**Searches & Use Cases**

|  |  |  |
| --- | --- | --- |
| № | Название | Входные паараметры |
| 1 | Найти, кто удалил фолдер | <<идентификатор фолдера>> |
| 2 | Найти, кто создал/остановил/перезапустил/удалил виртуальную машину | <<идентификатор виртуальной машины>> |
| 3 | Какие действия совершал конкретный пользователь за период времени | <<идентификатор\_пользователя>>  <<имя\_пользователя>> |
| 4 | Поиск событий по объектам определенного фолдера | <<идентификатор фолдера>>  <<имя фолдера>> |
| 5 | Срабатывание при создании credentials сервисных аккаунтов |  |
| 6 | Срабатывание на событие с созданием машины с белыми IP адресами |  |
| 7 | Срабатывание на создания "двуногих" виртуальных машин (с белыми IPv4-адресами и IPv6-адресами) - сценарий внутренних сервисов |  |
| 8 | Срабатывание на любое действие под привелигированным account с ролью “resource-manager.clouds.owner” | <<идентификатор\_пользователя>>  <<имя\_пользователя>> |
| 9 | Аномальное кол-во попыток неуспешной авторизации (!!требует корреляции!!). |  |
| 10 | Создание слишком широкого (небезопасного) ACL Security Group для ipv4, tcp |  |
| 12 | Загрузка image в облако не из разрешенного S3 Bucket |  |
| 13 | Подозрительные действия с хранилищем логов AuditTrails (S3 Bucket) | <<ID вашего Bucket>> |
| 14 | Назначение привелигированных прав доступа сервисному аккаунту на Folder. Роль admin. |  |
| 15 | Срабатывание на изменение прав доступа на симметричные ключи шифрования KMS |  |
| 16 | Создание ВМ с image\_id из Marketplace |  |
| 17 | Добавление публичного IP-адреса существующей виртуальной машине |  |