Selectel TechDay

ZeroTrust в Kubernetes:
Не пустые слова

Дмитрий Евдокимов
Founder&CTO Luntry

LUNTRY

Обо мне

WhoAmI

- Основатель и технический директор Luntry
- Опыт в ИБ более 10 лет
- Специализация безопасность контейнеров и Kubernetes
- Программный комитет DevOpsConf, HighLoad++
- Бывший автор статей и редактор рубрик в журнале “ХАКЕР”
- Автор Telegram-канала “k8s (in)security”
- Автор курса “Cloud Native безопасность в Kubernetes”
- Не верит, что систему можно сделать надежной и безопасной, не понимая ее
- Докладчик: BlackHat, HITB, ZeroNights, HackInParis, Confidence, SAS, OFFZONE, PHDays, Kazhackstan, DevOpsConf, KuberConf, VK Kubernetes Conference, HighLoad++, DevOops, БЕКОН и др.

LUNTRY

Содержание

Что такое ZeroTrust

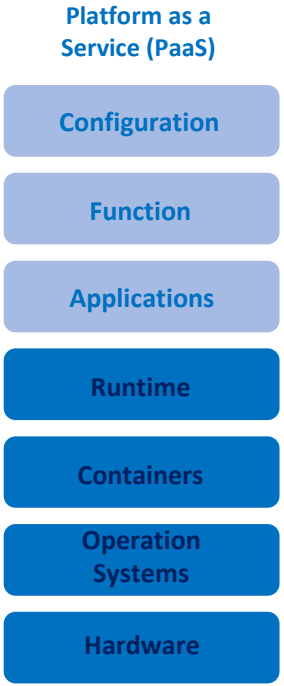
Что такое ZeroTrust?

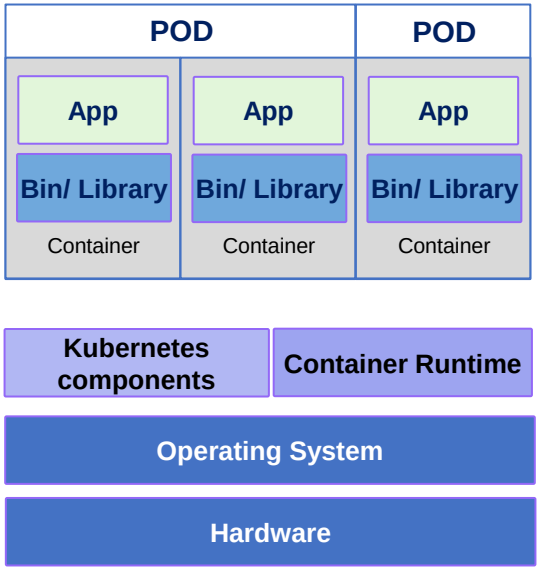
Cloud Native Security Whitepaper

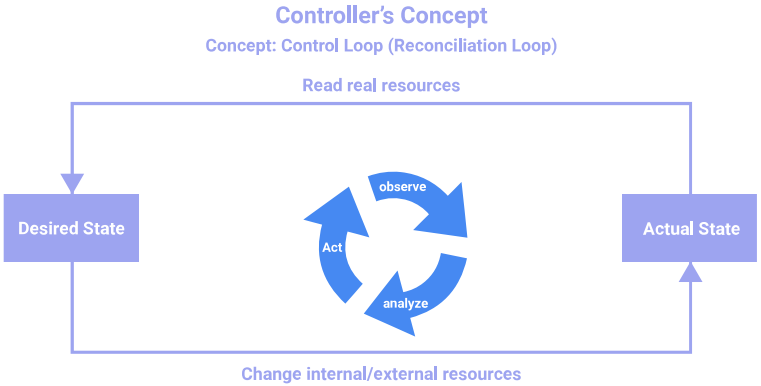
The perimeter for containerized applications deployed as microservices is the microservice itself. Therefore, it is necessary to define policies that restrict communication only between sanctioned microservice pairs. The inclusion of zero trust in the microservice architecture reduces the blast radius by preventing lateral movement should a microservice be compromised. Operators should ensure that they are using capabilities such as network policies to ensure that east-west network communication within the container deployment is limited to only that which is authorized for access. There is some initial work done to provide strategies for microservices security through NIST SP 800-204 and may serve as a guide for implementing secure microservice architectures.

Пару слов о Kubernetes

Kubernetes







Рекомендация: "Сочетание несочетаемого в Kubernetes: удобство, производительность, безопасность", Дмитрий Евдокимов

Суровая реальность

Все против нас

Безопасность образов контейнеров:

- Много известных уязвимостей (1-day)
- Уязвимости в собственном коде (0-day)
- Большая поверхность атаки (Living off the Land (LotL))
- Потенциально вредоносный код (Malware, backdoor, miners)
- Не соответствие лучшим практикам ИБ (Misconfiguration)

Безопасность микросервисов:

- Не соответствие лучшим практикам ИБ (Misconfiguration)

Проблемы были, есть и будут

Картину ухудшают:

- Нехватка ИБ кадров
- Не квалифицированные кадры
- Текучка кадров
- Сторонняя разработка
- Сроки
- Процессная волокита
- Регламенты
- Сертификаты
- …

Рекомендация: “Patch management не поможет, фиксики не спасут”, Дмитрий Евдокимов

Нивелируем проблемы ИБ в микросервисах

Безопасность в Kubernetes

Code	Images	Kubernetes manifest	Authentication	Authorization	Admission controllers	Audit	Runtime	Observability
SAST	Immutable	Labels, annotations	IAM	RBAC	LimitRanger	Kubernetes Audit Log	PodSecurityContext & SecurityContext	Asset management
DAST	Distroless images	IaC	PAM		ResourceQuota		seccomp, AppArmor, Selinux profiles	Security monitoring
IAST	Rootless containers	Security as Code			Validating/MutatingAdmissionWebhook		Sandbox/MicroVM	Application monitoring
RASP	SBOM	Compliance as Code			KubeletInUserNamespace		NetworkPolicy	Anomaly detection
SCA	Security scan	Configuration check			UserNamespacesSupport		Secret management	Compliance
	Secret scan				PolicyEngines/PSA/PSP/ValidatingAdmissionPolicy		Container specific OS	
	Sign				Kubernetes operators		Multitenancy	
	Registry staging							

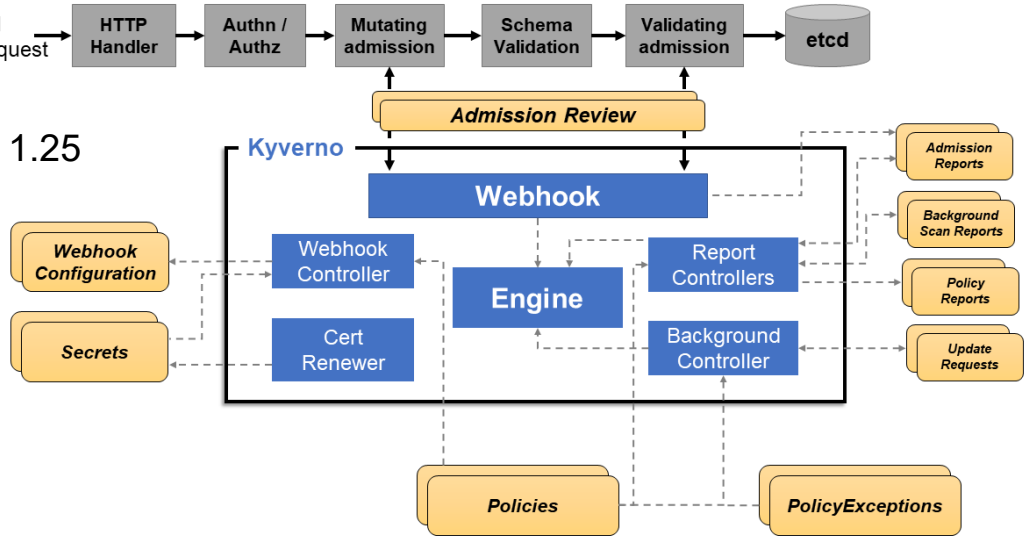
Рекомендация:

1) “Kubernetes: трансформация к SecDevSecOpsSec”, Дмитрий Евдокимов
2) “Классификация и систематизация средств безопасности для Kubernetes”, Дмитрий Евдокимов

Policy Engines

Не доверяем людям – не доверяем тому что кто-то пытается выкатить

- PODSECURITYPOLICY (PSP)
  - В deprecated статусе с 1.21 и удален в 1.25
- POD SECURITY ADMISSION (PSA)
  - В alpha стадии в 1.22
- VALIDATINGADMISSIONPOLICY
  - В alpha стадии в 1.26
- СОБСТВЕННАЯ РЕАЛИЗАЦИЯ
  - Свой Admission Controller
- POLICY ENGINES
  - Обязательно!!!

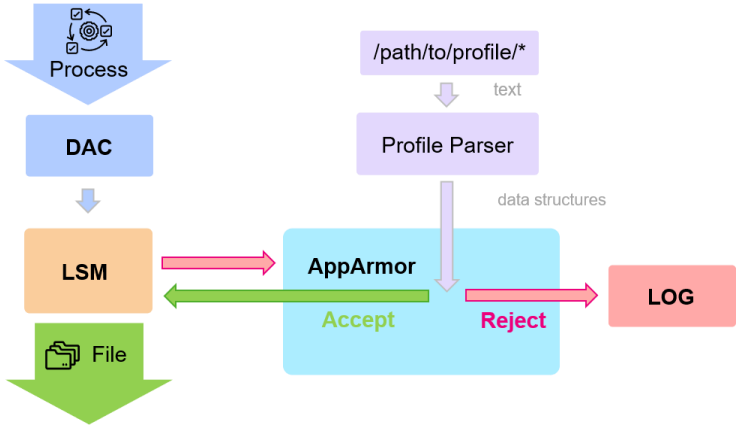


Рекомендация: “PolicyEngine в Kubernetes – что, как, зачем?”, Сергей Канибор

AppArmor

Не доверяем содержимому образа и строго его ограничиваем

- AppArmor (“Application Armor”) это Linux security modules (LSM)
- В профиле определяется какому файлу что можно в терминах capabilities и файловых прав доступа.
- Pathname-based подход
- Добавляется в Pod через аннотацию для контейнера.
- ОС: Ubuntu, SUSE, Debian

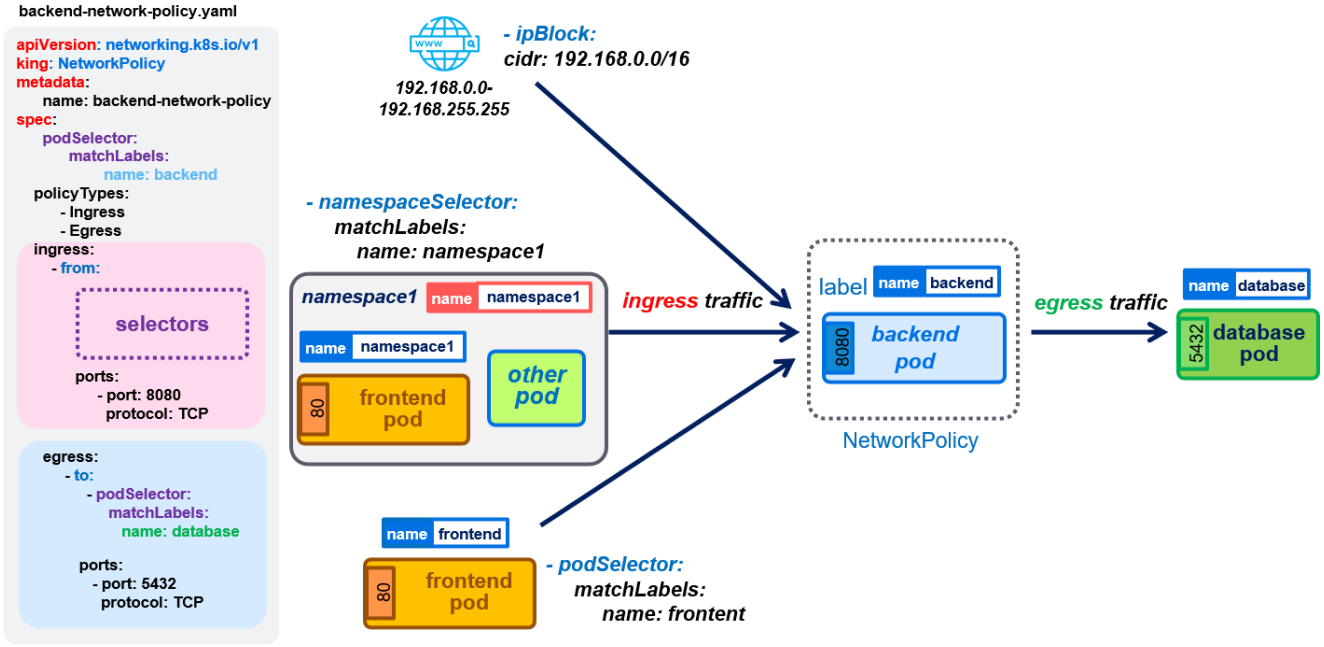


Рекомендация:

“AppArmor и Kubernetes: Настройка проактивной защиты для безопасности приложений”, Сергей Канибор, БЕКОН 2023

NetworkPolicy

Не доверяем логике взаимодействия между приложениями и строго ее ограничиваем по сети



Рекомендация:

“NetworkPolicy — родной межсетевой экран Kubernetes”, Дмитрий Евдокимов, Сергей Канибор

Как за каменной стеной

На все есть достойный ответ

Безопасность образов контейнеров:

- Много известных уязвимостей (1-day)
- Уязвимости в собственном коде (0-day)
- Большая поверхность атаки (Living off the Land (LotL))
- Потенциально вредоносный код (Malware, backdoor, miners)
- Не соответствие лучшим практикам ИБ (Misconfiguration)

Безопасность микросервисов:

- Не соответствие лучшим практикам ИБ (Misconfiguration)

Как за каменной стеной

На все есть достойный ответ

Безопасность образов контейнеров:

- Много известных уязвимостей (1-day)
- Уязвимости в собственном коде (0-day)
- Большая поверхность атаки (Living off the Land (LotL))
- Потенциально вредоносный код (Malware, backdoor, miners)
- Не соответствие лучшим практикам ИБ (Misconfiguration)

Безопасность микросервисов:

- ~~**Не соответствие лучшим практикам ИБ (Misconfiguration)**~~

- **Policy Engine**

Как за каменной стеной

На все есть достойный ответ

Безопасность образов контейнеров:

- ~~**Много известных уязвимостей (1-day)**~~
- ~~**Уязвимости в собственном коде (0-day)**~~
- ~~**Большая поверхность атаки (Living off the Land (LotL))**~~
- ~~**Потенциально вредоносный код (Malware, backdoor, miners)**~~
- ~~**Не соответствие лучшим практикам ИБ (Misconfiguration)**~~

Безопасность микросервисов:

- ~~Не соответствие лучшим практикам ИБ (Misconfiguration)~~

- Policy Engine
- **AppArmor**
- **NetworkPolicy**
  - Native
  - Calico
  - Cilium

Проактивный и реактивный подход к безопасности

Cyber-resilient culture: "In building a cyber-resilient culture, **the role of security is not to stop all incidents. It is to prevent a security incident from impacting the business**."

Vulnerabilities != vulnerable

Заключение

Основные масли

- Новые технологии это не только новые вызовы, но и новые возможности
- Стройте свою безопасность с мыслью, что вас точно взломают
- Policy-as-Code понятно и прозрачно для взаимодействия ИТ и ИБ
- За проактивной защитой будущее

Selectel TechDay

Спасибо за внимание!

Дмитрий Евдокимов
Founder&CTO Luntry

LUNTRY

www.luntry.ru
@Qu3b3
@k8security
de@luntry.ru

k8s (in)security