



— 2014 —

КОСМИЧЕСКАЯ ОДИССЕЯ СЕРВИС-МЕНЕДЖМЕНТА

Путешествие в процессах и функциях



Стыковка систем ITSM и мониторинг



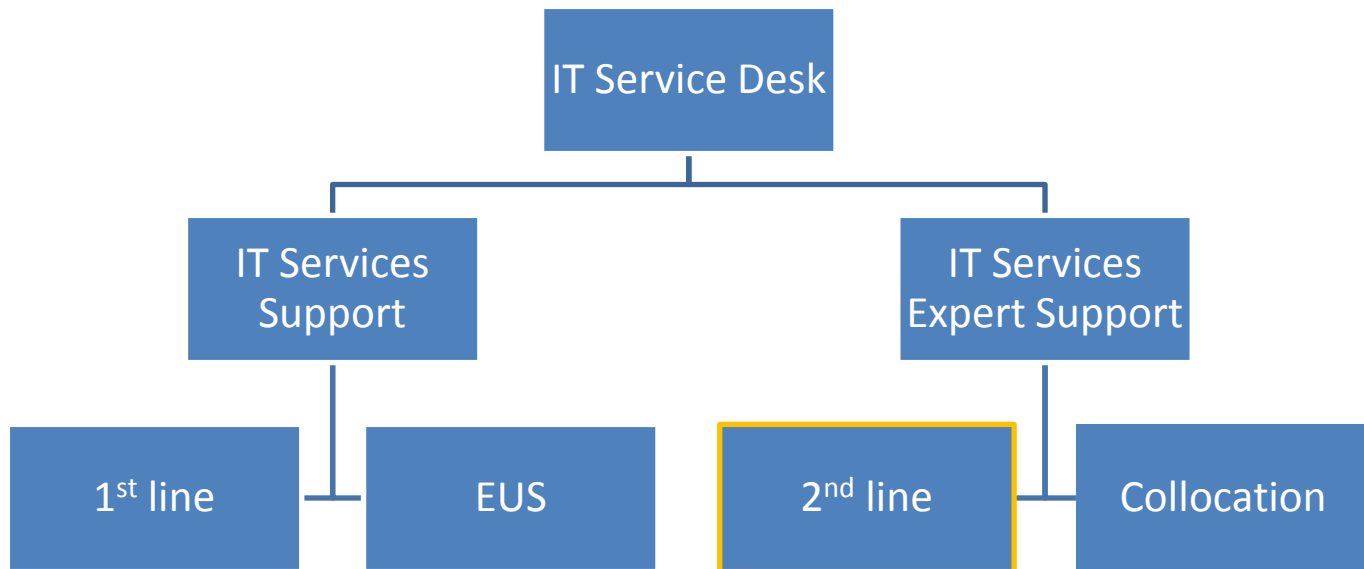
Павел Сулов

*Руководитель отдела экспертной ИТ поддержки,
Лаборатория Касперского.*

Содержание

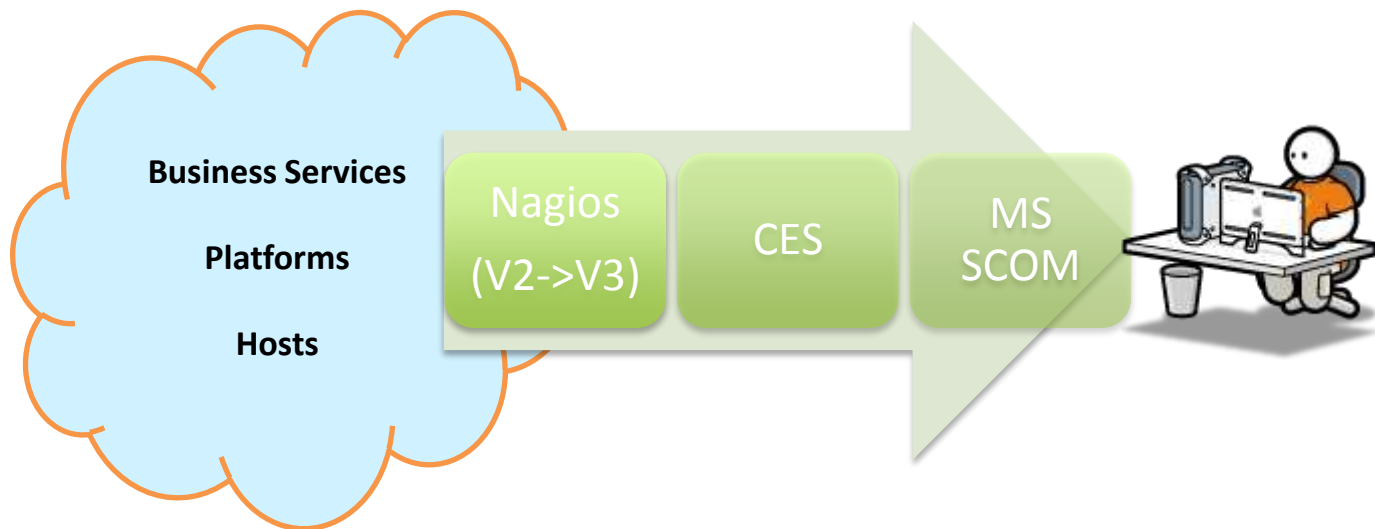
Как устроен Service Desk в Лаборатории Касперского	3
Обработка событий мониторинга в ЛК	4
Качественный анализ проверок	6
Как устроена интеграция	8
Измеряемые KPI	12
Решаемые проблемы	13

Как устроен *Service Desk* в Лаборатории Касперского.



Обработка событий мониторинга в ЛК

История изменений систем мониторинга.



Результатом применения различных систем мониторинга был плоский список проверок, который необходимо обработать руководствуясь документацией, Базой Знаний и личным опытом

Обработка событий мониторинга в ЛК

Проблемы:

- *Плоский список большого числа проверок на выходе системы мониторинга.*
- *Отсутствие приоритезации и иерархической зависимости между проверками.*
- *Отсутствие понимания эффективности дежурного администратора по обработке событий мониторинга.*
- *Затруднение эскалации сработавших проверок*

Разбивка по типам обработки

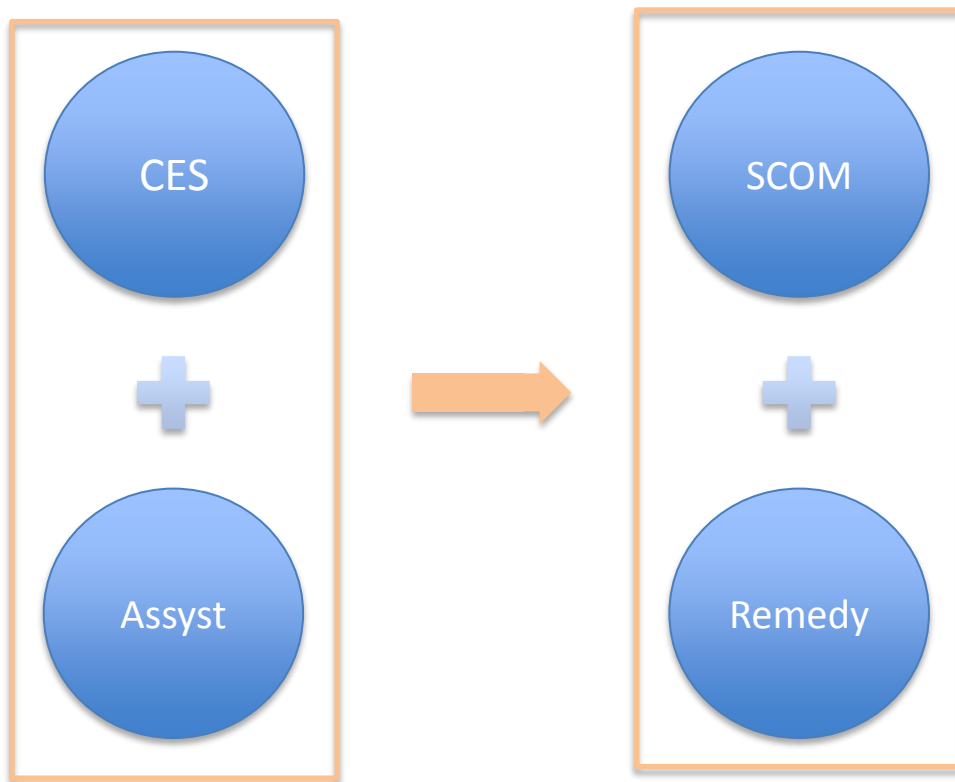


Качественный анализ проверок мониторинга

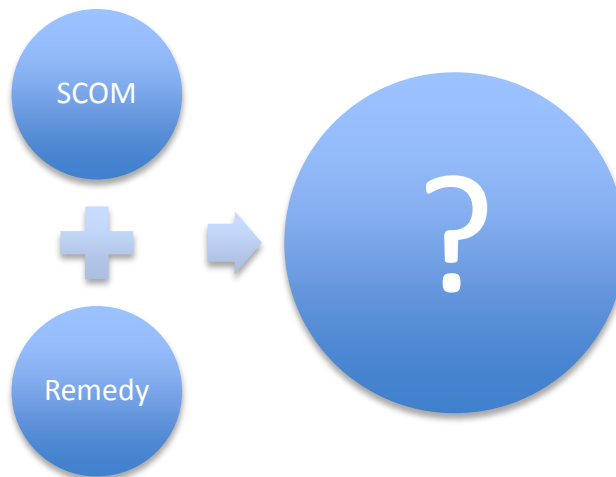
Что показал нам анализ проверок?

- До 5% проверок пропускаются администраторами, из-за отсутствия физической возможности просмотреть их («вылезла» за пределы экрана, «починилась» до того, как администратор взял проблему в работу и т.д.)
- Порядка 15% проверок не требуют обработки и\или эскалации, поскольку их срабатывание вызвано неисправностью смежного компонента системы.
- Даже такой поверхностный анализ приходится каждый раз проводить ручным методом, что требует больших трудозатрат.
- Отсутствует понимание количества (и %) решённых инцидентов мониторинга на 2ой и экспертной линиях.
- Отсутствие точного понимания времени, затрачиваемого на решение эвентов от мониторинга, а как следствие, трудозатрат.

Текущая интеграция



Интеграция. Как будет?



ITSM-система

Для Incident Management (+Crisis Management), Knowledge Management, Event Management, Problem Management, Service Transition в ЛК используется BMC Remedy.

Концепция интеграции

- ❑ Выделяются те события, которые необходимо обрабатывать в Remedy.
- ❑ Выделяются временные интервалы различных действий администратора для построения KPI.
- ❑ Фиксируются все действия, производимые различными группами поддержки, в ITSM-системе.

Интеграция. Как?



- > Каждой из проверок в SCOM добавляется признаки “Viewed” и “Action Required”
- > При проставлении у проверки в SCOM признака “Action Required”, в системе Remedy появляется соответствующий инцидент.
- > В свойствах проверки прописывается номер инцидента в Remedy.
- > В инциденте Remedy хранится ссылка на проверку в SCOM.
- > Фиксируются различные временные отсечки и переназначения инцидента между группами в Remedy.

Измеряемые KPI.

- Общее количество сработавших проверок за период времени и какое количество из них было проанализировано.
- Количество и % проверок, для которых не понадобилось действий (кроме анализа). Тем самым измеряется качество построения иерархии проверок, и как следствие «полезность» нагрузки на системного администратора.
- Количество и % проверок, которые потребовали анализа, обработки и действий по устранению. Тем самым измеряются трудозатраты.
- Количество и % проверок, устранённых без привлечения экспертов Зей линии.
- Количество и % проверок, которые были решены в установленный срок.
- Персональные метрики для сотрудников.

Какие проблемы решаются?

- Улучшается качество мониторинга за счёт:
 - Правильного размещения проверок в иерархии проверок бизнес- и технических сервисов, и как следствие, сокращение числа отображаемых проверок при поломке сервиса.
 - Удаления проверок, «засоряющих» мониторинг.
 - Сокращения времени на обработку событий мониторинга.
- Детальное отслеживание операционной ситуации и производительности конкретного сотрудника через метрики.
- Удобная эскалация на смежные линии поддержки, которые будут иметь доступ к исходной сработавшей проверке.

Спасибо за внимание!