InfoDiode: сценарии применения

Устройства передачи данных класса «диоды данных» используются для физического разделения сетей в условиях сохранения однонаправленного канала передачи информации. В брошюре представлены основные сценарии использования решений **InfoDiode** в различных отраслях экономики. Сценарии основаны на накопленном опыте применения устройств на практике. Приведенный перечень сценариев не является полным и представлен с целью демонстрации возможностей продукта по защите сетевого периметра предприятий и организаций.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.infodiode.ru

28.08.2024

Сценарии использования InfoDiode

Передача технологических данных критической инфраструктуры в недоверенный сетевой сегмент……..4

Передача из технологического сегмента данных о состоянии оборудования для целей мониторинга и диагностики…...6

Передача из технологического сегмента данных о состоянии оборудования и процессов для целей их обработки, анализа и визуализации в MES и БДРВ…….....8

Передача IIoT-трафика из технологического сегмента в корпоративный сегмент для контроля, мониторинга и визуализации цифровых двойников……..…….10

Передача критичных данных в целях резервного копирования в защищенное хранилище……..……..…….12

Передача SPAN-трафика технологического сегмента в SOC в рамках построения системы обнаружения вторжений на базе продуктов IDS/IPS…….…….14

Передача данных с датчиков в сетевой сегмент АСУ ТП через недоверенные сети……..16

Трансляция снимков экранов с АРМ в доверенном сегменте сети в целях оказания удалённой технической поддержки сторонними службами и организациями……..…….18

Передача технологических данных из производственного комплекса или объекта добычи в корпоративный сетевой сегмент……...……..20

Передача технологических данных в головной офис - из более доверенного в менее доверенный сетевой сегмент..…22

Передача данных для мониторинга производственной инфраструктуры в менее доверенный сетевой сегмент……..…..24

Передача данных с добывающего оборудования и смежных систем в менее доверенный сетевой сегмент..……...26

Передача данных технологической сети горно-обогатительного комбината (ГОК) в менее доверенный сетевой сегмент……..……28

Передача критичных данных в целях резервного копирования во внешнее хранилище……..30

Оказание технической поддержки клиентам через мессенджеры и иные каналы коммуникаций…….……32

Передача данных в лабораторию ИБ в составе SOC для изоляции и последующего анализа на предмет наличия вредоносного кода……...……34

Осуществление удалённого мониторинга состояния очистных сооружений и станций водоподготовки……...……36

Осуществление удалённого сбора данных с приборов учёта и мониторинг состояния объектов коммунального хозяйства……..……38

Предоставление доступа к клиническим исследованиям сторонней организации……...40

Предоставление клиентам ЦОД, покупающим услуги IaaS, данные сети управления о работе серверов и сетевого оборудования с целью мониторинга……..……..42

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарии использования InfoDiode

Агрегация в корпоративном сегменте данных с узлов управления……..……...……..44

Сбор данных мониторинга стрелочных переводов с местных узлов управления…….....46

Передача данных видеонаблюдения с защищаемого объекта в центр мониторинга безопасности или ситуационный центр……..…..……..48

Передача оповещений о киберугрозах из Deception-системы защищаемого сегмента в SOC…..……...50

Передача телеметрии и событий безопасности из технологического сегмента в SOC в рамках построения системы обнаружения вторжений на базе продуктов IDS/IPS…..……..52

Передача логов и событий информационной безопасности из технологического сегмента в SOC в рамках построения центра контроля информационной безопасности…..……..54

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

Энергетика, генерация

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача технологических данных критической инфраструктуры в недоверенный сетевой сегмент

ОТРАСЛЬ

ЭНЕРГЕТИКА

ЦЕЛЬ

Обеспечить передачу тегов OPC DA различных версий из технологического (защищаемого) сегмента в Historian корпоративного сегмента для решения задач анализа данных и планирования

РЕШЕНИЕ

Совместное применение комплекса продуктов KepServerEx, InfoDiode SMART, Aveva/Wonderware Historian

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с источником данных OPC DA с возможностью передачи данных внешним потребителям

О компании

Международная группа компаний, одна из ведущих в мире в сфере добычи и переработки минеральных ресурсов, с интегрированными, добывающими, перерабатывающими, энергетическими и логистическими предприятиями

Вызовы в области информационной безопасности

Чтобы выполнить свои обязательства перед потребителями поставщику электроэнергии требуется проводить мониторинг и анализ состояния систем генерации и оборудования. Данные для этого передаются из технологического сегмента в корпоративный. Однако по тому же каналу возможна организация атаки или попадание вредоносного ПО из корпоративного или иного внешнего сегмента. Это может привести к нарушению работы технологической сети, простою генерации и дорогостоящему ремонту.

Применяемый продукт

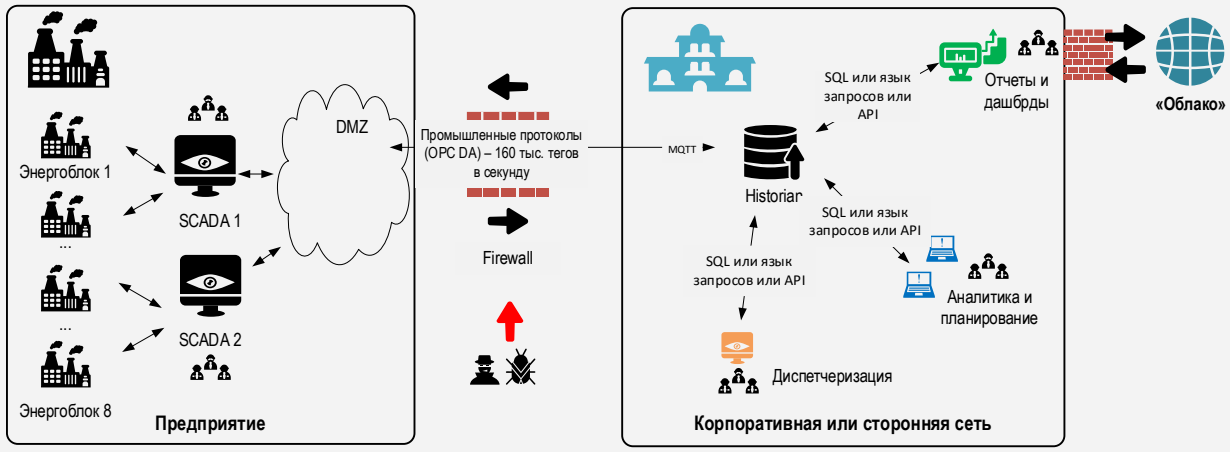
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно получать данные (OPC DA) с 8 энергоблоков технологического сегмента, направлять их в хранилище Historian, далее специалистам для мониторинга, аналитики и планирования
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для Historian

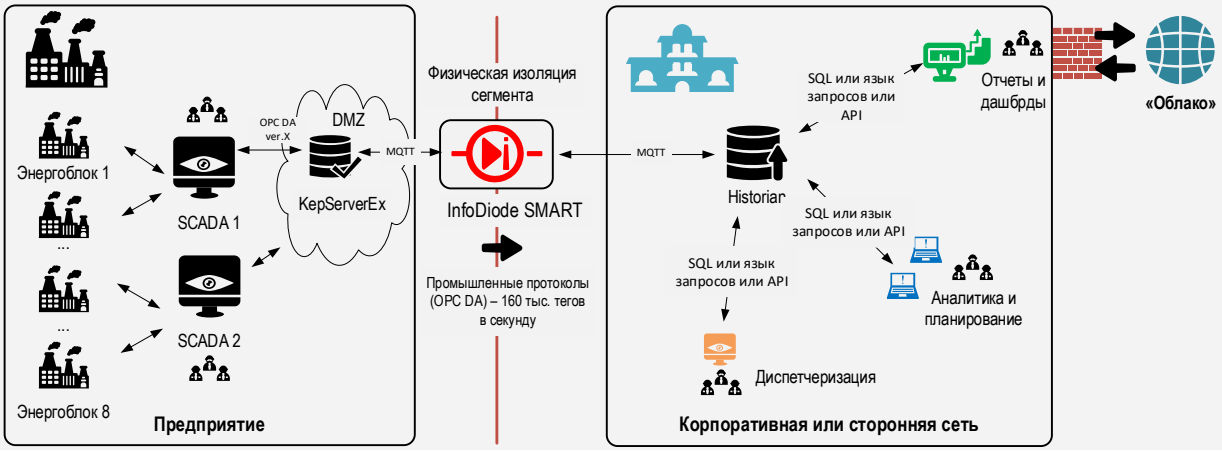
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети. Выполнено физическое отделение технологической сети от других, менее доверенных сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализован сбор данных с 8 энергоблоков и их передача по однонаправленному каналу через диод данных в центр планирования и аналитики, в хранилище Historian. Интенсивность передаваемых тегов — до 160 тыс. тегов OPC DA в секунду
- Реализована передача дополнительных данных для руководства и заинтересованных сотрудников в корпоративном сегменте (дашборды, витрины, отчеты)

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Энергетика, генерация

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача из технологического сегмента данных о состоянии оборудования для целей мониторинга и диагностики

ОТРАСЛЬ

ЭНЕРГЕТИКА

ЦЕЛЬ

Обеспечить передачу телеметрии по протоколу IEC-104 из технологического (защищаемого) сегмента в региональное диспетчерское управление и централизованный ситуационный центр

РЕШЕНИЕ

Совместное применение комплекса продуктов InfoDiode SMART, КОТМИ-14, СК-11

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с возможностью передачи данных в центр мониторинга

О компании

Многопрофильный холдинг, объединяющий активы в энергетике

Вызовы в области информационной безопасности

Энергогенерирующие предприятия попадают под нормы 187-ФЗ о безопасности объектов КИИ. В соответствии с требованиями необходимо физически ограничить возможность доступа к технологической сети извне, поскольку возможна организация атаки или попадание вредоносного ПО из корпоративного или иного внешнего сегмента. Это может привести к нарушению работы технологической сети, простою генерации и дорогостоящему ремонту. В то же время, для своевременной диагностики и профилактики оборудования необходим мониторинг и удаленная диагностика со стороны эксплуатационных служб и производителя оборудования.

Применяемый продукт

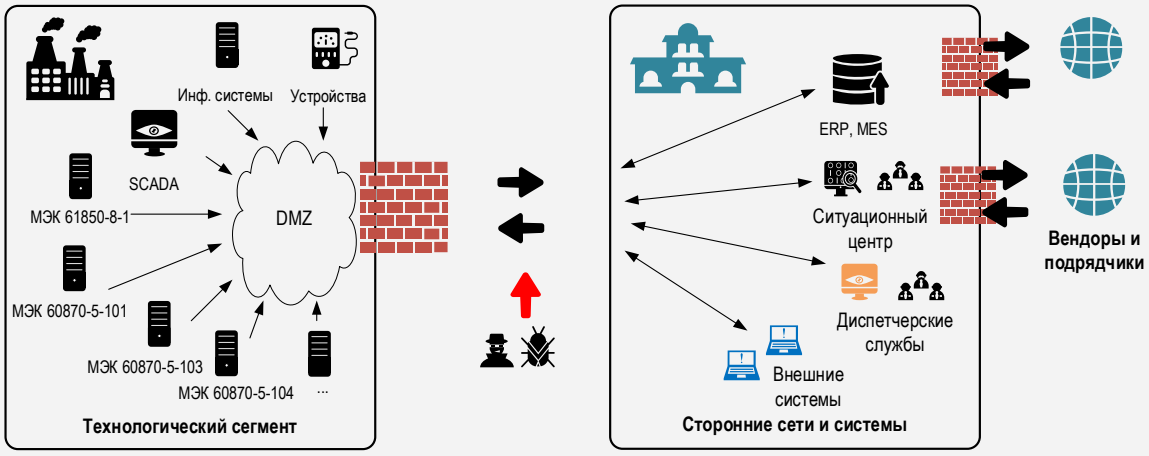
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Разделить сегменты сети с разными уровнями доверия и исключить любое внешнее воздействие на объект КИИ
- Регулярно собирать данные с оборудования в технологическом сегменте, направлять их в сторонние службы для мониторинга и оперативного контроля
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для внешних получателей

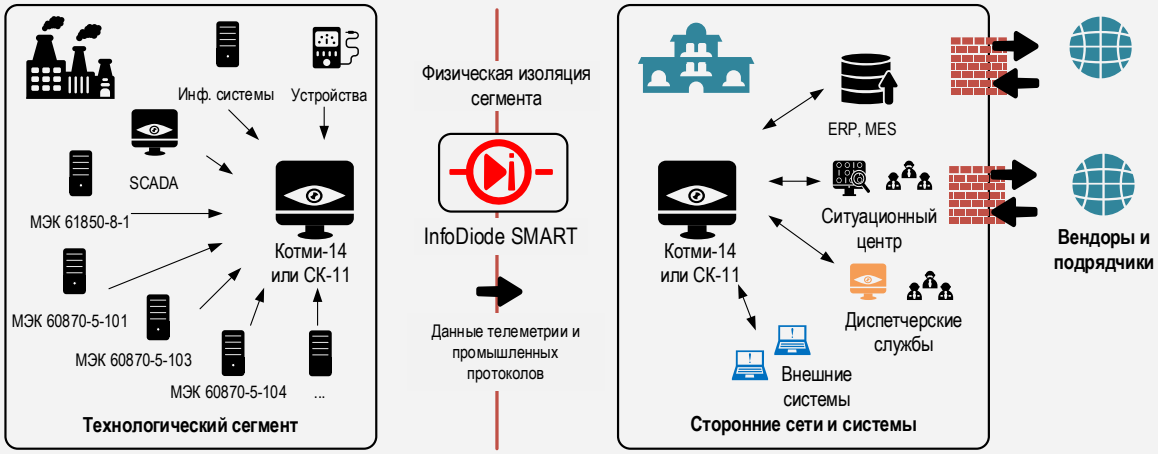
Архитектура: ДО



Результаты

- Выполнены требования государственного регулятора в рамках 187-ФЗ к объектам КИИ
- Выполнено физическое отделение технологической сети от других, менее доверенных, сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализован сбор данных с оборудования и их передача по однонаправленному каналу через диод данных удалённому потребителю, в том числе производителям и/или сторонним эксплуатационным службам
- Реализованы требования SLA о передаче данных о состоянии оборудования и объекта для целей мониторинга и оперативного контроля ситуационным или диспетчерским центром

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Промышленное производство

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача из технологического сегмента данных о состоянии оборудования и процессов для целей их обработки, анализа и визуализации в MES и БДРВ

ОТРАСЛЬ

ПРОМЫШЛЕННОСТЬ

ЦЕЛЬ

Обеспечить передачу данных из технологического (защищаемого) сегмента с целью обеспечения их агрегации и обработки в MES системе в менее доверенном сегменте

РЕШЕНИЕ

Совместное применение комплекса продуктов InfoDiode SMART, TL.Solutions, I-DS (Indusoft Digital Services)

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с возможностью передачи данных в MES для их сбора, обработки, анализа и визуализации

О компании

Крупное производственное предприятие

Вызовы в области информационной безопасности

Крупные промышленные предприятия попадают под нормы 187-ФЗ о безопасности объектов КИИ. В соответствии с требованиями необходимо физически ограничить возможность доступа к технологической сети извне, поскольку возможна организация атаки или попадание вредоносного ПО из корпоративного или иного внешнего сегмента. Это может привести к нарушению работы технологической сети, простою производства и дорогостоящему ремонту. В то же время, для оперативного управления и контроля производственных процессов необходимо обеспечить централизованный сбор и обработку данных из технологических сегментов предприятий.

Применяемый продукт

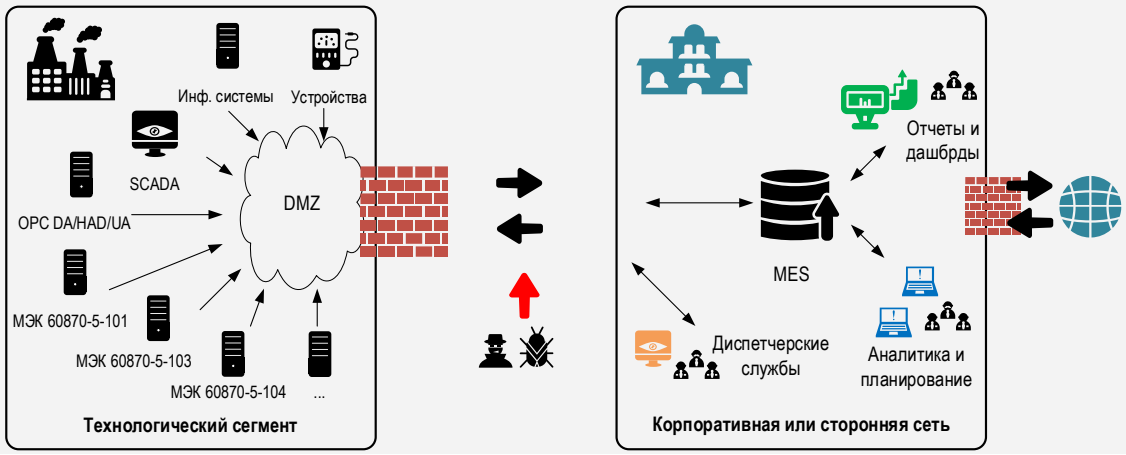
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Разделить сегменты сети с разными уровнями доверия и исключить любое внешнее воздействие на объект КИИ
- Регулярно собирать данные с оборудования в технологическом сегменте, направлять их в систему управления производственными процессами (Manufacturing Execution System, MES)
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для внешних получателей

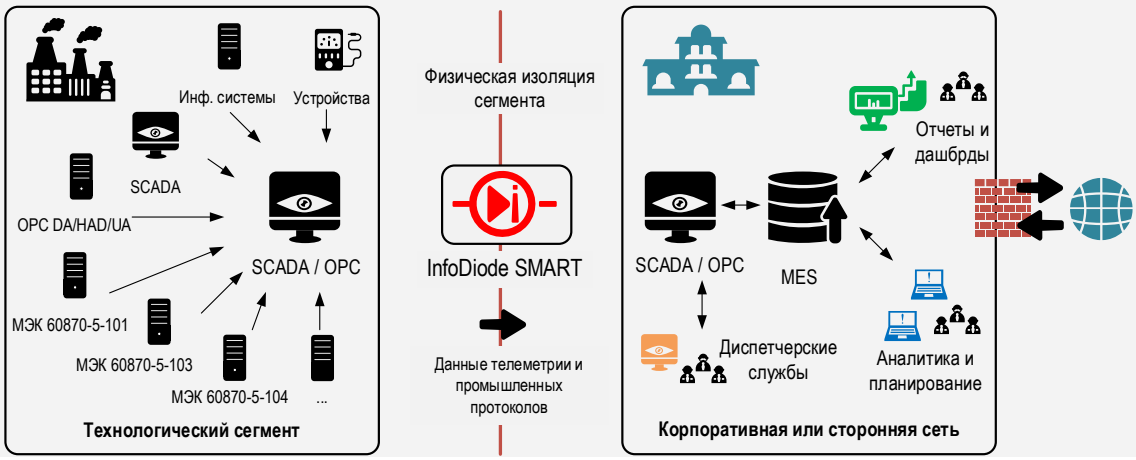
Архитектура: ДО



Результаты

- Выполнены требования государственного регулятора в рамках 187-ФЗ к объектам КИИ
- Выполнено физическое отделение технологической сети от других, менее доверенных, сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализован сбор данных с оборудования и их передача по однонаправленному каналу через диод данных в информационную систему управления производственными процессами (MES)
- Реализованы требования к скорости передачи информации о состоянии оборудования и объекта для накопления в базе данных реального времени

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Промышленное производство

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача IIoT-трафика из технологического сегмента в корпоративный сегмент для контроля, мониторинга и визуализации цифровых двойников

ОТРАСЛЬ

ПРОМЫШЛЕННОСТЬ

ЦЕЛЬ

Обеспечить передачу данных из технологического (защищаемого) сегмента с целью обеспечения удаленного мониторинга, диагностики и оптимизации работы оборудования в менее доверенном сегменте

РЕШЕНИЕ

Совместное применение комплекса продуктов InfoDiode SMART, IIoT.Istok

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с возможностью передачи данных в платформу промышленного интернета вещей (обработка, анализ и визуализация)

О компании

Крупное производственное предприятие

Вызовы в области информационной безопасности

Крупные промышленные предприятия попадают под нормы 187-ФЗ о безопасности объектов КИИ. В соответствии с требованиями необходимо физически ограничить возможность доступа к технологической сети извне, поскольку возможна организация атаки или попадание вредоносного ПО из корпоративного или иного внешнего сегмента. Это может привести к нарушению работы технологической сети, простою производства и дорогостоящему ремонту. В то же время, для оперативного управления и контроля производственных процессов необходимо обеспечить централизованный сбор и обработку данных из технологических сегментов предприятий.

Применяемый продукт

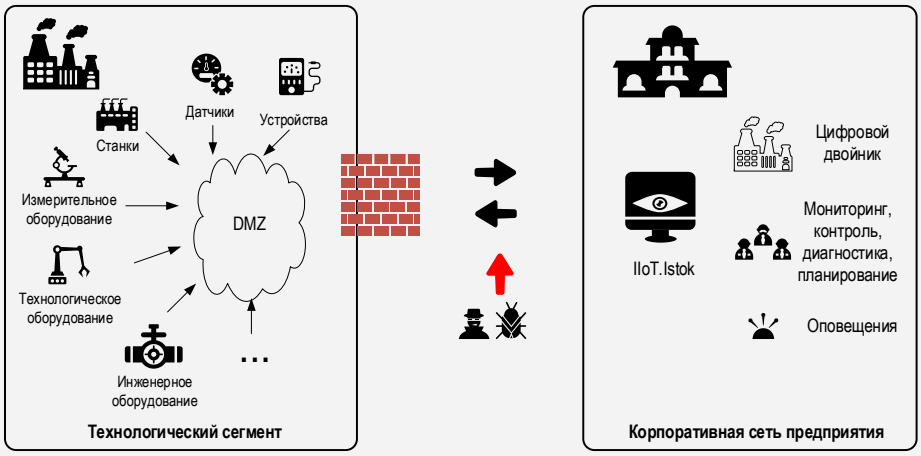
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Разделить сегменты сети с разными уровнями доверия и исключить любое внешнее воздействие на объект КИИ
- Непрерывно собирать данные с оборудования в технологическом сегменте, направлять их в платформу для промышленного интернета вещей
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для внешних получателей

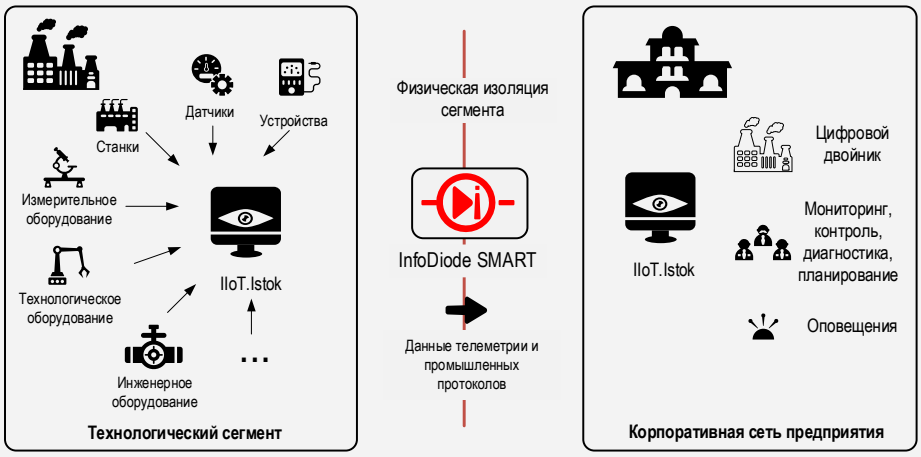
Архитектура: ДО



Результаты

- Выполнены требования государственного регулятора в рамках 187-ФЗ к объектам КИИ
- Выполнено физическое отделение технологической сети от других, менее доверенных, сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализован сбор данных IIoT с оборудования и их передача по однонаправленному каналу через диод данных в платформу для промышленного интернета вещей
- Реализованы требования к скорости передачи информации о состоянии оборудования и объекта для накопления в базе данных

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача критичных данных в целях резервного копирования в защищенное хранилище

ОТРАСЛЬ

ПРОМЫШЛЕННОСТЬ, ЭНЕРГЕТИКА

ЦЕЛЬ

Обеспечить регулярное резервное копирование информации из корпоративной сети в защищенное хранилище.

РЕШЕНИЕ

Применение аппаратно–программного комплекса InfoDiode PRO для создания изолированного сетевого сегмента, защищенного от внешнего воздействия

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) сетевого сегмента для хранения бэкапов систем, «снимков данных», резервных копий данных.

О компании

Вертикально интегрированный промышленный холдинг, управляющий активами в сфере энергетики, металлургии и горнорудной промышленности

Вызовы в области информационной безопасности

Устойчивое функционирование бизнес-процессов предприятия зависит, в том числе, и от наличия надежно функционирующей системы резервного копирования. В то же время, внешние соединения с основной сетью, а также места хранения резервных копий, могут подвергаться кибератакам. В этих условиях хранение данных на обычных ресурсах (ленточное хранилище, файловое хранилище и т.п.) повышает риски утери, компрометации данных. Предприятию требуется организация защищенного сегмента, который позволит сохранять эталонные копии данных для наиболее рискованных сценариев их потери, в том числе в результате действий злоумышленников.

Применяемый продукт

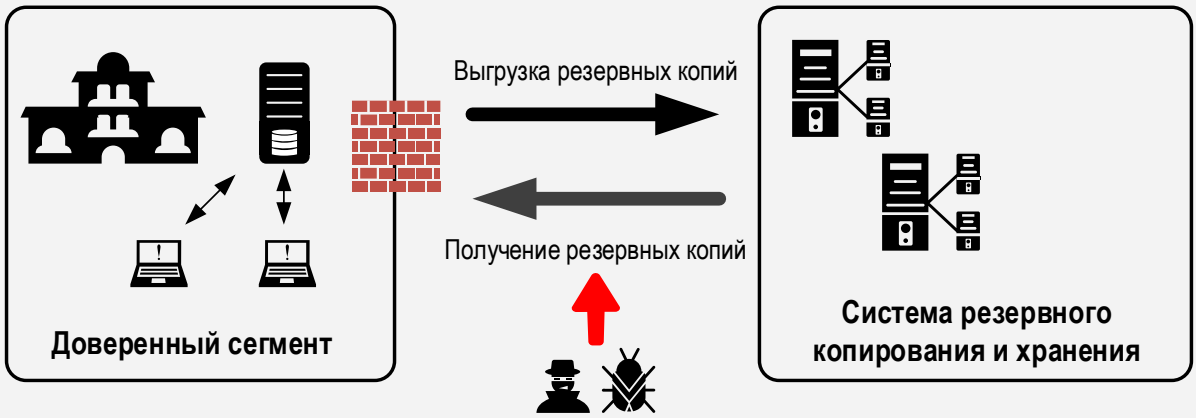
АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно передавать данные бэкапов на защищенный ресурс для целей гарантированного изолированного хранения резервных копий, «снимков данных», эталонных копий данных и систем
- Гарантированно исключить воздействие на защищенный сегмент, сделав невозможной организацию атаки по тому же каналу, по которому данные передаются на хранение

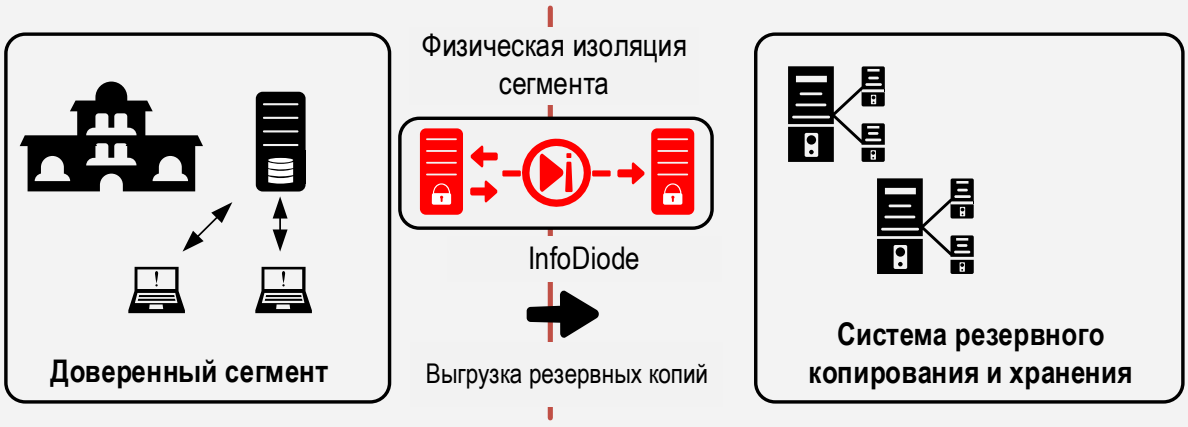
Архитектура: ДО



Результаты

- Выполнено физическое отделение защищенного/доверенного сегмента от менее доверенных сегментов. Исключена возможность проникновения злоумышленника в сегмент хранения данных и распространения (запуска) в нем вредоносных программ
- Обеспечена однонаправленная передача данных на внешнее защищенное хранилище, исключающая возможность воздействия на систему хранения бэкапов и резервируемые данные
- Обеспечена непрерывность бизнес-процессов предприятия благодаря организации строго детерминированного однонаправленного потока данных на внешний по отношению к корпоративной сети защищенный ресурс, снижены риски полной утери данных в случае успешной атаки злоумышленника на основной сегмент данных

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача SPAN-трафика технологического сегмента в SOC в рамках построения системы обнаружения вторжений на базе продуктов IDS/IPS

ОТРАСЛЬ

ПРОМЫШЛЕННОСТЬ, ЭНЕРГЕТИКА

ЦЕЛЬ

Обеспечить передачу промышленных протоколов из технологического (защищаемого) сегмента промышленного объекта в иные сетевые сегменты для решения задач обнаружения вторжений

РЕШЕНИЕ

Совместное применение аппаратного комплекса InfoDiode с решениями KICS for Networks или PTISIM в рамках построения СОВ

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с сохранением возможности передачи трафика для анализа и предотвращения вторжений

О компании

Крупное промышленное предприятие, имеющее значимый технологический сегмент, требующий дополнительных средств контроля - построения системы обнаружения вторжений (СОВ)

Вызовы в области информационной безопасности

В результате кибератаки на технологическую сеть могут существенно пострадать данные и оборудование, что приведёт к значимым нарушениям технологических процессов. Для предотвращения кибератак требуется осуществлять непрерывный мониторинг сетевого трафика технологического сегмента на предмет обнаружения признаков вторжения.

В то же время, учитывая, что центр мониторинга безопасности (SOC) расположен в другом сегменте сети, необходимо обеспечить надёжную защиту периметра технологического сегмента сети.

Применяемый продукт

АК InfoDiode - базовое аппаратное решение для передачи UDP, Syslog, SPAN трафика потребителям за пределами доверенного сегмента. Сертифицировано ФСТЭК УД (4). Обеспечивает защиту на аппаратном уровне, изолирует защищаемый сегмент.

InfoDiode RACK предназначен для монтажа в стойку.

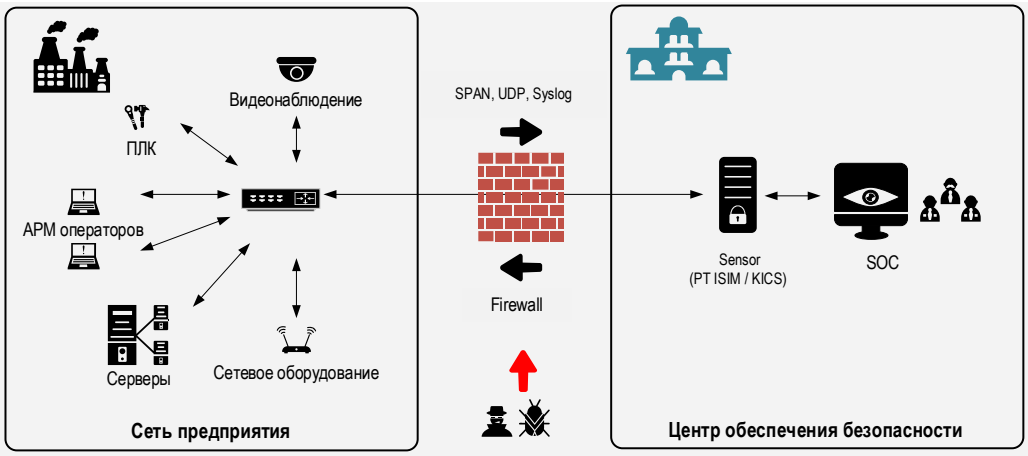
InfoDiode MINI предназначен для монтажа на DIN-рейку или Desktop вариант.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно получать SPAN-трафик с производственных сегментов в центр мониторинга безопасности для анализа и предотвращения вторжений, исключив установку доп ПО на АРМ в технологическом сегменте
- Обеспечить централизованный мониторинг сетевого трафика технологической сети
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для SOC

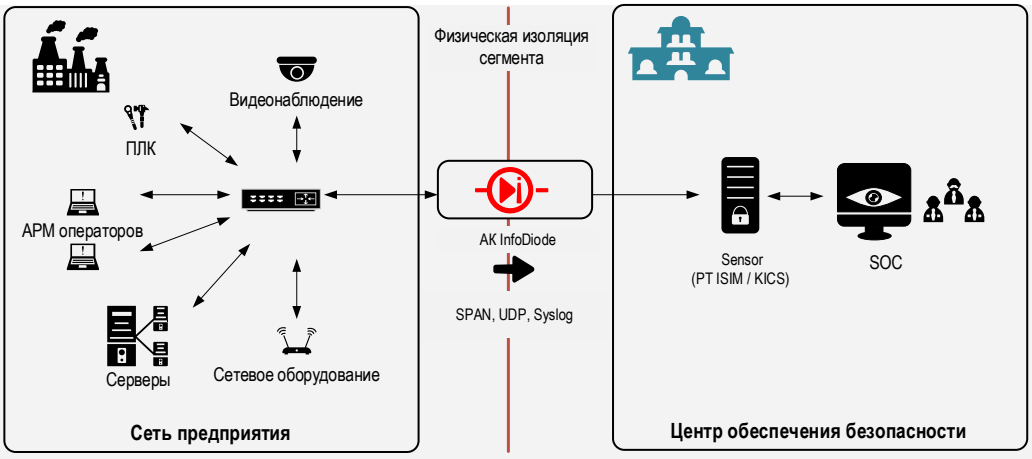
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети
- Выполнено физическое отделение технологической сети от других, менее доверенных сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализована передача SPAN-трафика с производственных объектов по однонаправленному каналу через диод данных в центр обеспечения безопасности (SOC), успешно решена задача по построению системы обнаружения вторжений (СОВ) на предприятии

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Промышленность, энергетика

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача данных с датчиков в сетевой сегмент АСУ ТП через недоверенные сети

ОТРАСЛЬ

ПРОМЫШЛЕННОСТЬ, ЭНЕРГЕТИКА

ЦЕЛЬ

Обеспечить безопасную передачу сигналов с оборудования и датчиков, размещенных на удалённых пунктах технологического сегмента сети, в SCADA для решения задач комплексного мониторинга объекта

РЕШЕНИЕ

Совместное применение аппаратного комплекса InfoDiode и коннекторов Modbus

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с сохранением возможности получения данных от внешних датчиков и оборудования

О компании

Крупная энергогенерирующая компания, промышленное предприятие

Вызовы в области информационной безопасности

Зачастую атакам подвергаются каналы связи, сопрягающие технологическую и корпоративную сети, однако не стоит забывать и про потенциальную уязвимость сегментов самой технологической сети. В результате кибератаки могут существенно пострадать данные и серверы приложений предприятия, что приведёт к существенным нарушениям технологических процессов. Объекты инфраструктуры, расположенные за пределами физического периметра объекта КИИ, находятся в менее доверенном сегменте, доступ из которого к КИИ должен быть ограничен и соответствующим образом защищен.

Применяемый продукт

АК InfoDiode - базовое аппаратное решение для передачи UDP, Syslog, SPAN трафика потребителям за пределами доверенного сегмента. Сертифицировано ФСТЭК УД (4). Обеспечивает защиту на аппаратном уровне, изолирует защищаемый сегмент.

InfoDiode RACK предназначен для монтажа в стойку.

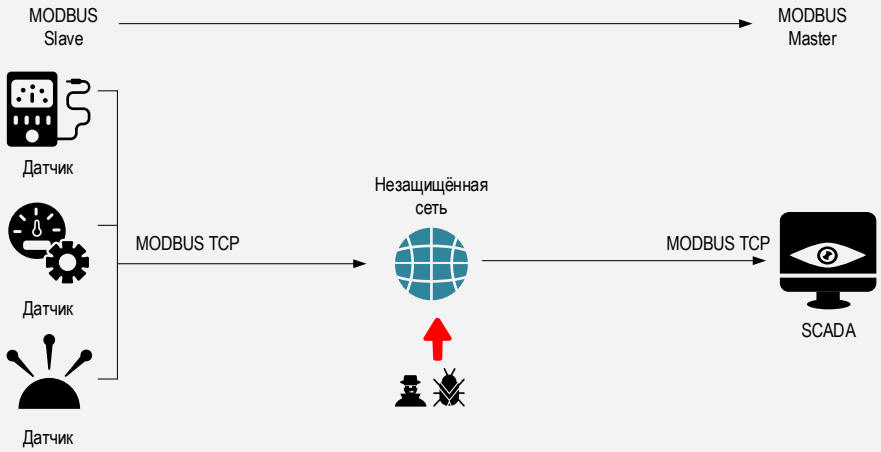
InfoDiode MINI предназначен для монтажа на DIN-рейку или Desktop вариант.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно получать данные с внешних объектов контроля (оборудования, датчиков), направлять их в единую систему SCADA в технологической сети для мониторинга, обработки и передачи в иные системы
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные с оборудования и датчиков, находящихся за пределами контролируемой зоны КИИ (физического периметра КИИ)

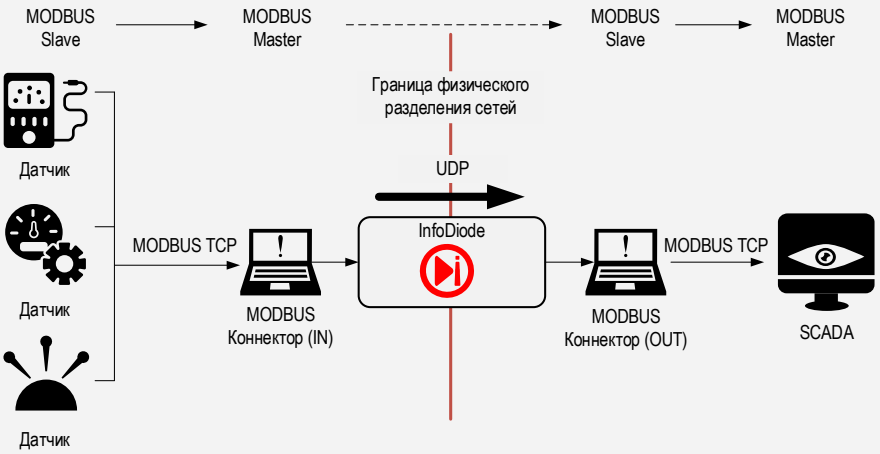
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети. Выполнено физическое отделение технологической сети от менее доверенных сетей передачи данных. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Обеспечена передача оповещений от устройств, расположенных за пределами физического периметра предприятия, в технологическую сеть, реализована передача трафика Modbus в целях сбора данных в SCADA
- Реализован сбор данных с внешних объектов контроля в единую систему SCADA и их передача по однонаправленному каналу через диод данных в технологическую сеть

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Промышленность, тех. поддержка

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Трансляция снимков экранов с АРМ в доверенном сегменте сети в целях оказания удалённой технической поддержки сторонними службами и организациями

ОТРАСЛЬ

ПРОМЫШЛЕННОСТЬ, ТРАНСПОРТ

ЦЕЛЬ

Обеспечить онлайн передачу снимков экрана с рабочих мест на производственном объекте в центр технической поддержки вендора, сторонней службы

РЕШЕНИЕ

Применение аппаратно–программного комплекса InfoDiode PRO для защиты периметра технологического сегмента сети

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента сети от любого внешнего воздействия с возможностью онлайн передачи снимков экрана для специалистов тех. поддержки

О компании

Промышленное предприятие с автоматизированным производственным циклом. Предприятие приобретает у сторонних вендоров и производителей услуги технической поддержки имеющегося на объекте оборудования и SCADA

Вызовы в области информационной безопасности

Современные высокотехнологичные производства требуют высочайшей квалификации кадров и уровня сопровождения. Нередко требуется поддержка специалистов по конкретным системам и процессам, в том числе от вендоров ИС и оборудования. Для этого данные с АРМ передаются из технологического сегмента в корпоративный, однако, по тому же каналу возможна организация атаки или попадание вредоносного ПО. Это может привести к нарушению производственных процессов и поломке дорогостоящего оборудования. Требуется обеспечить наглядное предоставление данных с АРМ оператора в техн. сегменте сторонним службам в целях оказания тех. поддержки

Применяемый продукт

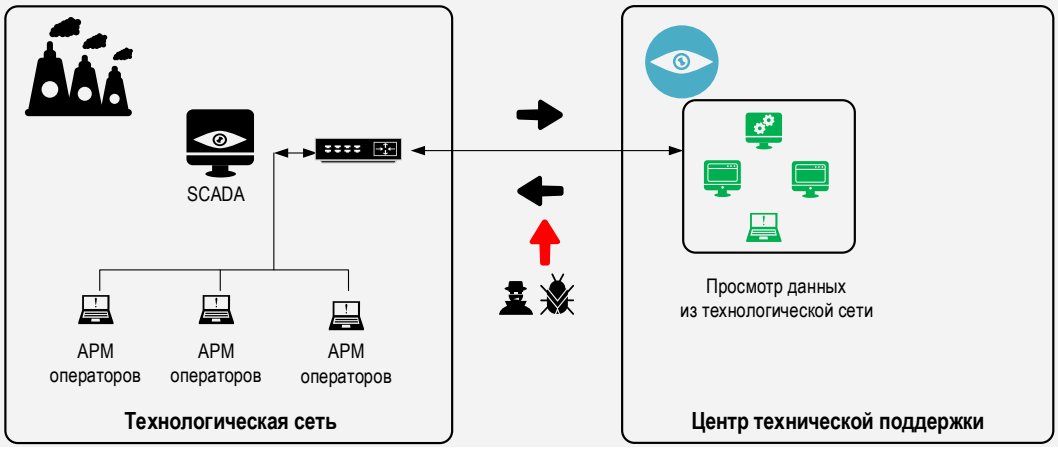
АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя этот сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Обеспечить передачу снимков экрана с SCADA и АРМ операторов на промышленном объекте во внешний центр технической поддержки
- Гарантированно исключить воздействие на информационные системы и оборудование промышленного объекта в условиях получения онлайн данных с мониторов операторов

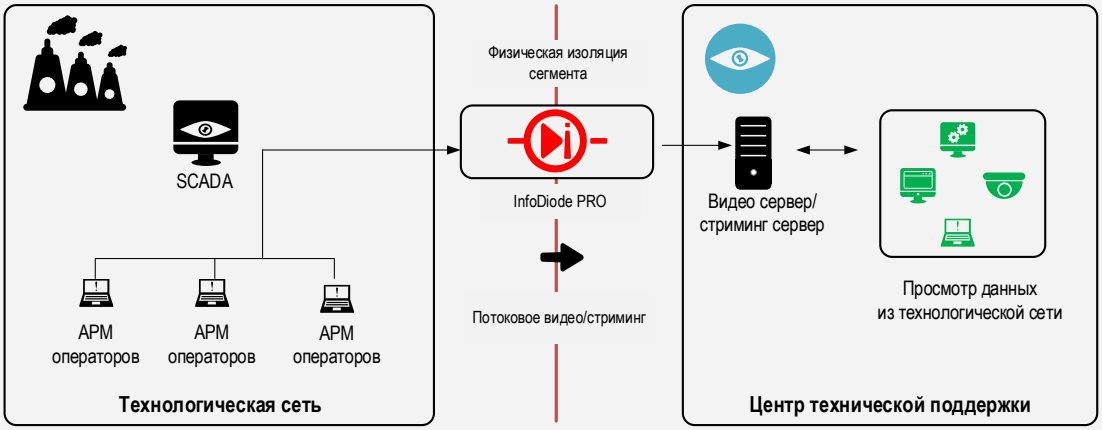
Архитектура: ДО



Результаты

- Выполнено физическое отделение технологического сегмента сети промышленного объекта от внешних сетей. Исключена возможность воздействия на информационные системы и оборудование
- Обеспечена направленная передача данных в центр технической поддержки, исключающая любые входящие соединения в технологический сегмент промышленного объекта
- Обеспечена передача онлайн снимков экрана в реальном времени с контрольных мониторов и устройств наблюдения специалистам технической поддержки сторонних служб и вендоров ПО и оборудования

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Производство минеральных удобрений

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача технологических данных из производственного комплекса или объекта добычи в корпоративный сетевой сегмент

ОТРАСЛЬ

ХИМИЧЕСКАЯ ПРОМЫШЛЕННОСТЬ

ЦЕЛЬ

Обеспечить передачу тегов OPC DA различных версий из технологического (защищаемого) сегмента потребителям в корпоративный сегмент для решения задач анализа данных и планирования

РЕШЕНИЕ

Совместное применение комплекса продуктов MasterOPC, InfoDiode SMART

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с источником данных OPC DA с возможностью передачи данных внешним потребителям

О компании

Один из ведущих производителей минеральных удобрений на мировом рынке

Вызовы в области информационной безопасности

Обеспечение непрерывного процесса на химическом производстве требует мониторинга и анализа производственных объектов и оборудования. Данные для этого передаются из технологического сегмента в корпоративный. Однако по тому же каналу возможна организация атаки или попадание вредоносного ПО из корпоративного или иного внешнего сегмента. Это может привести к нарушению работы технологической сети, дорогостоящему ремонту, возникновению техногенных катастроф.

Применяемый продукт

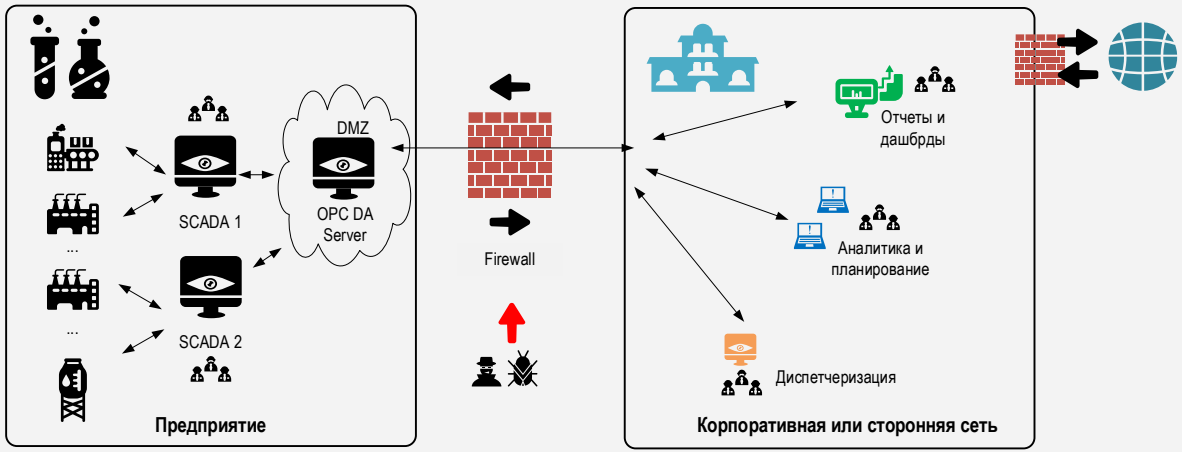
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно получать данные установок технологического сегмента, направлять их внешним потребителям и службам мониторинга для контроля, аналитики и планирования
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для сторонних потребителей

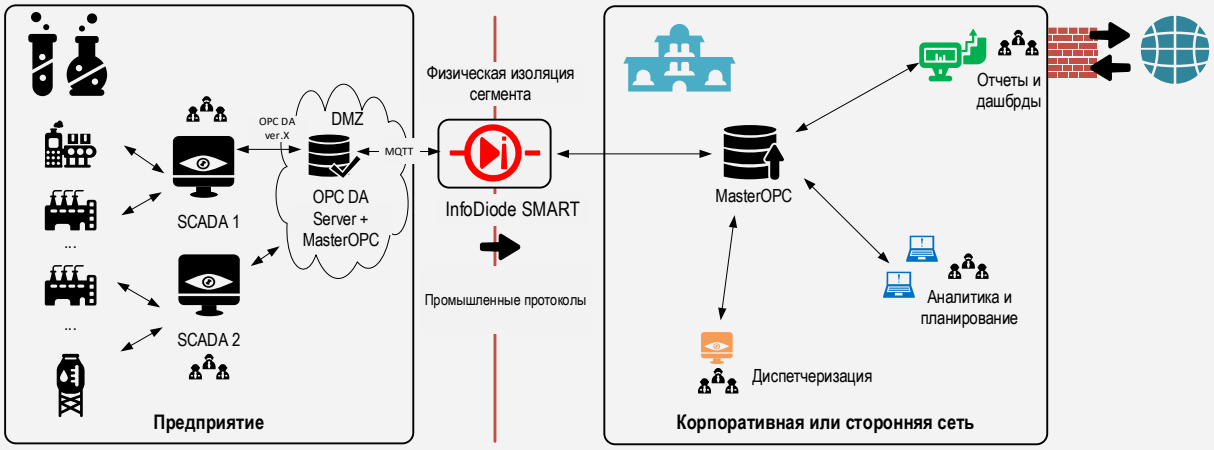
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети. Выполнено физическое отделение технологической сети от других, менее доверенных сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализован сбор данных с технологических установок и их передача по однонаправленному каналу через диод данных в подразделения мониторинга, планирования и контроля
- Реализована передача дополнительных данных для руководства и заинтересованных сотрудников в корпоративном сегменте (дашборды, витрины, отчеты)

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Нефтегазодобыча

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача технологических данных в головной офис - из более доверенного в менее доверенный сетевой сегмент

ОТРАСЛЬ

НЕФТЕГАЗ

ЦЕЛЬ

Обеспечить передачу пром. протоколов различных версий из технологического (защищаемого) сегмента внешним потребителям в целях централизованного мониторинга и контроля состояния

РЕШЕНИЕ

Совместное применение продуктов InfoDiode SMART, InfoDiode PRO и дополнительных коннекторов промышленных протоколов (при необходимости)

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с источником промышленного трафика с возможностью передачи данных внешним потребителям

О компании

Международная компания - одна из ведущих в мире в сфере добычи и переработки минеральных ресурсов с интегрированными добывающими, перерабатывающими, энергетическими и логистическими предприятиями

Вызовы в области информационной безопасности

Кибератака на объект и проникновение злоумышленника через типовые средства защиты могут привести к повреждению данных и серверов приложений в сегменте АСУ ТП, что приведёт к нарушениям технологических процессов. В результате компания, как минимум, вынуждена будет отключить соединение сегмента АСУ ТП с корпоративным сегментом и Интернет.

Наличие воздушного зазора хотя и предотвращает кибератаку на защищенный сегмент, но не позволяет обеспечить непрерывность бизнес-процессов и сторонний мониторинг технологических сегментов предприятий нефтегазовой компании.

Применяемый продукт

АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

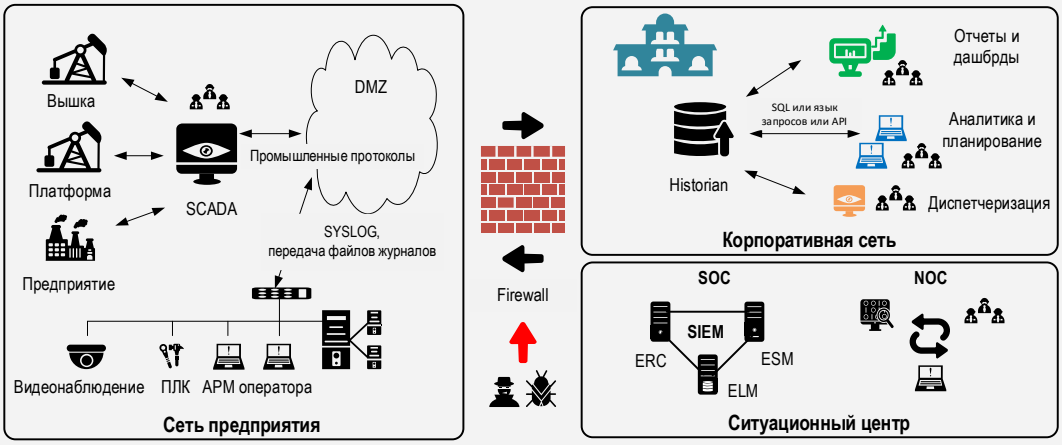
АПК InfoDiode PRO обеспечивает передачу файловых потоков (журналов, дистрибутивов, бэкапов баз данных, электронной почты), видео и UDP, Syslog, SPAN и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя защищаемый сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно передавать данные с объектов технологического сегмента в центры мониторинга, оперативной аналитики и планирования
- Обеспечить централизованный мониторинг безопасности и производительности технологической сети
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для ситуационных центров и центров SOC/NOC

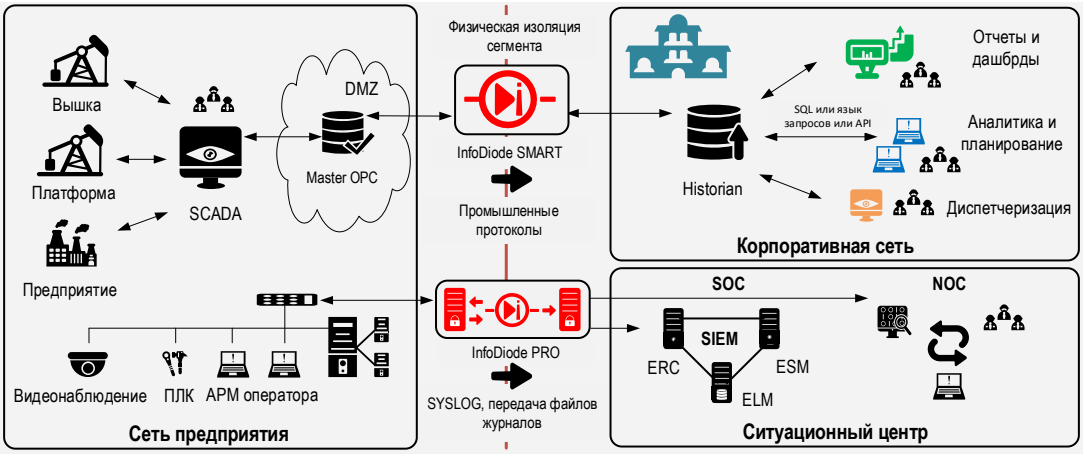
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети. Выполнено физическое отделение технологической сети от корпоративной и других, менее доверенных сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализован сбор данных с оборудования и их передача по однонаправленному каналу через диод данных в ситуационный и диспетчерский центры
- Реализована передача дополнительных данных для руководства и заинтересованных сотрудников в корпоративном сегменте (дашборды, витрины, отчеты)
- Обеспечена оперативная передача данных о безопасности и производительности технологического сегмента сети в центры мониторинга SOC/NOC

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Добыча газа

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача данных для мониторинга производственной инфраструктуры в менее доверенный сетевой сегмент

ОТРАСЛЬ

ДОБЫЧА, ТРАНСПОРТИРОВКА ГАЗА

ЦЕЛЬ

Обеспечить передачу промышленных протоколов из технологического (защищаемого) сегмента объектов добычи и транспортировки в иные сегменты для решения задач мониторинга производства

РЕШЕНИЕ

Совместное применение комплекса продуктов MasterOPC, InfoDiode SMART

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента/ объектов с источниками данных с сохранением возможности передачи данных внешним потребителям

О компании

Международная компания по добыче газа с объектами добычи, переработки и транспортировки газа

Вызовы в области информационной безопасности

В результате кибератаки могут существенно пострадать данные и серверы приложений как конечных объектов, так и промежуточных точек сбора данных, что приведёт к существенным нарушениям технологических процессов. В результате таких действий компания, как минимум, будет вынуждена отключить передачу данных из сегмента АСУ ТП в корпоративный сегмент и в глобальную сеть Интернет.

Несмотря на то, что разрыв соединения хотя и предотвратит дальнейшее распространение кибератаки, это приведёт к нарушениям непрерывности бизнес-процессов и мониторинга технологического сегмента.

Применяемый продукт

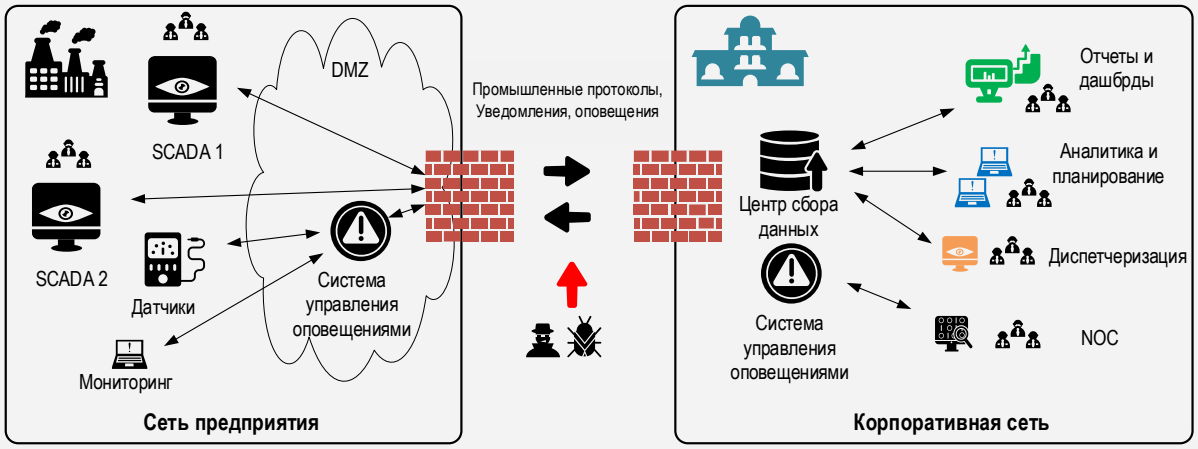
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно получать данные с объектов добычи, транспортировки, промежуточных центров мониторинга, направлять их в централизованные центры мониторинга и оповещения
- Обеспечить централизованный мониторинг сообщений о производительности технологической сети
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для внешний потребителей, центров NOC и других служб

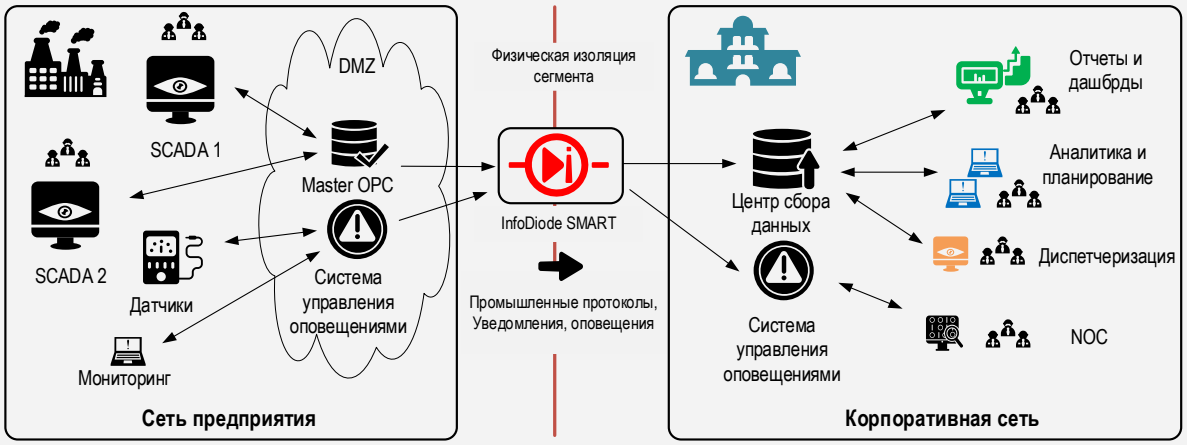
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети. Выполнено физическое отделение технологической сети от других, менее доверенных сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализован сбор данных с объектов добычи, транспортировки, промежуточных центров мониторинга и их передача по однонаправленному каналу через диод данных в центр планирования и мониторинга с обеспечением высокой производительности передачи данных
- Реализована передача дополнительных данных для руководства и заинтересованных сотрудников в корпоративном сегменте (дашборды, витрины, отчеты)
- Обеспечена передача оповещений от устройств технологической сети пользователям в иные сетевые сегменты

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Добыча полезных ископаемых

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача данных с добывающего оборудования и смежных систем в менее доверенный сетевой сегмент

ОТРАСЛЬ

ГОРНОДОБЫВАЮЩАЯ ПРОМЫШЛЕННОСТЬ

ЦЕЛЬ

Обеспечить передачу промышленных протоколов из технологического (защищаемого) сегмента объектов добычи в иные сегменты для решения задач мониторинга и планирования

РЕШЕНИЕ

Совместное применение комплекса продуктов Master OPC, InfoDiode SMART, Aveva/Wonderware Historian

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента горнодобывающего объекта с источниками данных с сохранением возможности передачи данных внешним потребителям

О компании

Крупная международная компания по добыче и переработке полезных ископаемых

Вызовы в области информационной безопасности

В результате кибератаки могут существенно пострадать данные и серверы приложений как конечных объектов, так и промежуточных точек сбора данных добывающего предприятия, что приведёт к существенным нарушениям технологических процессов. В результате таких действий компания, как минимум, вынуждена будет отключить передачу данных из сегмента АСУ ТП в корпоративный сегмент и в глобальную сеть Интернет, а также остановить производственные процессы. Что, в свою очередь, неизбежно приведет и к финансовым, и к репутационным потерям.

Применяемый продукт

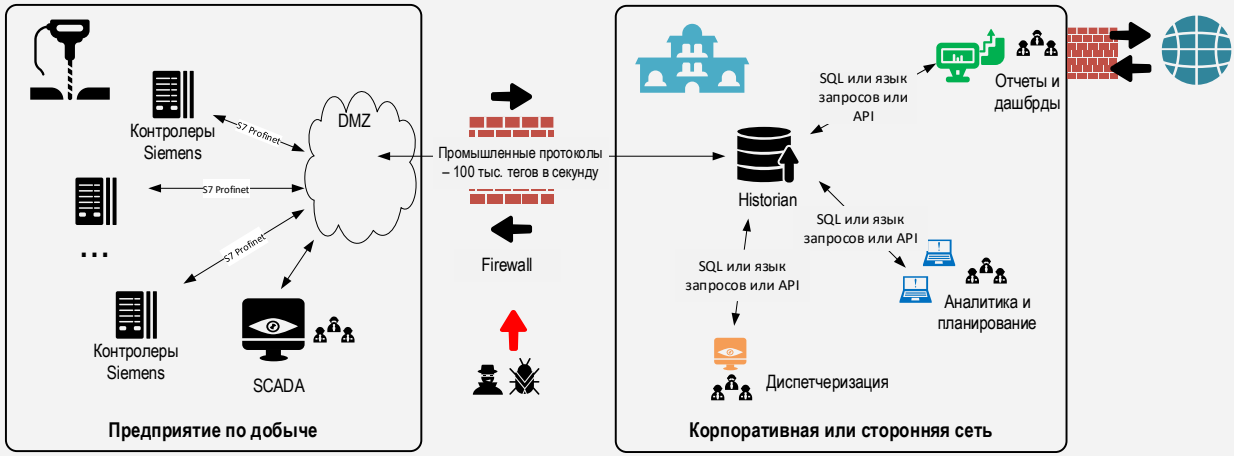
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно получать данные с объектов добычи, направлять их в единое хранилище Historian в корпоративной сети для последующей обработки и анализа, передачи в прочие информационные системы
- Обеспечить централизованный мониторинг серверов SCADA и OPC-серверов обогатительной фабрики
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные

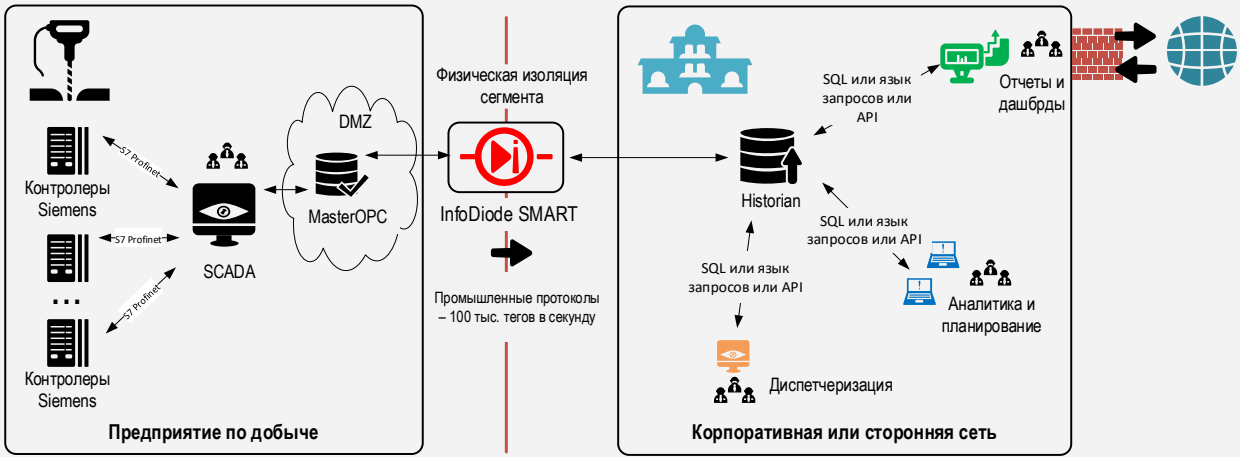
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети. Выполнено физическое отделение технологической сети от других, менее доверенных сегментов. Исключена возможность проникновения в технологический сегмент и распространение вредоносных программ
- Реализован сбор данных с объектов добычи и их передача по однонаправленному каналу через диод данных в единое хранилище Historian в корпоративной сети
- Реализована передача дополнительных данных для руководства и заинтересованных сотрудников в корпоративном сегменте (дашборды, витрины, отчеты)
- Обеспечена передача оповещений от устройств технологической сети пользователям в иные сетевые сегменты

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Добыча полезных ископаемых

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача данных технологической сети горно-обогатительного комбината (ГОК) в менее доверенный сетевой сегмент

ОТРАСЛЬ

ГОРНОДОБЫВАЮЩАЯ ПРОМЫШЛЕННОСТЬ

ЦЕЛЬ

Обеспечить передачу промышленных протоколов и файлов из технологического (защищаемого) сегмента объектов добычи в иные сегменты для решения задач мониторинга и планирования

РЕШЕНИЕ

Совместное применение комплекса продуктов InfoDiode с MasterSCADA или Альфа платформа

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента горнодобывающего объекта с источниками данных с сохранением возможности передачи данных внешним потребителям

О компании

Компания по добыче и переработке полезных ископаемых

Вызовы в области информационной безопасности

В результате кибератаки могут существенно пострадать данные и серверы приложений как конечных объектов, так и промежуточных точек сбора данных горно-обогатительного предприятия, что приведёт к существенным нарушениям технологических процессов. В результате таких действий компания, как минимум, вынуждена будет отключить передачу данных из сегмента АСУ ТП в корпоративный сегмент и в глобальную сеть Интернет, а также остановить производственные процессы. Что, в свою очередь, неизбежно приведет и к финансовым, и к репутационным потерям.

Применяемый продукт

АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

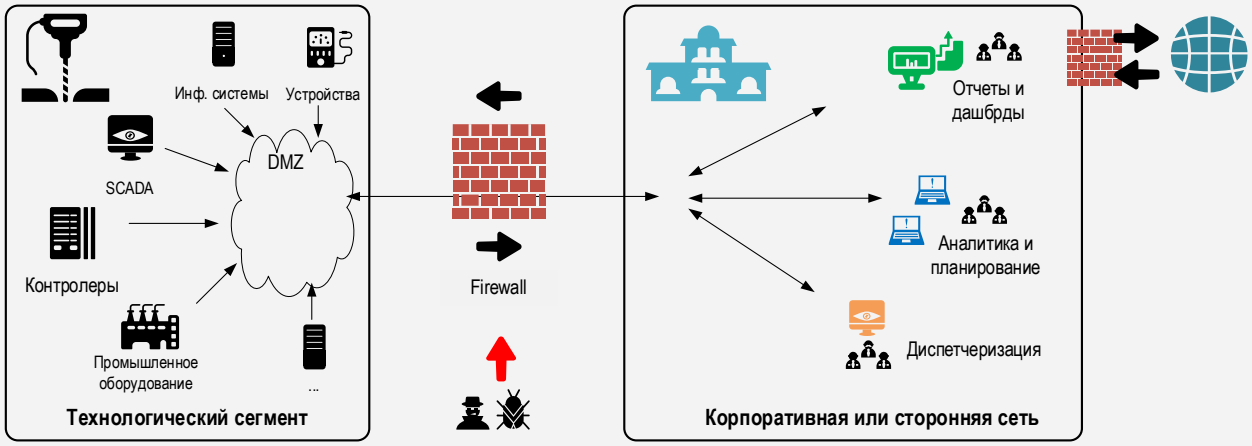
АПК InfoDiode PRO обеспечивает передачу файловых потоков (журналов, дистрибутивов, бэкапов баз данных, электронной почты), видео и UDP, Syslog, SPAN и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя защищаемый сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно получать данные с объектов переработки, направлять их в корпоративную сеть для последующей обработки и анализа, передачи в прочие информационные системы
- Обеспечить мониторинг серверов SCADA обогатительной фабрики и SCADA ее технологических участков
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные

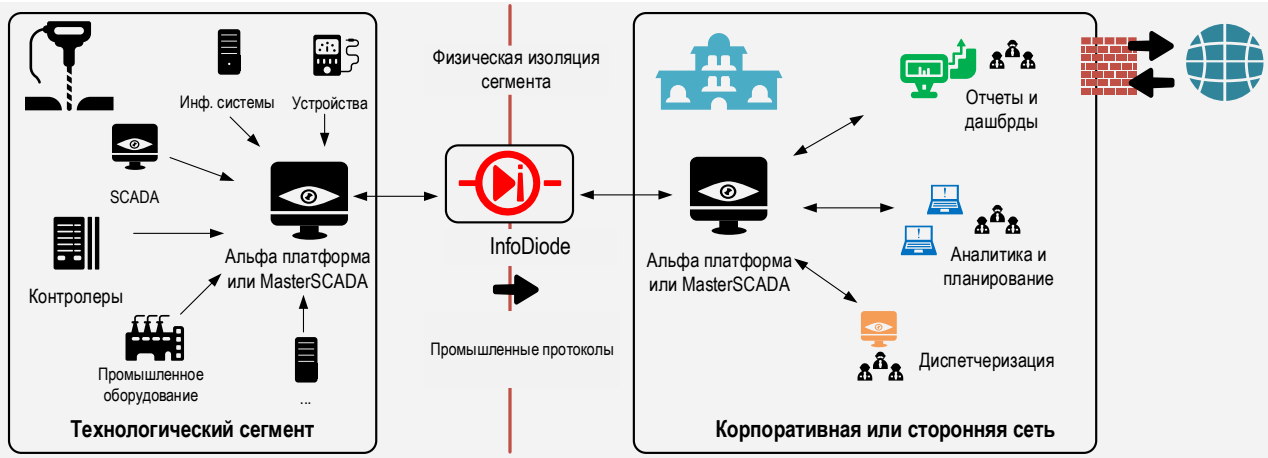
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети. Выполнено физическое отделение технологической сети от других, менее доверенных сегментов. Исключена возможность проникновения в технологический сегмент и распространение вредоносных программ
- Реализован сбор данных с объектов добычи и их передача по однонаправленному каналу через диод данных в корпоративную сеть
- Реализована передача дополнительных данных для руководства и заинтересованных сотрудников в корпоративном сегменте (файлы, дашборды, витрины, отчеты)
- Обеспечена передача оповещений от устройств технологической сети пользователям в иные сетевые сегменты

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Банки, финансовые организации

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача критичных данных в целях резервного копирования во внешнее хранилище

ОТРАСЛЬ

БАНКИ, ФИНАНСЫ

ЦЕЛЬ

Обеспечить регулярное резервное копирование информации из сети банка в защищенное хранилище.

РЕШЕНИЕ

Применение аппаратно–программного комплекса InfoDiode PRO для создания изолированного сетевого сегмента, защищенного от внешнего воздействия

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) сетевого сегмента для хранения бэкапов систем, «снимков данных», резервных копий данных.

О компании

Крупная финансовая организация из топ - 15.

Вызовы в области информационной безопасности

Устойчивое функционирование бизнес-процессов финансовой организации зависит, в том числе, и от наличия надежно функционирующей системы резервного копирования. В то же время, внешние соединения с основной сетью, а также места хранения резервных копий, могут подвергаться кибератакам. В этих условиях хранение данных на обычных ресурсах (ленточное хранилище, файловое хранилище и т.п.) повышает риски утери, компрометации данных. Банку требуется организация защищенного сегмента, который позволит сохранять эталонные копии данных для наиболее рискованных сценариев их потери, в том числе в результате действий злоумышленников.

Применяемый продукт

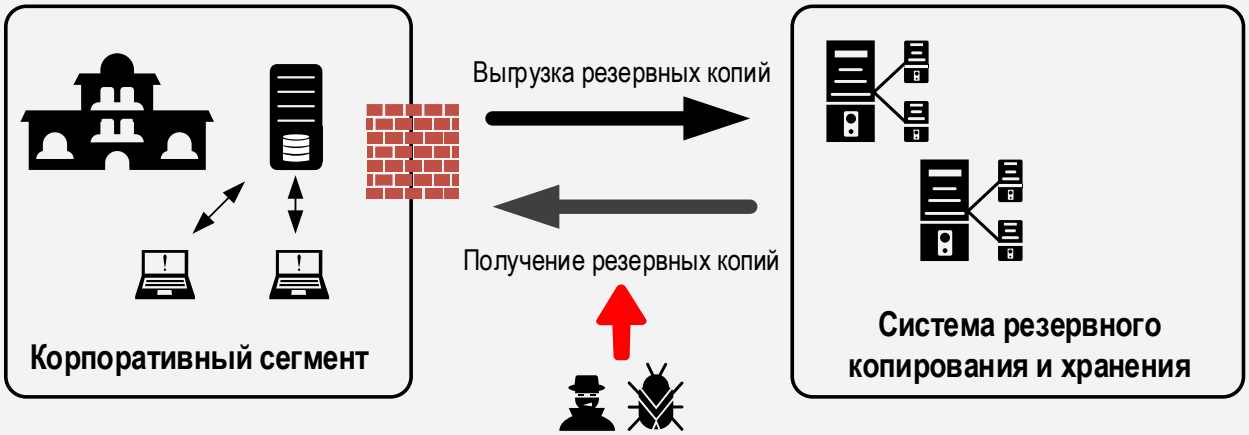
АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно передавать данные бэкапов на защищенный ресурс для целей гарантированного изолированного хранения резервных копий, «снимков данных», эталонных копий данных и систем
- Гарантированно исключить воздействие на защищенный сегмент, сделав невозможной организацию атаки по тому же каналу, по которому данные передаются на хранение

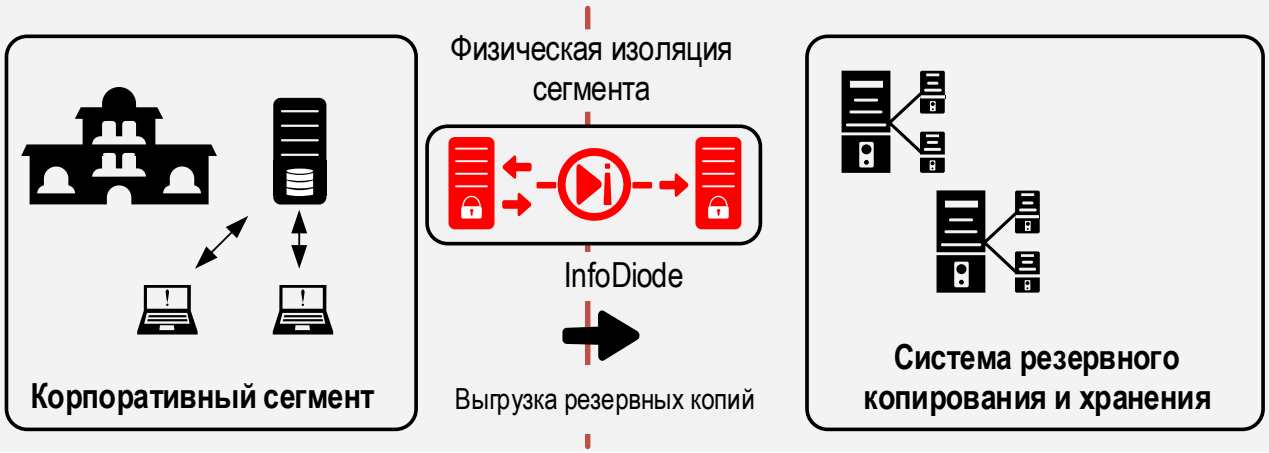
Архитектура: ДО



Результаты

- Выполнено физическое отделение защищенного сегмента от менее доверенных сегментов. Исключена возможность проникновения злоумышленника в сегмент хранения данных и распространения (запуска) в нем вредоносных программ
- Обеспечена однонаправленная передача данных на внешнее защищенное хранилище, исключающая возможность воздействия на систему хранения бэкапов и резервируемые данные
- Обеспечена непрерывность бизнес процессов финансовой организации благодаря организации строго детерминированного однонаправленного потока данных на внешний по отношению к корпоративной сети защищенный ресурс, снижены риски полной утери данных в случае успешной атаки злоумышленника на основной сегмент данных банка

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Оказание технической поддержки клиентам через мессенджеры и иные каналы коммуникаций

ОТРАСЛЬ

БАНКИ, ФИНАНСЫ

ЦЕЛЬ

Обеспечить взаимодействие операторов с клиентами посредством мессенджеров

РЕШЕНИЕ

Совместное применение двух аппаратно–программных комплексов InfoDiode PRO и решений Naumen для защиты сегмента с источником чувствительных данных

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) внутренней сети организации с возможностью получения и отправки сообщений через различные инструменты коммуникации с клиентом

О компании

Крупный банк из топ - 20. Контакт-центр банка использует данные, в том числе персональные, из защищенного сегмента.

Вызовы в области информационной безопасности

Взаимодействие с клиентами требует применения современных способов коммуникации и многоканальности (например, соцсетей, мессенджеров, эл. почты и т.п.) как для поддержки клиентов, так и для сопровождения основных процессов обслуживания и продаж. Отдел информационной безопасности считает, что использование файрволов более не гарантирует надлежащий уровень защиты от киберугроз. Организации требуется повысить уровень безопасности внутреннего сегмента сети, сохранив при этом возможность в режиме онлайн обрабатывать запросы от клиентов, полученные посредством различных каналов.

Применяемый продукт

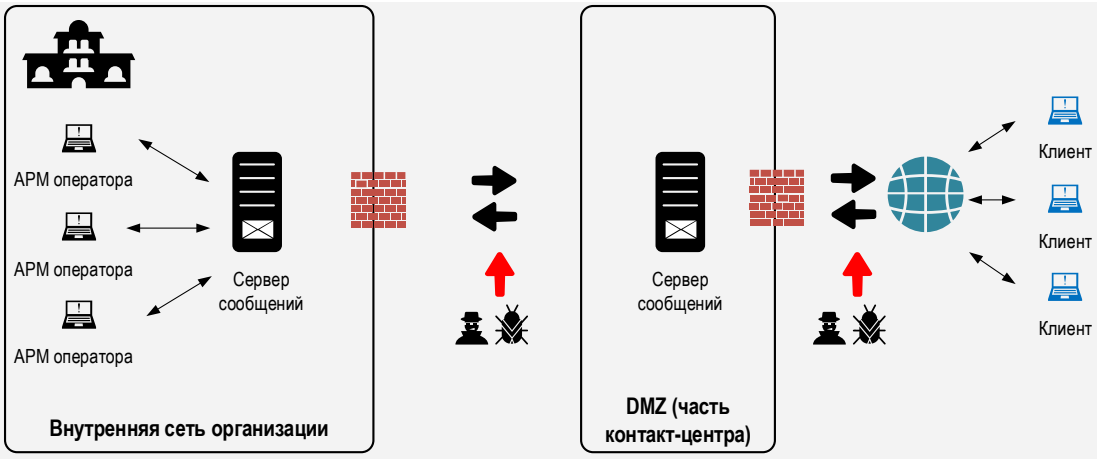
АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя этот сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Обеспечить защиту периметра, содержащего системы, базы данных, хранилища персональных и чувствительных данных посредством организации раздельных аппаратных однонаправленных каналов обмена сообщениями
- Гарантированно исключить внешние подключения, сделав невозможной утечку, порчу, компрометацию данных по каналам обмена информацией

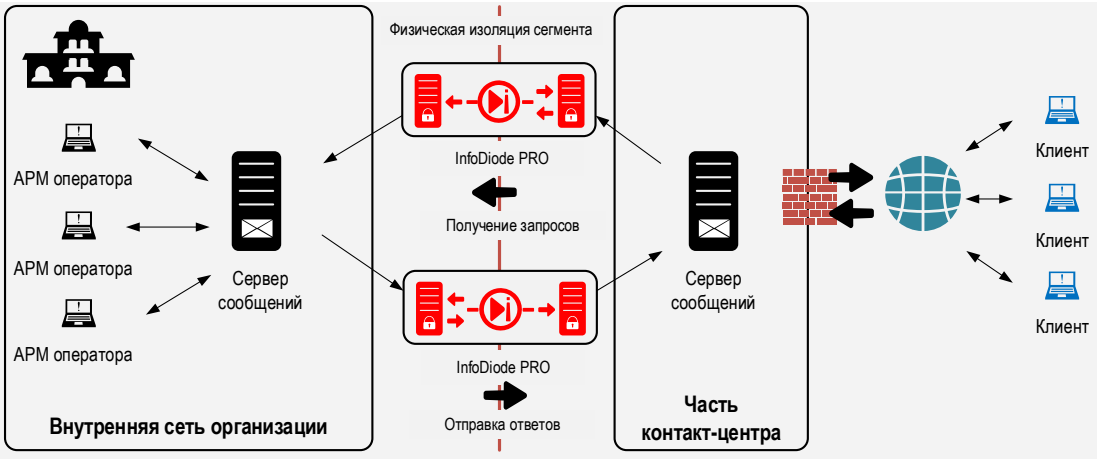
Архитектура: ДО



Результаты

- Выполнено физическое отделение внутренней сети организации от сегмента DMZ, в котором расположен прокси-сервер сообщений контакт-центра.
- Обеспечен обмен данными с клиентами специалистов контакт-центра, направленная передача обращений внутрь сети организации, исключающая утечку данных
- Обеспечена направленная передача ответов специалистов контакт-центра во внешний сегмент, исключающая воздействие на бизнес-процессы банка и распространение вредоносных программ
- Обеспечена непрерывность бизнес-процессов благодаря организации строго детерминированных взаимно однонаправленных потоков данных и контроль за каналами взаимодействия с недоверенными источниками данных

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Финансовые организации, SOC

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача данных в лабораторию ИБ в составе SOC для изоляции и последующего анализа на предмет наличия вредоносного кода

ОТРАСЛЬ

БАНКИ, ФИНАНСЫ

ЦЕЛЬ

Обеспечить передачу образов виртуальных машин и ПО, подозрительных файлов из сети организации в лабораторию информационной безопасности SOC или стороннего подрядчика

РЕШЕНИЕ

Применение аппаратно–программного комплекса InfoDiode PRO для защиты от утечек из лаборатории по каналу связи

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) сегмента сети лаборатории от утечек во внешние сети с возможностью передачи образов анализируемых систем во внутреннюю сеть лаборатории

О компании

Финансовая организация регионального уровня с филиальной структурой. Предприятие имеет сегмент SOC, включающий ИБ лабораторию.

Вызовы в области информационной безопасности

Лаборатория информационной безопасности отвечает за анализ нового и функционирующего программного обеспечения на наличие угроз кибербезопасности. В «песочнице» лаборатории могут быть развёрнуты заражённые информационные системы, которые могут представлять угрозу «общей сети» ИТ-инфраструктуры при пересечении периметра сегмента сети лаборатории. Необходимо предотвратить любую возможность негативного воздействия на внешние сегменты сети, сохраняя при этом канал связи для передачи данных в лабораторию информационной безопасности.

Применяемый продукт

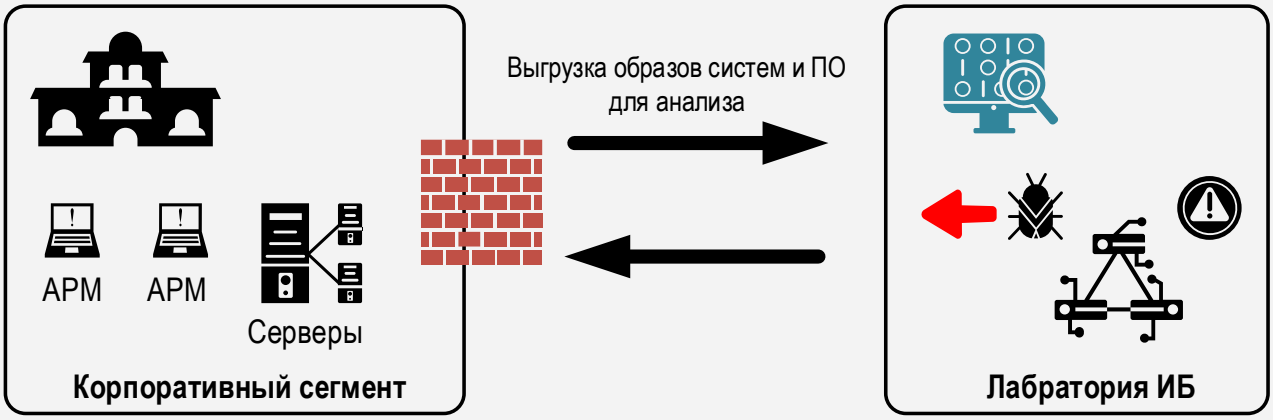
АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя этот сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно передавать данные из внешних сегментов сети в сеть лаборатории для анализа
- Гарантированно исключить утечки из сегмента сети лаборатории и их воздействие на корпоративный сегмент, сделав невозможным распространение киберугроз в «общей сети» организации и в ИТ-инфраструктуре организации

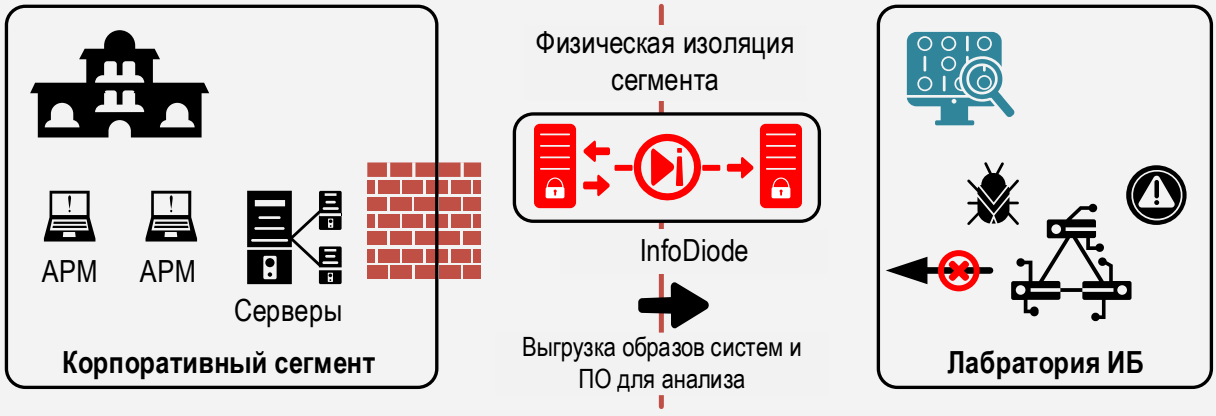
Архитектура: ДО



Результаты

- Выполнено физическое отделение сегмента сети ИБ лаборатории от иных сетей организации. Исключена возможность проникновения и распространения вредоносных программ из «песочницы» ИБ лаборатории
- Обеспечена однонаправленная передача данных в сегмент сети лаборатории, исключающая исходящие соединения в корпоративный сегмент
- Реализована возможность безопасного тестирования, направленного на диагностику и изучение ПО и дистрибутивов, исключая возможность обратного воздействия (в том числе непреднамеренного) на сеть-источник

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

ЖКХ, водоснабжение

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Осуществление удалённого мониторинга состояния очистных сооружений и станций водоподготовки

ОТРАСЛЬ

ВОДООЧИСТКА, ВОДОПОДГОТОВКА

ЦЕЛЬ

Обеспечить передачу оповещений и видеопотока с объекта в центр мониторинга и обеспечения безопасности

РЕШЕНИЕ

Применение аппаратно–программного комплекса InfoDiode PRO для защиты периметра технологического сегмента сети

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента сети от любого внешнего воздействия с возможностью передачи оповещений и видеопотока для целей мониторинга

О компании

Государственное унитарное предприятие, занимающееся очисткой и подготовкой воды для последующего использования потребителями

Вызовы в области информационной безопасности

Станции водоочистки и водоподготовки являются не только критически важными объектами инфраструктуры, но и потенциально могут представлять техногенную опасность. Обеспечение их постоянного мониторинга, в том числе удаленными диспетчерскими службами, органами управления и ситуационными центрами, является необходимым. В то же время нельзя допускать внешних воздействий на технологическую сеть самого объекта мониторинга, поскольку это может привести к существенным последствиям как для потребителей, так для и окружающей среды.

Применяемый продукт

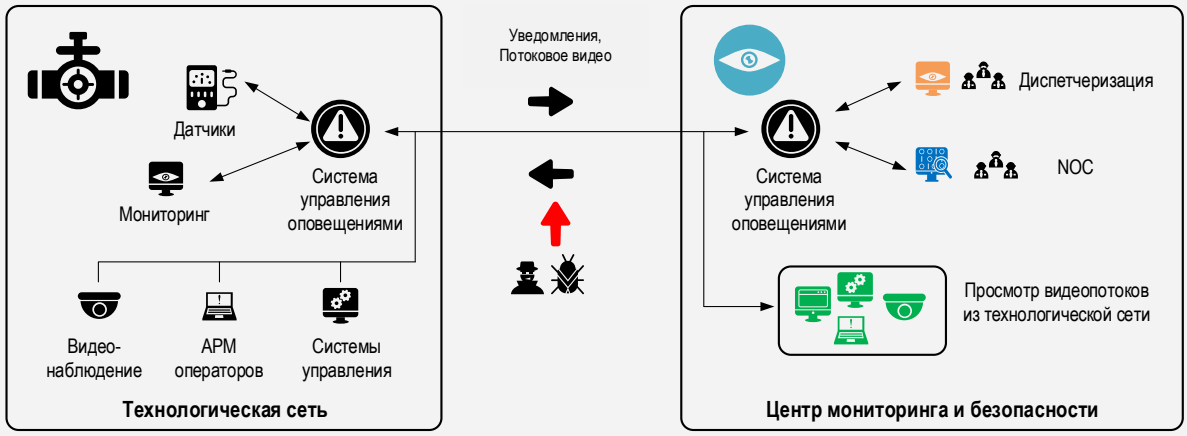
АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя этот сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно передавать уведомления о состоянии оборудования и технологической сети в центр мониторинга
- Обеспечить передачу видеопотока (с мониторов и видеокамер) с объекта КИИ в центр мониторинга
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможным распространение киберугроз на объект КИИ

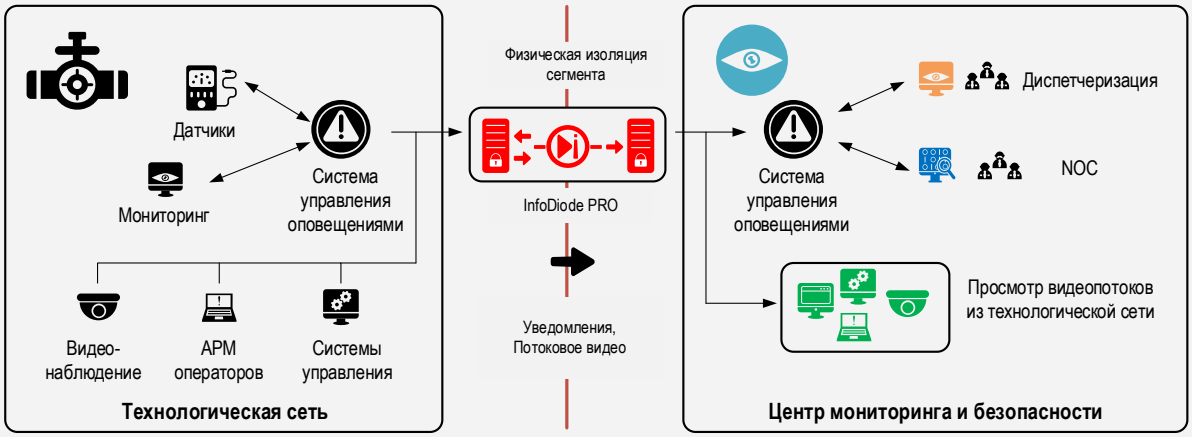
Архитектура: ДО



Результаты

- Выполнено физическое отделение сегмента технологической сети от внешних сетей. Исключена возможность воздействия на оборудование и распространения вредоносных программ в технологической сети
- Обеспечена направленная передача данных в центр мониторинга и безопасности, исключающая любые входящие соединения в технологический сегмент
- Обеспечена передача потока оповещений от устройств технологической сети пользователям в удалённом центре мониторинга
- Обеспечена передача потокового видео с контрольных мониторов и устройств видеонаблюдения в удалённый центр мониторинга и безопасности

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Осуществление удалённого сбора данных с приборов учёта и мониторинг состояния объектов коммунального хозяйства

ОТРАСЛЬ

ЖКХ

ЦЕЛЬ

Обеспечить передачу показаний приборов учёта, датчиков и видеопотока с объекта ЖКХ в центр мониторинга и обеспечения безопасности

РЕШЕНИЕ

Применение аппаратно–программного комплекса АПК InfoDiode для защиты периметра технологического сегмента сети

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента сети от любого внешнего воздействия с возможностью передачи показаний приборов учёта и датчиков, а также видеопотока для целей мониторинга

О компании

Управляющая компания, обслуживающая значительное количество объектов ЖКХ

Вызовы в области информационной безопасности

Обслуживание объектов ЖКХ требует как постоянного мониторинга различных систем (лифтовое хозяйство, пожарная охрана, защита от протечек и т.д.), так и регулярного сбора показаний приборов учёта для расчётов с потребителями и поставщиками. В то же время нельзя допускать внешних воздействий на технологическую сеть объекта, поскольку это может привести к существенным последствиям для потребителей, вплоть до угрозы жизни и здоровью, а также влиять на взаиморасчёты с поставщиками и потребителями коммунальных ресурсов.

Применяемый продукт

АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

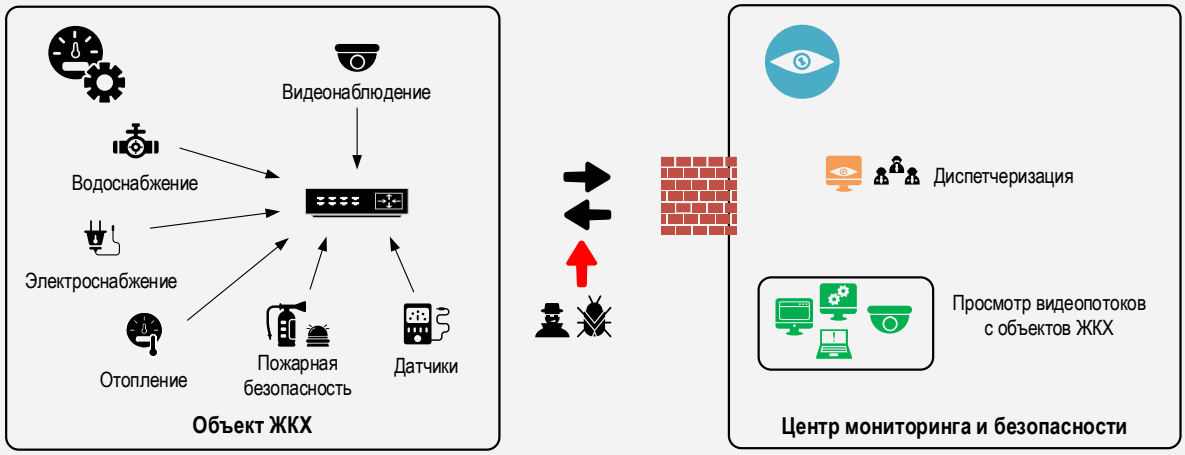
АПК InfoDiode PRO обеспечивает передачу файловых потоков (журналов, дистрибутивов, бэкапов баз данных, электронной почты), видео и UDP, Syslog, SPAN и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя защищаемый сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно передавать показания приборов учёта и датчиков с объектов ЖКХ в центр мониторинга
- Обеспечить передачу видеопотока (с мониторов и видеокамер) с объекта ЖКХ в центр мониторинга
- Гарантированно исключить воздействие на оборудование объекта ЖКХ

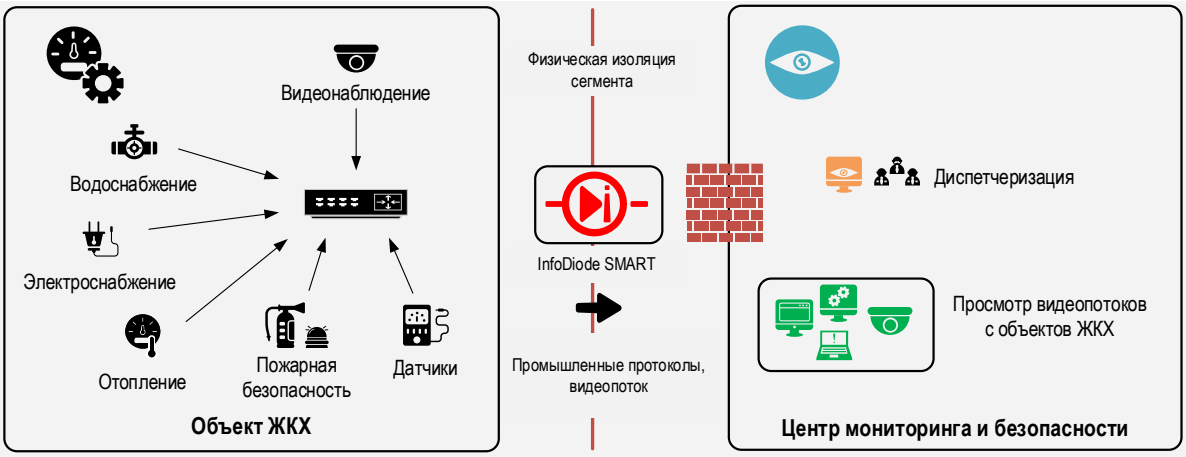
Архитектура: ДО



Результаты

- Выполнено физическое отделение технологического сегмента сети объекта ЖКХ от внешних сетей. Исключена возможность воздействия на оборудование и приборы учёта
- Обеспечена направленная передача данных в центр мониторинга и безопасности, исключающая любые входящие соединения в технологический сегмент объекта ЖКХ
- Обеспечена передача показаний приборов учёта и датчиков с объектов ЖКХ в удалённый центр мониторинга
- Обеспечена передача потокового видео в реальном времени с контрольных мониторов и устройств видеонаблюдения удалённом центре мониторинга и безопасности

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Здравоохранение, перс. данные

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Предоставление доступа к клиническим исследованиям сторонней организации

ОТРАСЛЬ

ЗДРАВООХРАНЕНИЕ, ИССЛЕДОВАНИЯ

ЦЕЛЬ

Обеспечить передачу данных пациентов (в т.ч деперсонифицированных) из клинической больницы сторонним потребителям. Защитить перс. данные и медицинские системы от кибератаки

РЕШЕНИЕ

Применение аппаратно–программного комплекса InfoDiode PRO для предотвращения прямого доступа к персональным данным пациентов

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) сети медицинского учреждения от любого внешнего воздействия с возможностью передачи обезличенных данных в сеть стороннего потребителя

О компании

Крупное медицинское учреждение, медицинский центр

Вызовы в области информационной безопасности

Медицинская информационная система (МИС) содержит информацию о пациентах, которая представляет собой врачебную тайну и, в том числе, относится к персональным данным. Доступ к информации о пациенте в МИС предоставляется только лечащему врачу и авторизованному персоналу медучреждения. В то же время сторонние организации (исследовательские центры, страховые компании и т.п.) нуждаются в этих данных и используют доступ напрямую к МИС без значимых ограничений. Требуется обеспечить ограниченный доступ к персональной информации пациентов, МИС и другим медицинским системам в соответствии с требованиями законодательства.

Применяемый продукт

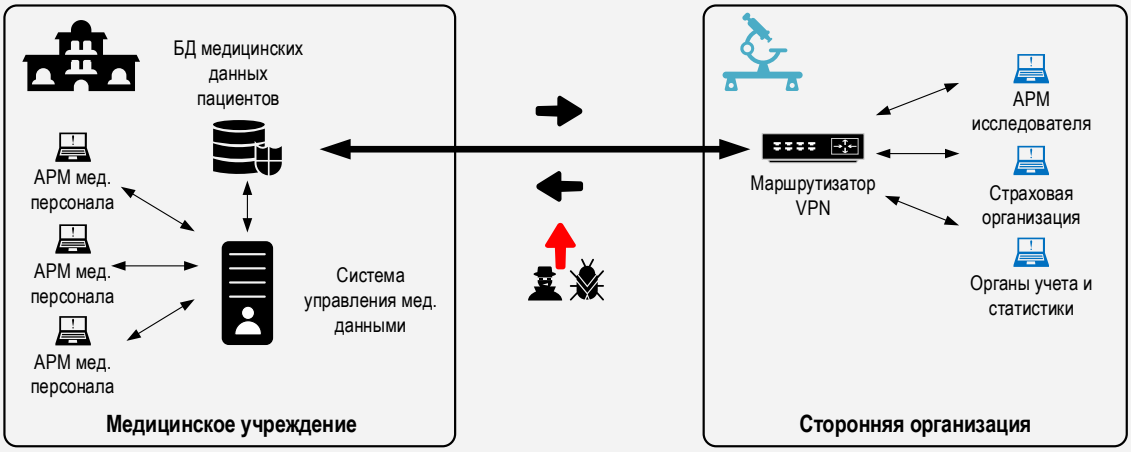
АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя этот сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Обеспечить доступ сторонним организациям статистики и учета к обезличенным данным медицинских записей
- Сохранить доступ к данным для сотрудников мед. учреждения через МИС в прежнем объёме
- Гарантированно исключить воздействие на сеть медицинского учреждения, сделав невозможным изменение медицинских данных, утечку персональных данных пациентов, повреждение МИС и оборудования

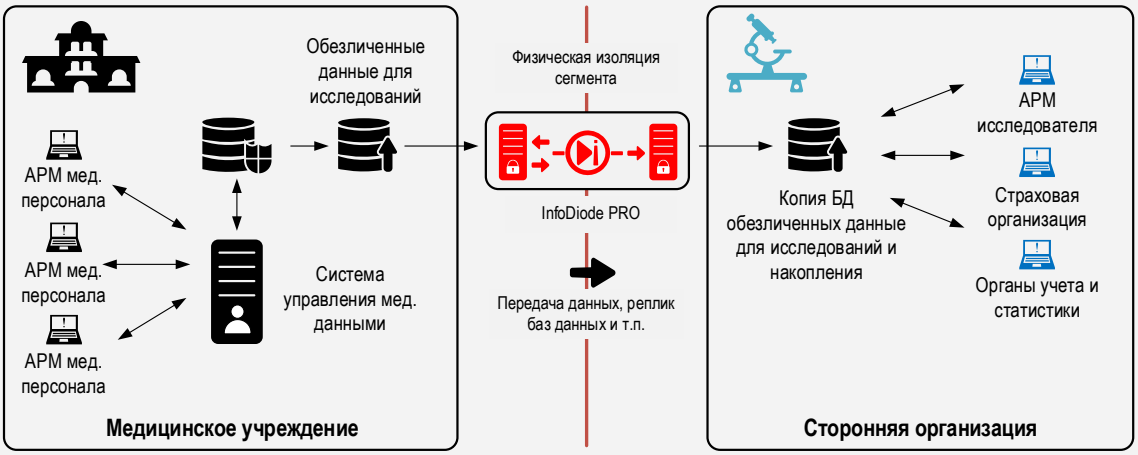
Архитектура: ДО



Результаты

- Выполнено физическое отделение сегмента сети медицинского учреждения от внешних сетей - потребителей информации. Исключена возможность воздействия на базу медицинских записей и неограниченного доступа к ним извне
- Обеспечено соответствие требованиям законодательства по ограничению доступа к чувствительной информации (персональным данным, данным врачебной тайны) и ее защите
- Обеспечен доступ исследовательского персонала, образовательных учреждений и органов статистики к обезличенным медицинским данным для проведения научных изысканий

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Предоставление клиентам ЦОД, покупающим услуги IaaS, данные сети управления о работе серверов и сетевого оборудования с целью мониторинга

ОТРАСЛЬ

ДАТА-ЦЕНТРЫ

ЦЕЛЬ

Обеспечить передачу данных из закрытой сети управления ЦОД для мониторинга оборудования, серверов и сервисов в SOC и NOC клиентов, приобретающих услуги ЦОД на принципах SaaS и IaaS

РЕШЕНИЕ

Применение аппаратно–программного комплекса InfoDiode PRO для предотвращения прямого доступа к сети управления ЦОД

ПРЕИМУЩЕСТВА

Защита на физическом уровне сети управления ЦОД от внешнего воздействия с возможностью передачи данных о состоянии инфраструктуры в центры мониторинга, диспетчерские, клиентам

О компании

Компания - владелец нескольких ЦОД, предоставляющая услуги размещения оборудования в собственных центрах обработки данных

Вызовы в области информационной безопасности

Центры обработки данных (ЦОД) предоставляют инфраструктуру в виде услуг IaaS сторонним организациям. Некоторым из этих организаций требуется получать технологические данные из сегмента сети управления ЦОД (температура, энергопотребление, состояние серверов, сетевого оборудования и т.п.), касающиеся именно их оборудования и сервисов. Вместе с тем, для обеспечения надёжности работы инфраструктуры и предотвращения киберугроз, необходимо исключить внешнее влияние на сеть управления ЦОД.

Применяемый продукт

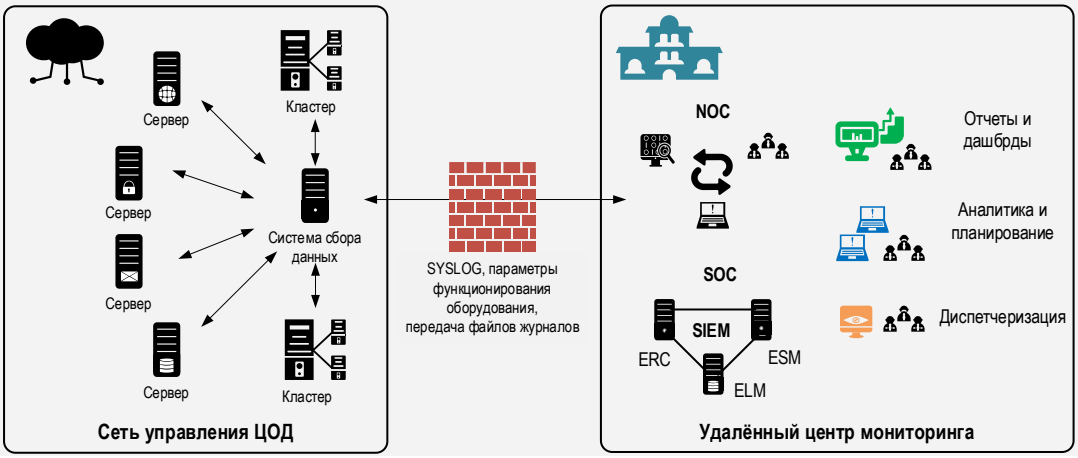
АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя этот сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Передавать данные оборудования и сервисов ЦОД в режиме онлайн - в сторонние центры мониторинга, диспетчерские службы, службы технической поддержки клиентов ЦОД. Расширить спектр услуг, предлагаемых клиентам, обеспечив удаленный и безопасный контроль за арендуемой инфраструктурой
- Гарантированно исключить воздействие на сеть управления и мониторинга ЦОД, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для внешних потребителей

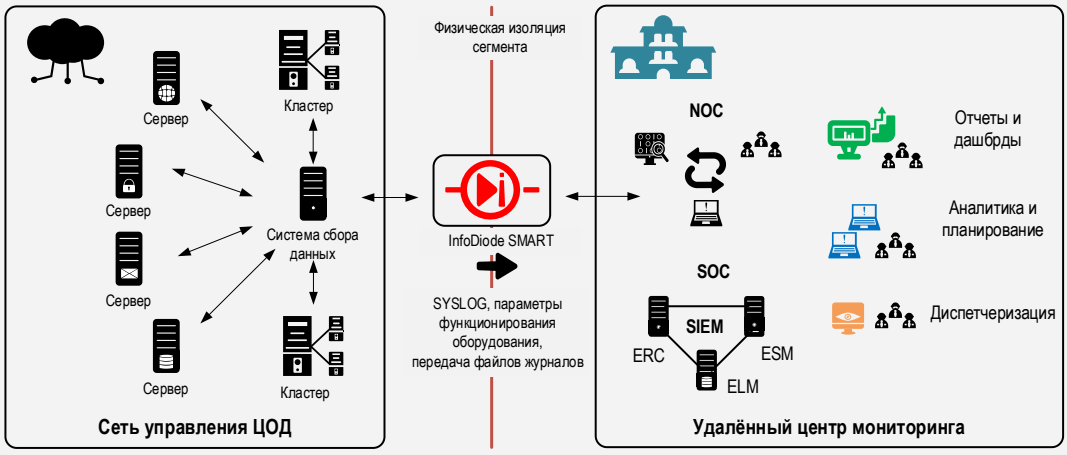
Архитектура: ДО



Результаты

- Реализован сбор данных с серверов и сетевого оборудования и их передача по однонаправленному каналу через диод данных внешним потребителям
- Существенно повышен уровень защиты сетевого периметра ЦОД за счет физического отделения сети управления и мониторинга от менее доверенных сетевых сегментов
- Исключена возможность проникновения в сегмент сети управления ЦОД и распространения вредоносных программ со стороны получателей информации о состоянии сети и оборудования ЦОД (клиентов, внешних служб ТП и т.п.)

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Агрегация в корпоративном сегменте данных с узлов управления

ОТРАСЛЬ

ТРАНСПОРТ

ЦЕЛЬ

Обеспечить передачу актуальных данных о состоянии ж/д инфраструктуры в центр управления ж/д сообщением

РЕШЕНИЕ

Применение аппаратно-программных комплексов InfoDiode для защиты периметра технологического сегмента сети

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) сегмента сети управления ж/д от любого внешнего воздействия с возможностью передачи данных мониторинга и состояния

О компании

Государственная вертикально-интегрированная компания, владелец инфраструктуры общего пользования и сети железных дорог

Вызовы в области информационной безопасности

Железные дороги являются объектом повышенной опасности. Актуальные данные о состоянии систем электроснабжения, управления ж/д переездами, текущем местоположении подвижного состава и т.п. необходимы для обеспечения безопасности перемещения пассажиров и грузов, проведения ремонтных и профилактических работ, актуализации расписания на электронных табло и в мобильных приложениях, предоставления сведений в ситуационные центры (мониторинга, SOC, NOC). Вместе с тем, необходимо обеспечить гарантированную защиту систем технологического сегмента для внешних воздействий.

Применяемый продукт

АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика.

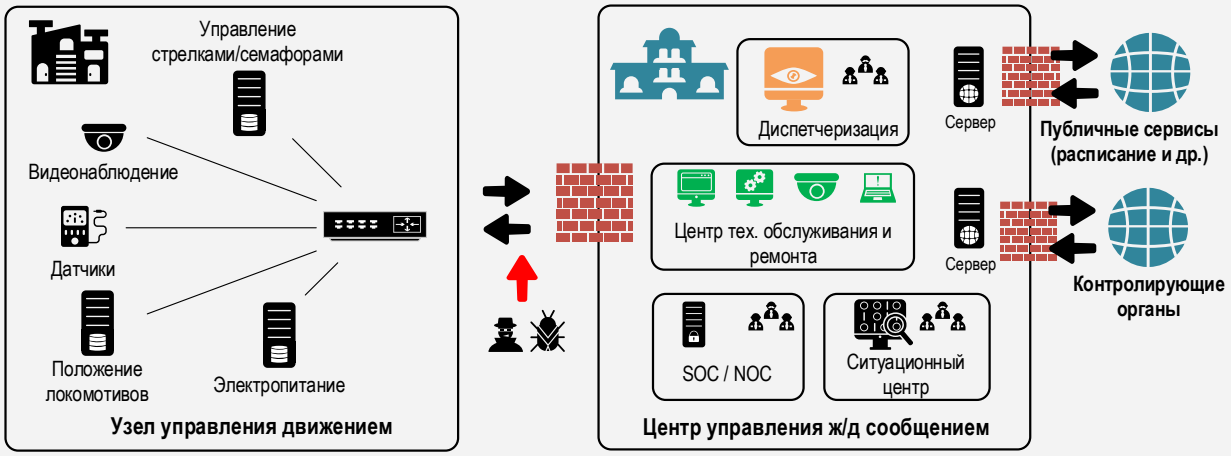
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким пром. протоколам через границу периметра. Специализированные коннекторы пром. протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их по однонаправленному каналу, обеспечив соответствие требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно передавать данные мониторинга и данные систем управления с узла управления в корпоративный сегмент
- Гарантированно исключить воздействие на ж/д инфраструктуру через канал связи, используемый для репликации данных и мониторинга

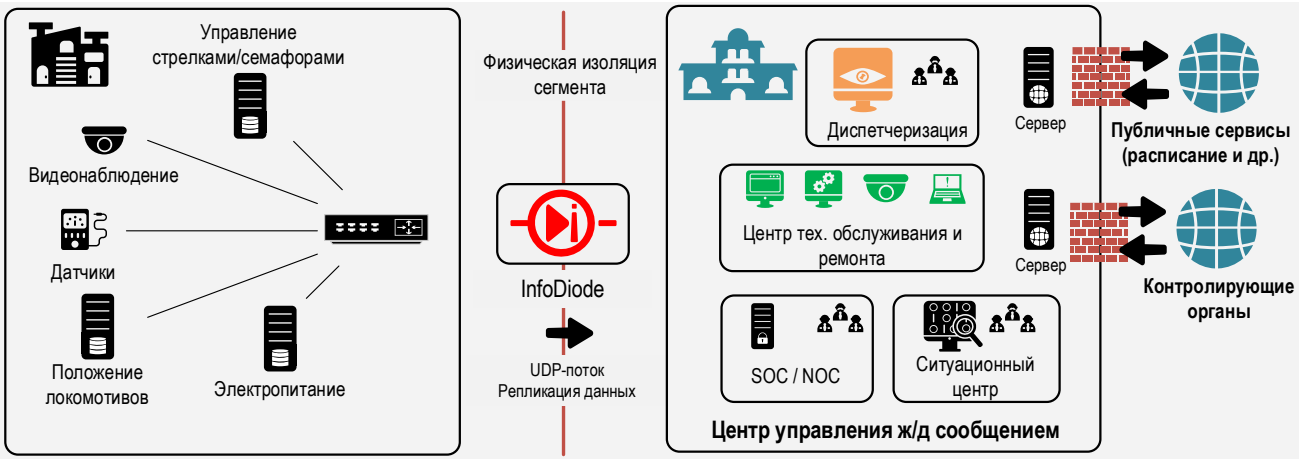
Архитектура: ДО



Результаты

- Выполнено физическое отделение сети узла управления ж/д от внешних сетей
- Исключена возможность воздействия на ж/д инфраструктуру из внешних сетей
- Исключены любые входящие соединения в технологический сегмент узла управления
- Обеспечена направленная передача данных мониторинга и репликации данных в центр управления

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Сбор данных мониторинга стрелочных переводов с местных узлов управления

ОТРАСЛЬ

ТРАНСПОРТ

ЦЕЛЬ

Обеспечить передачу показаний мониторинга стрелочных переводов в центр управления ж/д сообщением

РЕШЕНИЕ

Применение аппаратных комплексов Info-Diode для защиты периметра технологического сегмента сети

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) сегмента сети управления ж/д от любого внешнего воздействия с возможностью передачи показаний мониторинга стрелочных переводов

О компании

Государственная вертикально-интегрированная компания, владелец инфраструктуры общего пользования и сети железных дорог

Вызовы в области информационной безопасности

Железные дороги являются объектом повышенной опасности. Одними из ключевых объектов управления на железной дороге являются стрелочные переводы, некорректная работа которых может приводить к аварийным ситуациям с тяжёлыми последствиями, вплоть до смертельных. В связи с этим, необходимо осуществлять постоянный централизованный мониторинг стрелочных переводов, но, в то же время, нельзя допускать внешних воздействий на сеть управления объектами.

Применяемый продукт

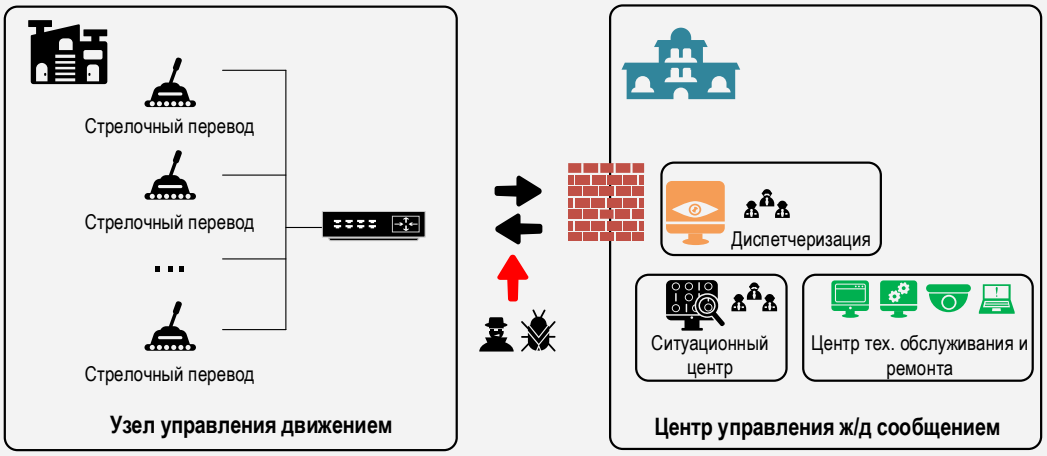
InfoDiode MINI - базовое аппаратное решение для монтажа на DIN-рейку или Desktop вариант. Обеспечивает передачу UDP, Syslog, SPAN трафика потребителям за пределами доверенного сегмента. Сертифицировано ФСТЭК УД (4). Обеспечивает защиту на аппаратном уровне, изолирует защищаемый сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно передавать данные мониторинга стрелочных переводов с узла управления в центр мониторинга
- Гарантированно исключить воздействие на стрелочные переводы через канал связи, используемый для мониторинга

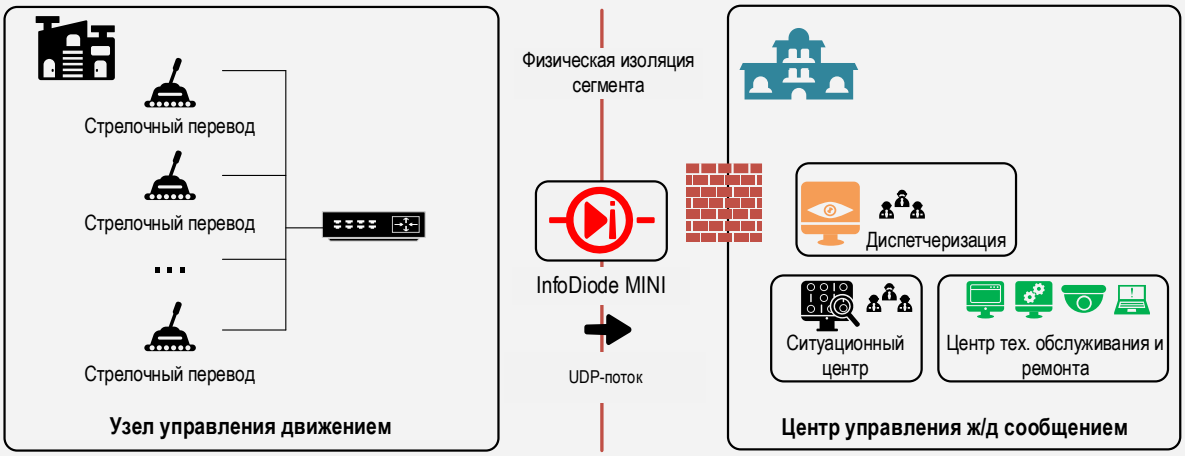
Архитектура: ДО



Результаты

- Выполнено физическое отделение сети узла управления ж/д от внешних сетей
- Исключена возможность воздействия на стрелочные переводы из внешних сетей
- Исключены любые входящие соединения в технологический сегмент узла управления
- Обеспечена направленная передача данных мониторинга стрелочных переводов в центр мониторинга

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача данных видеонаблюдения с защищаемого объекта в центр мониторинга безопасности или ситуационный центр

ОТРАСЛЬ

ИНФРАСТРУКТУРА, ОХРАНА

ЦЕЛЬ

Обеспечить безопасную передачу видео с камер наблюдения, размещенных на удалённых объектах, в единый центр мониторинга

РЕШЕНИЕ

Применение аппаратно-программного комплекса InfoDiode совместно с системой видеонаблюдения SecurOS

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) сети видеонаблюдения объекта с сохранением возможности передачи данных в единый центр мониторинга

О компании

Крупное территориально-распределённое предприятие, муниципальный и региональный ситуационный центр

Вызовы в области информационной безопасности

Система видеонаблюдения как часть общей сети объекта также может подвергаться атакам. Мотивация атаки злоумышленника может быть как прямой - выведение из строя самой системы физической безопасности объекта, так и косвенной - развитие атаки на сеть объекта с использованием камер и элементов системы видеонаблюдения как промежуточных узлов. В результате кибератаки могут существенно пострадать данные и серверы приложений организации, что приведёт к существенным угрозам безопасности на объекте. Необходимо защитить сетевой периметр средств обеспечения физической безопасности объекта, в том числе периметр системы видеонаблюдения.

Применяемый продукт

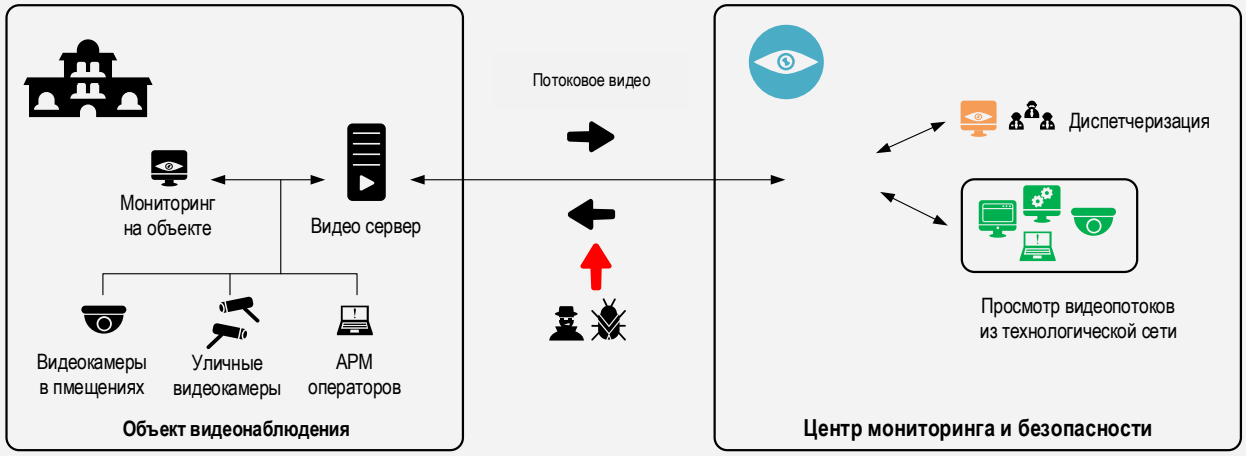
АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика за пределы доверенного сегмента целевым потребителям, изолируя этот сегмент.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- На постоянной основе передавать данные видеонаблюдения с объекта в центр мониторинга и предоставить возможность получать данные по выбранным объектам контроля
- Гарантированно исключить воздействие на информационную инфраструктуру объекта через канал связи, используемый для передачи видео внешним потребителям

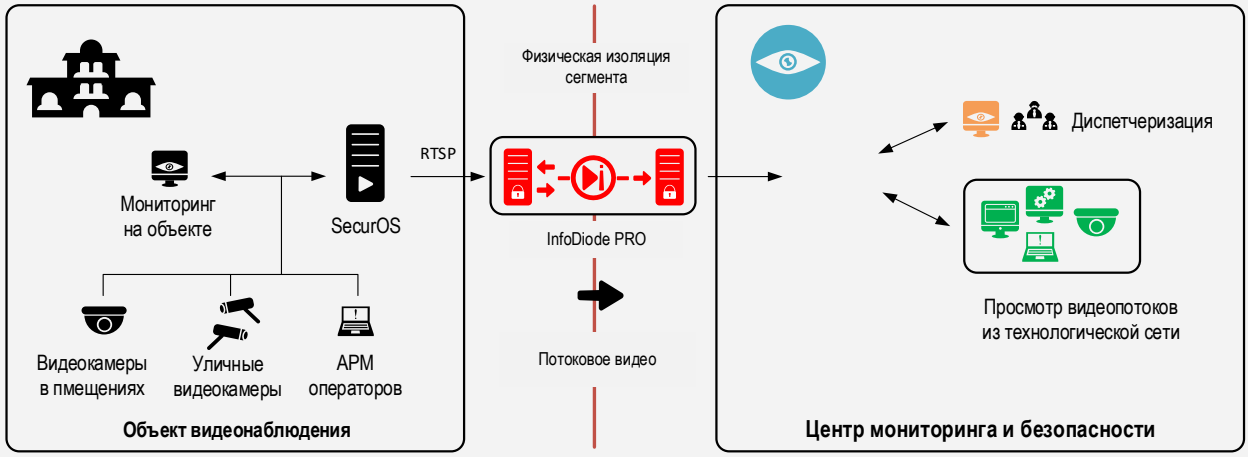
Архитектура: ДО



Результаты

- Выполнено физическое отделение сети объекта от внешних сетей
- Исключена возможность воздействия на информационную сеть объекта из внешних сетей
- Исключены любые входящие соединения в сеть видеонаблюдения объекта, исключено воздействие на сеть видеонаблюдения из менее доверенных сетевых сегментов
- Обеспечена передача данных видеонаблюдения в центр мониторинга в отношении требуемых объектов контроля

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Промышленность, энергетика, финансы

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача оповещений о киберугрозах из Deception-системы защищаемого сегмента в SOC

ОТРАСЛЬ

ПРОМЫШЛЕННОСТЬ, ЭНЕРГЕТИКА, БАНКИ

ЦЕЛЬ

Обеспечить передачу оповещений о киберугрозах из защищаемого сетевого сегмента организации в иные сетевые сегменты для решения задач обнаружения вторжений

РЕШЕНИЕ

Совместное применение аппаратно-программного комплекса InfoDiode и решений HoneyCorn в рамках построения СОВ

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) доверенного сегмента сети с сохранением возможности передачи оповещений в SOC для анализа и предотвращения киберугроз

О компании

Крупное промышленное, энергетическое или финансовое предприятие, имеющее значимый сегмент сети, требующий дополнительных средств контроля - построения системы обнаружения вторжений (СОВ) на базе Deception-систем

Вызовы в области информационной безопасности

В результате кибератаки на доверенную сеть может существенно пострадать критическая инфраструктура, что приведёт к значимым последствиям для организации. Для предотвращения кибератак требуется своевременно выявлять признаки вторжения, например, с применением киберловушек (Deception -систем) и передавать соответствующие оповещения в центр мониторинга безопасности (SOC) .

В то же время, учитывая, что SOC расположен в другом сегменте сети, необходимо обеспечить надёжную защиту периметра доверенного сегмента сети.

Применяемый продукт

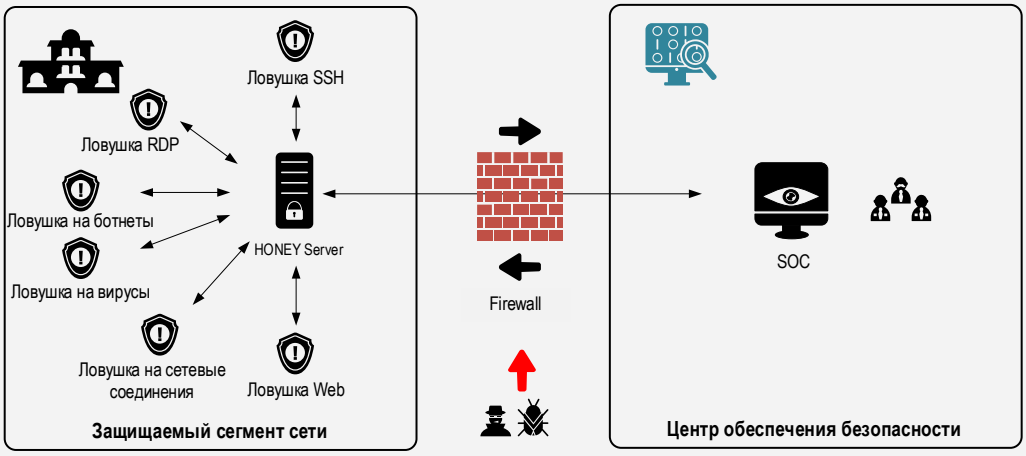
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Оперативно получать оповещения о киберугрозах из защищаемых сегментов в центр мониторинга безопасности для анализа и предотвращения вторжений от системы класса Deception
- Обеспечить централизованный мониторинг кибербезопасности защищаемого сегмента сети
- Гарантированно исключить воздействие на защищаемый сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для SOC

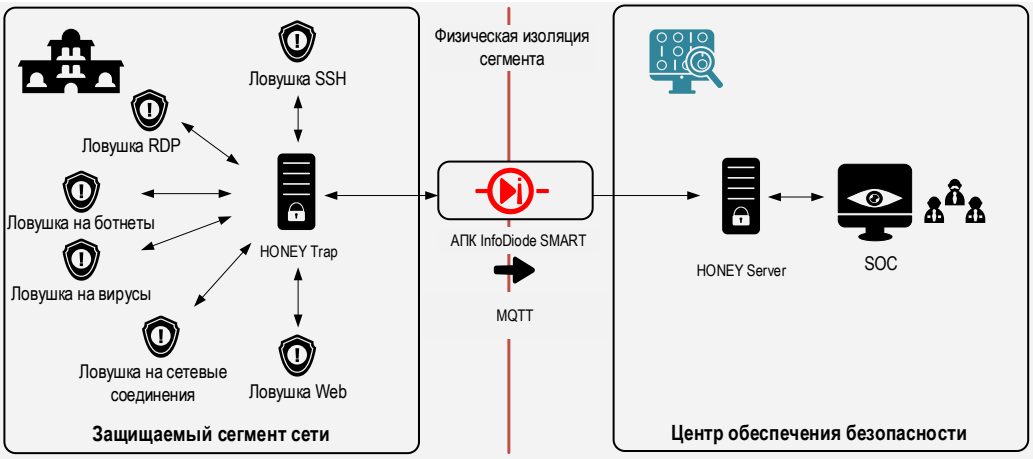
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети
- Выполнено физическое отделение защищаемой сети от других, менее доверенных сегментов. Исключена возможность проникновения в защищаемый сегмент и развитие кибератаки
- Реализована передача оповещений о киберугрозах с защищаемых объектов по однонаправленному каналу через диод данных в центр обеспечения безопасности (SOC).
- Успешно решена задача по построению системы обнаружения вторжений (СОВ) на базе Deception системы

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Промышленность, энергетика

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача телеметрии и событий информационной безопасности из технологического сегмента в SOC при построении системы обнаружения вторжений на базе продуктов IDS/IPS

ОТРАСЛЬ

ПРОМЫШЛЕННОСТЬ, ЭНЕРГЕТИКА

ЦЕЛЬ

Обеспечить передачу телеметрии и событий безопасности с антивирусов из технологического сегмента промышленного объекта в иные сегменты для решения задач обнаружения

РЕШЕНИЕ

Совместное применение аппаратно-программного комплекса InfoDiode с KICS for Nodes для передачи данных на сенсор KICS for Networks в рамках построения СОВ

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с сохранением возможности передачи трафика для анализа и предотвращения вторжений

О компании

Крупное промышленное предприятие, имеющее значимый технологический сегмент, требующий дополнительных средств контроля - построения системы обнаружения вторжений (СОВ)

Вызовы в области информационной безопасности

В результате кибератаки на технологическую сеть могут существенно пострадать данные и оборудование, что приведёт к значимым нарушениям технологических процессов. Для предотвращения кибератак требуется осуществлять непрерывный мониторинг технологического сегмента на предмет вирусной активности и обнаружения признаков вторжения.

В то же время, учитывая, что центр мониторинга безопасности (SOC) расположен в другом сегменте сети, необходимо обеспечить надёжную защиту периметра технологического сегмента сети.

Применяемый продукт

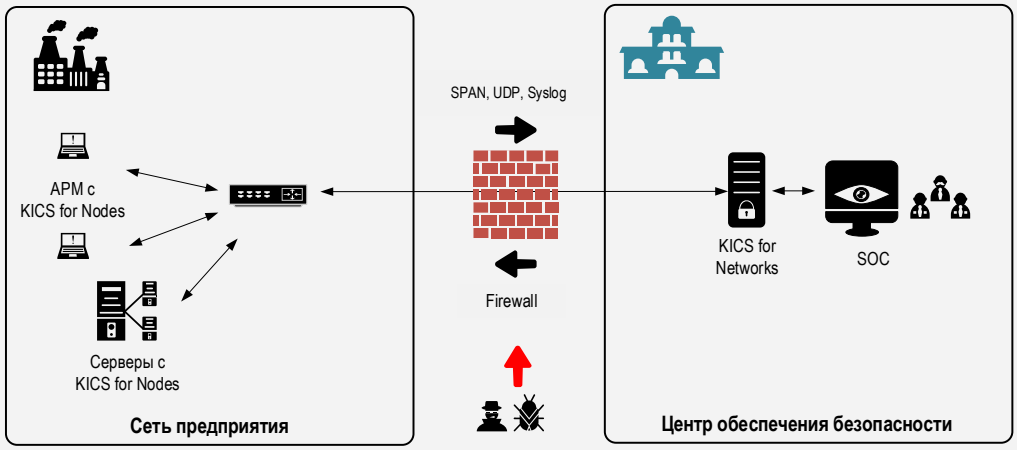
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким промышленным протоколам через границу периметра. Специализированные коннекторы промышленных протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их далее по однонаправленному каналу, обеспечив соответствие высочайшим требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно получать телеметрию средств комплексной защиты серверов и рабочих станций (данные об узлах, событиях безопасности, сессиях) из производственных сегментов в центр мониторинга безопасности
- Обеспечить централизованный мониторинг сетевого трафика технологической сети
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для SOC

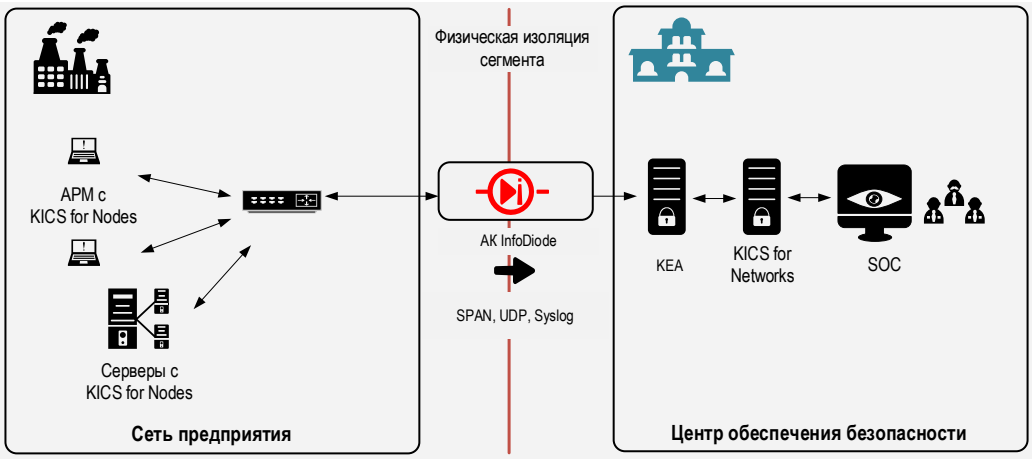
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети
- Выполнено физическое отделение технологической сети от других, менее доверенных сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализована передача телеметрии и событий ИБ с производственных объектов (АРМ, серверы) по однонаправленному каналу через диод данных в центр обеспечения безопасности (SOC), успешно решена задача по построению системы обнаружения вторжений (СОВ) на предприятии на базе решений KICS for Nodes с передачей данных KICS for Nodes на сенсоры KICS for Networks в Security Operation Center.

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Промышленность, энергетика

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ

Передача логов и событий информационной безопасности из технологического сегмента в SOC в рамках построения центра контроля информационной безопасности

ОТРАСЛЬ

ПРОМЫШЛЕННОСТЬ, ЭНЕРГЕТИКА

ЦЕЛЬ

Обеспечить передачу логов и событий безопасности из технологического (защищаемого) сегмента промышленного объекта в иные сетевые сегменты для контроля состояния ИБ и своевременного реагирования на инциденты

РЕШЕНИЕ

Совместное применение аппаратного комплекса InfoDiode с решениями R-Vision EVO в рамках построения ЦКИБ

ПРЕИМУЩЕСТВА

Гарантированная защита (на физическом уровне) технологического сегмента с сохранением возможности передачи трафика для анализа и предотвращения вторжений

О компании

Крупное промышленное предприятие, имеющее значимый технологический сегмент, требующий дополнительных средств контроля и реагирования - построения центра контроля информационной безопасности (ЦКИБ)

Вызовы в области информационной безопасности

В результате кибератаки на технологическую сеть могут существенно пострадать данные и оборудование, что приведёт к значимым нарушениям технологических процессов. Для предотвращения кибератак требуется осуществлять непрерывный мониторинг технологического сегмента на предмет обнаружения угроз ИБ и своевременно реагировать на них.

В то же время, учитывая, что центр мониторинга безопасности (SOC) расположен в другом сегменте сети, необходимо обеспечить надёжную защиту периметра технологического сегмента сети.

Применяемый продукт

АПК InfoDiode PRO решает задачи по передаче файловых потоков, дистрибутивов, бэкапов баз данных, реплик виртуальных машин, электронной почты, видео и другого трафика.

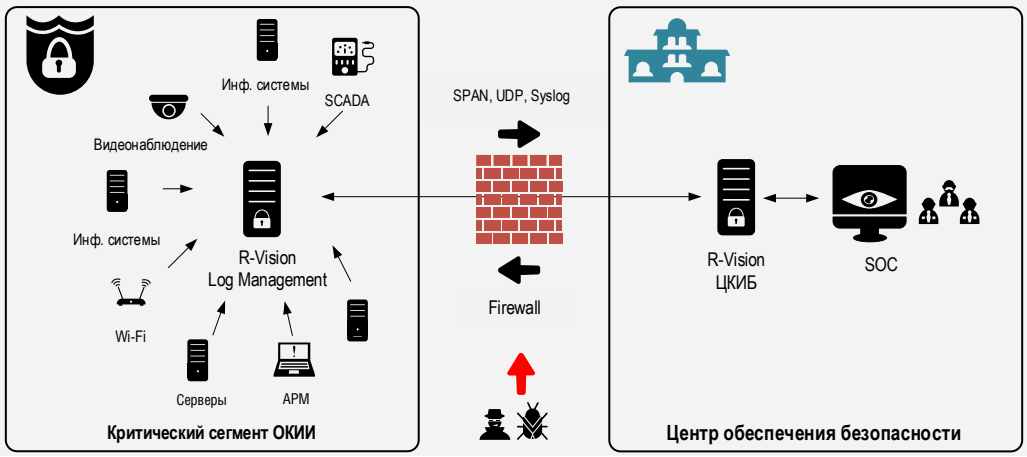
АПК InfoDiode SMART обеспечивает передачу данных одновременно по нескольким пром. протоколам через границу периметра. Специализированные коннекторы пром. протоколов позволяют собрать данные из каждого сегмента сети (от различных SCADA систем, контроллеров, OPC серверов, датчиков) и передать их по однонаправленному каналу, обеспечив соответствие требованиям изоляции защищаемого сегмента.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Требования

- Регулярно получать логи и события ИБ из производственных сегментов в ЦКИБ для управления инцидентами ИБ, автоматизации запуска сценариев реагирования, управления другими системами через механизм оркестрации
- Консолидировать информацию о состоянии ИБ в организации
- Гарантированно исключить воздействие на технологический сегмент, сделав невозможной организацию атаки по тому же каналу, по которому передаются данные для SOC

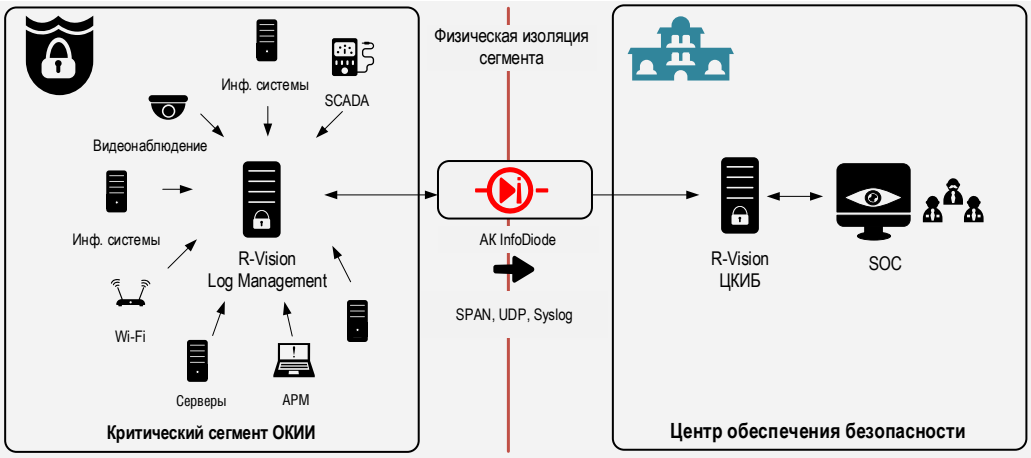
Архитектура: ДО



Результаты

- Повышен уровень информационной безопасности за счет эффективной сегментации сети
- Выполнено физическое отделение технологической сети от других, менее доверенных сегментов. Исключена возможность проникновения в технологический сегмент и распространения вредоносных программ
- Реализована передача логов и событий ИБ с производственных объектов по однонаправленному каналу через диод данных в центр обеспечения безопасности (SOC), успешно решена задача по построению центра контроля информационной безопасности (ЦКИБ) предприятия

Архитектура: ПОСЛЕ



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru