ITD GROUP

Решение для обеспечения безопасности и наблюдения за происходящим в Kubernetes

LUNTRY

Платформа Luntry – это security observability-решение для K8s, разработанное на основе eBPF.

Она предназначена для команд ИБ, DevOps и DevSecOps . Это решение позволяет справиться с такими задачами, как повышение прозрачности инфраструктуры, отслеживание изменений в Kubernetes, инвентаризация ресурсов, обеспечение безопасности.

С помощью Luntry можно упростить процесс планирования, повысить уровень согласованности действий команд, сократить временные затраты на поиск проблемы, увеличить уровень безопасности путем реализации концепции ZeroTrust.

- Полная картина происходящего в вашем Kubernetes-кластере без слепых зон.
- Понимание, как взаимодействуют между собой сервисы и приложения.
- Возможность быстро реагировать на сбои и инциденты в системе.
- Единое видение инфраструктуры всеми командами.
- Хронология эволюции вашего Kubernetes (Evolution timeline).
- Создание ресурсов и политик безопасности.

Решение Luntry – сенсорная система с поддержкой многокластерности и многопользовательности. Оно представляет собой набор контейнеров и YAML ресурсов для Kubernetes и устанавливается внутри Kubernetes-инфраструктуры клиента.

Время от установки решения до получения результата составляет всего 10 мин. При этом никакие данные не отправляются на внешние ресурсы, а остаются внутри вашей сети.

Luntry может эффективно работать с любыми видами Kubernetes-инфраструктуры: как внутрикорпоративными (On-Premise), так и расположенными на ресурсах облачных провайдеров (On-Cloud).

Все компоненты Luntry работают в отдельном пространстве имен Kubernetes. Для их работы не требуется никаких изменений со стороны команды разработчиков и DevOps-команды: ни в Kubernetes, ни в его микросервисах.

Luntry не модифицирует сервисы и не добавляет в них никакой дополнительной логики. Решение гарантирует отсутствие дополнительной нагрузки на микросервисы со своей стороны. Luntry совместимо с любыми сторонними разработкамих

Основная функциональность Luntry

1 **Управление уязвимостями образов**
На базе Kubernetes operators и в CI/CD

2 **Проверка Kubernetes ресурсов**
Policy Engine на базе Kyverno или OPA Gatekeeper

3 **Runtime Security**
- Обнаружение на базе eBPF сенсора
- Предотвращение на базе AppArmor политик

4 **Защита сети**
На базе NetworkPolicy или авторизационных политик ServiceMesh

5 **Анализ RBAC**
По субъектам, правам и ролям

6 **Интеграция с SIEM**
Выгрузка в syslog в CEF формате

Системные требования

Kubernetes: >= 1.16

Container Runtime: CRI совместимые (docker, containerd, cri-o)

CNI: Любой

OS kernel version: >= 4.18 >=3.10 (rhel7)

Для операционной команды и SRE

Наблюдение за инфраструктурой – важный аспект ее контроля

- Возможность планировать изменения и быстро решать проблемы с помощью ретроспективного анализа
- Видеть детальный контекст при анализе причин сбоев
- Визуализировать взаимодействия всех K8s компонентов и ресурсов
- Наблюдать за инфраструктурой, а также за любыми сторонними компонентами и их взаимодействиями
- Наблюдать за нетипичным поведением внутри инфраструктуры
- Возможность инвентаризировать ресурсы, видеть историю изменений
- Иметь необходимую информацию обо всех компонентах Kubernetes и возможность проведения корреляции событий в Kubernetes

Для разработчиков

Простой и понятный взгляд на сложную систему

- Видеть единую картину взаимодействий микросервисов
- Визуализировать жизненный цикл микросервисов в инфраструктуре Kubernetes
- Наблюдать за любым окружением Dev, Test, Stage и Prod
- Использовать дифференциальный анализ для поиска причин проблем и сбоев
- Отслеживать изменения и понимать причины их возникновения
- Обнаруживать необычное и нежелательное поведение и состояние
- Придерживаться Agile-принципов разработки
- Использовать в качестве портала для доступа к другим системам

Для команды информационной безопасности

Безопасность без слепых зон

- Сделать Kubernetes понятным на всех уровнях: от контейнеров до микросервисов
- Проводить поиск угроз, основанный на аномальном поведении внутри контейнеров и компонентов
- Поддерживать высокий уровень безопасности в быстром жизненном цикле разработки, наблюдая за быстро меняющейся инфраструктурой
- Планировать меры безопасности при помощи визуализации любых компонентов и их взаимодействий
- Использовать API для создания ресурсов NetworkPolicy и других настраиваемых ресурсов, связанных с безопасностью
- Использовать инструмент для Advanced Container Runtime Security
- Применять практики Shift Everywhere Security, Security-as-Code, Zero Trust

Для менеджмента

Единый опыт и знания о системе для эффективного управления

- Объединить знания о микросервисной инфраструктуре и скоординировать команды в компании
- Сократить time-to-market за счет возможности быстро принимать решения при добавлении изменений и возникновении проблем
- Видеть единую картину с актуальными данными о своей инфраструктуре для эффективного сотрудничества всех команд
- Посмотреть текущее состояние и историю изменений системы в любое время
- Стабильно управлять системой независимо от конкретных участников (bus factor)
- Оптимизировать ресурсы и время
- Сразу предоставить различным командам информацию об инфраструктуре в едином формате

LUNTRY

Решение для обеспечения
безопасности и наблюдения за
происходящим в Kubernetes

ITD GROUP

Официальный дистрибьютор – компания ITD Group

123557, Москва, Большой Тишинский переулок, д. 19, стр. 3

+7 (499) 502-13-75
info@iitdgroup.ru