**Тестовое задание с событиями**

Необходимо автоматизировать выявление данных из дампа журнала событий

и ответить на следующие вопросы.

Код скрипта доступен на github https://github.com/Sergey-K2/PSB\_test.git

1. Количество разных источников сообщений. Предоставить перечень.

См. report\_file.txt

1. Количество разных типов сообщений от Cisco ASA, встречающихся в дампе. Предоставить перечень.

См. report\_file.txt

3. Перечень различных IP-адресов, встретившихся в сообщениях Cisco ASA.

См. report\_file.txt (перечень для всех адресов, а не только Cisco ASA)

4.Для каждого типа сообщения выделить и описать (без автоматизации) ключевую информацию из события.

В логах представлена информация от устройств Cisco ASA и Juniper.

Представлена следующая информация:

- Priority Code Syslog (например <161> ) состоит из:

а) Данных об источнике (facility, указан в коде в начале сообщения <xxx>, рассчитывается путем деления кода на 8 без остатка);

б) Типа сообщения (severity, указан в коде в начале сообщения <xxx>, рассчитывается путем вычисления остатка от деления кода на 8;

- Временная метка (например Nov 13 15:35:09);

- IP-адрес устройства и имя устройства/кластера с указанием роли конкретного устройства (master, backup)(например 10.181.233.206 %ASA-1-10602 (для Cisco) , ZOO-ML-CE master (для Juniper);

- Severity + код сообщения (для Cisco, например 1-106021);

- Указание модуля, который отправил сообщение (например PFE\_FW\_SYSLOG\_IP);

- Тип устройства отправившего сообщение (например FW - фаервол);

- Интерфейс, на котором произошло событие (например ge-0/0/10.0 (для Juniper), on interface mgmt (для Cisco;)

- Флаг действия/действие( например A – allow (для Juniper), Deny (Cisco);

- Протокол (например tcp, на Сisco с указанием флагов);

- IP и порты источника и назначения;

- Количество пакетов в сессии (для Juniper).

Для сообщений с невысоким типом критичности, таких как Debug, Informational, Notice, Warning, наиболее важным является частота сообщения/события по конкретному элементу корпоративной сети.

При анализе сообщений с высоким типом критичности (Error, Critical, Alert, Emergency) важно иметь максимально подробную информацию, поэтому каждый элемент в сообщении лога является ключевым.

Автоматизацию можно выполнить на любом языке программирования.

В качестве результата предоставить исходный код и работающий прототип.

В случае невозможности автоматизации необходимо предоставить без кода ответы на вышеуказанные вопросы.