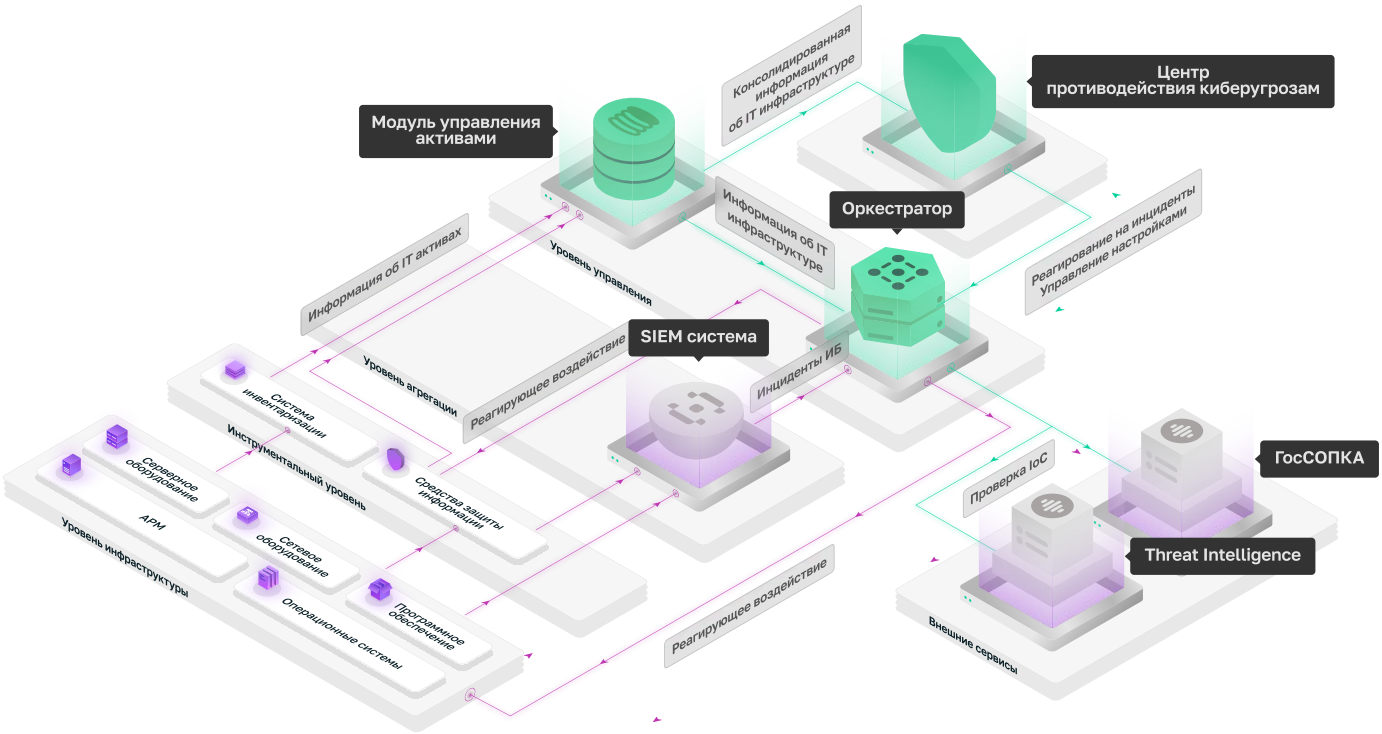
Защита корпоративного сегмента

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 инциденты 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

- Встроенный генератор Python-скриптов на базе ИИ
- Среда разработки и тестирования собственных скриптов и плейбуков на Ansible, Bash, Python, Powershell
- Автоматическое выполнение плейбуков, формируемых из коллекции заранее разработанных производителем скриптов
- Автоматическое выполнение рутинных задач, которые ранее производились вручную

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
- Генератор скриптов на базе ИИ и библиотека готовых сценариев реагирования на инциденты от вендора
- 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 ошибок, связанных с человеческим фактором
- Снижение нагрузки на аналитиков ИБ

ВОЗМОЖНОСТИ

Российское производство: № 26970 в реестре российского ПО, сертификат соответствия ФСТЭК России № 4433

Генератор Python-скриптов на базе ИИ и **инфраструктура разработки / отладки** сценариев реагирования

Набор планов мероприятий по реагированию и **сценариев** реагирования из **«коробки»**

Гетерогенность, кроссплатформенность, поддержка **различных** скриптовых **языков**

Отслеживание пораженных ИТ-активов

Поддержка ресурсно-сервисной модели

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

Иерархичная инфраструктура, мультитенантность

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

Закажите персональную демонстрацию и узнайте условия пилотного проекта

commercial@udv.group