Кибератаки –одна из причин аварий в электроэнергетике?

КАК, НОВАЯ РЕАЛЬНОСТЬ, ОТРАЖАЕТСЯ НА ЭКСПЛУАТАЦИОННОМ ПРОЦЕССЕ

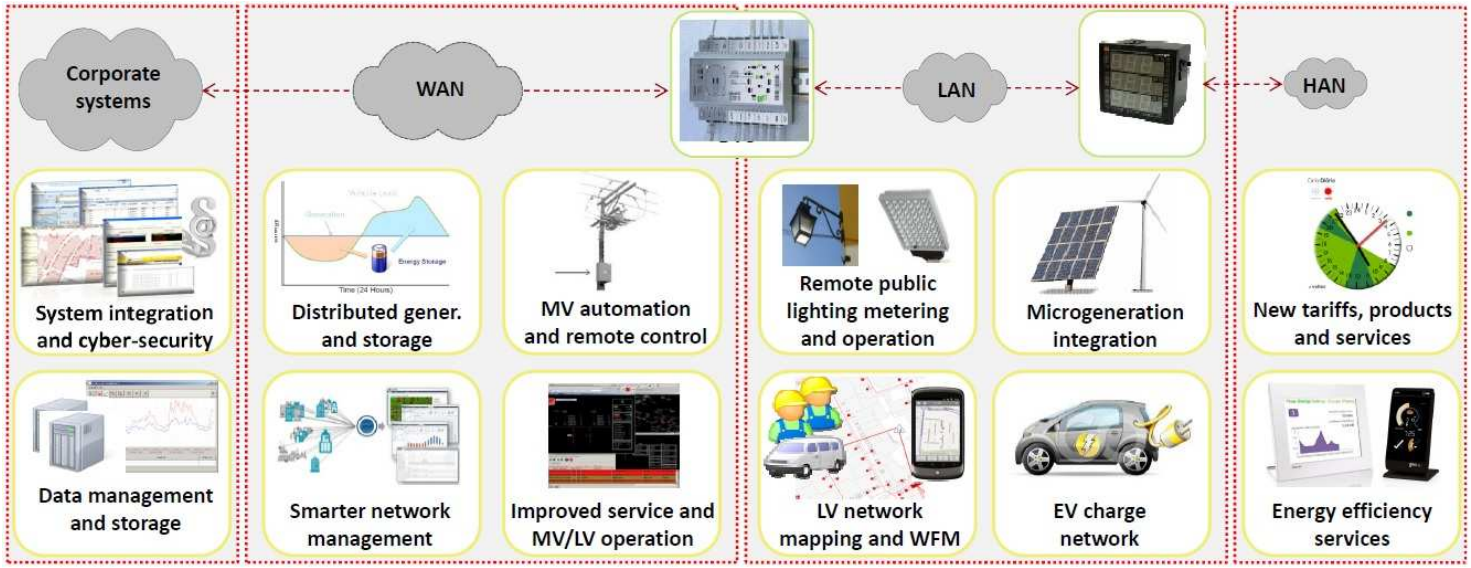
Генгринович Евгений

Советник Генерального Директора

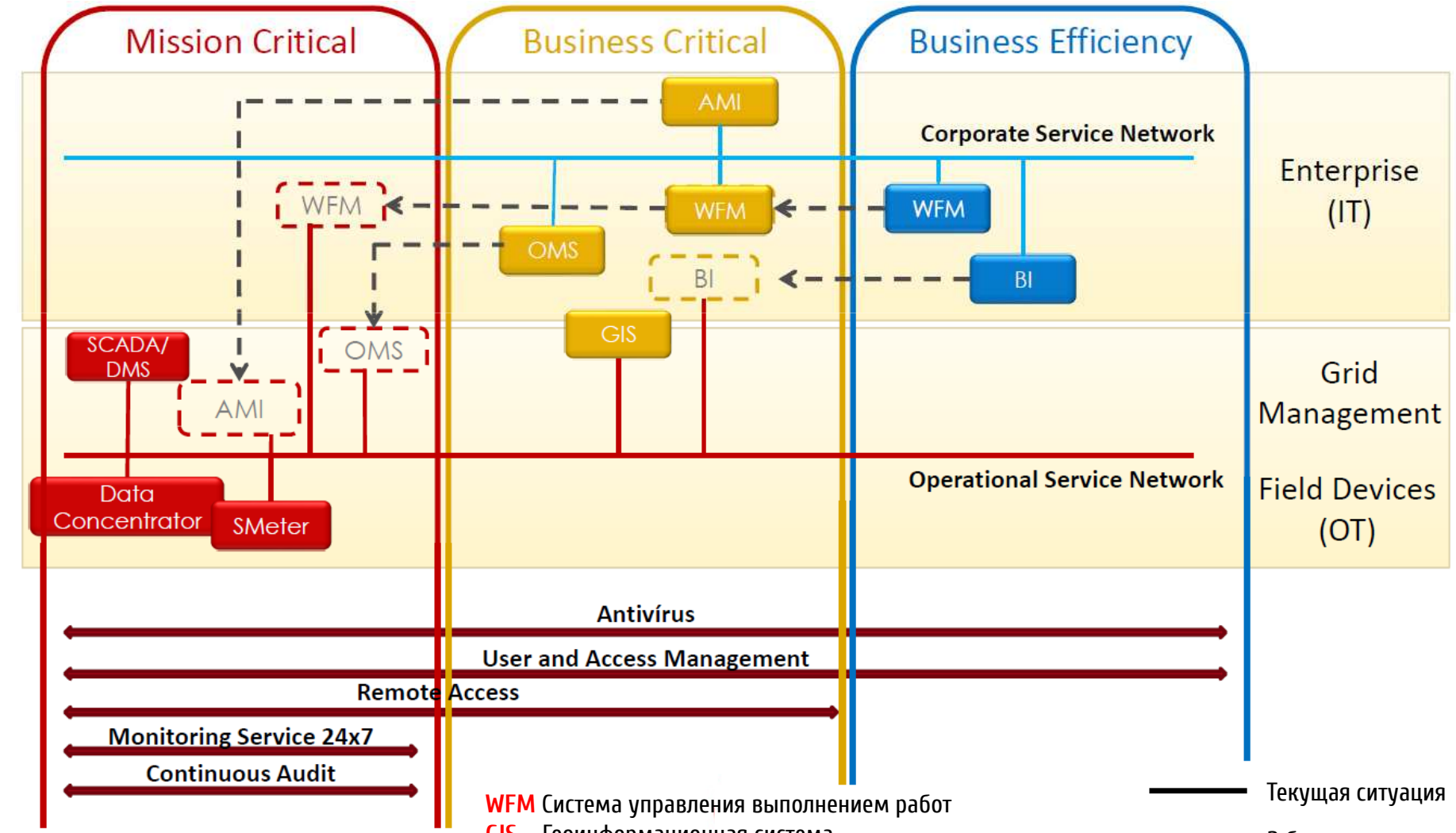
Изменения ландшафта

Классическая структура электрических сетей:

Современная (интегрированная с ИТ):



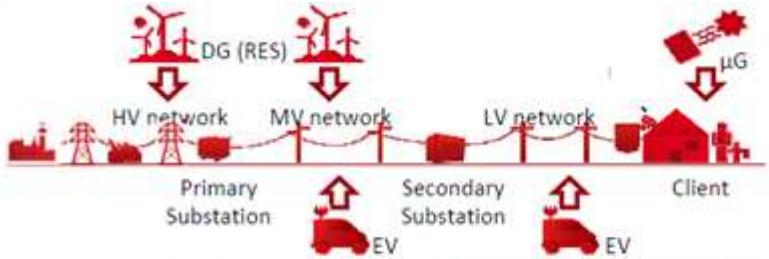
Типы задач и тенденции



OMS - Система управления нагрузкой

WFM Система управления выполнением работ
GIS Геоинформационная система
BI Бизнес показатели

Уровень потенциальных возможностей воздействия растет



От ... **... к новой Бизнес и ИТ стратегии**

Воздействие	• Непосредственно на промобъектах (подстанциях)	Новые вектора атак Угрозы везде
Коммуникации	• Нестандартные протоколы, изолированные сети	Стандартные протоколы. Интеграция с публичными сетями
Системы	• Нестандартное ПО и железо • Физический доступ	Стандартные ПО и железо Удаленный доступ
Специалисты	• Работники компании	Аутсорсинг

Technology

Угрозы

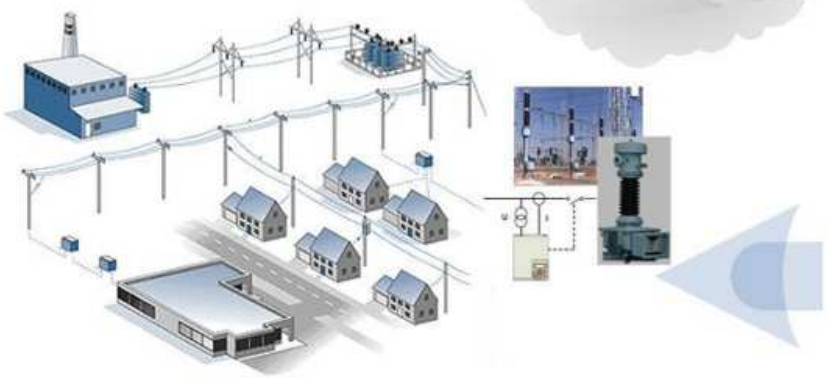
Security Through Obscurity | Security Perimeter | Defense in Depth

Термин «кибербезопасность»

- Защита информации и телекоммуникационных сетей, используемых в целях управления технологическими процессами, от неправомерного доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных, действий
- Неотъемлемая часть технологического процесса, основная цель, которой, обеспечить его непрерывность (доступность всех узлов) и целостность (в т.ч. и передаваемой между узлами РЗА/АСУ ТП информации)
- Способность системы управления успешно выполнять предусмотренные задачи в условиях кибератак, направленных на нанесение ущерба критически важным объектам, имуществу физических или юридических лиц, экономике, окружающей среде

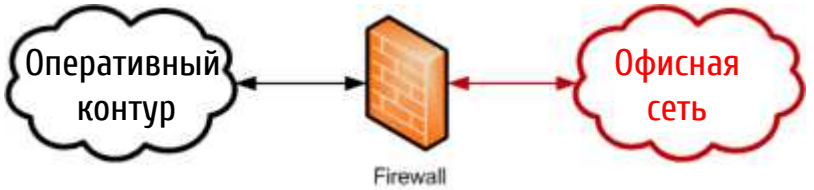
Защита периметра

Варианты обеспечения

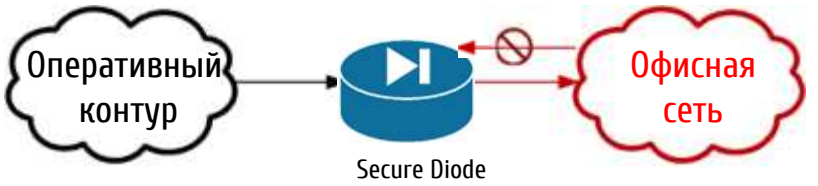


- Физический разрыв

- Интеллектуальный маршрутизатор

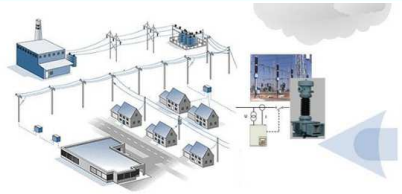


- Одностороннее, на физическом уровне, соединение IP-сетей



Вариант 2

Интеллектуальный маршрутизатор



Логическое разделение сетей

- Блокировка неавторизованного доступа
- Разрешение на авторизованные потоки данных

- **Преимущества:**
  - Проверенная технология
  - Автоматизированное и гибкое решение

- **Недостатки:**
  - Нет гарантии от несанкционированных изменений, ошибок администраторов, хакеров и недобросовестных пользователей

Фаерволы в SCADA сетях (особенности)

- Время и гарантия прохождения сигнала в задачах SCADA, является важным параметром
- Оперативно-диспетчерский персонал отвечает за надежность функционирования объектов и систем, а среда передачи данных, воспринимается как данность, настроенная и сконфигурированная при сдаче SCADA в эксплуатацию
- Изменение конфигураций сети передачи данных не допускается без подачи соответствующих заявок и получения разрешений
- Любые изменения требуют корректировки нормативно-технической документации, с последующим ее согласованием в установленном порядке

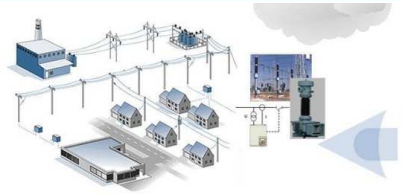
SkyBox – контроль изменений в телеком инфраструктуре SCADA сети

ITD Group

SKYBOX SECURITY

Вариант 3

Диод Данных



Однонаправленное, на физическом уровне, соединение сегментов сетей

- Данные могут быть переданы но не получены или наоборот

- **Преимущества:**
  - Автоматическое и гибкое решение
  - Взлом не возможен
  - Нет возможности онлайн-атак
  - Нет потерь данных
  - 100% защита !

- **Недостатки:**
  - Однонаправленное соединение

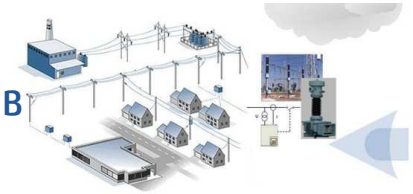
Secure Diode – как это работает?

Критическая инфраструктура

ITD Group

Критическая инфраструктура

Данные получены по любому из доступных (сервер передатчик) протоколов



Протокол ДатаДиода

Протокол ДатаДиода

Данные получены от сервера передатчика и розданы по любому из доступных (сервер приемник) протоколов

Корпоративная сеть

ITD Systems

Поддержка ICS/SCADA протоколов

ITD Group

ITD Systems

Сервер передатчик: МЭК 60870-5-101; МЭК 60870-5-104; OPC; МЭК 60870-5-103; МЭК61850-8-1 (MMS, GOOSE); Modbus (RTU, ASCII; TCP); Российские протоколы

Гранит; ТМ-800А-В; Компас; ТМ-120; ТМ-512; RPT-80; МКТ 1-3; UTM-7; UTK-1; UVTK-EN; VRTF-3; Систел; Уктус; MST (Элкомтех); Космотроника; КТ-96; Telekanal-M (аналог МЭК 870-5-101)

(В разработке: DNP3, ICCP)

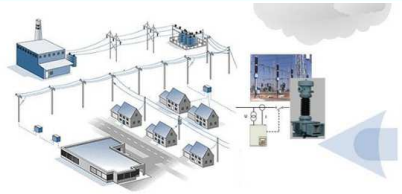
По запросу могут быть разработаны прочие.

Сервер приемник: МЭК 60870-5-101; МЭК 60870-5-104; OPC; Modbus (RTU, ASCII; TCP)

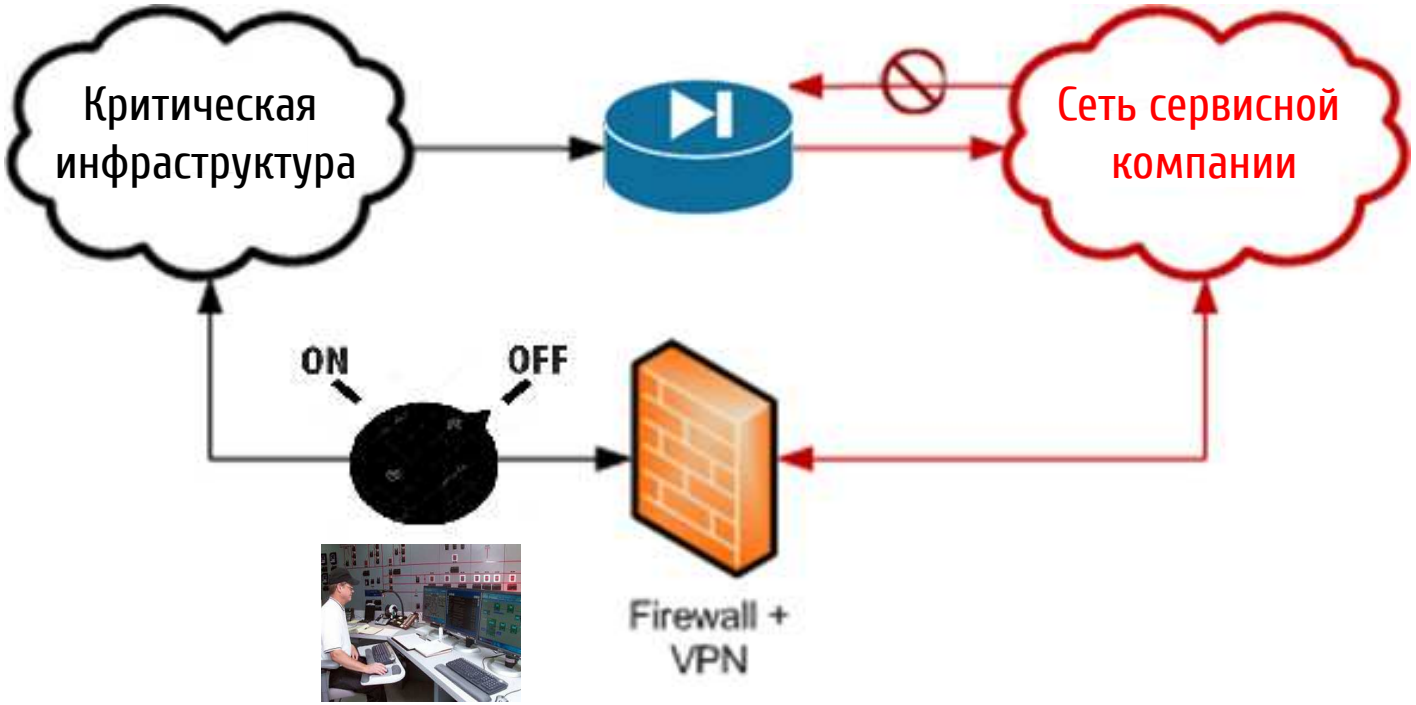
(В разработке: DNP3, ICCP)

По запросу могут быть разработаны прочие.

Решение для вендоров и сервисных компаний



- Снижение стоимости и сроков получения квалифицированной сервисной поддержки
- Предоставление 24/7 наблюдаемости объекта и возможности дистанционного управления (смены конфигурации) по запросу



Secure Diode
Бизнес-задачи (защита периметра)

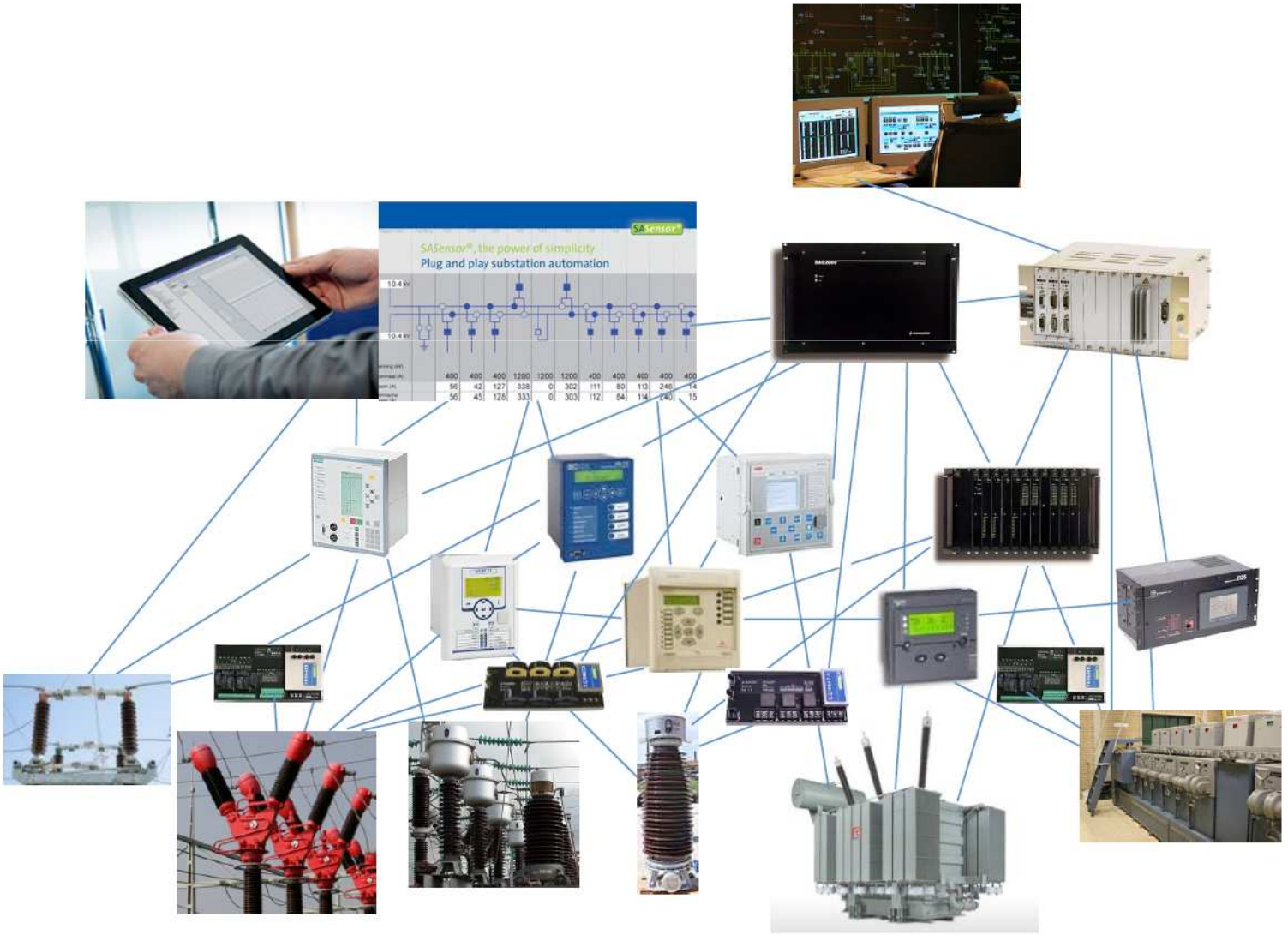
- Технологические данные в реальном времени
- Доступ к данным ICS с мобильных устройств
- Экономия средств на эксплуатации (удаленный доступ для вендоров и сервисных компаний)
- Предоставление технологических данных бизнес-приложениям (SAP, OSISOFT и.т.д)
- Предоставление данных надзорным органам
- Автоматическое обновление антивирусов и ОС в защищенных сегментах сети
- Работа с электронной почтой в защищенной сети (в сочетании с PineAPP Mail Secure)

ITD Systems

Эксплуатация оборудования
появление новых профессий (пример: химики)

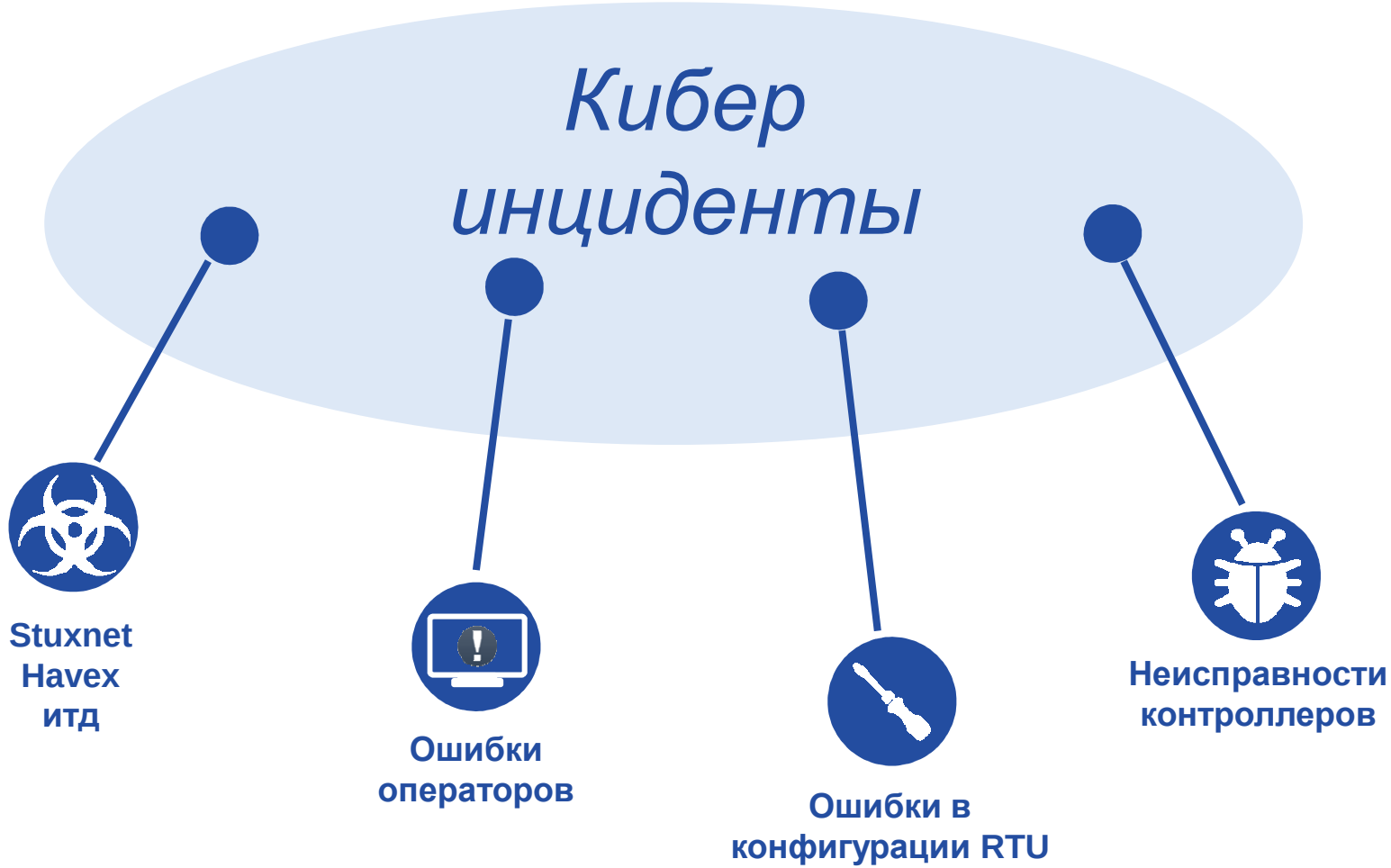
ITD Group

Эксплуатация оборудования
современная подстанция



Контроль состояния – Defence in Depth

Хакеры не основной источник проблем



Общая цель:

Технологическая надежность объекта управления

ITD Group

ОПЕРАТИВНОЕ УПРАВЛЕНИЕ

Процесс идет как положено?

NETWORKING

Что там с оборудованием и информа-ционными потоками?

CYBER SECURITY

Нам угрожает новый Stuxnet?

SilentDefense обеспечивает полную защиту ICS сетей

Архитектура SilentDefence

Пользователи

Инженеры ICS/
Специалисты ИБ

Операторы SOC/
Аналитики

Командный центр

syslog,
CEF,
LEEF

Корпоративные системы, в том числе SIEM

Сеть предприятия

События, логи

События, логи

События, логи

Сенсоры для мониторинга объекта

Объект 1

Сеть ICS/SCADA

Объект 2

Сеть ICS/SCADA

Объект n

Сеть ICS/SCADA

Сетевой трафик в реальном времени, используя SPAN порт на маршрутизаторе или физическое tap устройство. Сетевой трафик офлайн, используя PCAP

Поддерживаемые протоколы и корпоративные приложения

ПРОТОКОЛЫ ICS

- 10+ открытых ICS протоколов, включая:
  - DNP3
  - IEC 104
  - Modbus/TCP
  - EtherNet/IP (включая Rockwell)
  - OPC-DA/AE
  - Profinet
  - BACnet
  - IEC 61850 (MMS, GOOSE, SV)
  - ICCP
  - Synchrophasor
- Проприоритарные протоколы ABB, Emerson, Honeywell, Siemens, Yokogawa
- 20+ IT протоколов, включая SMB/CIFS and DCOM

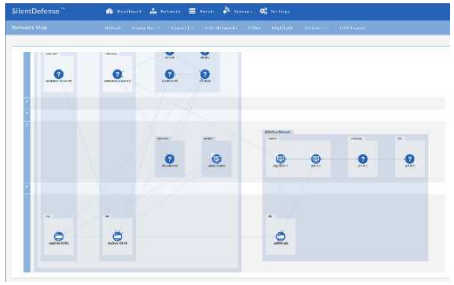
СЕРТИФИЦИРОВАННЫЕ ПРОТОКОЛЫ К КОРПОРАТИВНЫМ ПРИЛОЖЕНИЯМ

- SIM/SIEMs: HP ArcSight (CEF), IBM QRadar (LEEF), Check Point Smart Event, Fortinet FortinAnalyzer, McAfee Nitro, Splunk, Alien Vault
- Авторизация: Active Directory/LDAP
- Syslog

Основной функционал SilentDefence

ITD Group

Инвентаризация оборудования
Автоматически создает перечень устройств и коммуникаций, а также пассивных уязвимостей



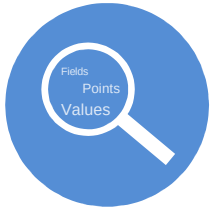
Визуальный анализ
Формирует в реальном времени схему сетевого взаимодействия

Встроенные модули
Определяет сканирование портов, атаки man-in-the-middle и ошибки в пакетах на уровне протоколов

Коммуникационные модели
Автоматически создает «белый список» разрешенных коммуникаций между устройствами, протоколы и типы операций.

Source addresses	Destination addresses	L7 protocols
		(Not set)
$ABB_SERVERS	$ABB_SERVERS	DCOM
$ABB_SERVERS	$ABB_SERVERS	CSLib
$ABB_SERVERS	$ABB_SERVERS	SMB, NetBIOS
$ABB_SERVERS	172.16.4.1	NotAKnownO...
$ABB_SERVERS	172.16.4.1	LDAP

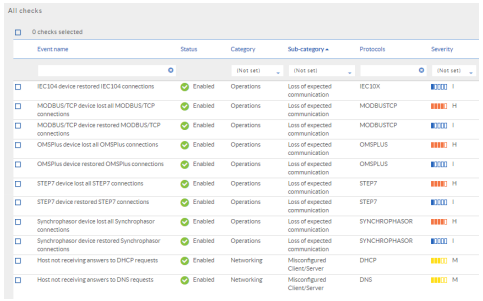
Специальные функции SilentDefence

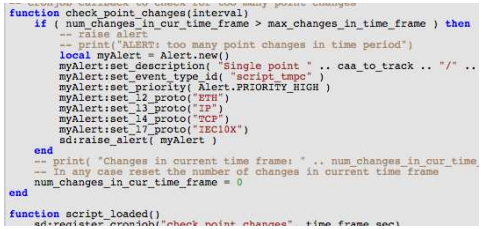


Поведенческий анализ протоколов
Автоматически создает «белый список» разрешенных процессов, параметров и значений

Библиотека сценариев атак на инфраструктуру
Готовые сценарии сетевых, операционных проблем и угроз

Механизм создания скриптов (API)
Позволяет создавать правила любой сложности для проверок в реальном времени



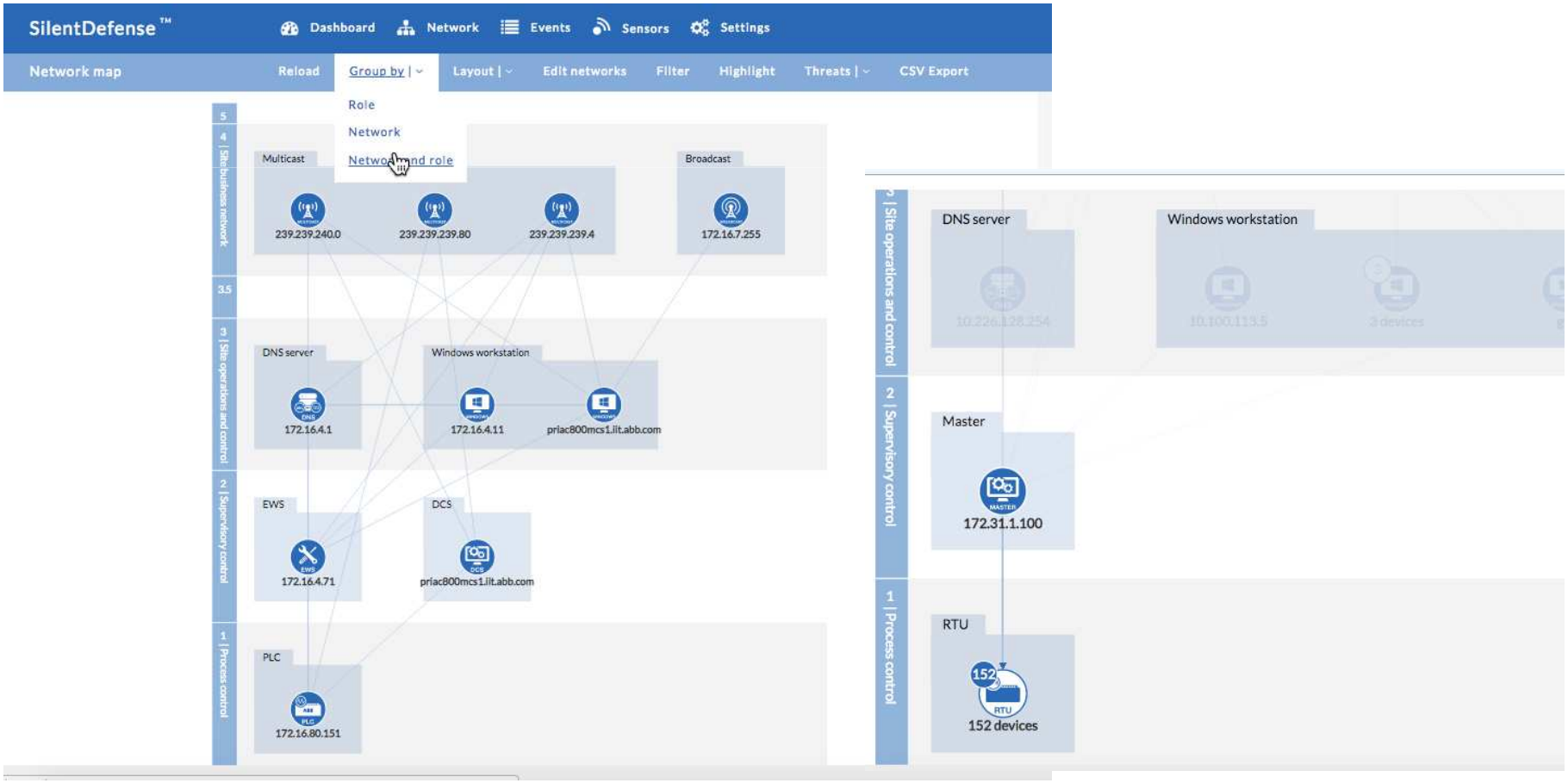


```
function check_point_changes(interval)
    if ( num_changes_in_cur_time_frame > max_changes_in_time_frame ) then
        -- raise alert
        -- print("ALERT: too many point changes in time period")
        local myAlert = Alert.new()
        myAlert:set_description( "Single point " .. caa_to_track .. "/" ..
        myAlert:set_event_type_id( "script_tmpc" )
        myAlert:set_priority( Alert.PRIORITY_HIGH )
        myAlert:set_l2_proto("ETH")
        myAlert:set_l3_proto("IP")
        myAlert:set_l4_proto("TCP")
        myAlert:set_l7_proto("IEC10X")
        sd:raise_alert( myAlert )
    end
    -- print( "Changes in current time frame: " .. num_changes_in_cur_time_
    -- In any case reset the number of changes in current time frame
    num_changes_in_cur_time_frame = 0
end

function script_loaded()
    sd:register_cronjob("check_point_changes", time_frame_sec)
```

Инвентаризация оборудования

- Управление инвентаризацией, заменой оборудования, контроль пассивных угроз



Библиотека сценариев атак на инфраструктуру

- Статические проверки, разработанные на основе аномалий, обнаруженных в процессе эксплуатации на реальных объектах, белый список механизмов обнаружения
- Не требует дополнительной конфигурации

☐	EtherNet/IP device lost all EtherNet/IP connections	Enabled	Operations	Loss of expected communication	ETHIP	H	The device has lost all its active EtherNet/IP connections. This may be due to networking problems (e.g. unstable network links), device malfunction or the device being decommissioned
☐	EtherNet/IP device restored EtherNet/IP connections	Enabled	Operations	Loss of expected communication	ETHIP	I	The device has restored EtherNet/IP communications, after a period of EtherNet/IP communication downtime
☐	Host not receiving answers to DHCP requests	Enabled	Networking	Misconfigured Client/Server	DHCP	M	Possible DHCP misconfiguration: the host is sending DHCP requests, but has not received any timely responses. This may be due to networking problems (i.e., the host cannot reach the DHCP server) or no DHCP server being present in the network
☐	Host not receiving answers to DNS requests	Enabled	Networking	Misconfigured Client/Server	DNS	M	Possible DNS misconfiguration: the host is sending DNS requests, but has not received any timely response. This may be due to networking problems (i.e., the host cannot reach the DNS server), an incorrect list of DNS servers configured on the host, or no DNS server being present in the network
☐	Use of insecure NTP protocol version (NTPv2)	Enabled	Security	Use of insecure protocol (version)	NTP	M	Insecure protocol version: NTP protocol version 2 suffers from security issues and vulnerabilities that have been addressed in later versions of the standard. Consider updating to the latest version of the protocol
☐	Use of insecure SSH protocol version (SSHv1)	Enabled	Security	Use of insecure protocol (version)	SSH	M	Insecure protocol version: SSH protocol version 1 suffers from security issues and vulnerabilities that have been addressed in later versions of the standard. Consider updating to the latest version of the protocol. References: CVE-2011-0949

Примеры выявляемых проблем (реальные проекты)

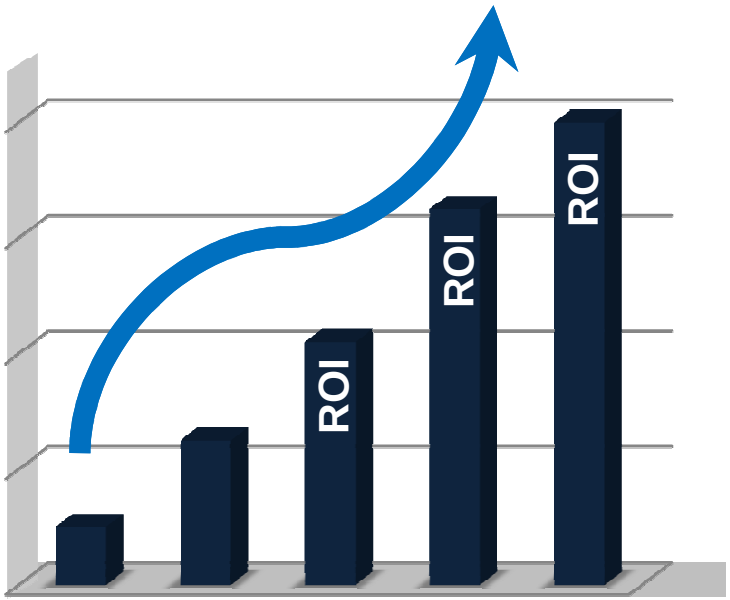
ITD Group

Безопасность	Сеть	Технология
Stuxnet Havex итд	Несанкцио-нированный доступ	Использование незащищенных протоколов
Нарушитель отправляет несанкциони рованные команды	Ошибки в конфигурации Firewall	Проблемы взаимодействия с первичными датчиками
Ошибочные измерения	Нестабиль-ность электросети	Отправка данных в несовмести-мом формате
Неисправные устройства	Погашение подстанции	Несанкциони-рованные переключения

Эффекты для бизнеса

SECURITY MATTERS

- ROI
  - Меньше сбоев
  - Меньше времени простоя
  - Меньше обслуживания
  - Избегаем штрафных санкций
  - Повышаем производительность
  - Выше качество обслуживания
- Непрерывность бизнеса
- Наблюдаемость в реальном времени



Более 40 реализованных проектов

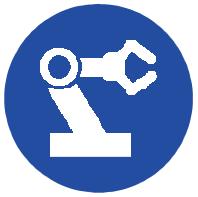
ITD Group

SECURITY MATTERS

Производство, передача и распределение электроэнергии

Передача, хранение и добыча природного газа

Питьевая вода



Производство

Химия и Фармацевтика

Добыча нефти

Технологические партнеры

ITD Group

BAE SYSTEMS

BOEING

Check Point
SOFTWARE TECHNOLOGIES LTD.

ezenta
Sikre rammer om IT

Honeywell

LEONARDO

macnica networks

PHOENIX CONTACT

paloalto networks

…и прочие

eyONet – услуга быстрого и легкого аудита ICS/SCADA сети

- Самая большая опасность для вашего производства, отсутствие информации о текущем уровне защищенности и живучести ICS/SCADA сети
- SecurityMatters разработала сервис **eyONet**, для автоматизации процесса аудита ICS / SCADA, который быстро определит угрозы непрерывности эксплуатационного процесса вашей компании

Три элемента кибербезопасности от ITD Group

КОНТРОЛЬ СОСТОЯНИЯ ОБЪЕКТА УПРАВЛЕНИЯ

SilentDefence	Нидерланды	Покупка, Сервис

АНАЛИЗ ИЗМЕНЕНИЙ В СЕТЕВОМ ОБОРУДОВАНИИ

SkyBox	Израиль	Покупка, Сервис

ОДНОНАПРАВЛЕННАЯ ПЕРЕДАЧА ДАННЫХ

Secure Diode	Россия	Покупка

СПАСИБО ЗА ВНИМАНИЕ!

ITD Group

Контакты: Генгринович Евгений Леонидович

Телефон: +7 (499) 502-1375

Мобильный: +7 (985) 928-8602

www.onewaynetw.ru

egengrinovich@iitdgroup.ru