

Follow the sun



ОПЫТ SOLAR JSOC В ПОСТРОЕНИИ
ГЕОРАСПРЕДЕЛЕННЫХ ДЕЖУРНЫХ СМЕН

SOC FORUM 2023



СТЕЧЕНКО НИКИТА

Руководитель отдела технической
обработки инцидентов ГК СОЛАР

Актуально

- [01] КОМПАНИЯМ С ДЕЖУРНЫМИ СМЕНАМИ,
РАБОТАЮЩИМИ 24/7
- [02] КОМПАНИЯМ, ПЛАНИРУЮЩИМ
ВНЕДРЯТЬ ФОРМАТ 24/7
- [03] КОМПАНИЯМ, ОЦЕНИВАЮЩИМ РЕНТАБЕЛЬНОСТЬ
ТАКОГО ФОРМАТА, РИСКИ И НЕОБХОДИМОСТЬ

Основные опасения при работе с геораспределенными командами*



Сложности с передачей информации



Отрыв от коллектива



Снижение качества экспертизы



Потеря в других филиалах контекста происходящего



Трудности с обучением и внедрением в рабочий процесс



Контроль работы удаленных сотрудников

* Тезисы сформулированы по результатам общения с компаниями, которые находятся в процессе планирования, стройки, расширения своего SOC

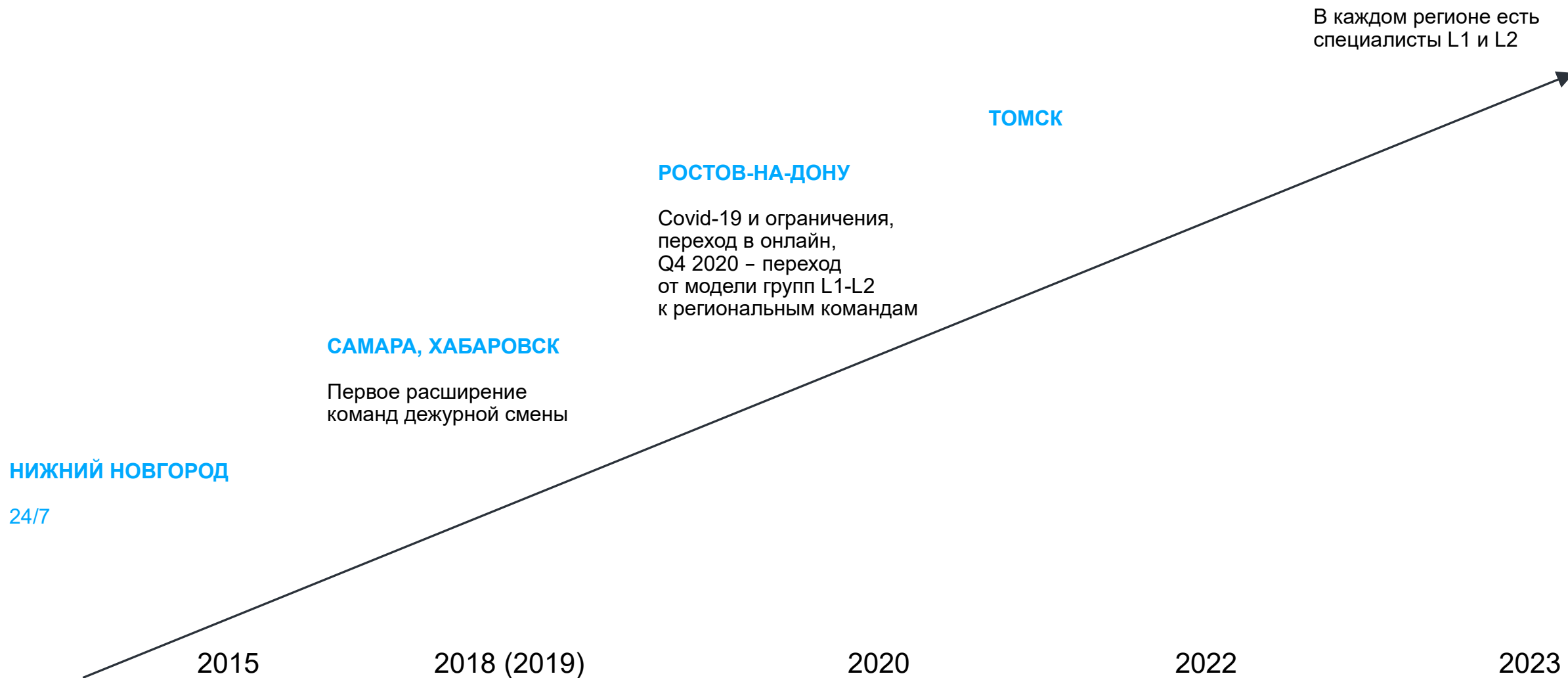
Очевидные плюсы расширения географии

НОВЫЕ ИСТОЧНИКИ
КАДРОВ

УХОД ОТ НОЧНЫХ СМЕН
ИЛИ СНИЖЕНИЕ ИХ ЧИСЛА

ГЕОРЕЗЕРВИРОВАНИЕ
БЕСПЕРЕБОЙНОГО ПРОЦЕССА

Как мы росли



Как менялось расписание

GMT+3
Москва
Нижний Новгород
Ростов-на-Дону

GMT+4
Самара

GMT+7
Томск

GMT+10
Хабаровск

ГОД	ГОРОД	ДЕНЬ	ВРЕМЯ	ДЕЖУРСТВО	СМЕНА
2016	Нижний Новгород	Будни	08:00-20:00	08:00-20:00	12 часов дневная, 12 часов ночная, «усиление» 5 на 8
			10:00-18:30		
			20:00-08:00		
		Сб, Вс, праздники	08:00-20:00	08:00-20:00	12 или 24 часа в субботу и воскресенье дежурства идут стык в стык
		20:00-08:00	20:00-08:00		
2019	Хабаровск	Будни	01:00-09:30	01:30-08:30	плавающая пятидневка
	Самара		08:00-16:30	08:00-13:30	8 часов в будни, 10 часов в выходные
	Нижний Новгород		10:00-20:00	13:00-18:30	10 часов дневная и 8 часов вечерняя дежурства идут с наслоением
			17:30-02:00	18:00-02:00	
	Хабаровск	Сб, Вс, праздники	01:00-09:30	01:30-08:30	плавающая пятидневка
	Самара		08:00-18:00	08:00-13:30	8 часов в будни, 10 часов в выходные
	Нижний Новгород		10:00-20:00	13:00-18:30	10 часов дневная и 8 часов вечерняя дежурства идут с наслоением
			17:30-02:00	18:00-02:00	
2023	Хабаровск	Любой	01:00-09:30	01:30-09:00	плавающая пятидневка
	Томск		05:00-15:00		10 часов дневная
	Самара		08:00-18:00	08:00-13:30	10 часов дневная, 8 часов вечерняя
	НН / Ростов-на-Дону		09:00-19:00		10 часов дневная, 8 часов вечерняя
	НН / Ростов-на-Дону		10:00-20:00	12:30-19:00	10 часов дневная, 8 часов вечерняя
	Самара		16:30-01:00		10 часов дневная, 8 часов вечерняя
	НН / Ростов-на-Дону		17:30-02:00	18:00-02:00	10 часов дневная, 8 часов вечерняя

Что важно учитывать при составлении расписания

ВРЕМЯ НА ПЕРЕСМЕНКУ

- чтобы новые сотрудники могли перестроиться на рабочую активность и в спокойном темпе подхватить задачи

БАЛАНС РАБОТЫ

- соблюдать баланс работы в субботу, воскресенье, праздники и вечерние смены
- непрерывный отдых минимум 2 дня подряд
- никаких дневных смен после вечерних/ночных, особенно, при переходе из недели в неделю
- помнить про ТК РФ

КОНТРОЛЬ ЗАГРУЗКИ СМЕНИ

- контроль за загрузкой каждой тайм-зоны
- корректировка смен на основании метрик, своих наблюдений и фидбэка сотрудников

НОРМА ЧАСОВ

- делать поправку на индивидуальную занятость: 20/30/40 часов в неделю
- контролировать норму часов

С чего начать

Вроде бы и очевидно, но...

[0] АВТОМАТИЗИРОВАТЬ ТО, ЧТО МОЖНО

- Посмотреть на процессы и задачи и понять, а точно ли нужны новые люди или можно упростить жизнь уже имеющимся?
- Оценить, на что приходятся основные трудозатраты и можем ли мы с этим что-то сделать?

[2] ЗАФИКСИРОВАТЬ И ОПИСАТЬ ПРОЦЕССЫ

- Зафиксировать и структурировать в БЗ рабочие процессы, плейбуки, статьи. Они должны быть реальными, использоваться в работе, быть не для галочки
- Должны быть понятны не только составителю, но и исполнителю

[1] ОЦЕНИТЬ ТЕКУЩУЮ ЗАГРУЗКУ ДЕЖУРНОЙ СМЕНЫ

- Учитывать не только статистические данные и свое восприятие, но и мнение сотрудников «с полей»
- Выделить проблемные тайм-зоны. Это может быть не только ночь, но и раннее утро по Москве

[4] НАЙТИ МЕСТО ДЛЯ РАСШИРЕНИЯ КОМАНДЫ

- Где уже есть офис компании
- Удобный с точки зрения часового пояса и профиля нагрузки регион
- Кадровые перспективы (вузы, оценка конкуренции и т. д.)
- Руководитель или специалист с опытом, вокруг которого будет строиться команда

[3] EMPLOYEE JOURNEY MAP

- Процесс обучения и адаптации должен быть описан и понятен как для ментора, так и для нового сотрудника
- Все основные вехи зафиксированы, а сами сроки прохождения обкатаны на практике
- «Играющий тренер» – в обучение вовлекаются только действующие специалисты

[5] СТАРТУЕМ

- После первичного онбординга в онлайн-формате командировем новых сотрудников в головной офис, знакомимся и погружаем их в процессы
- Неделя – минимум, две – оптимальный срок
- Далее: командировочный цикл в регион или из региона, но по мере роста локальной экспертизы острая потребность в этом отпадет

Про процессы

Есть опасение, что в геораспределенных командах теряется контекст происходящих срабатываний, образуются информационные вакуумы
Как мы с этим боролись

ВНЕДРЕНИЕ В ПРОЦЕСС

общие правила работы внедрять
в процесс, автоматизировать

осуществлять информирование
о появлении новой сущности,
вести хронологию изменений

проводить приемку со стороны
дежурной смены

REAL TIME

коммуникации между дежурными:
чаты, АКС, очное общение

ДОЛГОСРОЧНЫЕ УСТАНОВКИ

вся полезная, но временная
информация должна храниться
в одном месте

таблица в базе знаний со статусами:
что за установка, от кого информация
получена, на какой срок актуальна

ОТЧЕТ О ПРОИСШЕСТВИЯХ

для фиксации ситуаций, ведения
их истории и последующего анализа

отчеты о сбоях, происшествиях,
эскалациях

КРАТКОСРОЧНЫЕ УСТАНОВКИ

фиксация + уведомление всех
вовлеченных о краткосрочной установке
на понятный интервал времени

отдельный чат со сжатой информацией
оперативного характера

CASE REVIEW & INCIDENT HISTORY

доступ к истории всех инцидентов
за все время в режиме real time

контроль качества разбора, фиксация
результатов и донесение до всех
сотрудников положительных и
отрицательных моментов

Про технологии

ПРИОРИТИЗАЦИЯ ИНЦИДЕНТОВ

стандартизировать порядок взятия в работу подозрения на инцидент

внедрить весовую модель на основании: релевантности сценария; значимости активов; критичности влияния на инфраструктуру/бизнес; изолированности инцидента...

СВЯЗЫВАНИЕ АКТИВНОСТЕЙ

автоматизированный контроль за цепочками срабатываний

подсвечивание неизолированных и взаимосвязанных активностей на уровне SIEM/IRP/SD

ЦЕНТРАЛИЗАЦИЯ ПОТОКОВ ИНФОРМАЦИИ

максимально уходить от ситуаций, когда одну активность ведем в почте, другую – в Service Desk, для третьей есть IRP, а по этой вообще обсудим по телефону

сводить все к минимуму интерфейсов

PLAYBOOKS

настроить workflow в SD/IRP по автоматическому контролю выполнения необходимых этапов проведения расследования и дальнейшей обработки подозрения на инцидент

ПОДРОБНОСТИ НА НАВР



Опыт JSOC в менеджменте удаленных команд. Часть 1

SOC
FORUM
2023

РУКОВОДИТЕЛЬ ОТДЕЛА

Region Leaders

в каждом регионе есть свой локальный лидер, отвечающий за инженеров L1 и L2, чувствующий «боли» на местах за счет плотного контакта с командой

РУКОВОДИТЕЛЬ ОТДЕЛА

TL_1st line & TL_2nd line

есть отдельные тимлиды команд 1-й и 2-й линий, у каждого из них своя геораспределенная команда

практика перекрестных командировок: новые сотрудники ездят в головной офис на 1-2 недели для знакомства и погружения в процессы

TEAM LEAD

все сотрудники в одном регионе, их руководитель вместе с ними

Опыт JSOC в менеджменте удаленных команд. Часть 2

SOC
FORUM
2023



ЕДИНИЧНЫЕ УДАЛЕННЫЕ СОТРУДНИКИ

региональные менеджеры или руководители смежных подразделений, находящиеся рядом с удаленными сотрудниками, которые вовлекаются

в процесс адаптации, помогают отслеживать настроения и волнения функциональным руководителям из других регионов

практика 1x1 не только с сотрудниками, но и с этими самими руководителями



НЕБОЛЬШИЕ КОМАНДЫ

локальные активисты, ответственные сотрудники, которые выступают от лица коллектива, а может, будущие тимлиды



БОЛЬШИЕ КОМАНДЫ

команды со своим лидером, проведение регулярных встреч формата 1x1 между ним и руководителем, синхронизации между всеми региональными лидами

SOC FORUM 2023



n.stechenko@rt-solar.ru
ГК СОЛАР