VSCode-XP

Выпуск 0.1

Security Experts Community

июн. 14, 2023

Оглавление

1 Начало работы **3**
- 1.1 Основные возможности . . . 3
- 1.2 Использование проекта VSCode XP Workspace . . . 4
- 1.3 Требования . . . 4
- 1.4 Установка расширения . . . 4
- 1.5 Настройка расширения . . . 4
- 1.6 Выбор продукта . . . 5
- 1.7 Открытие базы знаний . . . 5
- 1.8 Импорт пакета экспертизы из файла формата KB . . . 5
- 1.9 Создание и удаление папки . . . 6
- 1.10 Обновление дерева объектов . . . 6

2 Разработка правил **7**
- 2.1 Создание пакета экспертизы . . . 7
- 2.2 Создание правила корреляции . . . 7
- 2.3 Создание правила обогащения . . . 8
- 2.4 Редактирование правила . . . 8
- 2.5 Изменение названия правила . . . 9
- 2.6 Добавление информации о правиле . . . 9
- 2.7 Настройка правил локализации . . . 9

3 Тестирование правил **11**
- 3.1 Создание интеграционного теста . . . 11
- 3.2 Создание модульного теста . . . 12
- 3.3 Сбор графов . . . 12
- 3.4 Проверка правил нормализации . . . 12
- 3.5 Запуск интеграционных тестов одного правила . . . 13
- 3.6 Запуск всех модульных тестов одного правла . . . 13
- 3.7 Корреляция необработанных событий . . . 14

4 Компиляция экспертизы для загрузки в продукты **15**
- 4.1 Обновление экспертизы в модулях коррелятора для EDR-решений . . . 15
- 4.2 Создание пакета экспертизы для SIEM-решений . . . 16

Язык eXtraction and Processing (XP) используется для создания правил преобразования данных в процессе обработки событий. На языке XP вы можете разрабатывать правила нормализации, корреляции и обогащения событий.

Расширение eXtraction and Processing позволяет разрабатывать и тестировать правила в VSCode и VSCodium, а также публиковать их в необходимый для вашего продукта формат.

Подробная информация о языке XP и разработке правил приведена в Справочнике разработчика продукта MaxPatrol SIEM.

Глава 1

Начало работы

1.1 Основные возможности

Возможности расширения:

- Просмотр и редактирование правил нормализации, агрегации, корреляции, обогащения и табличных списков.
- Создание из шаблонов правил корреляции, обогащения и нормализации.
- Просмотр, редактирование, создание интеграционных и модульных тестов для правил корреляции, обогащения и нормализации.
- Запуск интеграционных и модульных тестов для правил корреляции, обогащения и нормализации.
- Автоматическое дополнение ключевых слов, функций и типовых конструкций языка XP и полей таксономии.
- Статическая валидация исходного кода на типичные ошибки.
- Заполнение метаданных правил.
- Создание и редактирование правил локализации правил.
- Сбор графов правил, схемы и БД табличных списков.
- Проверка срабатываний всего графа корреляций на необработанные события.
- Распаковка и упаковка пакетов экспертизы в файлы формата KB.

*__Примечание.__ Для этих операций расширение использует дополнительные утилиты, которые доступны в отельном репозитории.

1.2 Использование проекта VSCode XP Workspace

Вы можете легко получить готовое окружение для разработки на XP, если воспользуетесь проектом VSCode XP Workspace. В нём всё собрано в единый Docker-контейнер, а редактирование происходит через веб-версию VSCode. Подробности в репозитории проекта.

1.3 Требования

Вы можете использовать расширение в Visual Studio Code (версия 1.75.0 или выше) и в VSCodium.

Для корректной работы расширения в операционной системе должны быть установлены следующие компоненты:

- Git версии 2.30 или выше;
- .NET Runtime версии 6.0.

1.4 Установка расширения

Чтобы установить расширение:

1. Откройте панель **Extensions** (Ctrl+Shift+X).
2. В строке поиска введите **xplang**.
3. В результатах поиска откройте расширение **eXtraction and Processing**.
4. Нажмите **Install**. Установка может занять несколько минут.

Расширение установлено. В панели **Activity Bar** появился значок 

.

1.5 Настройка расширения

Чтобы настроить расширение:

1. Перейдите в редактор настроек:
   - В Windows/Linux выберите **File** → **Preferences** → **Settings**.
   - В macOS выберите **Code** → **Preferences** → **Settings**.
2. В списке **Extensions** выберите **SiemContentEditor**.
3. В поле **Kbt Base Directory** введите путь к папке с утилитами, необходимыми для работы расширения.
4. В поле **Output Directory Path** введите путь к папке для собранных графов.

   Примечание. *Изменять значение других параметров расширения не рекомендуется.*

1.6 Выбор продукта

С помощью расширения вы можете разрабатывать экспертизу для MaxPatrol SIEM, PT XDR и SOLDR. Перед началом работы с экспертизой вам нужно выбрать продукт, в который она будет поставляться.

Чтобы выбрать продукт:

1. В панели **Action Bar** нажмите на значок  .
2. В левом нижнем углу экрана нажмите **Тип целевого продукта**.

   В верхней части экрана откроется окно выбора продукта.
3. Выполните одно из следующих действий:
   - Если вы работаете с MaxPatrol SIEM, выберите **SIEM**.
   - Если вы работаете с PT XDR или SOLDR, выберите **EDR**.

1.7 Открытие базы знаний

Для начала работы с правилами вам нужно открыть базу знаний. Если у вас нет базы знаний и вы хотите создать ее с нуля, вам нужно выбрать папку, в которой она будет размещена.

Чтобы открыть базу знаний:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите кнопку **Открыть базу знаний**.
3. Выберите папку.
4. Если содержимое папки не соответствует формату выбранного продукта, создайте в ней необходимые папки, нажав **Да** во всплывающем окне в правом нижнем углу экрана.
5. В панели **Дерево контента** нажмите  .

   В панели отобразится содержимое выбранной папки.

1.8 Импорт пакета экспертизы из файла формата KB

Вы можете импортировать в рабочую папку пакеты экспертизы из файла формата KB.

Чтобы импортировать пакеты экспертизы:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на корневой объект со значком  .
3. В открывшемся меню выберите **Извлечь пакеты из kb-файла**.
4. Выберите файл и нажмите кнопку **Открыть**.

   Запустится импорт пакетов экспертизы.

5. В панели **Дерево контента** нажмите  .

Пакеты экспертизы импортированы.

1.9 Создание и удаление папки

Вы можете создавать и удалять папки в вашей рабочей папке.

Чтобы создать папку:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на папку, в которой вы хотите создать новую папку.
3. В открывшемся меню выберите **Создать директорию**.
4. Введите имя папки и нажмите клавишу ENTER.

Папка создана.

Чтобы удалить папку:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на папку, которую вы хотите удалить.
3. В открывшемся меню выберите **Удалить**.

Папка удалена.

1.10 Обновление дерева объектов

Если файлы или папки из вашей базы знаний были изменены не в VSCode, то вам нужно обновить дерево объектов.

Чтобы обновить дерево:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите  .

Дерево обновлено.

Глава 2

Разработка правил

2.1 Создание пакета экспертизы

Чтобы создать пакет экспертизы:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на корневой объект со значком  .
3. В открывшемся меню выберите **Создать пустой пакет**.

   В верхней части экрана откроется окно для ввода названия пакета.
4. Введите название пакета и нажмите клавишу ENTER.

Пакет экспертизы создан.

2.2 Создание правила корреляции

Чтобы создать правило корреляции:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на папку, в которой вы хотите создать правило.
3. В открывшемся меню выберите **Создать корреляцию**.

   Откроется вкладка **Создание правила корреляции**.
4. В поле **Название корреляции** введите название правила корреляции.

5. Если требуется, в раскрывающемся списке **Шаблон** выберите шаблон для правила корреляции.

   При выборе шаблона правило создается с готовой структурой и заполненной информации о событии, на базе которого создан шаблон.

6. Нажмите кнопку **Создать**.

Правило корреляции создано.

2.3 Создание правила обогащения

Чтобы создать правило обогащения:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на папку, в которой вы хотите создать правило.
3. В открывшемся меню выберите **Создать обогащение**.

   Откроется вкладка **Создание правила обогащения**.

4. В поле **Название обогащения** введите название правила обогащения.
5. Если требуется, в раскрывающемся списке **Шаблон** выберите для правила обогащения.

   При выборе шаблона правило создается с готовой структурой.

6. Нажмите кнопку **Создать**.

Правило обогащения создано.

2.4 Редактирование правила

Чтобы отредактировать правило:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** выберите правило, которое вы хотите изменить.

   В редакторе отроется исходный код правила.

3. Внесите изменение в правило.
4. Сохраните изменения.

2.5 Изменение названия правила

Чтобы изменить название правила:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой на правило, название которого вы хотите изменить.
3. В открывшемся меню выберите **Переименовать**.

   Откроется окно **Новое имя правила**.
4. Измените название правила и нажмите клавишу ENTER.

Название правила изменено. Название в исходном коде правила обновлено автоматически.

2.6 Добавление информации о правиле

Вы можете добавить информацию о правиле в файл `metainfo.yaml`.

Чтобы добавить информацию о правиле:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на правило, для которого вы хотите добавить информацию.
3. В открывшемся меня выберите **Метаданные**.

   Откроется вкладка **Метаданные**.
4. Заполните необходимые поля.

Информация о правиле добавлена.

2.7 Настройка правил локализации

При регистрации нормализованного, агрегированного или корреляционного события в продукте с ним может быть связано описание на русском или английском языке (в зависимости от языка интерфейса). Сопоставление описаний с регистрируемыми событиями выполняется согласно заранее созданным правилам локализации. Для нормализованного события правила локализации создаются для правила нормализации, по которой выполняется нормализация этого события, для агрегированного или корреляционного события — для правила агрегации или корреляции, по которому регистрируется событие.

Для одного события может быть создано несколько правил локализации, в зависимости от указанного критерия. Например, вы можете создать, одно правило локализации для события выхода из системы и два правила локализации для события входа в систему, указав в качестве критерия результат входа — успешный или неуспешный.

Чтобы настроить правила локализации:

1. В панели **Action Bar** нажмите на значок  .

2. В панели **Дерево контента** нажмите правой кнопкой мыши на правило, для которого вы хотите настроить правила локализации.
3. В открывшемся меню выберите **Локализации**.

   Откроется вкладка **Локализации**.
4. Если требуется, введите описание правила на русском и английском языках.
5. В поле **Критерий** введите условие применения правила локализации.
6. В полях **Локализация** и **Localization** введите описание события на русском и английском языках.
7. При необходимости добавьте и настройте другие правила локализации с помощью кнопки +.
8. Нажмите кнопку **Сохранить**.

Правила локализации настроены.

Глава 3

Тестирование правил

3.1 Создание интеграционного теста

Интеграционные тесты нужны для отладки правил нормализации, корреляции и обогащения на необработанных событиях.

Чтобы создать интеграционный тест:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на правило, для которого вы хотите создать интеграционный тест.
3. В открывшемся меню выберите **Тесты**.

   Откроется вкладка **Тесты**.
4. Нажмите +.
5. В поле **Сырое событие** вставьте одно или несколько необработанных событий.
6. Нажмите кнопку **Конверт** и выберите MIME-тип необработанного события.
7. В поле **Код теста** введите тестовый сценарий.
8. Нажмите кнопку **Сохранить все**.

Интеграционный тест создан.

3.2 Создание модульного теста

Модульные тесты нужны для отладки правил корреляции и обогащения на нормализованных событиях.

Чтобы создать модульный тест:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** выберите правило, для которого вы хотите создать модульный тест.
3. В панели **Модульные тесты** нажмите +.
4. В редакторе введите тестовый сценарий.

   Тестовый сценарий должен содержать хотя бы одно нормализованное событие и ожидаемый результат.
5. Сохраните изменения.

Модульный тест создан.

3.3 Сбор графов

Для запуска модульных тестов вам нужно собрать все графы.

Чтобы собрать графы:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите .

   Запустится сбор графов. В панели **Output** будет выведен результат.

3.4 Проверка правил нормализации

Вы можете проверить работу правил нормализации на необработанных событиях. Перед началом проверки вам нужно создать *интеграционный тест*.

Чтобы проверить правила нормализации:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на правило, для которого создан интеграционный тест.
3. В открывшемся меню выберите **Тесты**.

   Откроется вкладка **Тесты**.
4. Выберите необходимый тест.
5. Выполните одно из следующих действий:

- Если вы хотите только нормализовать необработанные события, нажмите кнопку **Нормализовать**.
- Если вы хотите нормализовать и обогатить необработанные события, нажмите кнопку **Нормализовать + Обогатить**.

Запустится процесс нормализации. При успешном завершении отобразится нормализованное событие.

6. Если вы хотите запустить модульный тест по сформированному нормализованному событию, нажмите кнопку **Быстрый тест**.

3.5 Запуск интеграционных тестов одного правила

Чтобы запустить все интеграционные тесты одного правила:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на правило, для которого вы хотите запустить интеграционный тест.
3. В открывшемся меню выберите **Тесты**.

   Откроется вкладка **Тесты**.
4. Нажмите кнопку **Запустить все тесты**.

   Последовательно будут запущены все добавленные интеграционные тесты. В панели **Output** отобразятся подробные результаты их выполнения.

3.6 Запуск всех модульных тестов одного правла

Чтобы запустить все модульные тесты одного правила:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** выберите правило, для которого вы хотите запустить модульные тесты.
3. В панели **Модульные тесты** нажмите  .

   Последовательно будут запущены все добавленные модульные тесты. Если тест пройдет успешно, то напротив него появится значок  , если не успешно —  . В панели **Output** отобразятся подробные результаты тестов.

3.7 Корреляция необработанных событий

Для проверки правил вы можете пропустить через весь граф корреляций необработанные события. Перед этим вам нужно *собрать графы*.

Чтобы скоррелировать необработанные события:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите  .

   Откроется вкладка **Скоррелировать события**.
3. В поле **Сырое событие** вставьте одно или несколько необработанных событий, которые нужно пропустить через граф корреляций.
4. Нажмите кнопку **Конверт** и выберите MIME-тип необработанного события.
5. Нажмите кнопку **Скоррелировать события**.

   Запустится процесс корреляции. В блоке **Скоррелированные события** будут выведены скоррелированные события.

Глава 4

Компиляция экспертизы для загрузки в продукты

4.1 Обновление экспертизы в модулях коррелятора для EDR-решений

Чтобы обновить экспертизу в модулях коррелятора:

1. В панели **Action Bar** нажмите на значок  .
2. В главном меню в разделе **Terminal** выберите пункт **Run Build Task** или нажмите сочетание клавиш **Ctrl+Shift+B**.
3. В открывшемся окне выберите команду **XP: Pack EDR content**.

   Откроется окно для выбора папки с модулем «Коррелятор (Linux)».
4. Выберите папку с модулем «Коррелятор (Linux)» и нажмите кнопку **Выбрать эту директорию**.
5. Откроется окно для выбора папки с модулем «Коррелятор (Windows)».
6. Выберите папку с модулем «Коррелятор (Windows)» и нажмите кнопку **Выбрать эту директорию**.

Экспертиза в модулях обновлена.

4.2 Создание пакета экспертизы для SIEM-решений

Для переноса вашего набора правил в MaxPatrol SIEM вам нужно собрать их в файл формата KB.

Чтобы собрать пакет экспертизы:

1. В панели **Action Bar** нажмите на значок  .
2. В панели **Дерево контента** нажмите правой кнопкой мыши на объект со значком  .
3. В открывшемся меню выберите **Собрать пакет**.

   Откроется окно **Сохранение**.
4. Выберите папку, в которую вы хотите сохранить файл, и введите имя файла.
5. Нажмите кнопку **Сохранить**.

Экспертиза опубликована. Далее вам нужно импортировать файл в MaxPatrol SIEM.