



DataStar

SENSITIVE || MATTERS

КИБЕРБЕЗОПАСНОСТЬ IT/OT - ИНФРАСТРУКТУРЫ

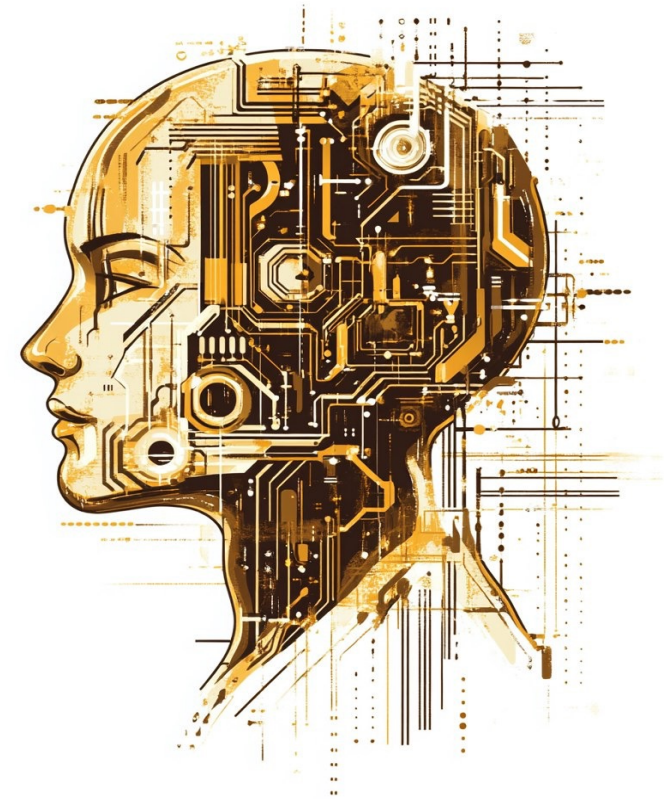
Подход и архитектура

Раздел 1

УСЛУГИ vCISO

vCISO (virtual Chief Information Security Officer)

Услуга, в рамках которой компания получает возможность мгновенного найма директора по кибербезопасности и его команды.



ДИРЕКТОР ПО КИБЕРБЕЗОПАСНОСТИ

VCISO (VIRTUAL CHIEF INFORMATION SECURITY OFFICER):

Комплекс услуг для мгновенного найма Директора по кибербезопасности и его команды для выстраивания стратегии развития, процессов и систем защиты Вашего бизнеса

ОПЫТ И ЗНАНИЯ

Комплекс услуг для мгновенного найма
Многолетний опыт и знания позволили нам разработать новый комплекс услуг: **virtual CISO (vCISO) или CISO-as-a-Service**, который позволяет получить экспертный опыт к передовым технологиям без многомиллионных инвестиций и увеличения штата компании.

СИЛЬНАЯ КОМАНДА

Команда менеджеров, методологов и экспертов по кибербезопасности, имеющая опыт работы в крупнейших компаниях



СТРАТЕГИЯ

Мы предлагаем не внедрение стандартных коробочных решений, а **создаем СТРАТЕГИЧЕСКУЮ программу кибербезопасности**, отвечающую Вашим потребностям

БИЗНЕС-ЗАДАЧИ

Мы **ориентированы именно на решение бизнес-задач кибербезопасности** в различных отраслях экономики, и хорошо понимаем тонкости современных технологий кибербезопасности

Услуги vCISO

Детально

-  Стратегия кибербезопасности
-  Управление проектами кибербезопасности
-  Оценка киберзащищенности
-  Управление киберрисками
-  Формирование команды кибербезопасности

-  Политики, регламенты и процедуры
-  Повышение осведомленности и обучение
-  Реагирование на инциденты
-  Соответствие требованиям кибербезопасности

Стратегия кибербезопасности

Сертифицированная команда виртуального CISO проводит аудит защищенности и зрелости системы кибербезопасности компании. Результат: анализ соответствия процессов и ИБ-систем требованиям регуляторов и международных стандартов безопасности (ISO 27001, NIST, PCI-DSS, **СТ РК ISO/IEC 27001-2023**)

ПРЕИМУЩЕСТВА

Помимо стратегии, компания получает:

- «Дорожную карту» развития киберзащиты бизнеса без затрат на собственный персонал и время его адаптации.
- Четкие сроки и бюджеты реализации проектов по стратегии развития и методике оценки результата.
- Рекомендации по необходимым собственным компетенциям бизнеса либо аутсорсинга процессов киберзащиты на внешнем рынке.

РЕЗУЛЬТАТ

Результатом оказания услуги является детальная **стратегия развития системы кибербезопасности компании**, включающая шаги кураторов кибербезопасности по персоналу и штатному расписанию, либо рекомендации по аутсорсингу, инвестиционным мероприятиям, с фиксацией результатов каждого этапа.

Стратегия развития разрабатывается в корреляции с бизнес-планами компании и интегрируется в существующие бизнес-процессы.

Управление проектами кибербезопасности

Команда vCISO осуществляет управление программой проектов или отдельными проектами по кибербезопасности в соответствии с требованиями к срокам и бюджетам

ПРЕИМУЩЕСТВА

Компания получает результат «под ключ» как услугу, при этом:

- снижает собственные затраты на содержание проектных команд,
- сокращает расходы на управление рисками в ходе реализации проектов.

РЕЗУЛЬТАТ

Руководители проектов имеют большой опыт реализации проектных программ в крупных компаниях.

В ходе начального анализа программы проектов выдаются рекомендации по ее актуальности, последовательности и целостности, исходя из нашего опыта реализации систем защиты на крупных предприятиях.

Оценка киберзащищенности

Команда vCISO проводит комплекс внешних и внутренних аудитов, тестов на проникновение с использованием активных и пассивных методов оценки. Цель – выработка «дорожной карты» устранения обнаруженных уязвимостей и несоответствий требованиям казахстанских и международных регуляторов

ПРЕИМУЩЕСТВА

Помимо комплексного плана мероприятий, в рамках дальнейшей поддержки компания получает:

- **сопровождение бизнеса для достижения точного результата** по разработанному плану мероприятий с минимальными издержками.

РЕЗУЛЬТАТ

Команда обладает сертифицированными аудиторами по требованиям российских и международных регуляторов, используя системы анализа защищенности и тестирования на проникновения ведущих производителей.

Результатом оказания услуги является комплексный план мероприятий по повышению киберзащищенности бизнеса, без дополнительных затрат на собственные команды аудиторов, технические средства анализа защищенности и тестирования на проникновение.

Управление киберрисками

В рамках услуги команда vCISO проводит внедрение процесса управления и методики оценки стоимости киберрисков, в соответствии с существующими бизнес-процессами компании

ПРЕИМУЩЕСТВА

Компания получает детальные «руководства к действию» по существующим бизнес-процессам в части обеспечения их кибербезопасности, при этом отсутствуют затраты на собственный штат специалистов в сфере кибербезопасности.

РЕЗУЛЬТАТ

Разрабатываются карты рисков, содержащие оценку эффективности принимаемых мер, стоимости реализации мероприятий по снижению риска и стоимости реализации риска для бизнеса.

Процесс управления и оценки рисков документируется и интегрируется в существующую бизнес-модель компании без снижения эффективности основных бизнес-процессов.

Формирование команды кибербезопасности

Команда vCISO проводит комплекс мероприятий по созданию собственного подразделения кибербезопасности в компании

ПРЕИМУЩЕСТВА

- Разрабатываемый план интегрируется с существующими бизнес-процессами и целями компании.
- Это существенно снижает затраты при создании подразделения собственными силами.

РЕЗУЛЬТАТ

Команда формирует план штатного расписания и требования к экспертизе на всех этапах развития направления кибербезопасности бизнеса. Он учитывает требования регуляторов, рынка технологий, начального состояния кибербезопасности в компании и разумной достаточности.

Компания получает детальный план по развитию направления, включающий проект бюджета подразделения, организационно-штатную структуру, описание функций и должностных обязанностей.

Политики, регламенты и процедуры

Команда vCISO оказывает услугу по созданию документационной системы кибербезопасности, разработке верхнеуровневых и низкоуровневых документов по кибербезопасности

ПРЕИМУЩЕСТВА

- Услуга не требует затрат на собственный штат методологов и экспертов.
- В рамках сервиса мы также формируем и передаем требования и обязанности исполнителей на процессах кибербезопасности для формирования собственной экспертизы исполнителей у компании.

РЕЗУЛЬТАТ

Наши сертифицированные методологи разрабатывают регламентирующие документы в соответствии с требованиями регуляторов и лучшими международными практиками, интегрируя описываемый процесс кибербезопасности в бизнес-модель предприятия без ущерба для бизнеса.

Результатом оказания услуги являются рабочие и документированные процессы обеспечения кибербезопасности бизнеса.

Повышение осведомленности и обучение

vCISO оказывает услуги по разработке программы повышения осведомленности пользователей бизнеса, проводит тренинги и обучающие семинары по кибербезопасности

ПРЕИМУЩЕСТВА

- Компания существенно снижает затраты на содержания штата экспертов в области кибербезопасности и получает полноценный выстроенный процесс кибербезопасности как услугу.
- Осведомленность и обучение пользователей –ключевой фактор успешности для недопущения реализации инцидентов кибербезопасности.

РЕЗУЛЬТАТ

Программы повышения осведомленности разрабатываются под каждого заказчика, исходя из уровня зрелости пользователей в вопросах кибербезопасности и бизнес-процессов компании.

По итогу внедрения процесса повышения осведомленности и обучения пользователей проводится тестирование бизнес-подразделений компании, разрабатываются отчеты с дальнейшими рекомендациями по процессу.

Реагирование на инциденты

Команда vCISO внедряет процесс управления инцидентами и расследования инцидентов кибербезопасности

ПРЕИМУЩЕСТВА

Для организации собственного ОЦИБ Вам не потребуется большой штат высококвалифицированных экспертов. Достаточно будет небольшой команды, которые после реализации задачи по созданию SOC будут осуществлять функцию контроля.

- Разрабатываемая процессная модель SOC будет интегрирована в существующую бизнес-модель при минимальных затратах на собственный штат экспертизы.

РЕЗУЛЬТАТ

Командой будет проведена разработка, документирование и интеграция процессов ОЦИБ Вашей компании в соответствии с лучшими практиками кибербезопасности.

Результатом оказания услуги является документированный и внедренный процесс управления и расследования инцидентов в сфере кибербезопасности, а также требования и функциональные обязанности к собственной экспертизе SOC, проект штатного расписания и бюджета

Соответствие требованиям кибербезопасности

Команда vCISO проводит сертифицированный аудит соответствия корпоративным, отраслевым и законодательным требованиям в области кибербезопасности

ПРЕИМУЩЕСТВА

Помимо услуги, компания получает:

- **детальный план приведения бизнеса к соответствию требованиям** с минимальными затратами на его реализацию.

РЕЗУЛЬТАТ

В результате оказания услуги командой разрабатываются карты соответствия с детальными планами по исправлению выявленных рисков, проектам и бюджетов на их устранение.

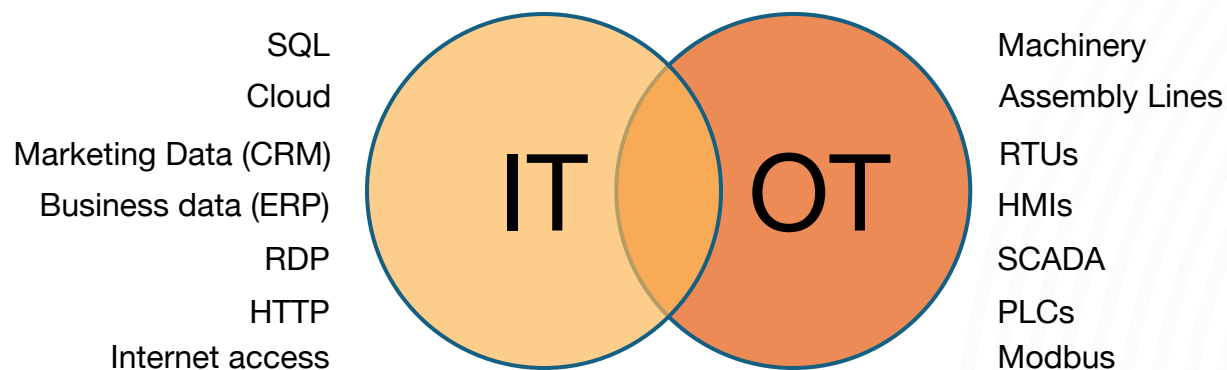
Наша экспертиза управляет соответствием в области **казахстанских и европейских требований законодательства**, международных стандартов в области кибербезопасности и лучшими практиками отрасли.

Раздел 2

ЗАЩИТА IT / OT / ICS ИНФРАСТРУКТУРЫ



Что мы защищаем?



ИТ-Активы

- Firewall
- Team work servers
- Mail & file servers
- Data storage
- Endpoint

Угрозы

- Не пропатченные уязвимости
- APT-атаки
- СПАМ и фишинг
- DDOS-атаки
- Несанкционированный доступ к структуре системы
- Проблемы с аутентификацией / авторизацией
- Недостаточная осведомленность о безопасности

Промышленные активы

- SCADA
- HMI
- OP workstations
- Network hardware
- PLC

Угрозы

- Нежелательные изменения внутри технологического процесса из-за вредоносного ПО или операционной ошибки
- Остановка АСУ ТП промышленных предприятий
- Запрещенный софт, usb и т.д. попадает внутрь сетей ICS
- Нарушение целостности ПЛК

Что мы предлагаем?

Модернизация существующих систем защиты промышленных КВОИКИ

Комплексный подход к построению промышленного ICS SOC, проектировка систем защиты АСУ ТП

Эксплуатация ТЗ КИИ по сервисной модели, модели импланта, иными способами

Внедрение средств защиты КВОИКИ

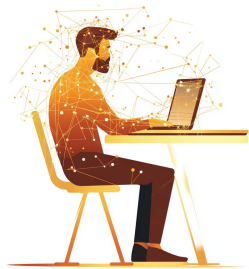
Повышение кибер осведомленности

Промышленная кибербезопасность (+ ESG) в целом

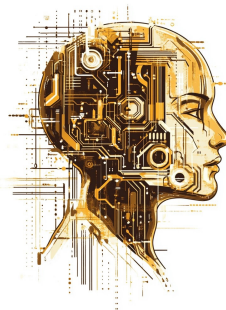
Стратегия и системный (прогнозирующий) подход к КВОИКИ

Личная кибербезопасность высшего руководства

Факторы успеха защиты АСУ ТП



ПОДГОТОВКА
ПЕРСОНАЛА



НАДЕЖНЫЙ ПРОМЫШЛЕННЫЙ
THREAT INTELLIGENCE



ОТРАБОТАННЫЕ
ПРОЦЕССЫ

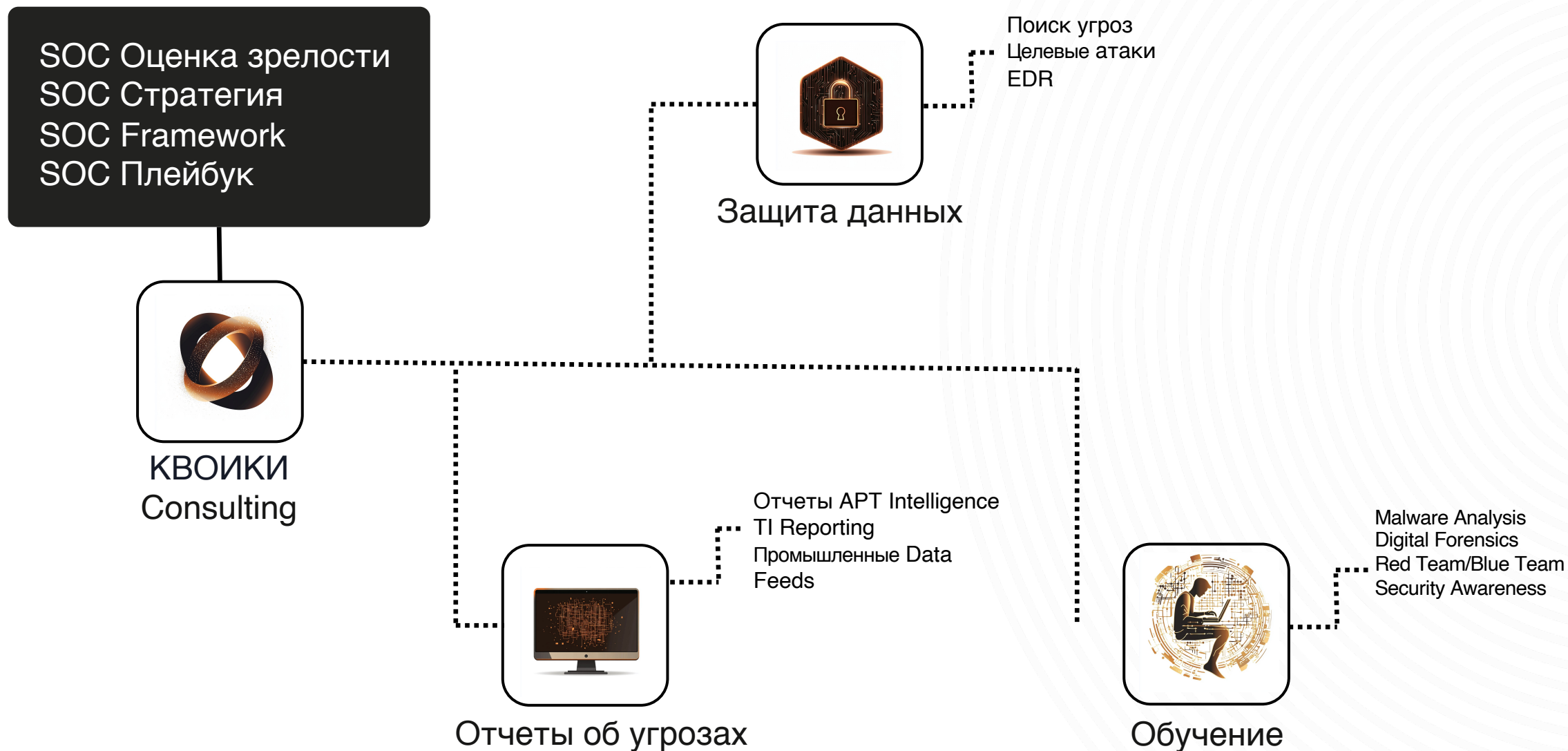


РАБОТА С
МЕНЕДЖМЕНТОМ

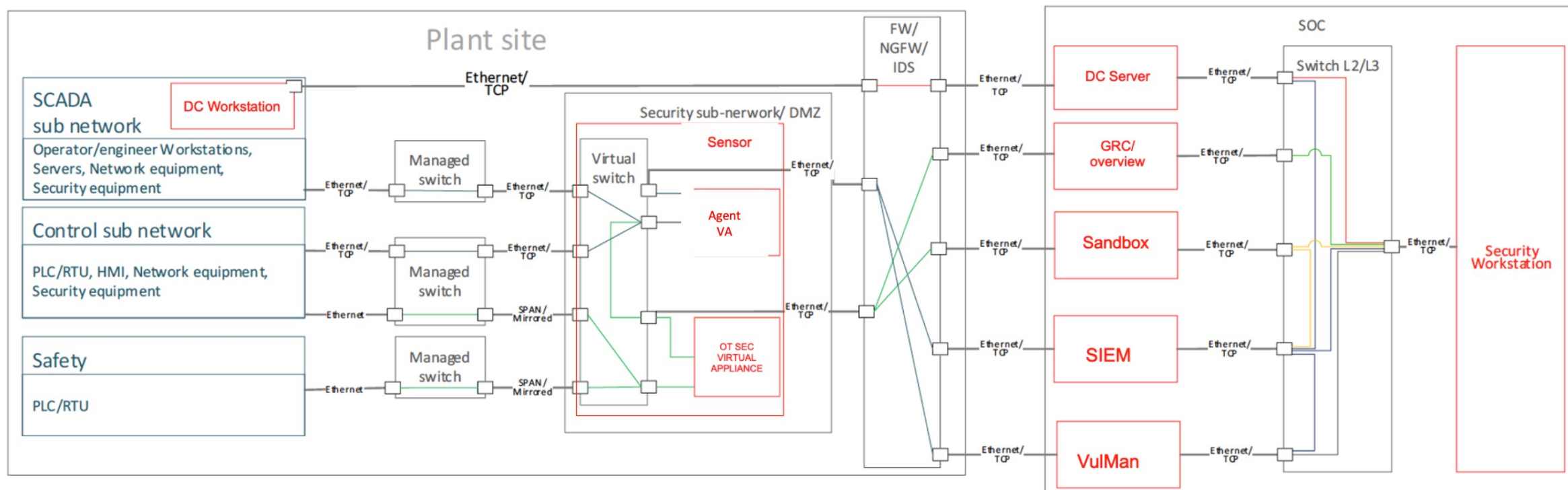


СОВРЕМЕННЫЕ
СЗ КВОИКИ

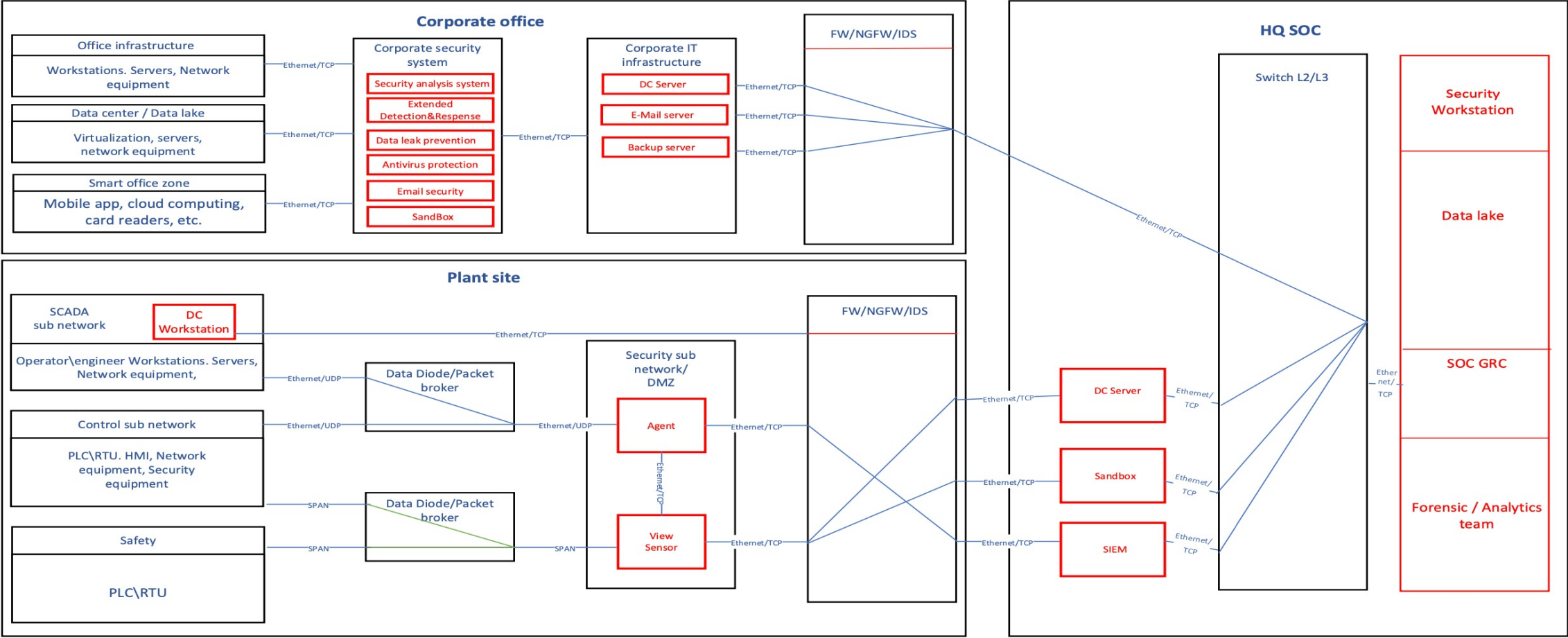
Что мы предлагаем?



Архитектура ОЦИБ-aaS

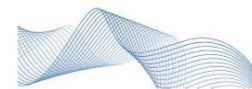


Архитектура ОЦИБ on-premise



Чем мы защищаем. Классы решений и вендоры

IM Incident management



Defensys

SIEM Security incident & event management



NTA Network traffic analysis



AM Anti-malware



VM Vulnerability management



CLAROTY



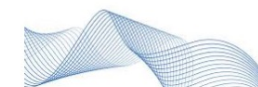
Defensys

DDS Data diode security

CLAROTY



TI Threat intelligence



Defensys

Распределение ответственности в проекте

КЛИЕНТ		DATASTAR	ДЕЙСТВИЯ OFFICE / IT	OT/ICS
Профайлинг команды	Утверждение	Ответственность	---	---
Найм	TBD	TBD	---	---
Ключевые элементы сервиса	Мониторинг	Ответственность	Автоматизированы	Автоматизированы
Эскалация	Мониторинг	Ответственность	Автоматизированы	Автоматизированы
Отчеты об инцидентах	Решение / ответственность	Ответственность	Автоматизированы	Автоматизированы
Тикеты инцидентов	Мониторинг	Ответственность	Автоматизированы	Автоматизированы
Обработка тикетов	Мониторинг	Ответственность	Автоматизированы	Ручной режим
Расследование инцидентов	Решение / ответственность	Ответственность	Ручной режим	Ручной режим
Управление инцидентами	Решение / ответственность	Ответственность	Автоматизированы	Ручной режим
Киберосведомленность	Повышение осведомленности	Ответственность	Автоматизированы	Автоматизированы



DataStar

SENSITIVE || MATTERS

Евгений Питолин Управляющий директор DataStar



contact me @ Facebook



@EVGENYPITOLIN



Contact me @ Instagram



Contact me @ telegram



Explore my LinkedIN

