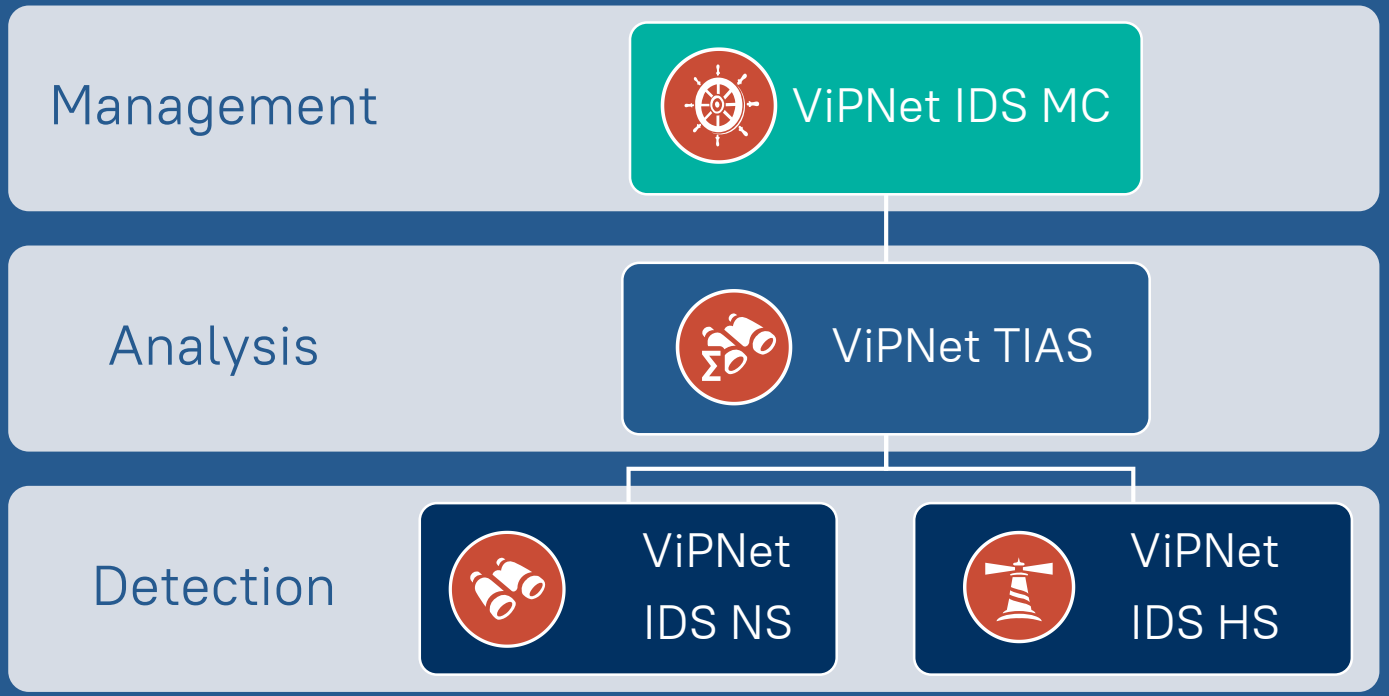
infotecs

Демонстрация возможностей решения TDR в условиях проведения сетевой атаки

Светлана Старовойт

О чем этот вебинар?

Состав решения TDR



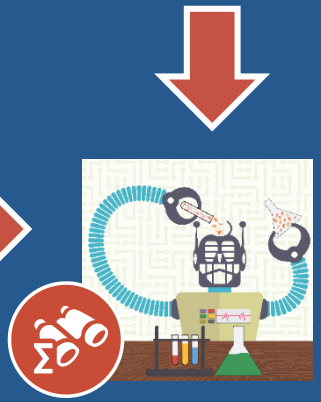
Как это работает?

infotecs

TI Feeds

Сенсоры IDS

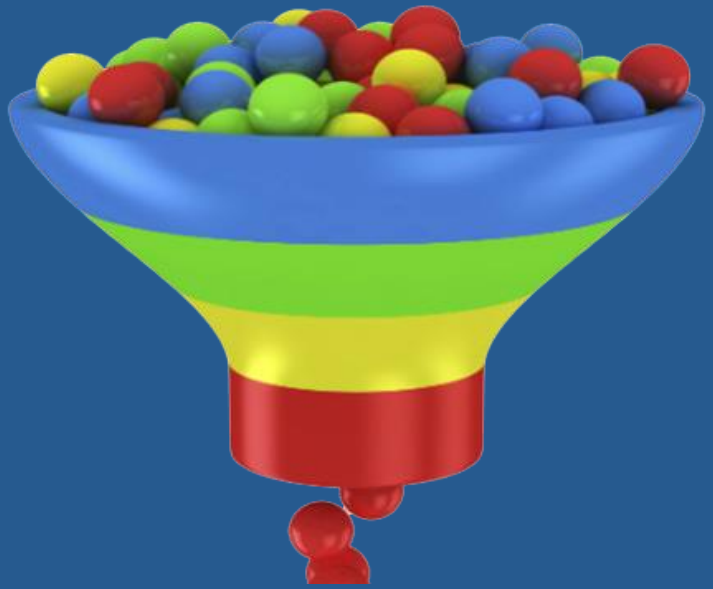
События ИБ



Модуль анализа
ViPNet TIAS

Инциденты
ИБ

Статистика работы центра мониторинга

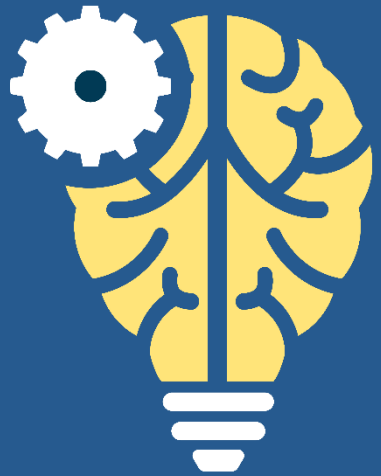


112 млн исходных событий

434 подтвержденных инцидента

Отличительные особенности

Machine Learning

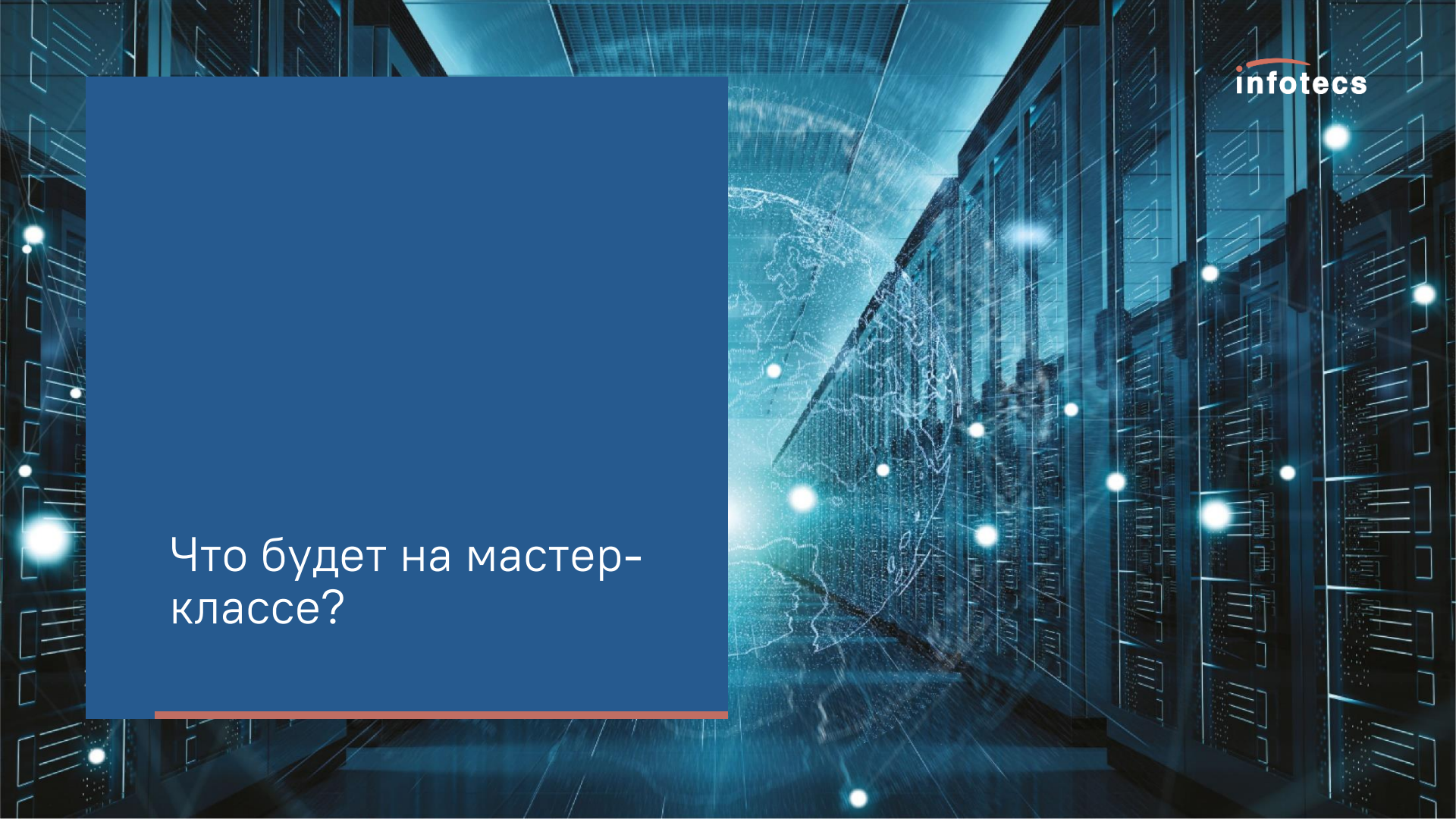


- математическая модель принятия решений;
- алгоритмы машинного обучения;
- ежемесячное переобучение;
- выявление атак нулевого дня.

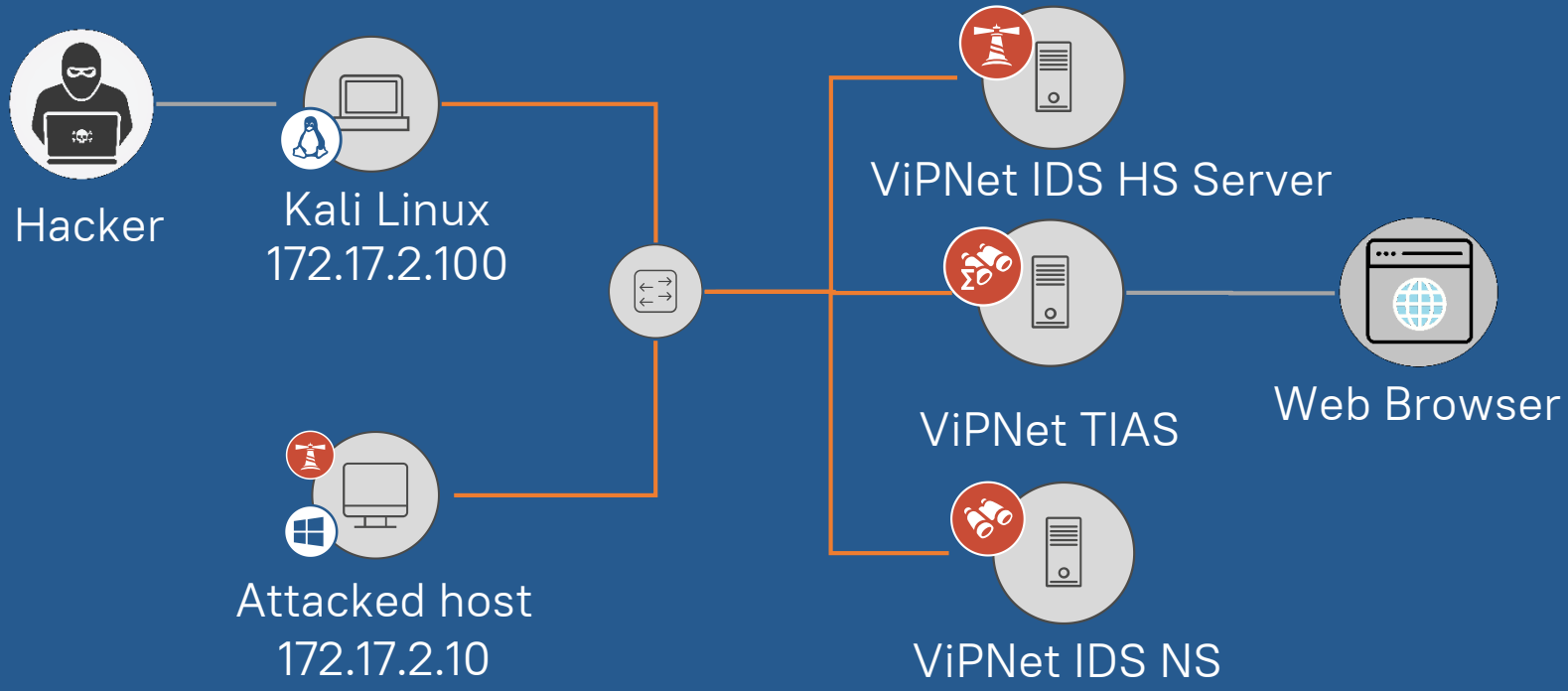
Threat Intelligence

infotecs

- индикаторы атак и компрометации;
- ТТП - тактики, техники, процедуры;
- информационный обмен:
  - СОПКА,
  - ФСТЭК,
  - RU-CERT;
- опыт клиентов - верифицированная и обезличенная информация.


infotecs
Что будет на мастер-классе?

Описание стенда



Предусловия

- В атакуемой сети развернуты продукты решения TDR;
- Атакуемый узел имеет белый IP-адрес;
- На атакуемом узле установлен агент IDS HS;
- На компьютере хакера установлен Kali Linux со специализированными утилитами.

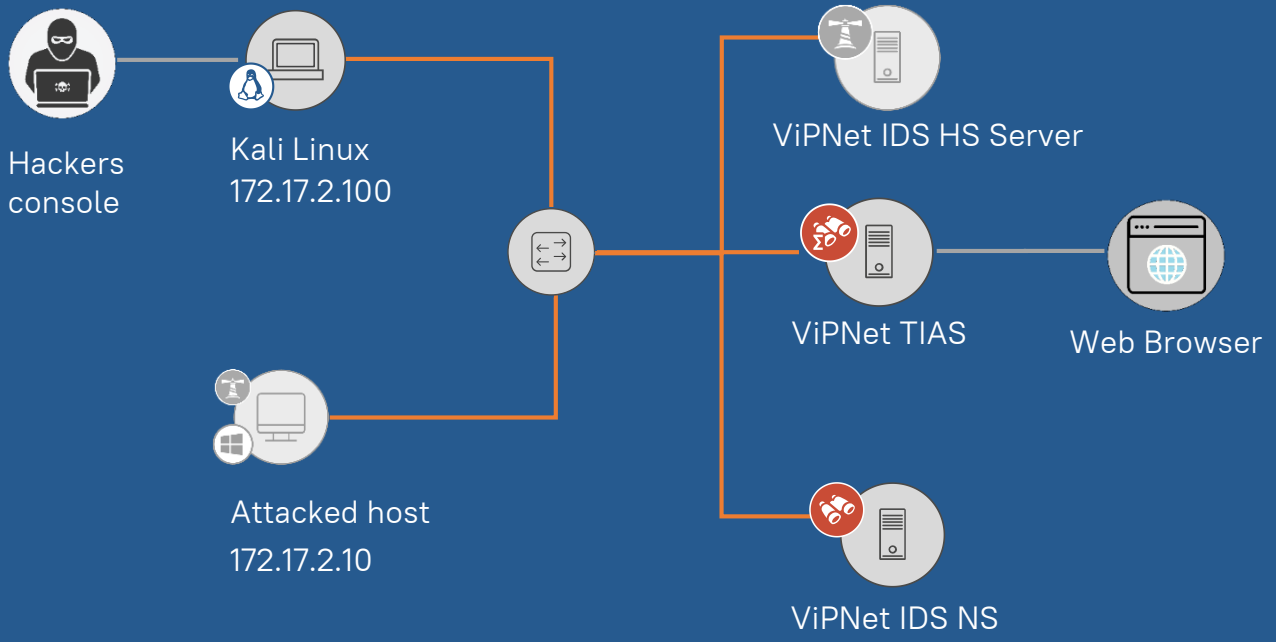
Cyber Kill Chain

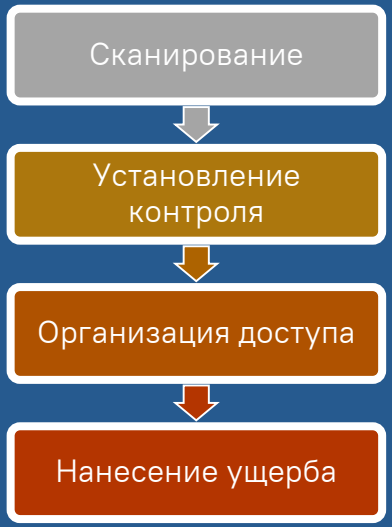
infotecs

infotecs

Мастер-класс

Описание стенда и этапы сценария





Ответы на вопросы!

Контакты

Светлана Старовойт

Старший менеджер
отдела развития продуктов

E-mail:
starovoytsg@infotecs.ru

infotecs

Спасибо
за внимание!