

Table of Contents

Table of Contents	1
Отчеты инцидентов	2
Общие сведения	3
Правила отчетов инцидентов	4
Созданные отчеты инцидентов	5
Шаблоны отчетов инцидентов	6

Documentation: ☒
Product: LogAn, SIEM
Version: 7.0.1, 7.1.0

В данном разделе администратор может формировать отчёты об инцидентах информационной безопасности. Отчеты могут создаваться в соответствии с созданными правилами и шаблонам; отчёт доступен для скачивания или передачи на коннектор.

Раздел состоит из трех подразделов - **Шаблоны отчетов инцидентов**, **Правила отчетов инцидентов** и **Созданные отчеты инцидентов**. Чтобы создать отчет, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило создания отчета.	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет.	Выбрать инцидент и сгенерировать отчет.
Шаг 3. Получить отчет.	Записи о создании отчетов доступны в разделе Созданные отчеты инцидентов .

Правила отчетов инцидентов

Documentation: ☒
Product: LogAn, SIEM
Version: 7.0.1, 7.1.0

Правило отчета задает параметры создаваемого отчета, а также способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
Название	Название правила.
Описание	Опциональное поле для описания правила.
Язык отчёта	Выбор языка, который будет использован в отчете.
Часовой пояс	Часовой пояс, который будет использоваться при формировании отчёта.
Формат отчёта	Формат (PDF, HTML), в котором будет создаваться данный отчет.
Коннектор	Коннектор, на который необходимо отправить отчёт (необязательно).
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

После создания правила пользователь может запустить создание отчёта по выбранному инциденту. После формирования отчёт доступен для скачивания локально или передачи на выбранный коннектор.

Созданные отчеты инцидентов

Documentation: ☒

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

В разделе **Созданные отчеты инцидентов** хранятся все сформированные отчеты. Отчеты создаются в формате pdf или html. Для каждого отчета указывается название отчета, которое совпадает с названием правила отчета, использованного для создания данного отчета, время создания отчета и файл отчета с указанием его размера. Все отчеты доступны для скачивания и удаления.

Время хранения готовых отчетов (ротация) настраивается по нажатию на кнопку **Настроить**.

Шаблоны отчетов инцидентов

Documentation: 

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов инцидентов делятся на 2 категории:

- **Форма ключ-заключение** — шаблоны, позволяющие настроить поля, которые необходимо отобразить в отчёте. Шаблоны данного типа пользователь может создавать самостоятельно.
- **Инциденты** — группа шаблонов для создания отчётов по инцидентам. Шаблоны предоставляются компанией UserGate.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

