Инциденты ИБ как отправная точка при построении SOC

Георгий Морозов

Менеджер по сопровождению корпоративных клиентов

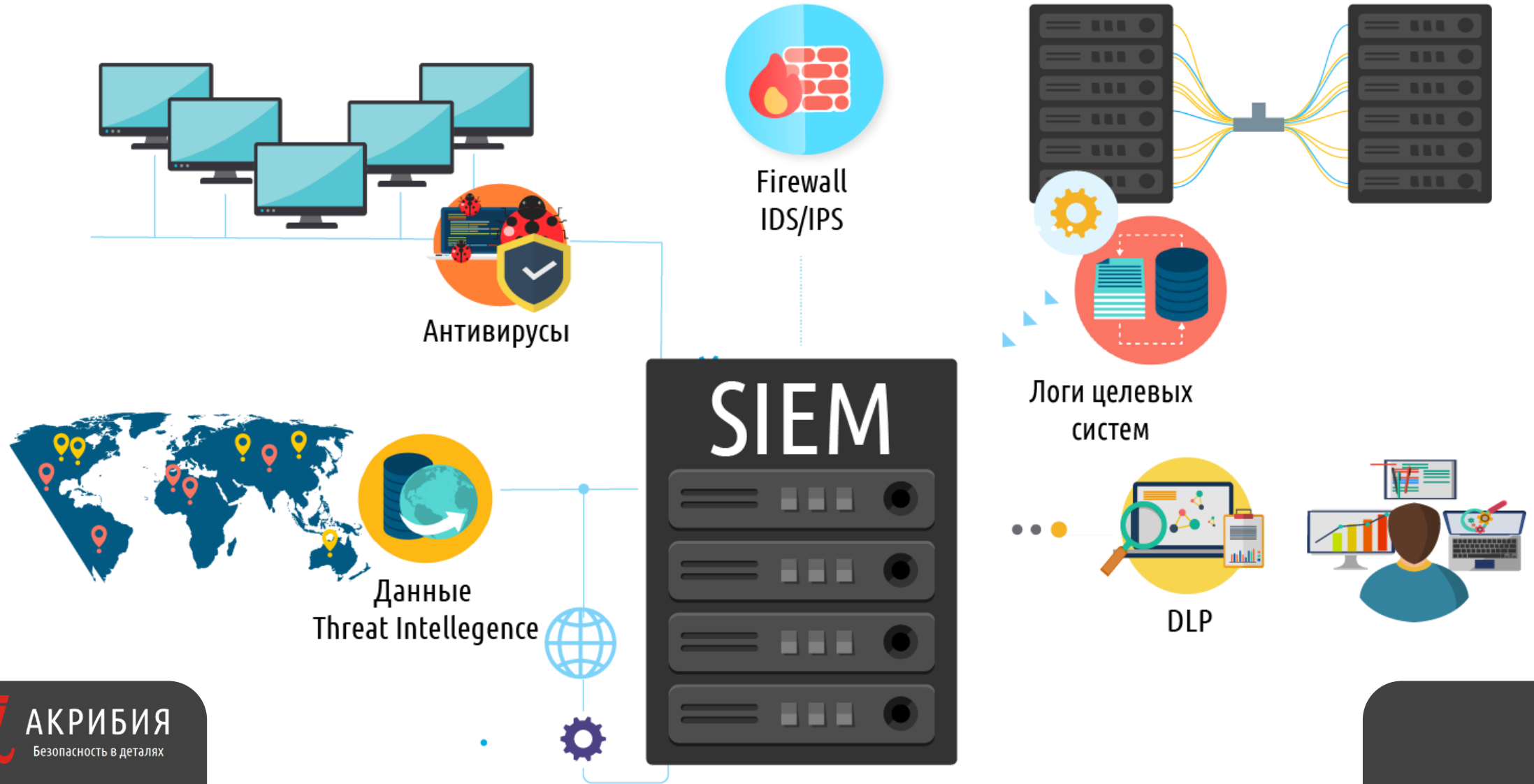
Вопросы, возникающие при внедрении SOC

Какую SIEM-систему выбрать?

Какие СЗИ и активы в инфраструктуре помогут в выявлении инцидентов?

Как регламентировать работу с инцидентами?

Типовые поставщики данных для SOC



Примеры выявляемых инцидентов

Что первично?

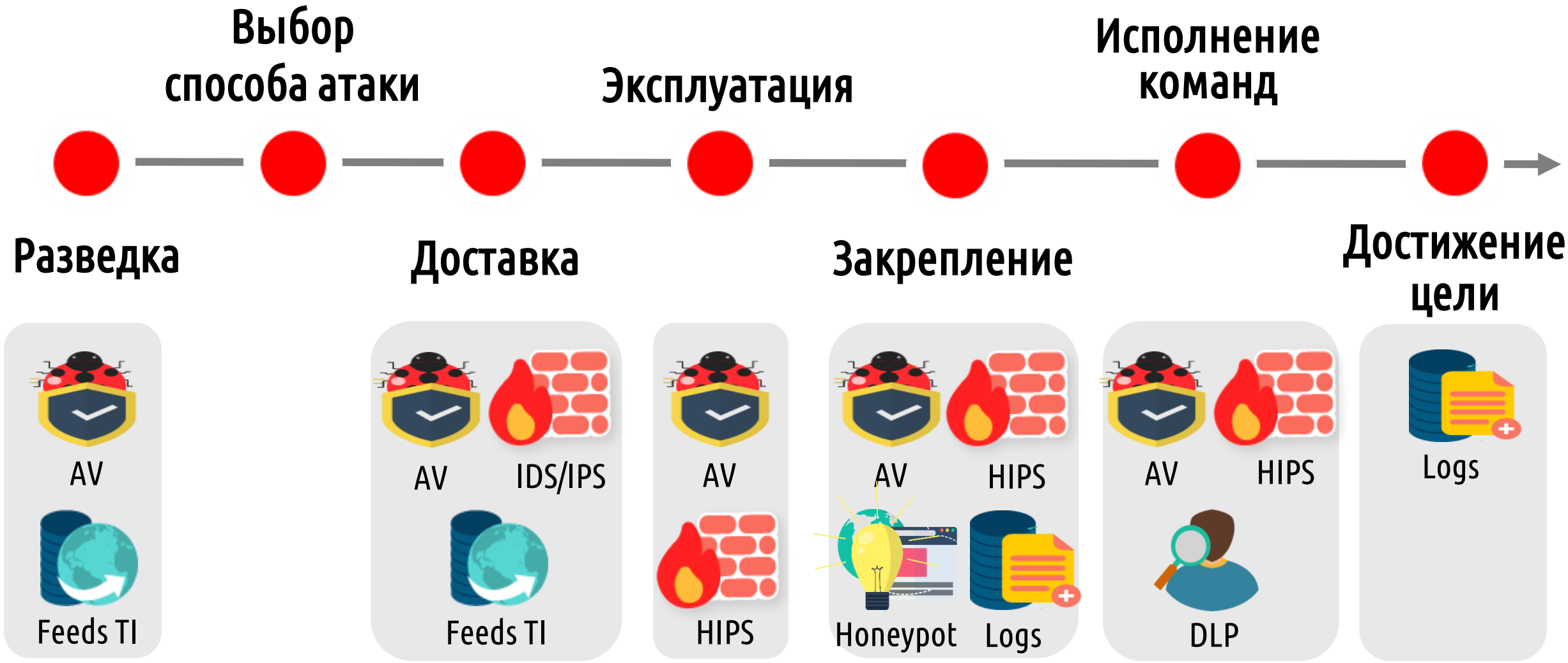
Инциденты ИБ

?

Архитектура SOC

Идентификация наиболее критичных инцидентов

Выявление хакерских атак



Мотивы злоумышленника

Цель	*Объект атаки*	*Активы*
прямая денежная выгода	ДЕНЬГИ	АБС, системы ДБО, Банк-клиенты
шантаж, вымогательство *продажа данных третьим лицам*	ДАННЫЕ	CRM-системы, финансовые показатели, информация о патентах
нанести вред *(по заказу / из неприязни)*	ИНФРА - СТРУКТУРА	АСУ ТП, информационные системы, веб-ресурсы

Инциденты, критичные для бизнеса

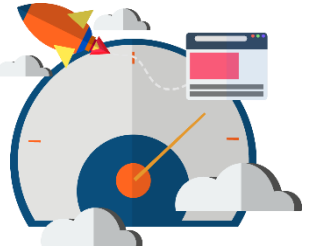
Мошенничество

Нарушение непрерывности бизнеса

Раскрытие конфиденциальной информации

Таргетированные кибератаки

Нарушение целостности информации



Ненадлежащее использование информационных ресурсов

Инцидент 1:

Мошенничество

Тип инцидента: *мошенничество*	**Критичность инцидента для бизнеса:** *средняя*
Тип нарушителя: *внутренний*	**Какое свойство информации нарушено:** *конфиденциальность*
Тип атакованной информационной системы: *CRM-система*	
События предшествующие инциденту *заявление клиента о наступлении страхового случая*	
Инструментарий, необходимый для выявления *DLP, логи почтового сервера*	

Инцидент 2:

Компрометация учетных данных

Тип инцидента: *утечка данных*	**Критичность инцидента для бизнеса:** *высокая*
Тип нарушителя: *внешний*	**Какое свойство информации нарушено:** *конфиденциальность*
Тип атакованной информационной системы: *веб-портал*	
События предшествующие инциденту *brute force атака с использованием базы данных , содержащей авторизационные пары логин/пароль*	
Инструментарий, необходимый для выявления *IPS-система, логи веб-сервера*	

EternalBlue [CVE-2017-0144]

Инцидент 3:

Нарушение целостности информации

Тип инцидента: *шифрование данных*	**Критичность инцидента для бизнеса:** *Высокая*
Тип нарушителя: *внешний*	**Какое свойство информации нарушено:** *доступность*
Тип атакованной информационной системы: *корпоративная сеть компании*	
События предшествующие инциденту *использование уязвимой версии Windows*	
Инструментарий, необходимый для выявления *TI, UEBA.*	

Преимущества инцидент-ориентированного подхода

Позволяет оценить значимость SOCa относительно ценности активов

Дает понимание, каких инструментов не хватает в инфраструктуре для детектирования

Позволяет выстроить процесс работы с инцидентом на всем жизненном цикле