#CloudMTS

Управление инцидентами в SOC MTS

Андрей Шамрай

Руководитель группы SOC #CloudMTS

#CloudMTS

Про SOC МТС

С 2005 года

существует
Корпоративный SOC

С 2016 года

предоставляем услуги
Коммерческим
заказчикам

Клиенты

несколько десятков
клиентов в различных
сферах деятельности

Сотрудники

высококвалифицированный
штат сотрудников SOC

SOC

один из крупнейших
SOC не только в России,
но и в Европе

SIEM

реализация крупного
промышленного SIEM
как сервис

Лицензия

лицензия ФСТЭК ТЗКИ №2012
на услуги по мониторингу
информационной
безопасности средств
и систем информатизации
(пункт «в»)

700 млн.

обрабатывается
около 700 млн. событий
в сутки

24/7

мониторинг
и реагирование на
инциденты 24/7

Сертификат

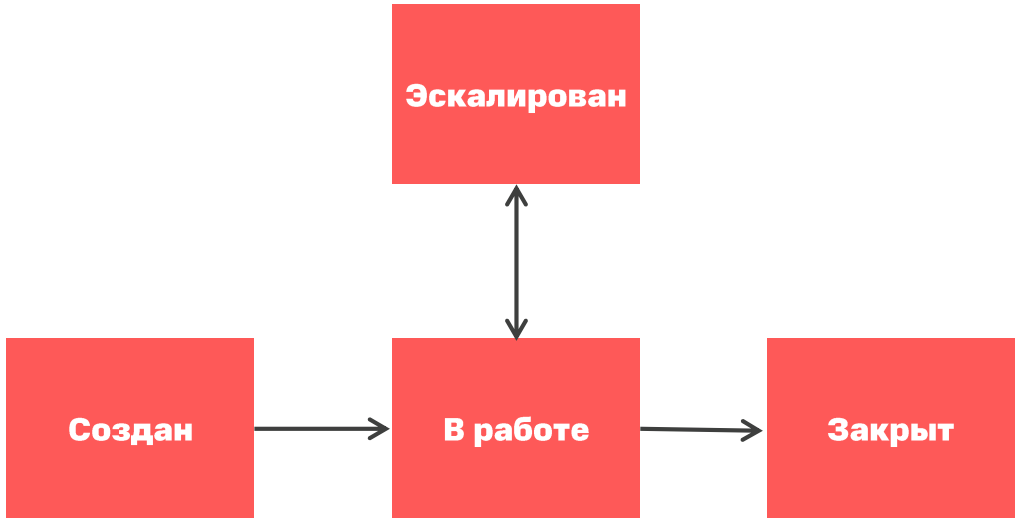
Сертификат ISO 27001
«Предоставление услуг
мониторинга и реагирования
на инциденты информационной
безопасности»

#CloudMTS

Жизненный цикл инцидента. Начало

Временные метрики:

- Реакция
- Реагирование
- Эскалация
- Обработка = Реакция + Реагирование
- Решение = Обработка + Эскалация

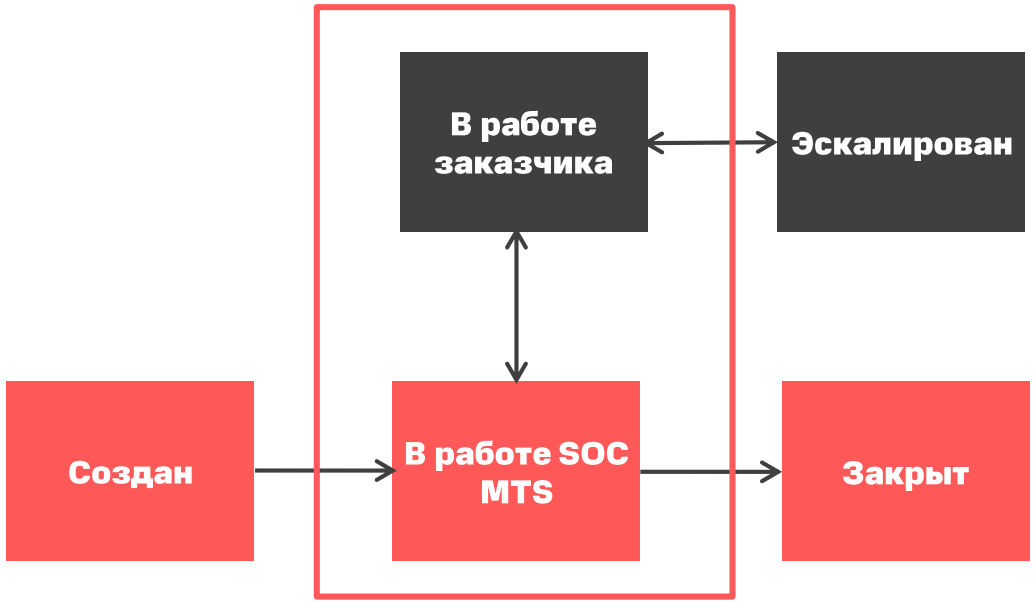


#CloudMTS

Жизненный цикл инцидента. Переходный период

Временные метрики:

- Реакция
- Информирование
- Реагирование
- Эскалация
- Обработка = Реакция + Информирование
- Решение = Обработка + Реагирование + Эскалация



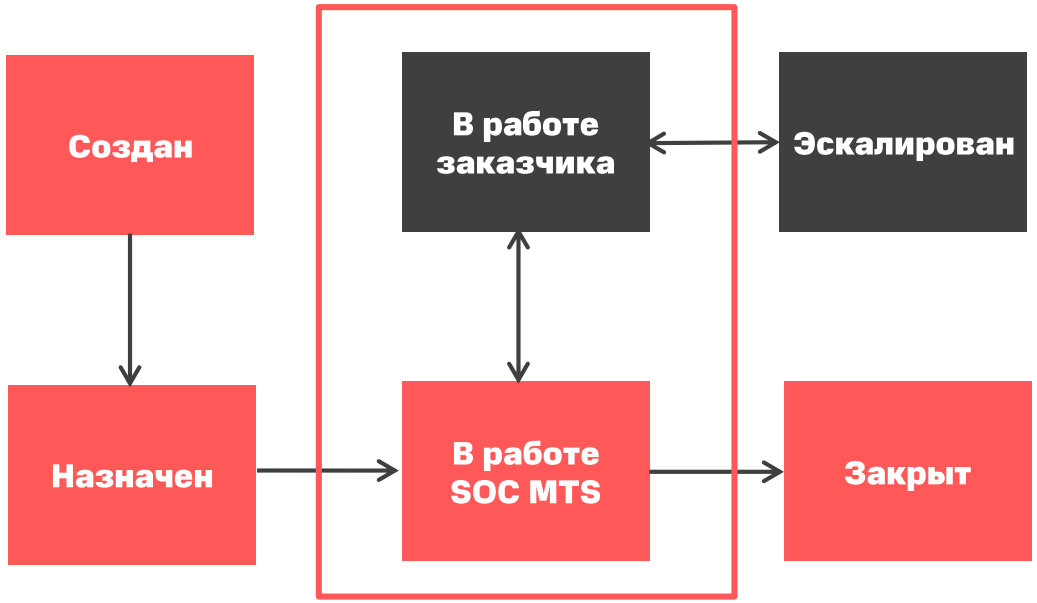
Количество	Реакция	Информирование	Реагирование	Обработка	Эскалация	Решение
667	7	17	29	53	302	355

#CloudMTS

Жизненный цикл инцидента. SOC MTS

Метрика для координатора инцидентов:

- Текущая нагрузка на аналитика
- Навыки
- Уровень иностранного языка



#CloudMTS

Статусы закрытия инцидента

Реальный инцидент. Действия злоумышленников. Например: успешная фишинговая атаки и отработала нагрузка из письма, кто-то подключил заражённый ноутбук в сеть и т.д.

Ложноположительный. Правило определило не то что мы хотели от него. Например, нашло HackTools в KMS.

Пентест. Все что связано с pentest'ом. Чтобы отличать их от реальных инцидентов.

Комплаенс. Нарушение. Инциденты связанные с поддержанием кибербезопасности в компании на должном уровне. Например, добавление пользователя в критичную доменную группу. Когда подтверждаем не легитимность действий. Например, случайно добавили в группу или решили не согласовывать с ИБ.

Комплаенс. Легитимно. Инциденты связанные с поддержанием кибербезопасности в компании на должном уровне. Например: добавление пользователя в критичную доменную группу. Закрываем с пометкой «Легитимно», когда подтверждается легитимность данных действий.

#CloudMTS

Статусы закрытия инцидента

Проблема сбора событий. Подтверждено. Нет событий с источника вследствие падения канала, либо других проблем. Ставим «Подтверждено», когда что-то предпринималось для исправления ситуации. Например: перезапускалось служба WEC на сервере.

Проблема сбора событий. Ложноположительное. Нет событий с источника вследствие падения канала, либо других проблем. Ставим «Ложноположительное», когда срабатывание правила было ложным. Например: отсутствие события с VPN концентратора, ввиду того что это не «болтливый» источник и мониторинг зафиксировал проблемы в выходные дни.

Связанный инцидент. Инциденты, которые возникают из-за какого-то одного действия. По которым ведется одно расследование и нужны одни действия со стороны заказчика по ним.

Доработка логики. Свойство инцидента выбрав которое в тикет системе будет создан инцидент в по доработке логики правила. Инцидент берёт в работу аналитик SOC.

#CloudMTS

Поля карточки инцидента

Базовые поля:

- уникальный порядковый номер инцидента
- тип инцидента. Имя правила, по которому сработал инцидент
- категория инцидента
- категория по MITRE. Тактика и техники
- категория по ГосСОПКА
- флаг принадлежности инцидента к КИИ
- критичность инцидента
- статус инцидента
- ключевые поля инцидента. Набор значений из события об инциденте из сторонней системы на основании которых можно сделать вывод об уникальности инцидента
- счётчик дублируемых инцидентов. Увеличивается на единицу, когда приходит инцидент с аналогичными ключевыми полями
- время последнего обновления счётчика дублируемых инцидентов
- сырое событие на основе которого создался инцидент

#CloudMTS

Поля карточки инцидента

Поля принадлежности:

- Customer/Tenat/Domain
- источник активности:
  - IP адрес
  - GEO IP
  - FQDN
  - Имя пользователя
- **Цель активности:**
  - IP адрес
  - GEO IP
  - FQDN
  - Имя пользователя

Поля принадлежности:

- ответственный исполнитель или группа
- комментарий к инциденту
- финальный комментарий к инциденту
- Файлы. Хранение файлов.

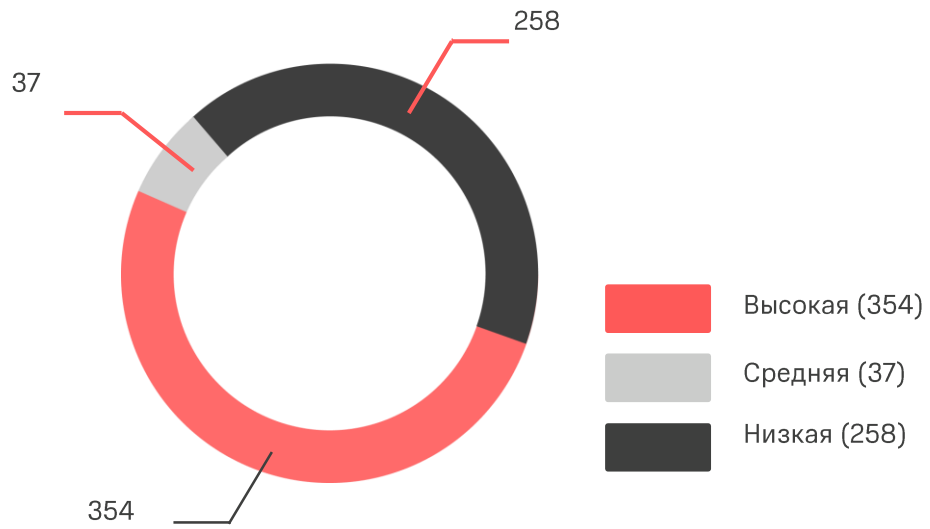
Поля временных меток:

- время создания инцидента
- время события на конечном устройстве которое передало событие
- время реакции
- время эскалирования инцидента
- время закрытия инцидента
- время последнего изменения инцидента

#CloudMTS

Основные метрики. Инциденты.

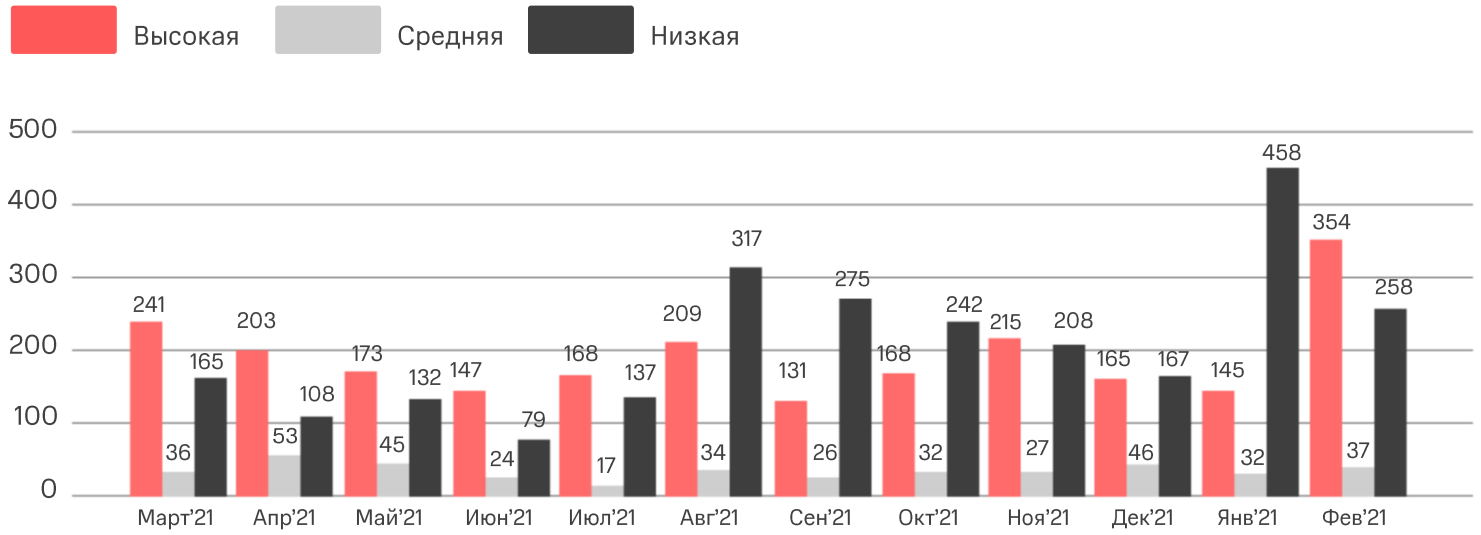
Распределение инцидентов по критичности



#CloudMTS

Основные метрики. Инциденты.

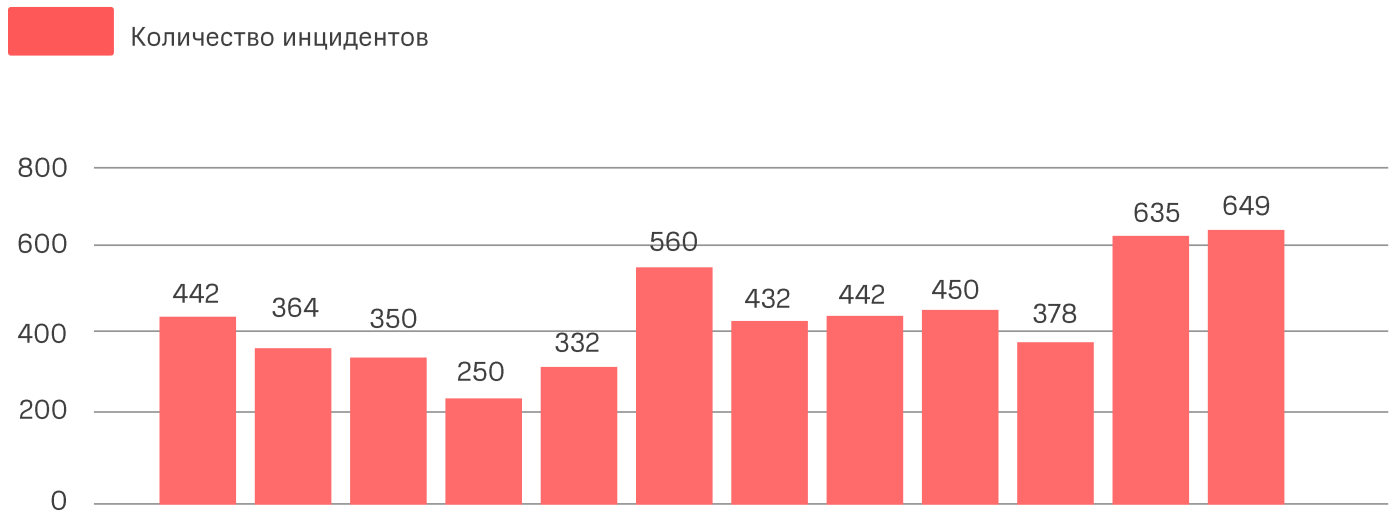
Динамика количества инцидентов разного уровня критичности по месяцам



#CloudMTS

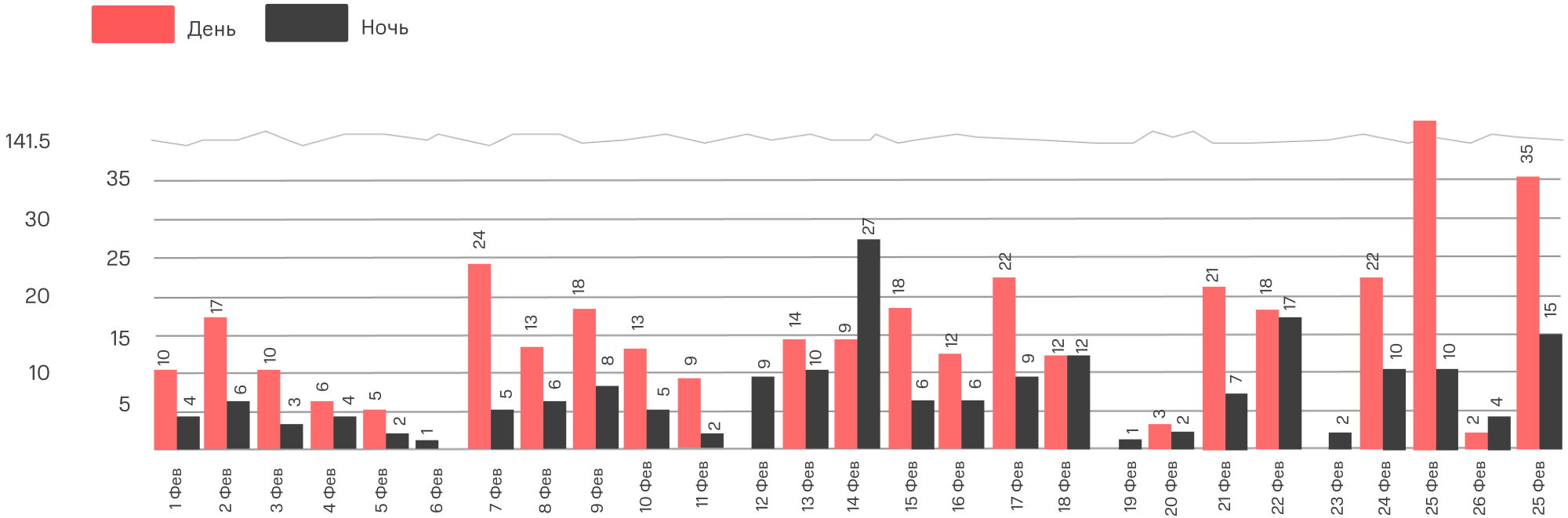
Основные метрики. Инциденты.

Динамика количества инцидентов по месяцам



#CloudMTS

Основные метрики. Инциденты.



#CloudMTS

Узнавайте первыми:

- о новинках и обновлениях продуктов #CloudMTS
- об актуальных мероприятиях
- о последних важных событиях месяца

Подпишитесь на рассылку:

#CloudMTS

Спасибо!