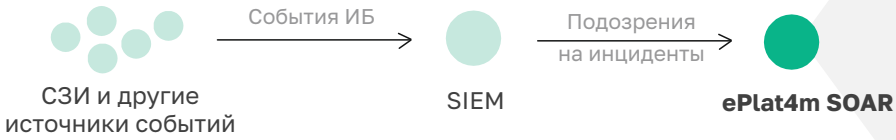
udv|group

UDV ePlat4m SOAR

Автоматизация деятельности центров противодействия киберугрозам

Интегрированная платформа оркестрации средств защиты информации и автоматизации функций информационной безопасности. Предназначена для обогащения данных, автоматической предварительной оценки и автоматизированного реагирования на основные типы инцидентов компьютерной безопасности.



- Оркестрация средств защиты информации
- Автоматизация выполнения рутинных операций службы ИБ
- Управление процессом реагирования на инциденты

ОРКЕСТРАЦИЯ

- Взаимодействие с внутренними информационными системами предприятия и внешними источниками информации в рамках сбора дополнительных сведений об инциденте
- Реализация реагирующего воздействия на любых компонентах ИТ-инфраструктуры (рабочие станции, серверное и сетевое оборудование и т.д.) при возникновении инцидента
- Централизованное управление средствами защиты информации

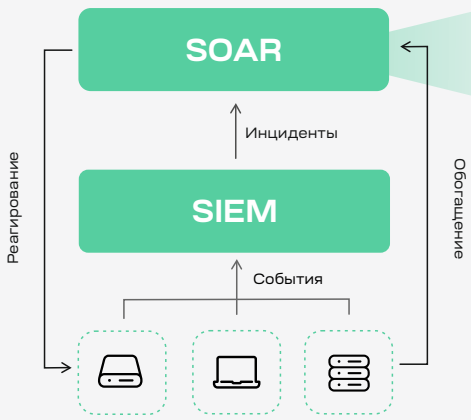
АВТОМАТИЗАЦИЯ

- Автоматическое выполнение плейбуков, формируемых из коллекции заранее разработанных производителем скриптов
- Автоматическое выполнение рутинных задач, которые ранее производились вручную
- Среда разработки и тестирования собственных скриптов и плейбуков

РЕАГИРОВАНИЕ

- Компетенции вендора по реагированию на различные типы инцидентов
- Управление процессами реагирования на инциденты и жизненным циклом инцидентов
- Ведение статистики, построение аналитических панелей мониторинга, формирование отчетности, направление уведомлений

UDV ePlat4m SOAR также включает модуль управления активами (Security CMDB). Модуль предназначен для формирования и поддержания в актуальном состоянии в режиме реального времени всеобъемлющей базы знаний об ИТ-активах, зависимостях между ними, а также связанных с ними ИБ-атрибутах. Данная информация предоставляется пользователю и внешним информационным системам как источник мастер-данных.



ИНФРАСТРУКТУРНЫЙ УРОВЕНЬ

UDV ePlat4m SOAR
SOAR-платформа для построения SOC организации, оркестрации средств защиты и автоматизации процессов реагирования на инциденты ИБ.

udv ePlat4m

Платформа для автоматизации бизнес-процессов и создания собственных приложений без навыков программирования:

- Визуальное «кодирование»
- Быстрая адаптация под требования Заказчика
- Лёгкая интеграция в ИТ-инфраструктуру
- Быстрое освоение персоналом

ВЫГОДЫ ОТ ВНЕДРЕНИЯ

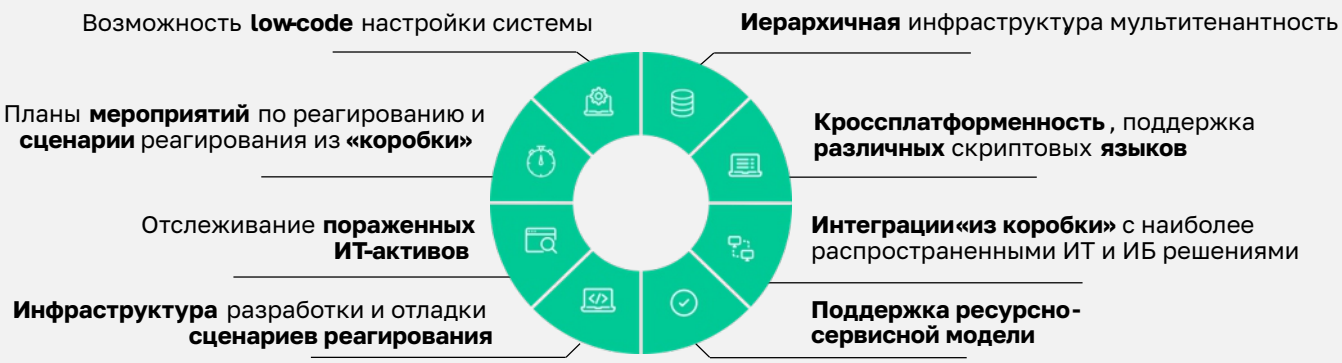
- Уменьшение числа обрабатываемых «вручную» инцидентов с 10 000 до 500
- Снижение времени реагирования на инцидент с 3 дней до 25 минут
- Автоматическая реакция для 30% инцидентов

Автоматизация процесса управления инцидентами → Уменьшение времени реагирования на инциденты и минимизация ущерба от них

Готовые сценарии реагирования на инциденты и сбор дополнительной информации → Повышение качества реагирования на инциденты

Автоматическое выполнение операций и проверка на ложно-положительные срабатывания → Уменьшение вероятности возникновения рисков, связанных с человеческим фактором

Уменьшение количества ручных операций → Снижение нагрузки на аналитиков ИБ



БЫСТРЫЙ СТАРТ: LITE-ВЕРСИЯ ДЛЯ АВТОМАТИЗАЦИИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

UDV ePlat4m IRP Lite — облегченная версия, предназначенная для быстрой автоматизации процесса реагирования на инциденты компьютерной безопасности. Эту версию отличают быстрая скорость инсталляции и первичной настройки за счёт отсутствия подсистемы обогащения данных об инцидентах и автоматических сценариев реагирования.

UDV ePlat4m SOAR	UDV ePlat4m IRP Lite Облегченное решение для автоматизации реагирования на инциденты компьютерной безопасности	UDV ePlat4m IRP Lite
4-6 часов	Длительность инсталляции и первичной настройки	30 мин.
ДА	Автоматизированные сценарии реагирования	ДА
ДА	Обогащение данных о возможных инцидентах	НЕТ
ДА	Плейбуки и автоматические сценарии реагирования	НЕТ
ДА	Оценка последствий инцидентов	ДА
ДА	База знаний и рекомендации по реагированию	ДА
ДА	Контроль SLA и отчетность	ДА