**Описание SIEM коннектора для Yandex.cloud**

**СОДЕРЖАНИЕ**

[**Назначение коннектора** 3](file:///E:\Документы%20АТБ\Коннектор%20яндекс\Коннектор%20событий%20ИБ%20YandexCloud%202022%2005.docx#_Toc103946670)

[**Архитектура коннектора** 4](file:///E:\Документы%20АТБ\Коннектор%20яндекс\Коннектор%20событий%20ИБ%20YandexCloud%202022%2005.docx#_Toc103946671)

[**Источники данных и события** 5](file:///E:\Документы%20АТБ\Коннектор%20яндекс\Коннектор%20событий%20ИБ%20YandexCloud%202022%2005.docx#_Toc103946672)

[**Анализ событий** 10](file:///E:\Документы%20АТБ\Коннектор%20яндекс\Коннектор%20событий%20ИБ%20YandexCloud%202022%2005.docx#_Toc103946673)

# **Назначение коннектора**

Коннектор мониторинга событий информационной безопасности (ИБ) для Yandex.Cloud (SIEM коннектор для Yandex.cloud) – это решение позволяющее собирать, сохранять и выполнять анализ событий аудита различных приложений Yandex.Cloud в SIEM системе организации.

Данный коннектор позволяет получать информацию из журналов событий Yandex.Cloud и отправлять её за пределы облака в SIEM систему, расположенную в инфраструктуре организации. Информация о событиях направляется в SIEM систему в формате CEF по протоколу syslog для проведения дальнейшего анализа и разбора инцидентов. Это позволяет выполнять мониторинг работы приложений Yandex.Cloud и выявлять инциденты ИБ.

Примеры анализируемых событий:

* фиксирование создания новых виртуальных машин;
* фиксирование добавления внешних сетевых интерфейсов к существующим виртуальным машинам;
* мониторинг управления ключами доступа;
* фиксирование добавления публичного IP-адреса для виртуальной машины и пр.

# **Архитектура коннектора**

Коннектор позволяет считывать аудитные логи (JSON фай) различных приложений Yandex.Cloud, собранные сервисом AuditTrail и направлять их в формате CEF по syslog в SIEM систему Заказчика, для дальнейшей обработки и анализа.

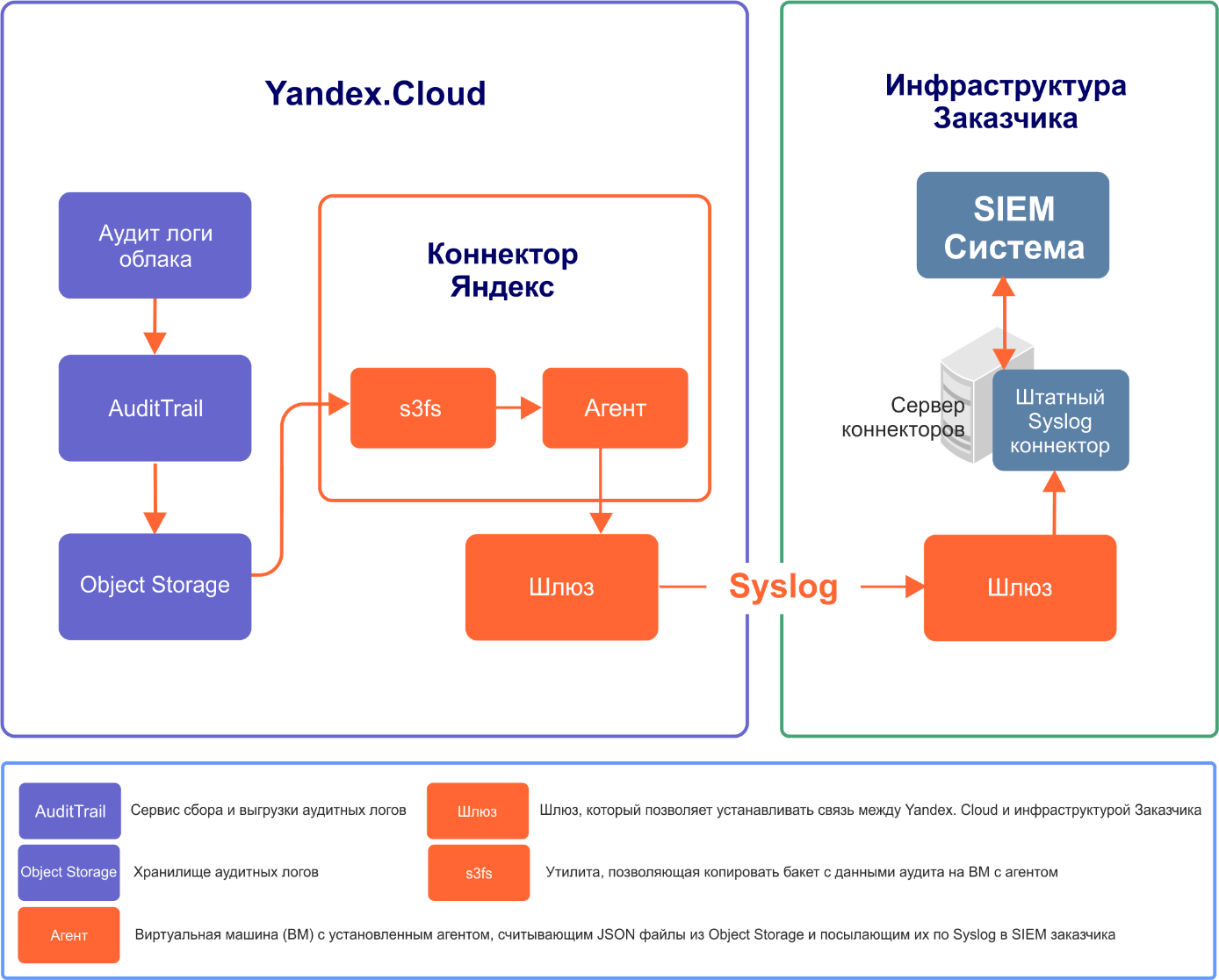


Рисунок 4. Архитектура коннектора

# **Источники данных и события**

Коннектор позволяет производить сбор событий со следующих источников Yandex.Cloud:

* Audit Trails;
* Cloud Logging;
* Compute Cloud;
* Identity and Access Management;
* Key Management Service;
* Yandex Lockbox;
* Network Load Balancer;
* Object Storage;
* Resource Manager;
* Virtual Private Cloud;
* YDB.

Перечень событий, сбор которых производится с сервиса Audit Trails, представлен в Таблице 1.

Таблица 1. Audit Trails

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | CreateTrail | Создание трейла |
|  | DeleteTrail | Удаление трейла |
|  | SetTrailAccessBindings | Назначение привязок прав доступа для трейла |
|  | UpdateTrail | Изменение трейла |
|  | UpdateTrailAccessBindings | Обновление привязок прав доступа для трейла |

Перечень событий, сбор которых производится с сервиса Cloud Logging, представлен в Таблице 2.

Таблица 2. Cloud Logging

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | CreateLogGroup | Создание лог-группы |
|  | UpdateLogGroup | Изменение лог-группы |
|  | UpdateLogGroup | Удаление лог-группы |
|  | SetLogGroupAccessBindings | Назначение привязок прав доступа для лог-группы |
|  | UpdateLogGroupAccessBindings | Обновление привязок прав доступа для лог-группы |

Перечень событий, сбор которых производится с сервиса Compute Cloud, представлен в Таблице 3.

Таблица 3. Compute Cloud

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | AddInstanceOneToOneNat | Добавление публичного IP-адреса виртуальной машине (ВМ) |
|  | AttachInstanceDisk | Подключение диска к ВМ |
|  | AttachInstanceFilesystem | Подключение файловой системы к ВМ |
|  | CreateDisk | Создание диска |
|  | CreateFilesystem | Создание файловой системы |
|  | CreateFilesystem | Создание образа диска |
|  | CreateInstance | Создание ВМ |
|  | CreateSnapshot | Создание снимка диска |
|  | DeleteDisk | Удаление диска |
|  | DeleteFilesystem | Удаление файловой системы |
|  | DeleteImage | Удаление образа диска |
|  | DeleteInstance | Удаление ВМ |
|  | DeleteSnapshot | Удаление снимка диска |
|  | DetachInstanceDisk | Отключение диска от ВМ |
|  | DetachInstanceFilesystem | Отключение файловой системы к ВМ |
|  | RemoveInstanceOneToOneNat | Удаление публичного IP-адреса ВМ |
|  | RestartInstance | Перезагрузка ВМ |
|  | RestartInstance | Запуск ВМ |
|  | StopInstance | Остановка ВМ |
|  | UpdateDisk | Изменение диска |
|  | UpdateFilesystem | Изменение файловой системы |
|  | UpdateImage | Изменение образа диска |
|  | UpdateInstance | Изменение ВМ |
|  | UpdateInstanceMetadata | Изменение метаданных ВМ |
|  | UpdateInstanceNetworkInterface | Изменение сетевых настроек ВМ |
|  | UpdateSnapshot | Изменение снимка диска |
|  | instancegroup.CreateInstanceGroup | Создание группы ВМ |
|  | instancegroup.DeleteInstanceGroup | Удаление группы ВМ |
|  | instancegroup.PauseInstanceGroup | Приостановка процессов управления группой ВМ |
|  | instancegroup.ResumeInstanceGroup | Возобновление процессов управления группой ВМ |
|  | instancegroup.StartInstanceGroup | Запуск группы ВМ |
|  | instancegroup.StopInstanceGroup | Остановка группы ВМ |
|  | instancegroup.UpdateInstanceGroup | Изменение группы ВМ |
|  | instancegroup.UpdateInstanceGroupAccessBindings | Назначение роли на группу ВМ |

Перечень событий, сбор которых производится с сервиса Identity and Access Management, представлен в Таблице 4.

Таблица 4. Identity and Access Management

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | AddFederatedUserAccounts | Добавление пользователя в федерацию |
|  | CreateAccessKey | Создание ключа доступа |
|  | CreateApiKey | Создание API-ключа |
|  | CreateCertificate | Добавление сертификата для федерации |
|  | CreateFederation | Создание федерации |
|  | CreateIamCookieForSubject | Вход федеративного пользователя |
|  | CreateKey | Создание пары ключей для сервисного аккаунта |
|  | CreateServiceAccount | Создание сервисного аккаунта |
|  | DeleteAccessKey | Удаление ключа доступа |
|  | DeleteApiKey | Удаление API-ключа |
|  | DeleteCertificate | Удаление сертификата для федерации |
|  | DeleteFederation | Удаление федерации |
|  | DeleteKey | Удаление пары ключей для сервисного аккаунта |
|  | DeleteServiceAccount | Удаление сервисного аккаунта |
|  | UpdateAccessKey | Обновление ключа доступа |
|  | UpdateApiKey | Обновление API-ключа |
|  | UpdateCertificate | Обновление сертификата |
|  | UpdateFederation | Обновление федерации |
|  | UpdateKey | Обновление пары ключей |
|  | UpdateServiceAccount | Обновление сервисного аккаунта |
|  | UpdateServiceAccountAccessBindings | Обновление списка привязок прав доступа |

Перечень событий, сбор которых производится с сервиса Key Management Service, представлен в Таблице 5.

Таблица 5. Key Management Service

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | CancelDeleteSymmetricKey | Отмена ранее запланированного уничтожения ключа |
|  | CancelSymmetricKeyVersionDestruction | Отмена ранее запланированного уничтожения версии симметричного ключа |
|  | CreateSymmetricKey | Создание симметричного ключа |
|  | DeleteSymmetricKey | Удаление симметричного ключа |
|  | RotateSymmetricKey | Ротация симметричного ключа |
|  | ScheduleSymmetricKeyVersionDestruction | Запланирование уничтожения версии симметричного ключа |
|  | SetPrimarySymmetricKeyVersion | Выбор основной версии симметричного ключа |
|  | SetSymmetricKeyAccessBindings | Выбор привязок прав доступа для симметричного ключа |
|  | UpdateSymmetricKey | Изменение симметричного ключа |
|  | UpdateSymmetricKeyAccessBindings | Обновление привязок прав доступа для симметричного ключа |

Перечень событий, сбор которых производится с сервиса Yandex Lockbox, представлен в Таблице 6.

Таблица 6. Yandex Lockbox

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | AddVersion | Добавление версии секрета |
|  | ActivateSecret | Активация секрета |
|  | CancelVersionDestruction | Отмена ранее запланированного уничтожения версии секрета |
|  | CreateSecret | Создание секрета |
|  | DeactivateSecret | Деактивация секрета |
|  | DeleteSecret | Удаление секрета |
|  | ScheduleVersionDestruction | Распланирование уничтожения версии секрета |
|  | SetSecretAccessBindings | Выбор привязок прав доступа для секрета |
|  | UpdateSecret | Изменение секрета |
|  | UpdateSecretAccessBindings | Обновление привязок прав доступа для секрета |

Перечень событий, сбор которых производится с сервиса Network Load Balancer, представлен в Таблице 7.

Таблица 7. Network Load Balancer

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | AddNetworkLoadBalancerListener | Добавление обработчика к сетевому балансировщику |
|  | AddTargetGroupTargets | Добавление ВМ к целевой группе |
|  | AttachNetworkLoadBalancerTargetGroup | Подключение целевой группы к сетевому балансировщику |
|  | CreateNetworkLoadBalancer | Создание сетевого балансировщика |
|  | CreateTargetGroup | Создание целевой группы |
|  | DeleteNetworkLoadBalancer | Удаление сетевого балансировщика |
|  | DeleteTargetGroup | Удаление целевой группы |
|  | DetachNetworkLoadBalancerTargetGroup | Отсоединение целевой группы от сетевого балансировщика |
|  | RemoveNetworkLoadBalancerListener | Удаление обработчика из сетевого балансировщика |
|  | RemoveTargetGroupTargets | Удаление ВМ из целевой группы |
|  | StartNetworkLoadBalancer | Запуск сетевого балансировщика |
|  | StopNetworkLoadBalancer | Остановка сетевого балансировщика |
|  | UpdateNetworkLoadBalancer | Изменение сетевого балансировщика |
|  | UpdateTargetGroup | Изменение целевой группы |

Перечень событий, сбор которых производится с сервиса Object Storage, представлен в Таблице 8.

Таблица 8. Object Storage

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | BucketAclUpdate | Изменение ACL бакета |
|  | BucketCorsUpdate | Изменение конфигурации CORS бакета |
|  | BucketCreate | Создание бакета |
|  | BucketDelete | Удаление бакета |
|  | BucketHttpsUpdate | Изменение HTTPS-конфигурации для бакета |
|  | BucketLifecycleUpdate | Изменение жизненного цикла объекта в бакете |
|  | BucketPolicyUpdate | Изменение политик доступа бакета |
|  | BucketUpdate | Изменение бакета |
|  | BucketWebsiteUpdate | Изменение конфигурации веб-сайта |
|  | ObjectCreate | Создание объекта в бакете |
|  | ObjectDelete | Удаление объекта в бакете |
|  | ObjectUpdate | Изменение объекта в бакете |

Перечень событий, сбор которых производится с сервиса Resource Manager, представлен в Таблице 9.

Таблица 9. Resource Manager

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | CreateCloud | Создание облака |
|  | CreateFolder | Создание каталога |
|  | DeleteCloud | Удаление облака |
|  | DeleteFolder | Удаление каталога |
|  | UpdateCloud | Изменение облака |
|  | UpdateCloudAccessBindings | Обновление привязок прав доступа для облака |
|  | UpdateFolder | Обновление каталога |
|  | UpdateFolderAccessBindings | Обновление привязок прав доступа для каталога |

Перечень событий, сбор которых производится с сервиса Virtual Private Cloud, представлен в Таблице 10.

Таблица 10. Virtual Private Cloud

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | CreateAddress | Создание адреса облачных ресурсов |
|  | CreateNetwork | Создание облачной сети |
|  | CreateRouteTable | Создание таблицы маршрутизации |
|  | CreateSecurityGroup | Создание группы безопасности |
|  | CreateSubnet | Создание облачной подсети |
|  | DeleteAddress | Удаление адреса облачных ресурсов |
|  | DeleteNetwork | Удаление облачной сети |
|  | DeleteRouteTable | Удаление таблицы маршрутизации |
|  | DeleteSecurityGroup | Удаление группы безопасности |
|  | DeleteSubnet | Удаление облачной подсети |
|  | MoveAddress | Перещение адреса облачных ресурсов в другой каталог |
|  | MoveNetwork | Перемещение облачной сети в другой каталог |
|  | MoveRouteTable | Перемещение таблицы маршрутизации в другой каталог |
|  | MoveSecurityGroup | Перемещение группы безопасности в другой каталог |
|  | MoveSubnet | Перемещение облачной подсети в другой каталог |
|  | UpdateAddress | Изменение адреса облачных ресурсов |
|  | UpdateNetwork | Изменение облачной сети |
|  | UpdateRouteTable | Изменение таблицы маршрутизации |
|  | UpdateSecurityGroup | Изменение группы безопасности |
|  | UpdateSubnet | Изменение облачной подсети |

Перечень событий, сбор которых производится с сервиса YDB, представлен в Таблице 11.

Таблица 11. YDB

|  |  |  |
| --- | --- | --- |
| № | Имя события | Описание |
|  | BackupDatabase | Создание бэкапа базы данных |
|  | CreateDatabase | Создание базы данных |
|  | DeleteBackup | Удаление бэкапа базы данных |
|  | DeleteDatabase | Удаление базы данных |
|  | RestoreBackup | Восстановление базы данных из бэкапа |
|  | StartDatabase | Запуск базы данных |
|  | StopDatabase | Остановка базы данных |
|  | UpdateDatabase | Изменение базы данных |

Необходимо отметить, что представленный выше набор событий может со временем изменяться в связи с развитием продукта Yandex.Cloud.

С актуальным составом событий сервисов Yandex.Cloud Вы можете ознакомиться в онлайн-документации по продукту Yandex.Cloud: <https://cloud.yandex.ru/docs/audit-trails/concepts/events>.

**Примеры получаемых событий**

Ниже представлены примеры мониторинга событий аудита приложений Yandex.Cloud в различных SIEM системах.

Изображение выглядит как стол

Автоматически созданное описание

Рисунок 1. Пример мониторинга событий аудита в SIEM системе ArcSight

*Изображение выглядит как текст

Автоматически созданное описание*

Рисунок 2. Пример мониторинга событий аудита в SIEM системе KUMA

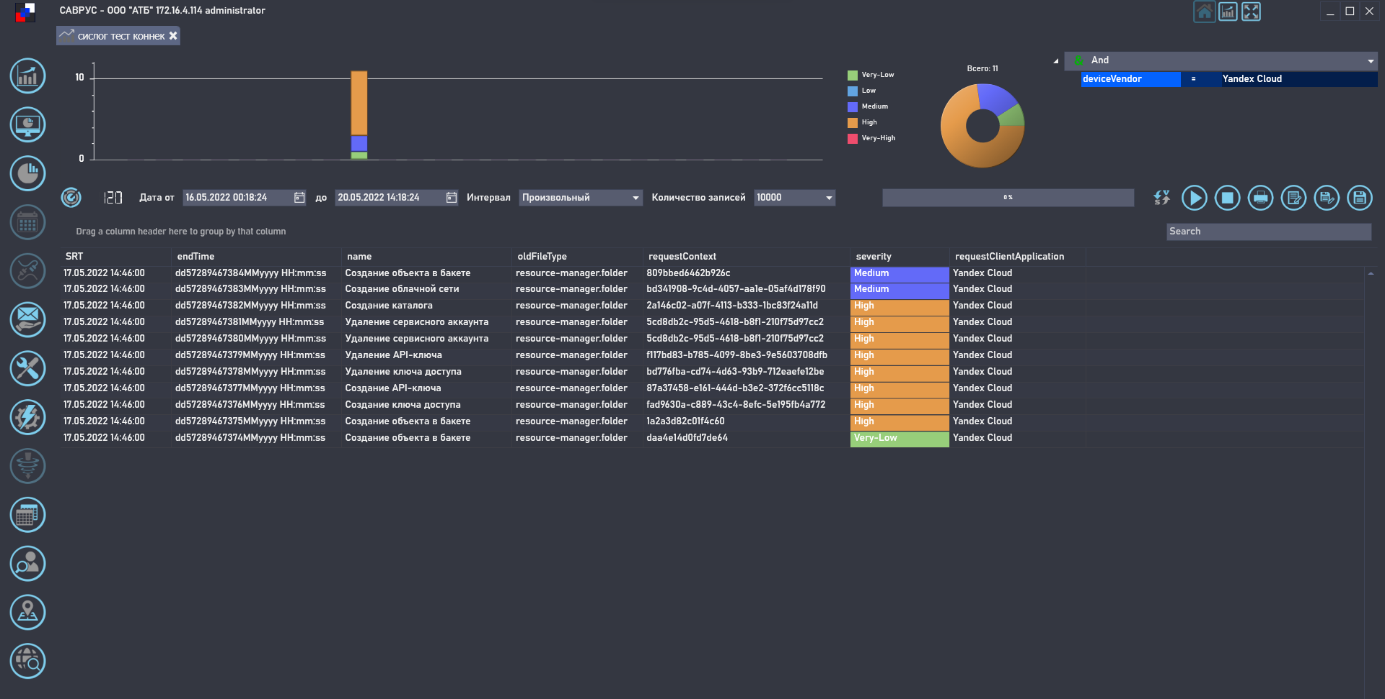


Рисунок 3. Пример мониторинга событий аудита в SIEM системе САВРУС

# **Анализ событий**

Для демонстрации возможностей анализа событий информационной безопасности Yandex.Cloud для SIEM ArcSight был разработан arb-пакет с примерами правил обработки событий, выложенный в свободном доступе по ссылке: <https://gitlab.ast-security.ru:14855/rodion/yandexcloudflex/blob/master/YandexCloud.arb>

Arb-пакет для SIEM ArcSight, включает следующие ресурсы:

* Parsing file (+map file);
* Dashboard, на котором отражена полезная статистика по событиям ИБ;
* набор фильтров, активных каналов и активных листов;
* набор правил корреляции (use cases).

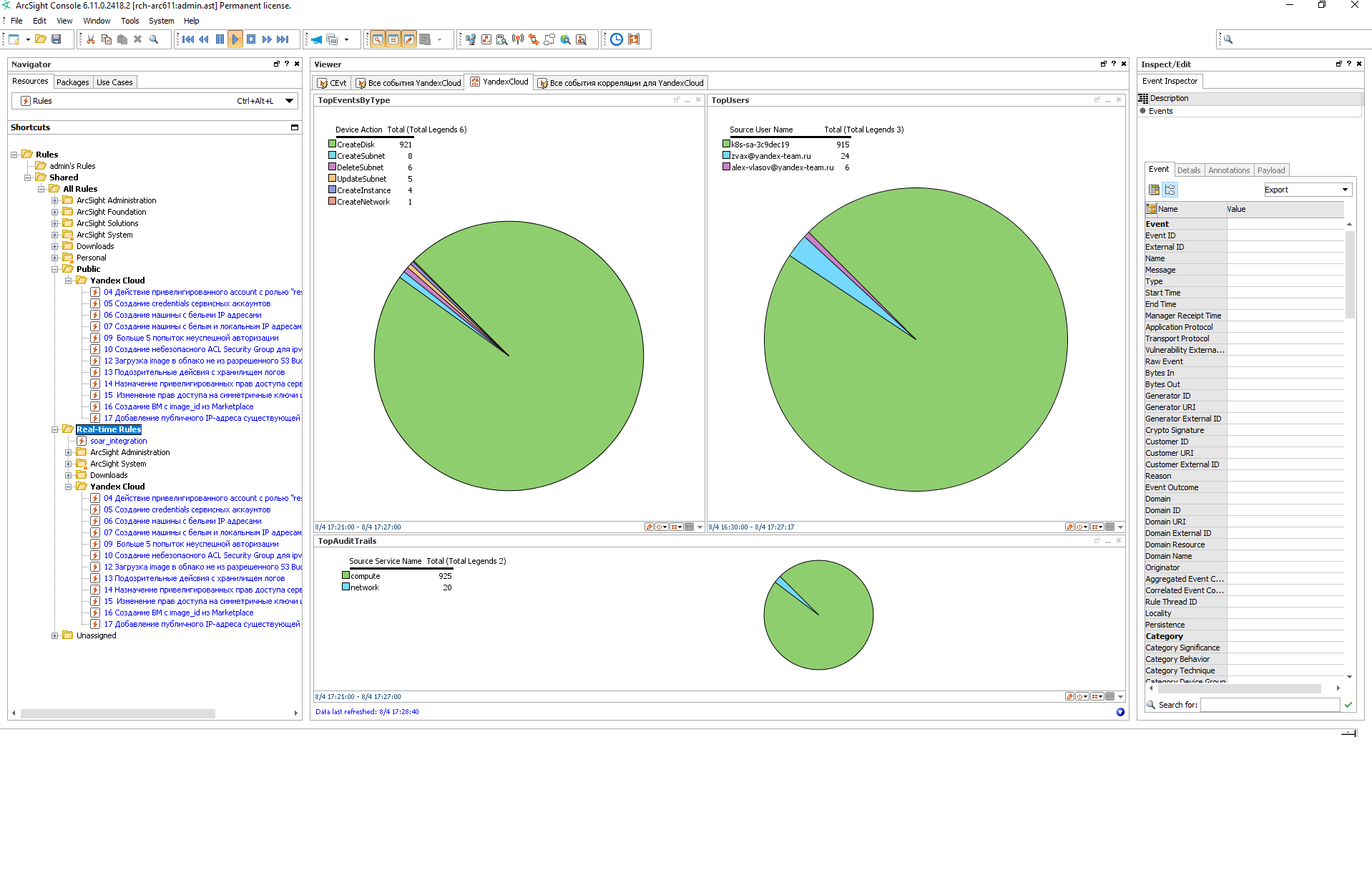


Рисунок 5. Анализ событий в SIEM ArcSight

**Активные каналы**, представленные в составе модуля описаны в Таблице 12

Таблица 12. Активные каналы

|  |  |  |
| --- | --- | --- |
| № | Наименование | Описание |
|  | Search:Yandexcloud: Find events by username | Поиск всех событий по конкретному username за конкретный период времени (необходимо ввести имя пользователя в поле user.name) |
|  | Serarch:Yandexcloud: Find events by folder\_name | Поиск всех событий по конкретному folder (необходимо ввести имя папки в поле cloud.folder.name) |

**Дашборд**, представленный в составе модуля, описан в Таблице 13

Таблица 13. Активные каналы

|  |  |  |
| --- | --- | --- |
| № | Наименование | Описание |
|  | AuditTrails Dashboard | Дашборд, который содержит в себе необходимую информацию для отслеживания состояния безопасности на основе событий AuditTrails |

Правила обработки событий **(Use cases)**, представленные в составе модуля, описаны в Таблице 14

Таблица 14. Правила обработки событий

|  |  |  |
| --- | --- | --- |
| № | Наименование | Описание |
|  | Yandexcloud:Creating of service-account's credentials (keys) | События создания всех видов ключей доступа для сервисных аккаунтов |
|  | Yandexcloud:Create instances with public IP | События создания ВМ с публичным IP адресом |
|  | Yandexcloud:Create instances with 2 interfaces | События создания ВМ с 2-мя интерфейсами |
|  | Yandexcloud: resource- manager.cloud.owner events | События любого действия под привилегированной УЗ resource- manager.cloud.owner events (необходимо ввести имя пользователя в поле user.name) |
|  | Yandexcloud: unauthorized events (permission denied) | События неуспешной авторизации (отказ в доступе) |
|  | Yandexcloud: Any create or  update SG (security group) | События любого изменения или создания Security Group |
|  | Yandexcloud:Create dangerous 0.0.0.0 ACL:SG | События создания слишком широкого ACL в Security Group (с префиксом 0.0.0.0/0) |
|  | Yandexcloud: Create image from S3 uri | Создание образа для ВМ с загрузкой из Object Storage бакета |
|  | Yandexcloud: Changes of S3  acl, policy | События изменений ACL и BucketPolicy S3 Object Storage |
|  | Yandexcloud: Bind IAM Admin  role to resources | События назначения общей роли Admin на ресурсы (folder/cloud, др. ресурс) |
|  | Yandexcloud: Bind access  rights to KMS key | События назначения прав на ключи KMS |
|  | Yandexcloud: Create instance with marketplace image | События создания ВМ с образом из Market place (как правило содержат платные лицензии) |
|  | Yandexcloud: Add public IP to  VM | События добавления публичного адреса существующей ВМ |
|  | Yandexcloud: Add access  binding VPC\_publicAdmin | События назначения роли vpc.public.admin |
|  | Yandexcloud: Connect admins from YC, Terraform | События обращения к API облака с помощью YC или terraform (user-agent), с указанием user name и ip адреса |
|  | Yandexcloud:Create public  address without antiddos | События создание публичного адреса без галочки защиты от DDOS |
|  | Yandexcloud:Create instance  without SG | События создания ВМ без Security Group |
|  | Yandexcloud:Create instance  with Serialport | События создания ВМ с включённым серийным портом |

Следует отметить, что хотя представленный в пакете набор ресурсов безусловно может быть полезен многим пользователям в исходном виде, все же для полноценного использования данного модуля требуется разработка новых и адаптация представленных ресурсов SIEM системы в соответствии с действительными потребностями пользователя в области мониторинга событий информационной безопасности.

Такую разработку и адаптацию пользователь может выполнить как самостоятельно, так и обратившись в техническую поддержку по данному продукту (услуга платная). Также при необходимость подобный набор ресурсов может быть разработан для других SIEM систем

Компания АТБ предоставляет услуги по сопровождению, поставке и внедрению SIEM систем, а также разработке дополнительных модулей и коннекторов. Контакты для связи: [info@ast-security.ru](mailto:info@ast-security.ru), +7 499 648 7548.