Сравнение решений по безопасности k8s

💰 - платное решение

✅ - функция выполняется

✅❗ - функция выполняется частично

| № | Функция | Aquasecurity enterprise💰 | \*-bench (kube,docker,linux) | Kube-hunter | Trivy | Starboard | Yandex CR vuln scanner    💰 | External Secrets | Luntry    💰 | Cilium enterprise    💰 | Sysdig    💰 | Osquery | Kubequery | Seccomp | | Falco  /Tracee  Tracee Logo | ClamAV | OPA Gatekeeper/Kyverno | Conftest/Kubesec | rbac-tool/ rback  / KubiScan | Weave Scope | Kubectl-graph/kubectl tree/kube-lineage |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Управление уязвимостями** | | | | | | | | | | | | | | | | | | | | | |  |
|  | Сканирование образов из image registry | ✅ |  |  | ✅ | ✅ | ✅ |  |  |  | ✅ |  |  |  | |  |  |  |  |  |  |  |
|  | Сканирование образов в запущенных workloads | ✅ |  |  |  | ✅ |  |  |  |  | ✅ |  |  |  | |  |  |  |  |  |  |  |
|  | Сканирование пакетов k8s node | ✅ |  |  |  |  |  |  |  |  | ✅ | ✅ |  |  | |  |  |  |  |  |  |  |
|  | Сканирование pentest k8s | ✅ |  | ✅ |  | ✅ |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |
|  | Сбор информации о системе ноды, юзерах, пакетах | ✅ |  |  |  |  |  |  |  |  | ✅ | ✅ |  |  | |  |  |  |  |  |  |  |
|  | Admission controller блокирующий на основе результатов сканера | ✅ |  |  |  |  |  |  |  |  | ✅ |  |  |  | |  |  |  |  |  |  |  |
| **Policy Engine** | | | | | | | | | | | | | | | | | | | | | |  |
|  | Политики уровня Admission Controller: runasnonroot, hostpath, priv | ✅ |  |  |  |  |  |  |  |  |  |  |  |  | |  |  | ✅ |  |  |  |  |
| **Runtime security** | | | | | | | | | | | | | | | | | | | | | |  |
|  | Политики runtime security на k8s node | ✅ |  |  |  |  |  |  | ✅❗  детект |  | ✅ |  |  |  | | ✅❗  детект |  |  |  |  |  |  |
|  | Политики runtime security на k8s container | ✅ |  |  |  |  |  |  | ✅❗  детект |  | ✅ |  |  |  | | ✅❗  детект |  |  |  |  |  |  |
|  | Политики на образы: non-root, base image, version of packets | ✅ |  |  |  |  |  |  |  |  | ✅ |  |  |  | |  |  |  | ✅ |  |  |  |
|  | Ограничение системных вызовов SYSCALLS | ✅ |  |  |  |  |  |  |  | ✅❗  детект | ✅ | ✅❗  детект |  | ✅ | | ✅❗  детект |  |  |  |  |  |  |
|  | Построение профиля контейнера(вызовы, файлы, сетевая активность и тд.) + ограничение | ✅ |  |  |  |  |  |  | ✅ |  | ✅ | ✅❗  детект |  |  | |  |  |  |  |  |  |  |
| **Антивирусная защита** | | | | | | | | | | | | | | | | | | | | | |  |
|  | Защита от malware внутри контейнеров | ✅ |  |  |  |  |  |  | ✅❗  детект |  | ✅ | ✅❗  детект |  |  | | ✅❗  детект | ✅ |  |  |  |  |  |
|  | Проверка памяти контейнера для защиты от fileless атак | ✅ |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |
|  | Защита от malware k8s node | ✅ |  |  |  |  |  |  | ✅❗  детект |  | ✅ | ✅❗  детект |  |  | | ✅❗  детект | ✅ |  |  |  |  |  |
| **Управление секретами** | | | | | | | | | | | | | | | | | | | | | |  |
|  | Доставка секретов в k8s | ✅ |  |  |  |  |  | ✅ |  |  |  |  |  |  | |  |  |  |  |  |  |  |
|  | Сканирование наличия секретов в yaml | ✅ |  |  |  |  |  |  |  |  | ✅ |  |  |  | |  |  | ✅ |  |  |  |  |
| **FIM (File integrity monitoring)** | | | | | | | | | | | | | | | | | | | | | |  |
|  | FIM файлов на k8s node | ✅ |  |  |  |  |  |  |  |  |  | ✅ |  |  | |  |  |  |  |  |  |  |
|  | FIM файлов внутри pods | ✅ |  |  |  |  |  |  |  |  |  | ✅ |  |  | |  |  |  |  |  |  |  |
| **Защита сети** | | | | | | | | | | | | | | | | | | | | | |  |
|  | Построение карты сети и сетевых политик | ✅ |  |  |  |  |  |  | ✅ | ✅ | ✅ |  |  |  | |  |  |  |  |  | ✅❗  Без генерации |  |
|  | Отгрузка Flow logs | ✅ |  |  |  |  |  |  | ✅ | ✅ |  |  |  |  | |  |  |  |  |  |  |  |
| **Compliance** | | | | | | | | | | | | | | | | | | | | | |  |
|  | Проверка k8s node на соответствие K8s CIS benchmark | ✅ | ✅ |  |  | ✅ |  |  |  |  | ✅ |  |  |  | |  |  |  |  |  |  |  |
|  | Проверка на соответствие CIS Linux /docker benchmark | ✅ | ✅ |  |  | ✅ |  |  |  |  | ✅ |  |  |  | |  |  |  |  |  |  |  |
|  | Проверка на соответствие custom compliance политикам | ✅ |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |
| **Анализ ролей** | | | | | | | | | | | | | | | | | | | | | |  |
|  | Визаулизация текущих доступов RBAC | ✅ |  |  |  |  |  |  | ✅ |  |  |  |  |  | |  |  |  |  | ✅ |  |  |
|  | Построение графа связей между ролями и объектами |  |  |  |  |  |  |  | ✅ |  |  |  |  |  | |  |  |  |  | ✅ |  |  |
| **Анализ объектов** | | | | | | | | | | | | | | | | | | | | | |  |
|  | Просмотр и анализ объектов k8s в удобном виде | ✅ |  |  |  |  |  |  | ✅ |  | ✅ |  | ✅❗  sql |  |  | |  |  |  |  |  |  |
|  | Построение карты взаимодейсвтия объектов k8s |  |  |  |  |  |  |  | ✅(с возможностью линковать url сторонних решений) |  |  |  |  |  |  | |  |  |  |  |  | ✅❗ограничено |
| **Отгрузка в SIEM** | | | | | | | | | | | | | | | | | | | | | |  |
|  |  | ✅  ELK, Splunk, AWS, и тд. |  |  |  |  |  |  | ✅❗  Syslog |  | ✅  ELK, Splunk, AWS, и тд. |  |  |  | |  |  |  |  |  |  |  |