STIA

Кибербезопасность промышленных систем в ТЭК

Докладчик: Кайпиев Амир Кайратович
Директор ТОО “Стройинжиниринг Астана” (далее - STIA)
Вице-президент ОЮЛ “Центр Кибербезопасности АСУ ТП/ОТ Центральной Азии”

Содержание

STIA

На протяжении более 20 лет повышаем безопасность и эффективность производства с помощью комплексной экспертизы: промышленная безопасность, НИОКР, разработка стандартов и нормативно-технической документации, а также полный цикл внедрения решений по кибербезопасности.

10
Технических регламентов

15
Технологических регламентов

22
НИОКР/НИР

400+
Экспертных заключений

181
Национальных стандартов

500+
Стандартов организаций

Выполненные проекты

STIA

в цифрах

4
Плана ликвидации аварий

333
Инструкции по Промышленной Безопасности

4
НПА в НГО

35
НТД НГО

6500+
Специалистов обучено и аттестовано (ПБ и ПБиОТ)

10
Межгосударственных стандартов

115
Учетная регистрация стандартов иностранных государств

STIA

Мы являемся партнерами крупнейших и лидирующих производителей

DRAGOS Honeywell FORTINET CROWDSTRIKE

Сертифицированные специалисты на мировом уровне

GIAC INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

GIAC RESPONSE AND INDUSTRIAL DEFENSE GRID

ISA/IEC 62443 CYBERSECURITY EXPERT ISA

Международные консультанты, имеющие мировое признание

Майкл Хоффман

Технический Директор (CTO) @ Dragos

GRID, GICSP, GSP, GPEN + 17 сертификатов
Сертифицированный инструктор @ SANS Intitute

Салтанат Маширова

Директор кибербезопасности ICS/OT @ CPX

GRID, GICSP, ISA/IEC 62443, CISM + 6 сертификатов
Член Экспертного Совета Агентства по вопросам Кибербезопасности Сингапура при Премьер-Министре
Женщина Года 2023 в Кибербезопасности

ICS/OT Cybersecurity Day

STIA

Страны с развитой промышленностью создают национальные программы и сообщества для защиты критической инфраструктуры.

Первое мероприятие, посвященное исключительно промышленной кибербезопасности в Казахстане

- Более 130 участников, включая руководителей и топ-менеджеров ведущих промышленных предприятий.
- Представители 27 ключевых компаний нефтегазовой и энергетической отрасли.
- По итогам мероприятия создано сообщество — Центр кибербезопасности АСУ ТП/ОТ (ICS/OT) и критических инфраструктур Центральной Азии (ICCC).

STIA

Информационная безопасность - это не только защита персональных данных

Информационная безопасность воспринимается, в основном, как защита данных - их целостности, конфиденциальности в системах Информационных Технологий (ИТ или IT).

Однако сегодня кибератаки обрели новый вектор развития - **промышленность**, а именно промышленные системы управления технологическими процессами. Теперь же, как и IT системы, критически важной целью кибербезопасности становится и **защита технологических процессов**, в случае сбоя которых появляются более тяжелые последствия.

Промышленные системы относятся к Операционным Технологиям (ОТ)

STIA

Операционные Технологии (ОТ) – это системы и технологии, которые управляют физическими процессами и объектами.

На ряду с IT, защита ОТ должна быть приоритетом для всех организаций, чья деятельность связана с критически важными процессами, управляемыми или поддерживаемыми кибер-физическими системами (например, АСУ ТП на производстве).

IT безопасность vs OT безопасность

STIA

IT безопасность

Приоритетность

- Конфиденциальность
- Целостность
- Доступность

Последствия

- Репутационный риск
- Утечка данных
- Финансовый риск

OT безопасность

Приоритетность

- **Безопасность жизнедеятельности**
- Целостность
- Доступность
- Конфиденциальность

Последствия

- Утечка данных
- **Риск повреждения оборудования**
- Репутационный риск
- **Риск для жизни**
- **Угроза благосостоянию государства**

Важность защиты кибербезопасности Операционных Технологий (ОТ) в топливно-энергетический комплексе (ТЭК)

В рамках цифровизации ТЭК внедряются решения способные повысить эффективность производства и возможности мониторинга. Однако эти технологии открывают новые уязвимости в системах для кибератак.

По данным многолетних исследований Dragos, 20 из 23 наиболее опасных киберпреступных организаций на промышленность нацелены на ТЭК

Возможные последствия атак

- Остановка производственных процессов
- Риск для жизни сотрудников и экологии
- Вывод из строя оборудования
- Подрыв репутации компании

Статистика не радует

Количество кибер атак увеличивается, следовательно и физических последствий

STIA

Dragos

2022: Рост инцидентов **150%**

2024: Ransomware* атаки: 1693 случая, рост **87%** с прошлого года

Прогноз: с каждым годом количество инцидентов будет удваиваться

Waterfall

2022: **218 кибер атак** и **57 из них** имели физические последствия

2023: **68 атак** нарушили работу 500 обьектов автоматизации

Mandiant (Google)

В последнее время, зафиксирована новая группа хакеров - Хактивисты

2022: Количество заявлений от хактивистов об атаках на OT-среды выросло вдвое

По оценке Dragos (2025), потенциальный годовой финансовый риск киберинцидентов в **OT превышает $300 млрд**, а средняя стоимость одного инцидента в 2024 году в промышленности по данным IBM — **$5,56 млн.**

Данные исследовательских компаний опираются на официальные и подтвержденные данные и не берут в счет неподтвержденные и засекреченные случаи

**Ransomware - киберпреступность с целью вымогания денежных средств*

Международный опыт

STIA

В данном направлении лидерами являются США, ЕС, Австралия и Сингапур. Оглядываясь на их опыт можно заметить следующие общие черты:

- Определение влиятельного регулятора: Создание специализированных органов, которые подчиняются напрямую главе государства/правительства. Например:Агентство по кибербезопасности и защите инфраструктуры США, Агентство по кибербезопасности Сингапура и т.д.
- Принятие законов и регулирование: ужесточение требований, внедрение дорожных карт и мастер-планов для промышленности, энергетики, ЖКХ.
- Стандартизация: разработка собственных стандартов или **внедрение международных**, к примеру IEC 62443, NIST, NERC CIP.
- Комплексные программы и инициативы: национальные стратегии, центры компетенций, государственно-частные альянсы.

Крупнейшие атаки на производства

STIA

STUXNET (2010)
Иран

HAVEX (2013)
США/ЕС

Немецкий ГМК (2014)
Германия

Blackenergy 3/ Sandworm (2015)
Украина

CRUSHOVERRIDE / Industroyer (2016)
Украина

TRISIS/TRITON (2017)
Саудовская Аравия

Colonial Pipeline (2021)
США

Industroyer 2 (2022)
Украина

PipeDream (2022)
Весь мир

STUXNET

STIA

В июне 2010 года произошла кибератака на иранский ядерно-обогатительный завод в Нетенз с использованием вредоносного программного обеспечения Stuxnet.

Методы проникновения

- Физический USB носитель (флешка) и уязвимый VPN канал

Цели и намерения

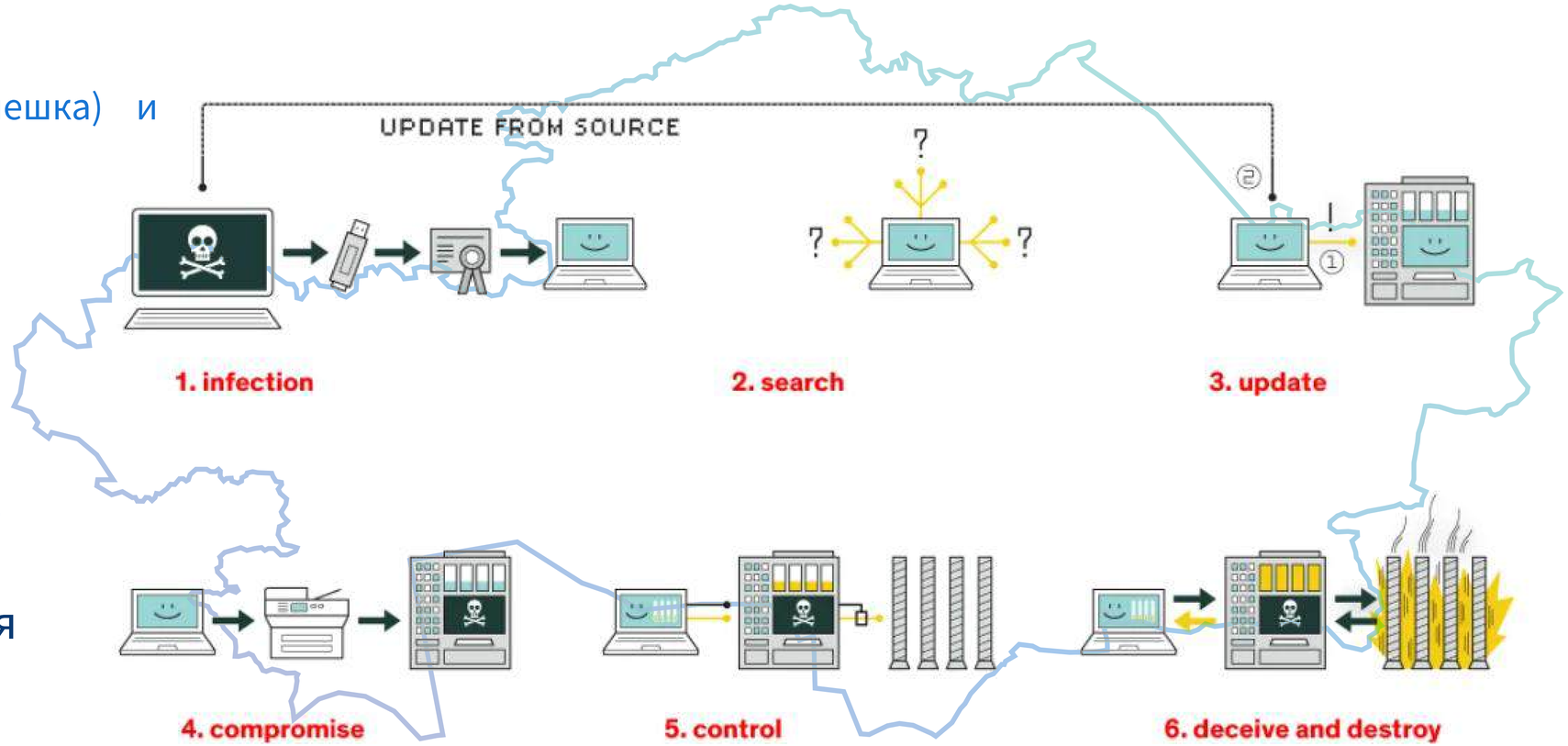
- Неизвестны

Последствия

- Были уничтожены 3000 центрифуг

Киберпреступная организация

- Предположительно организация спонсируемая США и Израилем, согласно множеству независимых СМИ (BBC, CNN и т.д.)



BlackEnergy 3/Sandworm

STIA

В декабре 2015 года произошла кибератака на энергетические системы Украины, известная как BlackEnergy или Sandworm. Во время атаки использовалось вредоносное ПО, которое позволило злоумышленникам получить доступ к системам управления электросетями.

Методы проникновения

- Вредоносное ПО вшитое в Word, Excel и Powerpoint файлы

Цели и намерения

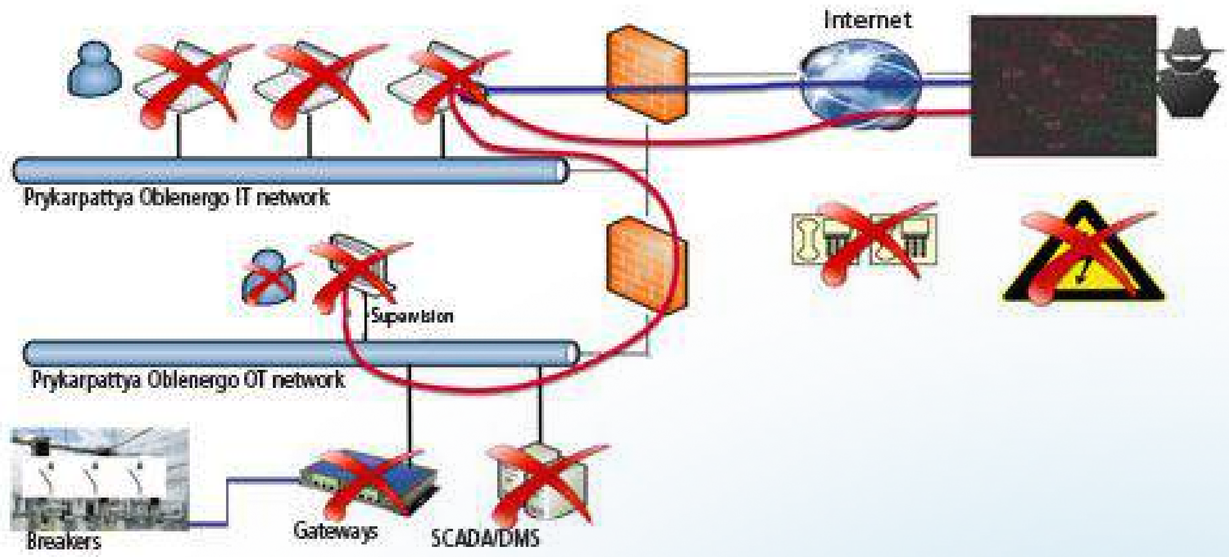
- Нанести ущерб энергетическим объектам Украины

Последствия

- 1,500,000 пользователей (230,000 объектов) остались без света и тепла на 6 часов
- Переход на ручной режим работы на несколько месяцев.

Киберпреступная организация

- Sandworm



CRUSHOVERRIDE

STIA

В декабре 2016 года произошла повторная кибератака на энергосистему Украины, известная как Crashoverride. Эта атака была нацелена на подстанции и использовала вредоносное ПО, которое позволило злоумышленникам получить доступ к управлению физическим процессом.

Методы проникновения

- Неизвестно

Цели и намерения

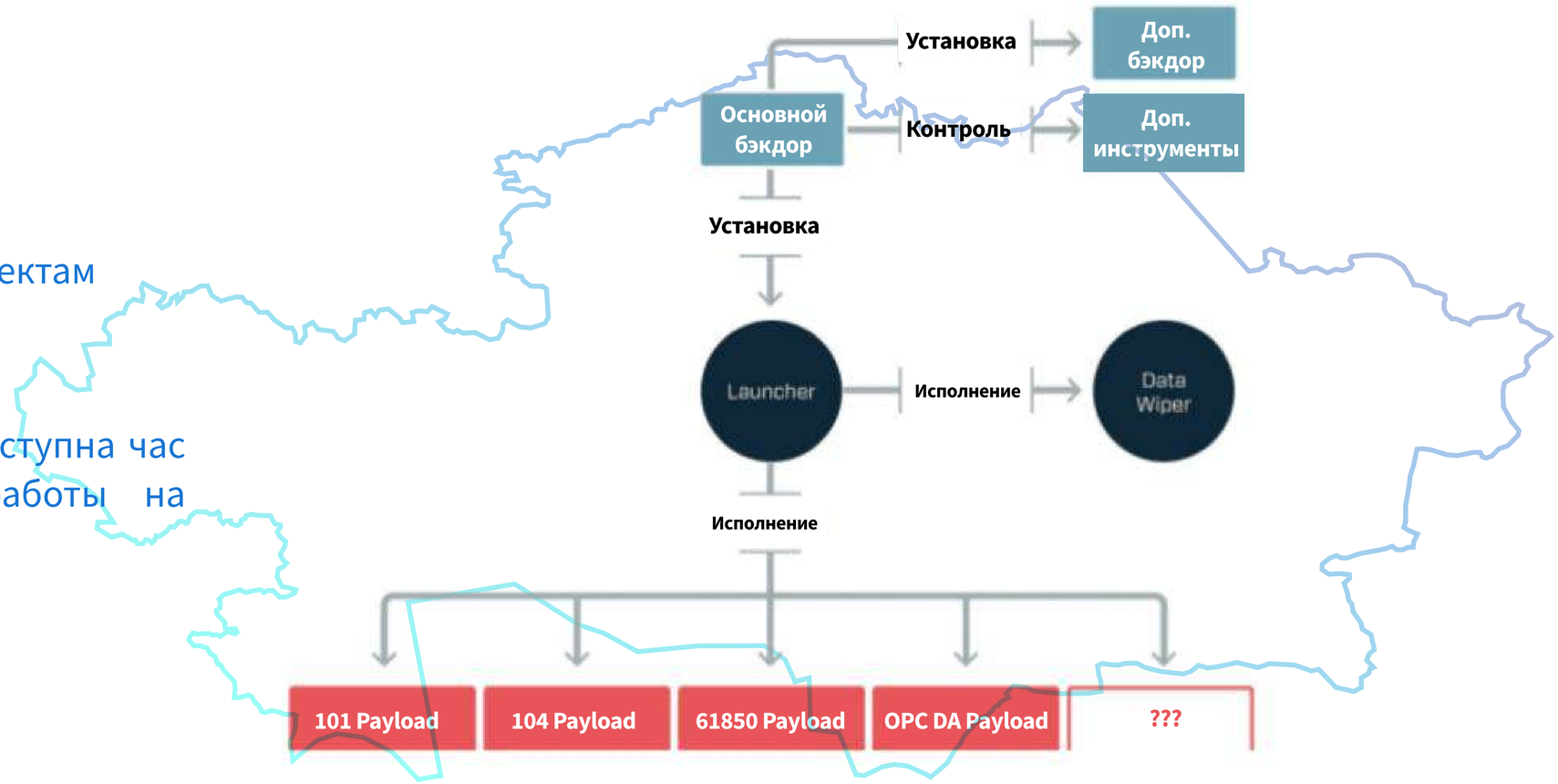
- Нанести ущерб энергетическим объектам Украины

Последствия

- электроэнергия в г.Киев была недоступна час и переход в ручной режим работы на несколько месяцев

Киберпреступная организация

- ELECTRUM



TRISIS/TRITON

STIA

В августе 2017 года произошла кибератака на промышленную систему безопасности Triconex НПЗ в Саудовской Аравии, известная как TRISIS или TRITON. Эта атака была направлена на системы безопасности, используемые для управления процессами на химических предприятиях.

Методы взлома

- Неизвестно

Цели и намерения

- Предположительно техногенная катастрофа

Последствия

- Остановки 2-х НПЗ

Киберпреступная организация

- XENOTIME

Проникновение в инфраструктуру

Тестирование TRISIS

Подключение к системе безопасности

Анализ системы безопасности

Перенос TRISIS на систему безопасности

Запуск TRISIS

Colonial Pipeline

STIA

В мае 2021 года произошла кибератака на Colonial Pipeline, крупнейшую трубопроводную компанию в США, которая поставляет топливо на восточное побережье страны. В результате атаки были временно приостановленны поставки топлива, вызвав масштабные перебои в снабжении и рост цен на топливо.

Методы взлома

- Взлом VPN подключения

Цели и намерения

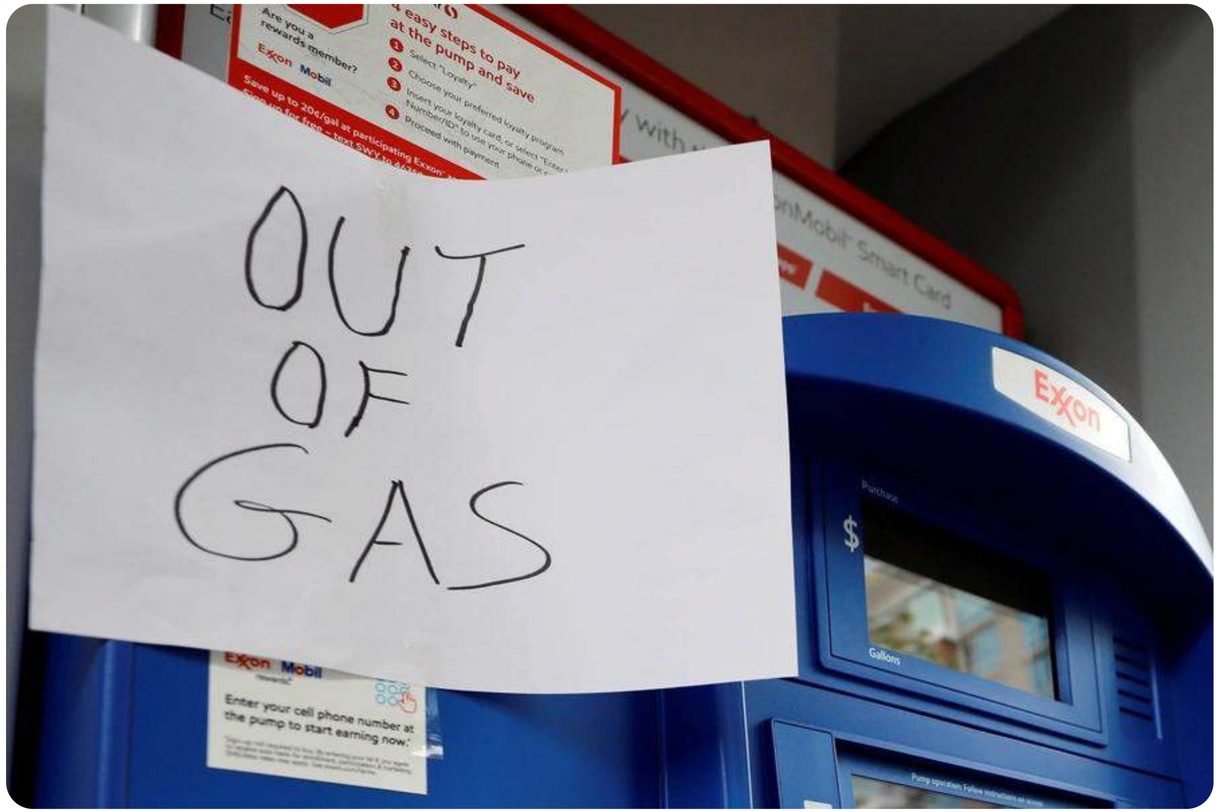
- Финансовая выгода

Последствия

- Трубопровод остановился на 6 дней, вызвав дефицит топлива в стране. Киберпреступной организации было выплачено более 75 биткоинов (почти $5 млн)

Киберпреступная организация

- DarkSide



Будущая угроза - Pipedream

В 2022 году, киберпреступная организация под названием Chernovite разработали комплекс инструментов для взлома промышленных сетей которые могут охватить большое количество вертикалей производств и критических инфраструктур

Уникальность угрозы

- Универсальный набор инструмента для определенного числа устройств

Цели и намерения

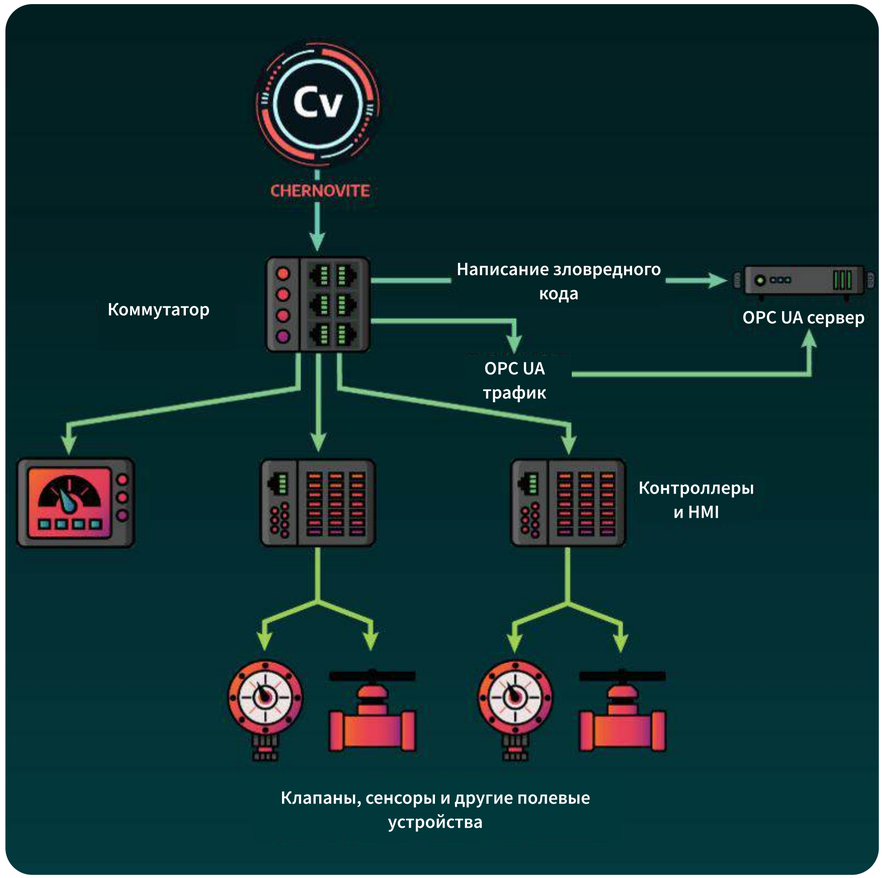
- Сократить время подготовки к атакам

Последствия

- За 2024г. появилось 3 новых мировых вредоносных ПО на базе Pipedram

Киберпреступная организация

- CHERNOVITE



Будущая угроза

STIA

Кибер атаки раньше

Высокая стоимость

Низкие шансы на успех

Длительное время подготовки

Невозможность переиспользования на другом объекте

Кибер атаки сейчас

Доступная стоимость

Высокие шансы на успех

Короткое время подготовки

Многократное повторное применение на множестве объектов

Первые шаги к киберустойчивой инфраструктуре

STIA

Для обеспечения кибербезопасности промышленности на хорошем уровне представляется необходимым осуществление, в целом по стране, комплекса мер, включающих в себя следующие меры:

- Анализ текущего состояния: проведение обследования на критически важных объектах и, с помощью оценки экспертов, оценить текущие потребности.
- Гармонизация международных стандартов: адаптация международных стандартов доказавших свою надежность в других странах под специфику нашей страны.
- Разработка единой дорожной карты: утверждение национального видения развития кибербезопасности критически важных обьектов.
- Корретировки в НПА: дополнения в Единые Требования ИКТ и ИБ требований для промышленных сетей.
- **Обучение специалистов: повышение кадрового ресурса.**

Методы защиты для предприятий

STIA

Научная работа “Sliding Scale of Cyber Security” от Rob M. Lee и Tim Conway

Архитектура

Планирование, создание и сопровождение систем с учетом требований безопасности.

Пассивная защита

Системы, добавленные к архитектуре для обеспечения надежной защиты или получения информации о угрозах без постоянного участия человека.

Активная защита

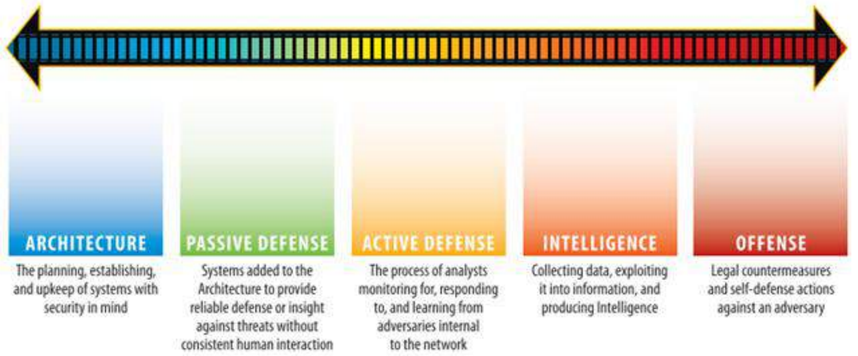
Процесс, при котором аналитики осуществляют мониторинг, реагируют и извлекают уроки из действий противников внутри сети.

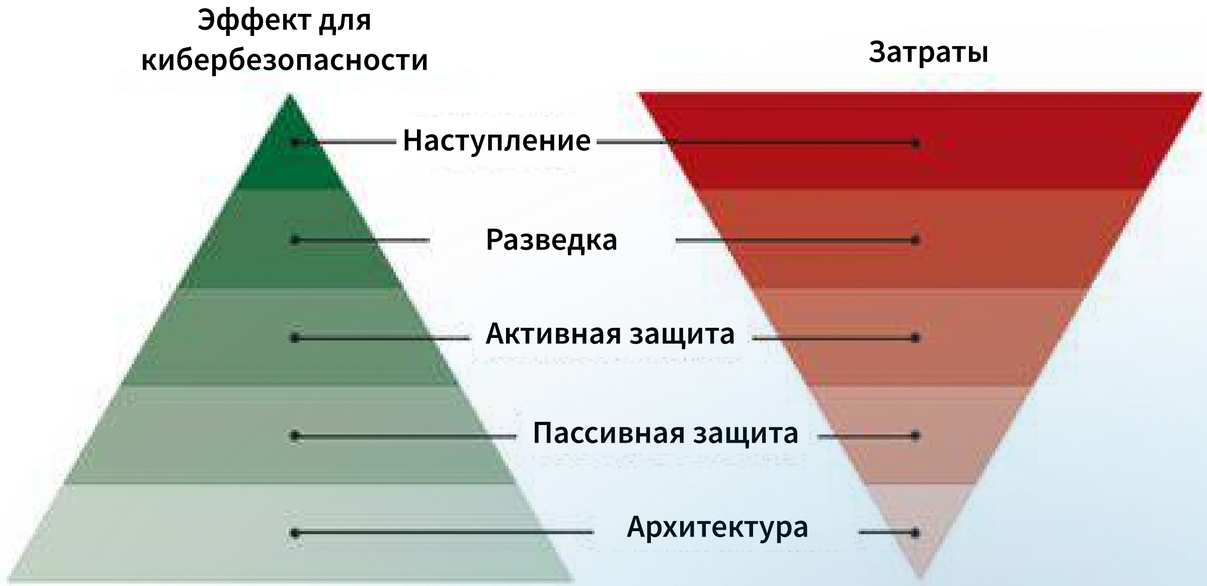
Разведка

Сбор данных, их преобразование в информацию и создание автоматических индикаторов кибер атак.

Наступление

Законные контрмеры и действия самозащиты, нацеленные против противника.





Методы защиты:

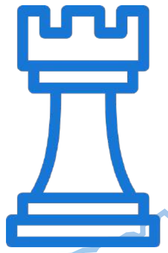
5 критических шагов кибербезопасности ICS/OT

1

План Реагирования на Инциденты в ICS

Разработка специального плана для быстрого реагирования на инциденты в OT-системах, с учетом уникальных угроз и устройств.

2



Защищённая Архитектура

Укрепление сетевой безопасности, ограничивая точки доступа и устраняя уязвимости с высоким уровнем риска.

3

Видимость и Мониторинг Сети

Ведение учета активов и отслеживание трафика для выявления угроз и аномалий в реальном времени.

4

Безопасный Удаленный Доступ

Применение многофакторной аутентификации (MFA) и контроль за удаленными подключениями для защиты сети.

5

Управление Уязвимостями на Основе Рисков

Оценивать уязвимости по их риску и разрабатывать стратегии их минимизации или устранения.

План реагирования на инциденты

STIA

Основываясь на реальных ситуациях, определить какими могут быть атаки и как на них реагировать. Регламентировать действия

Разбор инструментов злоумышленника при совершении атаки в Вашей сети и индикаторов обнаружения проникновения специалистами по ИБ.

Проведение настольных упражнений, в которых разбираются сценарии проникновения со специалистами по ИБ

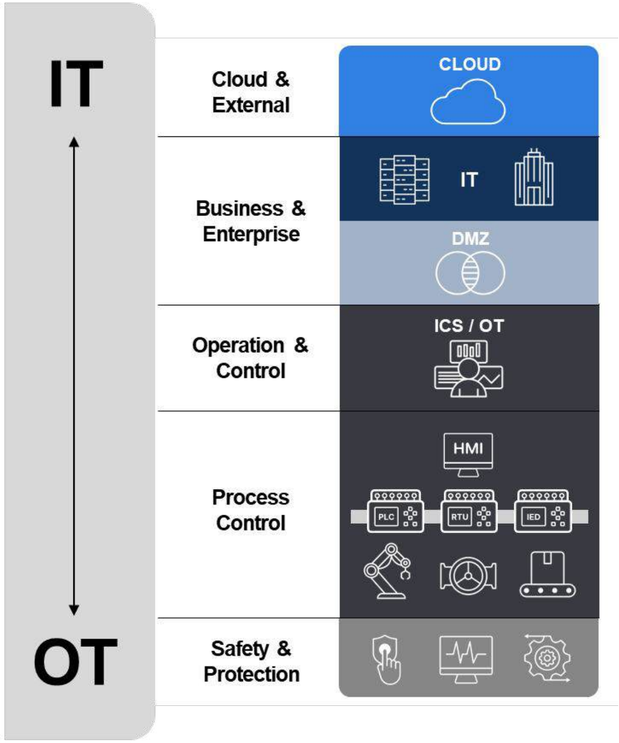
Защищенная инфраструктура

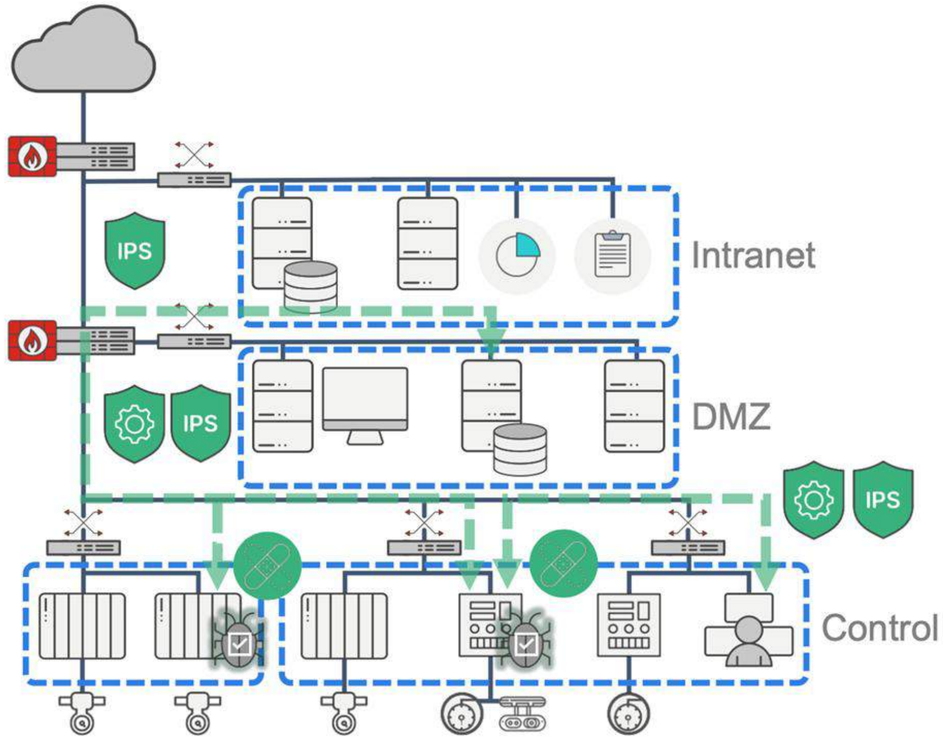
STIA

Сегментация сети

Ограничение двунаправленной коммуникации в сети

Возможность видимости и сбора данных





FortiGate - Межсетевой экран нового поколения

FortiSwitch - коммутатор нового поколения

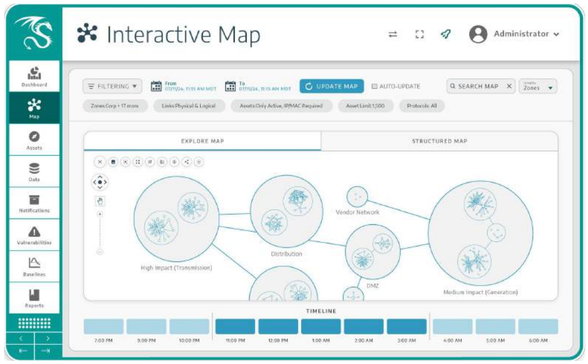
Видимость и мониторинг сети

STIA

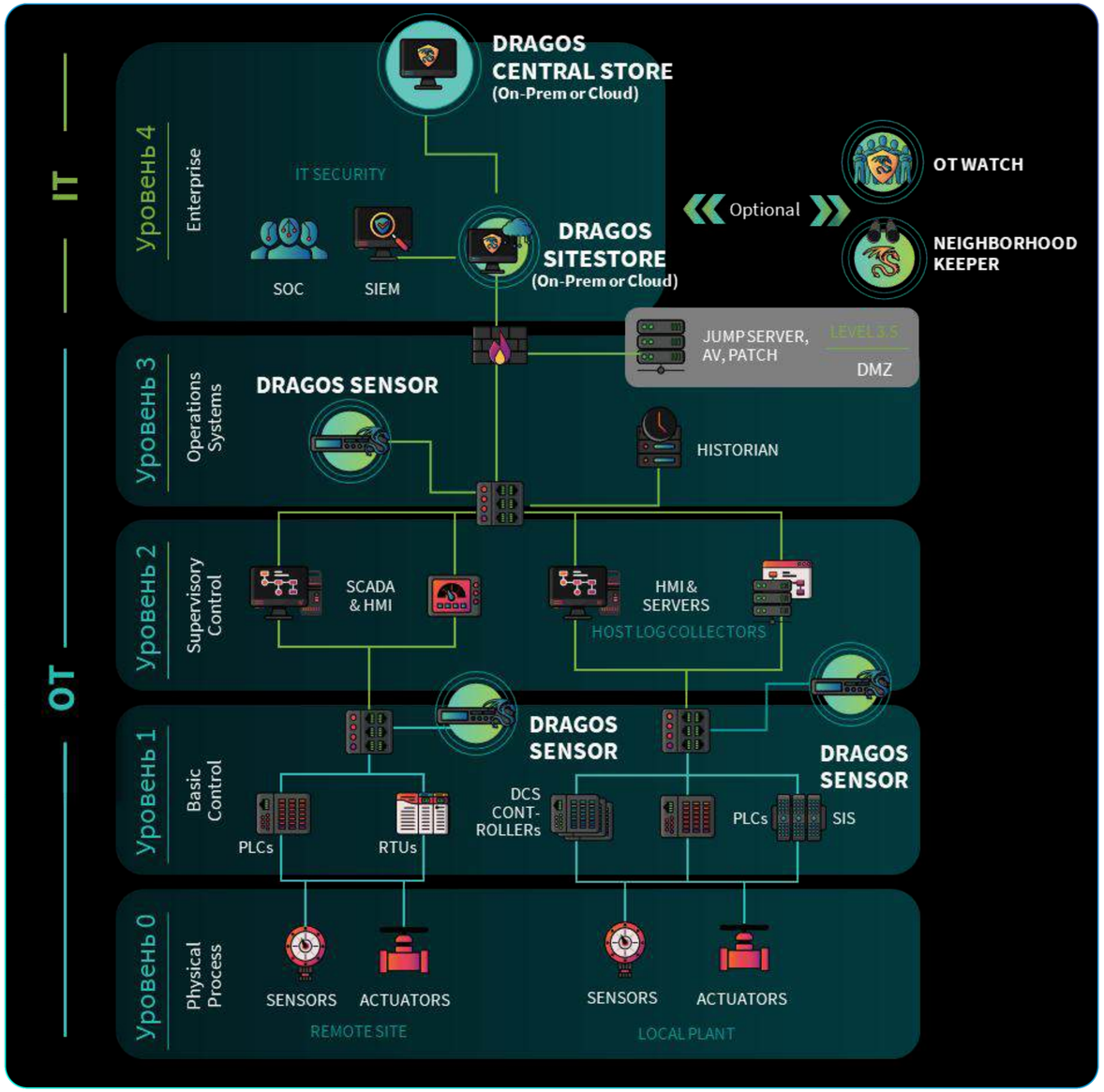
Невозможно защищать объект, не имея представления того, что в нем происходит в реальном времени

Для получения видимости промышленных сетей используются платформы, такие как:

Dragos Platform



FortiNDR



Безопасный удаленный доступ

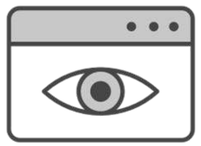
STIA

Гибкость

Скорость

Физическая безопасность

Но вместе с этим появляются риски взлома сети. Для безопасности удаленного доступа необходимо обеспечить



Контроль над удаленным доступом
Удостовериться, что только авторизованные пользователи имеют удаленный доступ

Управление секретной информацией
Хранение секретов надежно и автоматическое создание и ротация паролей

Мониторинг сессий
Пост-сессионный аудит и возможность уничтожить сессию в реальном времени

for OT

FortiSRA

Управление уязвимостями на основе рисков

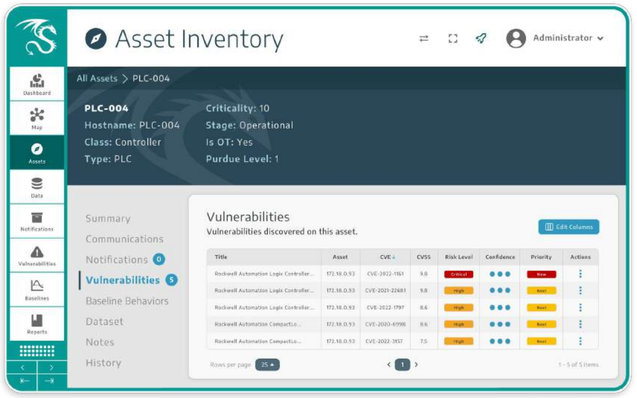
STIA

уязвимостей уже использовали для взломов промышленных сетей

уязвимостей находятся глубоко в промышленных сетях

уязвимостей могут вызвать потерю видимости и контроля над процессом

Dragos Platform



Заключение

Команда инженеров STIA провела обследование на более чем 10-и крупных предприятий в ТЭК РК для определения текущего положения кибербезопасности. В большинстве из них присутствуют схожие проблемы с:

- Нехваткой кадров, экспертизы и очень ограниченными мерами защиты
- Уязвимой архитектурой и оборудованием

Для решения данных проблем мы предлагаем:

- Предпринять государственные и регуляторные меры, которые обсуждались выше
- Предоставление базовых консультаций для проведения мероприятий требующих минимальных затрат и усилий, но при этом имеющих максимальный эффект на киберустойчивость предприятий
- Проведение тренингов по повышению кадрового ресурса
- Разработку ВНД для регламентирования работы с системами с точки зрения информационной безопасности для минимизации рисков
- Проведение обследование критически важных объектов ТЭК и предоставление базовых рекомендаций
- Привлечение отечественных и международных специалистов для определения верного вектора развития кибербезопасности на предприятиях ТЭК

STIA x ICCC

Станьте нашим партнером для повышения безопасности и эффективности!

Амир Кайпиев
📞 +7 700 077 61 61
📧 kaipiyev@stia.kz
🌐 stia.kz