Раз, два, три, четыре, пять…
Стали SOC мы выбирать!

28 ноября 2018г.

Руководитель Отдела информационной безопасности
Всеслав Соленик

О банке

Первый* специализированный ипотечный банк – один из лидеров в области ипотечного кредитования

- Входит в топ-5 банков на рынке ипотеки
- Количество выданных кредитов (с 2003г.) – более 150 000
- Объем выданных кредитов – более 350 млрд руб.
- Ипотечный кредитный портфель – более 160 млрд руб. (на 30.06.2018)
- С 2014 года банк является единой ипотечной платформой группы Societe Generale в России

Банк, ориентированный на качественное обслуживание клиентов

- Средняя оценка качества обслуживания 4,9 балла из 5 по данным регулярных опросов клиентов
- Прозрачная организация с иностранным капиталом, работающая по международным стандартам управления и делового поведения

Российский банк, имеющий рейтинги международных агентств

- Fitch – рейтинг BBB- (2017)
- Moody's – Ba1 (2017)

О банке

- **Представлен более, чем в 45 регионах** по всей России
- Общее количество работников Банка около **900**
- Головной офис и Отдел ИБ расположены в Москве

Предпосылки к внедрению SIEM и SOC

Стратегия развития ИБ

Вызовы и требования:

- *Директивы Группы SG*
- *Требования регуляторов*
- *Рост уровня зрелости при том же уровне ресурсов*
- *Эволюция атак и угроз*
- *Диджитализация бизнеса*
- *Лучшие практики*

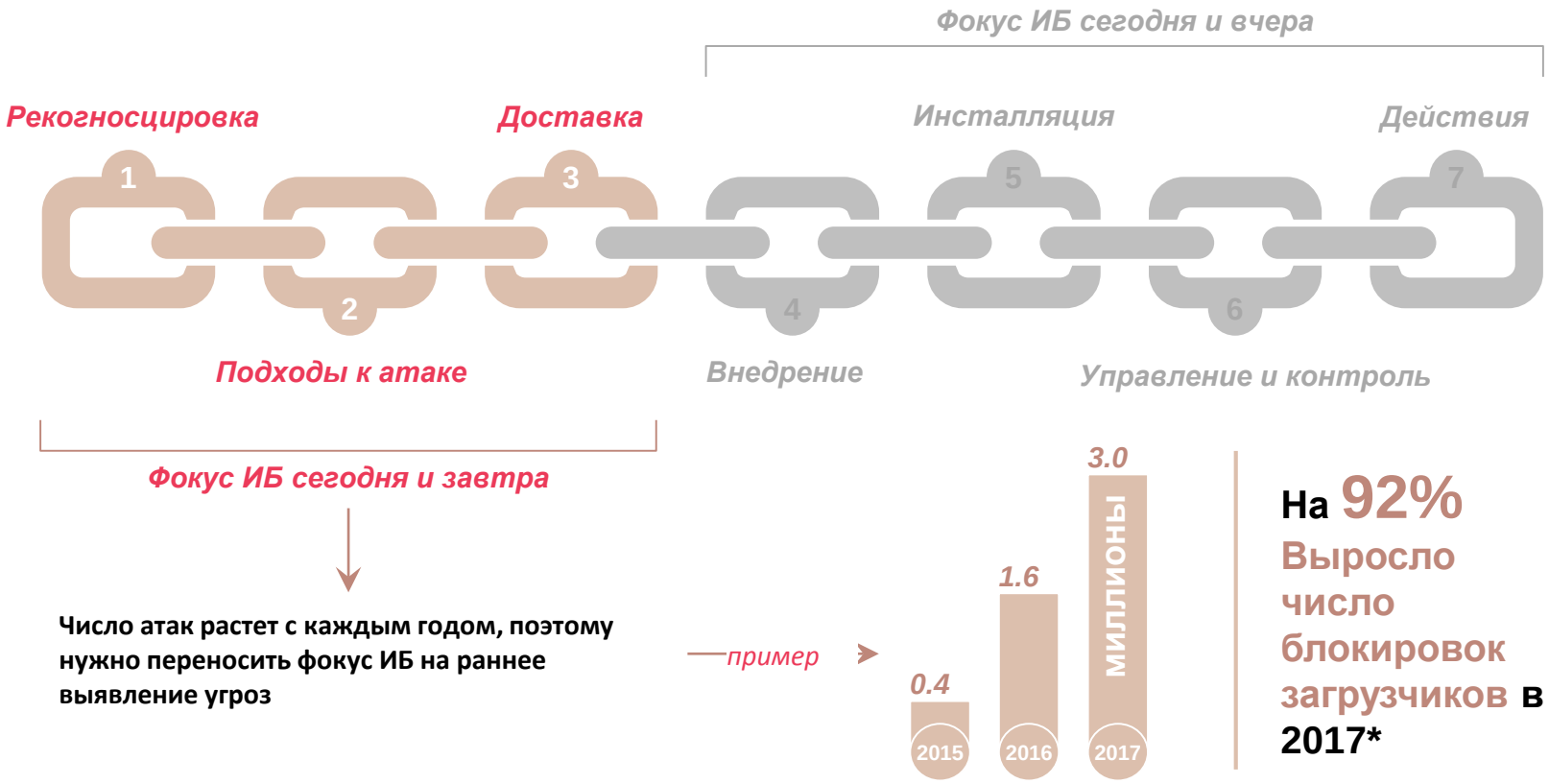
Цели внедрения LM/SIEM/SOC:

- **Процесс управления событиями. Стандартизация сбора и централизация хранения логов**
- **Автоматизация сбора и анализа событий**
- **Управление угрозами и уязвимостями (IoC).**
- **Управление инцидентами ИБ: раннее выявление, триаж, регистрация, оперативное реагирование**
- **Частичная автоматизация реагирования и оркестрация**
- **Расследование инцидентов, форензика**

А также:

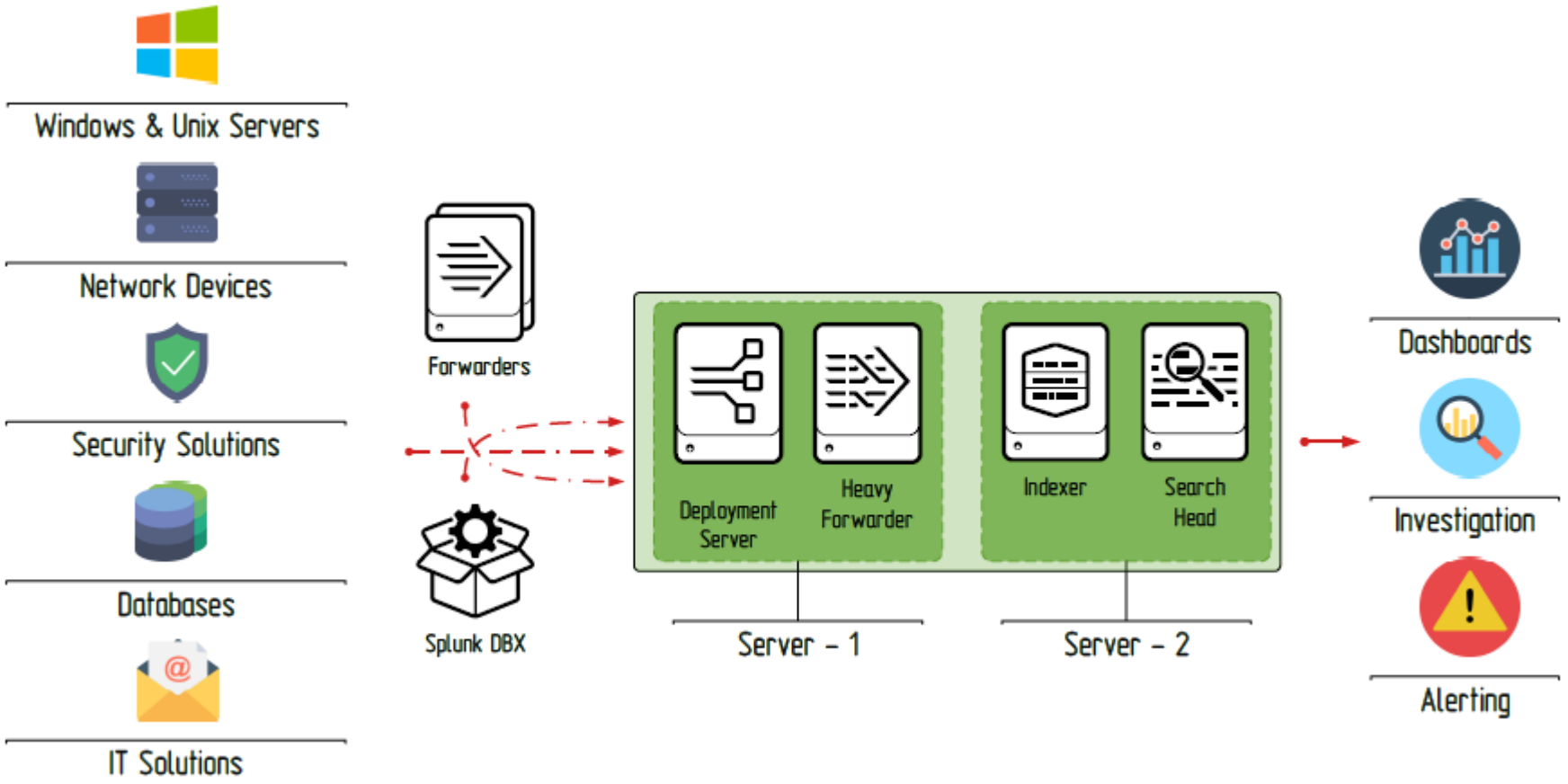
- Мониторинг метрик ИБ
- Дашборды и репортинг
- Управление активами и др. процессы ИТ
- Выявление аномалий по линии ИТ
- Снижение операционных рисков
- Взаимодействие с CERT SG, FinCERT
- Поведенческий анализ (UBA)

Изменение подхода на основе killchain

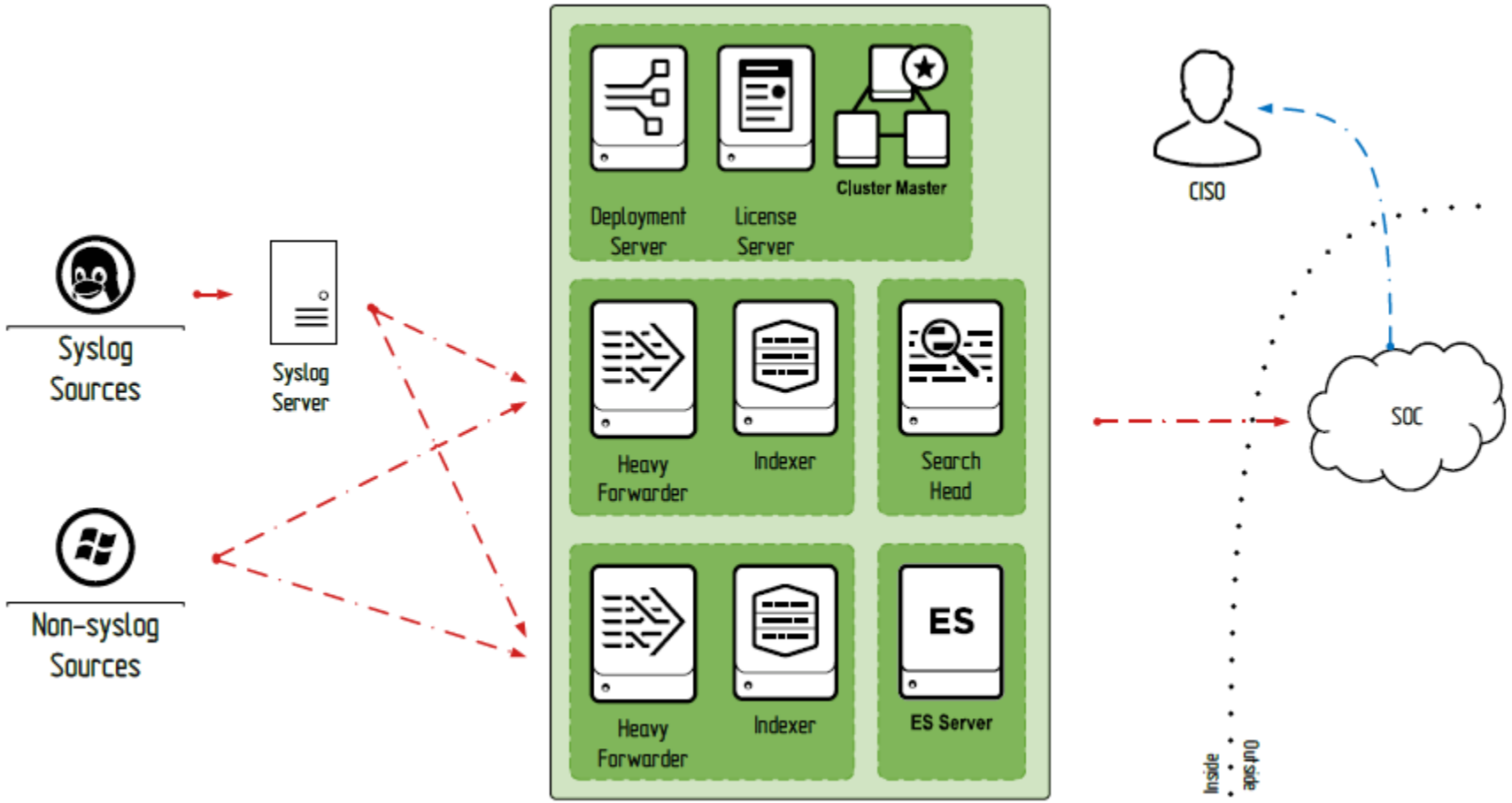


*согласноInternet Security Threat Report 2018, Symantec

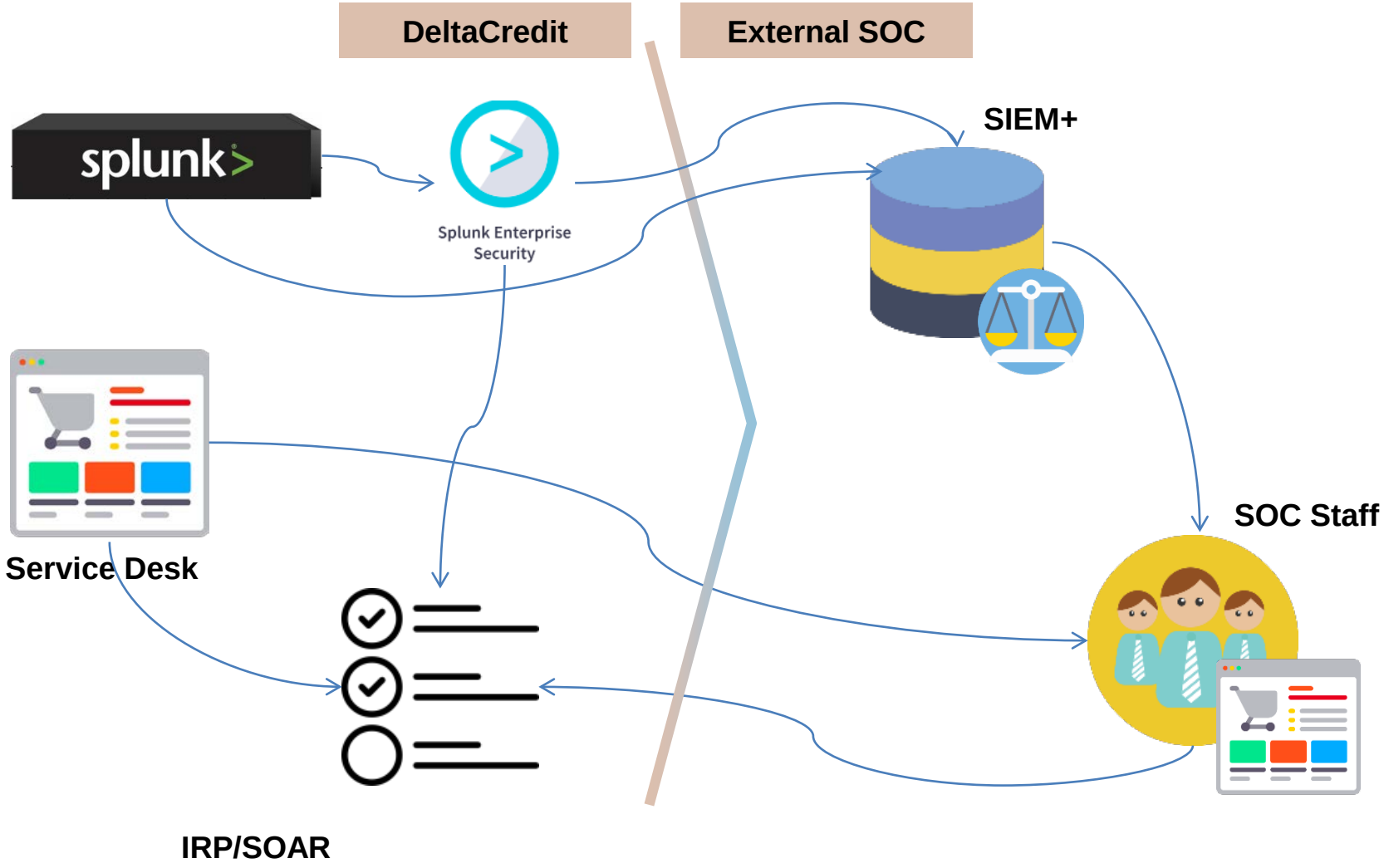
SIEM & SOC (Этап 1 – Сбор событий и метрики)



SIEM & SOC (Этап 2 – Корреляция и выявление)



SIEM & SOC (Этап 3 – Реагирование и оркестрация)



Как мы видели «наш» внешний SOC перед выбором

У нас есть SIEM и мы хотим ее использовать и развивать

Нам нужен гибкий подход со стороны партнера

Мы аутсорсим точечно то, что целесообразно (люди 24/7, компетенции, мониторинг)

Мы ориентируемся на best practice и стандарты

Бюджет, не превышающий затраты на обслуживание своего SOC

Разделение инвестиций

Прозрачность в ценообразовании, оценке ресурсов и трудозатрат

Контроль и управляемость сервиса

Комплаенс и конфиденциальность

Честное долговременное сотрудничество

Критерии выбора внешнего SOC

События ИС в нашем Splunk	• Все события и логи приходят из централизованного хранилища Банка на Splunk • Формат логов: syslog или CEF • Партнер не имеет доступа к ИС Банка
Опыт построения или сервиса SOC	• Наличие опыта (или специалистов с опытом) настройки SIEM/UBA, построения SOC • Наличие опыта предоставления сервиса SOC нескольким клиентам
Пилотный проект	• Ключевой критерий выбора поставщика услуг из-за их комплексности и сложности • Необходимо показать технологическую возможность сбора, разбора и анализа событий • Необходимо показать выявление аномалий и инцидентов в событиях Банка • Необходимо построить процесс коммуникации и реагирования • Пилот должен быть реализован в разумные сроки (до 3х месяцев)
Набор услуг	• Услуги 24/7 • Дополнительные услуги: выявление аномалий в активах, конфигурациях, процессах ИТ • Гибкость подхода к формированию пакета услуг и SLA
Время Go-live	• Наличие готовой платформы SOC у провайдера услуг • Интеграция со Splunk, включая маппинг событий • Настройка корреляционных правил для Банка
Корреляционные правила и доп. сервисы	• Наличие готовой базы корреляционных правил и их гибкость • Наличие экспертизы и правильный подход к построению правил и плейбукам • Наличие сервисов EDR, UBA, Big Data, SOAR, TI и компетенции в них
Стоимость услуг	• Прозрачность и адекватность ценообразования • Готовность к индивидуальным условиям при взаимной ценности договора для 2-х сторон • Стоимость технологических решений на стороне провайдера услуг

Внешний SOC – Кейс 1

События ИС в нашем Splunk	• HP ArcSight. Компетенции по Спланку отсутствуют • Syslog или CEF подходят, есть кейсы успешной интеграции • Партнер предложил делать маппинг силами Банка
Опыт построения или сервиса SOC	• Компания обладает обширным опытом в построении и оказании услуг SOC • Есть ряд референсных клиентов, в т.ч. банки
Пилотный проект	• Пилотный проект длился более полугода • Выбрано на пилот 3 источника, адаптирован подход, привлечена внешняя экспертиза • Со стороны партнера выделение ресурсов и активность коммуникаций были невысокими • Не удалось выполнить сбор событий с платформы Splunk Enterprise из-за отсутствия документации по настройке маппинга событий со стороны вендора ArcSight
Набор услуг	• Услуги 8/5 или 24/7 в зависимости от потребностей заказчика услуги • Набор услуг стандартизирован
Время Go-live	• 3-6 месяца. Есть готовая платформа SOC и все процессы • Интеграция со Splunk, включая маппинг событий – силами Банка • Есть опция настройки корреляционных правил для Банка
Корреляционные правила и доп. сервисы	• Экспертная база из 130 корреляционных правил. • 35 правил могут быть выбраны заказчиком для выявления инцидентов ИБ • Правила и плейбуки являются собственностью SOC – черный ящик.
Стоимость услуг	• Ценообразование достаточно закрытое, выше среднего по рынку • Готовность к индивидуальным условиям есть • Стоимость технологических решений переносится на заказчика

Внешний SOC – Кейс 2

События ИС в нашем Splunk	• Собственное решение на базе ELK стека и опционально - платформы IBM Q-Radar • Совместимость со Splunk подтверждают, компетенции начинают развивать • Партнер сделал маппинг событий своми силами
Опыт построения или сервиса SOC	• Есть опыт и экспертизой по внедрению SIEM, также у команды есть опыт оказания услуг SOC для организаций среднего масштаба • На рынке 2 года, есть порядка 5 клиентов
Пилотный проект	• Пилотный проект 2 месяца, успешно. Источники – порядка 10ти. • Со стороны партнера выделение ресурсов и активность коммуникаций были высокими • Коннектор и разбор событий были сделаны за 3 недели • Отсутствие на пилоте тикет-менеджмента в сервис-деске • Выявлено несколько аномалий и инцидентов
Набор услуг	• Услуги 8/5 или 24/7 в зависимости от потребностей заказчика услуги • Набор услуг стандартизирован, разделен на SOC и IRP+TI части • Готовность расширять услуги управлением инцидентами, мониторингом активов, ИТ процессов и пр.
Время Go-live	• 1-2 месяца. Есть готовая платформа SOC и все процессы • Заказчик только настраивает сбор и пересылку событий и задает требования • Есть опция настройки корреляционных правил для Банка
Корреляционные правила и доп. сервисы	• Экспертная база из 50 корреляционных правил для выявления инцидентов ИБ • Правила и плейбуки открыты для заказчика по запросу, но также собственность партнера
Стоимость услуг	• Ценообразование детальное, но закрытое. Среднее по рынку • Готовность к индивидуальным условиям есть • Стоимость технологических решений не переносится на заказчика явно

Внешний SOC – Кейс 3

События ИС в нашем Splunk	• Компания обладает экспертизой, но услуга SOC провайдера для нее новая • SOC на площадке Банка с использованием Splunk Enterprise Security. • Маппинг событий и интеграции проводить не требуется
Опыт построения или сервиса SOC	• Есть опыт и экспертиза по внедрению SIEM, но нет опыта сервиса SOC • Широкая экспертиза в работе с платформой Splunk Enterprise/Enterprise Security,
Пилотный проект	• Пилотный проект не проводился, потому что концепция изменилась и ввиду рисков построения услуги «с нуля». • Со стороны партнера велась доработка Splunk для банка – качество и коммуникации на высоком уровне
Набор услуг	• Услуги 8/5 или 24/7 в зависимости от потребностей заказчика услуги • Набор услуг не стандартизирован, строится с нуля под Заказчика • Готовность расширять услуги управлением инцидентами, мониторингом активов, ИТ процессов и пр.
Время Go-live	• 4-7 месяцев: используется технологическая платформа, построенная на стороне Банка, а также адаптированная база правил Splunk ES. • Есть опция настройки корреляционных правил и плейбуков для Банка
Корреляционные правила и доп. сервисы	• Отсутствует собственная готовая база корреляционных правил, но предалагается разработать корреляционные правила в количестве 50 штук. • Правила и плейбуки принадлежат заказчику
Стоимость услуг	• Ценообразование детальное, открытое. Ниже среднего по рынку • Готовность к индивидуальным условиям есть • Стоимость технологических решений на заказчике, т.к. на его площадке

Внешний SOC – Кейс 4

События ИС в нашем Splunk	• Собственное разработанное решение на базе Apache Spark • Не могут организовать сбор событий с платформы Splunk Enteprise и предлагают только услугу по мониторингу SIEM банка. Реагирование на инциденты на стороне Банка.
Опыт построения или сервиса SOC	• Достаточный опыт в построении и предоставлении услуги SOC • 2 года на рынке • Сейчас только один якорный заказчик, но активно идут на рынок
Пилотный проект	• Пилотный проект не проводился: компания не может выполнить сбор (забор) событий с платформы Splunk Enterprise.
Набор услуг	• Услуги 8/5 или 24/7 в зависимости от потребностей заказчика услуги • Набор услуг стандартизирован, пакетный, но для Банка ограничен мониторингом • Готовность расширять набор услуг при условия оказания их на площадке Банка
Время Go-live	• От 2-х месяцев: зависит от Заказчика. • Есть готовая платформа и набор правил, однако на своей платформе – неприменимо. • Есть опция дизайна корреляционных правил и плейбуков для Банка
Корреляционные правила и доп. сервисы	• Планируется использовать корреляционные правила для реагирования на инциденты ИБ, которые были разработаны Банком самостоятельно • Правила и плейбуки принадлежат заказчику
Стоимость услуг	• Ценообразование детальное. Среднее по рынку • Пакетные наборы услуг по фиксированной цене, но обсуждаемо • Стоимость технологических решений на заказчике, т.к. на его площадке

Внешний SOC – Кейс 5

События ИС в нашем Splunk	• Собственное разработанное решение на базе комплекса решений Apache Spark, Apache Hadoop, Kafka и Splunk Enterprise Security • Могут организовать сбор событий с платформы Splunk Enteprise. Маппинг не нужен
Опыт построения или сервиса SOC	• Объявили о начале предоставлении услуги SOC в апреле 2018 года • Сейчас идут пилотные проекты, возможно есть 1 заказчик • Опыт внедрения SIEM и консалтинга по SOC большой
Пилотный проект	• Пилотный проект не проводился, поскольку у компании отсутствует техническая платформа в промышленной эксплуатации. • Она гибко разворачивается под каждый пилот отдельно и это занимает значительное время.
Набор услуг	• Услуги 8/5 или 24/7 в зависимости от потребностей заказчика услуги • Набор услуг очень широкий и гибкий, вплоть до размещения платформы. Интересный, зрелый концепт SOC • Готовность расширять набор услуг по требованиям Заказчика
Время Go-live	• 4+ месяца: В настоящий момент у SOC провайдера отсутствует техническая платформа для организации сбора событий. • Есть опция дизайна корреляционных правил и плейбуков для Банка
Корреляционные правила и доп. сервисы	• Обладают экспертной базой корреляционных правил, но не указывают точное количество данных правил • Правила и плейбуки могут принадлежать заказчику • Наличие сервисов EDR, UBA, Big Data, SOAR, TI и компетенции в них
Стоимость услуг	• Ценообразование детальное. Среднее по рынку • Стоимость технологических решений явно переносятся на заказчика или могут принадлежать ему

ДЕЛЬТАКРЕДИТ
Ипотечный Банк

SOCIETE GENERALE GROUP

Благодарю за внимание
и готов ответить на ваши вопросы!

Соленик Всеслав Сергеевич
vsolenik@deltacredit.ru