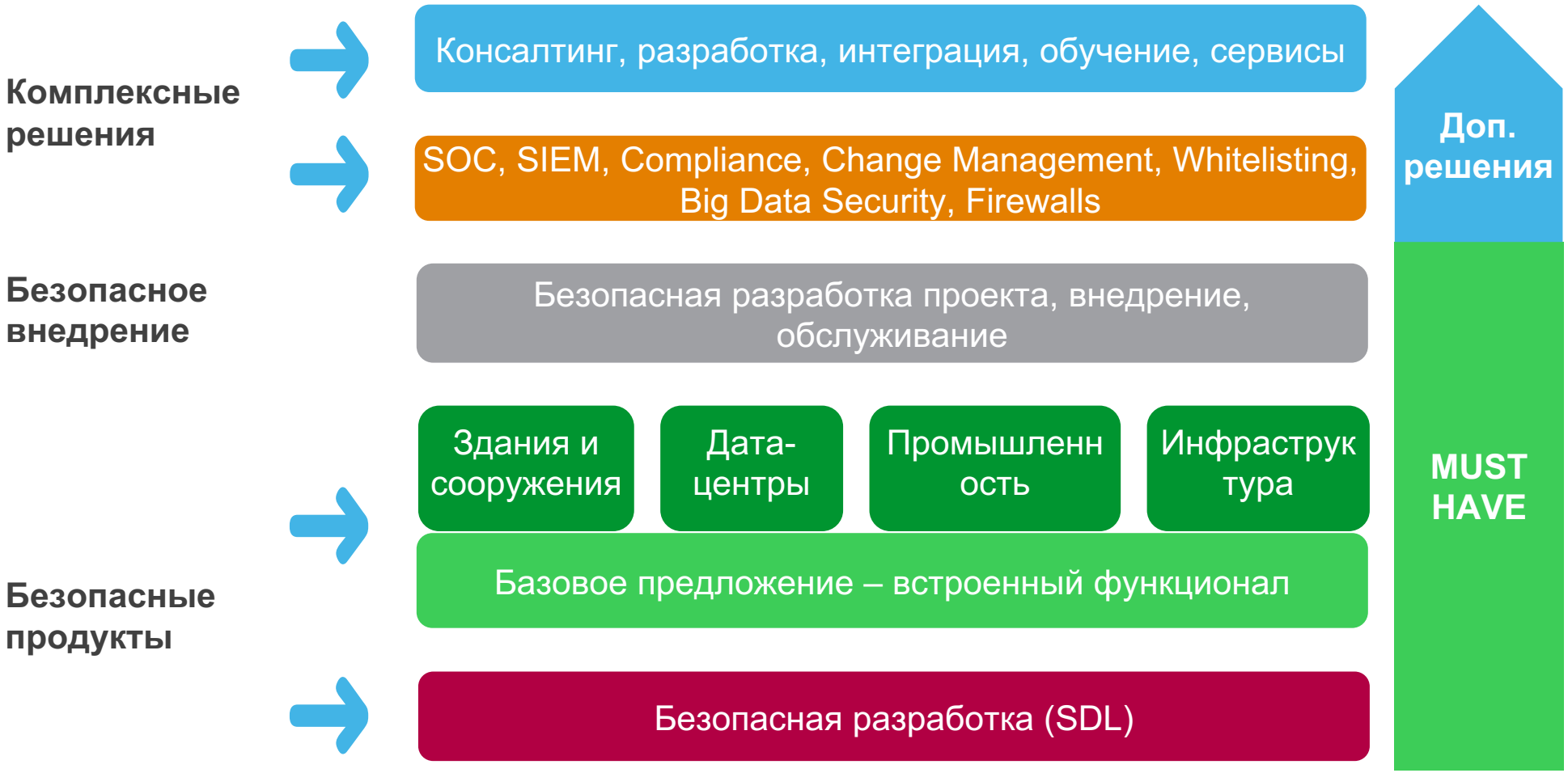
Эволюция систем безопасности АСУ ТП

Взгляд производителя: этапы, проблематика, пути решения

Ян Андреевич Сухих
Руководитель направления ИБ
АО «Шнейдер Электрик»

Этапы создания защищенной АСУ ТП

Этапы создания защищенной АСУ ТП (взгляд вендора)



Life Is On Schneider Electric

Подготовка комплексного решения

Состав комплексного решения по кибербезопасности

Доступ

- Авторизация, аутентификация и аккаунтинг
- Многофакторная аутентификация
- Сегментирование сети
- Безопасный удаленный доступ
- Физическая безопасность

Защита

- Защита конечных узлов (Anti Virus, Anti Malware)
- DLP, HIPS, белые списки
- Управление устройствами
- Доверенная загрузка/управление процессами
- Patch Management

Обнаружение

- Security Information & Event Management (SIEM)
- Системы мониторинга сети
- Обнаружение аномалий
- СОВ/СПВ (NIDS/NIPS)
- SOC (центры управления)

Реагирование

- Резервное копирование и восстановление
- Forensics (расследование киберпреступлений)
- Системы реагирования на инциденты

Проблематика

Проблемы защиты АСУ ТП

Нехватка кадров

Согласно расчетам мировой дефицит кадров в области кб к 2021 году составит 3,5 млн человек

Низкая защищенность предприятий

Промышленные предприятия не успевают за развитием кибер-угроз

Проблематика

Обслуживание

Как найти компромисс между удобством обслуживания и безопасностью

Протекционизм

Как найти компромисс между интересами бизнеса и требованиями регуляторов

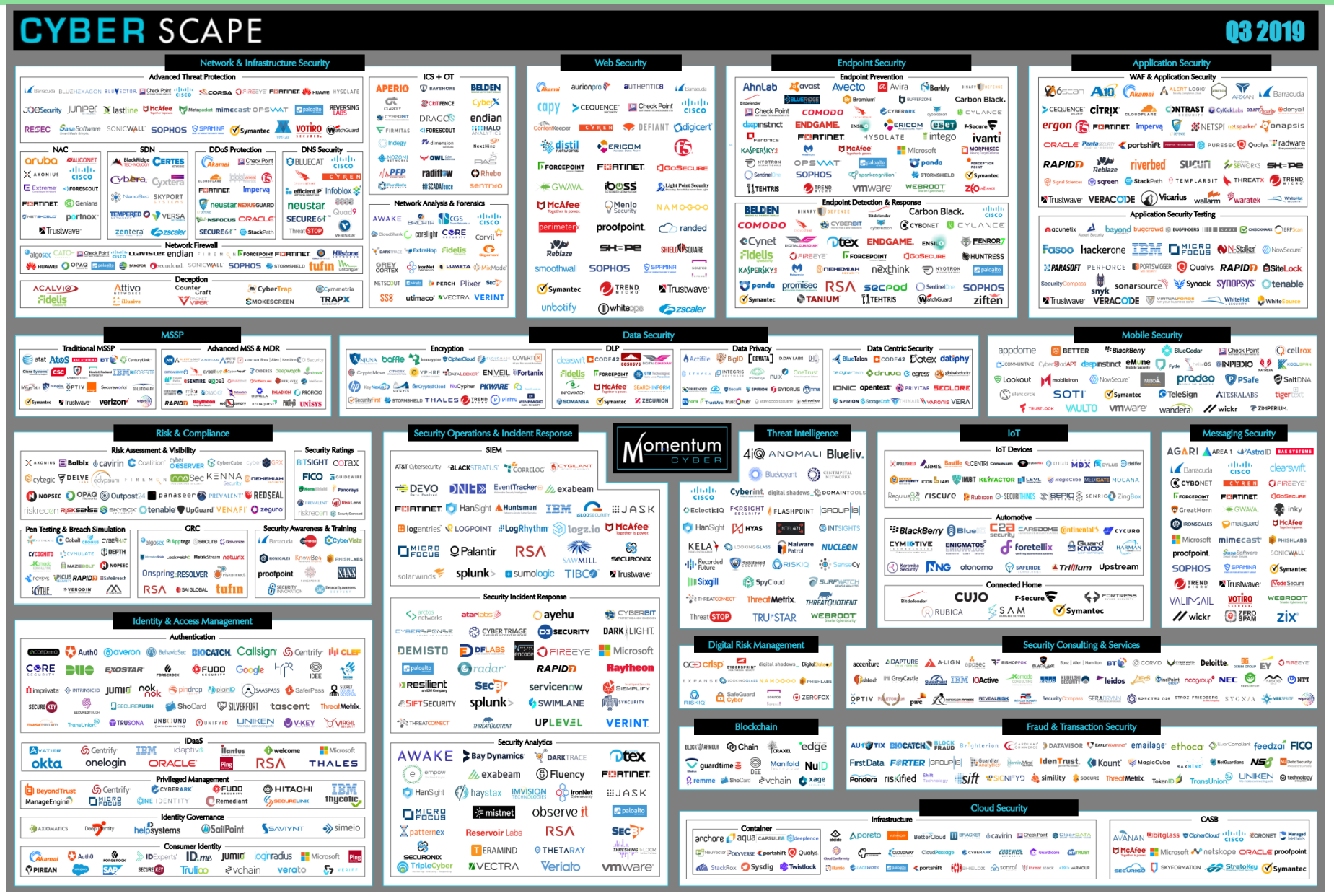
Огромное количество устаревшего оборудования

Жизненный цикл систем АСУ ТП составляет 15-25 лет

Интеграция с КИС

Правильное построение DMZ, настройка МСЭ, какие протоколы использовать

CYBERscape Q3 2019



Life Is On | Schneider Electric

Как мы можем помочь?

Реализация функций «доступ» и «защита»

Доступ

- Авторизация, аутентификация и аккаунтинг
- Многофакторная аутентификация
- Сегментирование сети
- Безопасный удаленный доступ
- Физическая безопасность

Защита

- Защита конечных узлов (Anti Virus, Anti Malware)
- DLP, HIPS, белые списки
- Управление устройствами
- Доверенная загрузка/управление процессами
- Patch Management

Обнаружение

- Security Information & Event Management (SIEM)
- Системы мониторинга сети
- Обнаружение аномалий
- СОВ/СПВ (NIDS/NIPS)
- SOC (центры управления)

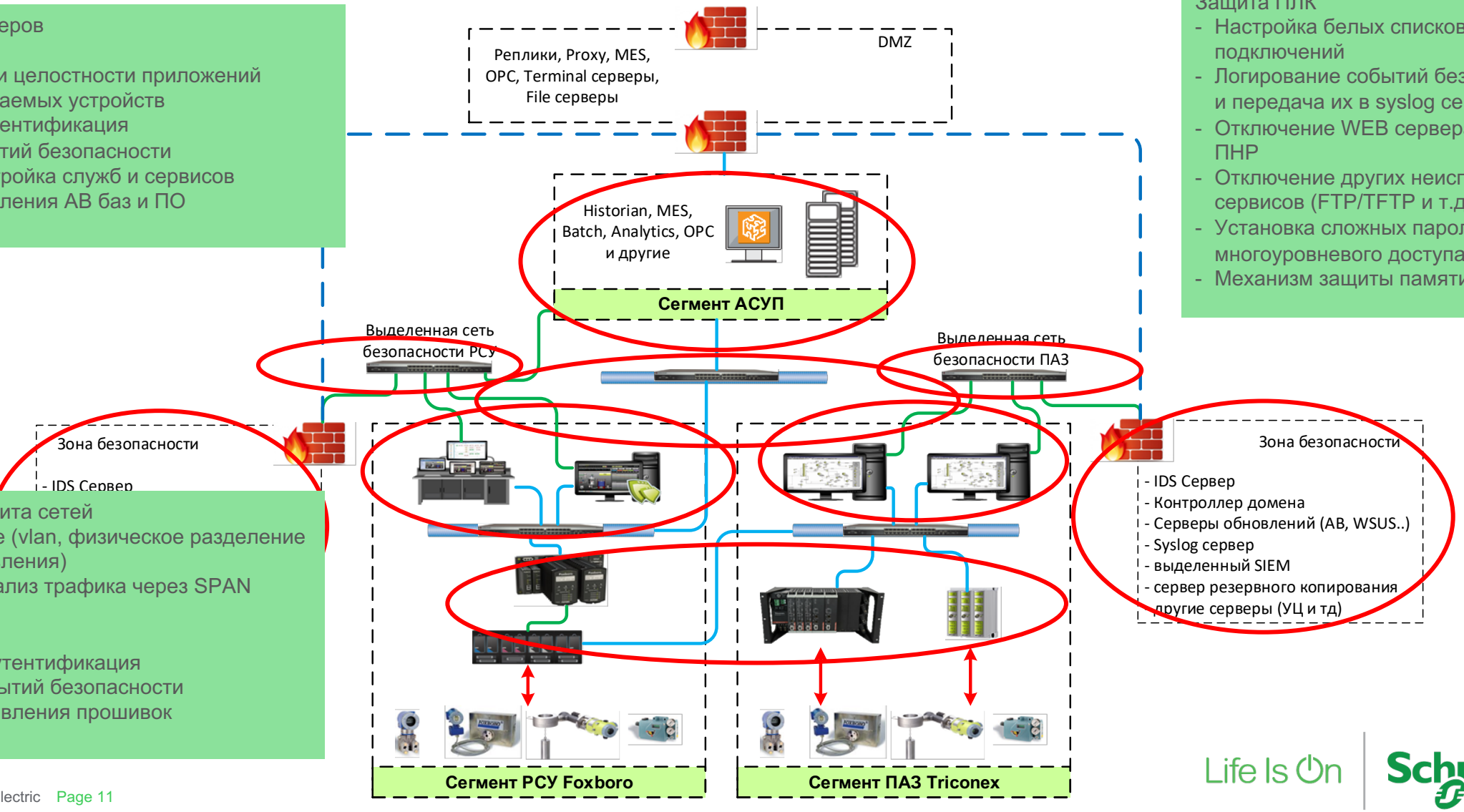
Реагирование

- Резервное копирование и восстановление
- Forensics (расследование киберпреступлений)
- Системы реагирования на инциденты

Базовое предложение (в соответствии с №187-ФЗ и МЭК 642443)

Защита АРМ и Серверов
- Антивирусное ПО
- Контроль запуска и целостности приложений
- Контроль подключаемых устройств
- Авторизация и аутентификация
- Логирование событий безопасности
- Оптимальная настройка служб и сервисов
- Регулярные обновления АВ баз и ПО
- Другие меры

Организация и защита сетей
- Сегментирование (vlan, физическое разделение ПАЗ и сети управления)
- Мониторинг и анализ трафика через SPAN порты (NIDS)
- Харденинг АСО
- Авторизация и аутентификация
- Логирование событий безопасности
- Регулярные обновления прошивок
- Другие меры



Защита ПЛК
- Настройка белых списков подключений
- Логирование событий безопасности и передача их в syslog сервер
- Отключение WEB сервера после ПНР
- Отключение других неиспользуемых сервисов (FTP/TFTP и т.д.)
- Установка сложных паролей и многоуровневого доступа
- Механизм защиты памяти

Реализация функций «доступ» и «защита» на практике

Стендирование и испытаний решений в НИОКР центре в г. Иннополис

1. Развернут испытательный стенд защищенной АСУ ТП. Включая ПЛК Modicon, РСУ Foxboro, ПАЗ Triconex, внедрены различные СрЗИ (АВЗ, СОВ, СПВ, МСЭ, AD, логирование, управление обновлениями и т.д), выполнен hardening ОС, организована DMZ
2. Проводятся пентесты защищенной АСУ ТП. С целью подтверждения надежность данной конкретной архитектуры и подхода к построению защищенных АСУ ТП в целом в НИОКР центре проводятся пентесты.

Нехватка кадров

Низкая защищенность

Интеграция с КИС

Обслуживание

Протекционизм

Устаревшие системы

Аутсорсинг функций мониторинга и реагирования

Доступ

- Авторизация, аутентификация и аккаунтинг
- Многофакторная аутентификация
- Сегментирование сети
- Безопасный удаленный доступ
- Физическая безопасность

Защита

- Защита конечных узлов (Anti Virus, Anti Malware)
- DLP, HIPS, белые списки
- Управление устройствами
- Доверенная загрузка/управление процессами
- Patch Management

Обнаружение

- Security Information & Event Management (SIEM)
- Системы мониторинга сети
- Обнаружение аномалий
- SOC (центры управления)

Реагирование

- Forensics (расследование киберпреступлений)
- Системы реагирования на инциденты

Целесообразность аутсорсинга

«ЗА»

Возможность сосредоточиться на профильной деятельности

- Содержать минимальный штат сотрудников ИБ (только ключевые компетенции, минимальные инвестиции)

Повышение уровня защищенности

- Качественный провайдер SOC обеспечит лучшее качество мониторинга и реагирования
- Сокращение времени реакции на инциденты

Удобство планирования

- Постоянные расходы, с которыми легко работать финансовым службам
- Простота прогнозирования затрат

«ПРОТИВ»

Доступ провайдера SOC к конфиденциальной информации

- Глубина раскрытия информации зависит от уровня интеграции с SOC. Могут применяться «гибридные» модели для снижения рисков
- Риски хранения, обработки информации

Стоимость услуг может показаться завышенной

- Неправильная настройка СрЗИ, агентов
- Сложно оценить стоимость до первого внедрения

Прочие риски (… а что если?)

- Оценка рисков и оценка мер по их компенсации

Реализация функций «обнаружение» и «реагирование» на практике

Тестирование решений в НИОКР центре в г. Иннополис

1. Реализована интеграция АСУ ТП с SOC наших партнеров. Можно в реальном времени посмотреть как работает SOC в случае имитации атаки на АСУ ТП
2. Интеграция с бизнес системами. В ближайшее время планируется интегрировать демо-стенд с решениями по реагированию на инциденты, управлению уязвимостями.

Нехватка кадров

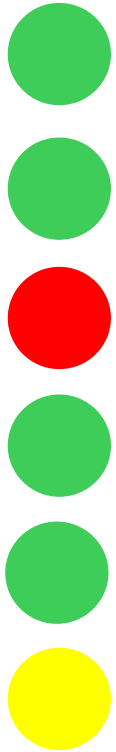
Низкая защищенность

Интеграция с КИС

Обслуживание

Протекционизм

Устаревшие системы




СПАСИБО!

Сухих Ян Андреевич

Руководитель направления ИБ

АО «Шнейдер Электрик»

M: +7 910 475 1750

D: +7 495 777 999 0 ext. 1268

E: yan.sukhikh@se.com