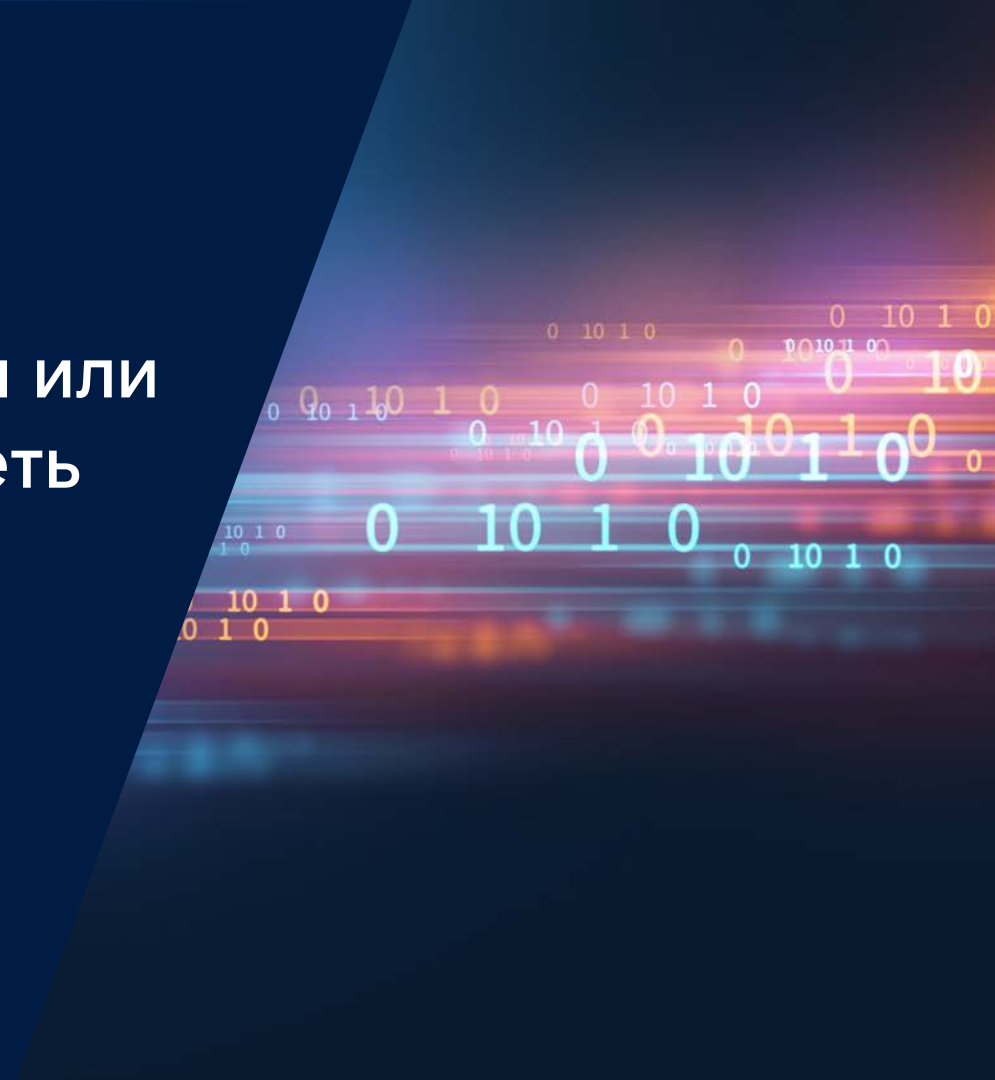
Внутренние показатели или как эффективно смотреть на линии SOC



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

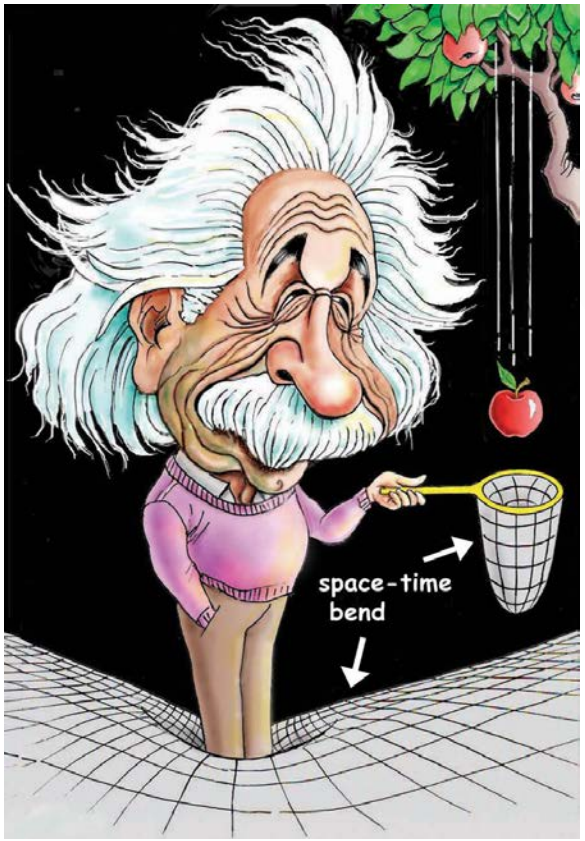
Ростелеком
Солар

Эффективность линий аналитики SOC

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

Да, но нет!

DISCLAIMER



Ростелеком
Солар

Линии аналитики Solar JSOC

Habr: «SOC – это люди»

1-я

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)

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

3-я (react)

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

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

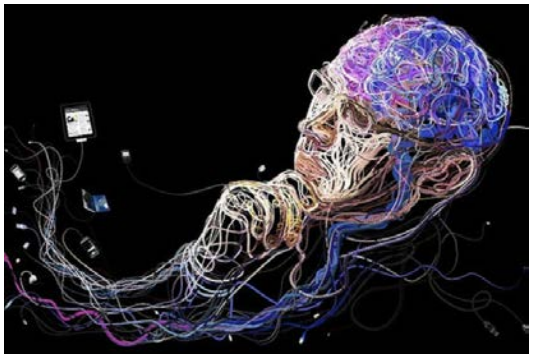
Soft Skills

Ростелеком
Солар

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

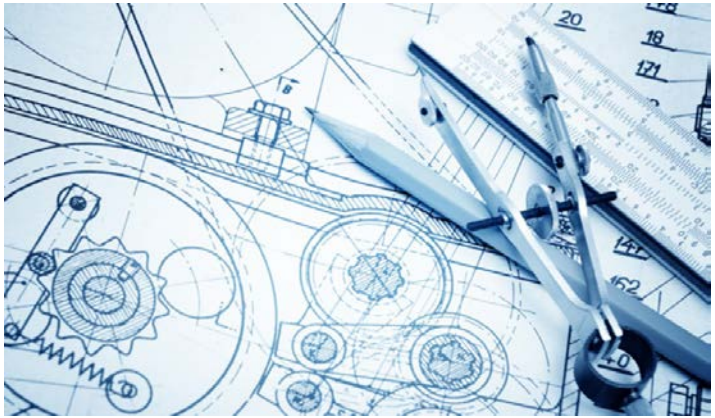
Компетенции

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

Количественные и **качественные** метрики

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

«Инцидентный конвейер»

Львиная доля расследования инцидентов сосредоточена тут

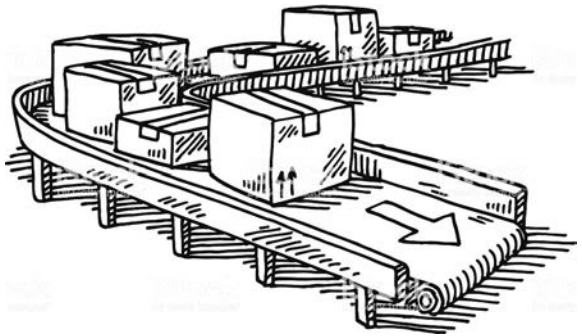
Количественные и качественные метрики

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



Ростелеком
Солар

Эффективность. Декомпозиция на показатели. Якоря.

Финансы

Тайминги

Качество

Ресурсы

«Нелинейные» показатели

- Качество контента/инструментария (CI/FP, Correlation Errors, Perfomance, 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 * ₽

=

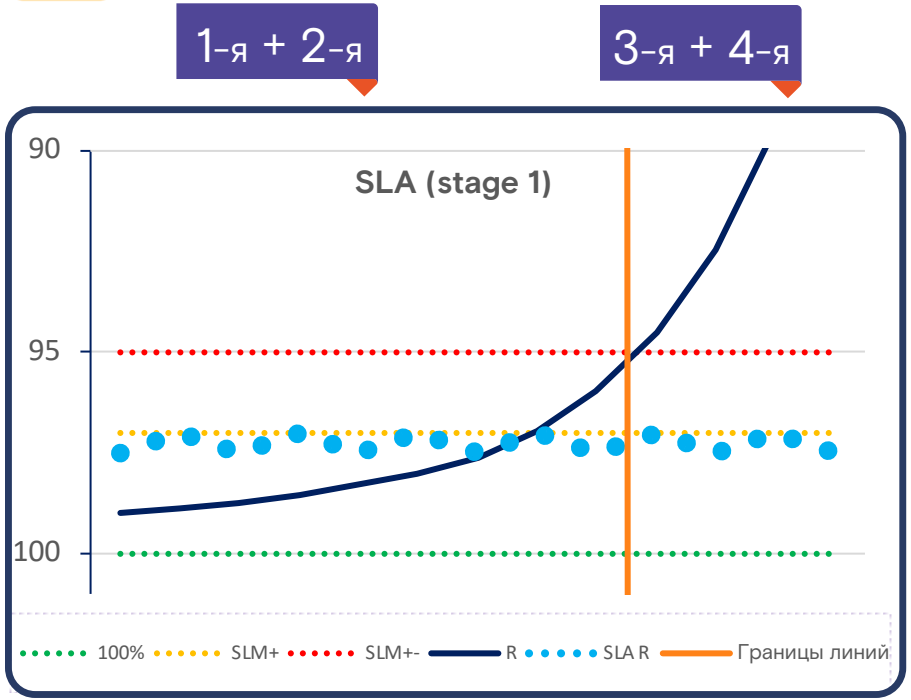
Интересующие финансовые показатели можно выразить через временно-ресурсные

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

T/Q/R. Ретроспектива. rev1

Для реализации части идей необходим запас по SLA



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

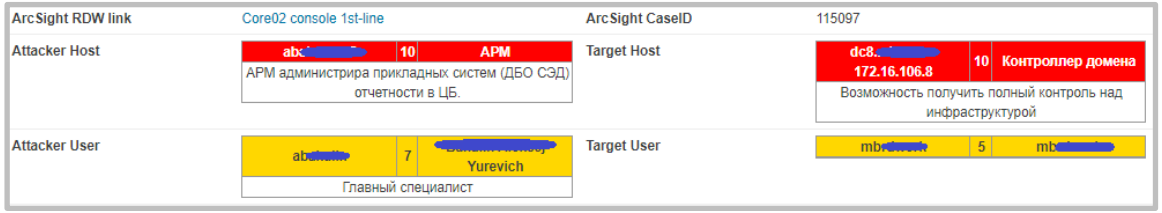
Что изменилось по сравнению с предыдущим этапом?

Ростелеком
Солар

T/Q/R. Ретроспектива. Changelog

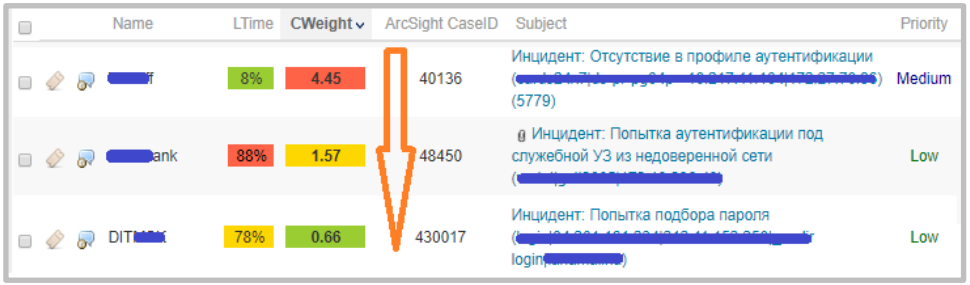
SIEM<->ServiceDesk

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



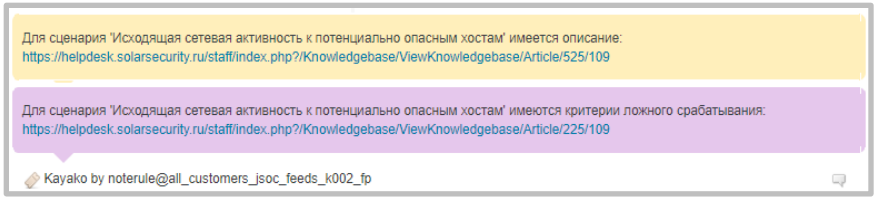
ServiceDesk&Process

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



ServiceDesk&Process

Спецтикет «JSOC Monitoring - дежурный» закрепляет ответственность за процессинг тикетов
Автоматизация: профиль информирования, заметки с ссылками на КВ и связанной с тикетом информацией



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]4.ru 10[redacted]6.126. Предполагаемая скомпрометированная учетная запись - CORP \ Bo[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 логах). НО - был один неуспешный под учеткой AAlyokhin. 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	weigth	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

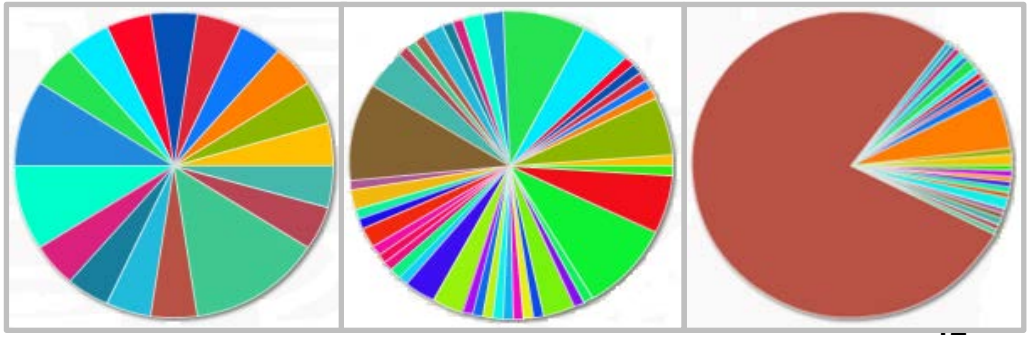
Парадигма «полное расследование за одну итерацию» меняется на «информирование в рамках профиля нотификации, затем обогащение информацией»

ServiceDesk&Dashboard

Статистические «блинчики» – быстрая оценка ситуации

Выработка инженеров

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

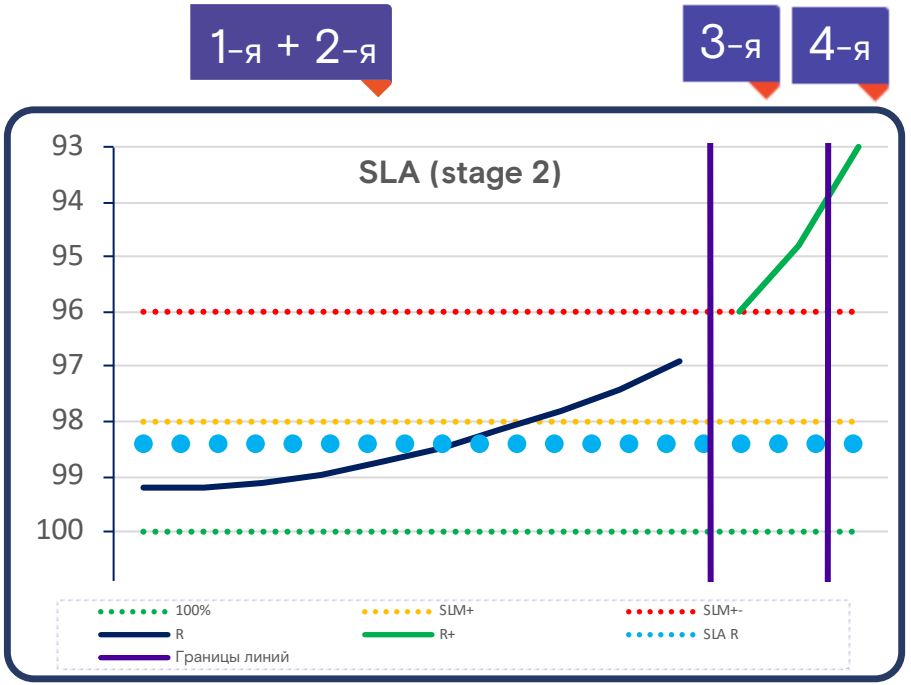


Ростелеком

Солар

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



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 стопор 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.

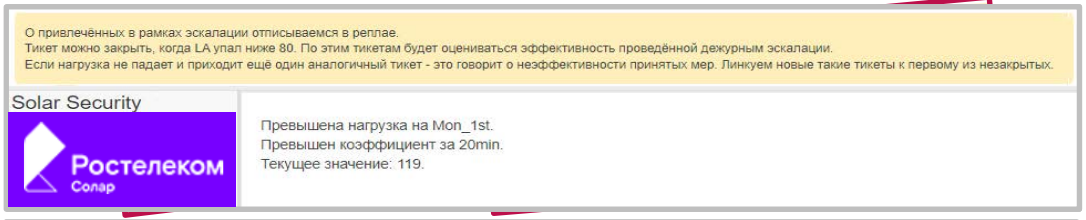
Кастомизация

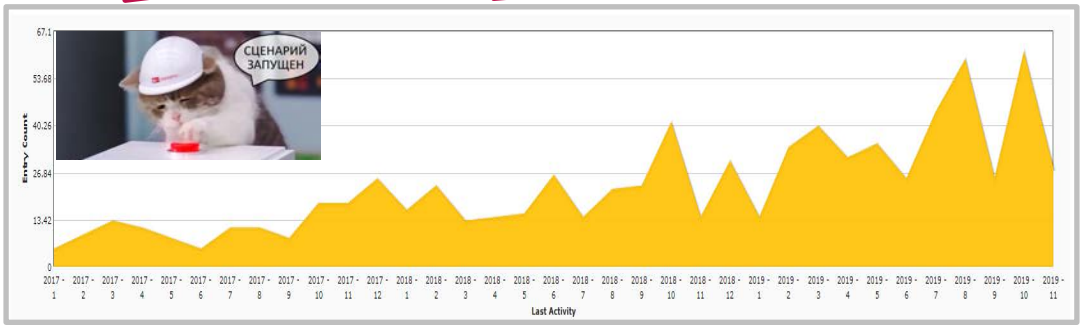
Маршруты уведомлений, нотисы, вариативная критичность, правила день/ночь, etc.

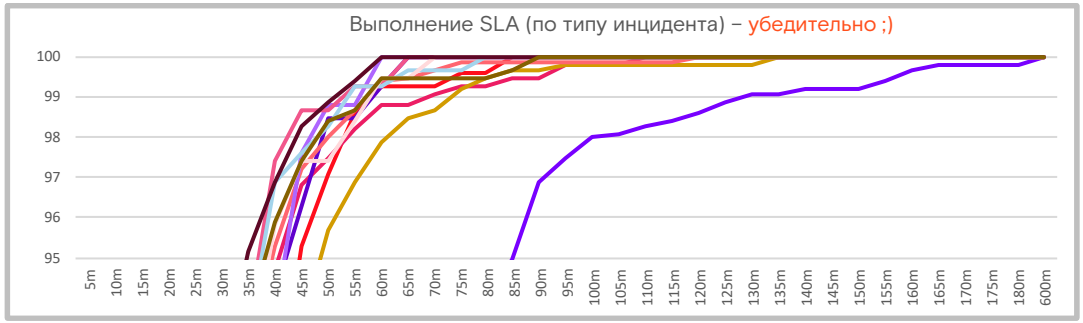
Statistic

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.





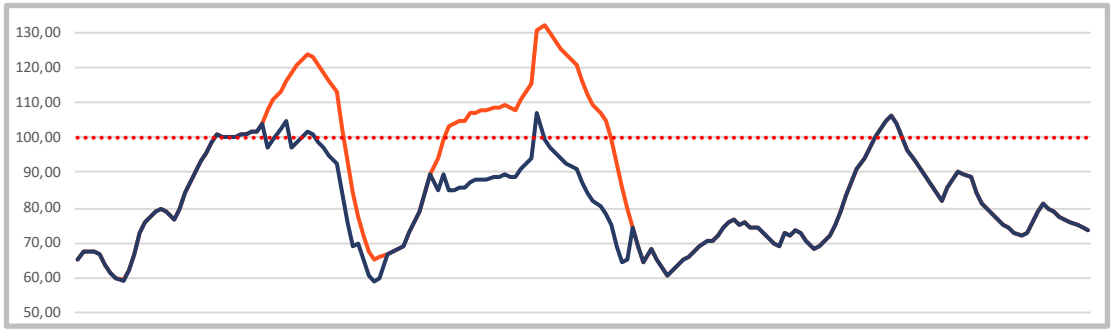


Ростелеком
Солар

T/Q/R. Ретроспектива. Changelog

ServiceDesk&SIEM

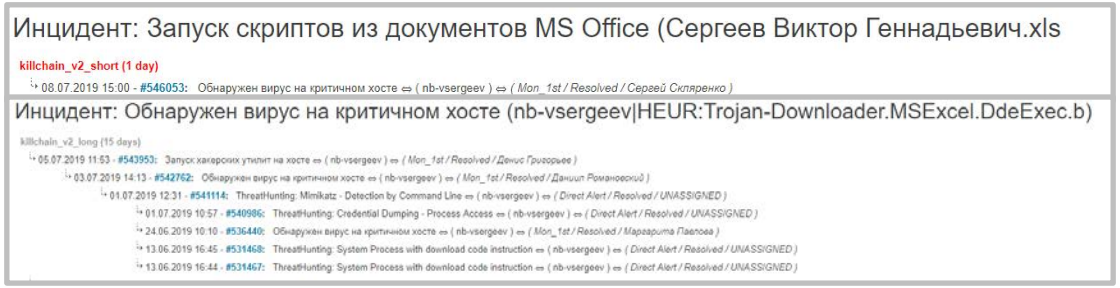
Загрузка линии LA 5-20-60 (привет, *nix☺)
Соотносит оценочную трудоемкость задач в очереди к имеющимся на линии ресурсам.
LA5 – уровень управления online-инженера
LA20 – уровень управления лидера группы
LA60 – уровень управления руководителя отдела
+ ресурсный лайфхак ;)



ServiceDesk

Инцидентный ~~«killchain»~~
агрегирование за 1 / 3 / 15 дней
Изолированный инцидент и инцидент с предысторией

Событийный «niahcllik/карма» - under construction



ServiceDesk&Process

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

Признак изолированности + критичность ассетов + 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%
- МультиSIEMность
- 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

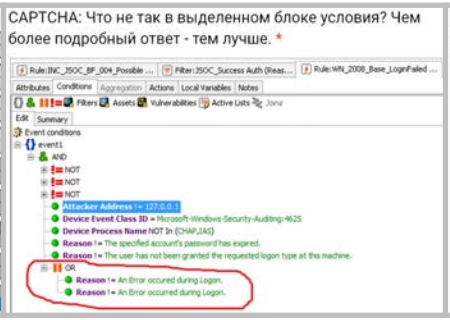
Engineer	Count	CntK	SLA					Case Review							CSLA React	CSLA Res	kpi 0.8 (SLA)	kpi 0.8 (∑)	kpi 0.2	∑
			SLM reac	SLA reac	SLM res	SLA res	SLA+ res	+++	++	+	-	--	---	∑						
	2001	117%	0	3	2	0	0	0	2	6	2	0	1	2	21	0	99%	96%	1	97%
	1540	69%	5	1	3	0	0	0	3	4	7	0	0	6	8	2	99%	50%	1	60%
	1625	106%	8	0	4	0	0	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%

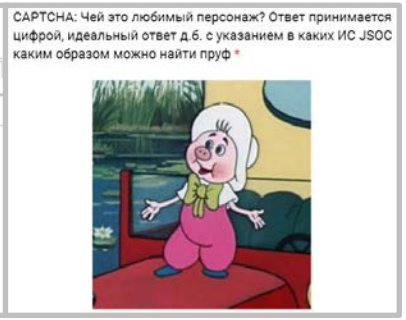
Расписание

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





Метрики vs ощущения

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Ростелеком
Солар