



# Внутренние показатели или как эффективно смотреть на линии SOC

Кривоногов Алексей.  
JSOC. Заместитель директора центра  
по развитию филиальной сети.

**Ростелеком**  
Солар

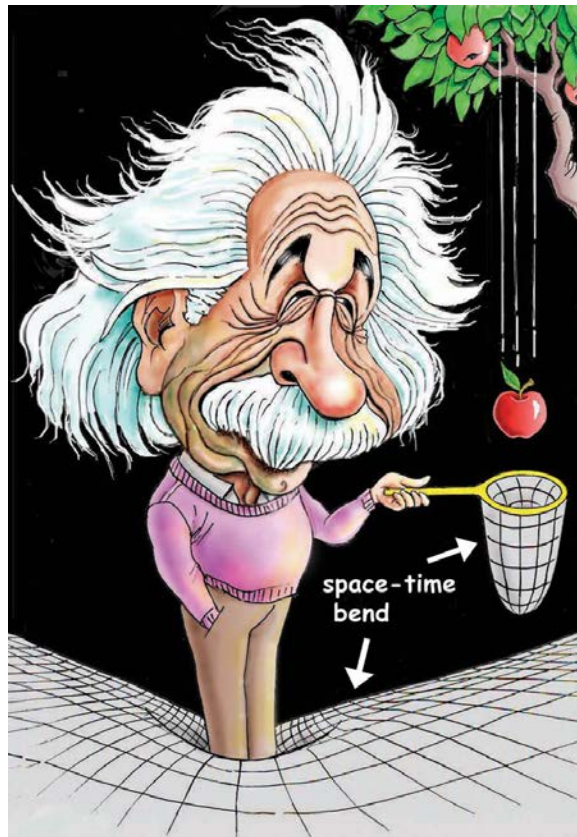


# Эффективность линий аналитики SOC

«Эффективность (лат. *effectivus*) – соотношение между достигнутым **результатом** и использованными **ресурсами**» ©wiki



# DISCLAIMER



**Ростелеком**  
Солар

# Линии аналитики Solar JSOC



Набр: «SOC – это люди»

## Задачи

- Обработка и расследование **типовых** инцидентов
- Построение типовых отчетов
- Обработка базовых запросов заказчиков
- Приемка новых заказчиков/сценариев

## Компетенции

- Знание основных механизмов и систем ИТ и ИБ
- Умение читать логи
- Владение основным инструментарием SIEM
- Работа по инструкции (но не ограничиваясь ей)

1-я

2-я

3-я (react)

4-я

## Задачи

- Добавление исключений по обратной связи
- Работа с контентом SIEM
- Подключение новых источников
- Обработка отчетов Threat Intelligence
- Дорасследование нетиповых технически сложных инцидентов
- Эскалация по экспертизе с 1-й и 2-й линий (консультации)

## Компетенции

- Опыт работы на 2-й линии Solar JSOC
- Уверенное знание основного инструментария расследования
- Regexp 80 level
- Базовые знания скриптотехники (PS, bash, python etc.)
- Навыки проведения глубокой аналитики

## Задачи

- Обработка и расследование **нетиповых** инцидентов
- Построение нетиповых отчетов
- Обработка запросов заказчиков
- Эскалация по экспертизе с 1-й линии (консультации)
- Приемка новых заказчиков/сценариев

## Компетенции

- Опыт работы на 1-й линии Solar JSOC
- Свободное владение всем инструментарием SIEM и др.
- «Свободное плавание» при расследовании

## Задачи

- Реагирование на нетиповые критические инциденты своих заказчиков
- Анализ аномальных активностей с целью выявления инцидентов
- Участие в расследовании инцидентов ИБ вне профиля сработки сценариев
- Разработка новых сценариев выявления инцидентов

## Компетенции

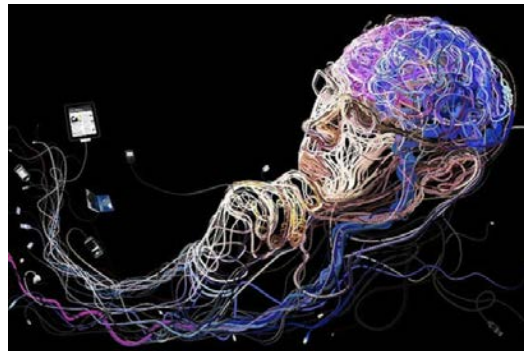
- Опыт разработки контента в SIEM
- TechSkills инженера реагирования x3
- Soft Skills

# Линии аналитики Solar JSOC

Исследования и разработка контента  
Анализ общей защищенности заказчика

Количественные и **качественные** метрики

4-я



#### Задачи

- Реагирование на нетиповые критические инциденты своих заказчиков
- Анализ аномальных активностей с целью выявления инцидентов
- Участие в расследовании инцидентов ИБ вне профиля сработки сценариев
- Разработка новых сценариев выявления инцидентов

#### Компетенции

- Опыт разработки контента в SIEM
- TechSkills инженера реагирования x3
- Soft Skills

# Линии аналитики Solar JSOC



## Задачи

- Добавление исключений по обратной связи
- Работа с контентом SIEM
- Подключение новых источников
- Обработка отчетов Threat Intelligence
- Дорасследование нетиповых технически сложных инцидентов
- Эскалация по экспертизе с 1-й и 2-й линий (консультации)

## Компетенции

- Опыт работы на 2-й линии Solar JSOC
- Уверенное знание основного инструментария расследования Regexp 80 level
- Базовые знания скриптотехники (PS, bash, python etc.)
- Навыки проведения глубокой аналитики

3-я (react)

Поддержка актуальности контента  
Тюнинг инструментария  
Экспертная помощь 1-й и 2-й линии

# Линии аналитики Solar JSOC

## Задачи

- Обработка и расследование **типовых** инцидентов
- Построение типовых отчетов
- Обработка базовых запросов заказчиков
- Приемка новых заказчиков/сценариев

## Компетенции

- Знание основных механизмов и систем ИТ и ИБ
- Умение читать логи
- Владение основным инструментарием SIEM
- Работа по инструкции (но не ограничиваясь ей)

1-я

2-я

## Задачи

- Обработка и расследование **нетиповых** инцидентов
- Построение нетиповых отчетов
- Обработка запросов заказчиков
- Эскалация по экспертизе с 1-й линии (консультации)
- Приемка новых заказчиков/сценариев

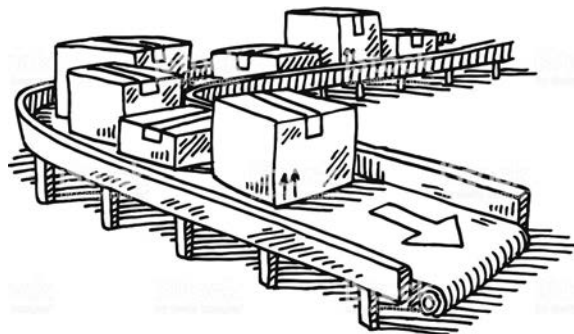
## Компетенции

- Опыт работы на 1-й линии Solar JSOC
- Свободное владение всем инструментарием SIEM и др.
- «Свободное плавание» при расследовании

## «Инцидентный конвейер»

Львиная доля расследования инцидентов сосредоточена тут

## Количественные и качественные метрики



# Эффективность. Декомпозиция на показатели. Якоря.



Финансы



Тайминги



Качество



Ресурсы



## «Нелинейные» показатели

- Качество контента/инструментария (CI/FP, Correlation Errors, Performance, etc...)
- Доступность инфраструктуры SOC (Zabbix, HealthChecks, Sustain, etc...)
- Непрерывность/полнота данных (HealthChecks, поступление событий, заполнение листов/трендов, etc...)
- Многое другое

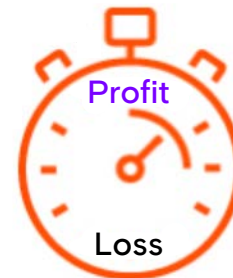


# Финансы

- Заложенные в P&L затраты на сопровождение контракта 1, 2, 3-й линиями аналитики во временном выражении

- Реальные трудозатраты сопровождения контракта 1-й линией \* ₺
- Реальные трудозатраты сопровождения контракта 2-й линией \* ₺
- Пропорциональные трудозатраты сопровождения 3-й линией \* ₺

=



Интересующие финансовые показатели можно выразить через временно-ресурсные



Нельзя рассчитывать на тайминги, собранные вручную!  
В случае инцидентов это не работает – очень короткий SLA



Не всегда процесс анализа инцидента можно релевантно разложить в таймлайн

Если это ваш случай, то совет – меняйте процесс :) В Solar JSOC релевантные трудозатраты используются для оценки большого числа очень полезных параметров. И собираться трудозатраты должны автоматически

Ростелеком

Солар

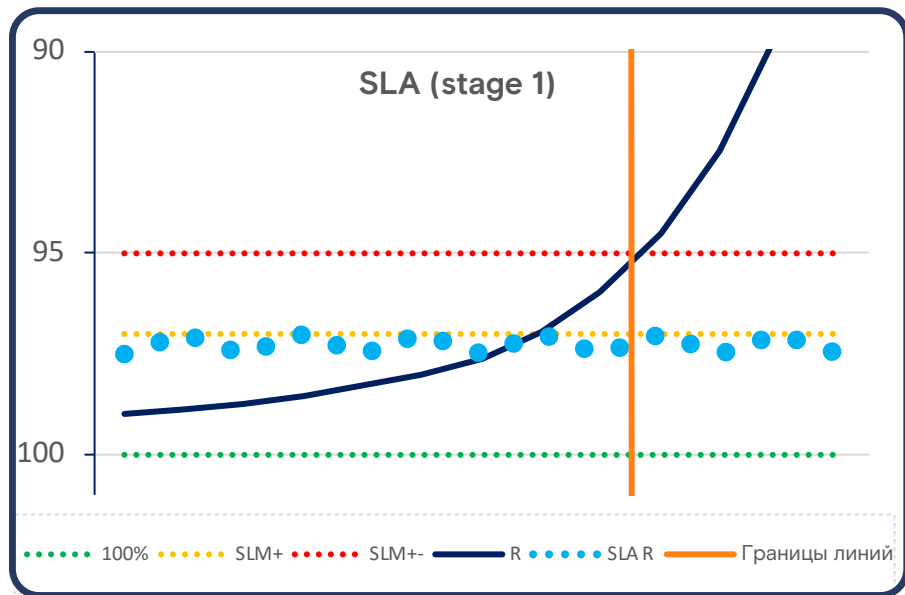
# T/Q/R. Ретроспектива. rev1



Для реализации части идей необходим запас по SLA

1-я + 2-я

3-я + 4-я



Ростелеком  
Солар

Как оцениваем эффективность?

- Общий процент выполнения SLA

Как обеспечиваем эффективность?

- Наполнение БЗ, повышение экспертизы линий
- Развитие инструментария анализа
- Развитие и оптимизация инструментария сопровождения

Что беспокоит?

- Критичность по договору != реалиям
- SLA по части высококритических инцидентов нереален
- Некоторые инциденты не в почете у инженеров
- «Размазанная» ответственность за SLA

Что изменилось по сравнению с предыдущим этапом?



# T/Q/R. Ретроспектива. Changelog

## SIEM<->ServiceDesk



В тикет проброшена информация, облегчающая **приоритизацию** и понимание, ссылка для быстрого доступа к кейсу SIEM

ArcSight RDW link	Core02 console 1st-line	ArcSight CaseID	115097
Attacker Host	abc [redacted] 10 APM APM администрира прикладных систем (ДБО СЗД) отчетности в ЦБ.	Target Host	dc8 [redacted] 10 Контроллер домена Возможность получить полный контроль над инфраструктурой
Attacker User	ab [redacted] 7 [redacted] Yurevich Главный специалист	Target User	mb [redacted] 5 mb [redacted]

## ServiceDesk&Process



В сервис-деске реализована приоритизация, учитывающая критичность ассетов. Инженеры обязаны брать самый горячий тикет, **не обращая внимания** на тайминг  
LTime – зеленая/желтая/красная зона тикетов – для оценки вероятности просрочек

Name	LTime	CWeight	ArcSight CaseID	Subject	Priority
[redacted]	8%	4.45	40136	Инцидент: Отсутствие в профиле аутентификации ([redacted])	Medium
[redacted]ank	88%	1.57	48450	Инцидент: Попытка аутентификации под служебной УЗ из недоверенной сети ([redacted])	Low
DIT [redacted]	78%	0.66	430017	Инцидент: Попытка подбора пароля ([redacted])	Low

## ServiceDesk&Process



Спецтиклет «JSOC Monitoring – дежурный» закрепляет ответственность за процессинг тикетов  
Автоматизация: профиль информирования, заметки с ссылками на KB и связанной с тикетом информацией

Для сценария 'Исходящая сетевая активность к потенциально опасным хостам' имеется описание:  
<https://helpdesk.solarsecurity.ru/staff/index.php?Knowledgebase/ViewKnowledgebase/Article/525/109>

Для сценария 'Исходящая сетевая активность к потенциально опасным хостам' имеются критерии ложного срабатывания:  
<https://helpdesk.solarsecurity.ru/staff/index.php?Knowledgebase/ViewKnowledgebase/Article/225/109>

Kayako by noterule@all\_customers\_jsoc\_feeds\_k002\_fp

# T/Q/R. Ретроспектива. Changelog



## SIEM<->ServiceDesk

Реализован механизм DA, DA&Mon, DA&Adm

5.	Подробное описание инцидента:	Выявлена попытка ввода пароля в окно логина на хосте SU- [REDACTED].ru 10 [REDACTED].126. Предполагаемая скомпрометированная учетная запись - CORP \ Во [REDACTED] Лист для проверки - JSOC_UM_007/Profile_Password Exposure Accounts
9.	Примечание:	Оповещение направлено с использованием механизма DirectAlert

## Process

### CaseReview

#### Цели

- Отследить изменение уровня качества расследования инцидентов
- Подсветить инженерам 1-й и 2-й линии типовые ошибки
- Доработать шаблоны и инструкции 1-й и 2-й линии
- Детектировать проблемные места в контенте SIEM
- Поощрить действительно качественные расследования инцидентов



#### Процедура

- Регулярная проверка качества расследования инцидентов
- Проверку проводят инженеры реагирования и аналитики
- Распределение типов инцидентов
- Более пристальное внимание за критическими инцидентами и инцидентами по новым сценариям
- Проведение внутренних семинаров

Case Review						
Additional Criteria	Тикет проверен, вопросов нет Доработка контента	Engineer	Choose an engineer	Rating	+	Description
\$Максим Жевнерев: Хорошо. Запоминаем как выглядит LateralMovement через удаленную установку служб. Чего не хватает в оповещении - откуда активность шла. В данном случае это не сильно просто (ибо нет успешных входов в логи). НО - был один неуспешный под учеткой AAluyokhin. Хорошо бы уметь это находить. Плюс в доработку контента - нужен автоматический конверт SID, как это сделано в учетках.						
Subject	time2resolve_owner	normtime_m	time2res_m	billtime_m	weigh	weight2
Инцидент: Обнаружение нового сервиса во внешнем периметре ([REDACTED]443;172.17.0.253[0](TCP) (737)	Данил Борисов,3150	16.6	52.5	30.0	3.2	3.16
Инцидент: Многочисленные блокировки учетной записи (W81) mingkh	Руслан Казаков,510	26.7	8.5	10.0	0.3	3.14

## Process



Парадигма «полное расследование за одну итерацию» меняется на «информирование в рамках профиля нотификации, затем обогащение информацией»

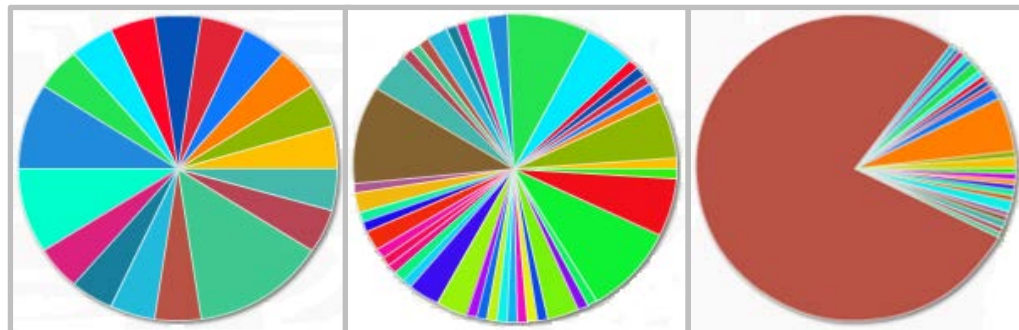
## ServiceDesk&Dashboard



Статистические «блинчики» – быстрая оценка ситуации

Выработка инженеров

Распределение инцидентов по типам и заказчикам (типичный звонок аналитику – опять твой CustomerName играет в PacMan-a)



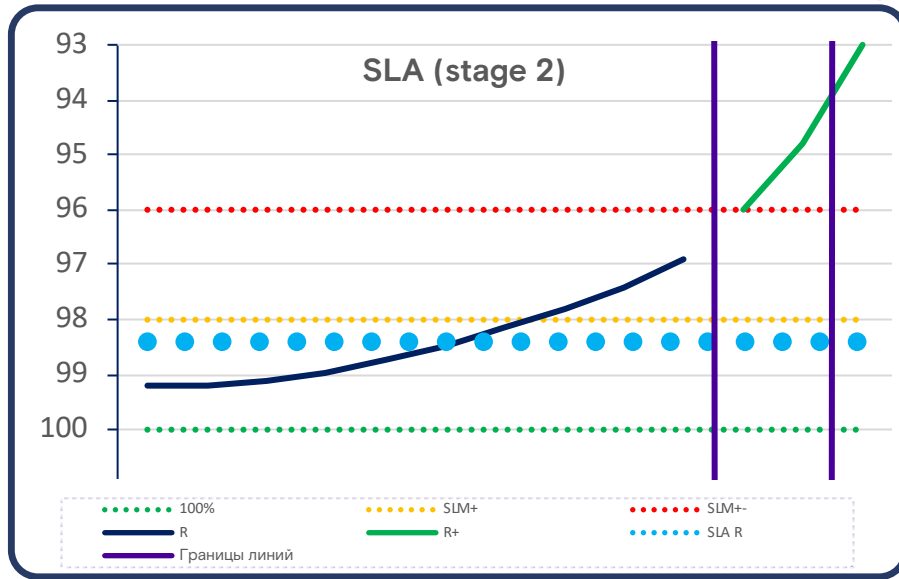
# T/Q/R. Ретроспектива. rev2



Для реализации части идей все еще необходим запас по SLA  
Необходимы глубокие расследования горячих инцидентов  
Масштабирование и выравнивание экспертизы ортогональны

1-я + 2-я

3-я 4-я



Как оцениваем эффективность?

- Процент выполнения SLA на 1-й линии
- CaseReview

Как обеспечиваем эффективность? Stage1 +

- CaseReview
- Выделенная линия технического сопровождения контента/расследования
- SLA локализован в рамках 1-й линии + «смотрящий» за SLA
- DA, DA&Mon, DA&Adm

Что беспокоит?

- Выбеги нагрузки до x10 от средней (+ моральный ступор в требовании невозможного от инженеров линий)
- Сложность синхронизации экспертизы в рамках 1-й линии
- Невозможность применения эскалационной модели 1 => 2
- Глубокое расследование «невыгодно» инженерам

Что изменилось по сравнению с предыдущим этапом?

- SLA ~97% => 98.4%, SLM 97% => 98%
- Оперативное профилирование сценариев/заказчиков
- Меньше «обезьяньей» работы
- На 1-й линии дополнительный функционал
- Более фактурные и разнообразные сценарии
- Более требовательный заказчик (глубина расследования)

# T/Q/R. Ретроспектива. Changelog



## ServiceDesk&Process

Основная задача дежурного – обеспечение ресурсоемкости линии. Запущена формальная процедура ресурсной эскалации.

## Process

Приемка/сопровождение изменений сценариев/заказчиков

### Соответствие требованиям

Контента SIEM, систем сопровождения, инструментария, описаний в KB, etc.

### Статистика

Частота сработок, оценка трудоемкости/сложности, соответствие критичности/SLA/трудоемкости etc.

### Кастомизация

Маршруты уведомлений, нотисы, вариативная критичность, правила день/ночь, etc.

## Statistic

Периодически собирается статистика по распределению времени решения инцидентов по типам. **Маркер приоритета тюнинга инструментария.** На ее основании **выставляются ограничения критичности SLA...** Ну или **принимаются риски.**

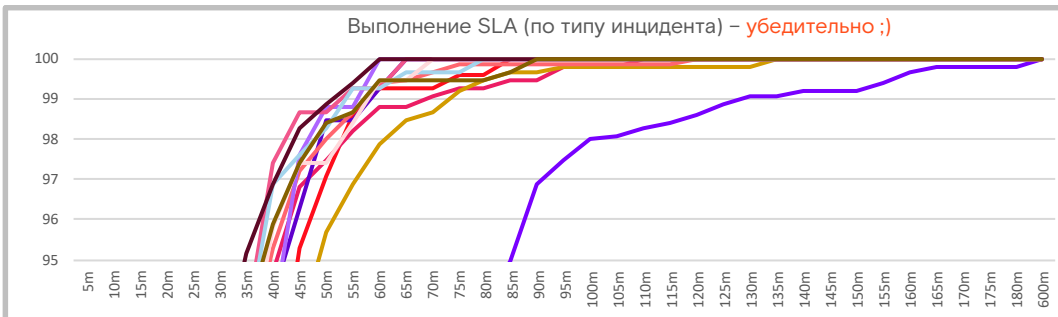
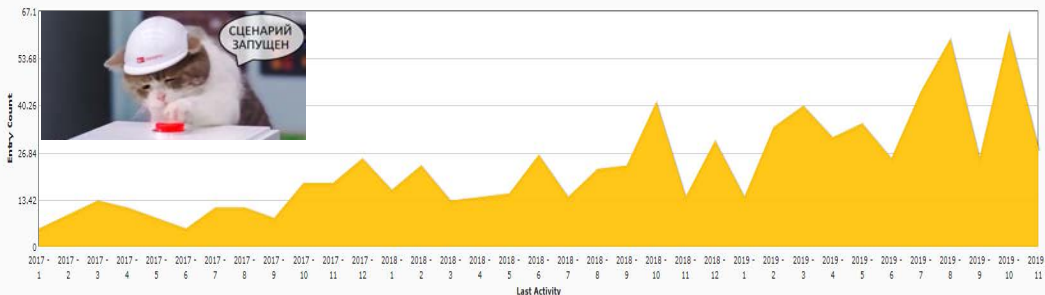
О привлечённых в рамках эскалации отписываемся в реглае.  
Тикет можно закрыть, когда LA упал ниже 80. По этим тикетам будет оцениваться эффективность проведённой дежурным эскалации.  
Если нагрузка не падает и приходит ещё один аналогичный тикет - это говорит о неэффективности принятых мер. Линкуем новые такие тикеты к первому из незакрытых.

Solar Security



Ростелеком  
Солар

Превышена нагрузка на Mon\_1st.  
Превышен коэффициент за 20min.  
Текущее значение: 119.



# T/Q/R. Ретроспектива. Changelog

## ServiceDesk&SIEM

Загрузка линии LA 5-20-60 (привет, \*nix@)

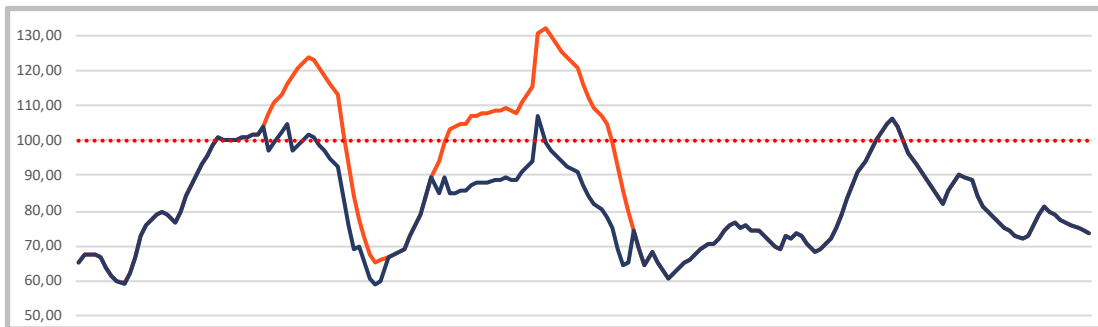


Соотносит оценочную **трудоемкость задач** в очереди к имеющимся на линии **ресурсам**.

LA5 – уровень управления **online-инженера**

LA20 – уровень управления **лидера** группы

LA60 – уровень управления **руководителя** отдела  
+ **ресурсный лайфхак** ;)



## ServiceDesk

Инцидентный «killchain»



агрегирование за 1 / 3 / 15 дней

Изолированный инцидент и **инцидент с  
предысторией**

Событийный «niahclick/карма» - under construction

Инцидент: Запуск скриптов из документов MS Office (Сергеев Виктор Геннадьевич.xls)

killchain\_v2\_short (1 day)

08.07.2019 15:00 - #546053: Обнаружен вирус на критичном хосте => ( nb-vsargeev ) => ( Mon\_tst / Resolved / Сергей Сплярко )

Инцидент: Обнаружен вирус на критичном хосте (nb-vsargeev|HEUR:Trojan-Downloader.MSExcel.DdeExec.b)

killchain\_v2\_long (15 days)

05.07.2019 11:53 - #543953: Запуск хакерских утилит на хосте => ( nb-vsargeev ) => ( Mon\_tst / Resolved / Денис Гусаров )

03.07.2019 14:13 - #542762: Обнаружен вирус на критичном хосте => ( nb-vsargeev ) => ( Mon\_tst / Resolved / Даниил Романовский )

01.07.2019 12:31 - #541114: ThreatHunting: Mimikatz - Detection by Command Line => ( nb-vsargeev ) => ( Direct Alert / Resolved / UNASSIGNED )

01.07.2019 10:57 - #540906: ThreatHunting: Credential Dumping - Process Access => ( nb-vsargeev ) => ( Direct Alert / Resolved / UNASSIGNED )

24.06.2019 10:10 - #536440: Обнаружен вирус на критичном хосте => ( nb-vsargeev ) => ( Mon\_tst / Resolved / Марина Павлова )

13.06.2019 16:45 - #531468: ThreatHunting: System Process with download code instruction => ( nb-vsargeev ) => ( Direct Alert / Resolved / UNASSIGNED )

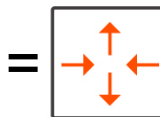
13.06.2019 16:44 - #531467: ThreatHunting: System Process with download code instruction => ( nb-vsargeev ) => ( Direct Alert / Resolved / UNASSIGNED )

## ServiceDesk&Process



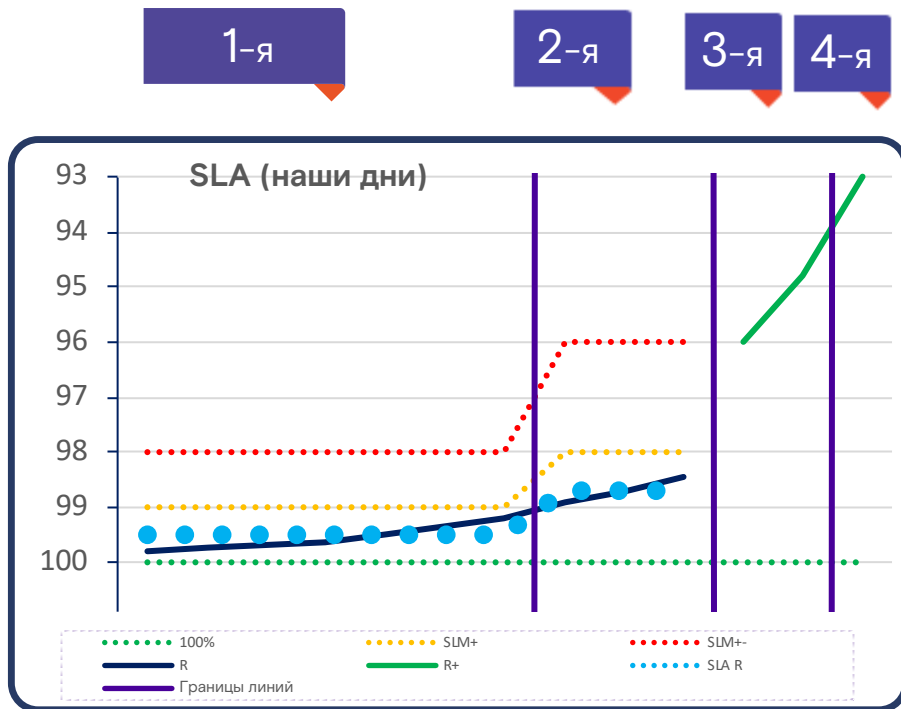
Балансировка! Теперь нам есть что противопоставить перемаршрутизации по экспертизе ;)

Признак изолированности + критичность активов + критичность сценария + оценочная трудоемкость + SLA-тайминг + LA линий + специфические keyfields + оценка сложности расследования + время сработки + кастомные сценарии + многое другое



Событийный  
роутер / балансировщик

# T/Q/R. Современность. rev3



Как оцениваем эффективность? Stage2 +

- Процент выполнения SLA на 1-й и 2-й линии
- LA, ресурсные эскалации

Как обеспечиваем эффективность? Stage2 +

- Балансировка нагрузки по необходимой экспертизе
- Ресурсные эскалации
- Георезервирование и частичный FTS

Что беспокоит?

- Разнородность контента и подходов к расследованию при мультиплатформенности
- Балансировка между регионами
- Выравнивание экспертизы между регионами

Что изменилось по сравнению с предыдущим этапом?

- SLA ~98,4% => ~99%, SLM 98% => 99-98%
- МультиСИЕМность
- Эффективно проходим пики нагрузки
- Проще погружение/синхронизация экспертизы на 1-й линии
- Сервис распределен по нескольким регионам
- Нет жесткой привязки к пропорции численности 1-й и 2-й линий

# T/Q/R. KPI. Расписание.

## KPI

### Количественные:


- число инцидентов
- приведенная трудоемкость
- взвешенная «полезность»
- нарушения SLM/SLA



### Case Review (качество):

- +- расследования
- соблюдение эскалации
- передача информации по смене
- выполнение DRP
- доп. активности/задачи
- etc.

### Трудовая дисциплина

Engineer			SLA						Case Review							CSLA React	CSLA Res	kpi 0.8 (SLA)	kpi 0.8 (Σ)	kpi 0.2	Σ
	Count	CntK	SLM reac	SLA reac	SLM res	SLA res	SLA+ res	+++	++	+	-	--	---	Σ							
	2001	117%	0	3	2	0	0	0	2	6	2	0	1	2	21	0	99%	96%	1	97%	
	1540	69%	5	1	3	0	0	0	3	4	7	0	0	6	8	2	99%	50%	1	60%	
	1625	106%	8	0	4	0	0	2	1	8	0	1	1	16	0	3	99%	102%	1	101%	
	2124	104%	2	0	10	0	0	0	6	2	2	1	2	-1	1	3	99%	83%	1	87%	
	1737	139%	3	0	0	0	0	2	3	13	1	1	1	26	0	4	100%	123%	1	118%	

## Расписание

### Ролевая модель

- гуглоформа с пожеланиями
- забавные/полезные капчи
- учет ограничений студентов
- автопроверки



Время составления расписания сократилось в **3 раза** с учетом составления вопросов для капчи

**примеры шаблонных смен**

NN01DN	10:00 - 20:00	10:00 - 20:00	17:30 - 2:00	20:00 - 8:00		
NN01DN	17:30 - 2:00	10:00 - 20:00	10:00 - 20:00	10:00 - 20:00		
NN01DN	10:00 - 20:00	17:30 - 2:00	10:00 - 20:00	17:30 - 2:00		
NN01DN	10:00 - 20:00	10:00 - 20:00	17:30 - 2:00	10:00 - 20:00		
NN01DA	10:00 - 20:00	10:00 - 20:00	10:00 - 20:00	10:00 - 20:00		
NN01WE	10:00 - 20:00	10:00 - 20:00	17:30 - 2:00	8:00 - 20:00		
NN01WE	10:00 - 20:00	10:00 - 20:00	17:30 - 2:00	8:00 - 20:00		
NN01WE	10:00 - 20:00	10:00 - 20:00	17:30 - 2:00	10:00 - 20:00		
NN01WE	10:00 - 20:00	17:30 - 2:00	10:00 - 20:00	17:30 - 2:00		
NN01WE	10:00 - 20:00	10:00 - 20:00	10:00 - 20:00	17:30 - 2:00		

CAPTCHA: Что не так в выделенном блоке условия? Чем более подробный ответ - тем лучше. \*

Rule: INC\_JSOC\_BF\_004\_Possible ... Filter: JSOC\_Success Auth (Reas... Rule: WH\_2008\_Base\_LoginFailed ...

Attributes Conditions Aggregation Actions Local Variables Notes

Event conditions

AND

- NOT
- NOT
- NOT
- NOT
- Device Event Class ID = Microsoft Windows Security-Auditing-625
- Device Process Name NOT In (CHAP,IAS)
- Reason != The specified account's password has expired.
- Reason != The user has not been granted the requested login type at the machine.
- Reason != An Error occurred during Login.
- Reason != An Error occurred during Login.

CAPTCHA: Чей это любимый персонаж? Ответ принимается цифрой, идеальный ответ д.б. с указанием в каких ИС JSOC каким образом можно найти пруф \*



# Метрики vs ощущения



**Ростелеком**  
Солар

# Контакты

Центральный офис

125009 г. Москва,  
Никитский переулок, 7с1

+7 (499) 755-07-70

[info@rt-solar.ru](mailto:info@rt-solar.ru)



**Ростелеком**  
Солар

