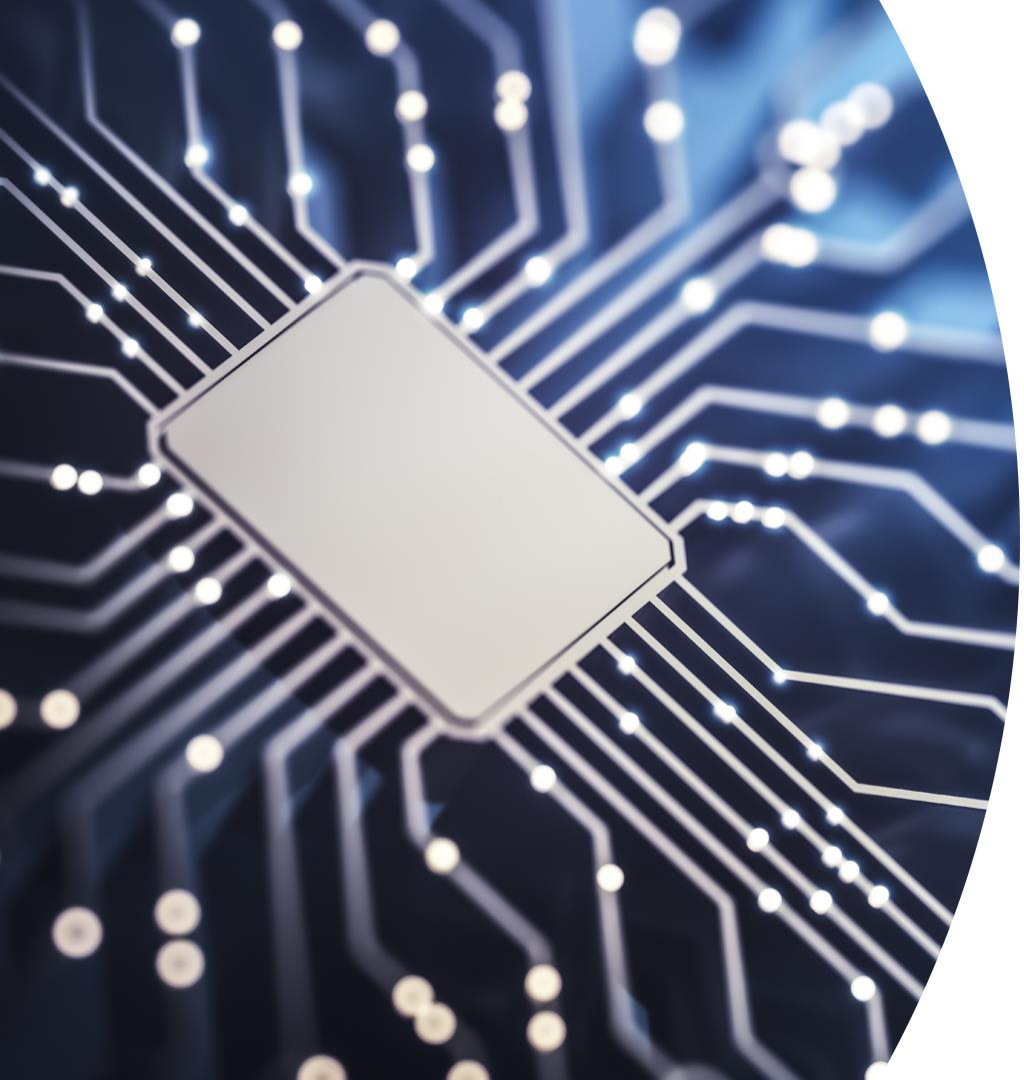
INFOWATCH® ARMA ARMA

Автоматизация в ИБ: создание системы защиты в условиях нехватки кадров

Душа Игорь
Директор по развитию продуктов



INFOWATCH®

Причина 1

Сокращение времени реакции, ускорение рутинных задач

- → Категорирование
- → Контроль подрядчиков
- → Настройка СЗИ
- → Внедрение СЗИ
- → Эксплуатация СЗИ

INFOWATCH®

Причина 2

«Кадровый голод» требует автоматизации

К 2022 году (ISC)² прогнозирует 1,8 млн. незаполненных должностей OT security, что дополняет нынешнюю нехватку кадров. **Адекватная реакция на недостаток квалифицированных кадров:**

- → Настройка систем интеграторами, а не эксплуатантом
- → Обучение уже нанятых сотрудников практическим навыкам
- → Автоматизация реагирования на инциденты
- → Использование внешних SOC

Как проходит день специалиста ИБ АСУ ТП

INFOWATCH®

→ **Работа с документами**
- Категорирование ОКИИ
- Составление ОРД
- Редактирование ОРД

→ **Формирование отчётов**
- Защищённость сети
- Инциденты

→ **Выявление инцидентов**
- Обнаружение вредоносной активности

→ **Реагирование на инциденты ИБ**
- Анализ журналов
- Выезд к рабочим станциям для решения инцидента
- Локализация инцидента и защита АСУ ТП
- Связь с ГосСОПКА

→ **Расследование инцидентов ИБ**

→ **Контроль подрядчиков**

→ **Установка / редактирование / настройка политик ИБ**
- Сокращение ложных срабатываний
- Настройка политик и прав на СЗИ
- Сокращение поверхности атаки

→ **Развёртывание / настройка / обновление СЗИ**

→ **Инвентаризация и учёт оборудования**

Зрелость процессов ИБ с точки зрения автоматизации

Уровни зрелости процесса

Высокая

Зрелость

Низкая

0

СЗИ отсутствуют

1

Внедрены базовые СЗИ

- Антивирус
- Шлюз на периметре

2

Внедрены средства управления активами. Есть актуальная информация

- Системы анализа защищенности
- SIEM
- Системы обнаружения вторжений

3

Сформирована базовая система автоматизации реагирования на инциденты

4

Встроен процесс составления новых сценариев автоматизации

Задачи для автоматизации

1. Автоматизация аудита, централизованного управления активами

- Поиск подключений к сетям общего доступа
- Автоматизация выявления уязвимостей, соответствия требованиям (SCAP)

2. Автоматизация реагирования на инциденты

- Добавление IP адресов, участвующих в инциденте в blacklist
- Изоляция скомпрометированной машины
- Перевод АСУ ТП в ручной режим управления

3. Обогащение данных об инцидентах

4. Автоматизация выпуска документов, категорирования и т.д.

5. Формирование отчетности об инцидентах

Как понять, что автоматизация работает?

Пример метрик для реагирования на инциденты

- Время реагирования
- Количество эскалаций за пределы ролей, определенных в playbook
- Количество возникающих нетиповых инцидентов
- Количество типовых инцидентов, которые не удалось устранить в рамках playbook

Инструменты

CONFIDENTIAL designator

Investigation Enrichment

IDPS signature generates an offense in the SIEM

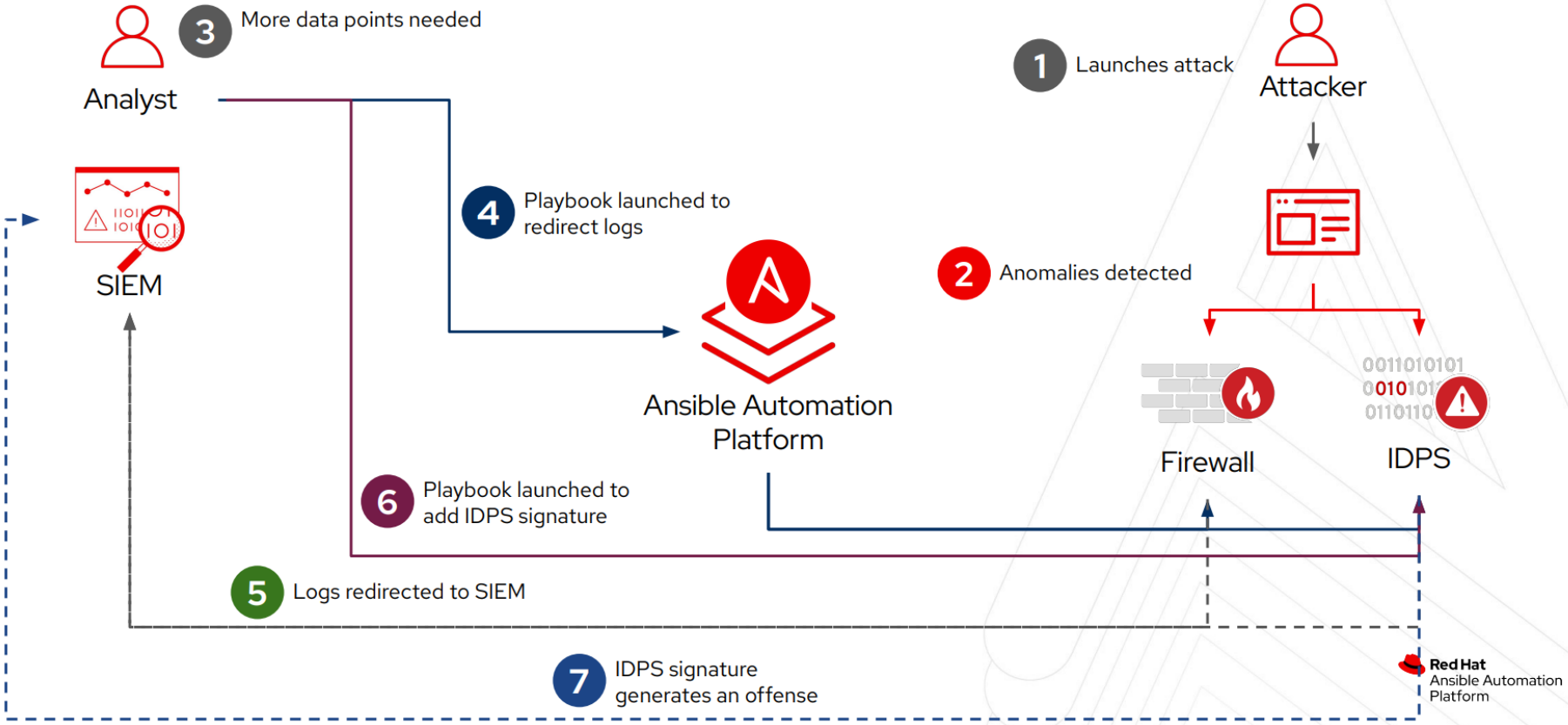
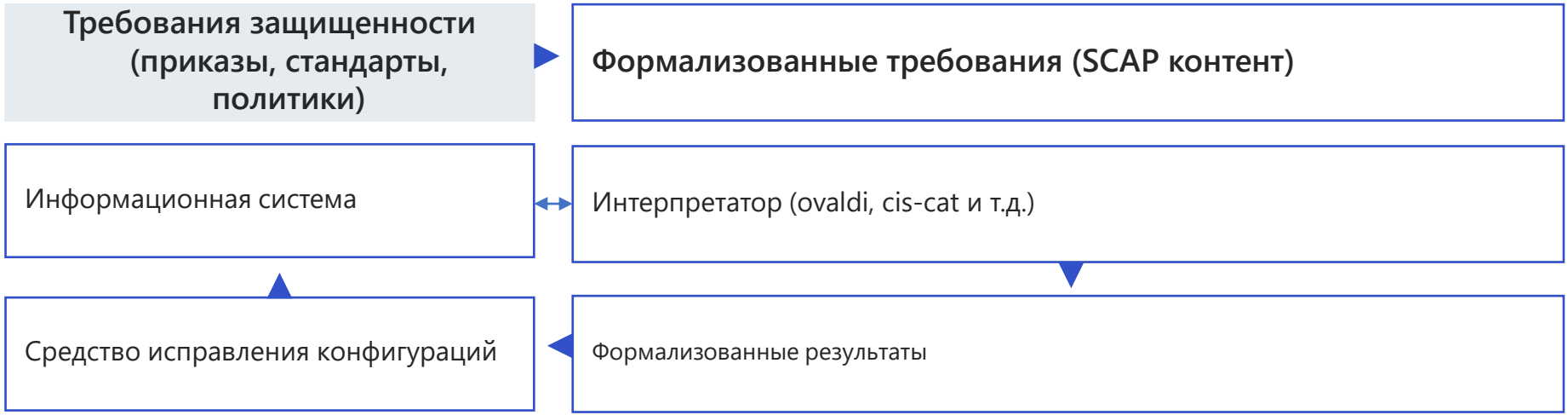


Схема процесса аудита с использованием SCAP



SOAR как первый шаг, XDR как стройная система

INFOWATCH®

XDR (eXtended Detection and Response) — платформа обнаружения и реагирования на угрозы с обширным покрытием:

Анализ данных на конечных устройствах

Сбор информации с телеметрии, сведений о поведении пользователя и программ и др.

Анализ сетевого трафика

Всех устройств в сети, в т. ч. IoT / IIoT, встраиваемых устройств и т. д.

Централизованное управление событиями и инцидентами ИБ, формирование реакции

- → Экономия на настройке: СЗИ интегрированы «из коробки», правила корреляции и сигнатуры уже встроены и обновляются вендором СЗИ
- → Проблема для SOAR – отсутствие стандартизации данных
- → Можно отследить всю цепочку атаки: от попытки проникновения до воздействия на АСУ ТП

Эволюция автоматизации задач сотрудников ИБ

INFOWATCH®

До внедрения SIEM

- Работа с документами
- Проведение ежедневных ТО СЗИ на разных участках
  - Снять логи
  - Загрузить обновления
  - Опломбировка USB-носителей
  - Выявление событий безопасности
  - Регистрация инцидентов ИБ
  - Реагирование на инциденты ИБ
  - Составление отчётов в ручном режиме
- Расследование инцидентов ИБ
- Контроль подрядчиков
- Инвентаризация оборудования и прочие задачи

После внедрения SIEM

- Работа с документами
- Формирование отчётов
- Выявление инцидентов
- Реагирование на инциденты ИБ
- Расследование инцидентов ИБ
- Контроль подрядчиков
- Установка / редактирование / настройка политик ИБ
- Развёртывание / настройка / обновление СЗИ
- Инвентаризация и учёт оборудования

Внедрение SOAR/XDR

- Работа с документами
- Реагирование на сложные инциденты ИБ
- Расследование инцидентов ИБ
- Контроль подрядчиков
- Развёртывание СЗИ

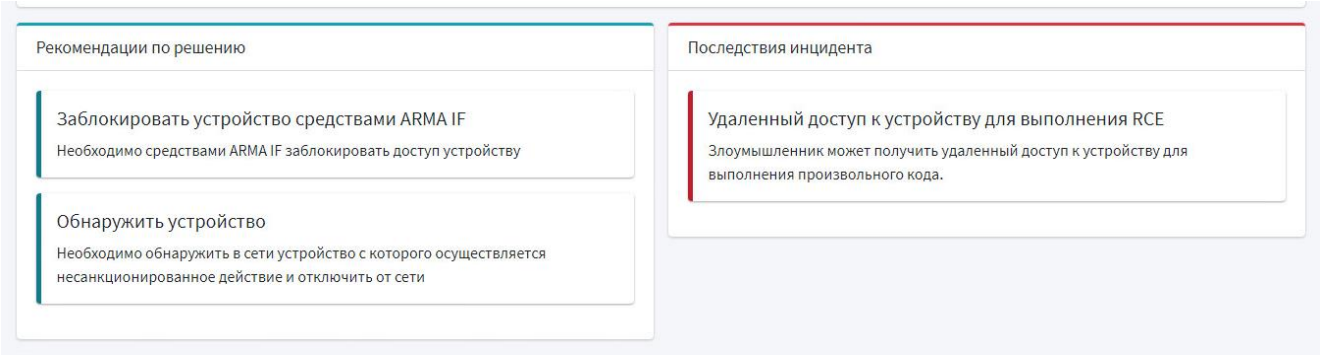
Задача 1

Установка / редактирование / настройка политик ИБ

- → Сокращение ложных срабатываний
- → Настройка правил корреляции
- → Сокращение поверхности атаки
- → Настройка политик ИБ

Решение: InfoWatch ARMA
Правила корреляции

Раньше	Сам писал правила корреляции, правила обнаружения вторжения, настраивал интеграцию между СЗИ
Сейчас	**InfoWatch ARMA** поставляет экспертизу «из коробки»: подход промышленного XDR



А также:

→ Возможность создания **пользовательских правил** корреляции

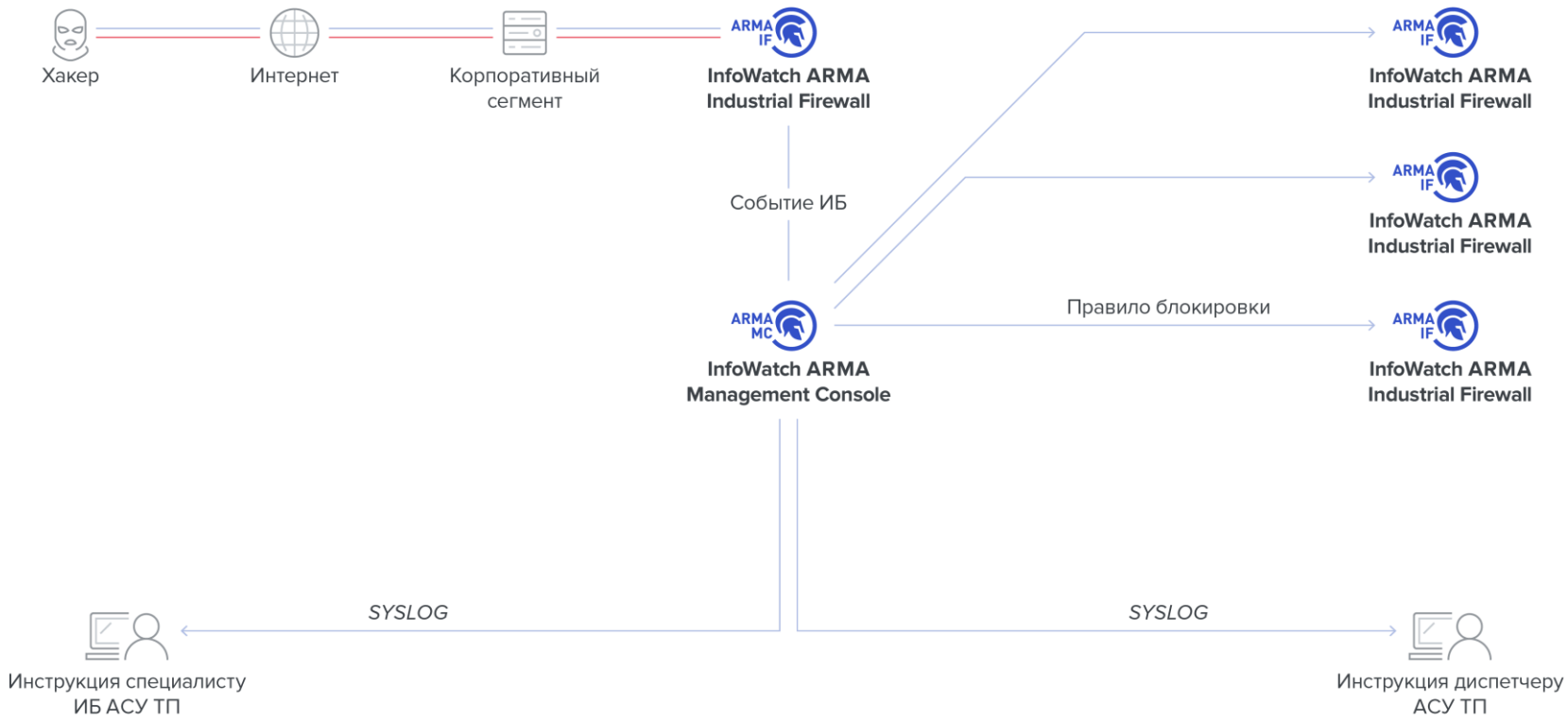
→ Возможность задать список **автоматических действий** на события безопасности

Задача 2

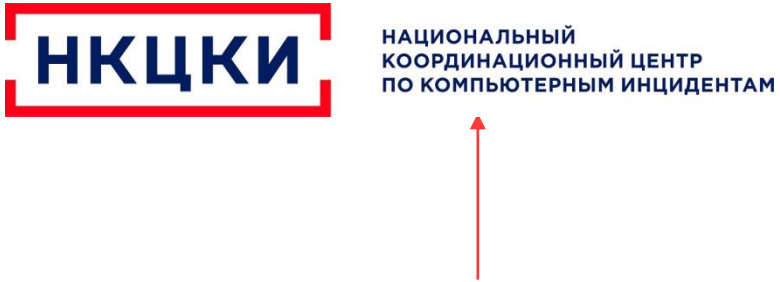
Реагирование на инциденты ИБ

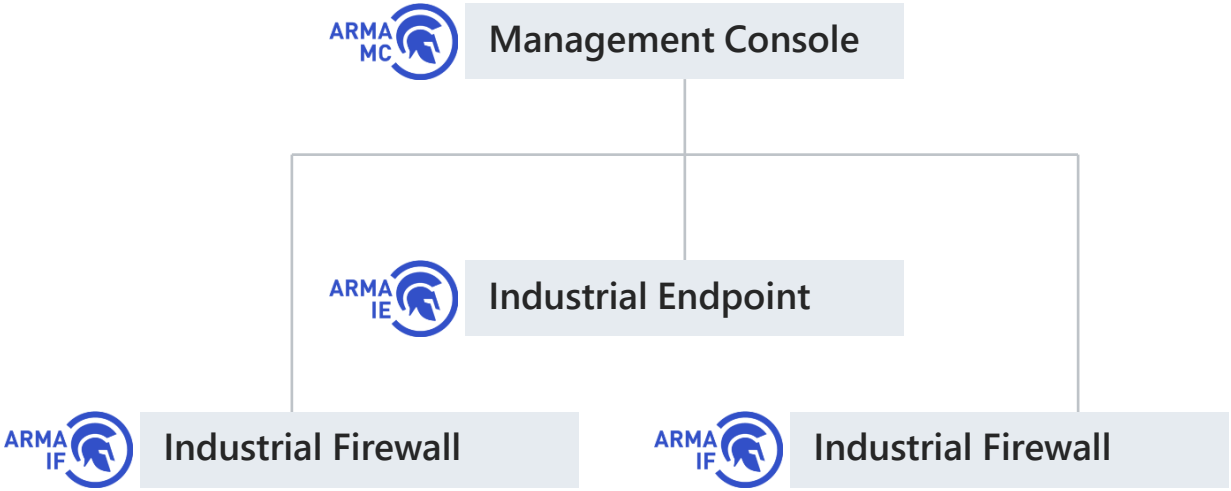
- → Анализ журналов
- → Выезд к рабочим станциям для решения инцидента
- → Локализация инцидента и защита АСУ ТП
- → Связь с ГосСОПКА

Решение: InfoWatch ARMA
Автоматизация реакции на инциденты



Решение: InfoWatch ARMA
Взаимодействие с ГосСОПКА





- → **Информирование ГосСОПКА об инцидентах** информационной безопасности
- → **Оперативный двусторонний обмен** информацией об инцидентах и угрозах безопасности

Задача 3

Выявление инцидентов ИБ

Задача 4

Работа с документами

- → Категорирование ОКИИ
- → Составление ОРД
- → Редактирование ОРД

INFOWATCH® ARMA ARMA

Есть необходимость автоматизации процессов ИБ? Подходите после секции.

/InfoWatchOut /InfoWatch /InfoWatch