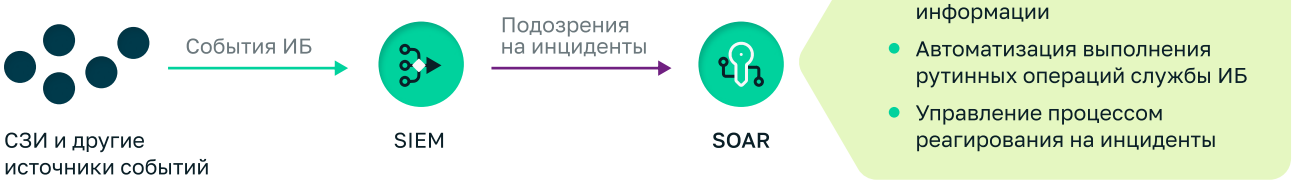
Защита корпоративных сетей

UDV 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

- 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 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 их жизненным циклом
- Ведение статистики, построение аналитических панелей мониторинга, формирование отчетности, направление уведомлений

ХАРАКТЕРИСТИКИ ПРОДУКТА

- Автоматизация процесса управления инцидентами
- Готовые сценарии реагирования на инциденты и сбор дополнительной информации
- Автоматическое выполнение операций и проверка на ложно-положительные срабатывания
- Уменьшение количества ручных операций

ВЫГОДЫ ОТ ВНЕДРЕНИЯ

- Уменьшение времени реагирования на инциденты и минимизация ущерба
- Повышение качества реагирования на инциденты
- Уменьшение вероятности возникновения рисков, связанных с человеческим фактором
- Снижение нагрузки на аналитиков ИБ

Быстрый старт: Lite-версия для автоматизации реагирования на инциденты

UDV 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 SOAR		UDV IRP Lite
4-6 часов	Длительность инсталляции и первичной настройки	30 мин
+	Автоматизированные сценарии реагирования	+
+	Обогащение данных о возможных инцидентах	−
+	Плейбуки и автоматические сценарии реагирования	−
+	База знаний и рекомендации по реагированию	+
+	Контроль SLA и отчетность	+

ВОЗМОЖНОСТИ

Обогащение данными информации о возможных инцидентах

Планы **мероприятий** по реагированию и **сценарии** реагирования из **«коробки»**

Отслеживание пораженных **ИТ-активов**

Инфраструктура разработки и отладки **сценариев реагирования**

Иерархичная инфраструктура, мультитенантность

Кроссплатформенность, поддержка различных скриптовых языков

Интеграции «из коробки» с наиболее распространенными ИТ и ИБ решениями

Поддержка ресурсно-сервисной модели

ПРЕИМУЩЕСТВА

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