VERSIUM

Versium – гибкая платформа для автоматизации бизнес-процессов в сфере информационной безопасности и ИТ.

Основное назначение:
Оптимизация и автоматизация ключевых процессов ИБ – от мониторинга инцидентов до управления уязвимостями, ИТ-активами, рисками и внутренними аудитами компании.

Для кого:
Крупные компании с развитой ИТ-инфраструктурой без привязки к конкретной отрасли, нуждающиеся в:

- Централизованном управлении ИБ-процессами в формате единого окна;
- Снижении операционных затрат;
- Повышении скорости реагирования на угрозы;
- Оптимизации процессов работы распределенных команд.

Ключевые признаки, когда необходима платформа автоматизации процессов:

1. Сложная ИТ-инфраструктура - когда в эксплуатации находятся десятки серверов, сетевых устройств, облачных сервисов и конечных точек;
2. Большой объем инцидентов - если ручное реагирование уже не справляется с объемом угроз и операционных событий.
3. Жесткие регуляторные требования - необходимость автоматизированного контроля соответствия стандартам и нормативам.
4. Использование SIEM-систем (MP SIEM, KUMA, Rusiem, Pangeo Radar, Splunk, IBM QRadar, ArcSight) - когда в SIEM ежедневно приходят тысячи событий, но только 1-2% расследуются. При этом требуется сократить время реагирования и оптимизировать процессы, связанные с обработкой инцидентов;
5. Перегруженность SOC-команды - если специалисты тратят слишком много времени на рутинные операции.

ОС для установки: Windows, Linux. Установка в Docker.

Системные требования:

- Процессор: 2,40GHz (4 core);
- Не менее 8Gb RAM;
- HDD, от 50 GB.

VERSIUM

Ключевые возможности

1. Гибкость и настройка

- **No-code инструменты** для настройки платформы – объекты/формы, рабочие процессы, отчеты.
- **Встроенный редактор кода** для возможности реализации и автоматизации бизнес-логики любой сложности.
- **Динамическая модель БД** – создание сущностей и атрибутов "на лету" без перезагрузки системы.

2. Интеграции и API

- **Динамические API** – создание эндпоинтов с кастомной логикой обработки данных (прием из ITSM, отправка в BI и др.).
- **Интеграционный модуль** – микросервисы на .NET для работы с любыми протоколами (забор, преобразование и передача данных в платформу).
- **Сбор событий** – из SIEM-систем и напрямую с источников.
- **Реагирование**: реализация действий во внешних системах.

3. Рабочие процессы

- **Конструктор процессов** – графический редактор процессов, поддержка сложных схем: параллельные/последовательные действия, ветвления по условиям.
- **Cron-задачи** – автоматизация периодических операций (например, регулярный сбор данных).
- **Построение любых бизнес-процессов с помощью графического редактора:**
    - Управление процессами ИБ;
    - Управление ИТ-активами;
    - Управление уязвимостями;
    - Реализация аудитов и кастомных задач;
    - Управление работой отдела/департамента;
    - И др.

4. Безопасность и контроль

- **Ролевая модель** – тонкая настройка прав (CRUD, API, меню, виджеты) + интеграция с Active Directory.

- **Авторизация**: локальная, AD, OAuth2.
- **Разграничение данных** – иерархический доступ (например, филиалы видят только свои данные, головной офис – все).

5. Надёжность и мониторинг

- **Логирование** всех запросов, исключений и бизнес-логики через **Serilog** с возможностью выгрузки во внешние системы.
- **Модуль инцидентов** – автоматическое реагирование на угрозы (например, изоляция заражённых узлов через интеграции).

6. Аналитика, дашборды и отчеты

- **Дашборды -** готовые аналитические панели с набором виджетов.
- **Кастомизация -** полнофункциональный редактор для разработки индивидуальных виджетов.
- **Автоматизированная генерация документов:**
  - Экспорт отчетов в популярных форматах (DOCX, XLSX);
  - Использование любых данных из системы.
- **Пространственное отображение -** графическое представление активов на карте.

Модули платформы

1. Автоматизация процессов ИБ

- **Управление инцидентами (SOAR/IRP)**:
  - Автоматический сбор и анализ данных из SIEM и других источников;
  - Встроенные сценарии реагирования с возможностью кастомизации;
  - Возможность реализации интеграций с любыми системами.
- **Управление уязвимостями (VM):**
  - Интеграция со сканерами уязвимостей;
  - Приоритизация угроз на основе критичности активов;
  - Автоматизированные процессы устранения уязвимостей.

2. Автоматизация процессов управления ИТ-активами (AM):

  - Сбор актуальных данных об оборудовании и ПО по расписанию;
  - Формирование единого каталога ИТ-активов;

- Классификация активов и определение ответственных.

3. Автоматизация управления рисками и соответствием (SGRC):

- Возможность реализации любой методологии для автоматизации оценки рисков;
- Возможность построения контроля выполнения требований регуляторов;
- Генерация отчетов для аудитов.

Преимущества

✓ **Гибкость** – адаптация под любые процессы без переписывания кода платформы.
✓ **Масштабируемость** – готовые интеграции + возможность подключения новых систем.
✓ **Безопасность** – многоуровневый контроль доступа и соответствие стандартам ИБ.
✓ **Автоматизация** – от рутинных задач до сложных сценариев реагирования на инциденты.