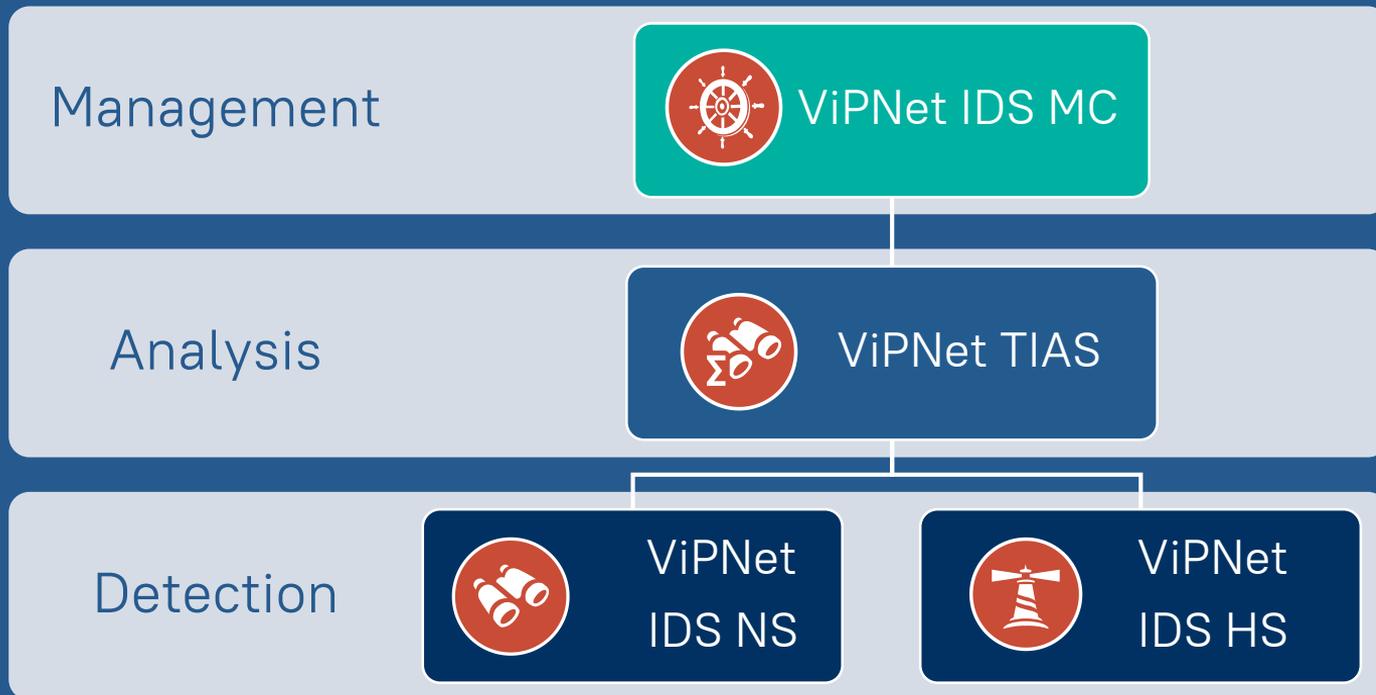


Демонстрация возможностей решения TDR в условиях проведения сетевой атаки

Светлана Старовойт

Состав решения TDR



Как это работает?



Статистика работы центра мониторинга



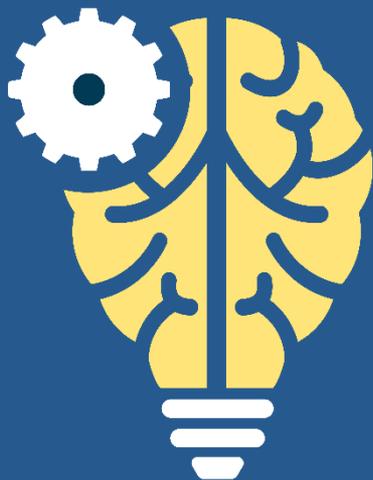
112 млн исходных событий

434 подтвержденных инцидента

The background of the slide is a futuristic data center. It features rows of server racks on the right side, illuminated with blue light. The floor is highly reflective, mirroring the lights and the racks. In the center, there is a glowing, abstract digital structure that looks like a network or a data flow visualization. The overall color palette is dominated by dark blues and teals, with bright white and light blue highlights from the lights and reflections.

Отличительные особенности

Machine Learning



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

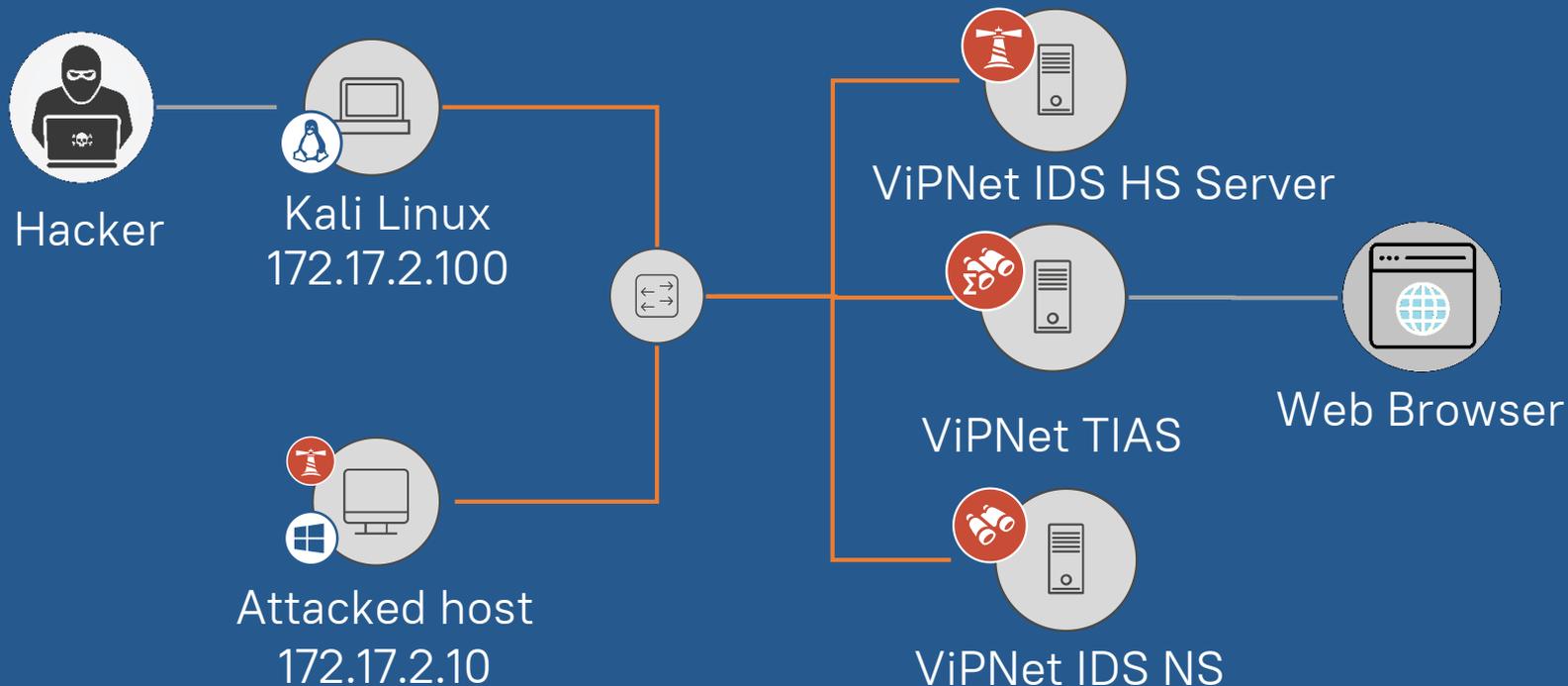
Threat Intelligence



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

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.

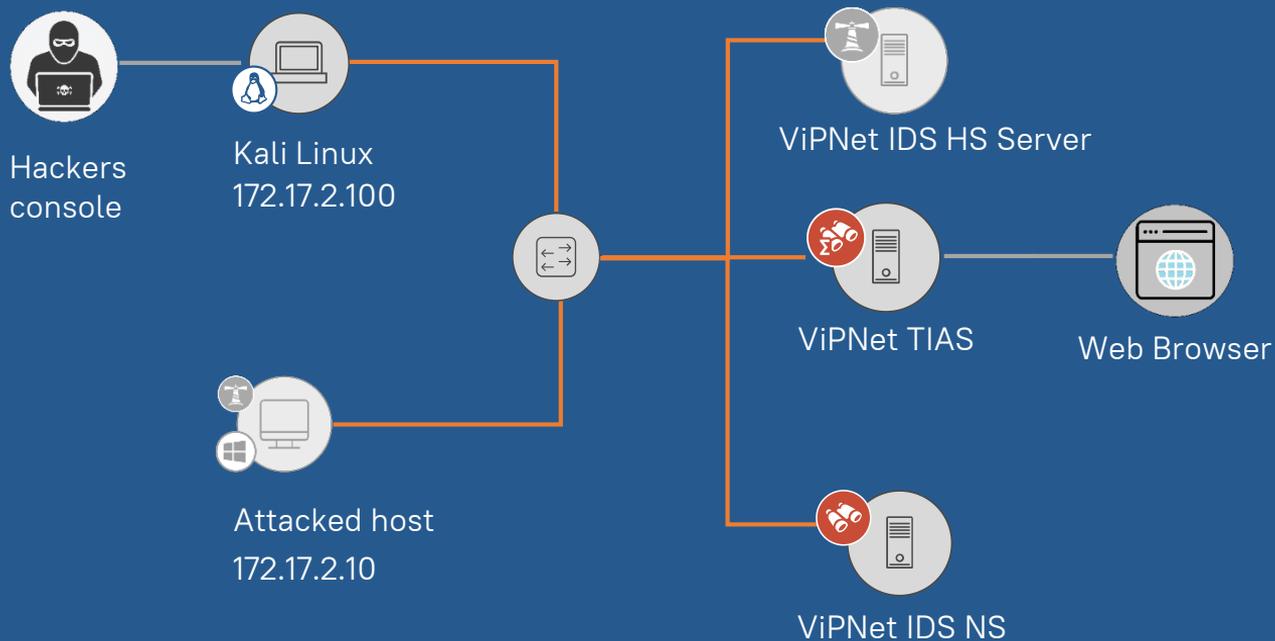
Cyber Kill Chain





Мастер-класс

Описание стенда и этапы сценария



Ответы на вопросы!

Контакты

Светлана Старовойт

Старший менеджер
отдела развития продуктов

E-mail:
starovoytsg@infotecs.ru

The logo for 'infotecs' features a small orange dot above the letter 'i', followed by a curved orange line that arches over the letters 'f' and 'o'. The word 'infotecs' is written in a bold, white, lowercase sans-serif font.

infotecs

A vertical orange line that acts as a separator between the logo and the text.

Спасибо
за внимание!