



ПЛАТФОРМА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ — ЕДИНАЯ СЛУЖБА
ДИСПЕТЧЕРИЗАЦИИ И КОНТРОЛЯ
SecurOS Dispatcher

КРАТКИЙ ОБЗОР

Основные сферы применения



Объекты дорожной инфраструктуры



Крупные промышленные предприятия



Объекты транспортной инфраструктуры



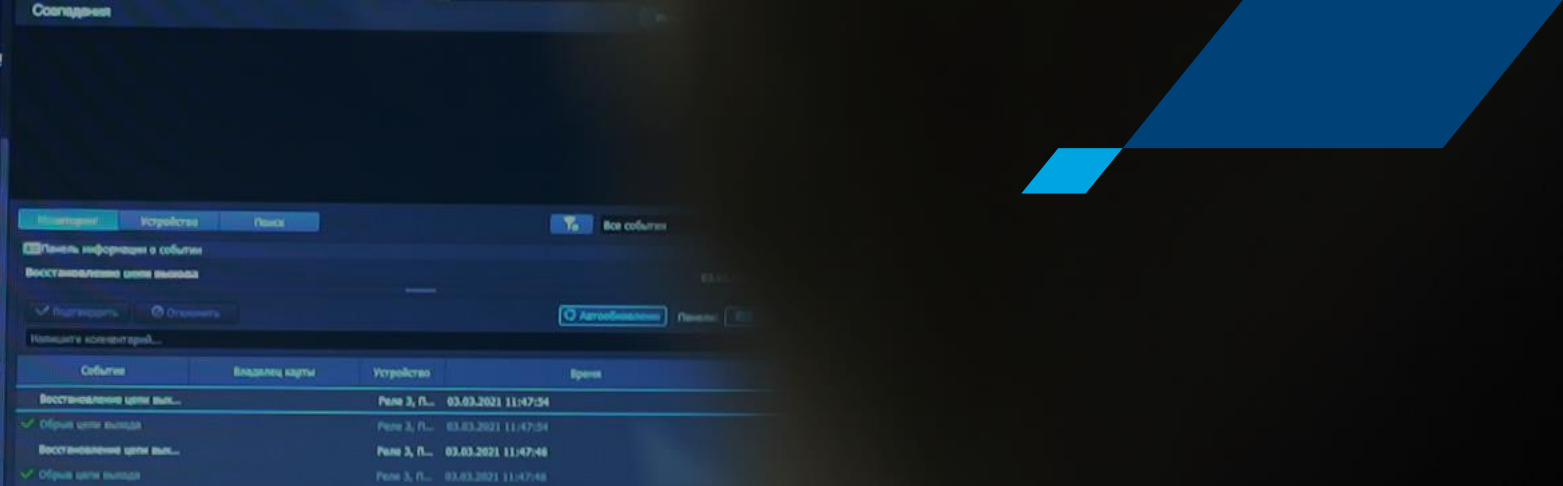
Территориально-разделенные объекты

SecurOS Dispatcher — программная платформа для оперативного централизованного контроля и автоматизированного управления Инцидентами: тревожными событиями и процессами, связанными с обеспечением безопасности, на крупных инфраструктурных объектах.

SecurOS Dispatcher собирает и обрабатывает данные от множества несвязанных между собой подсистем и устройств, предоставляет пользователям возможность управлять ими, а также работать с Инцидентами, источниками которых являются события, получаемые от интегрированных подсистем и устройств.

Платформа обеспечивает эффективную работу иерархически организованных диспетчерских служб, и их оперативное взаимодействие с зависимыми структурами и автономными ведомствами через единый интерфейс.

НАЗНАЧЕНИЕ



Централизованное управление безопасностью — интеграция разрозненных независимых программных и инженерно-технических средств обеспечения безопасности, мониторинга и контроля;

Поддержка должного уровня защищенности объектов — круглосуточный централизованный контроль состояния всего комплекса интегрированных средств;

Моментальная реакция на нештатные ситуации — непрерывная регистрация Инцидентов;

Повышение эффективности работы персонала — средства автоматизации и система поддержки принятия решений в удобном пользовательском интерфейсе;

Аудит действий пользователей — протоколирование действий операторов в целях контроля и оптимизации их работы;

Полная информированность о состоянии защищенности предприятия — формирование отчетов об Инцидентах и действиях операторов для последующего анализа и принятия управленческих решений.

ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Создание и редактирование типов Инцидентов (простых и составных);
- Управление статусом активности типов Инцидентов;
- Настройка индивидуальных сценариев обработки для каждого типа Инцидента;
- Задание инструкций* по выполнению регламентных процедур для каждого типа Инцидента
- Назначение ролей пользователям системы;
- Оперативное управление интегрированными датчиками через план-схему объектов;
- Возможность переключения части интегрированных устройств или отдельных локаций в режим «повышенного внимания»;
- формирование отчетов по действиям пользователей;
- Формирование отчетов по инцидентам.
- Ведение справочника организаций и персонала, допущенного к выполнению работ на соответствующей локации;
- Учет плановых работ.

* Инструкции включают требования и рекомендации по выполнению действий, которые должны произвести операторы тех или иных ролей для обработки Инцидента;

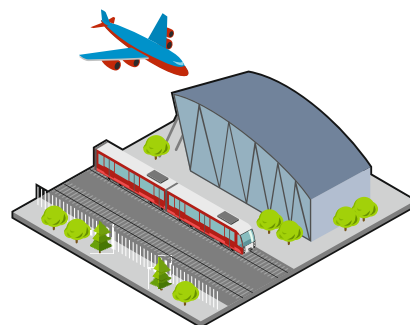
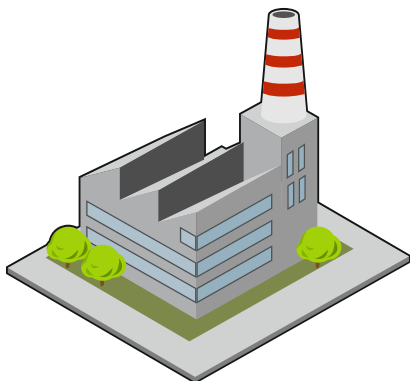
ОТРАСЛЕВАЯ НАПРАВЛЕННОСТЬ

Объекты топливно-
энергетического
комплекса



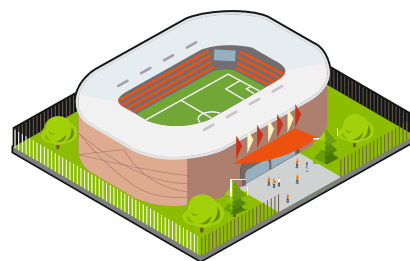
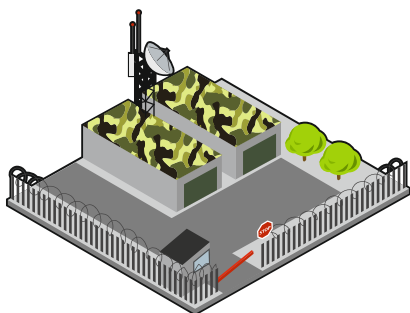
Дорожная
инфраструктура

Промышленные
предприятия



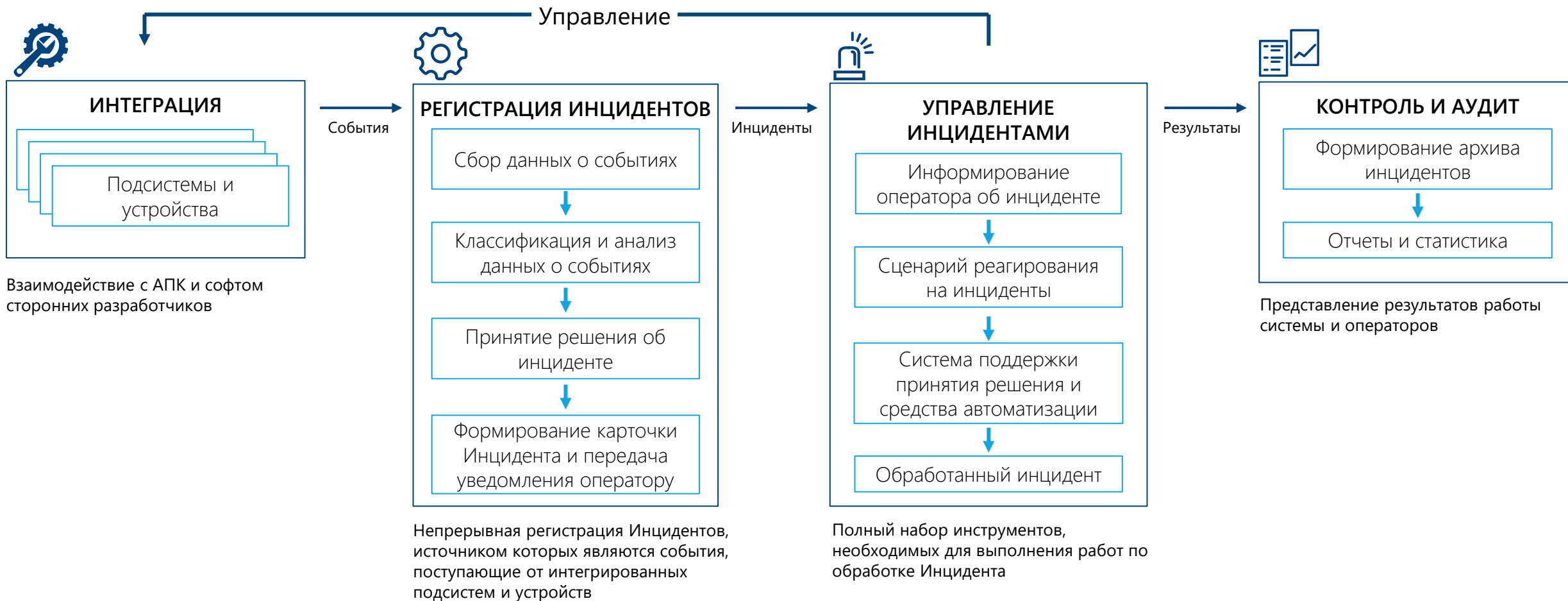
Транспортная
инфраструктура

Силовые
ведомства



Культурные и
спортивные
объекты

ОБЩИЙ ПРИНЦИП РАБОТЫ SECUROS DISPATCHER



ИНТЕГРАЦИЯ СТОРОННИХ СИСТЕМ И УСТРОЙСТВ В SECUROS DISPATCHER



Контроль периметра



Видеонаблюдение



СКД, СКУД



Видеоаналитика*



Шлагбаумы, турникеты, болларды



Информационные табло



Пожарная сигнализация



Световая сигнализация



Контрольные и охранные датчики



Весоизмерительное оборудование



Односторонняя и двусторонняя аудио связь



Досмотр днищ транспортных средств

* SecurOS Dispatcher поддерживает работу с множеством различных видеоаналитических детекторов и комплексов:

- Поведенческая аналитика (запрещенная зона, толпа, празднование, др.)
- Детекция и распознавание лиц людей
- Распознавание регистрационных знаков транспортных средств, номеров ж/д вагонов, номеров ISO-контейнеров
- Детекция аварий и нестандартных ситуаций на дорогах
- Контроль ношения защитных масок, наличия повышенной температуры тела, соблюдения дистанции
- Контроль выполнения технологических процессов и производственных регламентов
- Контроль соблюдения правил техники безопасности и ношения средств индивидуальной защиты
- Контроль качества выпускаемой продукции и маркировки продукции и пр.

ДЕТЕКЦИЯ ИНЦИДЕНТОВ



На основе событий, полученных от интегрированных систем/устройств, создаются правила генерации Инцидентов.

Инциденты могут быть простыми — состоящими из одного события, и составными — состоящими из нескольких событий, которые должны произойти за настраиваемый интервал времени.

Инциденты категорируются по двум трехуровневым параметрам:

1. «Приоритет» — по типу устройства
2. «Зона» — по месту нахождения устройства

По умолчанию критичность Инцидента оценивается по значению параметра «Зона», где 1 - это наиболее критичный инцидент, 3 - наименее критичный инцидент. Но если у устройства также настроен параметр «Приоритет», то он автоматически поднимает критичность Инцидента до своего значения.

Для каждого типа Инцидента настраиваются пошаговые инструкции — индивидуальные сценарии обработки, предписывающие выполнение конкретных операций в определенном порядке для тех или иных ролей пользователей.

Для каждого типа Инцидента можно настроить необходимое количество сценариев обработки — в зависимости от значения критичности Инцидента.

Сформированная «Карточка» Инцидента передается в обработку оператору согласно его роли и сценарию обработки.

ДЕТЕКЦИЯ ИНЦИДЕНТОВ | ИНТЕРФЕЙС АДМИНИСТРАТОРА



Выбор типов Инцидентов
для обработки системой

Создание новых типов Инцидентов

Создание и настройка
схем действий оператора

Главная | Типы инцидентов

Типы инцидентов

Показаны записи 1-20 из 24.

Код события	Название	
✗ MD_START	CAM-MD_START2	✎
✗ VCA_EVENT	CAM-VCA_EVENT	✎
✓ CONFIG_CORRUPTED	BOLID_CONFIG_CORRUPTED	✎
✓ ACCESS_ALARM	BOLID_LOOP-ACCESS_ALARM	✎
✓ FIRE_ALARM	BOLID_LOOP-FIRE_ALARM	✎
✓ AFSS_LAUNCH	BOLID_LOOP-AFSS_LAUNCH	✎
✓ QUIET_ALARM	BOLID_LOOP-QUIET_ALARM	✎
✓ ZONE_ALARM	BOLID_LOOP-ZONE_ALARM	✎
✓ RELAY_STATE_CHANGE	BOLID_RELAY-RELAY_STATE_CHANGE	✎
✓ RELAY_ON	BOLID_RELAY-RELAY_ON	✎
✓ NETWORK_ALARM	BOLID_CONTROLLER-NETWORK_ALARM	✎
✓ POWER_OUTPUT_DETACHED	BOLID_CONTROLLER-POWER_OUTPUT_DETACHED	✎
✓ TEMP_INCREASED	BOLID_CONTROLLER-TEMP_INCREASED	✎
✗ ACCESS_DENIED	BOLID_READER-ACCESS_DENIED	✎
✗ ALARM	BOLID_DEVICE-ALARM	✎
✓ DETACH	CAM-DETACH	✎
✓ DISCONNECTED	SLAVE-DISCONNECTED	✎

Добавить тип | Добавить схему

Главная | Создание типа инцидента

Создание типа инцидента

Условия формирования инцидента

Тип датчика: Код события:

Статус:

Приоритет:

Регламент работ:

Для отображения регламента в виде списка используйте HTML-теги UL и LI

Сценарий обработки:

Создать | Сохранить

Главная | Редактирование цепочки действий оператора

Редактирование цепочки действий оператора

Добавить действие

Подтверждение инцидента
Назначение ERP
Выполнение действий согласно регламента
Качественная идентификация пользователя
Специальный порядок взаимодействия и модуль анализа
Специальные действия по реагированию
Закрытие инцидента

Название схемы:

Название карточки:

Отправить

Настройки

Показаны записи 1-1 из 1.

Параметр	Значение	
Длина временного промежутка для составного инцидента (в секундах)	600	✎

УПРАВЛЕНИЕ ИНЦИДЕНТОМ



Оператор обрабатывает Инцидент, выполняя действия согласно регламенту предприятия, зафиксированному в пошаговой инструкции, которая сопровождает карточку Инцидента.

Оператор обязан зафиксировать выполнение каждого этапа инструкции в интерфейсе SecurOS Dispatcher, поэтому не сможет пропустить этап или изменить очередность выполнения.

Если оператор не принял Инцидент в обработку в течение обозначенного времени, тот автоматически эскалируется на уровень выше.

При необходимости временно покинуть рабочее место, оператор отправляет запрос старшему оператору. Одобрив запрос, старший оператор переназначает Инциденты на другого оператора.

Базовый список действий оператора в рамках обработки Инцидента:

- Обработка инцидента — выполнение действий в соответствии с регламентом;
- Быстрый переход к просмотру живого видео с камер или к просмотру записи Инцидента в архиве;
- Смена приоритета Инцидента;
- Отправка задания ГБР;
- Переход к объектам на карте;
- Управление объектами;
- Добавление текстовых комментариев и прикрепление файлов, подтверждающих выполнение регламентных процедур;
- Формирование кратких и полных (с картинками) отчетов об инцидентах (pdf)
- Перенаправление Инцидентов заместителю на время рабочих перерывов диспетчеров.

УПРАВЛЕНИЕ ИНЦИДЕНТОМ | ИНТЕРФЕЙС ОПЕРАТОРА



Вкладка «Инциденты»

НЕ РАССМОТРЕНО **237**

67 Проникновение 10:46

1 Срабатывание модуля газового пожаротушения 10:46

1 Хулиганство 10:47

! Авария 10:48

67 Авария 10:46

67 Срабатывание модуля 10:46

67 Авария 10:46

67 Авария 10:46

Срабатывание модуля газового пожаротушения
24 Май 2019 12:21 2434039539 Ожидание отчета

МЕСТОПОЛОЖЕНИЕ
64 КП № 17
Эстакада на продолжении Предлаторовой улицы в составе магистрали на сваях Дачный проспект- Предлаторова улица
Лестница, Съезд, Правая полоса

ИСТОЧНИК
Просмотрено
Воспроизвести отрезок
Перейти к камере
Местоположение на карте

КАМЕРА
CAM_01
Камера в коридоре с левой стороны

Отреagirовать Передать Ложное срабатывание

ИСТОРИЯ ДЕЙСТВИЙ
22 Май 2019
00:23 **Вадим Кабачков** Закрыл инцидент по причине:
00:02 **Вадим Кабачков** ГБР прибыла на место
21 Май 2019
23:23 **Вадим Кабачков** Рассмотрел заявку
23:23 **Артемий Петрушкин** Назначил ГБР
23:22 **Артемий Петрушкин** Изменил тип происшествия с «Авария» на «Хулиганство»
23:16 **Артемий Петрушкин** Рассмотрел заявку

Лента Инцидентов

Область работы с Инцидентом

История действий

Область работы

- Для начала обработки инцидента оператору ПУ ОТВ необходимо нажать кнопку «Отреagirовать».
- И обработка инцидента необходимо приступить в течение 2 минут после его появления, в противном случае инцидент будет эскалирован на уровень ЕДЦ.
- В случае нестандартной ситуации, по которой отсутствует регламенты обработки тревоги, требуется нажать кнопку «Передать» для оповещения оператора ЕДЦ об инциденте и его приоритизации.
- В случае ложного срабатывания датчика, необходимо отметить инцидент как Ложный с соответствующими комментариями для сохранения в истории инцидентов.
- Любая последующая обработка ложного инцидента происходит только старшим операторами с соответствующими правами доступа.
- В случае повторного срабатывания инцидента необходимо передать инцидент в работу Бригаде ГБР. В данном случае в карточке событий будет зафиксировано время передачи, и бригада ГБР будет доступна просмотр связанных с инцидентом материалов в реальном времени.
- После завершения всех действий согласно регламенту, данный этап фиксируется оператором в электронной форме карточки события с фиксацией времени и обстоятельств аварии.
- Все обработанные инциденты доступны для дальнейшего анализа и эскорта материалов из архива старшему оператору ЕДЦ.

Регламент обработки инцидента

АУДИТ



Действия пользователей в системе протоколируются. Система контролирует весь процесс работы оператора, вычисляет время реакции на каждый Инцидент, собирает статистику по действиям. Эти данные могут быть оформлены в виде файла отчета. Поддерживается выборка по дате или интервалу, по оператору, по типу Инцидента, по результату обработки Инцидента.

Также системой поддерживается формирование отчетов по Инцидентам (по типу, периоду, зоне и пр.) с последующей выгрузкой в файл.

Данные отчетов используются для последующего анализа и принятия управленческих решений.

Краткий отчет

Дата формирования отчета: 18.09.2023 13:03

Количество инцидентов: 2
Ложное срабатывание: 1
Подтверждено: 1

Дата	Статус	Локация	Работа	Ответственный	Датчик	Тип инцидента	Приоритет
18.09.2023 13:01	Ложное срабатывание	32 км		elder	4.20.646.2.5 (тип: CAM)	Срабатывание анализки	Приоритет зоны: 1 Приоритет датчика: 1
18.09.2023 13:02	Подтвержен	32 км		elder	4.20.668.1.2 (тип: CAM)	Срабатывание анализки	Приоритет зоны: 1 Приоритет датчика: 1

Полный отчет (многостраничный)

Полный отчет по инцидентам

Количество инцидентов: 2
Ложное срабатывание: 1
Подтверждено: 1



Дата: 18.09.2023 13:01
Статус: Ложное срабатывание
Локация: 32 км
Работа:
Ответственный: elder
Датчик: 4.20.646.2.5 (тип: CAM)
Тип инцидента: Срабатывание анализки
Приоритет: Высокий
ГРП: По назначению или по назначению работы
История действий оператора:
18.09.2023 13:01 - elder: Смена статуса инцидента. Ложное срабатывание



Дата: 18.09.2023 13:02
Статус: Подтвержен
Локация: 32 км
Работа:
Ответственный: elder
Датчик: 4.20.668.1.2 (тип: CAM)
Тип инцидента: Срабатывание анализки
Приоритет: Высокий
ГРП: По назначению или по назначению работы

История действий оператора:
18.09.2023 13:02 - elder: Смена статуса инцидента. В работу
18.09.2023 13:02 - elder: Подтверждение инцидента
18.09.2023 13:02 - elder: Передача Тим Аналитик (Тит)
18.09.2023 13:02 - elder: Выявление дефектов системы управления
18.09.2023 13:03 - elder: Завершение инцидента
18.09.2023 13:03 - elder: Смена статуса инцидента. Архивный

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

1. Комплексная защита инфраструктуры предприятия от угроз безопасности за счет консолидации всей доступной информации по Инциденту и автоматизации действий по реагированию

2. Оптимизация затрат на внедрение за счет отсутствия необходимости замены отдельных подсистем и устройств. Нет привязки к определенным вендорам

3. Максимальная оперативность в противодействии нарушениям и при урегулировании нештатных ситуаций и снижение влияния человеческого фактора за счет использования инструментов автоматизации и системы поддержки принятия решений

4. Улучшение трудовой дисциплины за счет наличия системы протоколирования действий диспетчеров

5. Повышение осведомленности о ситуации в целях содействия принятию управленческих решений



ISS — Интеллектуальные Системы Безопасности
Россия, Москва, ул. Мневники 17
+7 (495) 645-2121 | info@iss.ru | <https://iss.ru>

