AGENDA

1	СРАВНЕНИЕ СОВ — КАК ВЫБРАТЬ СРЕДСТВО ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ПРОМЫШЛЕННУЮ СЕТЬ	**Виталий Сиянов** / руководитель направления защиты АСУ ТП ЦИБ, «Инфосистемы Джет»
2	ЛАНДШАФТ УГРОЗ ДЛЯ СИСТЕМ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ	**Алексей Петухов** / руководитель направления защиты промышленных систем, «Лаборатория Касперского»
3	ПРОМЫШЛЕННАЯ КИБЕРБЕЗОПАСНОСТЬ В РОССИИ И МИРЕ: ПОДХОДЫ, ВЫЗОВЫ, ОСОБЕННОСТИ. КИБЕРБЕЗОПАСНОСТЬ АСУ ТП	**Ян Сухих** / руководитель направления ИБ, Schneider Electric
4	КИБЕРБЕЗОПАСНОСТЬ АСУ ТП. УПРАВЛЯТЬ НЕЛЬЗЯ ИГНОРИРОВАТЬ	**Дмитрий Даренский** / руководитель группы систем защиты промышленных сетей, Positive Technologies
5	АСУ ТП: BEFORE THE WAR. ПРЕЗЕНТАЦИЯ КИБЕРУЧЕНИЙ — АТАКИ ТЕХНОЛОГИЧЕСКИХ СЕГМЕНТОВ	**Лука Сафонов** / руководитель лаборатории практического анализа защищенности ЦИБ, «Инфосистемы Джет»

10 YEARS JETSECURITY CONFERENCE 2019

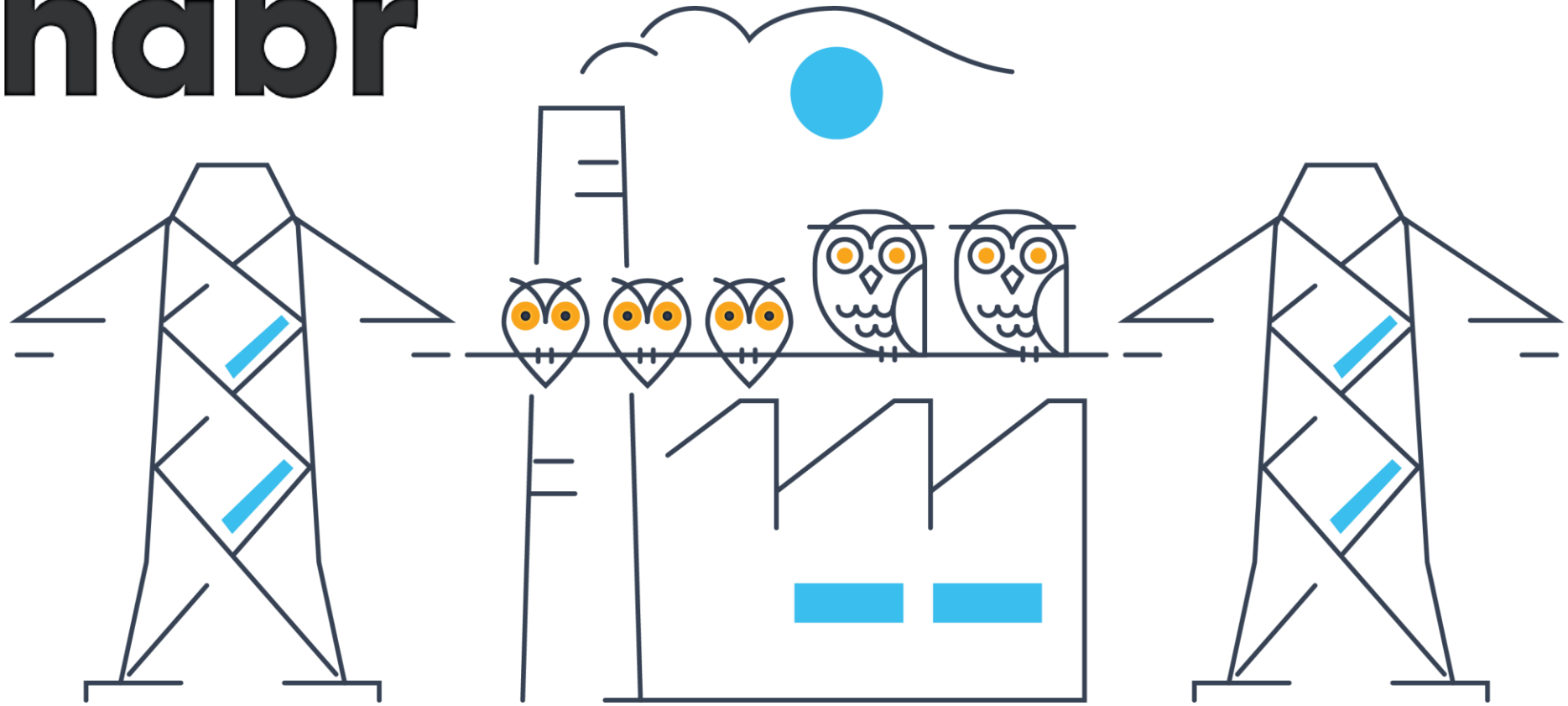
СРАВНЕНИЕ СОВ — КАК ВЫБРАТЬ СРЕДСТВО ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ПРОМЫШЛЕННУЮ СЕТЬ

Виталий Сиянов

Руководитель направления защиты АСУ ТП
va.siyanov@jet.su 8 926 629-13-23

СРАВНЕНИЕ СОВ

habr



ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Мониторинг технологической сети с возможностью поддержки технологических протоколов основных производителей АСУ ТП
- Автоматическое определение типа устройства (АРМ, сервер, ПЛК)
- Возможность контроля технологического процесса
- Обнаружение вторжений в технологическую сеть
- Передача зарегистрированных событий в сторонние системы мониторинга (SIEM) с возможностью их анализа
- Графическое построение карты технологической сети
- Создание и выгрузка отчетов
- Помощь в расследовании инцидентов

КРИТЕРИИ СРАВНЕНИЯ

Функциональные

Стоимостные

Нормативные

Сервисные

Общесистемные

KICS FOR NETWORKS

ПЛЮСЫ

- Возможность добавления индивидуальных событий мониторинга сети через консоль управления
- Возможность импорта тегов из CSV-файла, а также формирования списка тегов на основе распознавания трафика (для некоторых протоколов)
- Весь функционал доступен в одной лицензии
- Весь функционал в одном решении

МИНУСЫ

- Конфигурирование производится только через консоль управления, установленную на сервере. Через веб-интерфейс производится только **#мониторинг**
- Отчет о событиях формируется только через Kaspersky Security Center
- Отсутствие возможности индивидуальной настройки карты сети
- Закрытый прайс лист

ISIM

POSITIVE TECHNOLOGIES

ПЛЮСЫ

- Простота установки, настройки и дальнейшей эксплуатации
- Простой и понятный веб-интерфейс
- Мониторинг и управление сосредоточены в одном месте
- Графическое представление узлов сети с возможностью группировки
- Возможность хранения и экспорта сетевого трафика
- Создание отчётов и выгрузка в формате PDF

МИНУСЫ

- Создание индивидуальных правил для контроля сети только через вендора
- Полный функционал доступен только в PRO версии
- Закрытый прайс-лист

ЧТО ВЫБРАТЬ

KASPERSKY lab

POSITIVE TECHNOLOGIES

ЧТО ДЕЛАТЬ

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Виталий Сиянов

Руководитель направления защиты АСУ ТП
va.siyanov@jet.su
8 926 629-13-23