



Построение комплексной системы обнаружения и расследования инцидентов

Анатолий Фомин

CEO «SolutionFactory»

региональный продуктовый бизнес, работающий на стыке технологий,
образования и креативной экономики.

СТРАТЕГИЧЕСКАЯ ЦЕЛЬ

До конца 2028 года иметь в портфеле 10+ конкурентноспособных на разных рынках продуктов с оценкой более 10 млн \$ каждый.



**фабрика
решений**

5 стран

в которых работают
наши продукты

>200 проектов

над которыми мы
работали

6 продуктов

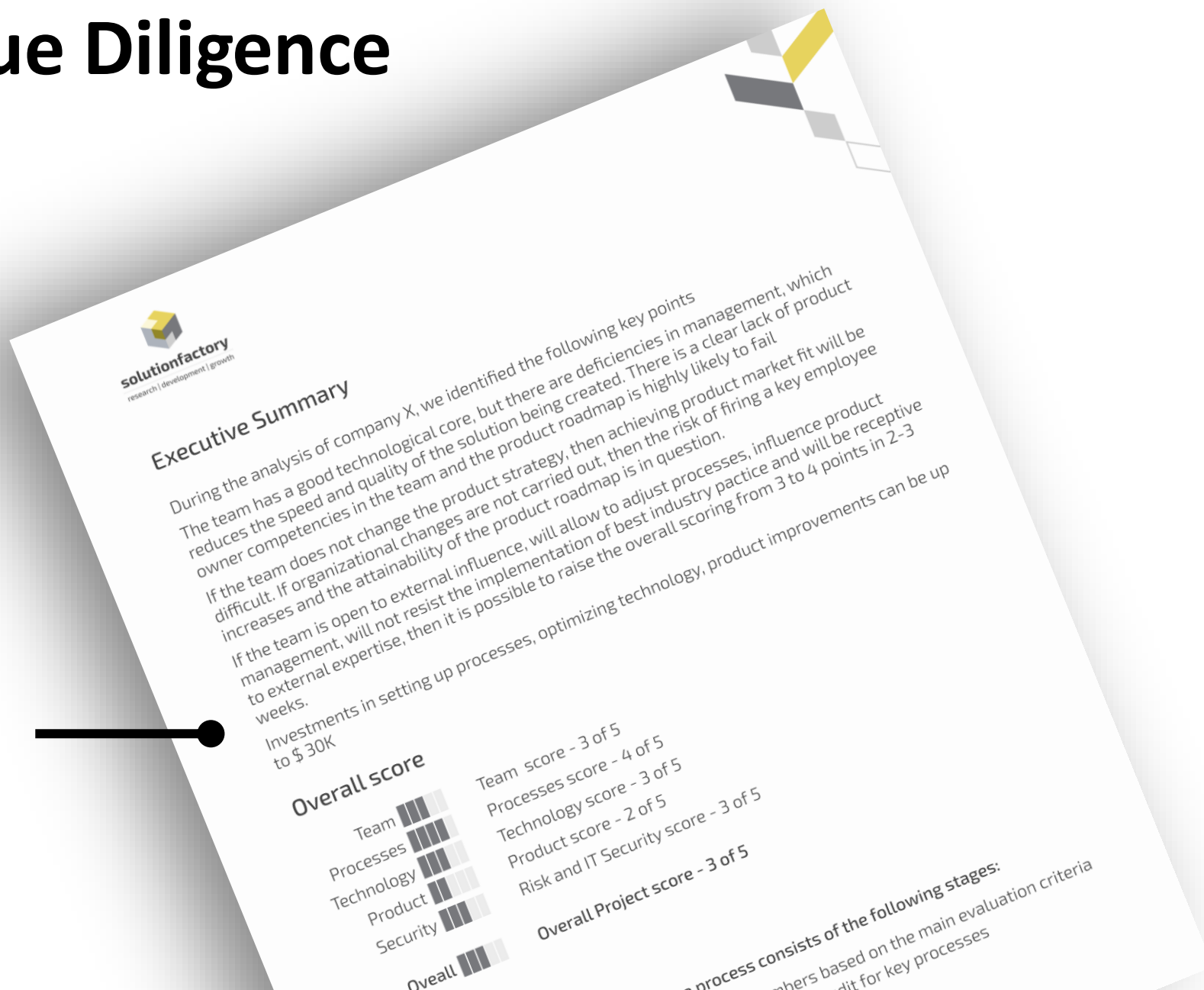
которые являются
собственностью
компании

93 инженера

в команде

Technical Due Diligence

Шаблон отчета-аудита
для венчурного фонда



TELCELL

Project
99,9%



фабрика
решений

Концепция:

SaaS платформа, которая трансформирует подход IT команд к мониторингу и управлению качеством услуг. В отличие от традиционных систем мониторинга (Datadog, NewRelic), которые фокусируются на технических метриках, ServiceVitals создает независимый реестр деградации пользовательского опыта — своего рода "черный ящик" приложения, который объективно фиксирует моменты, когда услуга перестает соответствовать ожиданиям пользователя. Важный аспект в том, что система фиксирует и инциденты связанные с информационной безопасностью.

Ключевой принцип: Система работает как внешний арбитр, независимый от IT отдела и отдела ИБ, который честно фиксирует:

- Начало проблемы (момент, когда пользователь испытал деградацию)
- Конец проблемы (момент, когда услуга восстановилась)
- Тяжесть и масштаб (сколько пользователей затронуто)
- Бизнес-последствия (потери, репутация)



фабрика
решений

Основная идея:

Это платформа объективного мониторинга качества обслуживания, которая: не доверяет ИТ-метрикам — создает независимый "судебный протокол" деградации сервиса с точки зрения пользователя и нарушения политик безопасности

- Преобразует наблюдения в знания — каждый инцидент → расследование → обучение → улучшение
- Управляет непрерывным циклом — от обнаружения через анализ к превентивным мерам
- Прозрачна для стейкхолдеров — открытый реестр инцидентов и действия команды (как Cloudflare Status)

Важные моменты:

- ✅ Система как "независимый арбитр" — она фиксирует инциденты объективно, не зависит от IT
- ✅ User-centric метрики — не только технические метрики, но и то, что пользователь действительно испытывает
- ✅ Непрерывный процесс улучшения — от инцидента → к расследованию → к action items → к предотвращению
- ✅ Прозрачность — status page как инструмент доверия и коммуникации с клиентами
- ✅ Культурный shift — от реактивного (fixing) к проактивному (preventing) подходу



На какие проблемы и как отвечает:

Проблема	Текущее состояние	Решение ServiceVitals
Субъективность	IT говорит "все было хорошо", пока не получат жалобу	Объективный реестр деградации независимо от жалоб
Реактивность	Проблемы выявляют пользователи, компания реагирует поздно	Система фиксирует проблему в момент возникновения
Разрозненность	Разные системы мониторинга, логи, тикеты разбросаны	Единый источник истины про инциденты и их статус

Как это решает проблему TelCell:

Было:

- ИТ говорит: "Все нормально, метрики в порядке"
- Пользователи говорят: "Приложение виснет"
- Руководство не знает, верить кому

Стало:

- Независимая система фиксирует: "С 14:23 по 14:45 пользователи 15 сек ждали QR код"
- Post-mortem: "Причина — DB N+1, контр-меры планируются"
- Статус-страница: все знают, что произошло, что делается
- Тренд: "В этом месяце было 3 инцидента, это на 40% меньше, чем в прошлом" — видно прогресс 5. Финансовые кома для расчета SLA и штрафов



фабрика
решений

Дополнительные идеи для расширения:

- **Predictive Alerting** — система учится на исторических данных и предупреждает за 5 минут до падения
- **Chaos Engineering Integration** — плановые "инцидентные учения" чтобы тестировать реакцию команды
- **Customer Impact Segmentation** — не все пользователи одинаковы (VIP vs обычные), разные SLA
- **Anomaly Detection** — ML автоматически обнаруживает аномалии, даже если триггеры не срабатывают
- **Бенчмарки конкурентов** — сравнение: "У нас MTTR = 15 мин, у Yota = 20 мин" (если у них есть публичная страница)





Анатолий Фомин

@av_fomin



ДАВАЙТЕ
ОБСУДИМ

LET'S
TALK

660021 РОССИЯ
СИБИРЬ
КРАСНОЯРСК
пр. Мира 115а стр.1
+7(965)-896-80-11

WE DELIVER
ULTIMATE
IT SOLUTIONS
BASED ON
CUTTING EDGE
TECHNOLOGIES

SOLUTIONFACTORY.RU

ООО "Фабрика Решений":



КРИТЕИ