История запроса, изменившего сервис

Виктор Пенский
Начальник отдела ИБ ПАО «Юнипро»

Антон Юдаков
Операционный директор Центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар»

Ростелеком Солар

юнипро

Эволюция сервиса SOC в ПАО «Юнипро»

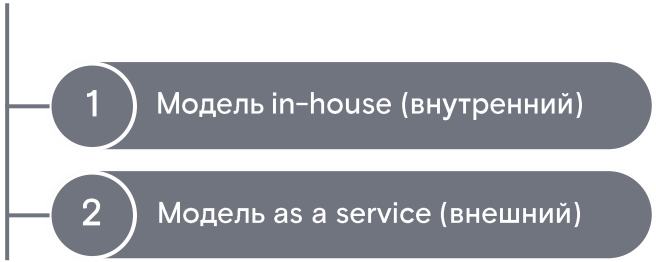
Ростелеком Солар

юнипро

История сотрудничества

Глобальная стратегия концерна Uniper

Реализация в ПАО «Юнипро» функции Security Operations Center:



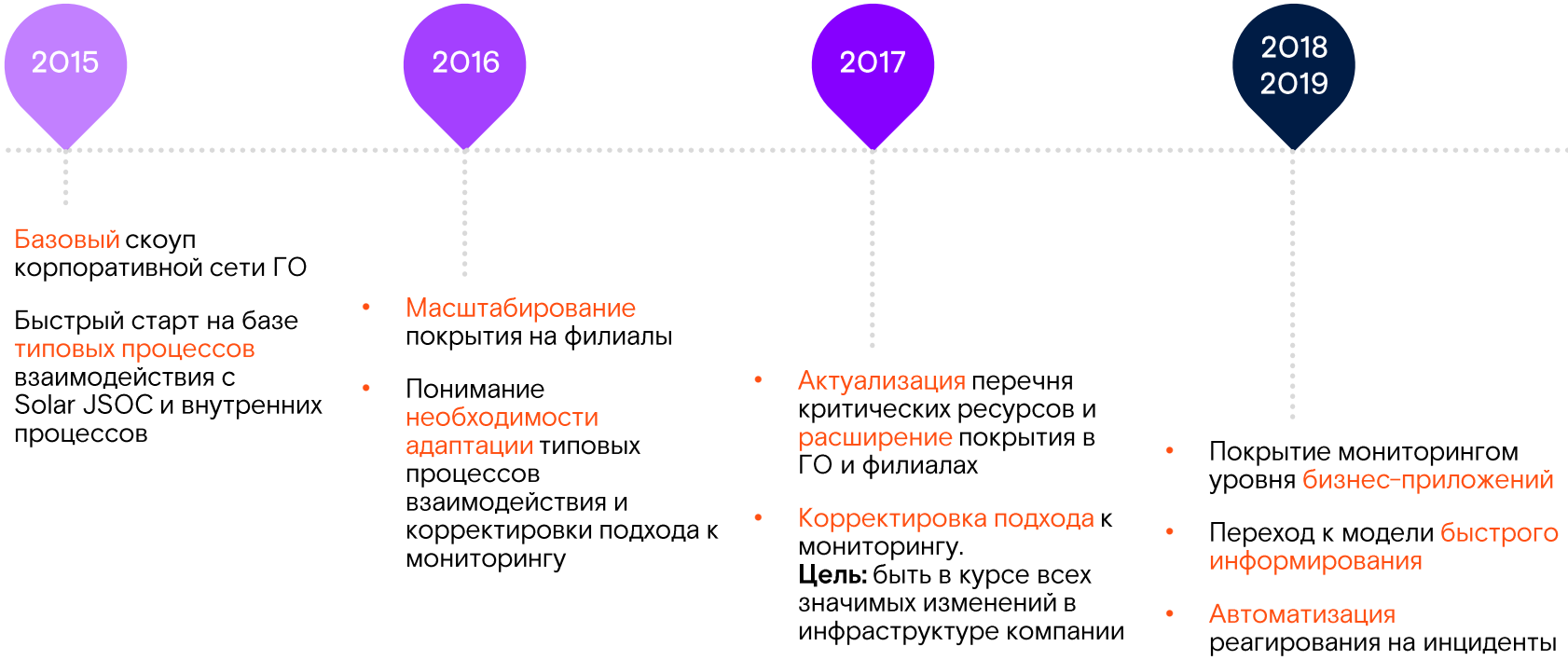
Гибридная модель:

- Мониторинг и расследование – as a service
- Анализ – совместно
- Реагирование – in-house

Ростелеком Солар

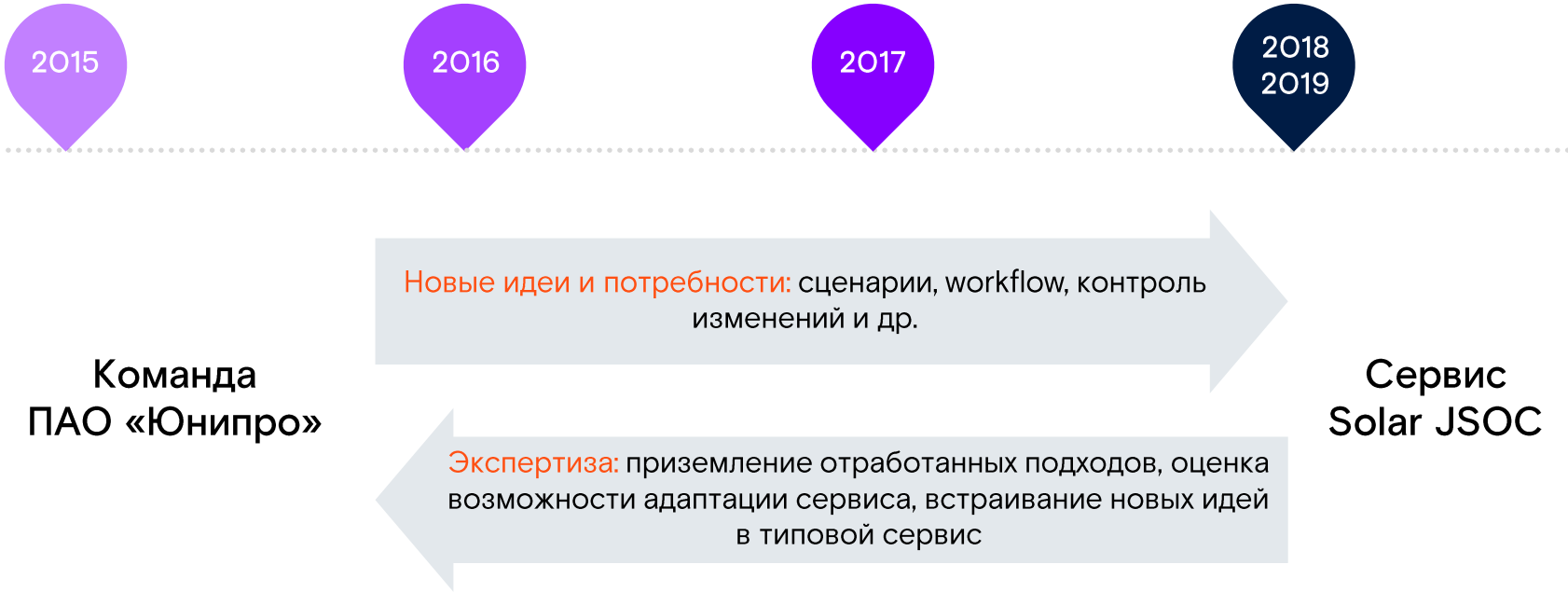
юнипро

Хронология развития сервиса и потребностей



Ростелеком Солар

Двустороннее взаимодействие поддерживает постоянное развитие сервиса



Ростелеком Солар

Практические кейсы и как они меняли сервис

Ростелеком Солар

юни про

Кейс 1. Новые идеи сценариев, которые стали типовыми (1/2)

Сотрудники ПАО «Юнипро» активно участвуют в разработке новых сценариев

15

специализированных сценариев было создано по инициативе команды ПАО «Юнипро»

7

из них были включены в типовые сценарии Solar JSOC для всех клиентов

Ростелеком Солар

юнипро

Кейс 1. Новые идеи сценариев, которые стали типовыми (2/2)

Пример: сценарий «Попытка ввода пароля в окне логина»

Цель: ошибка пользователя, особенно администратора, и ввод пароля в поле логина приводит к компрометации паролей от их учетных записей в журнале событий (в частности, Windows Event Log)

Выявление

- Собраны требования к паролям и правила именования учетных записей
- Реализованы корреляционные правила
- Автоматизировано обогащение информации по инциденту

Информирование

- Real-time уведомления только по критическим хостам и учетным записям (пароль маскируется автоматически)
- Собираемая статистика и детальная информация доступна только сотрудникам клиента

Реагирование

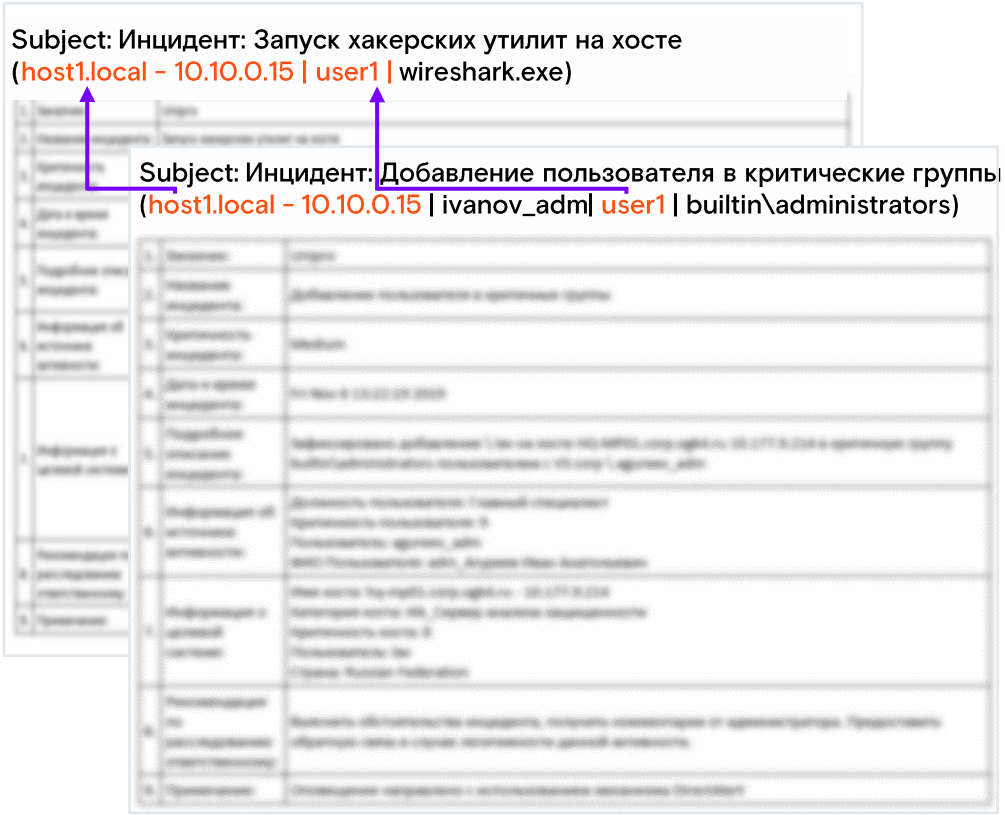
- По скомпрометированным учетным записям инициируется смена пароля
- По статистике выявляются наиболее невнимательные сотрудники и с ними проводится дополнительная работа

Ростелеком Солар

Кейс 2. Быстрая корреляция по ключевой информации (1/2)

Сотрудники ПАО «Юнипро»:

- Глубокое понимание своей инфраструктуры и процессов
- «Быстрая» корреляция по ключевым полям – достаточно увидеть ключевые поля в оповещении, чтобы выявить наиболее критические события или цепочки событий
- Оперативное реагирование на наиболее критические события
- Не отменяет обработку всех подозрений на инциденты, но помогает приоритизировать реагирование



Ростелеком Солар

юнипро

Кейс 2. Быстрая корреляция по ключевой информации (2/2)

Аналогичный принцип быстрой корреляции реализован в рамках сервиса Solar JSOC

Автоматизация:

- Автоматическое выстраивание «kill-chain» цепочек событий со связанными ключевыми полями
- Распределение подозрений на инциденты между линиями мониторинга Solar JSOC – связанные события обрабатываются одним филиалом/инженером, автоэскалация по экспертизе в случае явного выстраивания в «kill-chain»
- Эскалация приоритета подозрений на инциденты при появлении определенных значений в ключевых полях (учетные записи, хосты, сигнатуры и т.п.).

Ростелеком Солар

Кейс 3. Появление механизма быстрых оповещений (1/3)

Типовой процесс оповещения об инцидентах:

- Все подозрения на инциденты обрабатываются линиями мониторинга Solar JSOC
- Типовой SLA по информированию о критичных инцидентах – 30 минут

Требование:

сотрудникам ПАО «Юнипро» необходимо узнавать о критических инцидентах мгновенно, чтобы сразу инициировать процесс реагирования

Ростелеком Солар

Юнипро

Кейс 3. Появление механизма быстрых оповещений (2/3)

На стороне сервиса Solar JSOC был разработан и реализован механизм быстрых оповещений – автоматическая обработка и формирование оповещений без участия линий мониторинга

Принципы быстрых оповещений

- Полностью автоматическое формирование оповещения
- Максимальное обогащение контекстом по событию
- Механизмы защиты от флуда
- Применим для сценариев, где работу линии мониторинга можно максимально автоматизировать без потери качества оповещения

5 мин

SLA по информированию для ПАО «Юнипро»

Ростелеком Солар

Кейс 3. Появление механизма быстрых оповещений (3/3)

Что делать с остальными сценариями?

В ряде случаев нельзя полностью автоматизировать работу линий:

- необходимо проводить более глубокий анализ – только ручной труд
- ложные срабатывания нельзя полностью исключить на уровне корреляции
- часть действий линий просто технически не автоматизируема

Быстрые оповещения с последующей обработкой линией

- Реализован новый workflow: быстрое оповещение заказчика с последующим дополнительным анализом и дополнением контекста вокруг инцидента силами линий мониторинга

5 мин SLA по информированию о критичных инцидентах для ПАО «Юнипро»

+

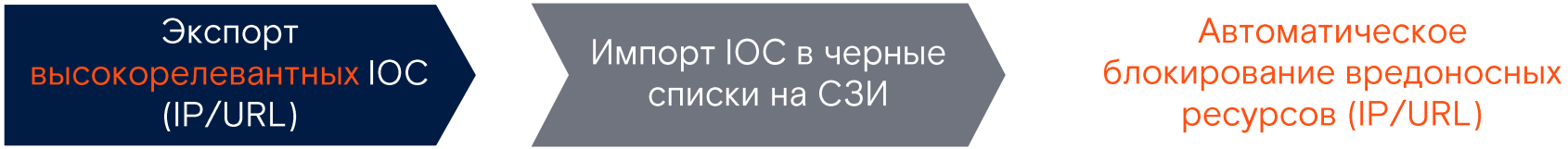
30 мин SLA по предоставлению дополнительной информации

Ростелеком Солар

юнипро

Кейс 4. Автоматическое реагирование (1/2)

В рамках оказания сервиса Solar JSOC осуществляет выявление фактов обращения хостов в сети ПАО «Юнипро» к вредоносным ресурсам



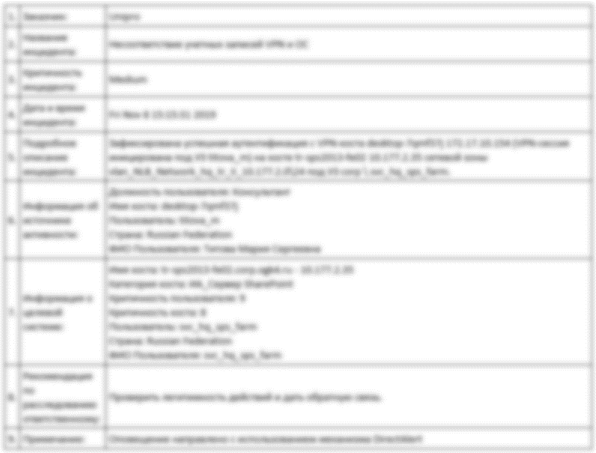
Ростелеком Солар

юнипро

Кейс 4. Автоматическое реагирование (2/2)

В рамках оказания сервиса Solar JSOC осуществляет усиленный контроль за действиями подрядчиков ПАО «Юнипро»

Subject: Инцидент: Несоответствие учетных записей VPN и ОС (10.1.1.125| Ivanov.i | petrov.a)



Выявление фактов:

- использования чужих привилегированных учетных записей сотрудников подрядчика для доступа к ресурсам внутри сети
- использования чужих учетных записей для подключения по VPN

Автоматическое блокирование учетной записи подрядчика и уведомление его по e-mail

Ростелеком Солар

Юнипро

Изменяя сервис – подходы к развитию

Lauren Macdonald, flickr, CC licensing

Ростелеком
Солар

юнипро

Благодарим за внимание!

Виктор Пенский
Начальник отдела ИБ ПАО «Юнипро»

Антон Юдаков
Операционный директор Центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар»

Ростелеком Солар

юнипро