Обработка событий в Saturn

В данной статье описана схема обработки событий и пайплайны, которые выполняют обработку событий.

На рисунке выше показана схема обработки событий в компоненте **Saturn**. Каждый из блоков представляет собой сущность в Системе:

- **input:** данный пайплайн является единой точкой входа в обработку для всех событий;
- **clone:** данный пайплайн осуществляет отправку всех событий в хранилище (ClickHouse), выполняет предобработку событий Windows, а также отправляет события в пайплайн identity, если включена фильтрация на основе правил корреляции;
- **pre_parse:** данный пайплайн осуществляет предварительный парсинг событий. События с тегом **unparsed** отправляются в пайплайн **clone**, а с тегом **parsed** — в пайплайн **pre_filtration**;
- **pre_filtration:** данный пайплайн осуществляет распределение событий в пайплайны в соответствии со значением поля **product** (в пайплайне **parse**). События с **product = auditd** отправляются в пайплайн **grouping**, события с тегом **unparsed** отправляются в пайплайн **clone**;
- **parse:** данный блок является совокупностью пайплайнов, каждый из которых обрабатывает события только для своего **product**. Псоле окончания процедуры парсинга, все события отправляются в пайплайн **clone**;
- **grouping:** данный пайплайн выполняет группировку событий **auditd**. События с тегом **unparsed** отправляются в пайплайн **clone**, а с тегом **parsed** — в блок **parse**;
- **identity:** данный пайплайн отвечает за распределение событий по тегам. Если в событиях **product =**

checkpoint_gaia/auditd/usergate/postgresql/cisco/esxi/nginx/unix_like/vsphere, пайплайн отправляет события в пайплайн **mpsiem_tags**. В ином случае события отправляется сразу в пайплайн **output_siem**;

- **output_siem:** данный пайплайн осуществляет отправку событий в MP SIEM;
- **mpsiem_tags:** если включена фильтрация событий на основе правил корреляций, пайплайн отправляет прошедшие фильтрацию события в пайплайн **output_siem**;

ID статьи: 187
Последнее обновление: 4 дек., 2024
Обновлено от: Егоров В.
Ревизия: 1
База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.2.0 -> LogIQ. Руководство разработчика -> Управление конфигурационными файлами -> Обработка событий в Saturn
https://docs.axel.pro/entry/187/