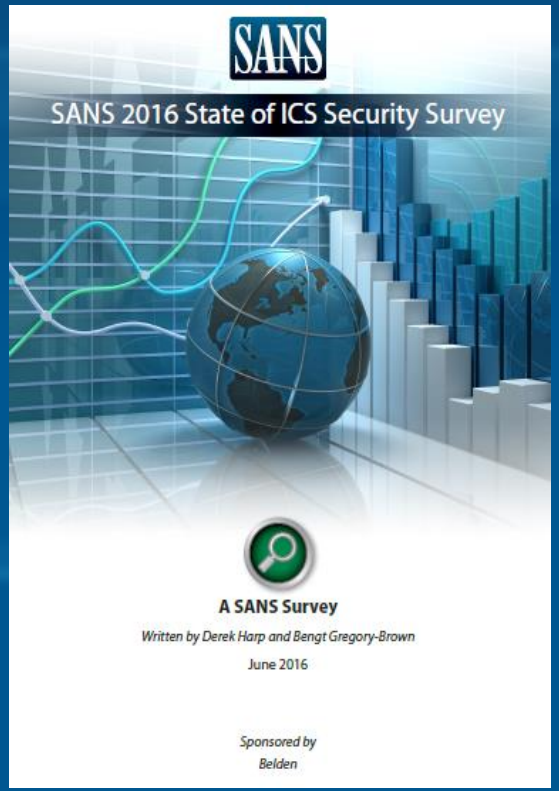
КОЛЛАБОРАЦИЯ ADVANTECH И KASPERSKY LAB НА ПУТИ К БЕЗОПАСНОЙ ПРОМЫШЛЕННОЙ ИТ-ИНФРАСТРУКТУРЕ

Дмитрий Швецов
ProSoft

SANS 2016 Состояние и исследование безопасности ICS



Ключевые результаты

Воспринимают уровень угрозы как серьезный или высокий для систем управления по сравнению с 43% в 2016 г

Возлагают ответственность за информацию об угрозах персоналу и 43% берут на себя ответственность за безопасность персонала

Рассматривают свои цепочки поставок или партнеров как главный источник угрозы

– Top Attack concern– External/Outsiders
– Top Target concern– коммерческие OS (Windows, Linux)
Ключевые активы: HMI, истории данных, АРМ операторов, АСУ ТП, Системы управления активами (ASM)

Несколько сил несут перемены и риски в промышленность

Увеличение подключений

50 млрд. подключенных устройств к 2020

- Gartner

Возрастающие регулирование

Глобальные нормативные изменения – главная задача

- Reuters,2015

Сближение IT-OT

- Все большее проникновение IP коммуникаций
- IIoT создает «пористые» границы

Возрастание Cyber Security рисков для ICS/Control Level

Рост событий влияющих на промышленную ИБ и АСУ ТП

- *2016 FireEye/iSight ICS Vulnerabilities Trend report*
- *2016 SANS State of ICS Security Survey Report*

Тенденция уязвимости АСУ ТП

- Раскрытие уязвимостей возрастает для ICS
- 123 вендора имеют ICS уязвимости
- 33% не имеют никаких исправление или публично доступных патчей

FireEye iSight Intelligence 2016

IIoT приносит новые вызовы ИБ

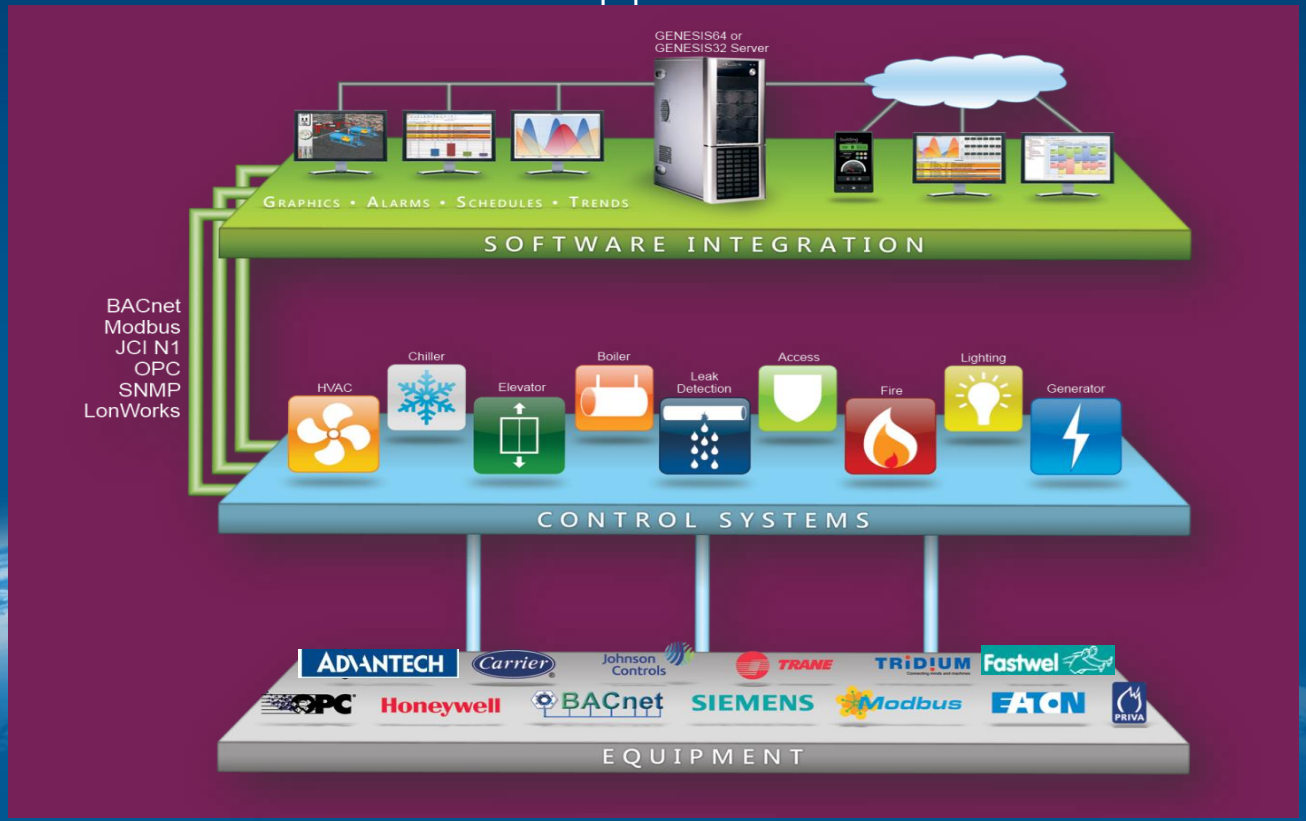
- Промышленная ИБ это не просто
- Большинство “вещей” уже существуют
  - Brownfield, not Greenfield
  - По существу используются небезопасные протоколы
  - Находящиеся там десятилетиями
- Конфигурация, тестирование и техническое обслуживание должны выполняться без отключения сети
- Патчи не практикуются
- Активное сканирование может повредить системы
- Системы должны демонстрировать отказоустойчивость - продолжать работать, даже под атакой или будучи поврежденными

3 ключа к успеху

Портфолио IIT - все уровни конвергентной модели безопасности

- Мониторинг параметров АСУ ТП
- Контроль потребления электроэнергии
- Поддержка протоколов промышленных и ИТ

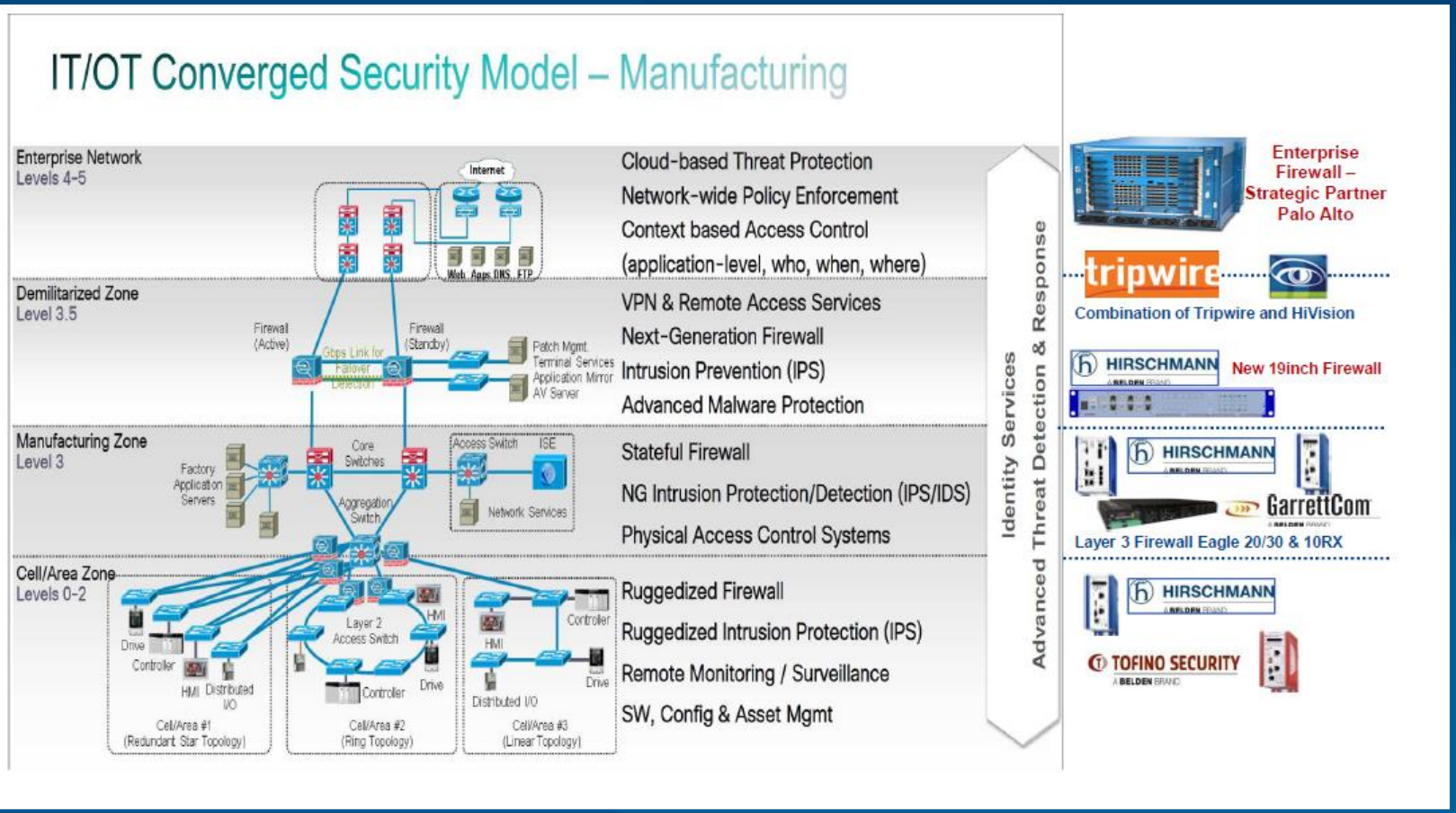
- Универсальное подключение
- Сертификация OPC UA
- Подключение к тысячам типов контроллеров
- Интеграция SNMP
- Мониторинг сетевых устройств



Поддержка гетерогенной промышленной среды

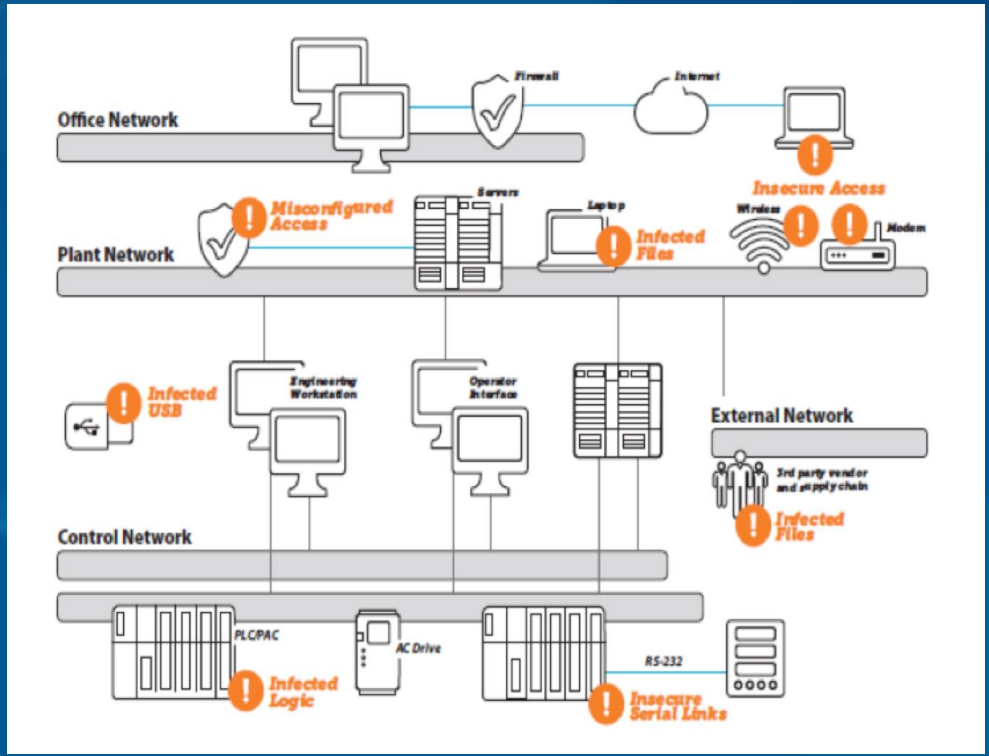
- Независимое от производителя решение
- Решения основанные на стандартах
- Инфраструктура промышленных сетей
- ICS/SCADA
- Опыт в ИБ – ядро компании
  - Мониторинг изменений и обнаружения угроз
  - Уведомления
  - Проверка уязвимости
  - Log Intelligence/SIEM
  - Автоматизация и интеграция

Все уровни конвергентной модели безопасности



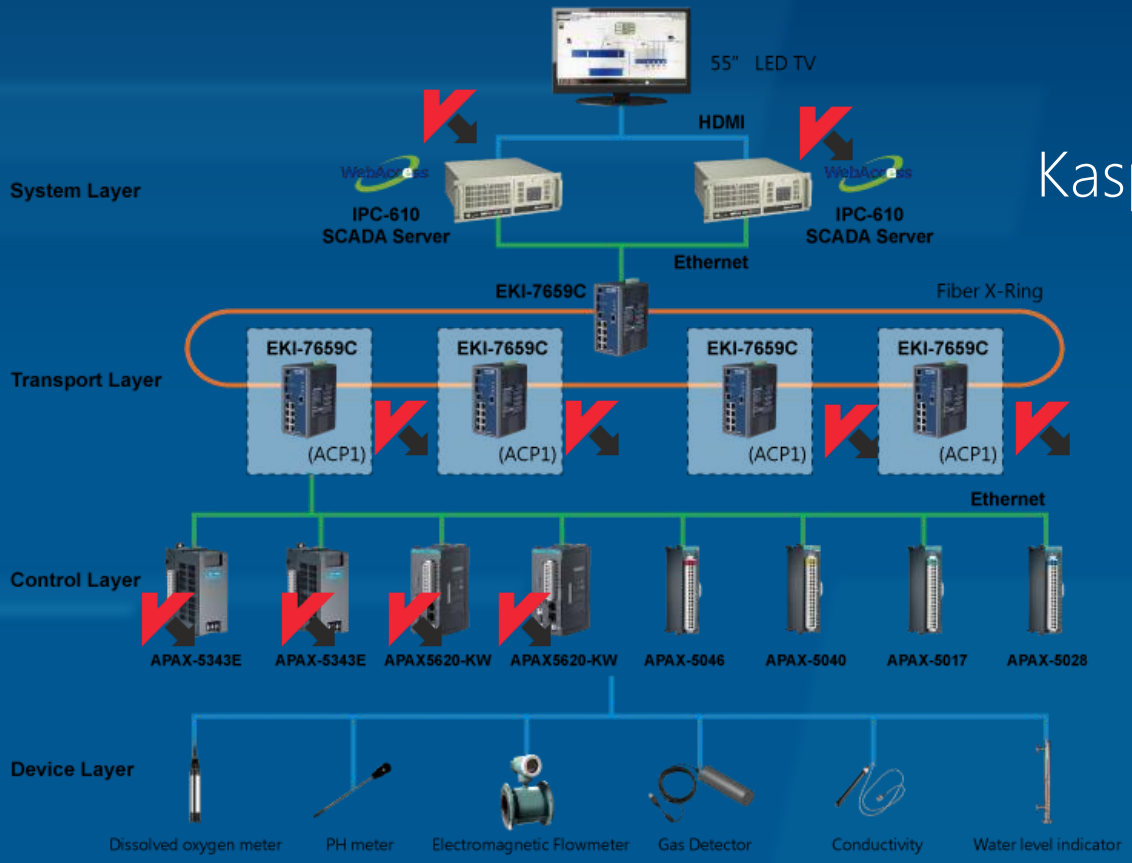
Технологии обнаружения уязвимостей

На что направлены атаки в АСУ ТП



- Конфигурации
  - Некорректные конфигурации
  - Слабые конфигурации
  - Подверженность уязвимостям
- Небезопасный доступ
  - Беспроводной
  - Модемный
  - Небезопасное интернет-окружение
  - Услуги удаленного доступа
- Неавторизованный доступ
- Утечка или кража учетных данных
- Зараженные файлы
- Зараженные USB
- Небезопасные последовательные ссылки
- Сложные среды с несколькими поставщиками

KICS FOR NETWORKS и технологии Advantech



Kaspersky Security Center

KICS for Networks

KICS for Nodes

Спасибо за внимание!