Дмитрий Мананников

Возможности применения мониторинга бизнес-процессов для целей различных бизнес функций

Дмитрий Мананников

Директор по безопасности OBI

Опыт управления безопасностью в коммерческих компаниях 17 лет

Имею успешный опыт выстраивания процессов безопасности в кредитно-финансовой сфере, энергетике, логистике и ИТ. Методолог. Автор ряда методик оценки эффективности безопасности.

Преподаватель в рамках программ МВА РАНХиГС

Современный уровень информатизации позволяет нам создавать цифровые двойники бизнес-процессов, которые в высокой степени отображает все события процесса в виде последовательности информационных артефактов, отслеживаемые в режиме реального времени.

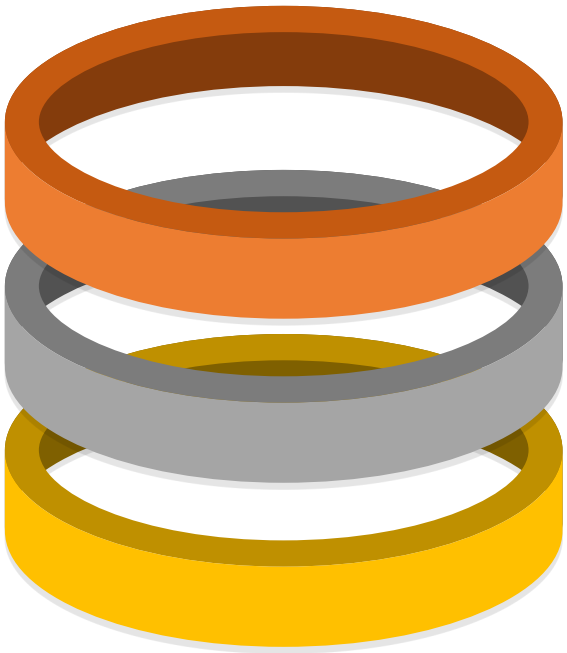
«простите, а МОНИТОРИНГ ПРОЦЕССОВ это тоже самое, что и BI?»

События в информационных системах

Последовательность событий в процессе, соответствующих действиям пользователей, работе систем, создаваемы и обрабатываемых документов и событий.

Логика процесса

Последовательность действий в процессе.

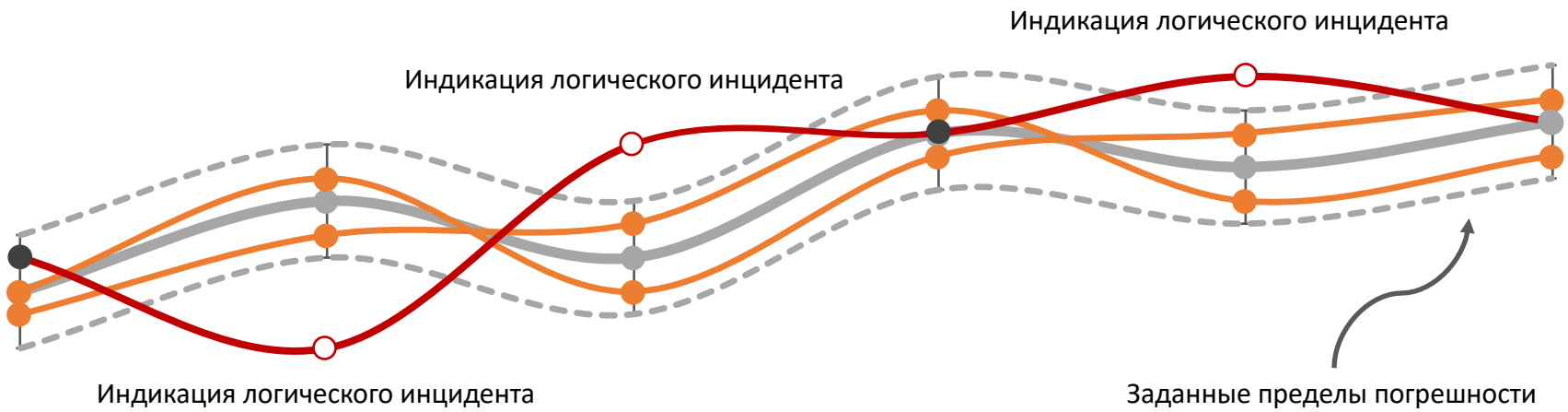


Максимальная достоверность цифрового двойника процесса

Достигается путем анализа трех информационных слоев. Поскольку полная картина бизнес-процесса не может быть восстановлена только лишь за счет данных основных (транзакционных систем). Данный подход позволяет воссоздать цифровой отпечаток процесса с точностью до 90%

1. **Контекстный**
   Информационный слой содержащий смысловую информацию. Данные электронной почты, корпоративных мессенджеров, содержимое документов и прочих.
2. **Транзакционный**
   Информационный слой содержащий данные и транзакции в основных продуктивных системах. ERP, CRM, DockFlow, WMS и прочих.
3. **Событийный**
   Информационный слой содержащий данные о событиях на уровне техники. Информация с контролеров домена, IOT устройств, различных датчиков и камер наблюдения и прочих.

ПОСТРОЕНИЕ МОДЕЛИ ОТКЛОНЕНИЙ



1 Даже если нет явной формализации процесса (его описания в какой либо из нотаций) процесс все равно существует в виде постоянной последовательности событий направленной на достижение единицы результата. Что позволяет его вычислить на уровне событий ИТ систем.

2 Мониторинг процесса в нескольких итерациях, позволяет построить автоматизированную контрольную среду. И выявлять любые отклонения от заданной логики, влекущие за собой изменение качества этого процесса, или потребляемых им ресурсов

Новые качества процесса *

Через измерение параметров процессов и их жизненного цикла, мы получаем новые (измеряемые) свойства процесса

Здоровье процесса

Как показатель соответствия единицы процесса условному эталонному процессу, или статистическим среднему значению совокупности процессов

Доверенность процесса

Как показатель легитимности процесса (или события внутри процесса) вычисляемое через сличение предшествующих ему событий или процессов

ИММУНИТЕТ ПРОЦЕССА

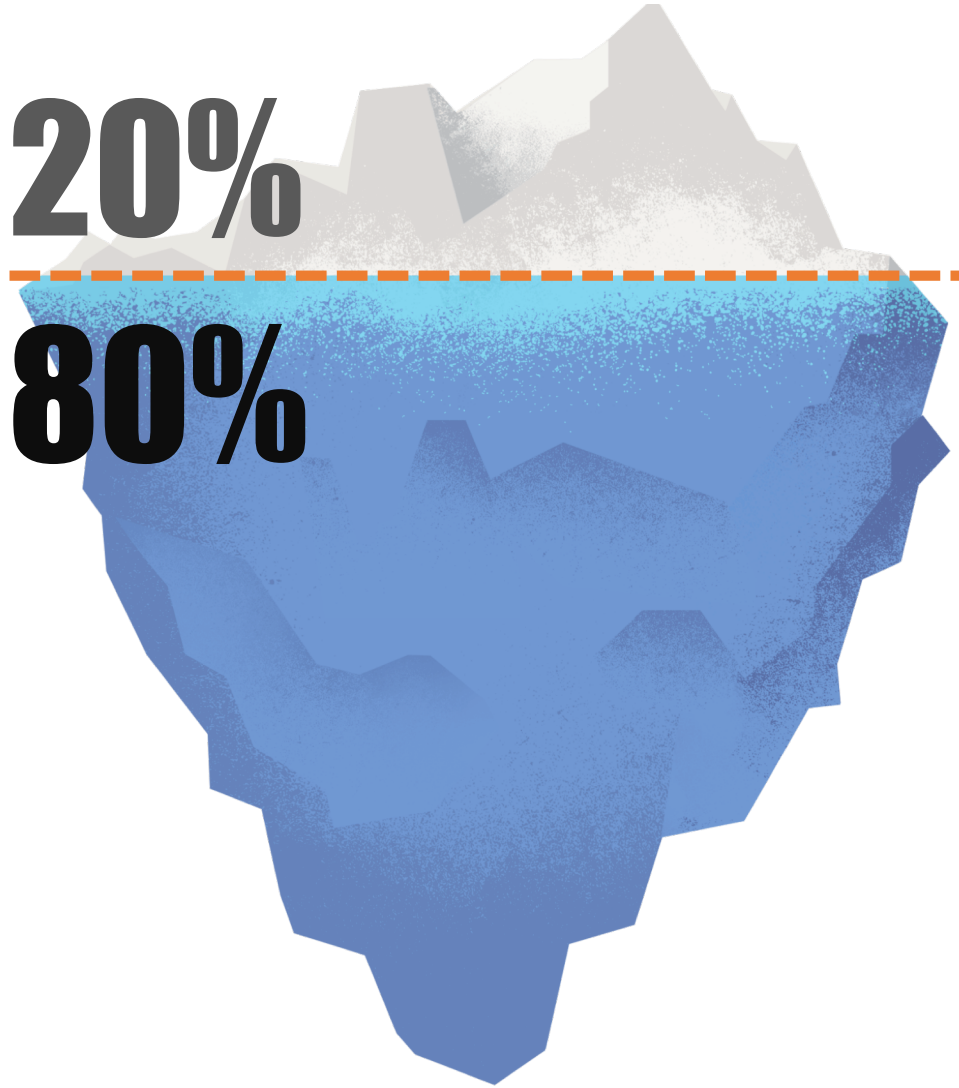
* «К проблеме оценки и обеспечения корректности бизнес-процессов» - Безопасность информационных технологий (Том 26, № 3 (2019))
Касперская, Кузьменко, Мананников, Хайретдинов, Щербаков

Мониторинг

18+

Инциденты

Причина и основа существования «безопасности» как функции. И единственная вещь на которую функция влияет. И единственная «переменная» изменение которой коррелирует с множеством «переменных» в функции. С бюджетом, стратегией, техническими или организационными нормами, зарплатами и количеством работников и прочими (всеми) другими.



инциденты
«БЕЗОПАСНОСТИ»

инциденты внутри
БИЗНЕС-ПРОЦЕССОВ

Ущерб являющийся следствием инцидентов в большей своей части лежит именно в области инцидентов внутри бизнес-процессов. По отдельности каждый из инцидентов подобного рода выглядит незначительным, и скорее воспринимается как ошибка чем злонамеренное действие. Однако в общей своей массе, совокупный ущерб от подобного рода инцидентов – значителен.
Что важно! Это не отложенные риски с прогнозируемой вероятностью наступления. Ущерб от инцидентов внутри бизнес-процессов, это фактически ежедневные потери имеющие прямую корреляцию с операционными показателями компании и качеством выпускаемого продукта.

Соотношение потерь от инцидентов в корпоративной среде

Разделение по уровням

Все инциденты равны, но некоторые инциденты равнее других. Или как это обычно работает…

safety

Инциденты которые по отдельности не «страшны», но в совокупности дают эффект, достаточный для инвестиций на коррекцию

«декостылизация»

security

Классические инциденты ИБ «как мы любим».

Приводящие к значительным ресурсным потерям.

Требующие полного «классического» цикла

operations

Инциденты живущие в рамках операционных «проблем».

Быстро решаемые. По совокупности потерь не тянущие даже на «костыли»

Локирование инцидентов

для всех инцидентов нам интересны следующие элементы

бизнес-логика

Почему это проблема?

В каком процессе?

В каком из блоков процесса?

Как повлияло на процесс?

Как повлияло на другие процессы

люди, техника и время

Где эта проблема?

Кто источник(роль\имя)?

Кто пострадавший (роль\имя)?

Где проблема в железе?

Где проблема в системе?

Когда она произошла?

регламенты

Вопреки чему эта проблема?

Нарушенные инструкции?

Нарушенные регламенты?

Обойдённые правила?

БИЗНЕС БЕНЕФИТЫ

Что данный подход дает в бизнес контексте

01

ОШИБКИ БИЗНЕС-АРХИТЕКТУРЫ

Фактически, статистика собираемая таким способом начнет показывать «бутылочные горлышки» в рамках существующих бизнес-процессов. И явится триггером для их реинжиниринга

02

КАЧЕСТВО ПРОЦЕССА\ПРОДУКТА

Инцидент (их совокупность) становится параметром для оценки качества процессов продуктов, которое можно учитывать при дизайне (помните - security by design?)

03

ПЕРФОМИНГ ПРОЦЕССОВ

Инцидент становится исчисляемым количественным параметром влияя на который мы получаем влияние на основной бизнес-показатель самого процесса

04

БЕНЧМАРКИНГ

Инциденты становятся одним из бенчмарков для внутренней оценки одинаковых процессов проходящих на разных площадках

КОМУ МОЖЕТ БЫТЬ ПОЛЕЗНО?

ОПЕРАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ	ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ	ВНУТРЕННИЙ КОНТРОЛЬ
Повышение операционных показателей, достигаемое за счет снижения количества ошибок в бизнес-процесса. И предотвращения перерасхода ресурсов	Формирование цифрового иммунитета процесса, свойства позволяющее предиктивно выявлять и не допускать любые ошибки процесса. Равно как и несанкционированные вмешательства, фрод и нарушения инструкций.	Снятие нагрузки на бизнес возникающей при процессах аудита, при этом увеличивая плотность аудитов до 100% от общего количества процессов. Тем самым делая бизнес абсолютно прозрачным.

Спасибо за внимание!

Возможно есть вопросы?

dmitriy.manannikov

dmitriy@manannikov.ru