Licenses containing objects

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

List of AuditTrails objects

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **ELK name** | **Description** | **ELK object** |
| Searches | | | |
| 1 | Search:Yandexcloud: Find events by username | Search for all events with a specific username over a specified time period (username must be specified in the user.name field) | Saved Query |
| 2 | Serarch:Yandexcloud: Find events by folder\_name | Search for all events in a specific folder (the folder name must be specified in the cloud.folder.name field) | Saved Query |
| Dashboard | | | |
|  | [AuditTrails Dashboard](https://c-c9qfr7e8e470ghr1lanf.rw.mdb.yandexcloud.net/app/dashboards#/view/33978670-e543-11eb-b941-f7bd9d79b315) | Dashboard containing the data required to monitor the security status based on AuditTrails events | DashBoard |
| Use cases | | | |
| 3 | Yandexcloud:Creating of service-account's credentials (keys) | Generating all types of service account access keys | Saved Query  Detection Rule |
| 4 | Yandexcloud:Create instances with public IP | Creating a VM with a public IP address | Saved Query  Detection Rule |
| 5 | Yandexcloud:Create instances with 2 interfaces | Creating a VM with two interfaces | Saved Query  Detection Rule |
| 6 | Yandexcloud: resource-manager.cloud.owner events | Any action performed under a privileged account resource-manager.cloud.owner (username must be specified in the user.name field) | Saved Query  Detection Rule |
| 7 | Yandexcloud: unauthorized events (permission denied) | Failed authorization (access denied) | Saved Query  Detection Rule  (превышение порога в 3 события создает алерт) |
| 8 | Yandexcloud: Any create or update SG (security group) | Any modification or creation of a Security Group | Saved Query  Detection Rule |
| 9 | Yandexcloud:Create dangerous 0.0.0.0 ACL:SG | Creating a Security Group ACL that is too broad (using 0.0.0.0/0 prefix) | Saved Query  Detection Rule |
| 10 | Yandexcloud: Create image from S3 uri | Creating a VM image by loading data from an Object Storage bucket | Saved Query  Detection Rule |
| 11 | Yandexcloud: Changes of S3 acl, policy | ACL Change and BucketPolicy in S3 Object Storage | Saved Query  Detection Rule |
| 12 | Yandexcloud: Bind IAM Admin role to resources | Assigning the general Administrator role to resources (folder/cloud, etc.). | Saved Query  Detection Rule |
| 13 | Yandexcloud: Bind access rights to KMS key | Assigning KMS keys | Saved Query  Detection Rule |
| 14 | Yandexcloud: Create instance with marketplace image | Creating a VM from a Marketplace image (typically contains paid licenses) | Saved Query  Detection Rule |
| 15 | Yandexcloud: Add public IP to VM | Adding a public address to an existing VM | Saved Query  Detection Rule |
| 16 | Yandexcloud: Add access binding VPC\_publicAdmin | Assigning a vpc.public.admin role | Saved Query  Detection Rule |
| 17 | Yandexcloud: Connect admins from YC, Terraform | Accessing the cloud API via YC or Terraform (user-agent), with the username and IP address specified | Saved Query  Detection Rule |
| 18 | Yandexcloud:Create public address without antiddos | Generating a public address without enabling ddos protection | Saved Query  Detection Rule |
| 19 | Yandexcloud:Create instance without SG | Creating a VM without a Security Group | Saved Query  Detection Rule |
| 20 | Yandexcloud:Create instance with Serialport | Creating a VM with a serial port enabled | Saved Query  Detection Rule |

List of k8s objects

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **ELK name** | **Description** | **ELK object** |
| Searches | | | |
| 1 | Search:Yandexcloud:k8s:Interesting fields | Searching for all k8s events based on the specific fields | Saved Query |
| Dashboard | | | |
| 2 | k8s-dashboard | Dashboard containing the information required to monitor the security status in response to k8s events | DashBoard |
| Use cases | | | |
| General | | | |
| 3 | Yandexcloud:k8s:unauthorized-events | Denied access - unauthorized | Saved Query  Detection Rule |
| 4 | Yandexcloud:k8s:assign-cluster-admin\_or\_admin | Assigning an administrator or cluster-administrator role (clusterrolebinding or rolebinding) | Saved Query  Detection Rule |
| 5 | Yandexcloud:k8s:success-connect-from-ip | Successful connection to a cluster from an external IP address | Saved Query  Detection Rule |
| 6 | Yandexcloud:k8s:network-policy-actions | NetworkPolicies: create, delete, and modify | Saved Query  Detection Rule |
| 7 | Yandexcloud:k8s:exec-to-container | Exec into a container (shell into a container) | Saved Query  Detection Rule |
| 8 | Yandexcloud:k8s:image-not-from-yandex-registry | Creating a pod with an image that is NOT from the Yandex container registry (does not apply to clients who use their own cr) | Saved Query  Detection Rule |
| 9 | Yandexcloud:k8s:create-pod-in-kube-system | Creating a pod in the kube-system namespace | Saved Query  Detection Rule |
| Falco | | | |
| 10 | Yandexcloud:k8s:falco:alerts | Any alert from Falco | Saved Query  Detection Rule |
| 11 | Yandexcloud:k8s:falco:delete | Falco deleted | Saved Query  Detection Rule |
| OPA Gatekeeper | | | |
| 12 | Yandexcloud:k8s:opa-gatekeeper-detection | OPA Gatekeeper triggered - denied events (only in enforce mode) | Saved Query  Detection Rule |
| 13 | Yandexcloud:k8s:OPA-delete-constraint | Modifying/deleting a Constraint object | Saved Query  Detection Rule |
| 14 | Yandexcloud:k8s:delete-opa-gatekeeper | Removing a gatekeeper from a k8s cluster | Saved Query  Detection Rule |
| Kyverno | | | |
| 15 | Yandexcloud:k8s:kyverno-gatekeeper-detection | Kyverno triggered - denied events (only in enforce mode) | Saved Query  Detection Rule |
| 16 | Yandexcloud:k8s:kyverno-delete-policy | Modifying/deleting a Kyverno Policy object | Saved Query  Detection Rule |
| 17 | Yandexcloud:k8s:delete-kyverno | Removing Kyverno from a k8s cluster | Saved Query  Detection Rule |