В какие лицензии входят объекты:

Объект ELK/License	**Free and open**	**Basic**	**Gold**	**Platinum**
Detection rule	-	+	+	+
Alerts	-	-	+	+
Saved Query (eql)	-	+	+	+
Dashboards (drilldown)	-	+	+	+
Support	-	-	-Business hrs -Critical: 4 hrs L2: 1 day L3: 2 days -Unlim incidents -Web and phone	-24/7/365 -Critical: 1 hr L2: 4 hrs L3: 1 day -Unlim incidents -Web and phone -emergency patches

Список объектов AuditTrails

№	**Название в ELK**	**Описание**	**Объект в ELK**
Searches			
1	Search:Yandexcloud: Find events by username	Поиск всех событий по конкретному username за конкретный период времени (необходимо ввести имя пользователя в поле user.name)	Saved Query
2	Serarch:Yandexcloud: Find events by folder_name	Поиск всех событий по конкретному folder (необходимо ввести имя папки в поле cloud.folder.name)	Saved Query
Dashboard			
	AuditTrails Dashboard	Dashboard, который содержит в себе необходимую информацию для отслеживания состояния безопасности на основе событий AuditTrails	DashBoard
Use cases			
3	Yandexcloud:Creating of service-account's credentials (keys)	События создания всех видов ключей доступа для сервисных аккаунтов	Saved Query Detection Rule
4	Yandexcloud:Create instances with public IP	События создания ВМ с публичным IP адресом	Saved Query Detection Rule
5	Yandexcloud:Create instances with 2 interfaces	События создания ВМ с 2-мя интерфейсами	Saved Query Detection Rule
6	Yandexcloud: resource-manager.cloud.owner events	События любого действия под привелигированной УЗ resource-manager.cloud.owner events	Saved Query Detection Rule

		(необходимо ввести имя пользователя в поле user.name)	
7	Yandexcloud: unauthorized events (permission denied)	События неуспешной авторизации (отказ в доступе)	Saved Query Detection Rule (превышение порога в 3 события создает алерт)
8	Yandexcloud: Any create or update SG (security group)	События любого изменения или создания Security Group	Saved Query Detection Rule
9	Yandexcloud:Create dangerous 0.0.0.0 ACL:SG	.События создания слишком широкого ACL в Security Group (с префиксом 0.0.0.0/0)	Saved Query Detection Rule
10	Yandexcloud: Create image from S3 uri	Создание образа для ВМ с загрузкой из Object Storage бакета	Saved Query Detection Rule
11	Yandexcloud: Changes of S3 acl, policy	События изменений ACL и BucketPolicy S3 Object Storage	Saved Query Detection Rule
12	Yandexcloud: Bind IAM Admin role to resources	События назначения общей роли Admin на ресурсы (folder/cloud, др. ресурс)	Saved Query Detection Rule
13	Yandexcloud: Bind access rights to KMS key	События назначения прав на ключи KMS	Saved Query Detection Rule
14	Yandexcloud: Create instance with marketplace image	События создания ВМ с образом из Market place (как правило содержат платные лицензии)	Saved Query Detection Rule
15	Yandexcloud: Add public IP to VM	События добавления публичного адреса существующей ВМ	Saved Query Detection Rule
16	Yandexcloud: Add access binding VPC_publicAdmin	События назначения роли vpc.public.admin	Saved Query Detection Rule
17	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	Saved Query Detection Rule
18	Yandexcloud:Create public address without antiddos	События создание публичного адреса без галочки защиты от ddos	Saved Query Detection Rule
19	Yandexcloud:Create instance without SG	События создания ВМ без Security Group	Saved Query Detection Rule
20	Yandexcloud:Create instance with Serialport	События создания ВМ с включенным серийным портом	Saved Query Detection Rule

Список объектов k8s

№	**Название в ELK**	**Описание**	**Объект в ELK**
Searches			
1	Search:Yandexcloud:k8s:Interesting fields	Поиск всех событий k8s по интересным полям	Saved Query
Dashboard			

2	k8s-dashboard	Dashboard, который содержит в себе необходимую информацию для отслеживания состояния безопасности на основе событий k8s	DashBoard
Use cases			
Общие			
3	Yandexcloud:k8s:unauthorized-events	События отказа в доступе - unauthorized	Saved Query Detection Rule
4	Yandexcloud:k8s:assign-cluster-admin_or_admin	Назначение cluster-admin или admin роли (clusterrolebinding или rolebinding)	Saved Query Detection Rule
5	Yandexcloud:k8s:success-connect-from-ip	Успешное подключение к кластеру с внешнего IP адреса	Saved Query Detection Rule
6	Yandexcloud:k8s:network-policy-actions	NetworkPolicies: создание, удаление, изменение	Saved Query Detection Rule
7	Yandexcloud:k8s:exec-to-container	Exec внутрь контейнера (шелл внутрь контейнера)	Saved Query Detection Rule
8	Yandexcloud:k8s:image-not-from-yandex-registry	Создание pod с image НЕ из Yandex container registry (не актуально для Клиентов использующих собственный cr)	Saved Query Detection Rule
9	Yandexcloud:k8s:create-pod-in-kube-system	Создание pod в kube-system namespace	Saved Query Detection Rule
Falco			
10	Yandexcloud:k8s:falco:alerts	Любой alert от Falco	Saved Query Detection Rule
11	Yandexcloud:k8s:falco:delete	Falco удален	Saved Query Detection Rule
OPA Gatekeeper			
12	Yandexcloud:k8s:opa-gatekeeper-detection	Срабатывание OPA Gatekeeper – denied events (только в режиме enforce)	Saved Query Detection Rule
13	Yandexcloud:k8s:OPA-delete-constraint	Изменение/удаление объекта Constraint	Saved Query Detection Rule
14	Yandexcloud:k8s:delete-opa-gatekeeper	Удаление Gatekeeper из кластера k8s	Saved Query Detection Rule
Kyverno			
15	Yandexcloud:k8s:kyverno-gatekeeper-detection	Срабатывание Kyverno – denied events (только в режиме enforce)	Saved Query Detection Rule
16	Yandexcloud:k8s:kyverno-delete-policy	Изменение/удаление объекта Kyverno Policy	Saved Query Detection Rule
17	Yandexcloud:k8s:delete-kyverno	Удаление Kyverno из кластера k8s	Saved Query Detection Rule