cyberART

Использование технологий Big Data для развития средств SOC

Низамеев Роберт

Менеджер по развитию бизнеса, CyberART

ICL SYSTEM TECHNOLOGIES

cyberART

Профессиональная сервисная служба в сфере кибербезопасности

- Более 50 экспертов
- Аналитика и данные
- Технические средства
- Security Operations Center

Типовые драйверы Big Data проектов

BIG DATA - инструмент SOC?

Текущая ситуация в SOC

cyberART

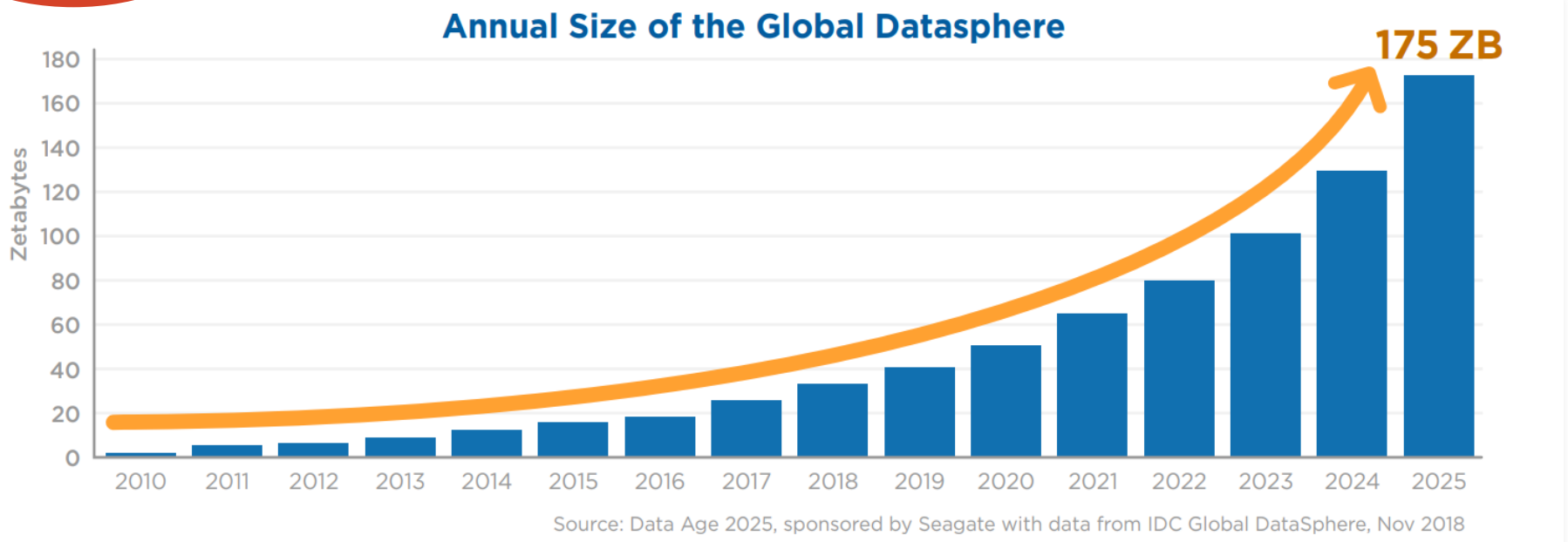
Большие объемы данных

+

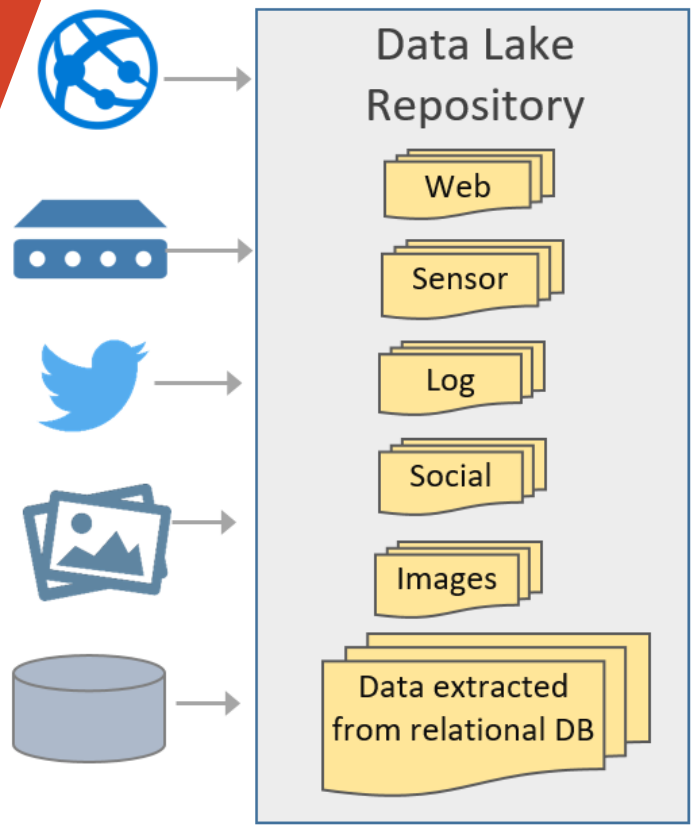
Быстрая генерация данных

+

Много разнородных источников



Что такое Security Data Lake



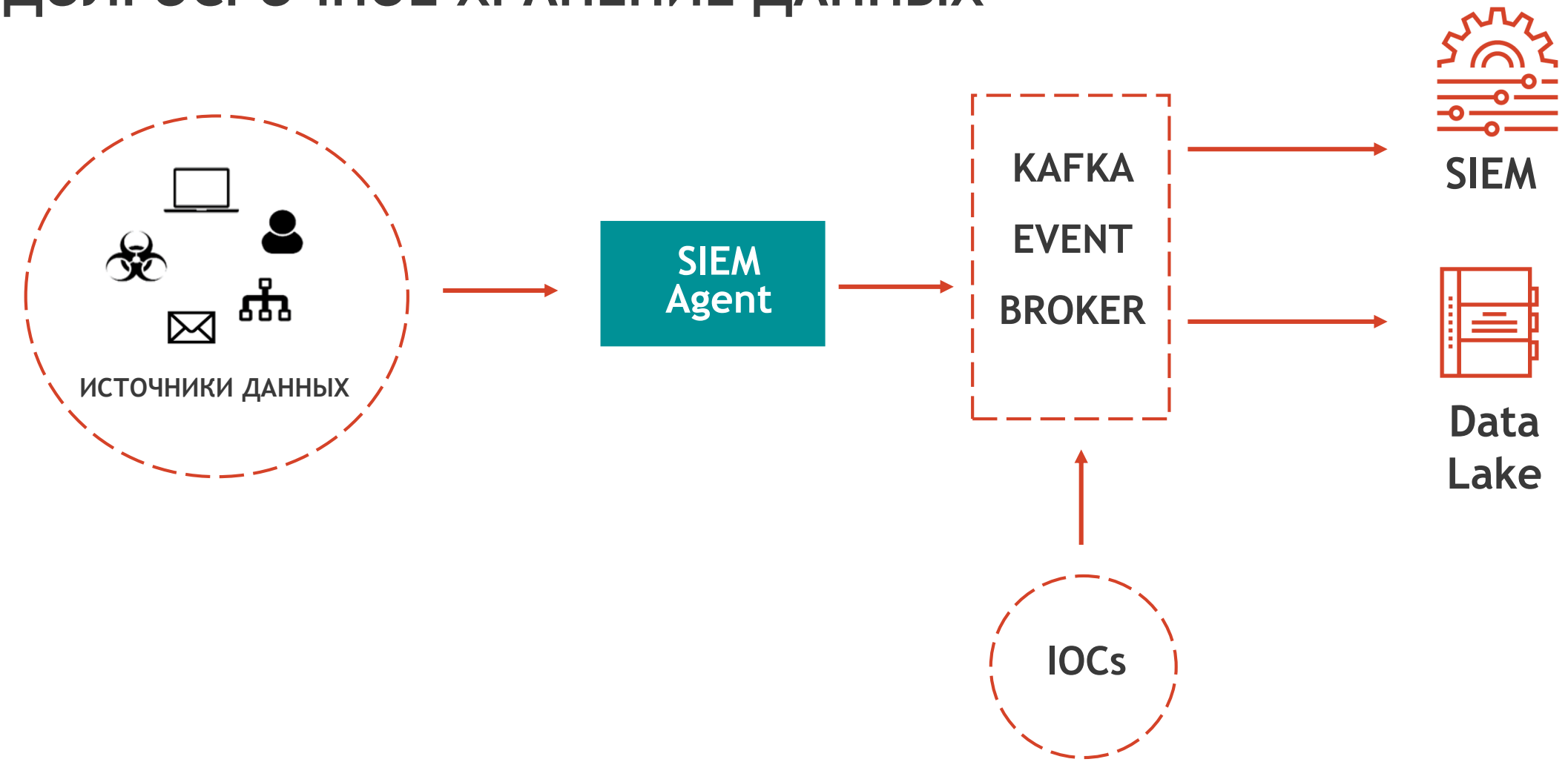
≠ SIEM

= Data Warehouse

Сценарии использования SDL

cyberART

ДОЛГОСРОЧНОЕ ХРАНЕНИЕ ДАННЫХ



Сценарии использования SDL

cyberART

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

- User Authentication Activity
- User Access Activity
- User Network Activity
- Environment Context
- User Context

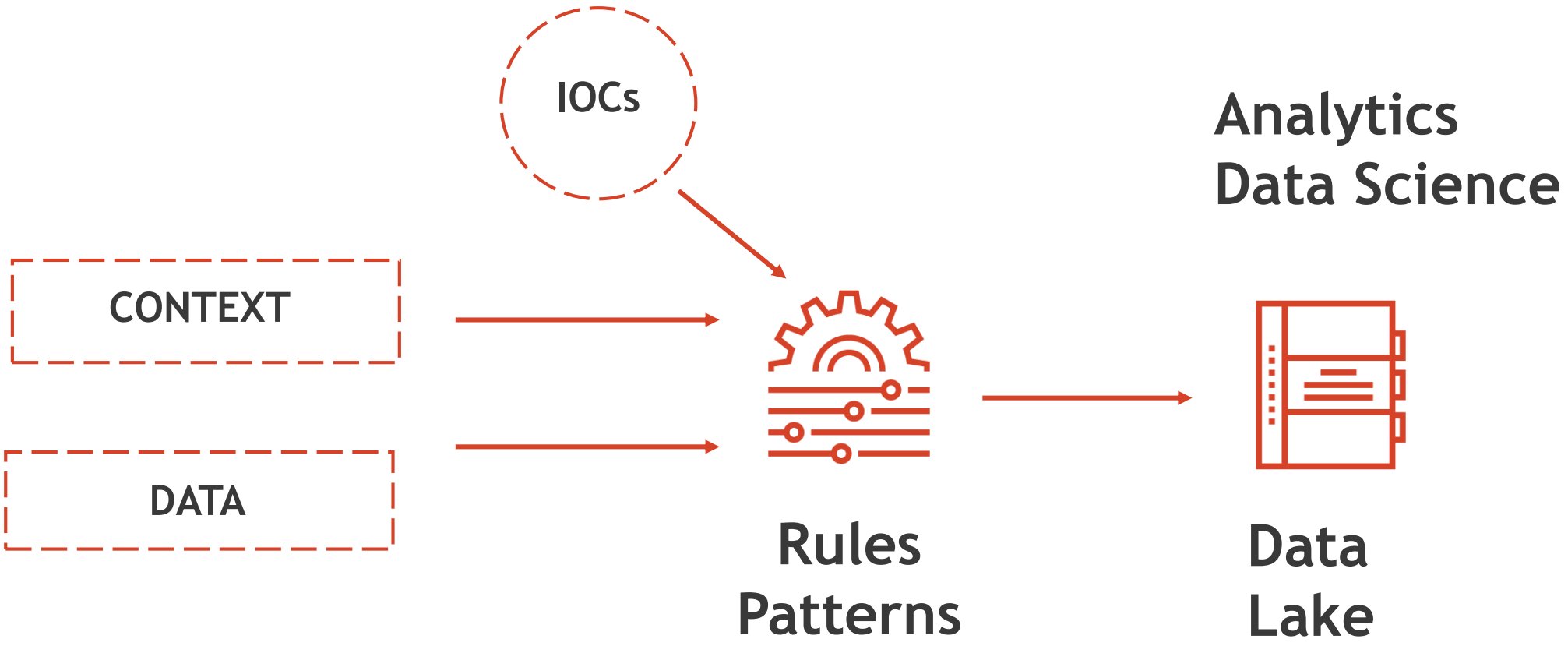
Data Lake

Analytics
Data Science

Сценарии использования SDL

cyberART

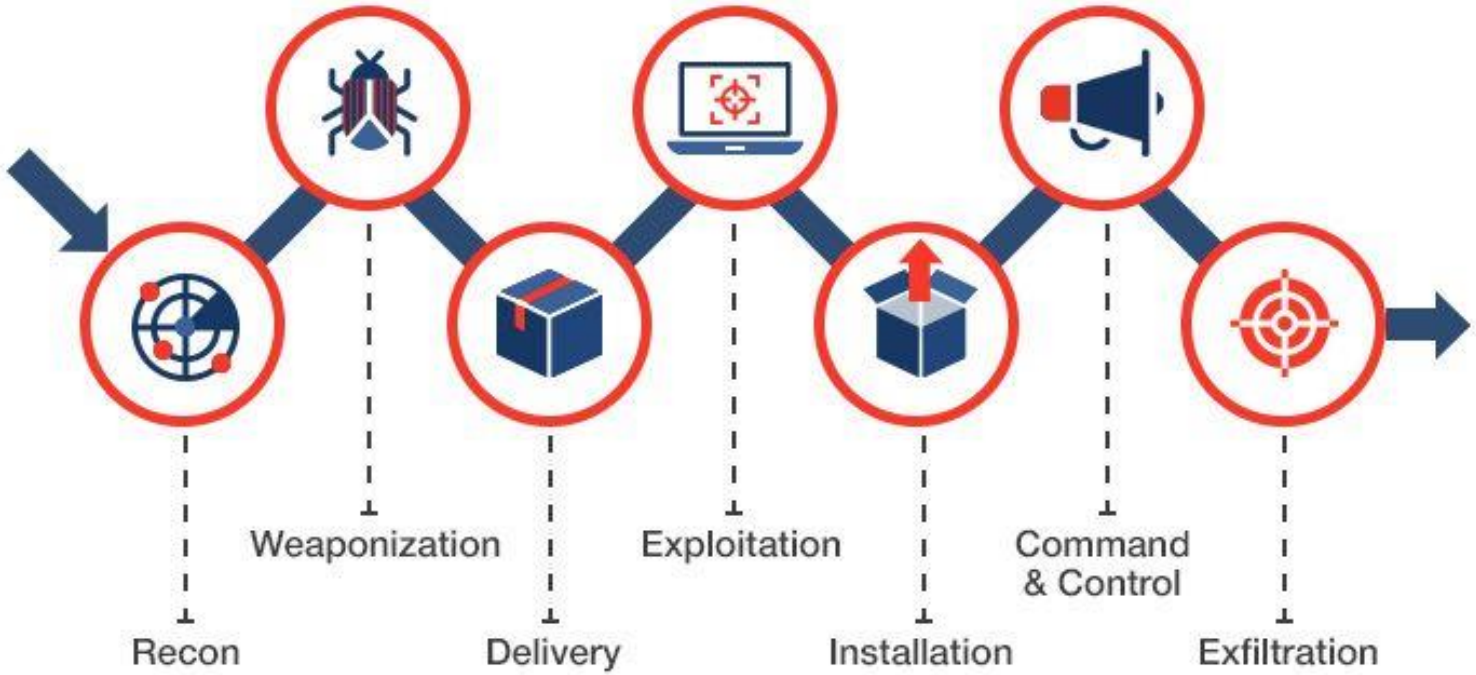
РЕТРОСПЕКТИВНЫЙ ПОИСК ИНДИКАТОРОВ И КОМПРОМЕТАЦИИ IOC



Сценарии использования SDL

cyberART

ПОИСК СЛОЖНОСОСТАВНЫХ АТАК



Сценарии использования SDL

cyberART

Хранилище большого объема структурированных данных

Обогащение существующих систем дополнительными событиями

Система оперативного Google-like поиска по событиям ИБ

Сбор и хранение инвентаризационной и контекстной информации по объектам учета

Профилирование поведения на основе событий

Etc.

Публичные кейсы SDL

cyberART

Anti-Money Laundering

Anti-APT

TIP

Cybersecurity Analyzer

ПРОВЕРЬТЕ СЕБЯ

Внедрены ли у вас базовые средства обеспечения ИБ

Важно ли для вас время реакции на неизвестные угрозы

Большое количество источников и огромный поток логов ежедневно

Беспокоит ли вас стоимость хранения событий информационной безопасности

Вам приходится принимать решения о необходимости удаления данных за предыдущие периоды или принимать это факт

Задаются ли вопросы на которые ИБ не может ответить сейчас и сможет, при наличии инструмента хранения и анализа большого объема данных

Есть ли необходимость в дополнительном контуре контроля

Варианты решений SDL (open source)

cyberART

ELK – ElasticSearch, LogStash, Kibana [open source]

- Распространенное решение по хранению и поиску данных в структурированном текстовом виде
- Хорошие средства визуализации
- Серьезный набор коннекторов и расширений

Cloudera (Hadoop), Parket, Impala [open source]

- Унифицированная платформа для больших данных (CDH), построенная на Apache Hadoop
- Широкое распространение в мире
- Parquet - позволяет хранить данные в колоночном формате, был созданный для Hadoop

CLOUDERA

Parquet

cloudera IMPALA

hadoop

cyberART

Вопросы?

Низамеев Роберт

Robert.Nizameev@icl.kazan.ru