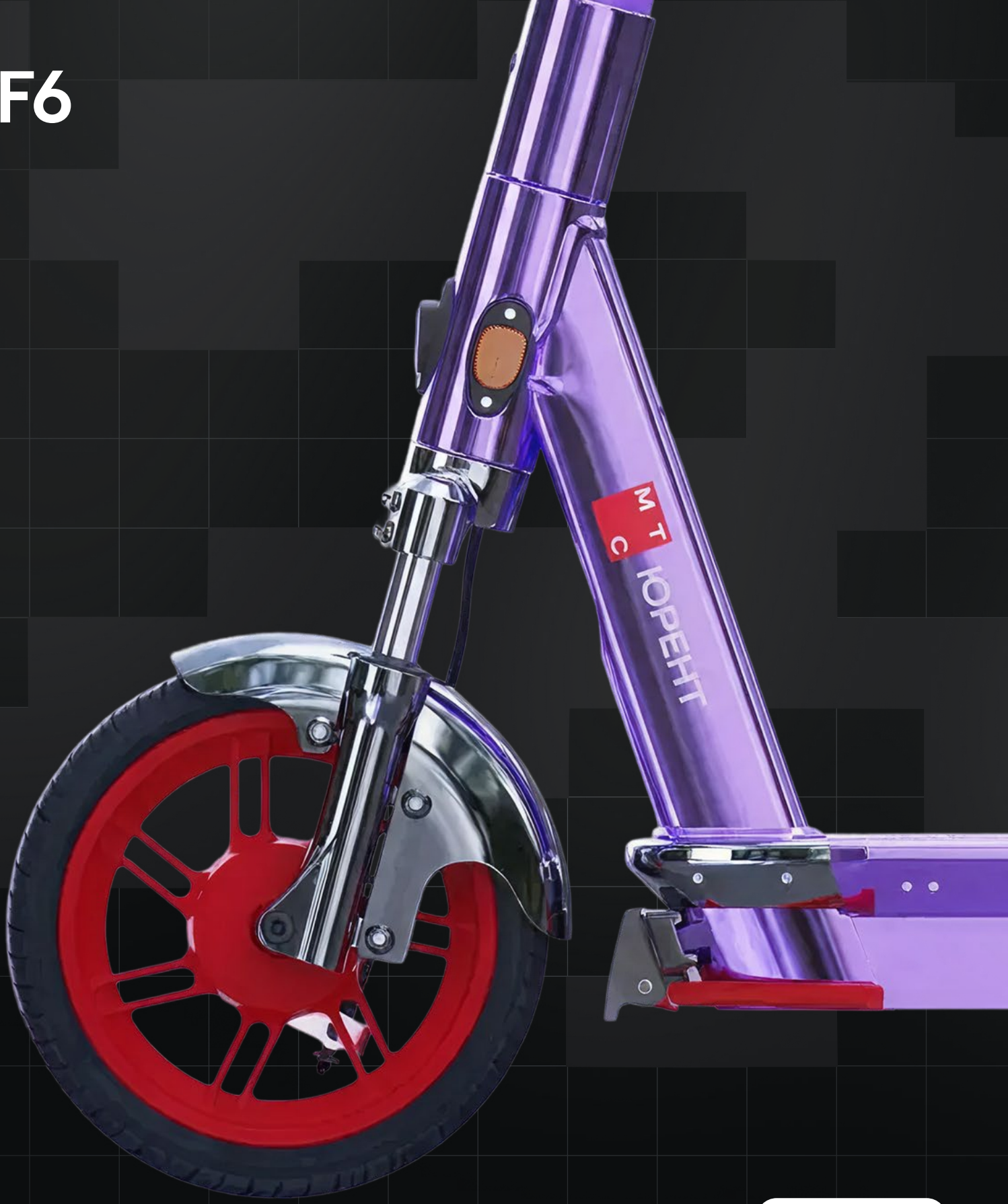
В МТС Юрент принципиально не рассматривают безопасность как набор «галочек» и список купленных продуктов. Каждый инструмент должен быть встроен в реальные процессы.

Использование F6 Threat Intelligence дало компании:

- живую, регулярно обновляемую модель угроз на основе реальных данных
- быстрые реакции на продажу доступов и появление учётных записей сотрудников в утечках
- возможность использовать данные потеницально скомпрометированных учетных записях и аналитику Threat Intelligence как основу для обучения и проверки сотрудников
- связку с MXDR, которая позволяет не только видеть угрозы, но и быстро действовать по каждому конкретному хосту

Для цифрового кикшерингового сервиса это превращает Threat Intelligence из формальных отчетов в рабочий инструмент, который ежедневно влияет на устойчивость сервисов МТС Юрент.

F6



Технологии для борьбы с киберугрозами

info@f6.ru +7 495 984-33-64 f6.ru