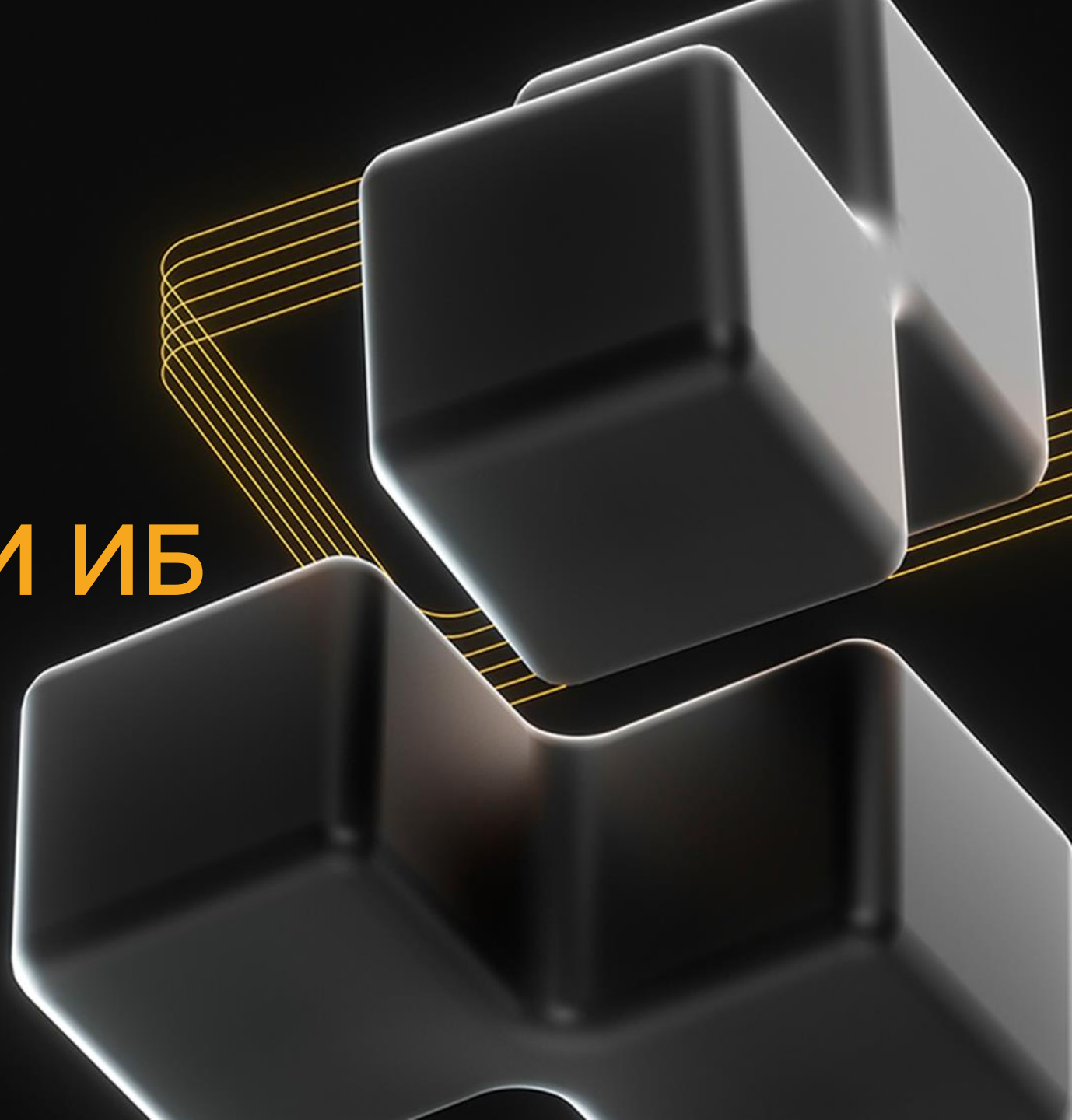
ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ

Эффективное внедрение решений SOAR



С чем сталкиваются крупные промышленные предприятия?

Стремительно меняющиеся тренды киберугроз требуют постоянного повышения квалификации сотрудников

Отсутствие типовых сценариев реагирования для всех видов инцидентов ИБ приводит к увеличению трудозатрат предприятий — на каждый сценарий разрабатывается новый процесс

Большой объем рутинных операций по обработке инцидентов ИБ приводит к неэффективному распределению ресурсов и выгоранию специалистов

Длительные сроки обработки инцидентов безопасности могут привести к ущербу вследствие простоя технологического процесса

Влияние человеческого фактора на процесс реагирования на инциденты ИБ может привести к репутационным и финансовым потерям

Процессы, которые возможно автоматизировать

Категорирование объектов КИИ

Классификация объектов защиты

Моделирование угроз

Контроль соответствия требованиям ИБ

Управление инцидентами, рисками и мероприятиями

Работа с документами по направлению

Инструменты автоматизации

SGRC (Security Governance, Risk Management and Compliance)

автоматизирует управление информационной безопасностью, рисками и соответствием требованиям законодательства

SOAR (Security Orchestration, Automation and Response)

автоматизирует процессы реагирования на инциденты ИБ, обеспечивают оркестрацию средств защиты информации
и обогащение данных о событиях безопасности

TIP (Threat Intelligence Platform)

обеспечивают обогащение систем управления ИБ данными киберразведки на основе открытых источников и баз данных ведущих игроков рынка

Security Awareness

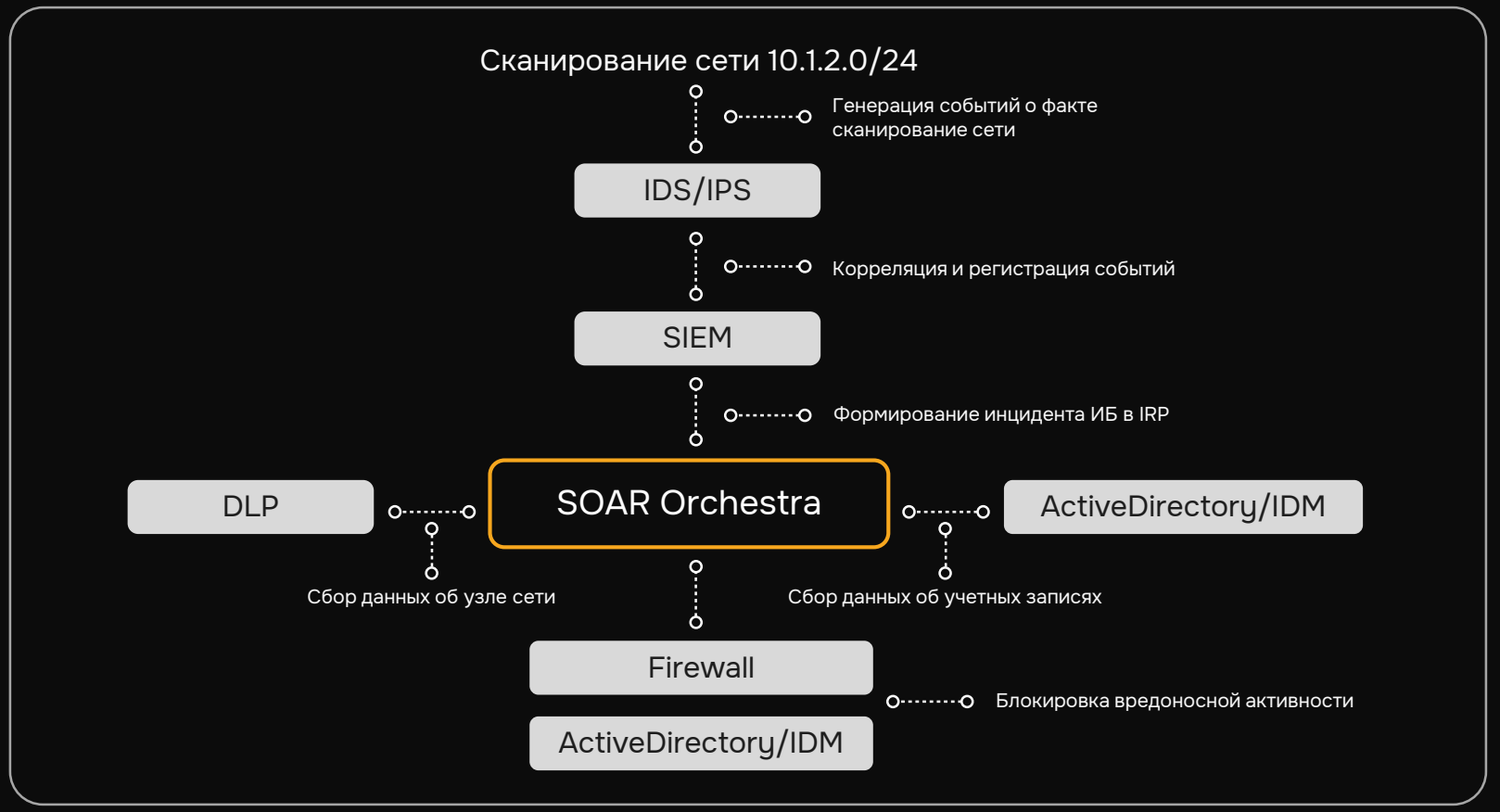
автоматизирует процесс повышения осведомленности персонала в области обеспечения ИБ

SOAR – инструмент автоматизации управления ИБ

- Управление ИТ-активами
- Регистрация, обработка и учет всех событий и инцидентов
- Обогащение данных об инцидентах
- Ранжирование событий по степени риска
- Автоматическое выполнение рутинных задач аналитика
- Запуск сценариев реагирования на инциденты ИБ (плейбуки)
- Координация средств защиты информации (оркестрация)
- Взаимодействие с ГосСОПКА

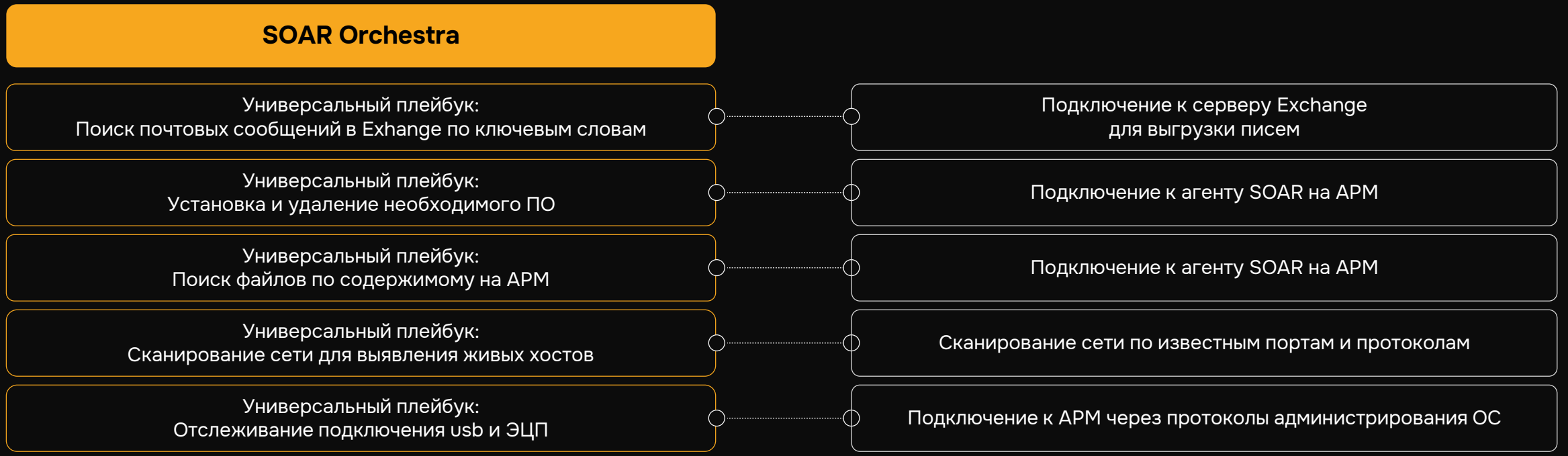
SOAR – гибкая система объединения систем защиты информации

Объединяя различные системы защиты в инфраструктуре компании,
SOAR позволяет автоматизировать реагирование на типовые инциденты ИБ



SOAR – централизованная система по обогащению данными

SOAR позволяет осуществлять централизованный сбор дополнительной информации по инцидентам ИБ. Также может служить инструментом для обогащения активами или другими артефактами.



Для кого SOAR может стать необходимым инструментом?

Численность сотрудников >1000	SOAR может помочь повысить эффективность работы с IT-активами, упрощая процессы инвентаризации и уменьшая вероятность ошибок
Ограниченные ресурсы	SOAR позволяет сократить время реакции на инциденты безопасности
Работа с большими данными	SOAR может автоматически выполнять рутинные задачи при обработке различных данных. Это может значительно сократить время и усилия, затрачиваемые на эти процессы
Большое количество типовых инцидентов	SOAR помогает в автоматическом реагировании на типовые инциденты, что сокращает время реагирования и уменьшает вероятность ошибок

Отрасли

Банки и финансовые компании | Госсектор | ИТ и телеком | Энергетика | Металлургия

Машиностроение | Сельское хозяйство | Торговля | Транспорт | Нефтегаз

Как SOAR поможет вашему бизнесу?

Даст возможность действовать на опережение и снизить возможные риски

Вовремя обнаруженные и оперативно обработанные инциденты помогут существенно снизить риск успешной кибератаки, минимизировать возможный финансовый и репутационный ущерб для компании

Позволит соответствовать отраслевым нормативам и внутренним стандартам

Системный взгляд на защищенность инфраструктуры позволит привести ее в соответствие требованиям регуляторов — например, регламентам ФСТЭК России (указам №187 и №239, приказу №21)

Поможет решить кадровый вопрос и снизить нагрузку на персонал

Автоматизация процессов управления ИБ уменьшает количество обрабатываемых вручную инцидентов, тем самым высвобождает человеческий ресурс и закрывает потребность в поиске дорогостоящих специалистов

Организует учет активов, типизацию инцидентов и сформирует сквозную аналитику

Система представляет данные по происшествиям и объектам защиты в наглядных дашбордах, графиках и таблицах, с которыми удобно работать и использовать в отчетах

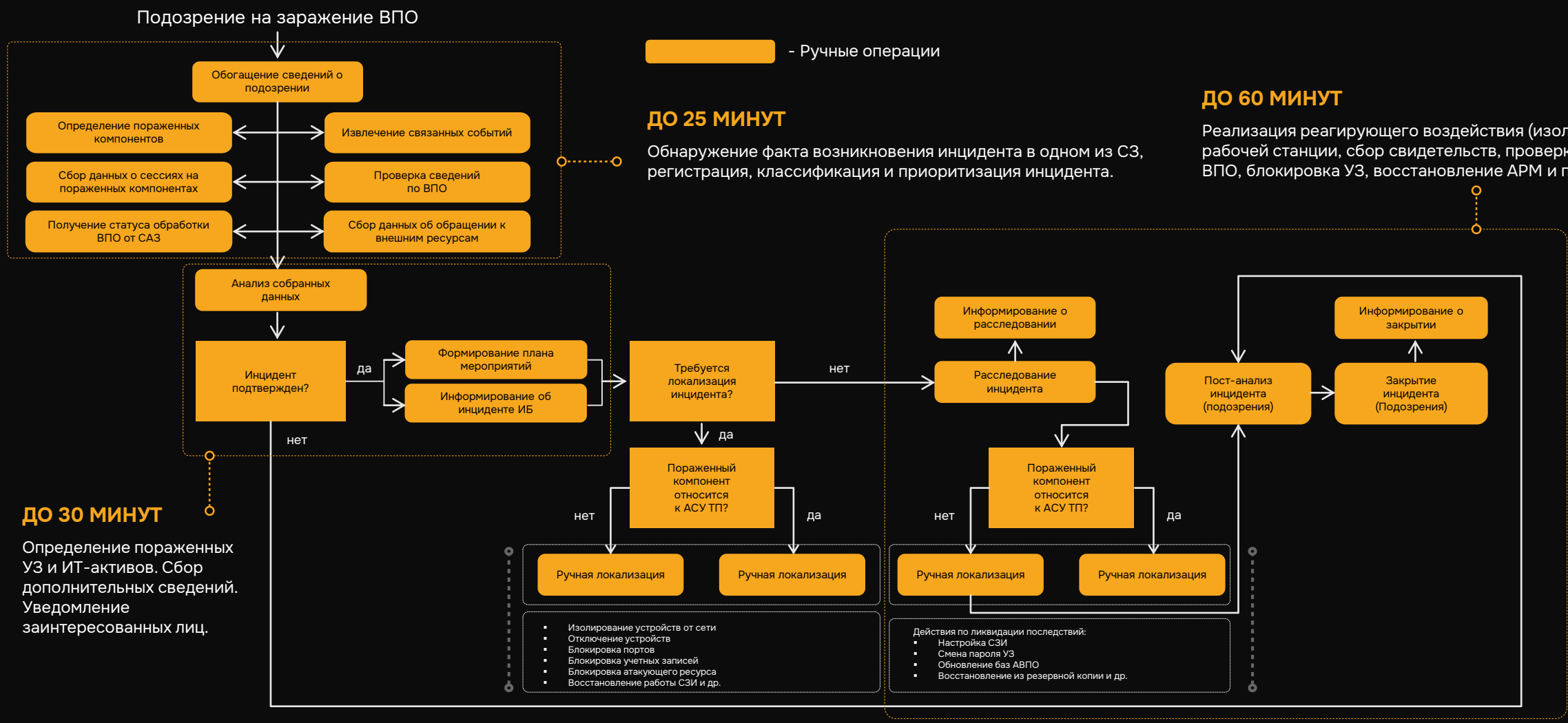
Около **70%** операций может быть автоматизировано

Скорость реагирования может быть увеличена в **480 раз**

Инцидент «Выявление вредоносной активности на оборудовании»: скорость реагирования

Действие	С SOAR-платформой	Без SOAR-платформы
Обнаружение факта возникновения инцидента в одном из средств защиты, регистрация, классификация и приоритизация инцидента	5 сек	10 мин
Определение пораженных учетных записей и ИТ-активов. Сбор дополнительных сведений. Уведомление заинтересованных лиц	5 сек	5-10 мин
Проверка IOC в Threat Intelligence базах, историческая корреляция инцидентов	5 сек	20 мин
Реализация реагирующего воздействия (изоляция рабочей станции, сбор свидетельств, проверка на ВПО, блокировка учетной записи, восстановление АРМ и пр.)	5 сек	40-60 мин
Фиксация событий, ведение задач по инциденту, подготовка отчетности для руководства	5 сек	20-30 мин
Скорость реагирования	До 1 минуты	До 95 минут

Инцидент «Выявление вредоносной активности на оборудовании»: автоматизация шагов по обработке инцидента (до)



ДО 25 МИНУТ

Обнаружение факта возникновения инцидента в одном из СЗ, регистрация, классификация и приоритизация инцидента.

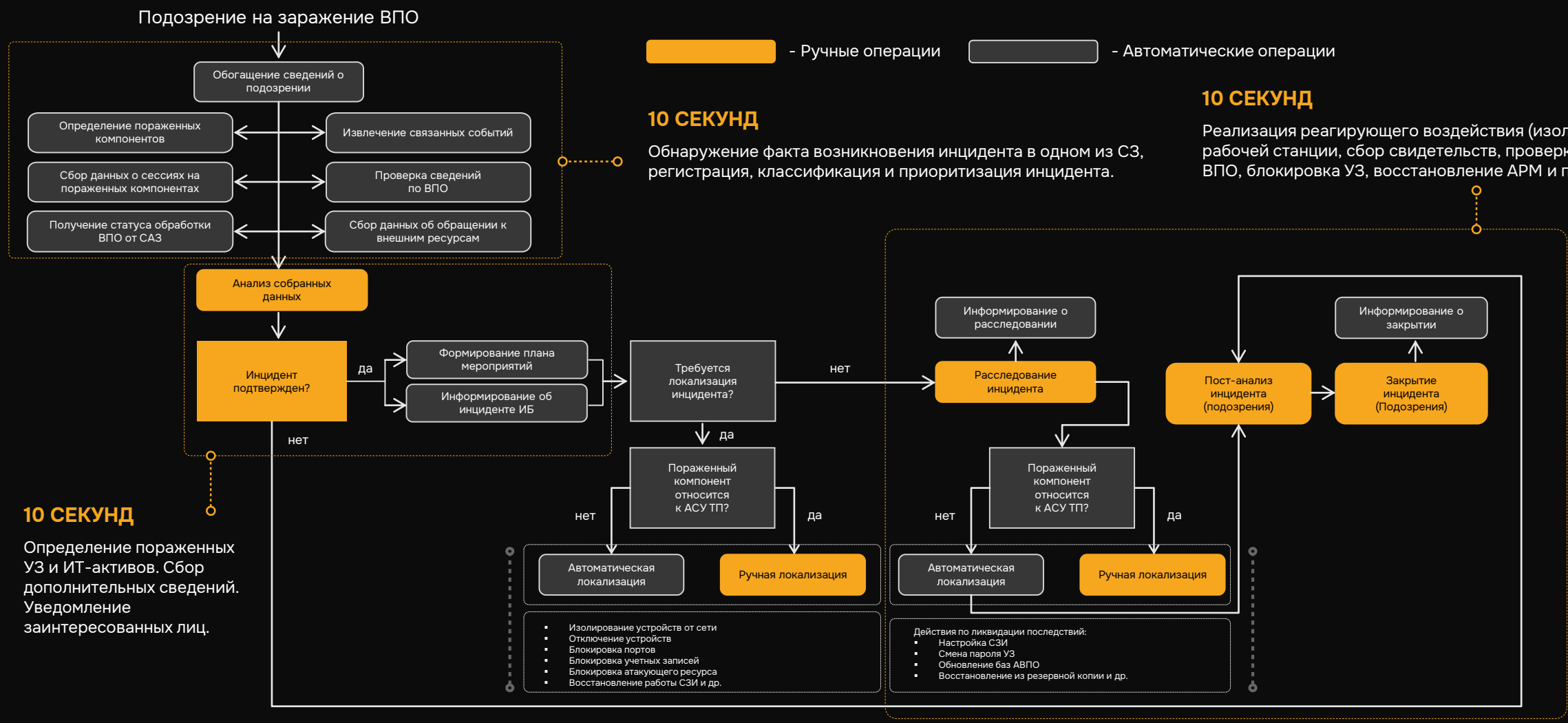
ДО 60 МИНУТ

Реализация реагирующего воздействия (изоляция рабочей станции, сбор свидетельств, проверка на ВПО, блокировка УЗ, восстановление АРМ и прочее).

ДО 30 МИНУТ

Определение пораженных УЗ и ИТ-активов. Сбор дополнительных сведений. Уведомление заинтересованных лиц.

Инцидент «Выявление вредоносной активности на оборудовании»: автоматизация шагов по обработке инцидента (после)



10 СЕКУНД

Обнаружение факта возникновения инцидента в одном из СЗ, регистрация, классификация и приоритизация инцидента.

10 СЕКУНД

Определение пораженных УЗ и ИТ-активов. Сбор дополнительных сведений. Уведомление заинтересованных лиц.

10 СЕКУНД

Реализация реагирующего воздействия (изоляция рабочей станции, сбор свидетельств, проверка на ВПО, блокировка УЗ, восстановление АРМ и прочее).

Инцидент «Выявление ВПО на оборудовании»

Оценка эффективности SOAR

До внедрения SOAR

- 23 ручных операций
- Реагирование до 95 минут

После внедрения SOAR

- 7 ручных операций
- 16 операций автоматизировано
- Реагирование до 1 минуты

Как выбрать SOAR?

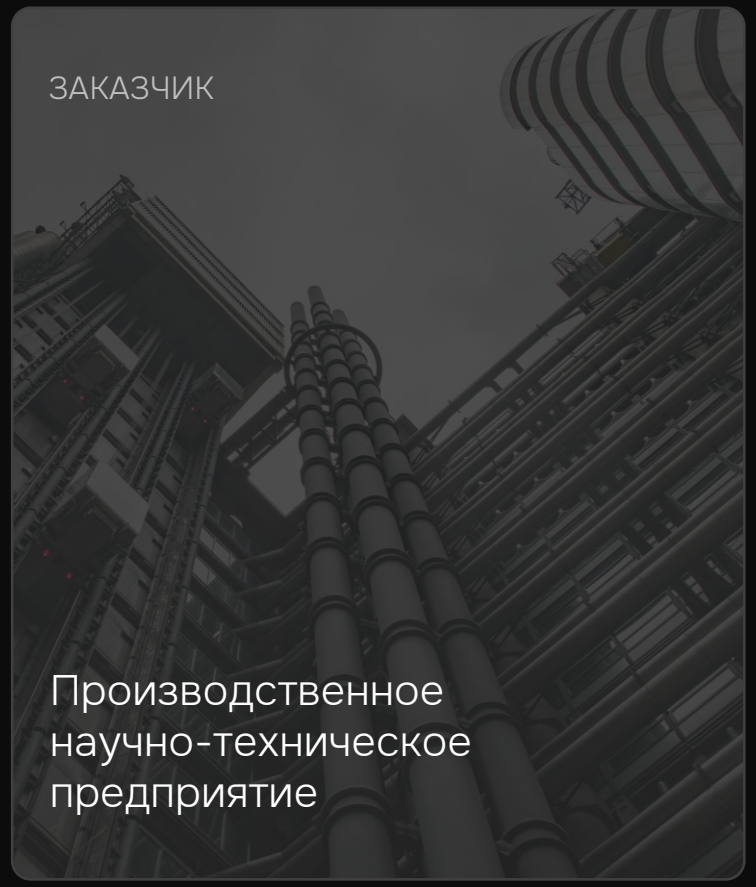
- Набор планов мероприятий и сценариев реагирования «из коробки»
- Качество интеграции с наиболее распространенными системами ИТ-инфраструктуры
- Мультитенантность или возможность изолированно обслуживать пользователей из разных организацией
- Возможности кастомизации (low-код платформы)
- Легкость настройки

Как оценить эффективность инструмента?

Критерии оценки эффективности внедрения SOAR

- Среднее время реагирования на инцидент до и после внедрения
- Доля операций, выполняемых в автоматическом режиме
- Количество инцидентов, обрабатываемых одним специалистом в единицу времени
- Операционные расходы на ликвидацию последствий инцидентов до и после внедрения, а также расходы на персонал
- Количество инцидентов, требующих участия специалиста до и после внедрения SOAR (данный показатель достигается за счет автоматической проверки подозрений на ложно-положительные сработки)

Кейс: внедрение ePlat4m Orchestra на промышленном предприятии



ЗАКАЗЧИК

Производственное научно-техническое предприятие

ЗАДАЧА

Выполнить требование регулятора по обработке инцидентов, создать удобный механизм обогащения данными

ЧТО СДЕЛАНО?

Подобрано и внедрено решение класса SOAR. Настроены модули интеграции с 6 системами для сбора активов (KSC, MP VM, Efros CI, ActiveDirectory) и информации об инцидентах (DLP, SIEM), а также функции SOAR по обработке этих данных. Разработан контент — готовые механизмы по обогащению инцидентов.

РЕЗУЛЬТАТ

Предприятие получило готовый инструмент по обработке инцидентов в формате единого окна. Здесь консолидируются все активы и события ИТ-инфраструктуры, происходит автоматическое обогащение и реагирование на события ИБ.

Преимущества работы с Центром кибербезопасности УЦСБ

Проектное управление

Над решением вашей задачи будет работать целая команда. Четкое распределение зон ответственности и ролей поможет обеспечить сдачу проекта в срок с результатами, отвечающими вашим ожиданиям или даже выше

Гибкость и фокусный подход

Мы не работаем по шаблону, а отталкиваемся от вашей специфики и потребностей, формируя состав услуг индивидуально. Качество нашей работы определяет ее польза для вашего бизнеса

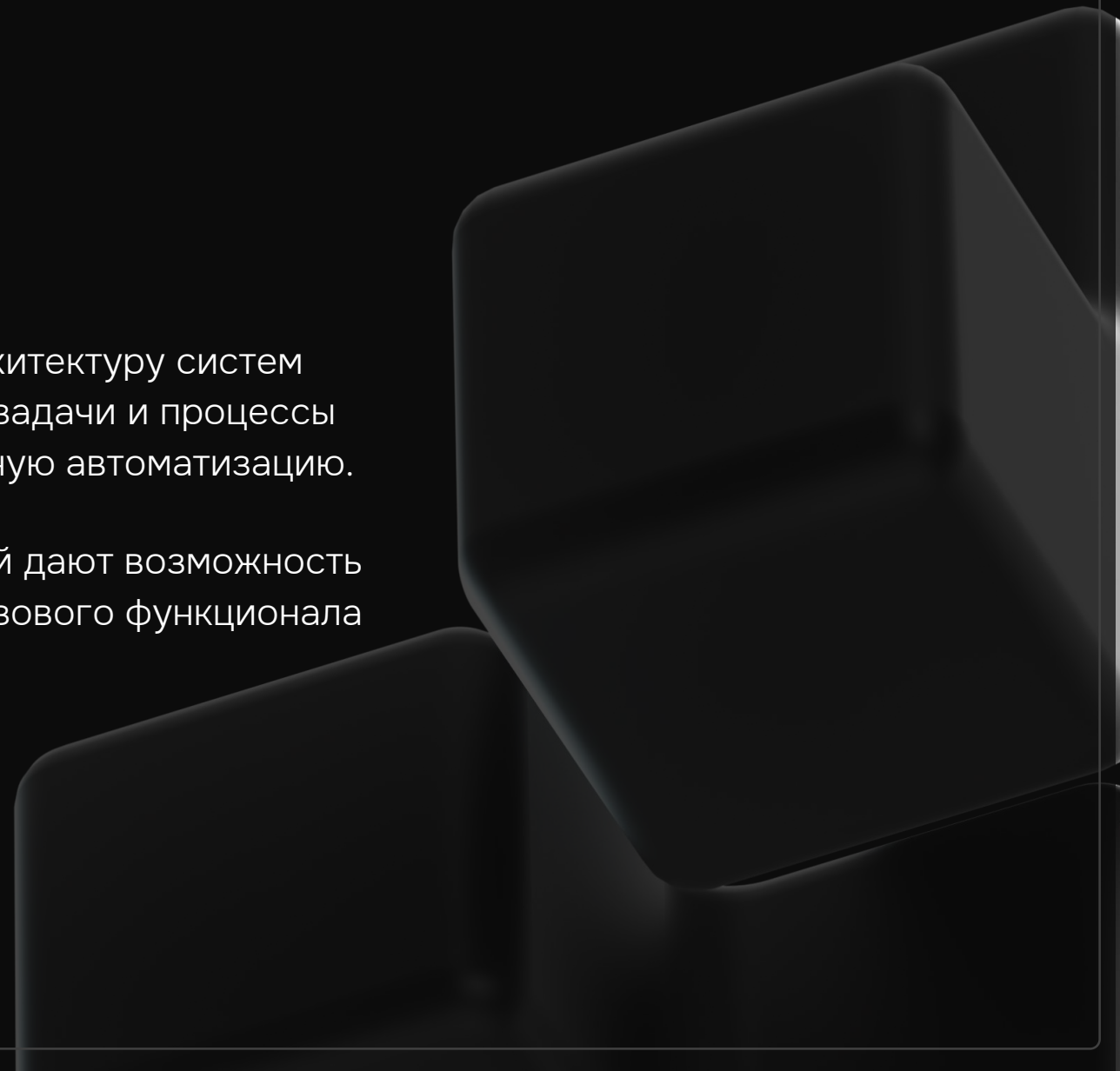
Все компетенции и инструменты в одном месте

Центр кибербезопасности УЦСБ объединяет исчерпывающий комплекс инструментов и услуг в области ИБ.
Какая бы потребность не возникла у вас завтра, мы всегда сможем предложить для нее адекватное решение.

Команда и экспертиза

Компетенции команды и глубокое погружение в архитектуру систем класса SOAR позволяют точно переложить бизнес-задачи и процессы на логику работы платформы, настроить качественную автоматизацию.

Партнерские отношения с разработчиками решений дают возможность обеспечить кастомную настройку и расширение базового функционала при необходимости.



ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

sec.ussc.ru

cybersec@ussc.ru