

R-Vision

Новые подходы в банальных процессах (SIEM, VM)



Вячеслав Ковалев

Руководитель пресейл-группы

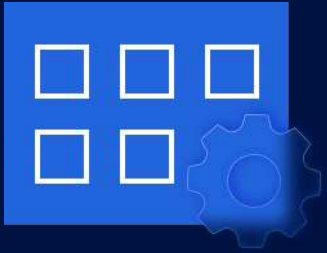


Процессы в LM/SIEM

Сбор и обработка событий ИБ

Используются продукты: LM и SIEM

Настройка модели данных



Модель событий

Позволяет собирать и хранить любую необходимую информацию



Настроенная модель событий



Универсальная модель данных с возможностью быстрого расширения



Доступно создание пользовательской модели данных

Настройка модели данных

R-SIEM Версия 1.9.1 Модели событий

Тенант: main_tenant

Создание модели события

Название: Новая модель событий

Описание: Введите описание

Схема

Ключ поля	Описание	Тип поля	Тип данных	Параметры типа д	Поле хранящее на	Может быть null
id	Уникальный идентификатор...	Служебное	UUID	-	-	✗
sourceIp	IP-адрес источника, от...	Служебное	IPv6	-	-	✗
tenantId	Идентификатор тенанта	Служебное	LCString	-	-	✗
art	Время получения события...	Служебное	DateTime	-	-	✗
Наименование						
+ Добавить строку						

Отменить Создать

Всего записей: 7

Подключение источников и распределение потоков данных

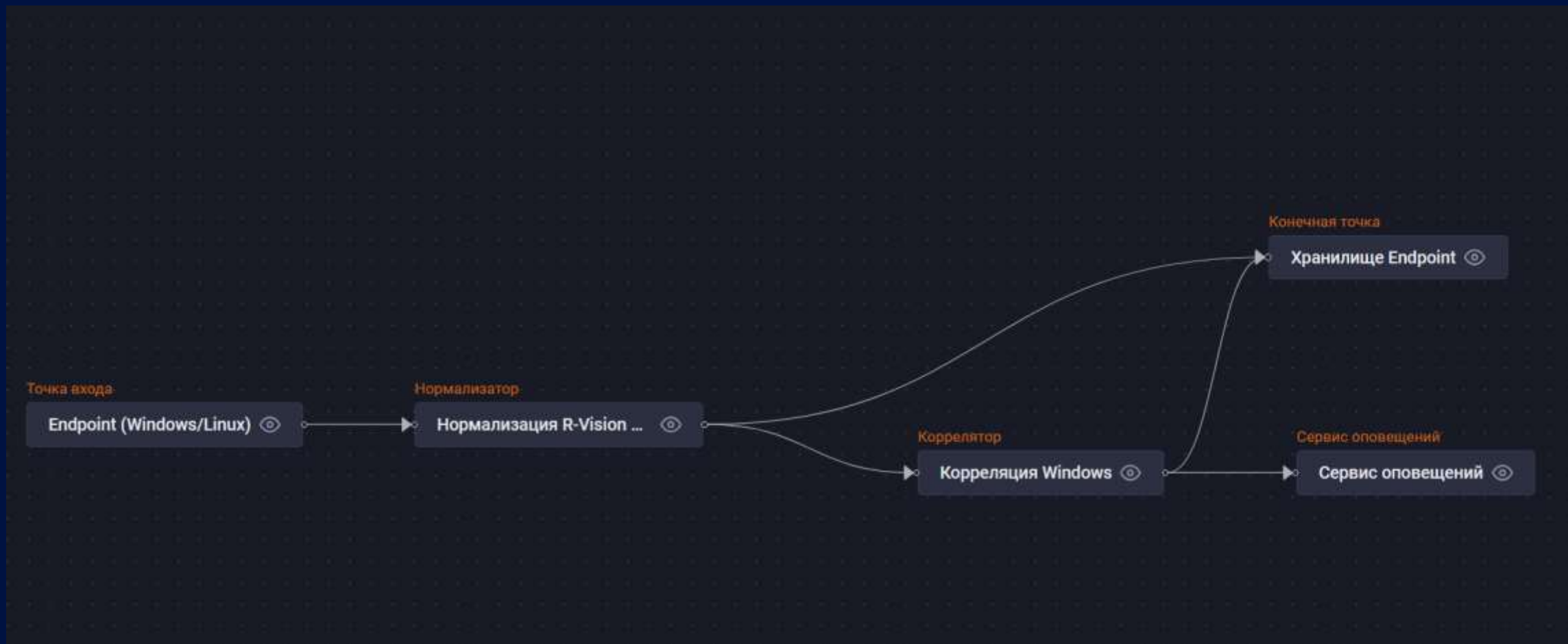


Конвейер обработки событий

Единое окно для работы со всеми элементами для сбора и обработки событий

- ✓ Визуальное управление потоком событий
- ✓ Быстрое подключение новых источников информации
- ✓ Гибкость при конфигурировании компонентов конвейера

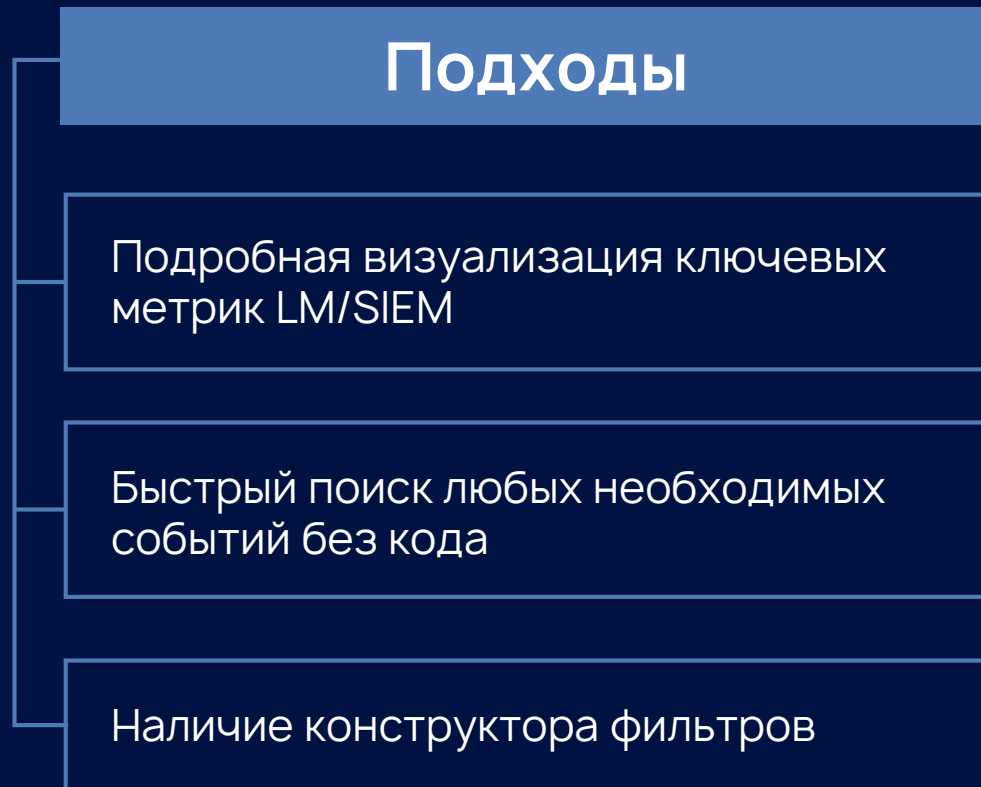
Подключение источников и распределение потоков данных



Работа с событиями ИБ

Используются продукты: LM и SIEM

Поиск и визуализация событий



Поиск и визуализация событий

Р. Поиск Хранилище событий: Windows Sysmon... Профиль

Введите запрос и нажмите кнопку Поиск. Последний период: 30 дней

Фильтры: eventType EQ Process Create, processID EQ 6254, NOT processGUID EQ {a23eae89-bd56-5903-0000-0010e9d95345}, NOT id EQ 2e03bfad-92df-4567-7... + Добавить фильтр

Совпадений 906. Интервал времени: 2024-09-01T11:31:18.389+03:00 - 2024-10-01T11:31:18.389+03:00. Скрыть график

id	timestamp	processGUID	eventType	processID	image
2e03bfad-92df-4567-7...	2024-09-27T15:08:12.000+03:00	{a23eae89-bd56-5903-0000-0...	Process Create	6254	C:/Users/Download...
afed57d3-6c72-49f1-802f-...	2024-09-27T15:08:11.000+03:00	{a23eae89-bd56-5903-0000-0...	Process Create	6254	C:/Users/Download...
6d86490f-0fb6-4880-a214-...	2024-09-27T15:08:10.000+03:00	{a23eae89-bd56-5903-0000-0...	Process Create	6254	C:/Users/Download...
f52e89c1-6543-4d10-9fc6-...	2024-09-27T15:08:09.000+03:00	{a23eae89-bd56-5903-0000-0...	Process Create	6254	C:/Users/Download...

Показывается первых 500 записей: 1 / 20. 00:00.524. Автоотслеживание

Детали события 2e03bfad-92df-456...

Скрыть пустые поля события

Дата и время

timestamp: 2024-09-27T15:08:12.000+03:00

Служебные данные

id: 2e03bfad-92df-4567-b9db-5338b60db595
tenantId: 00000000-0000-0000-0000-000000000000
collectorId: 5908686a-0ec9-437e-82de-3d88428b7f32
type: исходное событие

Сведения о событии

eventType: Process Create
processGUID: {a23eae89-bd56-5903-0000-0010e9d95345}
processID: 6254
image: C:/Users/rsmith/Downloads/mimikatz.exe
fileversion: 2.1.1.0
description: Mimikatz for Windows
product: mimikatz
company: gentilkiwi (Benjamin DELPY)

Работа с контентом правил

Используются продукты: LM и SIEM

Разработка и модификация контента



As Code

Набор инструментов для профессионалов, позволяющий разрабатывать правила под любые требования организации



Собственный плагин R-Object



Гибкость при создании правил



Детектирование инцидентов любой сложности



Валидация и подсветка синтаксиса

Разработка и модификация контента

Экспертиза

Профиль

Фильтр

Изменение правила корреляции

```
49 select:
50   ttl: 20
51
52 on_correlate: !vr1 |
53   if %virus_deleted.externalId == "GNRL_EV_OBJECT_DELETED">{
54     %tmp = "удалено"
55   } else if %virus_deleted.externalId == "GNRL_EV_OBJECT_CURED">{
56     %tmp = "вылечено"
57   } else{
58     %tmp = "запрещено"
59   }
60
61 . |- compact({
62   "dhost" : %virus_detected.dhost,
63   "dvc" : %virus_detected.dvc,
64   "suser" : %virus_detected.suser,
65   "cs6label" : "Antivirus message",
66   "cs6" : %virus_detected.msg,
67   "msg" : join(["На хосте", (to_string(%virus_detected.dvc) ?? "-"), "пользователя", (to_string(%virus_detected.suser) ?? "-"), "было обнаружено и", %tmp, "ВПО по пути", (to_string(%virus_detected.filePath) ?? "-"), "вердиктом",
```

Результат

```
[OK] First Test, where 1 and 2 is true and they're should be joined, but 3 with different hash
```

Отменить Сохранить черновик Обновить версию

Вложения 1 20 Всего записей: 12 Просмотр

Разработка и модификация контента



Конструктор

Помогает оперативно составить не сложные запросы для закрытия потребностей детектирования



Низкий порог входа



Визуализация логики правила



Интуитивный и понятный интерфейс

Разработка и модификация контента

The image displays three overlapping windows from a software interface for creating and configuring correlation rules. The windows are:

- Top Window: "Правило корреляции. Создание"**
 - Step 2: **Фильтр событий**
 - Section: **Событие A**
 - Fields: **Название** (Событие A), **Количество событий** (1)
 - Table for conditions:

Поле	Оператор	Значение
aggregation_name	=	Введите значение
 - Buttons: **+ Добавить событие**, **Общий фильтр** (toggle)
- Middle Window: "Правило корреляции. Создание"**
 - Step 3: **Объединение**
 - Section: **Объединение**
 - Fields: **ТТЛ окна корреляции** (1 сек.), **Таймаут события (опционально)** (1 сек.)
 - Section: **Объединение: Получение события**
 - Fields: **Событие** (dropdowns), **Выберите поле** (dropdowns)
 - Buttons: **+ Добавить поле**, **+ Добавить объединение**
- Bottom Window: "Правило корреляции. Создание"**
 - Step 4: **Настройка события корреляции**
 - Section: **Источники**
 - Fields: **Время триггера** (1 сек.), **Создавать оповещение** (Выключено)
 - Section: **Укажите, как формировать значения полей корреляционного события**
 - Fields: **Поле события** (dropdown), **Источники** (dropdown menu with options: **Значение**, **Значение из поля**, **Запрос в табличный список**)
 - Buttons: **+ Добавить поле**, **Сохранить как черновик**, **Назад**, **Далее**



Процессы в VM

Процесс управления уязвимостями



Проведение инвентаризации

Используются продукты: сканер уязвимостей

Инвентаризация

Даст полную информацию о защищаемых активах

Возможности:



Быстрое сканирование всей ИТ-инфраструктуры в режимах discovery и inventory



Импорт информации из любых источников (сканеры, СЗИ, ИТ-системы)



Автоматическая корреляция и дедупликация данных

От 3-х секунд

скорость сканирования одного устройства

Применение ресурсно-сервисной модели позволит сфокусировать внимание на защите **наиболее критичных хостов**

Инвентаризация

The screenshot displays a software interface for IT asset management. On the left, a sidebar titled "Группы ИТ-активов" (IT Asset Groups) lists various categories such as "Бухгалтерия и налоговый учет", "Электронная образовательная система", "Кадровая база завода", "Почтовый сервер завода", and several "Информационная система" (Information System) entries. The main area is titled "Схема взаимосвязей для Почтовый сервер завода" (Interconnection Scheme for Mail Server of the Factory). It features a central node labeled "Почтовый сервер завода" (Mail Server of the Factory) which is connected to a wide range of other nodes. These nodes include business processes like "Бизнес-процессы" and "Контроль за ходом производства", personnel such as "Иван Иванов" and "Филипп Баженов", and various departments like "Диспетчерская" and "Бюро механиков". The diagram also shows specific IP addresses and device identifiers, such as "openldap (192.168.122.1, 10.99.103.65)", "aldrp01 (10.99.103.75)", and several Windows machines (e.g., "WIN2019X64RU01 (10.99.101.157)"). A "Фильтр" (Filter) button is visible in the top right corner of the main window.

Выявление уязвимостей

Используются продукты: сканер уязвимостей

Выполнение задач на сканирование

Один
коллектор
сканера



Определение уязвимостей на сервере

Управление интервальным сканированием

Одна задача на все виды ОС

Автоподбор учетных записей

Расписание сканирования с техническими паузами

Приоритетизация уязвимостей

Используются продукты: VM

Определение уровня критичности уязвимостей

Расчет рейтинга на основе любых атрибутов:

- ✓ Уязвимости
- ✓ Оборудования
- ✓ Группы ИТ-активов

Приоритизация уязвимостей:

- ✓ По рекомендациям ФСТЭК
- ✓ На основании международных практик
- ✓ С учетом внутренних регламентов организации

Определение уровня критичности уязвимостей

R:Vision Расчет рейтинга уязвимости vkovalev

Поиск

Общие

Активы

Уязвимости

Справочники

Поля

Политики управления уя...

Расчет рейтинга уязвимости

База уязвимостей

Инциденты

Система защиты

Аудит и контроль

Риски

Задачи

Статус: Рассчитать сейчас

Отмена Сбросить

Формула расчета рейтинга уязвимости

$$CVSS*(0.4*TYPECOMP+0.2*PERCVUL+0.4*Internet)$$

Рейтинг уязвимости рассчитывается для каждой уязвимости на хосте. Рейтинг уязвимости рассчитывается на основе оценки CVSS, поэтому эту переменную нельзя удалить. Система работает с двумя версиями оценки CVSS: V2 и V3. По умолчанию используется CVSS V3, если для уязвимости доступны обе оценки. В остальных случаях используется CVSS V2. Для расчета рейтинга могут использоваться поля Уязвимости и поля с типом Справочник или Чек-бокс активов Оборудование, Группы ИТ-активов. После добавления в формулу каждому значению поля нужно задать коэффициент, который будет заменять текстовое значение поля при расчете.

Переменные

Добавить	Удалить	
ID	Наименование	
AC	Сложность атаки	
PR	Уровень привилегий (S-Changed)	
S	Влияние на другие компоненты системы	
CVSS	Уязвимости: Оценка CVSS	
TYPECOMP	Тип компонента ИС	
AV	Вектор атаки	
I	Влияние на целостность	
Internet	Доступность из Интернета	
C	Влияние на конфиденциальность	
UI	Взаимодействие с пользователем	
PERCVUL	Процент уязвимых компонентов	
PRU	Уровень привилегий (S-Unchanged)	
A	Влияние на доступность	

Поле актива

ID

Наименование

Список значений :

Значение	Коэффициент
----------	-------------

Добавить

Определение уровня критичности уязвимостей

База уязвимостей

26

vkovalev

е8412c_oval:redos:def:1199

Выберите организацию

Идентификатор	CVS	CVSS V3	Наименование	SCORE	Всего	Открытые	Критические	Уязвимости
<input type="checkbox"/> RVM-78b5aedc-a9ae-47e9-b691-ef4e35e8412c_oval:redos:def:1199		9.8	Уязвимость zlib	23.3	5 >	3 >	2 >	<div style="display: flex; width: 100%;"><div style="width: 75%; background-color: #f08080;"></div><div style="width: 25%; background-color: #ffa500;"></div></div> 2 1

Устранение уязвимостей

Используются продукты: VM

Обработка критичных уязвимостей

Выстроить процесс с помощью:



Учета компенсирующих мер



Построение статусной модели



Политик управления уязвимостям



Автоматизированная постановка задач и инцидентов



Интеграции с внешними Service Desk решениями

Обработка критических уязвимостей

The screenshot displays a software interface for incident management. The main section is a table with the following columns: 'Тип инцидента' (Incident Type), 'Уровень инцидента' (Incident Level), 'Статус инцидента' (Incident Status), 'Ответственный' (Responsible), and 'Статус SLA' (SLA Status). The table lists 15 entries, all of which are 'Обнаружение уязвимостей' (Vulnerability Detection) with a 'Критичный' (Critical) level and 'Расследование' (Investigation) status. The SLA status varies between 'SLA в норме' (SLA within norm) and 'Лимит превышен' (Limit exceeded).

Тип инцидента	Уровень инцидента	Статус инцидента	Ответственный	Статус SLA
Обнаружение уязвимостей	Критичный	Расследование	Ковалев Вячеслав (vkovalev)	SLA в норме
Обнаружение уязвимостей	Критичный	Расследование	Ковалев Вячеслав (vkovalev)	SLA в норме
Обнаружение уязвимостей	Критичный	Расследование	Noel, Hanae (a503770@rvlab...)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	emihalova	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Захаренко Егор (ezaharenko)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Захаренко Егор (ezaharenko)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Захаренко Егор (ezaharenko)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Noel, Hanae (a503770@rvlab...)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Noel, Hanae (a503770@rvlab...)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Noel, Hanae (a503770@rvlab...)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Noel, Hanae (a503770@rvlab...)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Noel, Hanae (a503770@rvlab...)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Noel, Hanae (a503770@rvlab...)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	emihalova	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	Noel, Hanae (a503770@rvlab...)	Лимит превышен
Обнаружение уязвимостей	Критичный	Расследование	vkirpal	Лимит превышен

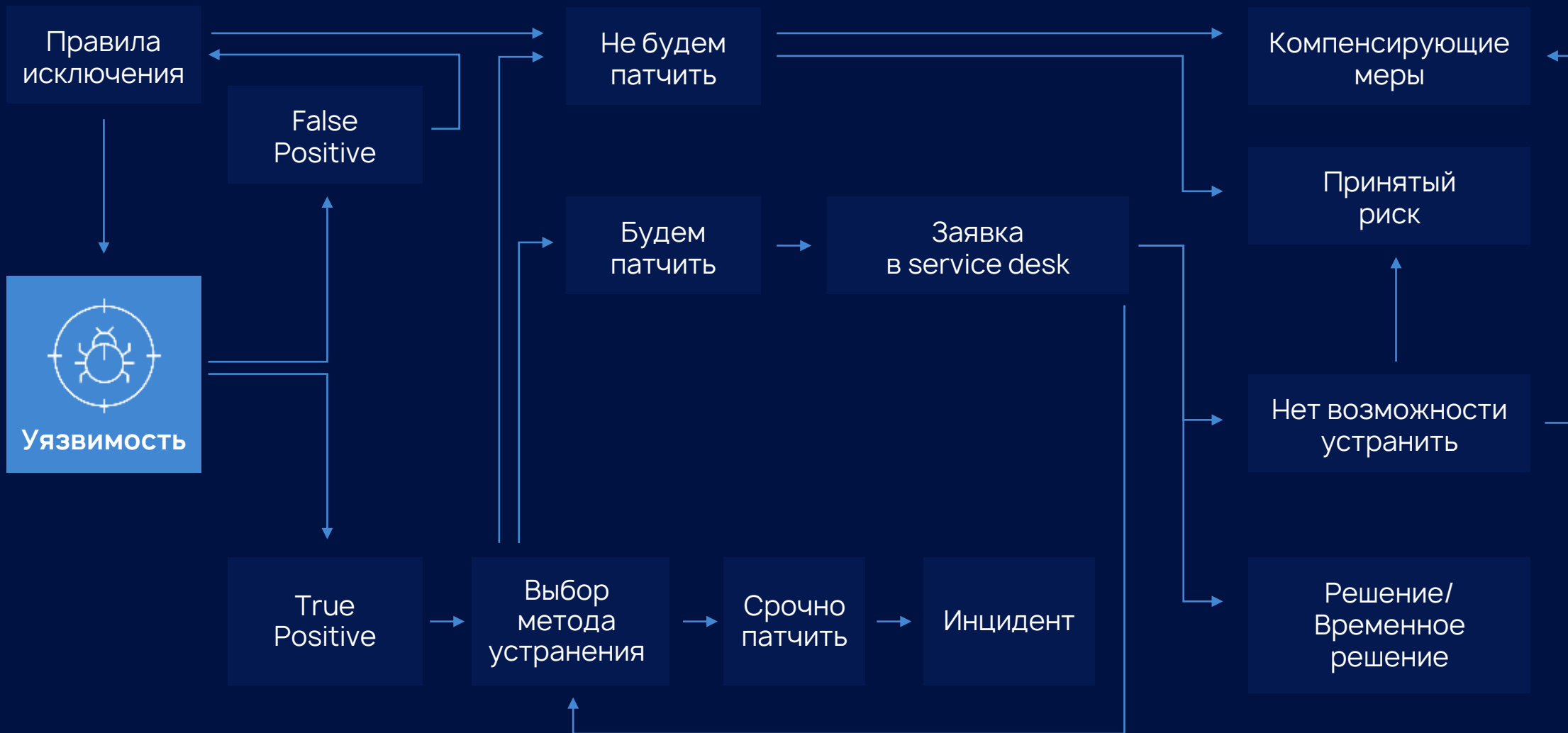
The right-hand side of the interface shows a detailed view of an incident with ID '24-10-1'. The incident type is 'Обнаружение уязвимостей'. The level is 'Критичный'. The creation date is '01.10.2024 14:20:57' and the last update date is '01.10.2024 14:21:14'. The description states: 'Обнаружены уязвимости: Уровень: Критический, Хосты: 1; Уровень: Высокий, Хосты: 0'. The source of information is 'Vulnerability Scanner'.

Обработка критических уязвимостей

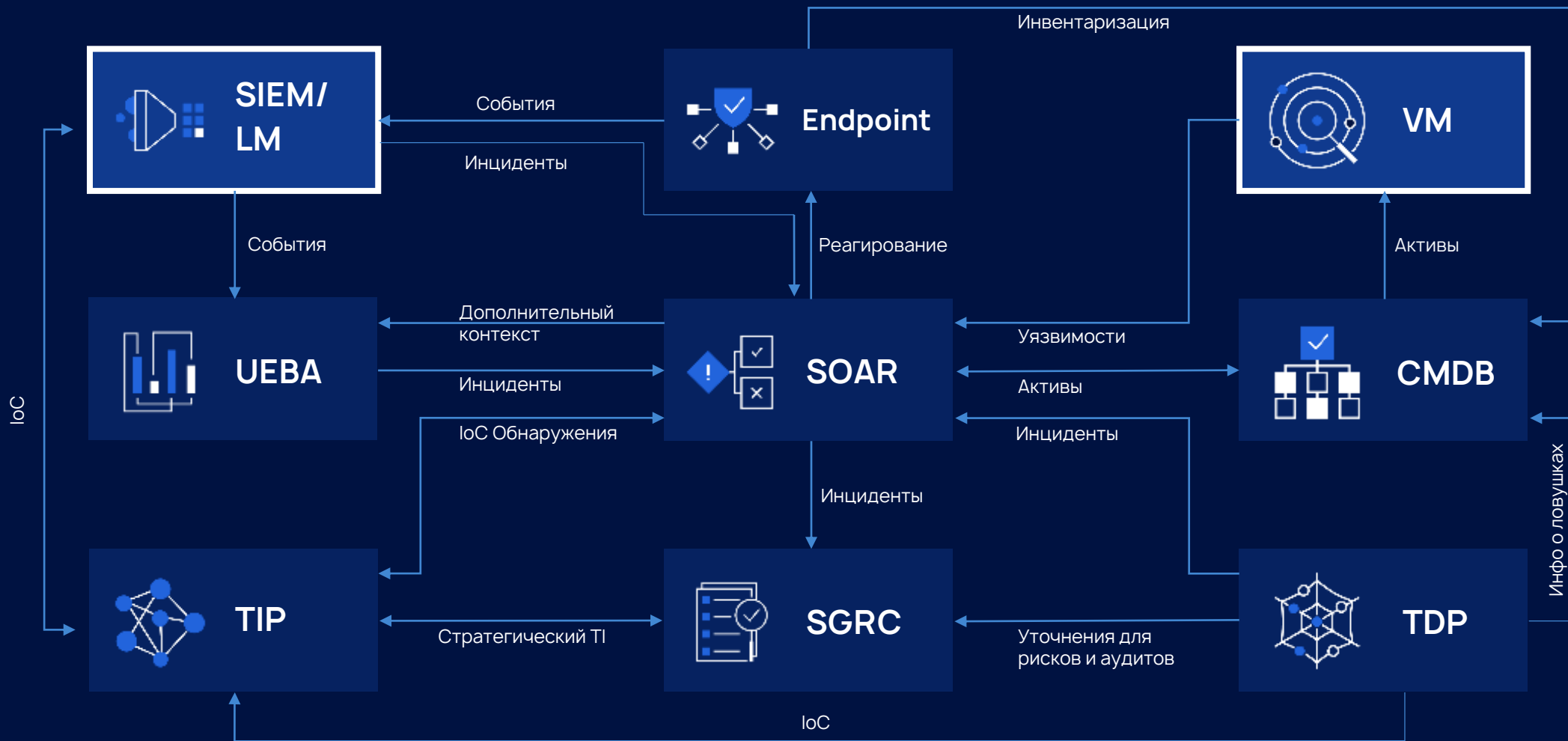
Инцидент 24-09-56: Статус задач в SD

ID	Наименование	Комментарии	Статус	Тип	Ссылка	Приоритет
ORG-2448	ИТ отдел - Обработка уязвимости	gvision : Устраним в течение 60-90 дней.	В работе	Внутренние задачи	http://10.99.103.143:8080/browse/ORG-2448	Highest

Как будем устранять уязвимость



Экосистема R-Vision Evo



R-Vision



Свяжитесь с нами удобным способом:

+7 (499) 322 80 40

sales@rvision.ru



Читайте наш Дайджест ИБ:

rvision.ru/blog



t.me/rvision_pro



vk.com/rvision_ru



rvision.ru